ExtremeXOS Release Notes

Software Version ExtremeXOS 16.1

Published October 2015

121120-00 Rev 03

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 95134
Tel: +1 408-579-2800
Toll-free: +1 888-257-3000

Table of Contents

Overview 5

New and Corrected Features in ExtremeXOS 16.1 5
RADIUS Authentication and Authorization Enhancements 6
Supported Platforms 6
New CLI Commands 6
Changed CLI Commands 7
ONEPolicy 8
Supported Platforms 8
Limitations 8
New Commands 8
Access Control List (ACL) Library Enhancements 11
Supported Platforms 13
Limitations 13
Class of Service (CoS) 14
Supported Platforms 14
Limitations 14
New CLI Commands 14
Changed CLI Commands 15
Command Usability Enhancements 17
Supported Platforms 17
Limitations 17
New CLI Commands 18
Changed CLI Commands 18
Access Control List (ACL) Two-Stage Policy 24
Platforms Supported 24
Limitations 24
New CLI Commands 25
Security Enhancements 26
Platforms Supported 26
New CLI Commands 27
Changed CLI Commands 27
Generalized Precision Time Protocol (gPTP) Enhancement 28
Limitations 28
Extreme Loop Recovery Protocol (ELRP) Port Shutdown 28
Supported Platforms 28
Limitations 28
Changed CLI Commands 29
Increase of Protocol-Independent Multicast (PIM) Control Packets 29
Supported Platforms 29
OpenFlow Updated Match Conditions and Actions 30
Supported Platforms 30
Alternate Stacking Supported on 1G Variant of Summit X460-G2 Series Switches 30
Supported Platforms 30

Two-Way Active Measurement Protocol (TWAMP) Light 31
Platforms Supported 32
Limitations 32
New CLI Commands 33
Flow Redirects (Policy-Based Routes) Limits Increase 35
Supported Platforms 35
Single Virtual Group for User Access Control Lists (ACLs) 35
Supported Platforms 35
40Gbps LR4 Parallel Single-Mode (PSM) Quad Small Form-Factor Pluggable (QSFP) Optical Transceiver 36
Supported Platforms 36
Changed CLI Commands 36
ExtremeXOS Images for Summit X480 Series Switches 37
New Hardware Supported in ExtremeXOS 16.1 38
Hardware Issues in ExtremeXOS 15.6 and Later 38
CLI Command Output Format of Ports Lists 38
Joint Interoperability Test Command (JITC) Compliance 39
ExtremeXOS Hardware/Software Compatibility and Recommendation Matrices 39
Compatibility with NetSight 39
Upgrading to ExtremeXOS 40
Downloading Supported MIBs 40
Tested Third-Party Products 40
Tested RADIUS Servers 40
Tested Third-Party Clients 41
PoE Capable VoIP Phones 41
Extreme Switch Security Assessment 42
DoS Attack Assessment 42
ICMP Attack Assessment 42
Port Scan Assessment 42
Service Notifications 42

Limits 43

Open Issues, Known Behaviors, and Resolved Issues 97

Open Issues 97
Known Behaviors 101
Resolved Issues in ExtremeXOS 16.1 102

1 Overview

These release notes document ExtremeXOS® 16.1 which adds features, adds supported hardware, and resolves software deficiencies.

This chapter contains the following sections:

- New and Corrected Features in ExtremeXOS 16.1 on page 5
- ExtremeXOS Images for Summit X480 Series Switches on page 37
- New Hardware Supported in ExtremeXOS 16.1 on page 38
- Hardware Issues in ExtremeXOS 15.6 and Later on page 38
- CLI Command Output Format of Ports Lists on page 38
- Joint Interoperability Test Command (JITC) Compliance on page 39
- ExtremeXOS Hardware/Software Compatibility and Recommendation Matrices on page 39
- Compatibility with NetSight on page 39
- Upgrading to ExtremeXOS on page 40
- Downloading Supported MIBs on page 40
- Tested Third-Party Products on page 40
- Extreme Switch Security Assessment on page 42
- Service Notifications on page 42

New and Corrected Features in ExtremeXOS 16.1

This section lists the new and corrected features supported in the ExtremeXOS 16.1 software:

- RADIUS Authentication and Authorization Enhancements on page 6
- ONEPolicy on page 8
- Access Control List (ACL) Library Enhancements on page 11
- Class of Service (CoS) on page 14
- Command Usability Enhancements on page 17
- Access Control List (ACL) Two-Stage Policy on page 24
- Security Enhancements on page 26
- Generalized Precision Time Protocol (gPTP) Enhancement on page 28
- Extreme Loop Recovery Protocol (ELRP) Port Shutdown on page 28

- Increase of Protocol-Independent Multicast (PIM) Control Packets on page 29
- OpenFlow Updated Match Conditions and Actions on page 30
- Alternate Stacking Supported on 1G Variant of Summit X460-G2 Series Switches on page 30
- Two-Way Active Measurement Protocol (TWAMP) Light on page 31
- Flow Redirects (Policy-Based Routes) Limits Increase on page 35
- Single Virtual Group for User Access Control Lists (ACLs) on page 35
- 40Gbps LR4 Parallel Single-Mode (PSM) Quad Small Form-Factor Pluggable (QSFP) Optical Transceiver on page 36

RADIUS Authentication and Authorization Enhancements

The RADIUS client software sends authentication requests using standard mechanisms for PAP, CHAP (RFC 2865 (13)) and EAP (RFC 3579 (12)).

This feature introduces authentication retransmission algorithm capability, which uses two retransmission algorithms in combination: Back-off Round Robin, and simple Round Robin. These retransmission algorithms provide server redundancy.

Eight authentication servers are now supported.

Supported Platforms

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, X450-G2, X440, and X430 series switches
- E4G-200 and E4G-400 cell site routers

New CLI Commands

```
configure radius algorithm [standard | round-robin]

configure [radius | radius-accounting] {mgmt-access
[primary | secondary] | netlogin [primary | secondary] |
<index>} retries <retries>

unconfigure radius-accounting [server index]

unconfigure radius [server index]
```

Changed CLI Commands

Changes are in bold.

configure radius {mgmt-access | netlogin} [primary | secondary | **index**] server [host_ipaddr | **host_ipV6addr** | hostname] {udp_port} client-ip [client_ipaddr | **client_ipV6addr**] {vr vr_name} {**shared-secret** {**encrypted**} secret}

configure radius [primary | secondary **index**] shared-secret {encryptedencrypted_secret | secret}

configure radius-accounting {mgmt-access | netlogin} [primary | secondary |**index**] server [host_ipaddr | **host_ipV6addr** | hostname] {udp_port} client-ip [client_ipaddr | **client_ipV6addr**] {vr vr_name} {**shared-secret** {**encrypted**} secret}

show radius {mgmt-access | netlogin} **{primary | secondary | index}**

show radius-accounting {mgmt-access | netlogin} **{primary | secondary | index}**

ONEPolicy

ONEPolicy allows you create profiles for securing and provisioning network resources based upon the role the user or device plays within the enterprise. By first defining the user or device role, network resources can be tailored to a specific user, system, service, or port-based context by configuring and assigning rules to the policy role. A policy role can be configured for any combination of Class of Service, VLAN assignment, classification rule precedence, or default behavior based upon L2, L3, and L4 packet fields. Hybrid authentication allows either policy or dynamic VLAN assignment, or both, to be applied through RADIUS authorization.

Supported Platforms

- Summit X450-G2
- Summit X460-G2
- Summit X670-G2
- Summit X770

Limitations

- ExtremeXOS only allows policy to be enabled if all the devices in the stack support policy. At the time of configuration a switch provisions the lowest common denominator of functionality. If a switch attempts to join the stack after policy is enabled, it must be able to support the existing level of functionality or it is not allowed to participate in policy.
- Only 'macdest', 'macsource', or 'port' policy rules can be applied to QinQ (that is, double-tagged) packets received on an untagged VMAN port.

New Commands

Policy Commands

```
enable policy

disable policy

configure policy vlanauthorization port [<port_list> |
all] [{enable | disable} {tagged | untagged}]

unconfigure policy vlanauthorization [{port <port_list>} |
all]
```

```
configure policy invalid action [default-policy | drop |
forward]

configure policy port <ports> admin-id <admin_id>

configure policy profile <profile_index> {name <name>}
{pvid <pvid>} {pvid-status <pvid_status>} {cos <cos>}
{cos-status <cos_status>} {egress-vlans <egress_vlan_list>}
{untagged-vlans <untagged_vlans>} {append | clear} {tci-
overwrite <tci_overwrite>}

configure policy rule admin-profile macsource <macsource>
| port <port>] {mask <mask>} { port-string [<port_string>
| all]} {storage-type [non-volatile | volatile]} {admin-
pid <admin_pid>} {tci-overwrite

configure policy rule profile_index | ether ether |
ip6dest ip6dest | ipdest ipdest | ipfrag | ipproto ipproto
| ipsourcesocket ipsourcesocket | iptos iptos | ipttl
ipttl | macdest macdest | macsource macsource | port port
| tcpdestportIP tcpdestportIP | tcpsourceportIP
tcpsourceportIP | udpdestportIP udpdestportIP |
udpsourceportIP udpsourceportIP] {mask mask } {port-string
[port_string | all]} {storage-type [non-volatile |
volatile]} {drop | forward} {cos cos}

configure policy maptable [response [tunnel | policy |
both] | <vlan_list> <profile_index>]

show policy state

show policy allowed-type <ports> {detail}

show policy capability

show policy dynamic override

show policy invalid [all | {action} {count}]

show policy maptable

show policy profile

show policy rule {all | {profile-index <profile_index> |
admin-profile} ether {<ether>} ipdest {<ipdest>} | ipfrag
| ipproto {<ipproto>} | ipsource {<ipsource>} | iptos
{<iptos>} | ipttl {<ipttl>} macdest {<macdest>} |
macsource {<macsource>} | port {<port>} | tcpdestportIP
```

```
{<tcpdestportIP>} | tcpsourceportIP {<tcpsourceportIP>} |
udpdestportIP {<udpdestportIP>} | udpsourceportIP
{<udpsourceportIP>}} {mask <mask>} {port-string
[<port_string> | all]} {storage-type [non-volatile |
volatile]} {drop | forward} {cos <cos> | admin-pid
<admin_pid>}}{detail | wide}

show policy vlanauthorization {port <port_list>}

unconfigure policy all-rules

unconfigure policy maptable [response | <vlan_list>]

unconfigure policy profile [all | <profile_index>]

unconfigure policy vlanauthorization [enable | disable]

unconfigure policy rule [<profile_index>] [all-pid-entries
| ipfrag | icmp6type | icmptype | ip6dest | ipdest |
ipproto | ipsource | iptos | ipttl | macdest | macsource
| port | tcpsourceportIP | udpsourceportIP | tcpdestportIP
| udpdestportIP] [all-traffic-entries | <data>] {mask
<mask>} {port-string <port_string>}]
```

Netlogin Commands

```
configure netlogin idle-timeout {dot1x | mac | web-based}
<timeout>

configure netlogin session-timeout {dot1x | mac | web-
based} <timeout>

configure netlogin ports [all | <port_list>] [allowed-
users <allowed_users> | authentication mode [optional |
required] | trap [all-traps | no-traps | [{success}
{failed} {terminated} {max-reached}]]]

configure netlogin trap max-users [enable | disable]

show netlogin timeout

show netlogin session {all | summary} {mac-address
<mac_address>} {ports <ports>} {agent [dot1x | mac | web-
based]}

show netlogin trap
```

```
unconfigure netlogin [idle-timeout | session-timeout]
{dot1x | mac | web-based}

unconfigure netlogin ports [all | <port_list>] [allowed-
users | authentication mode]

clear netlogin session [{mac <mac_address>} {port
<ports>}] {dot1x | mac | web-based}
```

Access Control List (ACL) Library Enhancements

To implement ONEPolicy requires enhancements to certain existing Access Control List (ACL) conditions and actions, plus the addition of some new ones:

- **ttl**—New condition with optional mask. Matches IPv4 Time-To-Live and IPv6 Hop Limit.

  Syntax: ttl <value> {mask <value>}

- **add-vlan-id**—New action that adds a new outer VLAN ID. If the packet is untagged it adds a VLAN tag to the packet. If the packet is tagged, it adds an additional VLAN tag. Only supported in VLAN lookup stage (VFP).

  Syntax: `add-vlan-id <value>`

- **ip-tos**—Existing condition that now accepts an optional mask.

  Syntax: `ip-tos <value> {mask <value>}`

- **vlan-format**—New condition matches packets based on its VLAN format. Can be one of the four values:

  untagged—all untagged packets

  single-tagged—all packets with only single tag.

  double-tagged—all packets with double tag

  outer-tagged—all packets with at least one tag (single tag or double tag)

  Syntax: `vlan-format <untagged | single-tagged | double-tagged | outer-tagged>`

- **replace-dscp-value**—New action that replaces the existing Differentiated services code point (DSCP) value of the packet.

  Syntax: `replace-dscp-value <value>`

- **ethernet-type**—Existing condition that can now accept an optional mask.

  Syntax: `ethernet-type <value> {mask <value>}`

- **destination-port**—Existing condition that can now accept an optional mask.

  Syntax: `destination-port <value> {mask <value>}`

- **source-port**—Existing condition that can now accept an optional mask.

  Syntax: `source-port <value> {mask <value>}`

- **fragments**—Existing condition that matches any fragment of a fragmented packet, including the first fragment. Previously, this condition didn't include the first fragment.

  Syntax: `fragments`

- **first-fragments**—Existing condition that matches only the first fragment of a fragmented packet. Previously, this condition also matched non-fragmented packets.

  Syntax: `first-fragments`

- **do-ipfix**—New action that records the matching packet. Can be used on both ingress and egress.

  Syntax: `do-ipfix`

- **do-not-ipfix**—New action that cancels recording for the matching packet. Can be used to reduce demand on egress IPFIX capacity (and to reduce recording loss) during packet flooding situations. For example, egress ACLs that recognize broadcast and/or IP multicast packets could prevent egress IPFIX recording. Can be used on both ingress and egress.

  Syntax: `do-not-ipfix`

- **redirect-port-copy-cpu-allowed**—The existing "redirect-port" action in ACL includes three hardware actions: RedirectPort, CopyToCpuCancel and GpDropCancel. Because of this, the "redirect-port" action cannot be used with another actions that try to copy a packet to CPU, like "copy-cpu-sdn". This new action redirects a packet out of an output port, but does not enforce a requirement that Copy to CPU must be canceled.

  Syntax: `redirect-port-copy-cpu-allowed <value>`

- **redirect-port-list-copy-cpu-allowed**—Same as redirect-port-copy-cpu-allowed, but allows redirect to a list of ports.

  Syntax: `redirect-port-list-copy-cpu-allowed <value {,<value>}>`

Supported Platforms

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, X450-G2, X440, and X430 series switches
- E4G-200 and E4G-400 cell site routers

Limitations

- **vlan-format** mistakenly identifies untagged packets as tagged in the IFP stage for the following switches: Summit X480, Summit X650, BlackDiamond 8900-G96T-c, BlackDiamond 8900-10G24X-c, BlackDiamond 8900-G48T-xl, BlackDiamond 8900-G48X-xl, and BlackDiamond 8900-10G8X-xl.
- **fragments** is partially supported on the BlackDiamond G48Te2 I/O modules. On this modules, this condition only matches fragmented packets and the last fragmented packet, and does not match the first fragment of the packet.
- **add-vlan-id**' is only available on switches with VFP stages.
- IPFIX actions are only supported on Summit X460, X460-G2, and X480 series switches, BlackDiamond 8900-xl and -96T modules, and BlackDiamond X8-100G4X and BDX X8 xl-series modules.

Class of Service (CoS)

Class of Service (CoS) prioritizes, rate-limits, rate shapes, and otherwise controls defined traffic types of a switch; it is used as part of a bandwidth management strategy. CoS is an enhancement to the existing Quality of Service (QoS) feature. CoS is typically configured using NetSight through the CoS Management Information Base (MIB).

Supported Platforms

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, X450-G2, X440, and X430 series switches
- E4G-200 and E4G-400 cell site routers

Limitations

- CoS reference tables have a fixed mapping.
- Both global and per-port meters cannot be configured at the same time on platforms that require the port meter map table.
- Per-port meter out-of-profile counters are not accurately supported.
- Flood out-of-profile counters and actions are the aggregate of all flood types (unknown unicast, multicast, and broadcast) for a given port.
- On Summit X670-G2 and X770 series switches and on BlackDiamond X8 modules: BDXB-100G4X, BDXB-100G4X-XL, and BDXB-40G12X-XL, when hybrid scheduling is configured on ports (WxRR with some queues in Strict-Priority), the SP queues must be contiguous.

New CLI Commands

```
create ports group <port_group>

delete ports group <port_group>

configure ports {group} <port_group> [[add|delete]
<port_list>]

show ports group {<port_group>}

unconfigure {meter} <metername> ports [<port_group> |
<port_list>]

clear ports [all|<port_list>|<port_group>] rate-limit flood
out-of-profile {disabled-ports} {status | counter}
```

```
unconfigure cos-index <cos_index> [{qosprofile} {ingress-
meter} {replace-tos}]

show cos-index {<cos_index>}

show meter {<metername>} out-of-profile {{disabled-ports}
ports [<portlist> | <port_group>] | global-count}

clear meter {<metername>} out-of-profile {disabled-ports}
{status | counters} {ports [ all | <portlist> |
<port_group>]}

configure ports [<port_list>|all] dot1p <dot1p_priority>

unconfigure qosscheduler ports [<port_list> | <port_group>
| all]
```

Changed CLI Commands

Changes are shown in bold

```
configure qosscheduler [strict-priority | weighted-round-
robin | weighted-deficit-round-robin] {ports [<port_list> |
<port_group> | all]}

show qosscheduler {ports [<port_list> | <port_group> |
all]}

configure {qosprofile} <qosprofile> [{maxbuffer
<buffer_percentage>} {weight <weight_value> | use-strict-
priority} {ports [<port_list> | <port_group> | all]}]

configure [ {qosprofile} { egress } <qosprofile> | {
qosprofile } ingress [<iqosprofile>]] [{minbw
<minbw_number>} {qos-weight <weight>} {maxbw
<maxbw_number>} | {committed_rate <committed_bps> [K | M]}
{qos-weight <weight>} {peak_rate <peak_bps> [K | M]} ]
{priority [<priority> | <priority_number>]} [ports
[<port_list> | <port_group> | all]]

show qosprofile {ingress | egress} [ports [<port_list> |
all | <port_group>] | NULL]

configure {qosprofile} {egress} <qosprofile> [wred [color
[tcp [green | red] | non-tcp [any | red]] {min-threshold
<min_thresh>} {max-threshold <max_thresh>} {max-drop-rate
<max_drop_rate>} | avg-weight <avg_weight>]] [ports
[<port_list> | <port_group> | all]]
```

```
configure {meter} <metername> [{committed-rate <cir>
<committed-rate-unit> {committed-burst-size <committed-
burst-size> [Kb|Mb]}} {peak-rate <pr> <peak-rate-unit>}
{peak-burst-size <peak-burst-size> [Kb|Mb]} {max-burst-size
<burst-size> [Kb | Mb]}] {out-actions [{disable-port}
{drop | set-drop-precedence {dscp [<dscp-value> | none]}}
{log} {trap}]} {ports [<port_group> | <port_list>]}

show meter {<meter_name>} {ports [<port_group>|port_list>]}
{out-actions}

configure ports [<port_list>|<port_group>] rate-limit
[egress [no-limit | <cir-rate> [Kbps | Mbps | Gbps] {max-
burst-size <burst-size> [Kb | Mb]}] | flood [broadcast |
multicast | unknown-destmac] [no-limit | <pps> {out-
actions [{log} {trap} {disable-port}]}]]

configure dot1p type <dot1p_priority> {qosprofile}
<qosprofile> {ingress-meter [<ing_meter> | none]}

[enable | disable] dot1p replacement ports [<port_list> |
all] {{qosprofile} <qosprofile>}

[enable | disable] diffserv replacement ports [<port_list>
| all] {{qosprofile} <qosprofile>}

show ports {<port_list> | <port_group> | tag <tag>} rate-
limit flood {out-actions | out-of-profile {disabled-ports}}
{no-refresh}
```

For the above command, the show screen for the rate-limit flood configuration now shows the port-group option. A separate screen shows the configured out-actions. Another screen shows a per-port out-of-profile status that indicates that the flood limit is exceeded on the port. Another screen show ports that are disabled.

The `show access-list meter` command now shows per-port meter out-of-profile counters for meters that are applied using ACL rules. The output shows the additional syslog,

The `clear access-list meter` command now allows the clearing of the out-of-profile per-port meters counters. When a per-port meter is specified, it clears the counter for the rule associated with the meter.

The `show port information details` command displays the default dot1p priority used for the internal priority for untagged traffic on a

specified port. Additionally, it displays the per-port/per-qosprofile dot1p and diffserv examination status.

Command Usability Enhancements

This feature changes a select set of commands so that you may specify VLANs by VID instead of by name. Some commands allow you to specify a list of VIDs.

Additionally, ExtremeXOS 16.1 introduces a new **`show system`** command that aggregates the output of the following commands:

- `show switch`
- `show version`
- `show temperature`
- `show power`
- `show fans`
- `show odometers`

Additionally, there is a new **`cli refresh`** command to set the auto refresh behavior for certain **`show`** commands. The **`cli refresh`** command controls the default behavior of show commands that have no-refresh/refresh options if neither is specified. Previously, these show commands had only a no-refresh option, but now have both so that the global setting can be overridden.

Finally, there is a new command, **`configure cli [{lines height} {columns width}`**, that configures the number of lines and columns for the current logon session only.

Supported Platforms

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, X450-G2, X440, and X430 series switches
- E4G-200 and E4G-400 cell site routers

Limitations

- For commands that accept a list of VIDs, if some VIDs in the list are unresolveable, the command continues to execute for the remaining VIDs.
- The command **`show configuration`** shows the individual commands with the VLAN names, not VIDs or VID lists.

New CLI Commands

```
show system

[enable | disable] cli refresh {session | permanent}

configure cli [{lines height} {columns width}]
```

Changed CLI Commands

The following commands are modified to allow you to specify VLANs by VID (or a list of VIDs) instead of by name:

```
configure mirror {<mirror_name>} add [vlan <vlan_id>
{ingress | [port <port> {ingress}} | port <port> vlan
<vlan_id> {ingress}]

configure mirror {<mirror_name>} delete [vlan <vlan_id>
{port <port>} | port <port> vlan <vlan_id>]

configure vlan <vlan_id> add secondary-ipaddress
[<ipaddress> {<netmask>} | <ipNetmask>]

configure vlan <vlan_id> delete secondary-ipaddress [all |
<ipaddress>]

configure vlan <vlan_id> ipaddress [<ipaddress> {<netmask>}
| <ipNetmask>]

configure vlan <vlan_id> name <new_name>

clear l2stats vlan <vlan_list>

configure ip-mtu <mtu> vlan <vlan_list>

configure ports [<port_list> | all] monitor vlan
<vlan_list> {rx-only | tx-only}

configure ports <port_list> {tagged} vlan <vlan_list>
[limit-learning <number> {action [blackhole | stop-
learning]} | unlimited-learning]

configure ports <port_list> {tagged} vlan <vlan_list>
[lock-learning | unlock-learning]

configure vlan <vlan_list> add ports [<port_list> | all]
{tagged | untagged | private-vlan translated}
```

```
configure vlan <vlan_list> delete ports [<port_list> |
all]

configure vlan <vlan_list> protocol {filter} <filter_name>

configure vlan <vlan_list> {qosprofile} [<qosprofile> |
none]

create vlan <vlan_list> {vr <vr-name>} {description <vlan-
desc>}

delete vlan <vlan_list>

[enable | disable] iparp gratuitous protect vlan
<vlan_list>

[enable | disable] ipforwarding {ipv4 | ipv6} vlan
<vlan_list>

[enable | disable] learning vlan <vlan_list>

[enable | disable] loopback-mode vlan <vlan_list>

[enable | disable] vlan <vlan_list>

unconfigure vlan <vlan_list> ipaddress

configure vman <vman_id> add ports [<port_list> | all]
{tagged | untagged {port-cvid <port_cvid>} | cep cvid
<cvid_first> {- <cvid_last>} {translate <cvid_first_xlate>
{- <cvid_last_xlate>}}}

configure vman <vman_id> ipaddress [<ipaddress> {<netmask>}
| <ipNetmask>]

configure vman <vman_id> ports [<port_list> | all] add
cvid <cvid_first> {- <cvid_last>} { translate
<cvid_first_xlate> {- <cvid_last_xlate>}}

configure vman <vman_id> name <new_name>

configure vman <vman_list> delete ports [<port_list> |
all]

configure vman <vman_list> ports [<port_list> | all]
delete cvid <cvid_first> {- <cvid_last>}

configure vman <vman_list> protocol {filter} <filter_name>
```

```
configure vman <vman_list> {qosprofile} [<qosprofile> |
none]

create vman <vman_list> {vr <vr-name>} {description <vlan-
desc>}

delete vman <vman_list>

[enable | disable] learning vman <vman_list>

unconfigure vman <vman_list> ipaddress

show ip dad vlan <vlan_list> {tentative | valid |
duplicate}

show ipv6 dad vlan <vlan_list> {tentative | valid |
duplicate} {detail}

show l2stats vlan <vlan_list>

show vlan <vlan_list> statistics

show [vlan <vlan_list> | vman <vman_list>] {ipv4 | ipv6}

configure vlan <vlan_list> add ports [all | <port_list>]
{tagged | untagged} {stpd} <stpd_name> {dot1d | emistp |
pvst-plus}

configure {stpd} <stpd_name> add vlan <vlan_list> ports
[all | <port_list>] {dot1d | emistp | pvst-plus}

configure {stpd} <stpd_name> delete vlan <vlan_list> ports
[all | <port_list>]

[enable | disable] {stpd} <stpd_name> auto-bind vlan
<vlan_list>

show vlan <vlan_list> stpd {blocked-ports}

show fdb vlan <vlan_list> {netlogin [all | mac-based-
vlans]}}

show fdb stats vlan <vlan_list>

show iparp security vlan <vlan_list>

show iparp stats vlan <vlan_list>

show iparp vlan <vlan_list>
```

```
show neighbor-discovery {cache {ipv6}} vlan <vlan_list>

show vlan <vlan_list> security

show netlogin {port <portlist>} vlan <vlan_list>

show netlogin {port <portlist>} vlan <vlan_list> dot1x
detail

show netlogin guest-vlan <vlan_list>

show netlogin authentication [service-unavailable |
failure] vlan <vlan_list>

show ip-security arp learning vlan <vlan_list>

show ip-security arp validation vlan <vlan_list>

show ip-security arp validation violations vlan
<vlan_list> ports [<ports> | all]

show ip-security dhcp-snooping vlan <vlan_list>

show ip-security dhcp-snooping entries vlan <vlan_list>

show ip-security dhcp-snooping information-option circuit-
id vlan-information vlan <vlan_list>

show ip-security dhcp-snooping violations vlan <vlan_list>
```

The following show commands are modified so that you can now, per command, set the auto refresh behavior:

```
debug hal show ports {<port_list>} qosmonitor { congestion
} { no-refresh | refresh }

show fdb stats [ports {all | <port_list>} | vlan {all} |
{vlan} <vlan_name> ] {no-refresh | refresh}

show iparp stats [[ <vr_name> | vr {all | <vr_name>} ]
{no-refresh | refresh} | {vr} summary ]

show iparp stats [vlan {all {vr <vr_name>}} | {vlan}
<vlan_name>] {no-refresh | refresh}

show iparp stats ports {all | <port_list>} {no-refresh |
refresh}
```

```
show fdb mac-tracking statistics {<mac_addr>} {no-refresh
| refresh}

show trill ports {<port_list>} [counters {no-refresh |
refresh | detail}]

show ports {<port_list> | tag <tag>} collisions { no-
refresh | refresh } {port-number}

show ports {<port_list> | tag <tag>} configuration { no-
refresh | refresh } {port-number}

show ports { <port_list> | tag <tag> | stack-ports {
<stack_port_list> } } txerrors { no-refresh | refresh }
{port-     number}

show ports {<port_list> | tag <tag>} packet {no-refresh |
refresh } {port-number}

show ports {<port_list> | tag <tag>} wan-phy errors {no-
refresh | refresh }

show ports {<port_list> | tag <tag>} wan-phy events {no-
refresh | refresh }

show ports {<port_list>} wan-phy overhead { no-refresh |
refresh } {port-number}

show ports { <port_list> | tag <tag> | stack-ports {
<stack_port_list> } } rxerrors { no-refresh | refresh }
{port-     number}

show ports {<port_list> | tag <tag>} anomaly { no-refresh
| refresh } {port-number} "

show ports {<port_list> | <port_group> | tag <tag>} rate-
limit flood {out-actions | out-of-profile {disabled-ports}}
{ no-refresh | refresh } {port-number}

show ports {<port_list>} ip-fix { no-refresh | refresh }
{port-number}

show ports { <port_list> | tag <tag> | stack-ports {
<stack_port_list> } } statistics { no-refresh | refresh }
{ wide   } {port-number}
```

```
show ports {<port_list> | tag <tag> } qosmonitor {egress |
ingress} { congestion } { packets | bytes } { no-refresh
|   refresh } {port-number}

show ports {<port_list> | tag <tag> } flow-control {rx-
pauses | tx-pauses} { no-refresh | refresh } {port-number}

show ports {<port_list>} wred { no-refresh | refresh }
{port-number}

show ports {<port_list>} eee { no-refresh | refresh }
{port-number}

show ports {<port_list> | tag <tag> } congestion { no-
refresh | refresh} {port-number}

show ports {<port_list>} vlan statistics { no-refresh |
refresh } {port-number}

show [vlan | {vlan} <vlan_name>] statistics {no-refresh |
refresh}

show ports {<port_list> | tag <tag> } {no-refresh |
refresh}

show ports {<port_list>} tdm errors {near-end} {total |
intervals | current {no-refresh | refresh}}

show ports {<port_list>} tdm configuration {no-refresh |
refresh} {port-number}

show ports {<port_list>} tdm {no-refresh | refresh}

show ports {<port_list>} tdm alarms {no-refresh | refresh}

show ports {<port_list>} dot1p out-of-profile {disabled-
ports} {no-refresh | refresh}

show ces {<ces_name>} errors {total | intervals |
dayIntervals | current {no-refresh | refresh}}
```

Access Control List (ACL) Two-Stage Policy

This feature exposes the VLAN Content Aware Processor/VLAN Filter Processor (VCAP/VFP) using the ExtremeXOS Access Control List (ACL) manager.

The VCAP/VFP is used to filter packets before ingress processing. It can be used to assign the VLAN, set a class ID, or perform other more traditional ACL actions, such as drop or count. In general, this stage's scale, actions, and match criteria are more limited than the ingress stage.

Platforms Supported

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, and X450-G2 series switches
- E4G-200 and E4G-400 cell site routers

Limitations

- The VFP match criteria, scale, and actions are more limited than that of the regular ingress ACLs—Ingress Content Aware Processor/ Ingress Filter Processor (ICAP/IFP).
- Rule actions in the VFP can be overridden by rule actions in the IFP.
- Packets are always presented to the IFP even when the VFP drops the packet
- The 'vlan-id' match criteria only works on packets received with an 802.1Q tag in the packet.

New CLI Commands

New ACL action modifier:

```
class-id <value 0-4095>
```

This action can be specified on any rule within a policy file or within a list of dynamic access-lists. When specified, this action signifies that the rule is installed in the “LOOKUP stage” access-list resource (VFP).

New ACL match criteria:

```
class-id <value 0-4095>
```

This match condition can be specified on any rule within a policy file or within a list of dynamic access-lists. A rule cannot both match a class-id and specify a class-id as an action. When a “class-id” match criteria is specified, the associated rule is programmed into the normal “INGRESS stage” access-list hardware resource (IFP).

Security Enhancements

This feature includes the following changes and enhancements:

- Configurable timed lockout that is applied to accounts after a configurable number of failed logon attempts.
- Stronger hash algorithm for account passwords.

NOTE

Due to the stronger hash algorithm, if you create accounts in ExtremeXOS 16.1, and then downgrade to versions earlier than ExtremeXOS 16.1, you may encounters problems using the passwords for these accounts.

For more information about this issue, visit: http://extr.co/1KfSszY.

- Removal of unmasked passwords in the command line interface.
- Stronger obfuscation of RADIUS and TACACS+ shared secrets.
- Integrity checking of downloaded images.
- Syslog alert issued when a configurable percentage of the Syslog memory buffer is filled.
- Optionally restricting the use of "`show log`" and "`show diagnostics` commands by non-administrator accounts.
- The "safe defaults" script (unconfigured switch startup wizard) enables these new options collectively, as well as forcing the user to change the default administrator and failsafe passwords.

Platforms Supported

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, X450-G2, X440, and X430 series switches
- E4G-200 and E4G-400 cell site routers

New CLI Commands

```
configure account [all | <name>] password-policy lockout-
time-period [<num_mins> | until-cleared]

configure log target memory-buffer alert percent-full
[<percent> | none]

configure cli password prompting-only [on | off]

configure log messages privilege [admin | user]

configure diagnostics privilege [admin | user]
```

Changed CLI Commands

The output of the this command now displays account lockout time period information:

```
show accounts password-policy
```

If a downloaded image does not have a signature, a warning message appears. You may choose to continue or terminate the installation:

```
download image [[<hostname> | <ipaddress>] <filename>
{{vr} <vrname>} {block-size <block_size>} | memorycard
<filename>] {<partition>} {msm <slotid> | mm <slotid> |
slot <slot-number>}
```

The log buffer percentage full and configurable percentage threshold information appears in the output of the following command:

```
show log configuration {target { upm {<upm_profile_name>}
| xml-notification {<xml_target_name>} | console | session
| memory-buffer | primary-msm | primary-mm | primary-node
| backup-msm | backup-mm | backup-node | nvram | syslog
{<ipaddress>|<ipPort>} {vr <vr_name>} {<local>} } | filter
{<filter-name>}}
```

The following command shows the current password prompting setting:

```
show management
```

Generalized Precision Time Protocol (gPTP) Enhancement

Previously, the number of Generalized Precision Time Protocol (gPTP)-capable ports was static. Switches now handle a variable number of ports based on the number of ports on the switch.

Limitations

- ExtremeXOS 16.1 slave ports synchronize to grandmasters, such as Symmetricom, and to other ExtremeXOS 16.1 clocks, but not to ExtrememXOS 15.7, and earlier. If networks of clocks are to be upgraded to ExtremeXOS 16.1, complete the upgrades simultaneously or staged starting closest to the grandmaster. Before beginning a staged upgrade, where an earlier version of ExtremeXOS must synchronize to an ExtremeXOS 16.1 clock, test the particular configuration beforehand.
- ExtremeXOS 16.1 slave clock ports must be configured with the "slave-only" option to synchronize to other ExtremeXOS 16.1 clocks.

Extreme Loop Recovery Protocol (ELRP) Port Shutdown

Extreme Loop Recovery Protocol (ELRP) detects loops by sending out an ELRP protocol data units (PDUs) out of one or more ports of a particular VLAN. ELRP takes system MAC addresses, changes them to a broadcast MAC address by appending "01:" to the front, and then sends out the PDUs. If PDUs are received back by ELRP, a loop is present. Each ELRP PDU is sent on a particular VLAN, so you must configure each VLAN that you wish to monitor.

In this ELRP enhancement, when a loop is detected using ELRP, an option to disable the port where the ELRP packet egresses is added to suppress the loop. You may specify a duration, which after it expires, the ports are enabled, or you can keep the ports disabled permanently until you choose to enable them.

Supported Platforms

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, X450-G2, X440, and X430 series switches
- E4G-200 and E4G-400 cell site routers

Limitations

- Entire port is blocked regardless of which VLAN that the loop was detected on.

Changed CLI Commands

Changes are shown in bold.

configure elrp-client periodic <vlan> ports <{portlist} | all> {interval <seconds>} [log |log-and-trap | trap] {disable-port {egress | ingress} {duration {<seconds>} | permanent}}

The output of the **show elrp** command now shows egress/ingress information in the "Action" column and there is a new column (Disable Port) showing disabled port status.

The output of the **show elrp disabled-ports** command now shows egress/ingress information in the new "Disable Direction" column.

Increase of Protocol-Independent Multicast (PIM) Control Packets

Previously, ExtremeXOS Protocol-Independent Multicast (PIM) implementation sends maximum 1,500 byte-size control packets that can accommodate 175 sources per multicast group.

The size of these control packets has now been increased to accommodate 3,000+ sources per group. This large control packet is fragmented at the IP layer and reassembled at the received node.

Supported Platforms

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, X450-G2, X440, and X430 series switches
- E4G-200 and E4G-400 cell site routers

OpenFlow Updated Match Conditions and Actions

ExtremeXOS 16.1 includes an upgrade to OpenFlow v1.3 by upgrading from version 1.4 to 2.1 of OpenVswitch. The match conditions and actions tables change as result of this upgrade.

Supported Platforms

- BlackDiamond X8 [all modules; single Master Switch Fabric Module (MSM) only]
- BlackDiamond 8800 [8900 (XL-series) and C-series; single Management Module (MM) only]
- Summit X770, X670, X480, X460, and X440

Alternate Stacking Supported on 1G Variant of Summit X460-G2 Series Switches

Alternate stacking is now available for 1G oriented Summit X460-G2 series switches with 10G VIM modules (VIM-2T or VIM-2X).

Supported Platforms

- Summit X460-G2-24t-GE4
- Summit X460-G2-24p-GE4
- Summit X460-G2-48t-GE4
- Summit X460-G2-48p-GE4

Two-Way Active Measurement Protocol (TWAMP) Light

This features is the light version of TWAMP, which is an industry standard (RFC 5357) for measuring round-trip performance between two devices that support the TWAMP protocols. TWAMP defines two protocols: the TWAMP-Control protocol and the TWAMP-Test protocol. The TWAMP-Control protocol is used to set up test sessions. The test sessions use the TWAMP-Test protocol to transmit and reflect performance measurement packets. The TWAMP-Control protocol uses TCP for communication, while the TWAMP-Test protocol uses UDP.

TWAMP defines four logical roles; Session-Sender, Session-Reflector, Server, and Control-Client. These logical roles can be split between two entities to form a client/server paradigm (referred to as the two-host implementation in the RFC). The logical roles of the Control-Client and the Server communicate using the TWAMP-Control protocol to set up test sessions. Each test session consists of a transmitter and a reflector, fulfilled by the logical roles of Session-Sender and Session-Reflector respectively.

The Control-Client initiates a TCP connection to the well-known TWAMP-Control port 862. After the TCP connection is established, the Server transmits the first message by sending the 'Server Greetings' message. The Control-Client responds with a 'Setup Response' message. The three-way TWAMP-Control handshake is completed when the Server responds with the 'Server Start' message. The 'Control-Client' is now able to transmit command messages to the Server.

The test sessions are set up using the 'Request-Session' command message, sent from the Control-Client to the Server. The Server replies with an 'Accept Session' message, which indicates if the Server is capable of accommodating the request. The Control-Client may send several 'Request-Session' command messages to set up multiple test sessions. To begin the tests, the Control-Client transmits a 'Start-Session' command message. The Server replies with a 'Start-Ack' message. The Control-Client does not begin its test until it receives the 'Start-Ack' message. This allows the Server ample time to configure the test sessions. The Control-Client stops the test sessions with a 'Stop-Sessions' message. The Server does not respond to this message.

This feature, TWAMP Light, consists of the TWAMP logical role of the Session-Reflector as defined in Appendix I of RFC 5357. This light version of TWAMP contains two entities: the Client entity takes on the TWAMP logical roles of Session-Sender, Server, and Control-Client, while the Server takes on the TWAMP logical role of the Session-Reflector. To establish TWAMP Light, you must configure endpoints, which define the destination of TWAMP-Test packets generated by the Client. An endpoint receiving a new TWAMP-Test packet creates a test session consisting of the following four-part tuple; client IP address, client UDP port, endpoint IP address, and endpoint UDP port. The tuple does not include the VR because it requires the Default VR for the first phase. A session timeout value, configured globally, determines the amount of time test sessions exist after the last reception of a TWAMP-Test packet. Test sessions are used to keep track of the session data, such as the sequence number. The Session-Reflector still responds to TWAMP-Test packets that do not match an existing test session or if a new test session cannot be created due to lack of resources.

Platforms Supported

- Summit X440, X460
- BlackDiamond 8800 with MSM128 and MSM48c

Limitations

- Endpoints may only be created on the default virtual router (VR-Default)
- Limit of 256 endpoints
- Maximum of 2,000 test sessions
- TWAMP-Test error-estimate field does not reflect Network Time Protocol (NTP) or Simple Network Time Protocol (SNTP) timing values

New CLI Commands

`[enable | disable] twamp reflector`

This command enables or disables the Session-Reflector. If you disable the Session-Reflector, the application terminates all current TWAMP test sessions.

`configure twamp reflector sessions <count> timeout <ref_wait>`

This command allows you to modify the number of test sessions to support and timeout value for those test sessions. The timeout value is the REFWAIT value specified in RFC5357.

`<count>`: range 0 – 2000 entries; default 2000

`<ref_wait>`: range 30 – 3600 seconds; default 900 seconds

`(un)configure twamp [add|delete] endpoint {vr <name>} ipaddress <ip> port <udp_port>`

This command allows you to configure and unconfigure the TWAMP endpoints. You specify the IP address and UDP port number for the endpoint. Removing the endpoint terminates all test sessions associated with the endpoint.

`<ip>`: The endpoint IP address, either IPv4 or IPv6

`<udp_port>`: The UDP port the endpoint listens on; range is 1,025–65,535

`<name>`: An optional VR may be used; default is VR-Default

```
show twamp reflector
```

This command displays the configured values and runtime information of the Session-Reflector and its endpoints:

```
Session Information
  Used: 165 of 200
  Timeout: 300 seconds
Endpoints Port  Sessions Rx Packets Tx Packets
-------------------------------------------------------------
19.1.1.100 5000  5          3091          3091
19.1.1.100 5001  40         5521          5521
19.1.1.100 5002  40         4728          4728
19.1.1.100 5003  40         3916          3916
18.1.1.100 5000  40         9266          9266

Displayed 5 endpoints
show twamp endpoint ipaddress <ip> port <udp_port>
```

This command displays the endpoint configured values, runtime data, and test session information. Specifying an IP address and port are optional:

```
TWAMP Endpoint
Endpoint Information
     Local Address: 19.1.1.100Listening Port:    5000
     Received Packets: 7948Transmitted Packets: 7948
     Active Sessions: 5

Session created on Thu Nov 13 15:41:49 2014
     Peer Address: 19.1.1.2  Port: 11001
     Sequence Number: 1575  Last recv'd packet: 84ms

Session created on Thu Nov 13 15:41:49 2014
     Peer Address: 19.1.1.2Port: 11002
     Sequence Number: 1555Last recv'd packet: 16ms
Session created on Thu Nov 13 15:41:49 2014
     Peer Address: 19.1.1.2Port: 11003
     Sequence Number: 1595Last recv'd packet: 241ms
```

```
Session created on Thu Nov 13 15:41:49 2014
     Peer Address: 19.1.1.2Port: 11004
     Sequence Number: 1729Last recv'd packet: 249ms

Session created on Thu Nov 13 15:41:49 2014
     Peer Address: 19.1.1.2Port: 11005
     Sequence Number: 1489Last recv'd packet: 15ms

Displayed 5 sessions
```

Flow Redirects (Policy-Based Routes) Limits Increase

The limit of number of flow redirects and flow redirect next hops has been increased. This allows you to install many more policy-based routes in the switch.

The number of flow redirects was limited to 256; that limit is increased to 4,096. The number of next hops was limited to 32 per flow redirect; this limit is increased to 4,096 next hops cumulatively across all flow redirects.

Supported Platforms

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, X450-G2, X440, and X430 series switches
- E4G-200 and E4G-400 cell site routers

Single Virtual Group for User Access Control Lists (ACLs)

This feature allows you to put all user rules into a single virtual group to prevent multiple rule matches and allow only the highest priority rule to do the matching and execute its actions.

Supported Platforms

- BlackDiamond X8 and BlackDiamond 8800 series switches
- Summit X770, X670, X670-G2, X480, X460, X460-G2, X450-G2, X440, and X430 series switches
- E4G-200 and E4G-400 cell site routers

40Gbps LR4 Parallel Single-Mode (PSM) Quad Small Form-Factor Pluggable (QSFP) Optical Transceiver

This feature adds support for the LR4 Parallel Single Mode (PSM) Quad Small Form-Factor Pluggable (QSFP) optical transceiver on 40G optical QSFP+ ports. Running in 4 × 10g mode allows gives you the capability of having four independent transmit and receive channels, each capable of 10Gbps operation over a 10km single mode fiber hydra MPO to 4xLC duplex patch cord terminated with standard 10G LR SFP+ optical transceivers.

Supported Platforms

- Black Diamond X8 Switch and Black Diamond 8900 series switches
- Summit X770, X460-G2, and X480 series switches
- Summit X670-G2-48x (stacked)

Changed CLI Commands

The following commands' output now display the PSM QSFP media type when detected:

```
show port configuration
```

```
show port transceiver information detail
```

ExtremeXOS Images for Summit X480 Series Switches

Due to additional functionality and new platforms supported, the ExtremeXOS 15.6 and later software image is too large to download onto the Summit X480 series switches. To resolve this issue, Summit X480 series switches now have two separate software image files used for both individual switches and stacks that include Summit X480 series switches.

Table 1: Summit X480 Series Switches Software Image Files

	Main Install image	Diagnostic image
Content	All Summit X480 content (except diagnostics)	Summit X480 diagnostics
File Name	`summitX480-16.1.xx.yy.xos`	`summitX480-16.1.xx.yy-diagnostics.xmod`
File Type	Standard ExtremeXOS image	XMOD image
Installation Notes	• Installing the main SummitX480 image over a previous release leaves the previous installation of the diagnostics image intact, as it is stored separately from the main ExtremeXOS image. You can continue to use the previously installed diagnostic version to run diagnostics. • The Summit XMODs, such as SSH can be used with the summitX480 ExtremeXOS image.	To update to a newer version of the diagnostics, you download and install the latest XMOD version. The diagnostics XMOD can be installed to the active or standby partition and diagnostics can be used immediately. There is no need to reboot or any other action to complete the installation.

The following scenarios will produce an error or warning message:

- Not having the diagnostic image installed on a Summit X480 series switch or slot.
- Installing the main Summit X480 image without the diagnostics image present.
- Installing the general Summit image (`summitX-16.1.xx.yy.xos`, rather than the Summit X480-specific image) on a Summit X480 series switch.

NOTE

If Summit X480 series switches require rescue recovery, you can use the `summitX-16.1.xx.yy.xos` file image, and this image installs the diagnostics capability.

New Hardware Supported in ExtremeXOS 16.1

This section lists the new hardware supported in ExtremeXOS 16.1:

- BDXB-40G12X-XL I/O, BDXA-G48T, and BDXA-G48X modules for the BlackDiamond X8 series switches
- Summit X450-G2 series switches:

  24t-10GE4, 24p-10GE4, 48t-10GE4, 48p-10GE4, 24t-GE4, 24p-GE4, 48t-GE4, 48p-GE4

Hardware Issues in ExtremeXOS 15.6 and Later

The E4G-200 cell site router front panel alarm DB15 connector capabilities are not currently supported.

CLI Command Output Format of Ports Lists

For ExtremeXOS 16.1 and later, the output of CLI commands showing ports lists does not display spaces between commas.

For example: “3:1,7:13” instead of “3:1, 7:13”

Joint Interoperability Test Command (JITC) Compliance

If you require Joint Interoperability Test Command (JITC) compliance, you can use the command `configure snmp compatibility get-bulk reply-too-big-action [standard | too-big-error]` to change ExtremeXOS from Ridgeline-compatible mode (`standard`), the default mode, to JITC-compliant mode (`too-big-error`).

Please note that switching to JITC-compliant mode causes Ridgeline to display potentially unreliable information.

ExtremeXOS Hardware/Software Compatibility and Recommendation Matrices

The *ExtremeXOS Hardware/Software Compatibility and Recommendation Matrices* 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 *ExtremeXOS Hardware/Software Compatibility and Recommendation Matrices* also provides information about which optics are supported on which hardware platforms, and the minimum software version required.

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

www.extremenetworks.com/documentation

Compatibility with NetSight

ExtremeXOS 16.1 is compatible with NetSight version 6.2.0.220 and later.

Upgrading to ExtremeXOS

For instructions about upgrading ExtremeXOS software. see the "Software Upgrade and Boot Options" chapter in the *ExtremeXOS User Guide*. The 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.
- SummitX software is required for E4G cell site routers.
- Beginning with ExtremeXOS 15.4, a limited hitless upgrade procedure is supported on the BlackDiamond X8 and BlackDiamond 8800 series switches
- For Summit X480 series switches, starting with ExtremeXOS 15.6, two separate software image files are used for both individual switches and stacks that include Summit X480 series switches. For more information, see ExtremeXOS Images for Summit X480 Series Switches on page 37.

Downloading Supported MIBs

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

https://esupport.extremenetworks.com/

Tested Third-Party Products

This section lists the third-party products tested for ExtremeXOS 16.1.

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:

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

2 Limits

This chapter summarizes the supported limits in ExtremeXOS 16.1.

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 books.

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	8
Access lists (meters)—maximum number of meters.	BlackDiamond 8000 series	
	e-series, group of 24 ports	512
	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 a-series modules	512 ingress, 512 egress
	BlackDiamond X8-100G4X and BDX X8-100G4X-XL modules	8,192 ingress, 1,024 egress
	BlackDiamond BDXB-40G12X-XL per group of 3 ports	8,192 ingress, 1,024 egress
	E4G-200	1,024 ingress 256 egress
	Summit X440, X430 per group of 24 ports	512 ingress
	Summit X460, E4G-400, per group of 24 ports	2,048 ingress, 256 egress
	Summit X480	4,096 ingress, 512 egress
	Summit X670 with VIM4-40G4x Summit X480 with VIM3-40G4X	512 ingress 512 egress
	Summit X460-G2, X450-G2	1,024 ingress, 512 egress
	Summit X770, X670-G2	1536 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	
	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 a-series modules	2,048 ingress, 1,024 egress
	BlackDiamond XB-100G4X modules	8,192 ingress, 1,024 egress
	BlackDiamond XB-100G4X-XL modules	139,264 ingress 1,024 egress
	BlackDiamond XB-40G12X-XL modules per group of 3 ports	139,264 ingress 1,024 egress
	BlackDiamond BDXB-40G12X-XL modules per group of 3 ports	139,264 ingress 1,024 egress
	Summit X440, X430 group of 24 ports	1,024 ingress
	Summit X460, E4G-400	4,096 ingress, 512 egress
	Summit X480	(up to) 61,440 ingress, 1,024 egress
	Summit X670	
	VIM4-40G4x	2,048 ingress 1,024 egress
	Summit X480	8,192 ingress/ 1,024 egress
	Summit X480	2048 ingress
	VIM3-40G4X	1024 egress
	Summit X770, X670-G2, X460-G2, X450-G2	4,096 ingress 1,024 egress
	E4G-200	2,048 ingress/ 512 egress

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Access lists (policies)—maximum number of rules in a single policy file in first stage (VFP)	Summit X450-G2, X460-G2, X460, X480, E4G-400	2,048 ingress only
	Summit X670-G2, X770, E4G200, X670	1,024 ingress only
Access lists (slices)—number of ACL slices.	BlackDiamond 8000 series	
	c-series, group of 48 ports	16
	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 a-series modules	10 ingress, 4 egress
	BlackDiamond X8-100G4X modules	16 ingress, 4 egress
	BlackDiamond XB-100G4X-XL modules	17 ingress, 4 egress
	E4G-200	8 ingress, 4 egress
	Summit X440, X430	4 ingress
	Summit X460, E4G-400, X460-G2, X450-G2	16 ingress, 4 egress
	Summit X480	17[b] ingress, 4 egress
	Summit X670	10 ingress, 4 egress
	VIM4-40G4x	
	Summit X480	10 ingress, 4 egress
	VIM3-40G4X	12 ingress 4 egress
	Summit X770, X670-G2	
Access lists (slices)—number of ACL slices in first stage (VFP)	Summit X450-G2, X460-G2, X670-G2, X770, E4G-200, E4G-400, X460, X480, X670	4 Ingress only

Table 2: Supported Limits (Continued)

Metric	Product	Limit
ACL Per Port Meters—number of meters supported per port.	Summit X430, X440	8
	Summit X450-G2, X460, X460-G2, X480, X670, X670-G2, X770	16
	E4G-200	8
	E4G-400	16
	BlackDiamond X8, BlackDiamond 8800	16
Meters Packets-Per-Second Capable	Summit X430, X440, X450-G2, X460, X460-G2, X670, X670-G2, X770	Yes
	Summit X480	No
	E4G-200, E4G-400	Yes
	BlackDiamond X8, BlackDiamond 8800 (8900-40G6X-c only)	Yes
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, X460-G2, X450-G2	1,024
	Summit X670, X670-G2	4,096
	Summit X430	100*
BFD sessions—maximum number of BFD sessions.	All platforms (default timers—1 sec)	512
	BlackDiamond X8 and 8800 (minimal timers—50 msec)	10[c]
	All Summits (minimal timers—100 msec)	10[c]
BGP (aggregates)—maximum number of BGP aggregates.	All platforms (except E4G-200, X430, X440, and X450-G2) with Core license or higher	256
BGP (networks)—maximum number of BGP networks.	All platforms (except E4G-200, X430, X440, and X450-G2) with Core license or higher	1,024
	BlackDiamond X8 series	1,024
BGP (peers)—maximum number of BGP peers. **NOTE:** With default keepalive and hold timers.	BlackDiamond X8 series	512
	BlackDiamond 8000 series	512
	BlackDiamond xl-series	512
	All Summits, except X450-G2, X480, X440, X430, E4G-200	128*
	E4G-400	128*
	Summit X480	512

Table 2: Supported Limits (Continued)

Metric	Product	Limit
BGP (peer groups)—maximum number of BGP peer groups.	BlackDiamond 8900 series BlackDiamond 8800 BlackDiamond X8 series Summit X480 Summit X770, X670-G2, X670v-48t, X670, X460-G2, X460 (with Core license or higher)	128 64 128 128 64
BGP (policy entries)—maximum number of BGP policy entries per route policy.	All platforms (except E4G-200, X430, X440, and X450-G2) with Core license or higher	256
BGP (policy statements)—maximum number of BGP policy statements per route policy.	All platforms (except E4G-200, X430, X440, and X450-G2) with Core license or higher	1,024
BGP multicast address-family routes—maximum number of multicast address-family routes.	BlackDiamond 8900 xl-series BlackDiamond X8 series BlackDiamond X8 xl-series Summit X460, X460-G2, X670, X670-G2, X770 Summit X480 E4G-400	524,256 (up to)[b] 25,000 1,048,544 (up to)[i] 25,000 524,256 (up to)[b] 25,000
BGP (unicast address-family routes)—maximum number of unicast address-family routes.	BlackDiamond 8900 xl-series BlackDiamond X8 series BlackDiamond X8 xl-series Summit X460, X460-G2, X670, X670-G2, X770 Summit X480 E4G-400	524,256 (up to)[b] 25,000 1,048,544 (up to) [i] 25,000 524,256 (up to)[b] 25,000
BGP (non-unique routes)—maximum number of non-unique BGP routes.	BlackDiamond 8900 xl-series BlackDiamond X8 series BlackDiamond X8 xl-series Summit X460, X460-G2, X670, X670-G2, X770 Summit X480 E4G-400	1,200,000 24,000 1,200,000 25,000 1,000,000 25,000
BGP ECMP—maximum number of equalcost multipath for BGP and BGPv6.	All platforms, except Summit X430, X440, and E4G-200 BlackDiamond 8800 G48Te2 (for BGPv6)	2, 4, or 8 N/A

Table 2: Supported Limits (Continued)

Metric	Product	Limit
BGPv6 (unicast address-family routes)—maximum number of unicast address family routes.	BlackDiamond 8900 xl-series BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond X8 series BlackDiamond X8 xl-series Summit X460, X460-G2 Summit X480 Summit X670, X670-G2, X770 E4G-400	20,000 6,000 240 8,000 20,000 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 c-series BlackDiamond 8000 e-series BlackDiamond X8 series BlackDiamond X8 xl-series Summit X460, X460-G2 Summit X480, X670, X670-G2, X770 E4G-400	24,000 18,000 720 24,000 24,000 18,000 24,000 18,000
BOOTP/DHCP relay—maximum number of BOOTP or DHCP servers per virtual router.	All platforms, except Summit X430	4
BOOTP/DHCP relay—maximum number of BOOTP or DHCP servers per VLAN.	All platforms, except Summit X430	4
CES TDM pseudowires—maximum number of CES TDM pseudowires per switch.	E4G-200 and E4G-400	256
Connectivity fault management (CFM)—maximum number or CFM domains. **NOTE:** With Advanced Edge license or higher.	All platforms	8
CFM—maximum number of CFM associations. **NOTE:** With Advanced Edge license or higher.	All platforms	256
CFM—maximum number of CFM up end points. **NOTE:** With Advanced Edge license or higher.	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. **NOTE:** With Advanced Edge license or higher.	BlackDiamond 8000 series BlackDiamond X8 series Summit series X460, E4G-200, E4G-400 (non-load shared ports) All other platforms	32 32 256 (non-load shared ports) 32 (load shared ports) 32
CFM—maximum number of CFM remote end points per up/down end point. **NOTE:** With Advanced Edge license or higher.	All platforms	2,000
CFM—maximum number of dot1ag ports. **NOTE:** With Advanced Edge license or higher.	All Summits, except X430, X450-G2	128
CFM—maximum number of CFM segments. **NOTE:** With Advanced Edge license or higher.	All platforms	1,000
CFM—maximum number of MIPs. **NOTE:** With Advanced Edge license or higher.	All platforms	256
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 X8, BlackDiamond 8800 Summit X440, X430 Summit X670 Summit X460, X460-G2, X770, X670-G2, X450-G2 Summit X480 E4G-200 E4G-400	4,096 1,024 2,048 4,094 8,192 2,048 4,094
Data Center Bridging eXchange (DCBX) protocol Type Length Value (TLVs)—maximum number of DCBX application TLVs.	All platforms	8

Table 2: Supported Limits (Continued)

Metric	Product	Limit
DHCPv6 Prefix Delegation Snooping—Maximum number of DHCPv6 prefix delegation snooped entries.	All platforms	256 (with Underlying Protocol Ripng) 128 (with Underlying protocol OSPFv3) 1,024 (with static routes)
DHCP snooping entries—maximum number of DHCP snooping entries.	All Summits BlackDiamond X8	2,048 6,000
Dynamic ACLs—maximum number of ACLs processed per second. **NOTE:** Limits are load dependent.	Summit X480, X670 with 50 DACLs with 500 DACLs BlackDiamond X8 BlackDiamond 8800	 10 5 N/A N/A
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 BlackDiamond X8 series Summit X670-G2, X450-G2, X460-G2, and X770 Summit X670, X480, X460, X440, E4G-200, E4G-400 Summit X430	64 64 64 32 4
EAPSv1 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8000 series BlackDiamond X8 series Summit series, E4G-200, E4G-400	2,000 2,000 1,000
EAPSv2 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8000 series BlackDiamond X8 series All Summits (except X430, X440), E4G-200, E4G-400	2,000 2,000 500
ELSM (vlan-ports)—maximum number of VLAN ports.	BlackDiamond 8000 series BlackDiamond X8 series All Summits, E4G-200, E4G-400	5,000 5,000 5,000
ERPS domains—maximum number of ERPS domains without CFM configured	BlackDiamond 8800 series BlackDiamond X8 series Summit series (except X430), E4G-200, E4G-400 Summit X430	32 32 32 4

Table 2: Supported Limits (Continued)

Metric	Product	Limit
ERPS domains—maximum number of ERPS domains with CFM configured.	BlackDiamond 8800 series BlackDiamond X8 series Summit X440, X770, X670, X670-G2, X480, X460-G2, X450-G2 Summit X460 Summit X430 E4G-200, E4G-400	16 16 16 32 4 32
ERPSv1 protected VLANs— maximum number of protected VLANs.	BlackDiamond 8800 series BlackDiamond X8 series All Summits, E4G-200, E4G-400	2,000 2,000 1,000
ERPSv2 protected VLANs— maximum number of protected VLANs	BlackDiamond 8800 series BlackDiamond X8 series All Summits (except X430), 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.	All platforms	64
ESRP VLANs—maximum number of ESRP VLANs.	BlackDiamond 8800 BlackDiamond X8 All Summits E4G-200. E4G-400	1,000 2,048 1,000 1,000
ESRP (maximum ping tracks)— maximum number of ping tracks per VLAN.	All platforms (except Summit X430)	8
ESRP (IP route tracks)—maximum IP route tracks per VLAN.	All platforms (except Summit X430)	8
ESRP (VLAN tracks)—maximum number of VLAN tracks per VLAN.	All platforms (except Summit X430)	1

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Forwarding rate—maximum L3 software forwarding rate.	BlackDiamond 8000 series	10,000 pps
	BlackDiamond X8 series	20,000 pps
	Summit X770	14.000 pps
	Summit X670-G2	25,000 pps
	Summit X670	14,829 pps
	Summit X480	14,509 pps
	Summit X460-G2	28,000 pps
	Summit X460	5,222 pps
	Summit X450-G2	27,000 pps
	Summit X440	5,418 pps
	E4G-200	8,718 pps
	E4G-400	5,536 pps
FDB (unicast blackhole entries)—maximum number of unicast blackhole FDB entries.	BlackDiamond 8800 c-series	32,000
	BlackDiamond 8000 e-series	8,000
	BlackDiamond 8900 series	
	8900 c-series 8900 xl-series 8900-40G6X-xm	32,000 524,288 (up to)[b] 128,000
	BlackDiamond X8 a-series modules	128,000
	BlackDiamond X8-100G4X modules	384,000
	BlackDiamond X8 XL-series module	384,000 [d]
	E4G-200, E4G-400	32,000
	Summit X440, X430	16,000
	Summit X480	524,288 (up to)[b]
	Summit X460	32,000
	Summit X460-G2	49,152[e]
	Summit X670 VIM4-40G4x, X480 VIM3-40G4X	128,000
	Summit X770, X670-G2	294,912[e]
	Summit X670, X670v-48t	130,000[e]
	Summit X450-G2	34,000
FDB (multicast blackhole entries)—maximum number of multicast blackhole FDB entries.	BlackDiamond 8000 series	1,024
	BlackDiamond X8 series	1,024
	Summit X480, X460-G2, X460, X440, X430, X450-G2	1,024
	Summit X770, X670, X670-G2, X670v-48t, X480 VIM3-40G4X	4,096
	E4G-200, E4G-400	1,024

Table 2: Supported Limits (Continued)

Metric	Product	Limit
FDB (maximum L2 entries)—maximum number of MAC addresses.	BlackDiamond 8000 c-series	32,768[f]
	BlackDiamond 8000 e-series	8,192[f]
	BlackDiamond 8000 (system), except 8900 xl-series	128,000[f]
	BlackDiamond 8900 xl-series	524,488 (up to)[b]
	BlackDiamond X8 a-series modules	128,000[f]
	BlackDiamond X8-100G4X modules	384,000[f]
	BlackDiamond X8 xl-series	1,048,576 (up to)[b g]
	E4G-200, E4G-400	32,000[f]
	Summit X440, X430	16,000[f]
	Summit X480 (40G4X)	524,488 (up to)[b]
	Summit X460	32,000[f]
	Summit X670-G2	294,912[f]
	Summit X460-G2	96,000[f]
	Summit X670	128,000[f]
	Summit X770	294,912[e f]
	Summit X450-G2	68,000[f]
FDB (Maximum L2 entries)—maximum number of multicast FDB entries.	BlackDiamond X8	1,024
	BlackDiamond 8800	1,024
	Summit X770, X670, X670-G2	4,096
	Summit X480, X460, X460-G2, X430, X440, X450-G2	1,024
	E4G-200, E4G-400	1,024
FIP Snooping VLANs	BlackDiamond X8	768
	BlackDiamond 8800 (8900-40G6X-c only)	
	Summit X670	
FIP Snooping Virtual Links (FPMA mode) per port group	BlackDiamond X8	1,908
	BlackDiamond 8800 (8900-40G6X-c only)	
	Summit X670	
FIP Snooping FCFs (with perimeter port) per port group	BlackDiamond X8	238
	BlackDiamond 8800 (8900-40G6X-c only)	
FIP Snooping FCFs (with Enode-to-FCF port)	BlackDiamond X8	212
	BlackDiamond 8800 (8900-40G6X-c only)	
	Summit X670	

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Identity management—maximum number of Blacklist entries.	All platforms, except Summit X430. Summit X430	512 N/A
Identity management—maximum number of Whitelist entries.	All platforms, except Summit X430. Summit X430	512 N/A
Identity management—maximum number of roles that can be created.	All platforms, except Summit X430. Summit X430	64 N/A
Identity management—maximum role hierarchy depth allowed.	All platforms, except Summit X430. Summit X430	5 N/A
Identity management—maximum number of attribute value pairs in a role match criteria.	All platforms, except Summit X430. Summit X430	16 N/A
Identity management—maximum of child roles for a role.	All platforms, except Summit X430. Summit X430	8 N/A
Identity management—maximum number of policies/dynamic ACLs that can be configured per role.	All platforms, except Summit X430. Summit X430	8 N/A
Identity management—maximum number of LDAP servers that can be configured.	All platforms, except Summit X430. Summit X430	8 N/A
Identity management—maximum number of Kerberos servers that can be configured.	All platforms, except Summit X430. Summit X430	20 N/A
Identity management—maximum database memory-size.	All platforms, except Summit X430. Summit X430	512 N/A
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, except Summit X430. Summit X430	100 N/A
Identity management— recommended number of ACL entries per identity. **NOTE:** Number of ACLs per identity based on system ACL limitation.	All platforms, except Summit X430. Summit X430	20 N/A
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 N/A

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IGMP sender—maximum number of IGMP senders per switch (IP multicast compression enabled).[m] **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 70 • Layer-2 IPMC forwarding caches— (IGMP/MLD/PIM snooping) in mixed-mode. on page 70	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 a-series modules BlackDiamond X8 b-series modules E4G-200 E4G-400 Summit X440 Summit X460 Summit X460-G2 Summit X450-G2 Summit X480 Summit X670 Summit X770, X670-G2 Summit X430	2,048[i] 500[i] 2,048[i] 4,096[i] 3,000[i] 12,000[i] 4,096[b] 64,000[i] 3,000[i j] 6,000[i j] 192[i] 6,000[i] 30,000[h] 21,000[h] 12,000[i] 3,000 77,500[i] 192
IGMP snooping per VLAN filters— maximum number of VLANs supported in per-VLAN IGMP snooping mode.	BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 a-series modules BlackDiamond X8 b-series modules E4G-200, E4G-400 Summit X460, X670, X440 Summit X460-G2, Summit X450-G2 Summit X480 Summit X770, X670-G2	2,000 448 1,000 4,000 1,000 1,000 4,000 1,000 1,000 1,500 2,048 4,000 2,000
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.[n]	BlackDiamond 8800 c-series	2,000
	BlackDiamond 8900 c-series	2,000
	BlackDiamond X8 series	2,000
	Summit X430, X460, E4G-200, E4G-400, X440	1,000
	Summit X480, X670, X670v-48t	2,000
	Summit X770, X670-G2, X460-G2, X450-G2	4,000
IGMPv2 subscriber—maximum number of IGMPv2 subscribers per switch.[n]	BlackDiamond 8800 c-series	20,000
	BlackDiamond 8900 c-series	20,000
	BlackDiamond X8 series	20,000
	Summit X430, X440, E4G-200	10,000
	Summit X460, X460-G2, X480, X670, E4G-400, X670v-48t, X450-G2	20,000
	Summit X770, X670-G2	30,000
IGMPv3 maximum source per group—maximum number of source addresses per group.	All platforms	250
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per port.[n]	BlackDiamond 8800 e-series	1,000
	BlackDiamond 8800 c-series	2,000
	BlackDiamond 8900 series	5,000
	BlackDiamond X8 series	3,000
	Summit X480, X670, X670v-48t, E4G-200, X440	1,000
	Summit X770, X670-G2, X460-G2, X450-G2	4,000
	Summit X460, E4G-400	2,000
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per switch.[n]	BlackDiamond 8800 e-series	10,000
	BlackDiamond 8800 c-series	20,000
	BlackDiamond 8900 series	30,000
	BlackDiamond X8 series	20,000
	Summit X670, X670v-48t, X480, E4G-200, X440	10,000
	Summit X460, X460-G2, E4G-400, X450-G2	20,000
	Summit X770, X670-G2	30,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
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).	BlackDiamond X8-100G4X modules	229,374 (up to)[h]
	Summit X670-G2, X770	131,072 (up to)[h]
	Summit X670, X480, X460, X440, X430	20,480
	Summit X460-G2	57,344 (up to)[h]
	Summit X450-G2	47,000 (up to)[h]
	E4G-200, E4G-400	20,480
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	172,000
	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	32,000[b]
	Per BlackDiamond 8900-G48X-xl or 8900-G48T-xl, up to 130,000 per system	16,000[b]
	Per BlackDiamond 8000 c-series, up to 18,000 per system	8,000
	Per BlackDiamond 8900-40G6X-xm, up to 22,000 per system	8,000
	Per BlackDiamond X8 a-series, up to 28,000 per system	15,750
	Per BlackDiamond X8 xl-series, up to 172,000 per system	172,000
	All other platforms	N/A

Table 2: Supported Limits (Continued)

Metric	Product	Limit
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 c-, xm-series BlackDiamond 8000 e-series BlackDiamond 8900 xl-series BlackDiamond X8 a-series BlackDiamond X8-100G4X modules BlackDiamond X8 xl-series E4G-200 E4G-400 Summit X440 Summit X670, X480 (40G4X) Summit X460, X480 Summit X460-G2 Summit X770, X670-G2 Summit X450-G2	8,000 1,000[i] 16,000 16,000 182,000(up to)[h] [j] 294,000 (up to) [i] 8,000 16,000 412 8,000 16,000 50,000 (up to)[h] 108,000 (up to)[h] 39,000 (up to)[h]
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 c-, xm-series BlackDiamond 8000 e-series BlackDiamond 8900 xl-series BlackDiamond X8 a-series BlackDiamond X8-100G4X modules BlackDiamond X8 xl-series E4G-200 E4G-400 Summit X440 Summit X460, X480 Summit X670, X480 VIM3-40G4X Summit X770, X670-G2 Summit X460-G2 Summit X450-G2	6,000[i] 500[i] 12,000[i] 12,000[i] 172,000 (up to)[h] [j] 290,000 (up to)[i] 6,000[i] 12,000[i] 380 12,000[i] 6,000[i] 98,000 (up to)[h] 43,000 (up to)[h] 29,000 (up to)[h]

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IP flow information export (IPFIX)—number of simultaneous flows.	BlackDiamond 8900 xl-series modules	4,096 ingress, 4,096 egress
	BlackDiamond 8900 c-series modules	4,096 ingress, 4,096 egress
	BlackDiamond X8 b-series modules	2,048 ingress, 2,048 egress
	Summit X460-24t/x/p, X460-G2	2,048 ingress, 2,048 egress
	Summit X480, X460-48t/x/p	4,096 ingress, 4,096 egress
	E4G-400	2,048 ingress, 2,048 egress
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 c-series	18,000[i]
	BlackDiamond 8000 e-series	1,000[i]
	BlackDiamond 8900 xl-series	40,000[b]
	BlackDiamond 8900-40G6X-xm	22,000[i]
	BlackDiamond X8 a-series	28,000[i]
	BlackDiamond X8-100G4X andX8 xl-series	311,000 (up to)[h] [i]
	E4G-200	18,000[i]
	E4G-400	20,000[i]
	Summit X440	448
	Summit X460	20,000[i]
	Summit X460-G2	73,000[h]
	Summit X480	40,000[b]
	Summit X670, X480 VIM3-40G4X	22,000[i]
	Summit X770, X670-G2	176,000 (up to)[h]
	Summit X450-G2	61,000 (up to)[h]
IPv4 routes—maximum number of IPv4 routes in software (combination of unicast and multicast 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
	BlackDiamond X8 with BDX X8 xl-series	1,048,544 (up to)[i]
	Summit X440	256
	Summit X460, X670, X770, X670-G2, X460-G2, X450-G2	25,000
	Summit X480	524,256 (up to)[b]
	E4G-200, E4G-400	25,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IPv4 routes (LPM entries in hardware)— number of IPv4 routes in hardware.	BlackDiamond 8800 c-series	12,000
	BlackDiamond 8000 e-series	480
	BlackDiamond 8900 xl-series	524,256 (up to)[b j]
	BlackDiamond 8900-40G6X-xm	16,000[e]
	BlackDiamond X8 series	16,000[e]
	BlackDiamond BDX X8 xl-series	1,048,544 (up to) [k]
	E4G-200, E4G-400	12,000
	Summit X440	32
	Summit X460, X460-G2	12,000
	Summit X480	524,256 (up to)[b j]
	Summit X480 VIM3-40G4X	16,000[j]
	Summit X670	12,000
	Summit X770, X670-G2, X450-G2	16,000
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	512
	BlackDiamond X8 series	2,048
	E4G-200, E4G-400	512
	Summit X440	254
	Summit X460, X480	512
	Summit X770, X670, X670-G2, X460-G2, X450-G2	2,048

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IPv6 host entries in hardware—maximum number of IPv6 neighbor entries in hardware.	BlackDiamond 8800 c-, xm-series	3,000[i]
	BlackDiamond 8000 e-series	250[i]
	BlackDiamond 8900-10G24X-c modules	2,000[i]
	BlackDiamond 8900-G96T-c modules	4,000[i]
	BlackDiamond 8900 xl-series	8,192 (up to)[b i]
	BlackDiamond X8 a-series	3,000[i]
	BlackDiamond X8-100G4X	49,000[i h]
	BlackDiamond X8 xl-series	49,000[i l]
	E4G-200	2,000[i]
	E4G-400	3,000[i]
	Summit X440	192[i]
	Summit X460, X670, X480 VIM3-40G4X	3,000[i]
	Summit X770, X670-G2	36,750[i]
	Summit X480, X670v-48t	6,000[i]
	Summit X460-G2	22,000[i]
	Summit X450-G2	12,000[i]
IPv6 routes (LPM entries in hardware)—maximum number of IPv6 routes in hardware.	BlackDiamond 8800 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
	BlackDiamond X8 xl-series	524,288 (up to) [l]
	E4G-200, E4G-400	6,000
	Summit X440	16
	Summit X460, X460-G2	6,000
	Summit X670, X480 (VIM3-40G4X), X670, X670-G2, X770, X450-G2	8,000
	Summit X480	245,760 (up to)[b]

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IPv6 routes with a mask greater than 64 bits in hardware—maximum number of such IPv6 LPM routes in hardware.	BlackDiamond 8000 c-, e-, xm-series	256
	BlackDiamond 8000 xl-series	245,760 (up to)[k]
	BlackDiamond X8 series	256
	BlackDiamond X8 xl-series	524,288 (up to) [l]
	E4G-200, E4G-400	256
	Summit X440, X460, X460-G2, X670, X670-G2, X770, X480 (VIM3-40G4X), X450-G2	256
	Summit X480	245,760 (up to)[k]
IPv6 route sharing in hardware—route mask lengths for which ECMP is supported in hardware.	Summit X460, X480, X670, X670V-48t, X450-G2	0–128
	E4G-200, E4G-400	0–128
	BlackDiamond 8800 (all I/O modules, except G48Te2)	0–128
	Summit X460-G2, X670-G2, X770	0–64 (> 64 single path only)
	BlackDiamond X8 a-series	0–128
	BlackDiamond X8-100G4X modules	0–64 (> 64 single path only)
	BlackDiamond X8 xl-series	0–128 [l]
	Summit X440, X430	N/A
	BlackDiamond 8800 G48Te2	N/A
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)[k]
	All other BlackDiamond 8000 series hardware	25,000
	BlackDiamond X8 series	25,000
	BlackDiamond X8 with xl-series	524,288 (up to) [l]
	Summit X460, X460-G2, X670, X670-G2, X770, X450-G2, E4G-200, E4G-400	25,000
	Summit X480	245,760 (up to)[k]
	Summit X440	256
IP router interfaces—maximum number of VLANs performing IPv4 and/or IPv6 routing. Excludes sub-VLANs.	Summit X460-G2, X670, X770, X670-G2, X450-G2, and BlackDiamond X8	2,048
	BlackDiamond 8800	512
	Summit X440	254
	Summit X480, X460	512
	E4G-200, E4G-400	512

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IP multicast static routes— maximum number of permanent multicast IP routes.	All platforms (except Summit X430, X440) Summit X430, X440	1,024 32
IP unicast static routes—maximum number of permanent IP unicast routes.	All platforms (except Summit X430, X440) Summit X430, X440	1,024 32
IP route sharing (maximum gateways)—Configurable maximum number of gateways used by equal cost multipath OSPF, BGP, IS-IS, static routes, or L2VPNs. Routing protocol OSPF is limited to 16 ECMP gateways per destination. Routing protocols BGP and IS-IS are limited to 8 ECMP gateways per destination. Static routes are limited to 32 next-hops. L2VPNs are limited to 16 LSPs per pseudowire on platforms that support 32 gateways, and 64 LSPs per pseudowire on platforms that support 64 gateways.	All platforms, except Summit X430, X440, X670, and BlackDiamond X8 Summit X670, BlackDiamond X8 Summit X430, X440 BlackDiamond 8800 G48Te2 (for IPv6)	2, 4, 8, 16, or 32 2, 4, 6, 8, 16, 32, or 64 N/A N/A
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 or higher, the total number of "destination+gateway" pairs is limited to 2,097,024. 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 BGP and IS-IS routing protocols, up to 16 gateways per destination for OSPF, or up to 32 gateways per destination for static routes.	BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 xl-series BlackDiamond 8900-40G6X-xm BlackDiamond X8 BlackDiamond X8 xl-series E4G-200, E4G-400 Summit X480 Summit X670, X670-G2, X770, X450-G2, X480 (VIM3-40G4X) Summit X460-G2, X460	12,256 480 524,256 (up to)[b] 16,352 16,352 1,048,544 (up to) [i] 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 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, Summit X670	
	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
	if maximum gateways is 64	30
	Summit X460, X460-G2, X450-G2, X480, X670, X670-G2, X770, 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.	BlackDiamond 8800	64
	BlackDiamond X8	64
	All Summits, except X440, X430	255
	Summit X440	32
IS-IS adjacencies—maximum number of supported IS-IS adjacencies.	BlackDiamond 8000 series	128
	BlackDiamond X8 series	128
	BlackDiamond 8900 xl-series	255
	Summit X440, X460, X460-G2, X480, X670, X670-G2, X770	128
	Summit X450-G2	N/A
	E4G-200	256
	E4G-400	128
IS-IS ECMP—maximum number of equal cost multipath for IS-IS.	All platforms, except Summit X440, X430	2, 4, or 8
	BlackDiamond 8800 G48Te2 (for IPv6)	N/A

Table 2: Supported Limits (Continued)

Metric	Product	Limit
IS-IS interfaces—maximum number of interfaces that can support IS-IS.	All platforms, except Summit X440, x430	255
IS-IS routers in an area—recommended maximum number of IS-IS routers in an area.	Summit X480 All other platforms, except Summit X440, X430	128 256
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 X8 xl-series BlackDiamond 8900 xl-series Summit X450-G2, X460, X460-G2, X670, X670-G2, X770, X480 E4G-400 E4G-200	20,000 20,000 30,000 30,000 20,000 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 X8 xl-series BlackDiamond 8900 xl-series Summit X480 Summit X450-G2, X460, X460-G2, X670, X670-G2, X770 E4G-200, E4G-400	25,000 25,000 120,000 120,000 50,000 25,000 25,000
IS-IS IPv4 L2 routes—recommended maximum number of IS-IS Level 2 routes.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond X8 xl-series BlackDiamond 8900 xl-series Summit X480 Summit X450-G2, X460, X460-G2, X670, X670-G2, X770 E4G-200, E4G-400	20,000 25,000 120,000 120,000 50,000 25,000 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 X450-G2, X460, X460-G2, X480, X670, X670-G2. X770 E4G-200, E4G-400	20,000 20,000 20,000 20,000 20,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
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	10,000
	BlackDiamond X8 series	10,000
	BlackDiamond X8 xl-series	40,000
	BlackDiamond 8900 xl-series	40,000
	Summit X480	25,000
	Summit X450-G2, X460, X460-G2, X670, X670-G2, X770, E4G-400	10,000
IS-IS IPv6 L2 routes—recommended maximum number of IS-IS Level 2 routes.	BlackDiamond 8000 series	10,000
	BlackDiamond X8 series	10,000
	BlackDiamond X8 xl-series	40,000
	BlackDiamond 8900 xl-series	40,000
	Summit X480	15,000
	Summit X450-G2, X460, X460-G2, X670, X670-G2, X770	10,000
	E4G-200, E4G-400	10,000
IS-IS IPv6 L1 routes in an L1/L2 router—recommended maximum number of IS-IS Level 1 routes in a L1/I2 router.	BlackDiamond 8000 series	10,000
	BlackDiamond X8 series	10,000
	BlackDiamond X8 xl-series	15,000
	BlackDiamond 8900 xl-series	15,000
	Summit X480	15,000
	Summit X450-G2, X460, X460-G2, X670, X670-G2, X770, E4G-400	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	20,000
	BlackDiamond X8 series	20,000
	BlackDiamond X8 xl-series	60,000
	BlackDiamond 8900 xl-series	60,000
	Summit X480	40,000
	Summit X450-G2, X460, X460-G2, X670, X670-G2. X770	20,000
	E4G-200, E4G-400	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	20,000
	BlackDiamond X8 series	20,000
	BlackDiamond X8 xl-series	60,000
	BlackDiamond 8900 xl-series	60,000
	Summit X480	40,000
	Summit X450-G2, X460,X460-G2, X670, X670-G2, X770	20,000
	E4G-200, E4G-400	20,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
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	20,000
	BlackDiamond X8 series	20,000
	BlackDiamond 8900 xl-series	20,000
	Summit X450-G2, X460, X460-G2, X480, X670, X670-G2, X770	20,000
	E4G-200, E4G-400	20,000
Jumbo frames—maximum size supported for jumbo frames, including the CRC.	All platforms	9,216
L2 VPN: VCCV (pseudowire Virtual Circuit Connectivity Verification) VPNs per switch—maximum number of VCCV enabled VPLS VPNs.	All platforms, except Summit X440, X430, and X450-G2	16
L2 VPN: VPLS MAC addresses—maximum number of MAC addresses learned by a switch.	BlackDiamond 8900 xl-series	512,000
	BlackDiamond 8900-40G6X-xm	128,000
	BlackDiamond X8 a-series modules	128,000
	BlackDiamond X8-100G4X modules	384,000
	BlackDiamond X8 xl-series	1,048,576 [g]
	E4G-200, E4G-400	32,000
	Summit X460	32,000
	Summit X480	512,000
	Summit X670, Summit X670V-48t, Summit X770	128,000
	Summit X480 (40G VIM)	121,000
	Summit X670-G2	140,000
	Summit X460-G2	55,000
L2 VPN: VPLS VPNs—maximum number of VPLS virtual private networks per switch.	BlackDiamond 8900 xl-series	1,023
	BlackDiamond 8900-40G6x-xm	1,023
	BlackDiamond X8 series	1,023
	E4G-200, E4G-400	1,023
	Summit X460, X460-G2, X480, X670, X670V-48t, X480 (40G VIM), X770, X670-G2	1,023
L2 VPN: VPLS peers—maximum number of VPLS peers per VPLS instance.	BlackDiamond 8900 xl-series	64
	BlackDiamond 8900-40G6x-xm	64
	BlackDiamond X8 series	64
	Summit X770, X670-G2, X670v-48t, X480, X460-G2	64
	Summit X670, X460	32
	E4G-200, E4G-400	32

Table 2: Supported Limits (Continued)

Metric	Product	Limit
L2 VPN: LDP pseudowires—maximum number of pseudowires per switch.	BlackDiamond 8900 xl-series	7,000
	BlackDiamond 8900-40G6X-xm	3,000
	BlackDiamond X8 series	7,000
	E4G-200, E4G-400	1,000
	Summit X770	7,800
	Summit X670-G2, X670v-48t, X480	7,000
	Summit X670	3,000
	Summit X460-G2	7,116
	Summit X460	1,000
L2 VPN: static pseudowires—maximum number of static pseudowires per switch.	BlackDiamond 8900 xl-series, BlackDiamond X8	7,116
	BlackDiamond 8900-40G6X-xm	3,020
	Summit X460, X480, X670V-48t	7,116
	Summit X770	15,308
	Summit X480-40G, Summit X670	3,020
	Summit X670-G2, X460-G2	7,000
	E4G-200	2,764
	E4G-400	6,860
L2 VPN: Virtual Private Wire Service (VPWS) VPNs—maximum number of virtual private networks per switch.	Summit X460	1,000
	Summit X480, X770	4,000
	Summit X480-40G VIM	2,047
	Summit X670	2,047
	Summit X670V-48t	4,000
	BlackDiamond 8900 xl-series	4,000
	BlackDiamond 8900-40G6X-xm	2,047
	BlackDiamond X8 series	4,000
	Summit X670-G2	4,090
	Summit X460-G2	1,023
	E4G-200, E4G-400	1,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
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	2,000
	BlackDiamond 8800 c- and xl-series switches	8,000
	BlackDiamond 8800 xm-series switches	15,000
	BlackDiamond X8 series switches	15,000
	E4G-200, E4G-400	8,000
	Summit X480, X460	8,000
	Summit X670, X670V	15,000
	Summit X440	5,000
	Summit X770, X670-G2	77,500[h]
	Summit X460-G2	32,000[h]
	Summit X430	5,000
	Summit X450-G2	20,000[h]
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, X670V, Summit X450-G2	15,000
	E4G-200 and E4G-400 cell site routers, Summit X460	8,000
	Summit X440	5,000
	Summit X770, X670-G2	77,500[h]
	Summit X460-G2	24,000
	Summit X480	8,000
Layer-3 IPMC forwarding caches—(PIM, MVR, PVLAN) in mixed-mode.[i] **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 a-series modules	6,000
	BlackDiamond X8-100G4X and modules	64,000
	E4G-200 cell site routers, Summit X670	3,000
	E4G-400 cell site routers, Summit X460, X480, X670V	6,000
	Summit X440	192
	Summit X770, X670-G2	77,500[h]
	Summit X450-G2	21,000[h]
	Summit X460-G2	26,000[h]

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

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Load sharing—maximum number of ports per load-sharing group. **NOTE:** * For custom algorithm ** For L2 and L3 algorithms **NOTE:** For a mix of Summit X770 and Summit X670 series switches in a stack, the limits are the Summit X670 limits.	BlackDiamond X8 series	64
	Summit X460-G2 (standalone)	32
	Summit X670 (standalone)	32 * 16 **
	Summit X670 (stacked) Summit X670-G2 (stacked)	64 * 16 **
	Summit X770 (standalone) Summit X670-G2 (standalone) Summit X460-G2 (standalone) Summit X450-G2 (standalone)	32
	Summit X770 (stacked) Summit X670-G2 (stacked) Summit X460-G2 (stacked) Summit X450-G2 (stacked)	64
	All other Summit series, SummitStacks, E4G cell site routers, 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
MAC Locking—Maximum number of MAC locking stations that can be learned on a port.	All platforms	64 (static MAC locking stations) 600 (first arrival MAC locking stations)
Meters—maximum number of meters supported	All platforms	2,048

Table 2: Supported Limits (Continued)

Metric	Product	Limit
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 **NOTE:** The Summit X430 can only support one egress mirroring instance.	All platforms	16 (including default mirroring instance)
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 All Summit series E4G cell site routers	128 128 128 128
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 All Summit series E4G cell site routers	128 128 128 128
Mirroring, one-to-many (monitor port)—maximum number of one-to-many monitor ports.	All platforms	16
MLAG ports—maximum number of MLAG ports allowed.	BlackDiamond 8000 series BlackDiamond X8 series All Summit series, except X430 E4G cell site routers	768 768 768 768
MLAG peers—maximum number of MLAG peers allowed.	All platforms, except Summit X430	2

Table 2: Supported Limits (Continued)

Metric	Product	Limit
MPLS RSVP-TE interfaces— maximum number of interfaces.	All platforms, except Summit X450-G2, X440, and X430	32
MPLS RSVP-TE ingress LSPs— maximum number of ingress LSPs.	All platforms, except Summit X450-G2, X440, and X430	2,000
MPLS RSVP-TE egress LSPs—maximum number of egress LSPs.	All platforms, except Summit X450-G2, X440 and X430	2,000
MPLS RSVP-TE transit LSPs— maximum number of transit LSPs.	All platforms, except Summit X450-G2, X440, and X430	2,000
MPLS RSVP-TE paths—maximum number of paths.	All platforms, except Summit X450-G2, X440, X430, and X670-G2 Summit X670-G2	1,000 2,000
MPLS RSVP-TE profiles—maximum number of profiles.	All platforms, except Summit X440, X430, X670-G2, and X450-G2 Summit X670-G2	1,000 2,000
MPLS RSVP-TE EROs—maximum number of EROs per path.	All platforms, except Summit X450-G2, X440, and X430	64
MPLS RSVP-TE fast reroute—MPLS RSVP-TE fast reroute (FRR) switching time.	E4G-200	50 msec
MPLS LDP peers—maximum number of MPLS LDP peers per switch.	Summit X460, Summit X670 Summit X480, Summit X480 (40G VIM), X670V-48t, X770, X670v-48t BlackDiamond 8900 xl-series BlackDiamond 8900-40G6x-xm BlackDiamond X8 series Summit X670-G2, X460-G2 E4G-400, E4G-200	32 64 64 64 64 128 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, X460-G2 Summit X670V-48t, X480 (40G VIM), X770, X670-G2	50 64 50 50 50 64

Table 2: Supported Limits (Continued)

Metric	Product	Limit
MPLS LDP ingress LSPs—maximum number of MPLS LSPs that can originate from a switch.	BlackDiamond 8900 xl-series	4,000
	BlackDiamond 8900-40G6X-xm	2,048
	BlackDiamond X8 series	2,048
	E4G-200	2,048
	E4G-400	4,000
	Summit X460, X480	4,000
	Summit X670, X670V-48t, X480 (40G VIM), X770	2,048
	Summit X670-G2	2,048
	Summit X460-G2	4,000
MPLS LDP-enabled interfaces—maximum number of MPLS LDP configured interfaces per switch.	Summit X460, X670	32
	Summit X480, X670V-48t, X770	64
	Summit X670-G2, X460-G2	128
	BlackDiamond 8900 xl-series	64
	BlackDiamond 8900-40G6x-xm	64
	BlackDiamond X8 series	64
	E4G-200, E4G-200	32
MPLS LDP Sessions—maximum number of MPLS LDP sessions.	BlackDiamond 8900 xl-series	64
	BlackDiamond 8900-40G6x-xm	64
	BlackDiamond X8 series	64
	Summit X770, X670v-48t, X480	64
	Summit X670-G2, X460-G2	128
	Summit X670, X460	32
	E4G-200, E4G-400	32
MPLS LDP transit LSPs—maximum number of MPLS transit LSPs per switch.	BlackDiamond 8900 xl-series	4,000
	BlackDiamond 8900-40G6X-xm	3,000
	BlackDiamond X8 series	4,000
	E4G-200	2,700
	E4G-400	4,000
	Summit X460, X480, X770, X670V-48t, X670-G2, X460-G2	4,000
	Summit X670, X480 (VIM3-40G4x)	3,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
MPLS LDP egress LSPs—maximum number of MPLS egress LSPs that can terminate on a switch.	BlackDiamond 8900 xl-series	7,000
	BlackDiamond 8900-40G6X-xm	3,000
	BlackDiamond X8 series	7,000
	E4G-200	2,700
	E4G-400	6,700
	Summit X460, X480, X670V-48t	7,000
	Summit X670, X480 (VIM3-40G4x)	3,000
	Summit X770	8,000
	Summit X670-G2, X460-G2	4,000
MPLS static egress LSPs—maximum number of static egress LSPs.	BlackDiamond 8900 xl-series, BlackDiamond X8	7,116
	BlackDiamond 8900-40G	3,020
	Summit X460, X480, X670V-48t, X460-G2	7,116
	Summit X480 (VIM3-40G4x), X670	3,020
	Summit X770	8,000
	Summit X670-G2	15,308
	E4G-200	2,700
	E4G-400	6,860
MPLS static ingress LSPs—maximum number of static ingress LSPs.	BlackDiamond 8900 xl-series	4,000
	BlackDiamond 8900-40G	2,048
	BlackDiamond X8	2,048
	Summit X460, X480, X460-G2	4,000
	Summit x480-40G, X670, x670V-48t, X770, X670-G2	2,048
	E4G-200	2,048
	E4G-400	4,000
MPLS static transit LSPs—maximum number of static transit LSPs	BlackDiamond 8900 xl-series	4,000
	BlackDiamond 8900-40G	3,000
	BlackDiamond X8	4,000
	Summit X460, X480, X670V-48t, X770, X670-G2, X460-G2	4,000
	Summit X480-40G, X670	3,000
	E4G-200	2,700
	E4G-400	4,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
MSDP active peers—maximum number of active MSDP peers.	BlackDiamond 8000 series	64
	BlackDiamond X8 series	64
	BlackDiamond 8900 series	64
	Summit X460, X480, X670, E4G-400, X670-G2, X460-G2, X450-G2	16
	Summit X770	64
MSDP SA cache entries—maximum number of entries in SA cache.	BlackDiamond 8000 series	16,000
	BlackDiamond X8 series	16,000
	BlackDiamond 8900 series	16,000
	Summit X480, X670, E4G-400, X450-G2	8,000
	Summit X670-G2, X770	14,000
	Summit X460-G2	10,000
	Summit X460	6,000
MSDP maximum mesh groups—maximum number of MSDP mesh groups.	BlackDiamond 8000 series	16
	BlackDiamond X8 series	16
	BlackDiamond 8900 series	16
	Summit X460, X480, X670, E4G-400	4
	Summit X770, X670-G2, X450-G2, X460-G2	16
Multicast listener discovery (MLD) IPv6 multicast data sender—maximum number of IPv6 multicast streams supported on a switch[m 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 70 • Layer-2 IPMC forwarding caches— (IGMP/MLD/PIM snooping) in mixed-mode. on page 70	BlackDiamond 8800 c-series	1,000
	BlackDiamond 8800 e-series	250
	BlackDiamond 8900 c-series	1,000
	BlackDiamond 8900-40G6X-xm	1,000
	BlackDiamond 8900 xl-series	3,000
	BlackDiamond X8 series	3,000
	E4G-200	1,500
	E4G-400	3,000
	Summit X440	90
	Summit X460, X480	3,000
	Summit X670	1,500
	Summit X770, X670-G2	30,000
	Summit X460-G2	14,000
	Summit X450-G2	10,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Multicast listener discovery (MLD) snooping per-VLAN filters—maximum number of VLANs supported in per-VLAN MLD snooping mode.	BlackDiamond e-series	250
	BlackDiamond 8800 c-series	1,000
	BlackDiamond 8900 c-series	500
	BlackDiamond 8900 xl-series	2,000
	BlackDiamond 8900-40G6X-xm	500
	BlackDiamond X8 a-series	500
	BlackDiamond X8 b-series	2,000
	E4G-400, Summit X460, X450-G2	1,000
	Summit X460-G2	1,200
	Summit X480	2,000
	Summit X440	250
	Summit X670, E4G-200	500
	Summit X770, X670-G2	1,200
	Summit X450-G2	512
Multicast listener discovery (MLD)v1 subscribers—maximum number of MLDv1 subscribers per port[n]	BlackDiamond 8800 c-series	500
	BlackDiamond xl-series	1,500
	BlackDiamond X8 Series	1,500
	Summit X440	750
	Summit X460, X480, X670, E4G-400	1,500
	Summit X770, X670-G2, X450-G2, X460-G2	4,000
Multicast listener discovery (MLD)v1 subscribers—maximum number of MLDv1 subscribers per switch[n]	BlackDiamond 8800 series	10,000
	BlackDiamond X8 series	10,000
	Summit X440	5,000
	Summit X460, X480, X670, E4G-400, X460-G2, X450-G2	10,000
	Summit X770, X670-G2	30,000
Multicast listener discovery (MLD)v2 subscribers—maximum number of MLDv2 subscribers per port[n]	BlackDiamond 8800 c-series	500
	BlackDiamond xl series	2,500
	BlackDiamond X8 series	2,000
	Summit X440, X450-G2, SummitStack	1,000
	Summit X460, X480, X670, E4G-400,	2,000
	Summit X770, X670-G2, X450-G2, X460-G2	4,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Multicast listener discovery (MLD)v2 subscribers—maximum number of MLDv2 subscribers per switch[n]	BlackDiamond 8800 series	10,000
	BlackDiamond xl series	10,000
	Summit X440, SummitStack	5,000
	Summit X460, X480, X670, E4G-400, X460-G2, X450-G2	10,000
	Summit X770, X670-G2	30,000
Multicast listener discovery (MLD)v2 maximum source per group—maximum number of source addresses per group	All platforms, except Summit X430	200
Multicast listener discovery (MLD) SSM-map entries—maximum number of MLD SSM mapping entries.	All platforms	500
Multicast listener discovery (MLD) SSM-MAP entries—maximum number of sources per group in MLD SSM mapping entries.	All platform	50
Multicast VLAN registration (MVR)—maximum number of MVR senders per switch (IP multicast compression enabled). **NOTE:** Assumes source-group-vlan mode. For additional limits, see: Layer-3 IPMC forwarding caches—(PIM, MVR, PVLAN) in mixed-mode.i on page 70	BlackDiamond 8800 c-series	6,000[i]
	BlackDiamond 8000 e-series	500[i]
	BlackDiamond 8900 c-series	6,000[i]
	BlackDiamond 8900 xl-series	12,000[b]
	BlackDiamond X8 a-series	6,000[i]
	BlackDiamond X8-100G4X and X8 xl-series	59,000
	8900-40G6X-xm module	3,000[i]
	Summit X440	192[i]
	Summit X460, E4G-400	6,000[i]
	Summit X480	12,000[b]
	Summit X670	
	VIM4-40G4x	3,000[i]
	Summit X770, X670-G2	77,500
	Summit X450-G2	21,000[h]
	Summit X460-G2	26,000
Network login—maximum number of clients being authenticated on MAC-based VLAN enabled ports.	BlackDiamond 8000 series (clients per module/per system)	1,024
	BlackDiamond X8 series	1,024
	Summit series	1,024
Network login—maximum number of clients being authenticated with policy mode enabled.	Summit X450-G2, X460-G2	1,024
	Summit X670-G2, X770	512

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Network login—maximum number of dynamic VLANs.	All platforms	2,000
Network login VLAN VSAs— maximum number of VLANs a client can be authenticated on at any given time.	All platforms	10
OSPFv2/v3 ECMP—maximum number of equal cost multipath OSPFv2 and OSPFv3.	All platforms, except Summit X450-G2, X440, X430, and E4G-200) Summit X450-G2 E4G-200 BlackDiamond 8800 G48Te2 (for IPv6)	16 4 8 N/A
OSPFv2 areas—as an ABR, how many OSPF areas are supported within the same switch.	All platforms (except X430, X440)	8
OSPFv2 external routes—recommended maximum number of external routes contained in an OSPF LSDB.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond X8 series BlackDiamond X8 xl-series Summit X460, X670, X770, X670-G2, X460-G2, X450-G2 Summit X480 E4G-400 E4G-200	20,000 130,000 20,000 130,000 5,000 130,000 5,000 5,000
OSPFv2 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 X460, X670, X670-G2, X460-G2 E4G-400 Summit X480, X770	7,000 7,000 7,000 2,000 2,000 7,000
OSPFv2 interfaces—recommended maximum number of OSPF interfaces on a switch.	**NOTE:** Active interfaces limit, with Advanced Edge license. (See below for Core license limits.) All platforms (except X430)	4
	All platforms (except X430 and X440) with Core license or higher (active interfaces only)	400
OSPFv2 links—maximum number of links in the router LSA.	All platforms, except Summit X450-G2, X770, and X430 Summit X450-G2 Summit X770	400 4 419

Table 2: Supported Limits (Continued)

Metric	Product	Limit
OSPFv2 neighbors—maximum number of supported OSPF adjacencies.	BlackDiamond 8000 series	128
	BlackDiamond 8900 xl-series	255
	BlackDiamond X8 Series	255
	Summit X460, X670, X770, X440, X670-G2, X460-G2	128
	Summit X480	255
	Summit X450-G2	4
	E4G-400, E4G-200	128
OSPFv2 routers in a single area—recommended maximum number of routers in a single OSPF area.	BlackDiamond 8000 series	100
	BlackDiamond 8900 xl-series	200
	BlackDiamond X8 series	100
	Summit X460, X670, X770, X670-G2, X460-G2, X450-G2	50
	Summit X480	200
	E4G-400	50
OSPFv2 virtual links—maximum number of supported OSPF virtual links.	All platforms (except X450-G2, X430, and X440) with Core license or higher	32
	Summit X450-G2	4
OSPFv3 areas—as an ABR, the maximum number of supported OSPFv3 areas.	All platforms (except X430 and X440) with Core license or higher	16
OSPFv3 external routes—recommended maximum number of external routes.	BlackDiamond 8000 series	10,000
	BlackDiamond X8 series	10,000
	BlackDiamond X8 xl-series	60,000
	BlackDiamond 8900 xl-series	60,000
	Summit X460, X670, X770, X670-G2, X460-G2, X450-G2	10,000
	Summit X480	60,000
	E4G-400	10,000
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 X460, X670, X770, X670-G2, X460-G2, X450-G2	3,000
	Summit X480	6,000
	E4G-400	3,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
OSPFv3 interfaces—maximum number of OSPFv3 interfaces.	**NOTE:** Active interfaces only, with Advanced Edge license. (See below for Core license limits.) All platforms (except X430)	4
	NOTE: With Core license or higher. (See above for Advanced Edge license limits.) BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X460, X670, X770 Summit X480 Summit X670-G2, X460-G2 E4G-200, E4G-400	 256 256 384 128 384 256 256
OSPFv3 neighbors—maximum number of OSPFv3 neighbors.	BlackDiamond 8000 series BlackDiamond X8 series BlackDiamond 8900 xl-series Summit X460, X670, X770, X670-G2, X460-G2, X450-G2 Summit X480 E4G-400	64 64 128 64 128 64
OSPFv3 virtual links—maximum number of OSPFv3 virtual links supported.	All platforms (except X450-G2, X430, and X440) with Core license or higher Summit X450-G2	16 4

Table 2: Supported Limits (Continued)

Metric	Product	Limit
PIM IPv4 snooping—maximum number of (S,G) entries programmed in the hardware (IP multicast 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 70 • Layer-2 IPMC forwarding caches— (IGMP/MLD/PIM snooping) in mixed-mode. on page 70	BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond X8 a-series BlackDiamond X8-100G4X and X8 xl-series E4G-200 E4G-400 8900-40G6X-xm Summit X440 Summit X480 Summit X460 Summit X670 Summit X770, X670-G2 Summit X450-G2 Summit X460-G2	6,000[i] 500[i] 6,000[i] 12,000[i] 6,000[i] 59,000[i] 3,000[i] 6,000[i] 3,000[i] 192[i] 12,000[i] 6,000[i] 3,000[i] 77,500 21,000 26,000
PIM IPv4—maximum routes—maximum number of (S,G) entries installed in the hardware (IP multicast compression enabled). **NOTE:** Assumes source-group-vlan mode. For additional limits, see: Layer-3 IPMC forwarding caches—(PIM, MVR, PVLAN) in mixed-mode.i on page 70	BlackDiamond 8800 c-series BlackDiamond 8000 e-series BlackDiamond 8900 c-series BlackDiamond 8900 xl-series BlackDiamond X8 a-series BlackDiamond X8-100G4X and X8 xl-series E4G-200 E4G-400 8900-40G6X-xm modules Summit X440 Summit X480 Summit X460 Summit X670 Summit X770, X670-G2 Summit X450-G2 Summit X460-G2	6,000[i] 500[i] 6,000[i] 12,000[i] 6,000[f] 60,000[f] 3,000[i] 6,000[i] 3,000[i] 192 12,000[i] 6,000[i] 3,000[i] 77,500 21,000 26,000

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 multicast compression enabled). **NOTE:** Assumes source-group-vlan mode. For additional limits, see: Layer-3 IPMC forwarding caches—(PIM, MVR, PVLAN) in mixed-mode.i on page 70	BlackDiamond 8800 c-series	6,000[i]
	BlackDiamond 8000 e-series	500[i]
	BlackDiamond 8900 c-series	6,000[i]
	BlackDiamond 8900 xl-series	12,000[i]
	BlackDiamond X8 a-series	6,000[i]
	BlackDiamond X8-100G4X and X8 xl-series	59,000[i]
	E4G-200	3,000[i]
	E4G-400	6,000[i]
	8900-40G6X-xm	3,000[i]
	Summit X440	192[i]
	Summit X480	12,000[i]
	Summit X460	6,000[i]
	Summit X670	3,000[i]
	Summit X770, X670-G2	77,500
	Summit X450-G2	21,000
	Summit X460-G2	26,000
PIM IPv6 (maximum routes)—maximum number of (S,G) entries installed in the hardware. **NOTE:** Assumes source-group-vlan mode.	BlackDiamond 8800 c-series	1,000
	BlackDiamond 8800 e-series	250
	BlackDiamond 8900 c-series	1,000
	BlackDiamond 8900-40G6X-xm	1,000
	BlackDiamond 8900 xl-series	3,000
	BlackDiamond X8 a-series	3,000
	BlackDiamond X8-100G4X and X8 xl-series	30,000[i]
	E4G-200	1,500
	E4G-400	3,000
	Summit X440	90
	Summit X460, X480, X670	3,000
	Summit X770, X670-G2	30,000
	Summit X450-G2	10,000
	Summit X460-G2	14,000
PIM IPv4 (maximum interfaces)—maximum number of PIM active interfaces.	All platforms, except Summit X430 and X440	512
	Summit X440	253
PIM IPv4 (maximum interfaces)—maximum number of PIM-snooping-enabled interfaces.	All platforms, except Summit X430	512

Table 2: Supported Limits (Continued)

Metric	Product	Limit
PIM IPv4 Limits—maximum number of multicast groups per rendezvous point	All platforms, except Summit X430	180
PIM IPv4 Limits—maximum number of multicast sources per group	BlackDiamond 8800 (E-series modules) BlackDiamond 8800 (C-series modules) BlackDiamond 8800 (xl-series modules) BlackDiamond X8 Summit X460-G2, X670-G2, X770, X450-G2 Summit X460, X480 Summit X670-48x Summit X670-48t Summit X440	1,000 3,000 4,000 3,000 5,000 1,200 1,000 4,000 175
PIM IPv4 Limits—maximum number of dynamic rendezvous points per multicast group	All platforms, except Summit X430	145
PIM IPv4 Limits—static rendezvous points	All platforms, except Summit X430	32
PIM IPv6 (maximum interfaces)—maximum number of PIM active interfaces	All platforms, except Summit X430	512
PIM IPv6 Limits—maximum number of multicast group per rendezvous point	All platforms, except Summit X430	70
PIM IPv6 Limits—maximum number of multicast sources per group.	BlackDiamond 8000 BlackDiamond X8 Summit X460-G2, X670-G2, Summit X460, X480 Summit X670 Summit X440 Summit X450-G2 Summit X770	1,280 1,500 2,500 43 2,000 175 2,000 2,500
PIM IPv6 Limits—maximum number of dynamic rendezvous points per multicast group	All platforms, except Summit X430	64
PIM IPv6 Limits—maximum number of secondary address per interface	All platforms, except Summit X430	70
PIM IPv6 Limits—static rendezvous points	All platforms, except the Summit X430	32

Table 2: Supported Limits (Continued)

Metric	Product	Limit
ONEPolicy Number of Roles/ Profiles—maximum number of policy roles/profiles.	Summit X450-G2, X460-G2, X670-G2, X770 All other platforms	63 N/A
ONEPolicy Rules per Role/ Profile—maximum number of rules per role/policy	Summit X450-G2, X460-G2, X670-G2, X770 All other platforms	Up to 952 N/A
ONEPolicy Authenticated Users per Switch—maximum number of authenticated users per switch	Summit X450-G2, X460-G2 Summit X670-G2, X770 All other platforms	Up to 1024 Up to 512 N/A
ONEPolicy Authenticated Users—maximum authenticated users with a combination of TCI disabled/enabled profiles	Summit X450-G2, X460-G2 Summit X670-G2, X770 All other platforms	682–1,022 341–510 N/A
ONEPolicy Authenticated Users per Port—maximum number of authenticated users per port	Summit X450-G2, X460-G2 Summit X670-G2, X770 All other platforms	Unlimited up to 1,024 Unlimited up to 512 N/A
ONEPolicy Permit/Deny Traffic Classification Rules Types—total maximum number of unique permit/deny traffic classification rules types (system/stack)	Summit X450-G2, X460-G2, X670-G2, X770 All other platforms	952 N/A
ONEPolicy Permit/Deny Traffic Classification Rules Types—maximum number of unique MAC permit/deny traffic classification rules types (macsource/macdest)	Summit X450-G2, X460-G2, X670-G2, X770 All other platforms	256 N/A
ONEPolicy Permit/Deny Traffic Classification Rules Types—maximum number of unique IPv6 permit/deny traffic classification rules types (ipv6dest)	Summit X450-G2, X460-G2, X670-G2, X770 All other platforms	256 N/A
ONEPolicy Permit/Deny Traffic Classification Rules Types—maximum number of unique IPv4 permit/deny traffic classification rules (typesipsource / ipdest / ipfrag / udpsourceportIP / udpdestportIP / tcpsourceportIP / tcpdestportIP / ipttl / iptos / iptype)	Summit X450-G2, X460-G2, X670-G2, X770 All other platforms	256 N/A

Table 2: Supported Limits (Continued)

Metric	Product	Limit
ONEPolicy Permit/Deny Traffic Classification Rules Types—maximum number of unique Layer 2 permit/deny traffic classification rules (ethertype/port)	Summit X450-G2, X460-G2, X670-G2, X770 All other platforms	184
Policy-based routing (PBR) redundancy—maximum number of flow-redirects.	All platforms	256o
Policy-based routing (PBR) redundancy—maximum number of next hops per each flow-direct.	All platforms	32o
Port-specific VLAN tags—maximum number of port-specific VLAN tags	All platforms, except Summit X450-G2, X440, and X430	1,023
Port-specific VLAN tags—maximum number of port-specific VLAN tag ports	BlackDiamond X8 and BlackDiamond 8800 xl-series Summit X480 Summit X460-48t Summit X460-24x, X670-48x Summit X670V-48t Summit X670v-48t stack Summit X770, X670-G2 Summit X460-G2 E4G-400 E4G-200	8,090 3,800 7,200 3,400 3,600 7,200 6,400 4,000 3,400 3,800
Private VLANs—maximum number of subscribers. Assumes a minimum of one port per network and subscriber VLAN.	BlackDiamond 8800 c-, e-, xl-series with eight modules of 48 ports 8900-G96T-c modules BlackDiamond X8 series Summit X770 Summit X670-G2, X670v-48t Summit X670 Summit X480 Summit X460-G2, X460 Summit X440 Summit X430 Summit X450-G2 E4G-200 E4G-400	383 767 103 63 47 23 53 25 27 51 11 33

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.	Summit X770, X670-G2, X460-G2, X450-G2 Summit X670, X480, X460, X460, X480 Summit X440 E4G-200, E4G-400	1,024 512 127 512
Private VLANs—maximum number of private VLANs in an L2-only environment.	BlackDiamond 8800 c-, e-series BlackDiamond 8900 series BlackDiamond X8 series E4G-200 E4G-400 Summit X440 Summit X480 Summit X670 Summit X460 Summit X770, X670-G2, X460-G2, X450-G2 Summit X430	384 2,046 2,046 597 1,280 127 597 597 820 1,280 255
PTP/1588v2 Clock Ports	Summit X770, X460-G2, X670-G2, and E4G-200, E4G-400 cell site routers	32 for boundary clock 1 for ordinary clock
PTP/1588v2 Clock Instances	Summit X770, X670-G2, X460-G2, and E4G-200, E4G-400 cell site routers	2 combinations: • Transparent clock + ordinary clock • Transparent clock + boundary clock
PTP/1588v2 Unicast Static Slaves	Summit X770, X670-G2, X460-G2, and E4G-200, E4G-400 cell site routers	40 entries per clock port
PTP/1588v2 Unicast Static Masters	Summit X770, X670-G2, X460-G2, and E4G-200, E4G-400 cell site routers	10 entries per clock type
Route policies—suggested maximum number of lines in a route policy file.	All platforms	10,000
RIP Learned Routes—maximum number of RIP routes supported without aggregation.	All platforms, except Summit X430	10,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
RIP neighbors—maximum number of RIP neighbors.	E4G-200	256
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 X440 Summit X460, X670-G2, X460-G2 Summit X480 Summit X670, X770, X450-G2 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 X480 Summit X460, X670, X670-G2, X460-G2, X770, X450-G2 E4G-200	3,000 3,000 5,000 5,000 3,000 3,000
Spanning Tree (maximum STPDs)—maximum number of Spanning Tree Domains on port mode EMISTP.	All platforms (except Summit X430 and Summit X440) Summit X440 Summit X430	64 32 16
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, X770, X670-G2 Summit X460, X480, X440, X460-G2 Summit X430 Summit X450-G2 E4G-400	256 256 128 50 128 128
Spanning Tree—maximum number of multiple spanning tree instances (MSTI) domains.	All platforms (except Summit X430 and Summit X440) Summit X440 Summit X430	64 32 5

Table 2: Supported Limits (Continued)

Metric	Product	Limit
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.	BlackDiamond X8	500
	BlackDiamond 8800	500
	BlackDiamond 8900 MSM 128/XL	500
	Summit X770, X670-G2, X670v-48t, X670	500
	Summit X480, X460-G2, X460, X450-G2	600
	E4G-200	500
	E4G-400	600
	Summit X440	250
	Summit X430	100
Spanning Tree—maximum number of VLANs on all MSTP instances.	BlackDiamond X8	1,000
	BlackDiamond 8800	1,000
	BlackDiamond 8900 MSM 128/XL	1,000
	Summit X770	1,024
	Summit X670-G2, X670v-48t, X670, X480	1,000
	Summit X460-G2, X460, X450-G2	1,024
	E4G-200	1,000
	E4G-400	1,024
	Summit X440	500
	Summit X430	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 and Summit X440)	4,096
	Summit X440	2,048
	Summit X430	1,024
Spanning Tree (maximum VLANs)—maximum number of STP-protected VLANs (dot1d and dot1w).	BlackDiamond X8	1,024
	BlackDiamond 8800	1,024
	BlackDiamond 8900 MSM 128/XL	1,024
	Summit X770	1,024
	Summit X670-G2, X670v-48t, X670, X480	560
	Summit X460-G2, X460, X450-G2	600
	E4G-200	500
	E4G-400	600
	Summit X440	500
	Summit X430	128

Table 2: Supported Limits (Continued)

Metric	Product	Limit
SSH (number of sessions)—maximum number of simultaneous SSH sessions.	All platforms	8
Static MAC multicast FDB entries—maximum number of permanent multicast MAC entries configured into the FDB.	BlackDiamond 8000 c-, e-, xl-series BlackDiamond X8 series All Summits E4G-200, E4G-400	1,024 1,024 1,024
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
TRILL—trees rooted from switch	BlackDiamond X8 Summit X670, X770	1 1
TRILL—computed trees	BlackDiamond X8 Summit X670, X770	1 1
TRILL—TRILL VLANs	BlackDiamond X8 Summit X670, X770	4 4
TRILL—forwarding VLANs	BlackDiamond X8 Summit X670, X770	4,095 4,095
TRILL—forwarding ports	BlackDiamond X8 Summit X670, X770	All All
TRILL—RBridge FDB entries	BlackDiamond X8 Summit X670 Summit X770	128,000 128,000 288,000
TRILL—ECMP RBridge next hops	BlackDiamond X8 Summit X670, X770	8 8
TRILL—neighbor adjacencies	BlackDiamond X8 Summit X670, X770	32 32
TRILL—nodes	BlackDiamond X8 Summit X670, X770	256 256
TRILL—links	BlackDiamond X8 Summit X670, X770	2,000 2,000

Table 2: Supported Limits (Continued)

Metric	Product	Limit
Virtual routers—maximum number of user-created virtual routers that can be created on a switch. **NOTE:** Virtual routers are not supported on Summit X440 series switches.	BlackDiamond 8000 c-, xl-, xm-series BlackDiamond X8 series E4G-200, E4G-400 Summit X460, X460-G2, X480, X670, X670-G2, X770, X450-G2	63 63 63 63
Virtual router forwarding (VRFs)—maximum number of VRFs that can be created on a switch. **NOTE:** Subject to other system limitations.	All platforms, except Summit X440 and X430	960 *
Virtual router protocols per VR—maximum number of routing protocols per VR.	All platforms, except Summit X440, X430	8
Virtual router protocols per switch—maximum number of VR protocols per switch.	All platforms, except Summit X440, X430	64
VLAN aggregation—maximum number of port-VLAN combinations on any one superVLAN and all of its subVLANs.	All platforms (except Summit X430, X440) Summit X440, X430	1,000 256
VLANs—includes all VLANs. **NOTE:** ExtremeXOS supports only 4,092 user-configurable VLANs. (VLAN 1 is the default VLAN, and 4,095 is the management VLAN, and you may not configure them.)	All platforms	4,094
VLANs—maximum number of port-specific tag VLANs.	BlackDiamond 8800 xl-series only, BlackDiamond X8 series BlackDiamond X8 xl-series Summit X460, X770, X480, E4G-400, X670-G2, X460-G2 Summit X670, X670V-48t E4G-400 E4G-200	1,023 4,093 4,093 1,023 4,093 2,047
VLANs—maximum number of port-specific tag VLAN ports	Summit X460, X670, X670V-48t, X460-G2, BlackDiamond 8800 xl-series only, BlackDiamond X8, E4G-400, E4G-200 BlackDiamond X8 xl-series Summit X770, X670-G2 Summit X480	4,096 32,767 8,192 16,383

Table 2: Supported Limits (Continued)

Metric	Product	Limit
VLANs (Layer 2)—maximum number of Layer 2 VLANs.	All platforms	4,094
VLANs (Layer 3)—maximum number of VLANs performing IPv4 and/or IPv6 routing. Excludes sub-VLANs.	Summit X460-G2, X670, X770, X670-G2, X450-G2, and BlackDiamond X8 Summit X440 Summit X480, X460 E4G-200, E4G-400	2,048 254 512 512
VLANs (maximum active port-based)—(Maximum active ports per VLAN when 4,094 VLANs are configured with default license)	BlackDiamond X8 BlackDiamond 8800 series Summit X770, X670-G2, X670v-48t, X670, X480, X460-G2, X460, X450-G2 E4G-200 E4G-400 Summit X440 Summit X430	32 32 32 12 32 7 2
VLANs (maximum active protocol-sensitive filters)—number of simultaneously active protocol filters in the switch.	All platforms, except Summit X450-G2 Summit X450-G2	15 16
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 Summit X770 Summit X670-G2, X670v-48t Summit X670 Summit X480 Summit X460-G2 Summit X460 E4G-200 E4G-400 Summit X440 Summit X430 Summit X450-G2	with eight modules of 48 ports (383) 8900-G96T-c modules (767) 103 63 47 53 53 57 11 33 25 27 51

Table 2: Supported Limits (Continued)

Metric	Product	Limit
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.	Summit X770, X670-G2, X450-G2, X460-G2 Summit X670, X480, X460 E4G-200, E4G-400 Summit X440	1,024 512 512 127
VLAN translation—maximum number of translation VLAN pairs in an L2-only environment.	BlackDiamond 8800 c-, e-series BlackDiamond 8900 xl-series BlackDiamond X8 series Summit X460 E4G-400, E4G-200 Summit X430 Summit X480, X670, X770, X670-G2, X460-G2 Summit X450-G2 Summit X440	384 2,046 2,046 2,000 2,000 512 2,046 1,024 127
VRRP (v2/v3-IPv4) (maximum instances)—maximum number of VRRP instances for a single switch, with Advanced Edge license or higher.	BlackDiamond X8, 8800 c-series MSM-48c, and BlackDiamond 8900 xl-series 8900-MSM128 Summit X770, X670, X670-G2, X460-G2, X480, X450-G2 E4G-200, E4G-400 Summit X460 Summit X440	511 511 128 255 32
VRRP (v3-IPv6) (maximum instances)—maximum number of VRRP instances for a single switch, with Advanced Edge license or higher. (VRRP-VRRPv3-IPv6)	BlackDiamond X8, 8800 c-series MSM-48c, and BlackDiamond 8900 xl-series 8900-MSM128 Summit X770, X670, X670-G2, X460-G2, X450-G2 E4G-200, E4G-400 Summit X460 Summit X480 Summit X440	511 511 255 255 255 15
VRRP (v2/v3-IPv4/IPv6) (maximum VRID)—maximum number of unique VRID numbers per switch.	All platforms with Advanced Edge license or higher, except Summit X430	7

Table 2: Supported Limits (Continued)

Metric	Product	Limit
VRRP (v2/v3-IPv4/IPv6) (maximum VRIDs per VLAN)—maximum number of VRIDs per VLAN.	All platforms with Advanced license or higher, except for Summit X430	7
VRRP (v2/v3-IPv4/IPv6) (maximum ping tracks)—maximum number of ping tracks per VLAN.	All platforms with Advanced Edge license or higher, except Summit X430	8
VRRP (maximum ping tracks)—maximum number of ping tracks per VRRP Instance under 128 VRRP instances, with Advanced Edge license or higher.	All platforms, except the Summit X440 Summit X440 Hello interval: 20 centiseconds Hello interval: 1 second	8 (20 centisecond or 1 second hello interval) 1 1
VRRP (v3-IPv6) (maximum ping tracks)—maximum number of ping tracks per VRRP Instance under 128 VRRP instances, with Advanced Edge license or higher.	All platforms, except the Summit X440 Summit X440 Hello interval: 20 centiseconds Hello interval: 1 second	8 (20 centisecond or 1 second hello interval) 1 (IPv6) 1 (IPv6)
VRRP (v2/v3-IPv4/IPv6) (maximum iproute tracks)—maximum number of IP route tracks per VLAN.	All platforms with Advanced Edge license or higher, except Summit X430	8
VRRP (v2/v3-IPv4/IPv6)—maximum number of VLAN tracks per VLAN.	All platforms with Advanced Edge license or higher, except Summit X430	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 X480, X670 with 100 DACLs with 500 DACLs Summit X450-G2 with 100 DACLs	 10 3 10 3 4 1 10
XNV authentication—maximum number of VMs that can be processed (combination of local and network VMs).	All platforms, except Summit X430 and X450-G2 Summit X450-G2	2,048 1,024

Table 2: Supported Limits (Continued)

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

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. Based on in “none more-l2” mode.
e. Based on forwarding internal table configuration "more l2”.
f. Effective capacity varies based on actual MAC addresses and VLAN IDs used and hash algorithm selected.
g. Based on “l2-only mode”.
h. Based on forwarding internal table configuration "more l3-and-ipmc”.
i. Based on forwarding external table configuration "l3-only ipv4".
j. The limit depends on setting configured with `configure iproute reserved-entries`.
k. Based on forwarding external table configuration "l3-only ipv4”.
l. Based on forwarding external table configuration "l3-only ipv6”.
m. The IPv4 and IPv6 multicast entries share the same hardware tables, so the effective number of IPv6 multicast entries depends on the number of IPv4 multicast entries present and vice-versa.
n. If IGMP and MLD are simultaneously configured on the switch, the number of effective subscribers supported would be appropriately lessened.
o. Sum total of all PBR next hops on all flow redirects should not exceed 1024.
p. 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.

This chapter contains the following sections:

- Open Issues on page 97
- Known Behaviors on page 101
- Resolved Issues in ExtremeXOS 16.1 on page 102

Open Issues

The following are new open issues for supported features found in ExtremeXOS 16.1.1.

Table 3: Open Issues, Platform-Specific, and Feature Change Requests (CRs)

CR Number	Description
General	
xos0061053	ExtremeXOS supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.
xos0061052	ExtremeXOS accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which reportedly suffer from several cryptographic flaws. An attacker may be able to exploit these issues to conduct man-in-the-middle attacks or decrypt communications between the affected service and clients.
xos0060993	Nessus scan detects the following medium vulnerabilities in ExtremeXOS: • SSH: CBC Mode Ciphers Enabled • SSH: Weak Mac Algorithms Enabled
xos0061129	In a multi-peer setup with many routes (over 150K), a few routes from the preferred peer do not become active in the BGP RIB. Disabling, and then re-enabling peer, restores all routes.
xos0060930	When ONEPolicy is enabled and you reach the configured maximum number of authenticated sessions, sessions continue to attempt to authenticate, and then terminate if successful.
xos0061027	For SummitStacks, creating or deleting non-default QoS profiles may cause some ports to flap.

Table 3: Open Issues, Platform-Specific, and Feature Change Requests (CRs)

CR Number	Description
xos0061492	For the Summit X430 series switches, you can only create around 3,900 VLANs, which is short of the limit of 4,094. For Summit X440 series switches, you can only create 4,094 VLANs and 40–43K VPIF, whereas 53K VPIF was obtainable in ExtremeXOS 15.7.1.
xos0061198	Disabling VPN-VRF affects traffic on another VPN-VRF.
BlackDiamond 8800 Series Switches	
xos0060136	With NetLogin with MAC enabled and with dynamic VLAN configured, if FDB ageout timer is configured as 50, sometimes FDB does not synchronize and the command `show netlogin mac` shows clients authenticated on nlvlan itself.
BlackDiamond X8 Series Switches	
xos0060085	The command `show iproute reserved-entries statistics` displays the incorrect maximum value for IPv4 local hosts: "16,384" versus the correct value of "65,533".
SummitStack	
xos0061784	Failover with ONEPolicy enabled with thousands of user sessions authenticated may result in some sessions being tracked incorrectly on the new master, which may result in inconsistent session behavior for those sessions.
xos0061799	Precedence order between policy port rules and policy MAC-based rules is not preserved following a master/backup failover.
xos0061614	On Summit X450-G2/X440 mixed stacks, executing the command `show stacking` causes the master to become unresponsive after rebooting backup.
Summit X450-G2 Series Switches	
xos0061070	Summit X450-G2 1G switches (X450-G2-xxx-GE4) display incorrect log messages when SFP+ optics are inserted into any of the 1G SFP ports. Incorrect Log message example: "`The configuration for the SF+_LR optic module is not correct - please configure port 50 for auto-negotiation Off and speed 10000`"
xos0061097	On Summit X450G2 stack of eight, back-to-back failovers while sending slow-path traffic across eight slots, produce the following error: `04/01/2015 13:36:33.65 <Erro:Kern.Card.Error> Slot-5: bcm_tx_list() returned -4: Invalid parameter` Issue does not occur, if slow-path traffic is stopped.
Summit X460 Series Switches	
xos0061599	On Summit X460 series switches, after configuring limit learning, traffic is doubled for the non-blackholed MAC addresses, whereas traffic is blocked correctly for blackholed MAC addresses.

Table 3: Open Issues, Platform-Specific, and Feature Change Requests (CRs)

CR Number	Description
Summit Series Switches	
xos0060283	The SMON MIB (RFC 2613) which was used to configure mirroring using SNMP is not available in ExtremeXOS.
ACLs	
xos0061183	On BlackDiamond X8 and 8800 series switches, if failover occurs during an active ESVT test, sometimes it might persist in "running" state.
BGP	
xos0060352	BGP speaker accepts invalid updates (for example, invalid IP addresses such as 0.0.0.0/24). These are installed in BGP LOCAL RIB, as well as in route table.
xos0061411	Route table installs sub-optimal BGP routes (next-hop) to kernel, while the BGP RIB shows different paths when same routes are received from two different peers in local-RIB **Workaround:** Disable, and then enable peer or disable, and then enable BGP.
Clocking (1588v2)	
xos0060785	Precision time feature limitations for ExtremeXOS 16.1: • ExtremeXOS 16.1 slave ports sync to grandmasters, such as Symmetricom, and to other ExtremeXOS 16.1 clocks, but not to ExtrememXOS 15.7, and earlier. If networks of clocks are to be upgraded to ExtremeXOS 16.1, complete the upgrades simultaneously or staged starting closest to the grandmaster. Before beginning a staged upgrade, where an earlier version of ExtremeXOS must sync to an ExtremeXOS 16.1 clock, test the particular configuration beforehand. • ExtremeXOS 16.1 slave clock ports must be configured with the “slave-only” option to sync to other ExtremeXOS 16.1 clocks.
DHCP/BOOTP	
xos0061219	Parallel-mode-enabled DHCP offer is sent using primary IPv4 address to the client for multiple offers received from server for different IPv4 addresses.
FDB	
xos0059655	Error appears when deleting static blackhole FDB entries.
MPLS	
xos0061018	After failover, traffic fails across VPLS configured with 64 LSPs across LAG.
xos0061276	MPLS LSP (LDP/RSVP) is not formed when BGP is used as IGP routing protocol.
xos0061374	With an L2VPN session between two Label Edge Routers (LERs), broadcast packets egressing the LERs are corrupted.

Table 3: Open Issues, Platform-Specific, and Feature Change Requests (CRs)

CR Number	Description
NetLogin	
xos0060488	With upload and download of NetLogin with UPM XSF file, UPM profile is not executed for the user-authenticate and unauthenticate events.
xos0060280	Enabling NetLogin mac on mirrored ports does not produce an error.
xos0061444	With both HTTP and HTTPS enabled, sending HTTP request from NetLogin client causes HTTPS to be given preference and switch returns with HTTPS response.
xos0061546	Client goes unauthenticated after VLAN VSA move from untagged to tagged in MAC base. The following error message appears: `<Info:nl.ClientAuthFailure> MSM-B: Authentication failed for Network Login MAC user 000000000005 Mac 00:00:00:00:00:05 port 8:19`
xos0061820	Dot1x clients move to authentication failure VLAN when web-based NetLogin is enabled globally.
xos0061797	Dot1x client moves to authentication failure VLAN if authentication failed due to incorrect supplicant password or framework failure, such as error in VLAN movement, etc.; even if web-based NetLogin is enabled.
xos0061375	Re-authentication fails for some NetLogin authenticated clients after changing the EXTREME_NETLOGIN_EXTENDED_VLAN VSA (211) with scaled number of NetLogin authenticated clients.
xos0061450	Even though HTTPS is disabled, after reboot ports stay open and HTTPs requests are accepted, and logging on to the switch using HTTP is permitted.
xos0061116	After disabling NetLogin dot1x, attempting to enable NetLogin dot1x produces an error indicating that NetLogin is already enabled on a port.
OSPF	
xos0061100	CPU utilization monitor incorrectly displays 99% CPU usage for OSPF while restarting OSPF process.
xos0060463	OSPFv3 external routes are flushed after the command `restart ports all` is executed in area border router.
ONEPolicy	
xos0061847	If ONEPolicy is enabled and Summit X670-G2 or X770 series switches are inserted and/or a slot is rebooted, the Summit X670-G2 or X770 fails to properly enable ONEPolicy. An error message similar to the following appears: `mm/dd/yyyy hh:mm:ss.ms <Erro:HAL.IPv4ACL.Error> Slot-2: pibAclWrapReserveSlices failed for slot 1 unit 1 with rv=-14` **Workaround:** Change ONEPolicy enable state.

Known Behaviors

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

Table 4: Known Issues, Platform-Specific, and Feature Change Requests (CRs)

CR Number	Description
Summit X460-G2 Series Switches	
xos0059693	Only 'macdest', 'macsource', or 'port' policy rules can be applied to QinQ (that is, double-tagged) packets received on an untagged VMAN port.
ACL	
xos0060980	Two-stage ACL with tunnel configuration does not work when class-id is greater than “1”.
NetLogin	
xos0061484	Ports added using command line are removed by NetLogin on multiple VLAN VSA movement.
xos0060216	NetLogin MAC client does not move to service unavailable VLAN with dot1x MAC- and web-enabled on same port with auth database order as local.
xos0060140	Movement from non-NetLogin VLAN to multiple untagged VLANs does not occur in MAC-based mode.
xos0060351	In NetLogin web non-policy mode, you are unable to add more than one VLAN with VSA 211 (untagged VLAN) in MAC-based mode.
STP/RSTP/MSTP	
xos0058362	Ports configured as auto with auto-edge feature turned on, do not have this status correctly shown in `show <stpd> port` command. Port operation mode appears as “Point-point”. **Workaround:** Port operation mode appears correctly in `show <stpd> port detail` command.

Resolved Issues in ExtremeXOS 16.1

The following issues were resolved in ExtremeXOS 16.1. ExtremeXOS 16.1 includes all fixes up to and including ExtremeXOS 11.6.5.3, and earlier, 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 12.6.5, ExtremeXOS 12.7.1, ExtremeXOS 15.1.5, ExtremeXOS 15.2.4, ExtremeXOS 15.3.3, ExtremeXOS 15.4.1, ExtremeXOS 15.5.1, ExtremeXOS 15.5.2, ExtremeXOS 15.6.1, ExtremeXOS 15.6.2, and ExtremeXOS 15.7.1. For information about those fixes, see the release notes for the specific release.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs)

CR Number	Description
General	
xos0051961	Unable to block IPv6 traffic from SSH/Telnet/Web interface by access-profile policy.
xos0055108	The bound IP address is not being reflected in the command `show vlan`.
xos0055358	Device manager is reporting incorrect slot type after clearing a slot while that slot is disabled.
xos0055399	After multiple failures in a main ring, the Ring Protection Link (RPL) of the sub-ring stays in the blocked state in an RPL neighbor node of the sub-ring causing traffic to fail between the nodes in the sub-ring.
xos0056987	With ELSM enabled on port p1 on two switches, with 10 seconds as the ELSM hello interval, and trap receiver configured on the both switches (or managed in Ridgeline, which configures the trap receiver by itself), and then disable/enable port p1 on both switches. Switches send two linkup traps.
xos0057211	Traffic gets forwarded for blackholed MAC address when limit learning is enabled.
xos0057226, xos0057225	Creating an account with a 32-character long name, and then opening an SSH session from that user, causes the switch to crash.
xos0057254	For every reauthorization of NMS clients the policies attached are unbound and bound back again in the peer (not in the authenticator).
xos0057297	When MD5 password is different for both broadcast server and client, the NTP session is established anyway, and no warning is indicated in "leap indicator".
xos0057391	Configured restrict-list entry is shown as user, and active peer interface is removed from NTP peer when its IP address is configured in deny option.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0057392	NTP session still shows synchronized after disabling port in NTP client interface.
xos0057462	SSL certificate generated in switch uses a weak hashing algorithm, MD5, which is known to be vulnerable to collision attacks.
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.
xos0057517	With global NTP server configured and an NTP session established between server and broadcast client, after disabling NTP, the peer looses it active peer status (*), but for the broadcast client, status (*) is not removed.
xos0057547	The output of the **`show configuration nettools`** command does not show IPv6 smart relay configuration for VLANs in user-created virtual routers.
xos0057570	Executing the command **`configure bootprelay ipv6 prefix-delegation snooping add`**, the ipv6-prefix valid timer alone is updated and gateway is not updated for the same prefix, which is in the prefix delegation snooping table.
xos0057590	Intermittently, 50% traffic loss is seen after one MLAG peer is rebooted.
xos0057599	After giving gateway as the same interface address on VLAN in **`config bootprelay ipv6 prefix-del snooping add`** command, error does not occur and the same route is added in snooping table and rtmgr table.
xos0057746	Dynamic routes learned using bootp for indirect routes are not deleted after disabling the baseline protocol (Ripng/Static route) for the gateway.
xos0057849	Client session using ciphers aes128-ctr, aes192-ctr, aes256-ctr is not working.
xos0057976	DHCP bootprelay option 82 with aggregation port shows incorrect circuit ID.
xos0058324	Add port number to output of all **`show port`** commands along with existing display string.
xos0058325	Add multicast tx counter to **`show port stat`** command.
xos0058326	Add a flag that indicates MLAG membership to the output of the **`show port info`** command.
xos0058327	In **`show port <port> info detail`** command, order the VLAN listing alphabetically.
xos0058337	Generate Syslog message or trigger an SNMP trap when the log memory buffer is filled up to 90% of configured log lines.
xos0058349	Enabling DHCP on any VLAN with IP address already configured does not produce error.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0058384	XNV Dynamic VLAN: With VM-tracking enabled on MLAG peer ports, dynamic VLANs are not created for tagged and untagged traffic.
xos0058393	The TCL command `clock format` is not available for CLI scripting and attempting to use it produces an error.
xos0058668	After rebooting DHCPv6, client remains in rebooting state.
xos0058719	Dynamic routes added by prefix delegation snooping remain active even after disabling and unplugging the client connected to the port.
xos0059173	Traffic loss occurs since the destination IP address is missing in kernel after port fail.
xos0059222	SFLOW-sampled packets are flooded out of VLANs when these same packets are software learned.
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**.
xos0059247	ARP entries incorrectly point to ISC port after MLAG peer is rebooted.
xos0059315	Unable to add static routes with tunnel address as the next-hop.
xos0059524	Link status is incorrect when auto-polarity setting is off.
xos0059558	XNV Dynamic VLAN: Running the command `unconfigure vm-tracking local-vm mac-address 00:00:00:00:00:01 vlan-tag`, FDB is not removed from dynamic VLAN and the command `show vm-tracking` displays no entries.
xos0059581	Rtmgr process ends unexpectedly when OSPF external routes are deleted from the route table.
xos0059597	Static ARP entries are created as blackhole in HAL IPV4adj, thus the next hop information for the routes with those adjacency as gateway are not programmed properly in l3 defip table.
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.
xos0059851	When a DHCP client receives an IP address that conflicts with a static IP address configured in a VLAN, the static IP address is removed from the VLAN and the DHCP client stops.
xos0059952	XNV Dynamic VLAN: After disabling dynamic VLAN on vmt-enabled port, the "v" flag is not removed from the output of the `show fdb` command.
xos0059983	RADIUS shared secret password obfuscation is too weak.
xos0060088	Kernel oops triggered rarely during continuous addition/deletion of ARP entries for long duration in presence of high CPU utilization.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0060100	Kernel oops occurs due to memory corruption caused by slow-path forwarded traffic.
xos0060119	Changing the primary TACACS server configuration locks out TACACS-authenticated users.
xos0060228	HAL process ends unexpectedly in rare circumstances while rebooting switch with default speed configuration on 10G ports
xos0060228	HAL process ends unexpectedly in rare circumstances while rebooting switch with default speed configuration on 10G ports.
xos0060478	There is no command to configure the idle timeout of SFTP sessions. The idle timeout is fixed at 60 minutes.
xos0060713	Executing the command `clear cpu-monitoring` sets the dirty bit(*).
xos0060825	Double-tagged CFM frames are dropped by kernel in VMAN environment.
xos0060977	MPLS traffic is egressing switch with incorrect label causing packet loss.
xos0061178	Dynamic ACL for gratuitous ARP violation on LAG member ports are incorrectly getting installed on LAG master ports.
xos0061517	LACP Adjacency failed while forwarding the PDU with l2pt profile over L2VPN tunnel when MPLS PHP enabled.
BlackDiamond 8800 Series Switches	
xos0061338	PSTAG packets are fail over fabric link.
xos0059736	Process rtmgr ends unexpectedly with signal 11 after executing the command `disable bgp`.
xos0059648	Static ARP entries are not properly synced with new Master Switch Fabric Module after failover.
xos0059009	After deleting ingress and egress ports from one slot and adding them to another slot, MPLS LSP routes do not get installed in hardware.
xos0058972	Layer 2 packets are not forwarded with non-multicast destination MAC addresses for static multiport FDB entries.
xos0058895	With a two-tier MLAG and PVLAN configured, process mcmgr ends unexpectedly with signal 10 and 11 after disabling, and then re-enabling MLAG ports, and disabling remote MLAG peer ISC ports.
xos0058776	Process MPLS crashed with signal 11 after disabling MPLS with broadcast traffic on pseudowire.
xos0058394	BGP routes are missing in XL-series modules after disabling, and then enabling, BGP with 20,000 routes.
xos0057624	Traffic loss occurs on PVLAN after restarting VRRP process in VRRP Master switch.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0057469	After master switch fabric module. (MSM) failover, NMS period re-authentication does not work.
xos0055337	Issuing the command `clear slot` on a disabled slot does not clear the pre-existing port numbers associated with the previous module type in that slot. I/O module stays in VLAN sync.
xos0050664	Process DCBGP ends unexpectedly with signal 11 while rebooting neighbor switches in a scaled, multi-homed setup.
xos0050732	On BlackDiamond 8800 series switches, the process DCBGP ends unexpectedly with signal 6/11 after rebooting the switch.
xos0054970	BlackDiamond 8800-xl cards and Summit X480 series switches should not allow Layer 2 Protocol Tunneling and Filtering to be configured over VPLS/VPWS.
BlackDiamond X8 Series Switches	
xos0060180	Data traffic over L3VPN: From Core to Access on 100G-XL modules traffic is dropped completely, This issue does not occur while using ports from BDXA-10G48T card.
xos0060073	On the BDXB-100G4X-XL module, known unicast traffic is flooded across all PSTag ports of VLAN, instead of going out using one port even though MAC address was learned.
xos0059953	With DHCP client and server configuration, process Nettools ends unexpectedly with signal 6 after running failover.
xos0059927	For the 100G4X and 100G4X-XL modules, tagged data traffic is not going to untagged service VMAN after deleting tagged service VMAN from the VPLS instance, and then creating new untagged service VMAN and attaching it to the VPLS.
xos0059710	Ports on the 100G4X I/O module are reported as having their links down.
xos0059534	Running two failovers leads to traffic drop for some unicast streams.
xos0059343	The process snmpMaster might end unexpectedly during upgrade from ExtremeXOS 15.3 to 15.5 for some SNMP community names.
xos0059156	VRRP control packets are dropped due to congestion in tx queue under scaled environments.
xos0056300	Traffic does not switch back to primary port when smart redundancy is enabled.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description

xos0056773	Resetting a connected I/O fabric module, produces the following error messages:
	`04/07/2014 10:09:10.07 <Erro:Kern.Card.Error> Slot-7: pca9506_read, not enough buffer provided (need 5 bytes, have 1 bytes)`
	`04/07/2014 10:09:10.57 <Erro:Kern.Card.Error> Slot-7: i2c-1: bus busy, addr=0x23 rw=1 cmd=0x0 size=2 retry=0`
	`04/07/2014 10:09:10.57 <Erro:Kern.Card.Error> Slot-7: Failed to read data from INPUT_PORT_0_COMMAND (-145)`

xos0057560	Accessing ScreenPlay while running a script can cause the thttpd process to end unexpectedly with the following error: `<Erro:DM.Error> MM-A: Process thttpd Failed MM-A rebooted`
xos0057827	After master switch fabric module. (MSM) failover, L2 MC traffic destined to IGMP receivers is not forwarded from ports that are the IGMP member ports sending joins.
xos0058375	ACLs to match VLAN-ID, CVID parameters do not work for slow path forwarded packets.
xos0058413	BDXB-100G4X module reboots with kernel oops with scaled route traffic above 12K IPv4 routes and above 32 IPv4 local hosts.
xos0058553	On BlackDiamond X8 series switches, in large topology (~2,000 pseudo-wires and lots of LSPs and ILM), disabling all VPLS sessions on switch causes SMAC learning to take longer than usual if the traffic comes from a different pseudowire. Traffic loss occurs during this interval.
xos0058615	ESVT: Loopback port fails to indicate "Link State" of "L". The loopback port is physically looped back. However, if user traffic is in the VLAN, then potentially unwanted traffic can get looped causing issues.
xos0058640	Traffic forwarding inconsistencies occur after restarting MPLS process.
xos0058793	BDX8 XL modules flood decapsulated VPLS traffic, causing bandwidth problems.
xos0058814	Traffic fails to transmit over pseudowire with attachment circuit VMAN carrying CEP-CVID.
xos0058842	Tagged VLAN traffic is dropped at ingress of 100G4X-XL module port, when the same port is added to another CEP-VMAN VPLS. This issue does not occur on non-100G4X-XL modules/ports.
xos0058870	MPLS encapsulation and decapsulation fail when network ports are part of 100G slot.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0058979	With distributed ARP mode on, L3 traffic is slow-path forwarded when next hop entry (IPv4 adjacency) is stored in IPv4 LPM and IPv4 LPM is in external TCAM. If IPv4 adjacency is stored in IPv4 L3 hash table (that is: full LPM or iproute reserved-entries set to maximum), the same traffic is forwarded correctly in hardware. Traffic is also forwarded correctly in hardware if IPv4 LPM table is internal (TCAM mode set to "none").
xos0059104	ACL policies are not installed in hardware after management module failover.
Summit Family Switches	
xos0056230	SNMP query on ?extremeMemoryMonitorsystemTable? does not show backup information, if slot2 is master and slot1 is backup.
xos0057106	When mirroring is configured to be triggered through clearflow, mirroring does not work and produces the following error: `06/26/2014 17:14:16.40 <Warn:HAL.IPv4ACL.Warning> : Could not enable mirroring for ACL rule since mirror acl-rule-1 is not active.`
xos0058241	XNV Dynamic VLAN: After disabling, and then enabling, vm-tracking, the `show vm-tracking` command displays the incorrect number of network VMs authenticated with NMS as the authentication method.
xos0058253	Label-switch paths (LSP) does not work when iproute sharing max-gateways is equal to “4”.
xos0058841	NetLogin dot1x IPARP entry is not shown after the iparp detection is turned off and then on.
xos0059030	ARP entries incorrectly point to ISC port after MLAG peer is rebooted.
xos0059248	Identity management: Identity management ends unexpectedly with signal 11 repeatedly when NetLogin MAC addresses are scaled to 512–3,000.
xos0059345	Summit X460-G2-1G switches do not produce warning log messages (not compatible) when 100LX10 optics are inserted in the highest numbered 1G ports.
xos0059406	AVB ACLs are not getting unbound when AVB ports transition from non-boundary to boundary ports.
xos0059950	In Summit series switches, you cannot download bootROM images from memory card.
SummitStack	
xos0060362	VPWS/VPLS traffic stops after stack failover, and then failback, when access and core ports are from different slots.
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.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0060115	Expected <Info:Kern.Info> log messages are not shown for log filter events.
xos0059462	Timezone configuration is not applied to standby nodes after stack reboot.
xos0059049	SNMP: Traversing the EntityPhysicalTable takes around about four minutes.
xos0058851	IPFIX egress interface field reports an incorrect value for a SummitStack.
xos0050066	Process ipSecurity PID 1588 signal 11 ends unexpectedly with cleanup session in IPAddresecurity.
xos0056075	After issuing the command `restart process ospf-5` on a SummitStack, H-VPLS (spoke) nodes fail to encapsulate packets to VPLS pseudowires. Traffic is restored after about 15 minutes.
xos0057438	Memory depletion occurs in Backup/Standby nodes of SummitStack with highly scaled IPFIX flow records.
xos0057767	Static FDB associated with VPLS service VLAN is not programmed in hardware after reboot when "disable learning" is configured.
xos0058133	SummitStacks use slot MAC address in DHCP packets when enabling DHCP on Management VLAN.
xos0058145	Traffic is dropped when enabling MAC-Locking on VMAN CEP ports that are part of the stack backup node. Issue does not occur when ports are on master node in stack.
xos0058809	Process "vlan" doe not respond after removing and unconfiguring slot in a stack.
Summit X430 Series Switches	
xos0057028	In Summit X430 series switches, kernel gets stuck for few seconds while installing boot v1.0.1.5 from ExtremeXOS.
Summit X440 Series Switches	
xos0059571	When creating many VLANs on adjoining devices with MVRP enabled, switch has many dynamic VLANs created on it, causing the switch to reset.
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.
xos0050402	The command `enable inline-power legacy` does not power up pre-standard PoE devices, such as Cisco phone 7940/7960 that do not work with IEEE 802.3af standard detection and legacy capacitive detection. The `enable inline-power legacy` command now powers up legacy PoE devices that rely on the capacitive detection instead.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0054084	In Summit X440 stacks with about 500 identities, restarting the idmgr process, causes the IdMgr process to end unexpectedly with signal 11.
xos0058547	In Summit X440-24t switches, the maximum hotspot temperature should be changed to 70 C.
xos0058889	The output of the `show fans` command always indicates no fan installed (`Empty`).
xos0059380	Executing the command `l3 l3table hash VRF=0 IP=<IPaddr>` in BCM shell produces a Kernel oops.
Summit X460 Series Switches	
xos0056342	Misleading power supply unit (PSU) traps are sent when PSUs are inserted or powered on/off.
xos0058053	Summit Stack run failover takes longer than usual time to boot the backup node.
xos0058250	Installing an ExtremeXOS image on a SummitStack after copying the image to the switch using SCP fails when there is no backup module assigned to the stack.
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.
xos0059671	On Summit X460 series switches with 750 W power supplies installed, log messages "`Power usage data unknown`" appear.
xos0060057	Root port only sends STP agreement BPDU for the CIST and first two MSTIs.
xos0060517	When the service VLAN and L2 VMAN (untagged port) is configured on same port, after deleting port from VMAN, service VLAN's traffic is affected.
Summit X460-G2 Series Switches	
xos0060736	gPTP propagation delay is not calculated correctly and ports become AVB incapable.
xos0061150	In X460-G2, CLI allows half-duplex config for ports even it is not supported.
xos0059827	During Summit stack failover, Kernel oops appears infrequently, caused by corruption in VR ID of resolved ARPs.
xos0059763	In Summit X460G2-24x-10G switches, the first VIM-2x(10G port 33) sometimes remains in ready state after reboot. This problem does not occur with the second VIM-2x port (34).
xos0059652	Combo copper ports do not work in Summit X460G2-24x-10G4 switches until SFP is also connected.
xos0055189	In Summit X460-G2 stacks, the command `show power` fails to display power usage and produces the error "`Failed reading Slot-B power on time`" during slot reboot.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0059395	Summit X460-G2 series switches do not produce warning log message (not compatible) when 100LX10 optics are inserted in the highest numbered 1G ports.
xos0055999	For Summit X670-G2 and X460-G2 series switches, currently the ENTITY-MIB:entPhysicalIsFRU for fan and power modules shows the values as FALSE. However since these fan modules and power modules are replaceable units, this should be shown as TRUE.
xos0058438	With MLAG and VRRP IPv6 configuration running for two days, Watchdog timer error, watchdog reboot, and memory depletion occur.
xos0058517	The command `enable vman cep egress filtering` incorrectly drops VLAN traffic if a port is part of both a VMAN and a VLAN.
xos0058896	Running slow path traffic for long durations causes Summit X460-G2 stack instability.
xos0059240	High CPU utilization and MAC learn thrashing occurring on fabric links forming a X460-G2 stack.
xos0059577	On Summit X460G2 series switches, can?t install ExtremeXOS SSH XMOD image.
Summit X480 Series Switches	
xos0059471	STP1D-ELSM: Traffic is not forwarding to STP1D "FORWARDING" port in stack/chassis.
Summit X670 Series Switches	
xos0059128	In Summit X670 series switch, all LEDs are blinking at a faster rate.
Summit X670-G2 Series Switches	
xos0060948	Kernel crashes on Summit X670G2-48x-4q switches when stack ports are configured for v80 stacking.
xos0059445	Link flaps occur when stacks are firmed with 3 m/5 m QSFP+ passive copper cables.
xos0058867	In Summit X670G2-48x-4q stack, system crash occurs with "`Process ipSecurity pid 1644 died with signal 11`" error after deleting VLAN with aged timer for ARP entry configuration from IPAddreSecurity.
Summit X770 Series Switches	
xos0059573	Factory installed image incorrectly references “x450” in the image name.
xos0058536	In a SummitStack, with X770 and X670-G2 series switches, after a run failover on master Summit X770, backup Summit X770, does not sync. The reverse works fine, and the Summit X670-G2 comes to synced state.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0055746	Stacking port link flap occurs on Summit X770 series switches when using 3-meter QSFP+ cables.
xos0053310	On Summit X770 series switches, partitioned 10G ports 77,78,81,82 do not appear in the output of the `edp ports all` command. Due to this, bi-directional traffic across these ports is not working even though the port is up with speed 10G.
xos0055686	VPLS: IGMP hello packets received on pseudowire are not forwarded to service ports on Summit X770 series switches.
E4G-200 Cell Site Routers	
xos0060715	SNMP get does not return the product name for E4G-200-12x.
xos0058951	Executing `show ces ces1 details` command when CES state is “signaled” causes process ces pid to end unexpectedly with signal 6.
xos0058239	In E4G-200 cell site routers, power supply status displays incorrect value in the output of the `show power` command.
ACL	
xos0054720	With network-zone configured, the command `show access-list port 1:1 detail` reverses the IP address match criteria.
xos0058810	Both `show access-list usage acl-slice` and `debug hal show device acl-slice slot <slot> unit <unit>` commands show the same output.
xos0059330	With dual master switch fabric module (MSM) installed, clear-flow ACL intermittently fails.
BGP	
xos0060670	Switch becomes unresponsive and resets after issuing command `show bgp neighbor`.
xos0061310	DCBGP process ends unexpectedly after disabling BGP peer switches after the switch receives VPNv4 routes with the same next hop from two different L3VPN peers.
ERPS	
xos0059320	CCM is dropped for "Hardware Down MEPs" when they are received on ports that are blocked by ERPS.
FDB	
xos0059146	With port-specific tags configured, source MAC addresses are removed and re-learned for all incoming ARP packets causing flooded traffic a for short time interval.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
IP General	
xos0050794	DCBGP process ends unexpectedly with signal 11 when rebooting or issuing the command `disable/enable bgp` on neighboring switches.
xos0058418	With inter VR routing configuration, traffic flows at line rate. After disabling the egress port, kernel panic occurs.
xos0058432	In Summit X670-G2 and X770 series switches for internal-table configuration, more L2 IPv4Mcast cache entries are limited to 4,000 instead of 8,000.
Identity Management	
xos0058112	The output of the command `show identity-management entries` displays the ID name and domain name as null.
xos0058481	ACL error occurs when identity management detections are turned on and off.
MLAG	
xos0056340	Unknown Layer 2 traffic from Isolated subscriber VLANs are forwarded to the remote MLAG ports, even though local MLAG ports are up.
xos0058153	MLAG state flaps continuously when MLAG peers have different versions of ExtremeXOS.
xos0060693	FDB entries in MLAG peers are learned in the incorrect VMAN if the MLAG port is untagged in one VMAN and has CEP CVID configuration in another VMAN.
MPLS	
xos0060346	Traffic is not forwarded to secondary path after failover when LSP is added to VPLS.
xos0059729	Packet duplication occurs after upgrading one of the provider edge (PE) switches in VPLS tunnel.
xos0059266	VPLS: Traffic is dropped after RSVP LSP failover. Failover from primary path to secondary path (same LSP) works.
xos0058948	Changing service VLAN tag results in FDB not being learned. Learning resumes when you revert the VLAN tag. This issue on both BlackDiamond X8 and Summit X670G2 stacks.
xos0058785	Changing LSR-id of P node causes data traffic drop at ingress of a VPLS provider edge (PE) switch.
xos0058502	Traffic for existing VPLS instance is affected, when a port is removed from untagged VMAN of different VPLS instance.
xos0059733	LSP load sharing does not occur on Summit X460-G2 and BlackDiamond X8-100G4X switches.
xos0058460	Unable to configure multiple LSP from core node to spoke node in Summit X460-G2 and X670-G2 series switches.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0058395	STP is not working properly when added to VPLS.
NetLogin	
xos0061069	In Netlogin ISP mode, client MAC addresses configured as static FDBs are removed after reboot.
xos0060633	Possible memory leak while cleaning the authVLANlist in NetLogin during unautherization.
xos0059434	Unable to re-initialize MAC-authenticated client using extremeMacAuthClientInitialize OID.
xos0058929	The number of reported NetLogin authenticated clients reduces to zero even though clients are in fact authenticated. This happens only when the protocol-order is configured as dot1x> mac> web and some re-authentication-timer is configured.
xos0058610	On disabling NetLogin dot1x, several clients' authenticated value is not cleared fully and the command `show netlogin dot1x` shows the number of clients authenticated as "6" instead of "0".
xos0059557	Executing the command `configure netlogin add mac-list 00:00:00:11:11:11 000000111111 ports 1` produces the following error: `ERROR: Invalid mask length supplied, must be between 1 and 48. Error was thrown and the mac list was not created`
xos0059592	NetLogin authentication protocol order resets to default after save, reboot, and then restart.
xos0059593	The `show netlogin mac` command output no longer shows the default mac mode configuration.
xos0058054	Disabling NetLogin mac,dot1x,web-based is not disabling NetLogin mac,dot1x,web-based.
xos0053634	MAC-lockdown-timeout on user ports does not work as expected if Netlogin is enabled on those ports.
OpenFlow	
xos0061479	Openflow process signal 6 ends unexpectedly on Summit X460 stacks.
xos0060009	Some flows cannot be installed when OpenFlow FDB table is turned on.
xos0059776	When MS Lync application (MSLync 2.0 solution) attempts to install a LYNC OpenFlow flow with action set queue and set field IP DSCP with Hybrid Mode enabled, a OFPBAC_BAD_QUEUE error occurs. The flow is not installed. The flow is properly installed after rebooting the switch.
xos0059621	Lync should be able to install flows for hybrid VLANs without knowing the VID for those VLANs.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
xos0059604	In a stacked environment the Datapath ID changes with every stack reboot. This may cause OneController to go out of sync as the NodeID change s(stale nodes and flows in OneController).
xos0059288	Cannot install multiple XMOD files in BlackDiamond 8800 and BlackDiamond X8 switches due to lack of space.
xos0059160	Sending a flow install with the vlan-id-present field set to false from the OneController causes the flow to fail to install with an ExtremeXOS bad port error message. The flow installs properly by setting the field to true
xos0059139	OneController uses set_field:0->vlan_vid for strip VLAN action causing an ExtremeXOS error.
xos0058978	Flows with both output port and controller actions cannot be added.
xos0058117	After enabling, and then disabling, OpenFlow globally and on a VLAN with standard mode, you cannot enable learning on the VLAN anymore.
Optics	
xos0057346	Link flaps occur when optics such as 10/100/1000 Base-T or 100FX is inserted into Summit X460-G2 and X480 series switches.
xos0059579	SFP+ ports do not link up with active optical breakout cable. Cable is identified as not supported and treated as a 3rd-party cable.
OSPF	
xos0059574	OSPF packets larger than 8,192 are dropped even with jumbo frame enabled.
xos0056243	OSPF process ends unexpectedly during frequent route re-calculation caused by switch reboot or master switch fabric module. (MSM) failover or BFD flap events.
xos0058221	Rarely, OSPFv3 process ends unexpectedly with signal 11 when link flaps occur.
xos0059305	OSPF consumes a large amount of memory when a large number of Link State Acknowledgment packets are queued up for transmission.
PoE	
xos0058994	POE is not delivering power to several model phones when legacy mode is enabled.
Python	
xos0060600	EPM process signal 5 ends unexpectedly when creating a new process with a dash in the name.

Table 5: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) (Continued)

CR Number	Description
RIP	
xos0058683	RIP packets are dropped when another VLAN has a secondary IP address configured.
SNMP	
xos0060103	SNMP walk does not return all VLANs under extremePortVlanStatsTable.
xos0058130	Q-Bridge MIB: On doing SNMP walk for dot1qVlanStaticEgressPorts and dot1qVlanStaticUntaggedPorts for ports in different slots, invalid port number values are returned.
xos0058110	Q-BRIDGE MIB: dot1qPortGvrpStatus and dot1qGvrpStatus should return value as "2" with MVRP disabled globally and at the per port level, but it returns value as "0" which is incorrect as per RFC.
TWAMP	
xos0060243	The process rtmgr ends unexpectedly while changing IP address on VLAN when switch is booted with configuration such that an IP route has local or loopback interface address as gateway.
xos0060780	With VRRP enabled, local VLAN's direct route is not installed in hardware after reconfiguring the VLAN's IP address.
VLAN	
xos0058698	Traffic stops egressing after adding the egressing port to some other VLAN that is having PSTag configuration with other ports.
xos0057435	Packets are dropped when learning is disabled in a VLAN when its associated ports are configured with limit learning in another VLAN.
VRRP	
xos0060794	VRRP advertisement interval configuration got changed after upgrading EXOS from 12.6 to 15.4 or above releases. Issue happens only when interval is configured in milliseconds.
xos0053821	IPv6 neighbor advertisements for VRRP virtual IP address uses virtual MAC address as source MAC address instead of switch MAC address.
xos0061222	Gratuitous ARP packets for VRRP virtual IP addresses have ARP sender addresses as physical MAC addresses, instead of VRRP virtual MAC addresses.
XML	
xos0058020	When both the HTTP and HTTPS are enabled, only HTTPS works,