Extreme®
Connect Beyond the Network

ExtremeXOS Release Notes

Software Version ExtremeXOS 22.1

121169-00 Rev 01

Published November 2016

Legal Notice

Extreme 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 on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Support

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

For information, contact:
Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

Preface

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
☞	General Notice	Helpful tips and notices for using the product.
📝	Note	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚡	Warning	Risk of severe personal injury.
New	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words enter and type	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Platform-Dependent Conventions

Unless otherwise noted, all information applies to all platforms supported by ExtremeXOS® software, which are the following:

- ExtremeSwitching® switches
- Summit® switches
- SummitStack™

When a feature or feature implementation applies to specific platforms, the specific platform is noted in the heading for the section describing that implementation in the ExtremeXOS command documentation (see the Extreme Documentation page at http://documentation.extremenetworks.com). In many cases, although the command is available on all platforms, each platform uses specific keywords. These keywords specific to each platform are shown in the Syntax Description and discussed in the Usage Guidelines sections.

Terminology

When features, functionality, or operation is specific to a switch family, such as ExtremeSwitching™ or Summit®, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the *switch*.

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at internalinfodev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- Global Technical Assistance Center (GTAC) for Immediate Support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge — Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub — A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal — Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related Return Material Authorization (RMA) numbers

Related Publications

ExtremeXOS Publications

- *ACL Solutions Guide*
- *ExtremeXOS 22.1 Command Reference Guide*
- *ExtremeXOS 22.1 EMS Messages Catalog*
- *ExtremeXOS 22.1 Feature License Requirements*
- *ExtremeXOS 22.1 User Guide*
- *ExtremeXOS OpenFlow User Guide*
- *ExtremeXOS Quick Guide*
- *ExtremeXOS Legacy CLI Quick Reference Guide*
- *ExtremeXOS Release Notes*
- *Extreme Hardware/Software Compatibility and Recommendation Matrices*
- *Switch Configuration with Chalet for ExtremeXOS 16.2 and Earlier*
- *Using AVB with Extreme Switches*

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing

1 Overview

These release notes document ExtremeXOS 22.1 which adds features and resolves software deficiencies.

New and Corrected Features in ExtremeXOS 22.1

This section lists the new and corrected features supported in the 22.1 software:

Change of Authorization (Dynamic Authorization)

The RADIUS protocol, defined in (RFC2865), does not support unsolicited messages sent from the RADIUS server to the Network Access Server (NAS). However, it may be desirable for changes to be made to session characteristics, without requiring the NAS to initiate the exchange. For example, it may be desirable for administrators to be able to terminate user session(s) in progress. Alternatively, if the user changes authorization level, this may require that authorization attributes be added/deleted from user session(s). To overcome these limitations, several vendors have implemented additional RADIUS commands to enable unsolicited messages to be sent to the NAS. These extended commands provide support for Disconnect and Change-of-Authorization (CoA) packets.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Limitations

The following features of Change-of-Authorization (RFC5176) are not implemented in ExtremeXOS:

- Reverse Path Forwarding Check—Typically this is used in a proxy scenario. This check is used to determine if the IP address indicated by the RADIUS attributes is a routable destination address for a request sent by the switch software.
- IPSEC encryption—End-to-end encryption of both the RADIUS requests and responses.
- Disconnect-Request and Change-of-Authorization packets identifying sessions with anything other than the Calling-Station-Id attribute containing a properly formatted MAC address. In addition to the Calling-Station-ID attribute, you can also use a NAS-Port attribute, which indicates the index of the specific port the session is connected to.
- Acct-Session-Id attribute—This is an alternate means of session identification. Sessions are currently uniquely identified by port and MAC address pair.
- Retransmissions of Disconnect-Request or Change-of-Authorization ACK and NAK packets—Retransmissions of packets is the responsibility of the device initiating the dynamic authorization transactions.

New CLI Commands

```
enable radiusdynamic-authorization
```

```
disable radiusdynamic-authorization
```

```
configure radius dynamic-authorization index server [host_ipaddr |
host_ipV6addr | hostname] client-ip [client_ipaddr | client_ipV6addr] {vr
vr_name} {shared-secret {encrypted} secret}
```

```
show radius dynamic-authorization index
```

Changed CLI Commands

Changes are underlined.

```
unconfigure radius {dynamic-authorization [server index]
```

The following command was updated to show dynamic authorization status:

```
show radius
```

Link Layer Discovery Protocol (LLDP) System Name Added to Show Output

The output of the `show lldp neighbors` command now shows the system name.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Changed CLI Commands

The following is the revised output of the `show lldp neighbors` command:

```
# show lldp neighbors
===============================================================================
        Neighbor           Neighbor                          Neighbor
Port    Chassis ID         Port ID            TTL     Age    System-Name
===============================================================================
1:2     00:04:96:99:8C:31  1:23               120     7      Not-Advertised
```

```
11:123  FF:FF:FF:FF:FF:FF  FF:FF:FF:FF:FF:FA  65535   65535 Extreme-440-
G2
1:21    02:04:96:9A:30:BF  2:27               120     27    Extreme-460-G2-Stac
k-switch
1:27    02:04:96:9A:30:BF  2:27               120     0     Vaishnaviv123456789
0123456789012345678901234567890123456789012345678901234567890123456789012345678
9012345678901234567890123456789012345678901234567890123456789012345678901234567
890123456789012345678901234567890123456789012345678901234567890123456789012345
===============================================================================
```

Untagged Port Auto-Move Option

This feature allows you to globally enable moving of untagged ports directly (without having to first change the port VLAN configuration—delete the port) from untagged VLANs to either different untagged VLANs or tagged VLANs. You can elect to turn this feature off, on, or have it on, but inform you when such a move occurs.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

New CLI Commands

```
configure vlan untagged-ports auto-move [ on | off | inform ]
```

Changed CLI Commands

The following command is changed to show this feature's status (shown in bold):

```
show vlan
```

```
# show vlan
Untagged ports auto-move: Off
--------------------------------------------------------------------------------------
Name            VID  Protocol Addr       Flags                Proto  Ports  Virtual
                                                                         Active router
                                                                         /Total
---------------------------------------------------------------------------------------
Default         1    ---------------------------T---------------  ANY    2 /33  VR-Default
Mgmt            4095 -------------------------------------------  ANY    1 /1   VR-Mgmt
...
```

Historical List of Recently Executed CLI Commands (Journal)

ExtremeXOS 22.1 retains a list of the most recently executed CLI commands (journal). The journal retains as many as 200 commands along with the timestamp and user name. Commands are saved even after logging off, rebooting, or switch crashes.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Limitations

- Commands executed using North Bound interfaces (For example: SNMP, Extreme Management Center, web) are not supported.
- The command `show cli journal` is not checkpointed in backup slot.

New CLI Commands

```
show cli journal
```

```
configure cli journal size size
```

Changed CLI Commands

The `show management` command now shows the configured size of the journal.

New ONEPolicy Profiles

The following new ONEPolicy profiles are available:

Table 3: Platform Rule Allocation

Table Profile Name	Table Name	X460-G2, X450-G2	X670-G2 X770	X440-G2 X620
Default	Auth Users (max) MAC Rules IPv6 Rules IPv4 Rules L2 Rules ExtremeXOS App/ System Rules	1,024 256 256 256 184 2,048 (8 Slices)	512 256 256 256 184 2,048 (4 Slices)	256 0 0 256 184 1,024 (4 Slices)
less-acl more-ipv4	Auth Users (max) MAC Rules IPv6 Rules IPv4 Rules L2 Rules ExtremeXOS App/ System Rules	1,024 256 256 768 184 1,024 (4 Slices)	512 256 256 256 184 2,048 (4 Slices)	256 0 0 256 184 1,024 (4 Slices)
less-acl more-ipv4-no-ipv6	Auth Users (max) MAC Rules IPv6 Rules IPv4 Rules L2 Rules ExtremeXOS App/ System Rules	1,024 256 0 1,024 184 1,024 (4 Slices)	512 256 0 512 184 2,048 (4 Slices)	256 0 0 256 184 1,024 (4 Slices)
more-ipv4-no-ipv6	Auth Users (max) MAC Rules IPv6 Rules IPv4 Rules L2 Rules ExtremeXOS App/ System Rules	1,024 256 0 512 184 2,048 (8 Slices)	512 256 0 512 184 2,048 (4 Slices)	256 0 0 256 184 1,024 (4 Slices)
more-mac-no-ipv6	Auth Users (max) MAC Rules IPv6 Rules IPv4 Rules L2 Rules ExtremeXOS App/ System Rules	1,024 512 0 256 184 2,048 (8 Slices)	512 512 0 256 184 2,048 (4 Slices)	256 0 0 256 184 1,024 (4 Slices)

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Removal of SNMP Default Users and Community String

Previous versions of ExtremeXOS came with default SNMP behavior that when not configured prudently could be potentially exploited. In ExtremeXOS 22.1, this default behavior is removed or the user is guided to manage SNMP access more carefully:

- SNMP v1/v2c: As with most of the vendors, Extreme switches previously had default community strings for read-only and read-write access ("public" and "private," respectively). Many network administrators change community string to keep intruders from getting their network information. ExtremeXOS 22.1 removes SNMP default community names "private" and "public".
- SNMP v3: SNMP request authentication can be done using User-based Security Model (USM). In USM, there are users that can have associated password for authentication and privacy. ExtremeXOS 22.1 removes default values for USM.

During initial switch setup, you are prompted to configure SNMP community string and SNMPv3 user as desired.

These changes in ExtremeXOS 22.1 SNMP behavior do *not* affect switch upgrades. Switches that already have saved SNMP configurations continue to use their existing configurations.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Changed CLI Commands

Changes are underlined.

```
configure snmpv3 delete user [all | [[hex hex_user_name] | user_name]
{engine-id engine_id}]
```

```
configure snmpv3 delete community [all | {[[hex hex_community_index] |
community_index} | {name [[hex hex_community_name] | community_name}]
```

The following commands no longer have the **`default-user`** option:

```
enable snmpv3 default-group
```

```
disable snmpv3 default-group
```

P-BRIDGE MIB RFC4363

ExtremeXOS 22.1 implements the following groups of the P-BRIDGE MIB (RFC4363):

- dot1dDeviceCapabilities
- dot1dPortCapabilities table
- dot1dPortDefaultUserPriority

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Addition of dot1qVlanCurrentTable in Q-BRIDGE MIB (RFC4363)

The ExtremeXOS 22.1 now implements dot1qVlanCurrentTable in Q-BRIDGE MIB (RFC4363).

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Port Link-Flap Detection

This feature detects excessive link flapping (link going up and down rapidly) on a physical port and can take the following actions:

- Disables port—After the port is disabled due to excessive link flapping, the port either stays down for the configured disable time value or can be re-enabled manually.
- Reports issue to Syslog—Adds an entry in the log for a link down event.
- Generates SNMP trap—SNMP trap generated for a link down event.

You can configure the interval, threshold (maximum number of link down events), and disable time; and which of the preceding actions to take on a per port basis.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches

New CLI Commands

```
configure ports [port_list | all] link-flap-detection [on | off]
```

```
configure ports [port_list | all] link-flap-detection [{interval [interval
| indefinitely]} {threshold threshold} {disable-time [disable_time |
untilcleared]}]
```

```
unconfigure ports [port_list | all] link-flap-detection {interval}
{threshold} {disable-time}
```

```
configure ports [port_list | all] link-flap-detection action [add |
delete] [{{disable-port} {log} {trap}} | all-actions]
```

```
clear ports [port_list | all] link-flap-detection status
```

```
clear ports [port_list | all] link-flap-detection counters
```

```
show ports [port_list | all] link-flap-detection [disabled-ports |
configuration | counters {refresh | no-refresh}]
```

Changed CLI Commands

The following show commands are changed to provide link-flap detection information:

show ports {*port_list* | **tag** *tag*} {**no-refresh** | **refresh**}

show port {**mgmt** | *port_list* | **tag** *tag*} **information** {**detail**}

Open-Shortest Path (OSPFv3) Virtual Routing and Forwarding (VRF) and Management Information Base (MIB) Support

ExtremeXOS 22.1 supports multiple Virtual Routing and Forwarding (VRFs) in the same virtual router (VR). Each VRF can have a separate instance of a routing protocol with its own routing table. OSPFv3 can run in a VRF and support multiple instances of the protocol in different VRFs at the same time. This allows more scalable deployments of OSPFv3 as ExtremeXOS can have more VRFs than VRs, and OSPFv3 VRF instances belonging to the same VR run in a single ExtremeXOS process. Each VR still has its own process, so different VRs have very low impact on one another.

Additionally, all tables and variables of the OSPFv3-MIB (draft-ietf-ospf-ospfv3-mib-10) are now supported. and subset of the traps in RFC 5643.

Supported Platforms

For VRF: Summit X450-G2, X460-G2, X670-G2, X770 series switches.

For MIB: Summit X450-G2, X460-G2, X670-G2, X770 and ExtremeSwitching X440-G2, X620 series switches.

Limitations

- Only non-VPN VRFs are supported. OSPFv3 is blocked on VPN VRFs.
- BGP does not support VPN-IPv6 routes, so PE-CE support is not available.
- SNMP SET requests for OSPFv3 MIB objects are not supported.

New CLI Commands

enable snmp traps **ospfv3**

disable snmp traps **ospfv3**

Changed CLI Commands

The following show command now displays OSPFv3-related SNMP trap status (shown in bold):

show ospfv3

```
OSPFv3              : Enabled             RouterId            : 10.1.1.1
RouterId Selection  : Configured          ASBR                : No
ABR                 : No                  ExtLSAs             : 0
ExtLSAChecksum      : 0x0                 OriginateNewLSAs    : 3
ReceivedNewLSAs     : 0                   SpfHoldTime         : 10s
Num of Areas        : 1                   LSA Batch Interval  : 30s
10M Cost            : 100                 100M Cost           : 50
1000M Cost (1G)     : 40                  10000M Cost (10G)   : 20
40000M Cost (40G)   : 20                  100000M Cost (100G) : 10
Graceful Restart    : Both                Grace Period        : 120s
Restart Status      : None
Last Restart Exit Reason: None
Import Policy File  : none
SNMP Traps    : Disabled
```

```
Redistribute:
  Protocol               Status    Cost      Type  Tag    Policy
  direct                 Disabled  20        2     ---    none
  e-bgp                  Disabled  20        2     ---    none
  i-bgp                  Disabled  20        2     ---    none
  ripng                  Disabled  20        2     ---    none
  static                 Disabled  20        2     ---    none
  isis-level-1           Disabled  20        2     ---    none
  isis-level-2           Disabled  20        2     ---    none
  isis-level-1-external  Disabled  20        2     ---    none
  isis-level-2-external  Disabled  20        2     ---    none
```

Spanning Tree Protocol (STP) Bridge Priority Incrementing/Decrementing by One

This feature allows you to configure all STP modes (RSTP/MSTP) bridge priority in increments of 1 or 4,096. Allowing this level of granularity of the priority allows a large range of priority values for the backup root functionality. Once priority reaches 0, the backup root is unable to provide for rapid recovery in a lost root situation. In that case, priority returns to its initial configured (or default) value, and the process starts again. Loss of root should be a rare event, but this feature setting provides a buffer in situations where network downtime to reset the root is not often available.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

New CLI Commands

```
configure stpd stpd_name priority-mode [dot1d | dot1t]
```

Changed CLI Commands

The following commands are changed to accommodate changes from the STP Bridge Priority Incrementing/Decrementing by One Feature:

```
show stpd
```

```
configure stpd stpd_name priority priority
```

Disable Forwarding of Spanning Tree Protocol (STP) Bridge Protocol Data Units (BDPUs)

This feature allows you to disable forwarding of Spanning Tree Protocol (STP) Bridge Protocol Data Units (BPDUs) when STP is disabled on a switch.

When STP is disabled globally, BPDUs received on a port are forwarded to other ports that are part of same VLAN causing the switch to transparently forward STP/RSTP/MSTP BPDUs. This transparent forwarding causes one-to-many peer in the network trouble where STP is disabled. To avoid this transparent forwarding of BPDUs, this feature provides the ability to discard the BDPUs when there is no STP configuration enabled on the switch.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

New CLI Commands

```
configure stpd bpdu-forwarding [on | off]
```

Removal of Virtual Extensible LAN (VXLAN) Untagged Member Port Sharing Restriction

For Virtual Extensible LANs (VXLANs), the restriction that untagged member ports cannot share the same Ethernet port with other VLANs is removed.

Supported Platforms

Summit X770 and X670-G2 series switches, standalone, and in stacks that have these series switches slots only.

Increase in Equal-Cost Multi-path Routing (ECMP) Path from 16 to 64 for Open Shortest Path First (OSPFv2)

The maximum number of Equal-Cost Multi-path Routing (ECMP) paths is increased from 16 to 64 for Open Shortest Path First (OSPFv2). On new configurations, ECMP now defaults to 16 instead of 4.

This change appears in the Table 4 on page 31 table.

Supported Platforms

Summit X460-G2, X670-G2, and X770 series switches.

Multiple Registration Protocol (MVRP) over Multi-switch Link Aggregation (MLAG)

This feature adds support for Multiple Registration Protocol (MRP) on Multi-switch Link Aggregation (MLAG). The objective of running MVRP over MLAG is to propagate the VLANs across the MLAG peers and to have the VLAN database synced, so that the remote switches/servers continue to see a single logical connection.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Changed CLI Commands

The following command now has a flag showing if the MVRP-enabled port is an MLAG port:

```
show mvrp
```

Virtual Router Redundancy Protocol (VRRP) VRID Scaling Increase

This change increases the Virtual Router Redundancy Protocol (VRRP) maximum number of unique VRID numbers per VLAN and per switch from 31 to 256.

This change appears in the Table 4 on page 31 table.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Equal-cost Multi-path Routing (ECMP) Hashing Alternatives for IPv4/IPv6

A new set of hashing options are available to control traffic distribution of IPv4 or IPv6 packets among Equal-Cost Multi-path (ECMP) routes. You can dynamically choose between the existing ECMP hash method ("default") and the new "custom" hash method. Within each of these two hash methods, several hash algorithm options are available to vary traffic distribution among multiple equal-cost IP gateways.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770 series switches as standalone or in stacks.

New CLI Commands

configure iproute sharing **hash-method custom** {**hash-algorithm** [**xor** | **crc-16** | **crc-32** [**lower** | **upper**]]}

Changed CLI Commands

Changes are underlined.

configure iproute sharing {**hash-method** **default**} **hash-algorithm crc** [**lower** | **upper**]

The following show commands now display the current hash algorithm:

```
#show ipconfig ipv4
Use Redirects : Disabled
...
  Route Sharing Hash : CRC Lower, Default Method
- or -
  Route Sharing Hash : XOR, Custom Method
#show ipconfig ipv6
Route Sharing                : Disabled
...
    Route Sharing Hash          : CRC Lower, Default Method
- or -
    Route Sharing Hash          : XOR, Custom Method
```

Virtual Extensible LAN (VXLAN) VXLAN Virtual Network Identifier (VNI) Access Control List (ACL) Match Criteria

Starting with ExtremeXOS 22.1, user ACLs can additionally match the Virtual Extensible LAN (VXLAN) Virtual Network Identifier (VNI) on an egress-terminated VXLAN packet (egress VTEP scenario), or on a transit switch. The VNI match criteria is available for both static and dynamic ingress Access Control Lists (ACLs).

The following match criteria syntax can be added to the "if" clause of a policy rule:

vxlan-vni *vni number*

The following policy example matches VNI 100 and increments a counter:

```
entry countvni100 {
 if {
      vxlan-vni 100;
 } then {
      count vni100;
}}
```

Supported Platforms

Summit X770 and X670-G2 series switches (standalone), and stacks that have X770 and X670-G2 slots only.

Secure Connection from EMS to Syslog

This feature supports secure connections from EMS to remote Syslog servers using the OpenSSL library of APIs. The configuration of an EMS Syslog server target is enhanced to enable management of information necessary for establishing a trusted channel using TLS and providing for X509v3 authentication. Additionally, new EMS events are created as necessary for logging secure connection failure conditions and configuration changes.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Changed CLI Commands

Changes are underlined.

```
configure syslog [{add} [ipaddress {udp-port {udp_port}} | ipPort | ipaddress tls-port {tls_port}] {vr vr_name} [local] | delete [ [ipaddress {udp-port {udp_port}} | ipPort | ipaddress tls-port {tls_port} ] {vr vr_name} [local] | all {local} {vr vr_name}]]
```

```
enable log 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 [[all | ipaddress {udp-port {udp_port}} | ipPort | ipaddress tls-port {tls_port}] {vr vr_name} {local}]]
```

```
disable log 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 [[all | ipaddress {udp-port {udp_port}} | ipPort | ipaddress tls-port {tls_port} ] {vr vr_name} {local}]]
```

```
configure log target [upm [all | upm_profile_name] | xml-notification [all | xml_target_name] | console | session | memory-buffer | primary-msm | primary-mm | primary-node | backup-msm | backup-mm | backup-node | nvram | syslog [all | ipaddress {udp-port {udp_port}} | ipPort | ipaddress tls-port {tls_port} ] {vr vr_name} {local}] [filter filter-name {severity severity {only}} |severity severity {only}]
```

```
unconfigure log target [console | session | memory-buffer | nvram | syslog
[all | ipaddress {udp-port {udp_port}} | ipPort | ipaddress tls-port
{tls_port} ] {vr vr_name} {local} | xml-notification {xml_target_name}]
format
```

```
configure log target [upm [all | upm_profile_name] | xml-notification [all
| xml_target_name] | console | session | memory-buffer | primary-msm |
primary-mm | primary-node | backup-msm | backup-mm | backup-node | nvram |
syslog [all | ipaddress {udp-port {udp_port}} | ipPort | ipaddress tls-
port {tls_port} ] {vr vr_name} {local}] match {any | regex}
```

```
configure log target syslog [all | ipaddress {udp-port {udp_port}} |
ipPort | ipaddress tls-port {tls_port} ] {vr vr_name} {local} from
source-ip-address
```

```
configure log target syslog [all | ipaddress {udp-port {udp_port}} |
ipPort | ipaddress tls-port{tls_port} ] {vr vr_name} {local} format
[timestamp [ seconds | hundredths | none]] [date [ dd-Mmm-yyyy | yyyy-mm-dd
| Mmm-dd | mm-dd-yyyy | mm/dd/yyyy | dd-mm-yyyy | none]] {event-name
[component | condition | none]} {process-slot} {severity} {priority}
{source-function} {source-line} {host-name} {tag-id} {tag-name}
```

The following show command now displays the port type (TLS or UPD) (shown in bold):

```
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 {udp-port {udp_port}} | ipPort | ipaddress tls-port
{tls_port} } {vr vr_name} {local} } | filter {filter-name}}
```

```
# show log configuration target syslog
Log Target      : syslog; 10.68.6.3:6555 (vr VR-Mgmt), local0
    Enabled     : yes
    Filter Name : DefaultFilter
    Match regex : Any
    Severity    : Debug-Data (through Critical)
    Format      : PRI Mmm DD HH:MM:SS HOSTNAME TAG:
    Port Type   : TLS
    Recnct Cnt  : 0
    Recnct Msg  : No Error
```

Reconciliation of Events with Syslog Servers

The Syslog server targets now each maintain a queue of formatted messages that have not been sent to the server. Syslog server targets connecting to servers using TCP (including a secure) connections are driven with a dispatcher callback, which when the connection is writeable, dequeues the next message to be sent and writes it to the open socket.

The EMS server attempts to established connection when secure Syslog target is enabled. If enable command is issued from CLI, target is enabled only if connection is successful. If enable command is issued from loading a configuration, target is enabled regardless of connection result. If connection the is not successful, reconnection is attempted every 5 minutes until connection is successfully established.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Changed CLI Commands

The following show command now displays reconnection attempts and messages (shown in bold):

```
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 {udp-port udp_port} | ipPort | ipaddress tls-port
tls_port } {vr vr_name} {local}} | filter {filter-name}}
```

```
# show log configuration target syslog
Log Target      : syslog; 10.68.6.3:6555 (vr VR-Mgmt), local0
    Enabled     : yes
    Filter Name : DefaultFilter
    Match regex : Any
    Severity    : Debug-Data (through Critical)
    Format      : PRI Mmm DD HH:MM:SS HOSTNAME TAG:
    Port Type   : TLS
    Recnct Cnt  : 2
    Recnct Msg  : CA Certificate not found. Use 'Download ssl certificate trusted-ca'
command to download a CA certificate.
```

Modification of User Account Roles

Previously, ExtremeXOS only supported two roles for login sessions:

- administrative (or “admin” privilege having ‘write’ permission)
- non-administrative (or “user” privilege having ‘read-only’ permission).

You can now change a local user account's privileges to be administrative or not. If an account is changed, any sessions that are currently logged in with that account are cleared, and therefore forced to log in again with the new privilege.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

New CLI Commands

```
configure account [all | name ] privilege [admin |user]
```

Secure Authentication of Syslog Server and SSH Client Using X.509 Certificate

This feature in ExtremeXOS supports the secure authentication of Syslog server and SSH client to an ExtremeXOS device using an X.509 certificate. The following are the primary aspects to a Public-Key Infrastructure (PKI) configuration:

- Trusted CA—The X509v3 certificates of Certificate Authority (CA).
- Peer Certificate—The X509v3 certificate of the peer, signed by one of the above trusted CAs.

- OCSP—Online Certificate Status Protocol used to find the revocation status of the peer certificate.
- OCSP Signature CA—To support Trusted Responder Model (TRM) of OCSP, the X509v3 certificate of the OCSP Responder is required. The OCSP signature CA is only required for TRM; it is not used for DTM and common issuer.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Limitations

- All certificates should be in PEM format files.
- Downloading CA certificate chain is not supported.
- Individual CA certificates in a certificate chain should be downloaded one-by-one using the following command: `download ssl ipaddress certificate {ssl-cert | trusted-ca | ocsp-signature-ca} cert_file`
- Downloading CA certificate of size greater than 7.5KB is not recommended.
- Certification Revocation Lists (CRLs)—not supported.
- OCSP stapling—not supported.
- Nonce is always disabled in OCSP request.
- OCSP is not done for the OCSP responder certificate. Therefore, the OCSP responder certificate should satisfy any of following criteria, failing which the OCSP response is rejected:
  - OCSP responder certificate should be self-signed (OR).
  - OCSP responder certificate should contain `id-pkix-ocsp-nocheck` extension.

New CLI Commands

```
unconfigure ssl certificate [trusted-ca | ocsp-signature-ca] [file_name |
all]
```

Changed CLI Commands

Changes are underlined.

```
download ssl ipaddress certificate {ssl-cert | trusted-ca | ocsp-signature-
ca} cert_file
```

```
show ssl {[trusted-ca | ocsp-signature-ca] [file_name | all]}
{manufacturing} {certificate | detail}
```

Secure Shell (SSH) Public Key Infrastructure (PKI) with X509v3 Certificate-Based Authentication

This feature adds Secure Shell (SSH) Public Key Infrastructure (PKI) with X509v3 Certificate-Based Authentication to ExtremeXOS.

Previously, the ExtremeXOS SSH server supported the following two types of authentication methods to authenticate the SSH clients:

- Password-based authentication—Simple mapping of configured user and password.
- User key-based authentication—User generates the key pair (public and private keys). The public key is copied to the switch and associated to a particular user name. When the user tries to login to the

switch with their private key, the ExtremeXOS SSH server verifies the key and its association to the user. If this succeeds, the login is allowed. If key-based authentication fails, it fails back to password-based authentication.

The major disadvantage with user key-based authentication is scalability. As number of users increase, more keys are copied and stored on the switch. This problem can be solved with the PKI. Additionally, PKI provides added security, certificate revocation checking, avoiding manual mapping of key with user, etc.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Limitations

- Certificate-based authentication is supported only for ExtremeXOS SSH server, not for ExtremeXOS SSH client.
- Revocation check is done only for the SSH client-end certificate using Online Certificate Status Protocol (OCSP) only at the time of login. No periodic revocation checks occur.
- The SSH client certificate must have client authentication purpose in the extendedKeyUsage field.
- Username must be present in CommonName (CN) in the subject of the certificate. The login username and this CN must match for access to be granted.
- Support only for RSA, DSA-based SSH client certificates.

Random Number Entropy

This feature has dev/random seed OpenSSL's Deterministic Random Bit Generation (DRBG) for improved cryptography. Truly random number generation is essential for producing secure keys for encrypting and decrypting messages.

In ExtremeXOS, cryptographic functions are implemented using the OpenSSL library. The OpenSSL library uses a DRBG to generate random numbers. This DRBG is seeded with random numbers from the /dev/urandom device in the default configuration. However, in devices with few entropy sources, it is possible for the /dev/urandom device to provide the same seeds to OpenSSL instances running on different devices, resulting in two or more devices generating the same keys or sometimes different RSA keys having a common factor. It is also possible that after a reboot, the /dev/urandom device may provide the same seed that it provided on the last boot to OpenSSL instances running on the switch. This feature solves this problem by modifying OpenSSL such that it seeds its DRBG with random bits from the /dev/random device, instead of the /dev/urandom device.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Critical Security Parameter (CSP) Zeroization and Read-Verify

Critical Security Parameter (CSP) comprises information that is either user- or system-defined and is used to operate a cryptography module in processing encryption functions including cryptographic keys and authentication data, such as passwords (the disclosure or modification of which can compromise the security of a cryptographic module or the security of the information protected by the module).

CSP zeroization applies to flash memory, SSH private keys, and SSH session keys (present in volatile memory) stored in a switch.

Zeroization of Flash

Flash memory mounted in `/config` and `/scratch` directories are zeroized currently after using the command **`unconfigure switch erase all`**. As part of this feature, read-verify is done before rebooting switch to bootrom.

Zeroization of SSH Keys

SSH private keys are first stored temporarily in `/etc/` directory for converting it into correct format, and allowing Openssh to parse key file. After this is completed, and private key is loaded in key data structure (key file in `/etc` directory is zeroized). The key file is compared with `/dev/zero` to verify zeroization. After this is done, the key file is removed. An EMS appears if read-verify fails. Final keys are saved in EEPROM when you execute **`save configuration`**. This is zeroized and deleted by running same the command **`unconfigure switch erase all`**. Zeroization is verified by reading wkninfo object stored in EEPROM for SSH key, which should not have any data. Zeroization of SSH keys saved in EEPROM can also be accplished using the commands **`unconfigure switch all`** or **`unconfigure switch`**.

Zeroization of Session Keys in RAM

Zeroization of SSH session keys (stored in RAM) was already being accomplished in earlier versions of ExtremeXOS. This feature makes no changes to this.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

Disable Ciphers/Message Authentication Code (MACs) in Secure Shell (SSH) (Secure Mode)

Secure Shell (SSH) mode can operate in two modes: default, which supports all ciphers/Message Authentication Code (MACs) and secure mode, which supports only highly secure ciphers/MACs. This feature provides the ability to configure the required ciphers/MACs, and disable the ciphers/MACs that are not required.

Openssh-6.5p1 supports Diffie-Hellman group 1 and Diffie-Hellman group 14 as part of the key exchange algorithms. By default, both Diffie-Hellman group 1 and Diffie-Hellman group14 are supported. You can configure the minimal supported Diffie-Hellman group as 14 to avoid using the weaker Diffie-Hellman group 1 on the SSH server.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

New CLI Commands

```
configure ssh2 enable [cipher [cipher |all] | mac [mac |all]]
configure ssh2 disable [cipher [cipher |all] | mac [mac |all]]
```

```
show ssh2
```

```
show ssh2 {ciphers | macs}
```

```
configure ssh2 dh-group minimum [1 | 14]
```

Changed CLI Commands

The following show command is changed to show the secure mode status and the minimal supported Diffie-Hellman group (shown in bold):

```
show ssh2
```

```
 show ssh2
SSH module configuration details:
SSH Access            : Disabled
Key validity          : Invalid
TCP port              : 22
VR                    : all
Access profile        : not set
Secure Mode           : Off
Diffie-Hellman Groups : 1 (1024 bits prime), 14 (2048 bits prime)
Idle time             : 60 minutes
Ciphers               : Not configured
Macs                  : hmac-md5-etm@openssh.com, hmac-sha1-etm@openssh.com,
                        hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com,
                        hmac-ripemd160-etm@openssh.com, hmac-sha1-96-etm@openssh.com,
                        hmac-md5-96-etm@openssh.com, hmac-md5, hmac-sha1,
                        hmac-sha2-256, hmac-sha2-512, hmac-ripemd160,
                        hmac-ripemd160@openssh.com, hmac-sha1-96, hmac-md5-96
```

RSA Keys Supported

ExtremeXOS now supports RSA keys.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

VXLAN NSX Controller Support

This feature introduces support for VMware's NSX® for Multi-Hypervisor™ controllers using OVSDB hardware_vtep schema.

As part of the Software Defined Networking (SDN), the networking industry has defined abstracted models for various network functions and control. The OVSDB Hardware VTEP Schema is a standards-based approach that allows a Network Virtualization Controller such as VMware NSX to configure a hardware switch that implements VXLAN termination (VTEP). ExtremeXOS supports version 1.3 of the schema.

The NSX controller provides gateways with information about:

- Other remote VXLAN tunnel endpoints that instantiate a virtual network. This includes information about the VXLAN Network Identifier (VNI) and the tunnel endpoint IP addresses.

- MAC addresses of remote virtual machines (VMs) and the tunnel to which each MAC address is bound.
- The virtual network to tenant interface mapping. The controller instructs the gateway on how to map a port or a <port, 802.1Q> tag pair to a VNI.

Supported Platforms

Summit X770 and X670-G2 standalone, and stacks that have Summit X770 and X670-G2 slots only.

Limitations

The following OVSDB capabilities are not supported in ExtremeXOS:

- IPv6 addresses for OVSDB manager.
- IPv6 addresses in Hardware VTEP Schema.
- Support for stacks wherein at least one node is not VXLAN capable.
- MLAG for VTEP redundancy.
- Except for show commands, OVSDB and ExtremeXOS commands should not be used simultaneously to manage VXLAN.

New CLI Commands

```
configure ovsdb schema hardware_vtep [add | delete] connection client [tcp
| ssl] ipaddress remote_ip {port remote_port}

configure ovsdb schema hardware_vtep [add | delete] connection server [tcp
| ssl] {ipaddress local_ip} port local_port

configure ovsdb schema hardware_vtep delete connection all

configure ovsdb schema hardware_vteplogical_binding_stats update-interval
{[none |interval]}

disable ovsdb

disable ovsdb schema hardware_vtep {control-layer-only}

enable ovsdb

enable ovsdb schema hardware_vtep

show ovsdb

show ovsdb schema hardware_vtep

show ovsdb schema hardware_vtep tablename {detail}

unconfigure ovsdb

unconfigure ovsdb schema
```

Resiliency Enhancement for IPv4 and IPV6 Static Routes

The ExtremeXOS Resiliency Enhancement feature provides a resilient way to use Equal-Cost Multi-Path (ECMP) to load balance IPv4 traffic among multiple servers or other specialized devices. ExtremeXOS automatically manages the set of active devices using ECMP static routes configured with ping protection to monitor the health of these routes. Such servers or specialized devices do not require special software to support Bidirectional Forwarding Detection (BFD), or IP routing protocols such as OSPF, or proprietary protocols to provide keepalive messages. ExtremeXOS uses industry-standard and required protocols ICMP/ARP for IPv4 to accomplish the following automatically:

- Initially verify devices and activate their static routes, without waiting for inbound user traffic, and without requiring configuration of device MAC addresses.
- Detect silent device outages and inactivate corresponding static routes.
- Reactivate static routes after device recovery, or hardware replacement with a new MAC address.

ExtremeXOS previously supported similar protection and resiliency using BFD on IPv4 static routes. However, BFD can only be used when the local and remote device both support BFD.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches.

New CLI Commands

```
configure iproute add [default | ipv4_or_ipv6_network] gateway
{protection [bfd | ping |none]}
```

```
configure iproute {ipv4 | ipv6} protection ping interval seconds miss
misses
```

```
enable iproute {ipv4 | ipv6} protection ping
```

```
disable iproute {ipv4 | ipv6} protection ping
```

```
show iproute {ipv4 | ipv6} protection ping {v4_or_v6_gateway} {vr vr_name}
{detail}
```

Changed CLI Commands

The following are revised commands for the ExtremeXOS Resiliency Enhancement for IPv4 and IPv6 Static Routes feature:

- The configuration settings for static route ping protection enable/disable, interval, and misses for IPv4 appear in the `show ipconfig` command, and for IPv6 in the `show ipconfig ipv6` command.
- A new route flag letter "I" appears in the `show iproute` and `show iproute ipv6` commands to indicate static routes with ICMP ping protection. Flag letter "I" uses the same column as flag letter "b" because BFD and ping protection are mutually exclusive. If the route flags also show "U" for Up, then ping protection detected the gateway is up.

Ability to Add Tenant VMANs to Virtual Extensible LANs (VXLANs)

ExtremeXOS 21.1 had the ability to add and delete tenant VLANs to Virtual Extensible LANs (VXLANs). This feature adds the ability to add/delete tenant VMANs to VXLANs.

Supported Platforms

Summit X770 and X670-G2 series switches (standalone), and stacks that have X770 and X670-G2 slots only.

Limitations

- Multi-switch Link Aggregation (MLAG) does not function if the Inter-Switch Connection (ISC) port is added to an untagged tenant VMAN.
- Non-Tenant VLANs/VMANs do not function if the port also has an untagged tenant VMAN.

Changed CLI Commands

Changes are underlined.

```
configure virtual-network vn_name [add | delete] [{vlan} vlan_name | vman
vman_name]
```

```
show virtual-network { vn_name | vxlan vni vni | [vlan vlan_name | vman
vman_name]}
```

Kerberos Authentication Type Support

Kerberos authentication support in ONEPolicy is achieved using NAC with IDM XML events.

With NetLogin, ONEPolicy, and IDM enabled, once the MAC address is authenticated and IDM table is populated with the MAC user and with Kerberos correlated user, using XML target configured in ExtremeXOS, the IDMGR events are be sent to Extreme Management Center server using HTTP/HTTPS. Extreme Management Center after receiving the XML event decides what to do with the profiles configured for Kerberos.

Supported Platforms

Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 series switches

Summit X460-G2 Series Switches Have Advanced Edge License

Summit X460-G2 series switches now have the Advanced Edge License as their default base license level.

For more information about licenses, see *ExtremeXOS 22.1 Feature License Requirements*.

VLAN Option Formatting in Commands

For commands with a **`vlan_list`** option, the input into this option must not contain spaces.

Example

The `enable stpd auto-bind` command VLAN ID input should be entered as:

```
enable stpd auto-bind vlan 10,20-30
```

Not:

```
enable stpd auto-bind vlan 10, 20-30
```

Circuit Emulation Service (CES) No Longer Supported

Starting with ExtremeXOS 21.1, Circuit emulation service (CES) is no longer supported.

OpenFlow and SSH Included in ExtremeXOS Base Image

OpenFlow and SSH are now included in the ExtremeXOS base image starting with ExtremeXOS 21.1. A separate XMOD file is no longer required.

ExtremeXOS SSH Server Upgraded with OpenSSH v6.5

ExtremeXOS 16.1 and earlier versions generated DSA-2048 keys using `ssh keygen` provided by the SSH-Toolkit library. Starting with ExtremeXOS 21.1, ExtremeXOS generates more secure RSA-2048 keys due to switching to using the OpenSSH library, which does not support DSA-2048.

When upgrading to ExtremeXOS 21.1 and later, SSH keys generated by earlier ExtremeXOS versions (16.1 and earlier) are compatible and do *not* need to be re-generated.

Note

If a switch is downgraded from ExtremeXOS 21.1 or later to previous releases, with RSA key saved, the key becomes invalid.

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”

Extreme Hardware/Software Compatibility and Recommendation Matrices

The *Extreme Hardware/Software Compatibility and Recommendation Matrices* provide information about the minimum version of ExtremeXOS software required to support switches, as well as SFPs, XENPAKs, XFPs, and other pluggable interfaces.

This guide also provides information about which optics are supported on which hardware platforms, and the minimum software version required.

The latest version of this and other ExtremeXOS guides are at: http://documentation.extremenetworks.com

Compatibility with Extreme Management Center (Formerly NetSight)

ExtremeXOS 22.1 is compatible with Extreme Management Center (formerly NetSight) version 7.0 and later.

Upgrading ExtremeXOS

For instructions about upgrading ExtremeXOS software, see "Software Upgrade and Boot Options" in the *ExtremeXOS 22.1 User Guide*.

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.` appears. An ExtremeXOS modular software package (.xmod file) can still be downloaded and installed on either the active or alternate partition.

Supported MIBs

The Extreme Networks MIBs are located on the eSupport website under Download Software Updates, located at: https://esupport.extremenetworks.com.

You need to provide your serial number or agreement number, and then the MIBs are available under each release.

For detailed information on which MIBs and SNMP traps are supported, see the *Extreme Networks Proprietary MIBs* and *MIB Support Details* sections in the *ExtremeXOS 22.1 User Guide*.

Tested Third-Party Products

This section lists the third-party products tested for ExtremeXOS 22.1.

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

2 Limits

This chapter summarizes the supported limits in ExtremeXOS 22.1.

Table 4 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.

The scaling and performance information shown in Table 4 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 4 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.

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 4: 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.	ExtremeSwitching X620, X440-G2	1,024 ingress, 256 egress
	Summit X770, X670-G2, X450-G2, X460-G2	1,024 ingress, 512 egress
Access lists (policies)—suggested maximum number of lines in a single policy file.	All platforms	300,000
Access lists (policies)—maximum number of rules in a single policy file.[a]	Summit X460-G2, X450-G2, X770, X670-G2	4,096 ingress, 1,024 egress
	ExtremeSwitching X620, X440-G2	2,048 ingress, 512 egress

Table 4: 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 Summit X670-G2, X770 ExtremeSwitching X620, X440-G2	2,048 ingress only 1,024 ingress only 512 ingress only
Access lists (slices)—number of ACL slices.	Summit X460-G2, X450-G2	16 ingress, 4 egress
	Summit X770, X670-G2	12 ingress, 4 egress
	ExtremeSwitching X440-G2, X620	8 ingress, 4 egress
Access lists (slices)—number of ACL slices in first stage (VFP).	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	4 ingress only
ACL Per Port Meters—number of meters supported per port.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	16
Meters Packets-Per-Second Capable	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	Yes
AVB (audio video bridging)—maximum number of active streams.	Summit X450-G2, X460-G2, X770, and ExtremeSwitching X620, X440-G2 Summit X670-G2	1,024 4,096
BFD sessions (Software Mode)—maximum number of BFD sessions.	Summit X460-G2, X670-G2, X450-G2, X770 (default timers—1 sec) Summit X460-G2, X670-G2, X450-G2, X770 (minimal timers—100 msec)	512 10 [c]
BFD sessions (Hardware Assisted)—maximum number of BFD sessions.	Summit X460-G2	900 (PTP not enabled) 425 (PTP enabled) 256 (with 3 ms transmit interval)
BGP (aggregates)—maximum number of BGP aggregates.	Summit X460-G2, X670-G2, X770 with Core license Summit X450-G2, and ExtremeSwitching X440-G2, X620	256 Not supported
BGP (networks)—maximum number of BGP networks.	Summit X460-G2, X670-G2, X770 with Core license Summit X450-G2, and ExtremeSwitching X440-G2, X620	1,024 Not supported
BGP (peers)—maximum number of BGP peers. Note: *With default keepalive and hold timers.	Summit X460-G2, X670-G2, X770 with Core license Summit X450-G2, and ExtremeSwitching X440-G2, X620	128* Not supported
BGP (peer groups)—maximum number of BGP peer groups.	Summit X460-G2, X670-G2, X770 with Core license Summit X450-G2, and ExtremeSwitching X440-G2, X620	64 Not supported
BGP (policy entries)—maximum number of BGP policy entries per route policy.	Summit X460-G2, X670-G2, X770 with Core license Summit X450-G2, and ExtremeSwitching X440-G2, X620	256 Not supported

Table 4: Supported Limits (continued)

Metric	Product	Limit
BGP (policy statements)—maximum number of BGP policy statements per route policy.	Summit X460-G2, X670-G2, X770 with Core license Summit X450-G2, and ExtremeSwitching X440-G2, X620	1,024 Not supported
BGP multicast address-family routes—maximum number of multicast address-family routes.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	25,000 Not supported
BGP (unicast address-family routes)—maximum number of unicast address-family routes.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	25,000 Not supported
BGP (non-unique routes)—maximum number of non-unique BGP routes.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	25,000 Not supported
BGP ECMP—maximum number of equalcost multipath for BGP and BGPv6.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	2, 4, 8, 16, 32, or 64 Not supported
BGPv6 (unicast address-family routes)—maximum number of unicast address family routes.	Summit X460-G2 Summit X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	6,000 8,000 Not supported
BGPv6 (non-unique routes)—maximum number of non-unique BGP routes.	Summit X460-G2 Summit X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	18,000 24,000 Not supported
BOOTP/DHCP relay—maximum number of BOOTP or DHCP servers per virtual router.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2*, X620*	4
BOOTP/DHCP relay—maximum number of BOOTP or DHCP servers per VLAN.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2, X620	4
Connectivity fault management (CFM)—maximum number or CFM domains. Note: With Advanced Edge license or higher.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2, X620	8
CFM—maximum number of CFM associations. Note: With Advanced Edge license or higher.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2, X620	256

Table 4: Supported Limits (continued)

Metric	Product	Limit
CFM—maximum number of CFM up end points. Note: With Advanced Edge license or higher.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2, X620	32
CFM—maximum number of CFM down end points. Note: With Advanced Edge license or higher.	Summit X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2, X620 Summit X460-G2	32 256 (non-load shared ports) 32 (load shared ports)
CFM—maximum number of CFM remote end points per up/down end point. Note: With Advanced Edge license or higher.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2, X620	2,000
CFM—maximum number of dot1ag ports. Note: With Advanced Edge license or higher.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2, X620	128
CFM—maximum number of CFM segments. Note: With Advanced Edge license or higher.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2, X620	1,000
CFM—maximum number of MIPs. Note: With Advanced Edge license or higher.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X620, X440-G2	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.	Summit X460-G2, X770, X670-G2, X450-G2 ExtremeSwitching X440-G2, X620	4,094 1,024
Data Center Bridging eXchange (DCBX) protocol Type Length Value (TLVs)—maximum number of DCBX application TLVs.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X440-G2, X620	8

Table 4: Supported Limits (continued)

Metric	Product	Limit
DHCPv6 Prefix Delegation Snooping—Maximum number of DHCPv6 prefix delegation snooped entries.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X620, X440-G2	256 (with Underlying Protocol Ripng) 128 (with Underlying protocol OSPFv3) 1,024 (with static routes)
DHCP snooping entries—maximum number of DHCP snooping entries.	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X620, X440-G2	2,048
Dynamic ACLs—maximum number of ACLs processed per second. Note: Limits are load dependent.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 with 50 DACLs with 500 DACLs	10 5
EAPS domains—maximum number of EAPS domains. Note: An EAPS ring that is being spatially reused cannot have more than four configured EAPS domains.	Summit X670-G2, X450-G2, X460-G2, and X770 ExtremeSwitching X440-G2, X620	64 32
EAPSv1 protected VLANs—maximum number of protected VLANs.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	1,000
EAPSv2 protected VLANs—maximum number of protected VLANs.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620 ExtremeSwitching X440-G2	500 Not supported
ELSM (vlan-ports)—maximum number of VLAN ports.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620	5,000
ERPS domains—maximum number of ERPS domains without CFM configured.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	32
ERPS domains—maximum number of ERPS domains with CFM configured.	Summit X450-G2, X670-G2, X770, and ExtremeSwitching X620 Summit X460-G2	16 32
ERPSv1 protected VLANs—maximum number of protected VLANs.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	1,000
ERPSv2 protected VLANs—maximum number of protected VLANs.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	500
ESRP groups—maximum number of ESRP groups.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X440-G2, X620	31

Table 4: Supported Limits (continued)

Metric	Product	Limit
ESRP domains—maximum number of ESRP domains.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	64
ESRP VLANs—maximum number of ESRP VLANs.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	1,000
ESRP (maximum ping tracks) —maximum number of ping tracks per VLAN.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8
ESRP (IP route tracks)— maximum IP route tracks per VLAN.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8
ESRP (VLAN tracks)— maximum number of VLAN tracks per VLAN.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	1
Forwarding rate—maximum L3 software forwarding rate.	Summit X770 Summit X670-G2 Summit X460-G2 Summit X450-G2 ExtremeSwitching X440-G2 ExtremeSwitching X620	11,000 pps 21,000 pps 25,000 pps 24,000 pps 21,000 pps 23,000 pps
FDB (unicast blackhole entries)—maximum number of unicast blackhole FDB entries.	Summit X460-G2 Summit X770, X670-G2 Summit X450-G2 ExtremeSwitching X620, X440-G2	49,152[f] 294,912[f] 34,816[f] 16,384[f]
FDB (multicast blackhole entries)—maximum number of multicast blackhole FDB entries.	Summit X460-G2, X450-G2, and ExtremeSwitching X440-G2, X620 Summit X770, X670-G2	1,024 4,096
FDB (maximum L2 entries)— maximum number of MAC addresses.	Summit X460-G2 Summit X770, X670-G2 Summit X450-G2 ExtremeSwitching X620, X440-G2	98,300[f] 294,912[f] 68,000[f] 16,384[f]
FDB (Maximum L2 entries)— maximum number of multicast FDB entries.	Summit X770, X670-G2 Summit X450-G2, X460-G2, and ExtremeSwitching X620, X440-G2	4,096 1,024
Identity management— maximum number of Blacklist entries.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	512
Identity management— maximum number of Whitelist entries.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	512
Identity management— maximum number of roles that can be created.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	64
Identity management— maximum role hierarchy depth allowed.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	5

Table 4: Supported Limits (continued)

Metric	Product	Limit
Identity management—maximum number of attribute value pairs in a role match criteria.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	16
Identity management—maximum of child roles for a role.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8
Identity management—maximum number of policies/dynamic ACLs that can be configured per role.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8
Identity management—maximum number of LDAP servers that can be configured.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8
Identity management—maximum number of Kerberos servers that can be configured.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	20
Identity management—maximum database memory-size.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	512
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.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	100
Identity management—recommended number of ACL entries per identity. Note: Number of ACLs per identity based on system ACL limitation.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	20
Identity management—maximum number of dynamic ACL entries configured as an individual dynamic rule, or as an ACL entry in a policy file.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	500
IGMP snooping per VLAN filters—maximum number of VLANs supported in per-VLAN IGMP snooping mode.	Summit X460-G2 Summit X450-G2 Summit X770, X670-G2 ExtremeSwitching X620, X440-G2	1,500 2,048 2,000 1,000

Table 4: Supported Limits (continued)

Metric	Product	Limit
IGMPv1/v2 SSM-map entries—maximum number of IGMPv1/v2 SSM mapping entries.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	500
IGMPv1/v2 SSM-map entries—maximum number of sources per group in IGMPv1/v2 SSM mapping entries.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	50
IGMPv2 subscriber—maximum number of IGMPv2 subscribers per port.[n]	Summit X770, X670-G2, X460-G2, X450-G2 ExtremeSwitching X440-G2, X620	4,000 3,500
IGMPv2 subscriber—maximum number of IGMPv2 subscribers per switch.[n]	Summit X770, X670-G2 Summit X460-G2, X450-G2 ExtremeSwitching X620, X440-G2	30,000 20,000 17,500
IGMPv3 maximum source per group—maximum number of source addresses per group.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	250
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per port.[n]	Summit X770, X670-G2, X460-G2, X450-G2 ExtremeSwitching X440-G2, X620	4,000 3,500
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per switch.[n]	Summit X460-G2, X450-G2 Summit X770, X670-G2 ExtremeSwitching X620, X440-G2	20,000 30,000 17,500
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).	Summit X670-G2, X770 Summit X460-G2 Summit X450-G2 ExtremeSwitching X440-G2, X620	131,072 (up to)[h] 57,344 (up to)[h] 47,000 (up to)[h] 20,480
IPv4 ARP entries in hardware with minimum LPM routes—maximum recommended number of IPv4 ARP entries in hardware, with minimum LPM routes present. Assumes number of IP route reserved entries is 100 or less.	Summit X460-G2 Summit X770, X670-G2 Summit X450-G2 ExtremeSwitching X620 ExtremeSwitching X440-G2	50,000 (up to)[h] 108,000 (up to)[h] 39,000 (up to)[h] 1,500 1,000
IPv4 ARP entries in hardware with maximum LPM routes—maximum recommended number of IPv4 ARP entries in hardware, with maximum LPM routes present. Assumes number of IP route reserved entries is “maximum.”	Summit X460-G2 Summit X770, X670-G2 Summit X450-G2 ExtremeSwitching X620 ExtremeSwitching X440-G2	43,000 (up to)[h] 98,000 (up to)[h] 29,000 (up to)[h] 1,500 1,000

Table 4: Supported Limits (continued)

Metric	Product	Limit
IP flow information export (IPFIX)—number of simultaneous flows.	Summit X460-G2	2,048 ingress 2,048 egress
	Summit X450-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	N/A
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. Assumes number of IP route reserved entries is 0, and number of IPv4 ARP entries present is 100 or less.	Summit X460-G2 Summit X770, X670-G2 Summit X450-G2 ExtremeSwitching X440-G2, X620	73,000[h] 176,000 (up to)[h] 61,000 (up to)[h] 3,500
IPv4 routes—maximum number of IPv4 routes in software (combination of unicast and multicast routes).	Summit X670-G2, X460-G2, X450-G2, X440-G2, X620	25,000
IPv4 routes (LPM entries in hardware)— number of IPv4 routes in hardware.	Summit X460-G2 Summit X770, X670-G2, X450-G2 ExtremeSwitching X620, X440-G2	12,000 16,000 480
IPv6 6in4 tunnel—maximum number of IPv6 6in4 tunnels.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X440-G2, X620	255
IPv6 addresses on an interface—maximum number of IPv6 addresses on an interface.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	255
IPv6 addresses on a switch—maximum number of IPv6 addresses on a switch.	Summit X770, X670-G2, X460-G2, X450-G2 ExtremeSwitching X620, X440-G2	2,048 510
IPv6 host entries in hardware—maximum number of IPv6 neighbor entries in hardware.	Summit X770, X670-G2 Summit X460-G2 Summit X450-G2 ExtremeSwitching X440-G2 ExtremeSwitching X620	36,750[i] 22,000[i] 12,000[i] 1,000 1,500
IPv6 routes (LPM entries in hardware)—maximum number of IPv6 routes in hardware.	Summit X460-G2 Summit X670-G2, X770, X450-G2 ExtremeSwitching X620, X440-G2	6,000 8,000 240
IPv6 routes with a mask greater than 64 bits in hardware—maximum number of such IPv6 LPM routes in hardware.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	256

Table 4: Supported Limits (continued)

Metric	Product	Limit
IPv6 route sharing in hardware—route mask lengths for which ECMP is supported in hardware. Note: * >64 single path only	Summit X460-G2, X670-G2, X770, X450-G2, and ExtremeSwitching X620 ExtremeSwitching X440-G2	0–64 * Not supported
IPv6 routes in software—maximum number of IPv6 routes in software.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	25,000
IP router interfaces—maximum number of VLANs performing IPv4 and/or IPv6 routing. Excludes sub-VLANs.	Summit X460-G2, X770, X670-G2, X450-G2 ExtremeSwitching X620, X440-G2	2,048 510
IP multicast static routes—maximum number of permanent multicast IP routes.	Summit X460-G2, X670-G2, X450-G2, X770	1,024
IP unicast static routes—maximum number of permanent IP unicast routes.	Summit X460-G2, X670-G2, X450-G2, X770 ExtremeSwitching X620, X440-G2	1,024 480
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 64 ECMP gateways per destination. Routing protocols BGP is limited to 64 ECMP gateways per destination, while IS-IS is limited to 8. Static routes are limited to 64 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.	Summit X460-G2, X670-G2, X450-G2, X770, and ExtremeSwitching X620 ExtremeSwitching X440-G2	2, 4, 8, 16, 32, or 64 N/A

Table 4: Supported Limits (continued)

Metric	Product	Limit
IP route sharing (total destinations)—maximum number of unique destinations used by multipath OSPF, OSPFv3, BGP, IS-IS, or static routes.	Summit X670-G2, X770, X450-G2 Summit X460-G2 ExtremeSwitching X620 ExtremeSwitching X440-G2 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.	16,352 12,256 480 N/A
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.	Summit X670-G2, X770 default maximum gateways of 16 if maximum gateways is 2 if maximum gateways is 8 if maximum gateways is 16 if maximum gateways is 32 if maximum gateways is 64 Summit X460-G2, X450-G2 default maximum gateways of 4 if maximum gateways is 2 if maximum gateways is 8 if maximum gateways is 16 if maximum gateways is 32 if maximum gateways is 64 ExtremeSwitching X620 default maximum gateways of 4 if maximum gateways is 2 if maximum gateways is 8 if maximum gateways is 16 if maximum gateways is 32 if maximum gateways is 64 ExtremeSwitching X440-G2	1,022 1,022 1,022 1,022 510 254 1,022 1,022 510 254 126 62 126 126 126 126 62 30 N/A
IP multinetting (secondary IP addresses)—maximum number of secondary IP addresses per VLAN.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	255
IS-IS adjacencies—maximum number of supported IS-IS adjacencies.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X620, X440-G2	128 N/A

Table 4: Supported Limits (continued)

Metric	Product	Limit
IS-IS ECMP—maximum number of equal cost multipath for IS-IS.	Summit X450-G2, X670-G2, X770, X460-G2 ExtremeSwitching X620, X440-G2	2, 4, or 8 N/A
IS-IS interfaces—maximum number of interfaces that can support IS-IS.	Summit X450-G2, X670-G2, X770, X460-G2 ExtremeSwitching X620, X440-G2	255 N/A
IS-IS routers in an area—recommended maximum number of IS-IS routers in an area.	Summit X450-G2, X670-G2, X770, X460-G2 ExtremeSwitching X620, X440-G2	256 N/A
IS-IS route origination—recommended maximum number of routes that can be originated by an IS-IS node.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X620, X440-G2	20,000 N/A
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.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X620, X440-G2	25,000 N/A
IS-IS IPv4 L2 routes—recommended maximum number of IS-IS Level 2 routes.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X620, X440-G2	25,000 N/A
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.	Summit X450-G2, X460-G2, X670-G2. X770 ExtremeSwitching X620, X440-G2	20,000 N/A
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.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X620, X440-G2	10,000 N/A
IS-IS IPv6 L2 routes—recommended maximum number of IS-IS Level 2 routes.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X620, X440-G2	10,000 N/A
IS-IS IPv6 L1 routes in an L1/L2 router—recommended maximum number of IS-IS Level 1 routes in a L1/l2 router.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X620, X440-G2	10,000 N/A
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.	Summit X450-G2, X460-G2, X670-G2. X770 ExtremeSwitching X620, X440-G2	20,000 N/A

Table 4: Supported Limits (continued)

Metric	Product	Limit
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.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X620, X440-G2	20,000 N/A
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.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X620, X440-G2	20,000 N/A
Jumbo frames—maximum size supported for jumbo frames, including the CRC.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	9,216
L2 VPN: VCCV (pseudowire Virtual Circuit Connectivity Verification) VPNs per switch—maximum number of VCCV enabled VPLS VPNs.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X620, X440-G2	16 N/A
L2 VPN: VPLS MAC addresses —maximum number of MAC addresses learned by a switch.	Summit X770 Summit X670-G2 Summit X460-G2 Summit X450-G2, and ExtremeSwitching X620, X440-G2	128,000 140,000 55,000 N/A
L2 VPN: VPLS VPNs—maximum number of VPLS virtual private networks per switch.	Summit X460-G2, X770, X670-G2 Summit X450-G2, and ExtremeSwitching X620, X440-G2	1,023 N/A
L2 VPN: VPLS peers—maximum number of VPLS peers per VPLS instance.	Summit X770, X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X620, X440-G2	64 N/A
L2 VPN: LDP pseudowires—maximum number of pseudowires per switch.	Summit X770 Summit X670-G2 Summit X460-G2 Summit X450-G2, and ExtremeSwitching X620, X440-G2	7,800 7,000 7,116 N/A
L2 VPN: static pseudowires—maximum number of static pseudowires per switch.	Summit X770 Summit X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X620, X440-G2	15,308 7,000 N/A
L2 VPN: Virtual Private Wire Service (VPWS) VPNs—maximum number of virtual private networks per switch.	Summit X770 Summit X670-G2 Summit X460-G2 Summit X450-G2, and ExtremeSwitching X620, X440-G2	4,000 4,090 1,023 N/A

Table 4: Supported Limits (continued)

Metric	Product	Limit
Layer-2 IPMC forwarding caches—(IGMP/MLD/PIM snooping) in mac-vlan mode. Note: • The internal lookup table configuration used is "l2-and-l3". • IPv6 and IPv4 L2 IPMC scaling is the same for this mode. • Layer-2 IPMC forwarding cache limits—(IGMP/MLD/PIM snooping) in mixed-mode are same.	Summit X770, X670-G2 Summit X460-G2 Summit X450-G2 ExtremeSwitching X620, X440-G2	73,000 24,000 14,000 5,000
Layer-3 IPv4 Multicast—maximum number of <S,G,V> entries installed in the hardware (IP multicast compression enabled). Note: • Limit value same for MVR senders, PIM Snooping entries. PIM SSM cache, IGMP senders, PIM cache. • The internal lookup table configuration used is "more l3-and-ipmc". • Assumes source-group-vlan mode as look up key. • Layer 3 IPMC cache limit in mixed mode also has the same value.	Summit X460-G2 Summit X450-G2 Summit X770, X670-G2 ExtremeSwitching X620, X440-G2	26,000 21,000 77,500 1,500

Table 4: Supported Limits (continued)

Metric	Product	Limit
Layer-3 IPv6 Multicast—maximum number of <S,G,V> entries installed in the hardware (IP multicast compression enabled). Note: • Limit value same for MLD sender per switch,PIM IPv6 cache. • The internal lookup table configuration used is "more l3-and-ipmc”. • Assumes source-group-vlan mode as look up key.	Summit X770, X670-G2 Summit X460-G2 Summit X450-G2 ExtremeSwitching X620, X440-G2	30,000 14,000 10,000 700
Load sharing—maximum number of load sharing 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.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	128
Load sharing—maximum number of ports per load-sharing group.	ExtremeSwitching X620, X440-G2 (standalone and stacked)	8
	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) Summit X670-G2	64
Logged messages—maximum number of messages logged locally on the system.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	20,000
MAC-based security—maximum number of MAC-based security policies.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	1,024
MAC Locking—Maximum number of MAC locking stations that can be learned on a port.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	64 (static MAC locking stations) 600 (first arrival MAC locking stations)

Table 4: Supported Limits (continued)

Metric	Product	Limit
Meters—maximum number of meters supported.	Summit X460-G2, X450-G2, X670-G2, X770 ExtremeSwitching X440-G2, X620	2,048 N/A
Maximum mirroring instances	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 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	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.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	128
Mirroring, one-to-many (filters)—maximum number of one-to-many mirroring filters. Note: This is the number of filters across all the active mirroring instances	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	128
Mirroring, one-to-many (monitor port)—maximum number of one-to-many monitor ports.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	16
MLAG ports—maximum number of MLAG ports allowed.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	768
MLAG peers—maximum number of MLAG peers allowed.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	2
MPLS RSVP-TE interfaces—maximum number of interfaces.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	32 N/A

Table 4: Supported Limits (continued)

Metric	Product	Limit
MPLS RSVP-TE ingress LSPs—maximum number of ingress LSPs.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	2,000 N/A
MPLS RSVP-TE egress LSPs—maximum number of egress LSPs.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	2,000 N/A
MPLS RSVP-TE transit LSPs—maximum number of transit LSPs.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	2,000 N/A
MPLS RSVP-TE paths—maximum number of paths.	Summit X460-G2, X770 Summit X670-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	1,000 2,000 N/A
MPLS RSVP-TE profiles—maximum number of profiles.	Summit X460-G2, X770 Summit X670-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	1,000 2,000 N/A
MPLS RSVP-TE EROs—maximum number of EROs per path.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	64 N/A
MPLS LDP peers—maximum number of MPLS LDP peers per switch.	Summit X770 Summit X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	64 128 N/A
MPLS LDP adjacencies—maximum number of MPLS LDP adjacencies per switch.	Summit X460-G2 Summit X770, X670-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	50 64 N/A
MPLS LDP ingress LSPs—maximum number of MPLS LSPs that can originate from a switch.	Summit X770, X670-G2 Summit X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	2,048 4,000 N/A
MPLS LDP-enabled interfaces—maximum number of MPLS LDP configured interfaces per switch.	Summit X770 Summit X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	64 128 N/A
MPLS LDP Sessions—maximum number of MPLS LDP sessions.	Summit X770 Summit X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	64 128 N/A
MPLS LDP transit LSPs—maximum number of MPLS transit LSPs per switch.	Summit X770, X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	4,000 N/A
MPLS LDP egress LSPs—maximum number of MPLS egress LSPs that can terminate on a switch.	Summit X770 Summit X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	8,000 4,000 N/A
MPLS static egress LSPs—maximum number of static egress LSPs.	Summit X460-G2 Summit X770 Summit X670-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	7,116 8,000 15,308 N/A

Table 4: Supported Limits (continued)

Metric	Product	Limit
MPLS static ingress LSPs—maximum number of static ingress LSPs.	Summit X460-G2 Summit X770, X670-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	4,000 2,048 N/A
MPLS static transit LSPs—maximum number of static transit LSPs	Summit X770, X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	4,000 N/A
MSDP active peers—maximum number of active MSDP peers.	Summit X770, X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	64 N/A
MSDP SA cache entries—maximum number of entries in SA cache.	Summit X670-G2, X770 Summit X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	14,000 10,000 N/A
MSDP maximum mesh groups—maximum number of MSDP mesh groups.	Summit X770, X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	16 N/A
Multicast listener discovery (MLD) snooping per-VLAN filters—maximum number of VLANs supported in per-VLAN MLD snooping mode.	Summit X460-G2 Summit X770, X670-G2 Summit X450-G2 ExtremeSwitching X620, X440-G2	1,200 1,200 512 600
Multicast listener discovery (MLD)v1 subscribers—maximum number of MLDv1 subscribers per port.[n]	Summit X770, X670-G2, X450-G2, X460-G2 ExtremeSwitching X620, X440-G2	4,000 3,500
Multicast listener discovery (MLD)v1 subscribers—maximum number of MLDv1 subscribers per switch.[n]	Summit X460-G2, X450-G2 Summit X770, X670-G2 ExtremeSwitching X620, X440-G2	10,000 30,000 10,000
Multicast listener discovery (MLD)v2 subscribers—maximum number of MLDv2 subscribers per port.[n]	Summit X450-G2 SummitStack Summit X770, X670-G2, X460-G2 ExtremeSwitching X620, X440-G2	4,000 2,000 4,000 3,500
Multicast listener discovery (MLD)v2 subscribers—maximum number of MLDv2 subscribers per switch.[n]	SummitStack Summit X460-G2, X450-G2 Summit X770, X670-G2 ExtremeSwitching X620, X440-G2	5,000 10,000 30,000 10,000
Multicast listener discovery (MLD)v2 maximum source per group—maximum number of source addresses per group.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	200
Multicast listener discovery (MLD) SSM-map entries—maximum number of MLD SSM mapping entries.	Summit X450-G2, X460-G2, X670-G2, X770 ExtremeSwitching X440-G2, X620	500 50

Table 4: Supported Limits (continued)

Metric	Product	Limit
Multicast listener discovery (MLD) SSM-MAP entries—maximum number of sources per group in MLD SSM mapping entries.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	50
Network login—maximum number of clients being authenticated on MAC-based VLAN enabled ports.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	1,024
Network login—maximum number of clients being authenticated with policy mode enabled.	Summit X450-G2, X460-G2 Summit X670-G2, X770 ExtremeSwitching X620, X440-G2	1,024 512 256
Network login—maximum number of dynamic VLANs.	Summit X460-G2, X450-G2, X670-G2, X770 ExtremeSwitching X440-G2, X620	2,000 1,024
Network login VLAN VSAs—maximum number of VLANs a client can be authenticated on at any given time.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	10
ONEPolicy Roles/Profiles—maximum number of policy roles/profiles.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	63
ONEPolicy Rules per Role/Profile—maximum number of rules per role/policy.	Summit X450-G2, X460-G2	IPv6 rules: 256 IPv4 rules: 256 L2 Rules: 184 MAC Rules: 256
	Summit X670-G2, X770	IPv6 Rules: 256 L2 Rules: 184 MAC Rules: 256 IPv4 Rules: 256
	ExtremeSwitching X620, X440-G2	IPv6 and Mac Rules: 0 Ipv4 Rules: 256 (per switch) L2 Rules: 184 (per switch)
ONEPolicy Authenticated Users per Switch—maximum number of authenticated users per switch.	Summit X450-G2, X460-G2 Summit X670-G2, X770 ExtremeSwitching X620, X440-G2	Up to 1,024 Up to 512 Up to 256
ONEPolicy Authenticated Users— maximum authenticated users with a combination of TCI disabled/enabled profiles.	Summit X450-G2, X460-G2 Summit X670-G2, X770 ExtremeSwitching X620, X440-G2	682–1,022 341–510 TCI disabled: 170 TCI enabled: 256

Table 4: Supported Limits (continued)

Metric	Product	Limit
ONEPolicy Authenticated Users per Port—maximum number of authenticated users per port.	Summit X450-G2, X460-G2 Summit X670-G2, X770 ExtremeSwitching X620, X440-G2	Unlimited up to 1,024 Unlimited up to 512 Unlimited up to 256
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 ExtremeSwitching X620, X440-G2	952 440
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 ExtremeSwitching X620, X440-G2	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 ExtremeSwitching X620, X440-G2	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 ExtremeSwitching X620, X440-G2	256 256
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 ExtremeSwitching X620, X440-G2	184 184
OSPFv2/v3 ECMP—maximum number of equal cost multipath OSPFv2 and OSPFv3.	Summit X460-G2, X670-G2, X770, X450-G2 ExtremeSwitching X620 ExtremeSwitching X440-G2	For OSPFv2: 64 way; for OSPFv3: 32 way 4 way N/A
OSPFv2 areas—as an ABR, how many OSPF areas are supported within the same switch.	Summit X460-G2, X670-G2, X770 Summit X450-G2, ExtremeSwitching X440-G2, X620	8 4

Table 4: Supported Limits (continued)

Metric	Product	Limit
OSPFv2 external routes—recommended maximum number of external routes contained in an OSPF LSDB.	Summit X770, X670-G2, X460-G2, X450-G2 ExtremeSwitching X440-G2, X620	5,000 2,400
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.	Summit X670-G2, X460-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	2,000 1,000
OSPFv2 interfaces—recommended maximum number of OSPF interfaces on a switch (active interfaces only).	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	4 (with Advanced Edge licence)
	Summit X450-G2, X460-G2, X670-G2, X770	400 (with Core license)
OSPFv2 links—maximum number of links in the router LSA.	Summit X460-G2, X670-G2 Summit X450-G2, and ExtremeSwitching X620, X440-G2 Summit X770	400 4 419
OSPFv2 neighbors—maximum number of supported OSPF adjacencies.	Summit X770, X670-G2, X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	128 4
OSPFv2 routers in a single area—recommended maximum number of routers in a single OSPF area.	Summit X770, X670-G2, X460-G2 Summit X450-G2, ExtremeSwitching X440-G2, X620	50 4
OSPFv2 virtual links—maximum number of supported OSPF virtual links.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	32 4
OSPFv3 areas—as an ABR, the maximum number of supported OSPFv3 areas.	Summit X460-G2, X670-G2, X770 Summit X450-G2, ExtremeSwitching X440-G2, X620	16 4
OSPFv3 external routes—recommended maximum number of external routes.	Summit X770, X670-G2, X460-G2, X450-G2 ExtremeSwitching X440-G2, X620	10,000 1,200
OSPFv3 inter- or intra-area routes—recommended maximum number of inter- or intra-area routes.	Summit X770, X670-G2, X460-G2 Summit X450-G2, ExtremeSwitching X440-G2, X620	3,000 500

Table 4: Supported Limits (continued)

Metric	Product	Limit
OSPFv3 interfaces—maximum number of OSPFv3 interfaces.	Summit X770, X670-G2, X460-G2, X450-G2 ExtremeSwitching X440-G2, X620 Note: Active interfaces limit, with Advanced Edge license. (See below for Core license limits.)	4 N/A
	Summit X770 Summit X670-G2, X460-G2 Summit X450-G2, ExtremeSwitching X440-G2, X620 Note: With Core license. (See above for Advanced Edge license limits.)	128 256 4
OSPFv3 neighbors—maximum number of OSPFv3 neighbors.	Summit X770, X670-G2, X460-G2 Summit X450-G2, ExtremeSwitching X440-G2, X620	64 4
OSPFv3 virtual links—maximum number of OSPFv3 virtual links supported.	Summit X770, X670-G2, X460-G2 with Core license Summit Summit X450-G2, ExtremeSwitching X440-G2, X620	16 4
OVSDB Manager Connections—Maximum number of connections to managers that can be configured (either of TCP, PTCP, SSL, or PSSL).	Summit X770, X670-G2	8
OVSDB Managed Switches—Maximum number of OVSDB-managed switches.	Summit X770, X670-G2	1
PIM IPv4 (maximum interfaces)—maximum number of PIM active interfaces.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620, (Advanced Edge License)	512 4
PIM IPv4 (maximum interfaces)—maximum number of PIM-snooping enabled interfaces.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	512
PIM IPv4 Limits—maximum number of multicast groups per rendezvous point.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	180
PIM IPv4 Limits—maximum number of multicast sources per group.	Summit X460-G2, X670-G2, X770, X450-G2 ExtremeSwitching X440-G2, X620	5,000 1,500
PIM IPv4 Limits—maximum number of dynamic rendezvous points per multicast group.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	145
PIM IPv4 Limits—static rendezvous points.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	32
PIM IPv6 (maximum interfaces)—maximum number of PIM active interfaces.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620 (Advanced Edge License)	512 4

Table 4: Supported Limits (continued)

Metric	Product	Limit
PIM IPv6 Limits—maximum number of multicast groups per rendezvous point.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	70
PIM IPv6 Limits—maximum number of multicast sources per group.	Summit X460-G2, X670-G2 Summit X450-G2 Summit X770 ExtremeSwitching X440-G2, X620	2,500 2,000 2,500 550
PIM IPv6 Limits—maximum number of dynamic rendezvous points per multicast group.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	64
PIM IPv6 Limits—maximum number of secondary address per interface.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	70
PIM IPv6 Limits—static rendezvous points.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	32
Policy-based routing (PBR) redundancy—maximum number of flow-redirects.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	256[o]
Policy-based routing (PBR) redundancy—maximum number of next hops per each flow-direct.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	32[o]
Port-specific VLAN tags—maximum number of port-specific VLAN tags.	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	1,023 N/A
Port-specific VLAN tags—maximum number of port-specific VLAN tag ports.	Summit X770, X670-G2 Summit X460-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	6,400 4,000 N/A
Private VLANs—maximum number of subscribers. Assumes a minimum of one port per network and subscriber VLAN.	Summit X770 Summit X670-G2 Summit X460-G2 Summit X450-G2 ExtremeSwitching X440-G2 ExtremeSwitching X620	103 63 53 51 47 15
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 ExtremeSwitching X440-G2 ExtremeSwitching X620	1,024 255 510

Table 4: Supported Limits (continued)

Metric	Product	Limit
Private VLANs—maximum number of private VLANs in an L2-only environment.	Summit X770, X670-G2, X460-G2, X450-G2 ExtremeSwitching X440-G2, X620	1,280 255
PTP/1588v2 Clock Ports	Summit X770, X460-G2, X670-G2 ExtremeSwitching X440-G2, X620	32 for boundary clock 1 for ordinary clock N/A
PTP/1588v2 Clock Instances	Summit X770, X670-G2, X460-G2 ExtremeSwitching X440-G2, X620	2 combinations: • Transparent clock + ordinary clock • Transparent clock + boundary clock N/A
PTP/1588v2 Unicast Static Slaves	Summit X770, X670-G2, X460-G2 ExtremeSwitching X440-G2, X620	40 entries per clock port N/A
PTP/1588v2 Unicast Static Masters	Summit X770, X670-G2, X460-G2 ExtremeSwitching X440-G2, X620	10 entries per clock type N/A
Route policies—suggested maximum number of lines in a route policy file.	Summit X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	10,000
RIP Learned Routes—maximum number of RIP routes supported without aggregation.	Summit X770, X670-G2, X460-G2, and ExtremeSwitching X440-G2, X620	10,000
RIP interfaces on a single router—recommended maximum number of RIP routed interfaces on a switch.	Summit X670-G2, X460-G2 Summit X770, X450-G2 ExtremeSwitching X440-G2, X620	256 256 128
RIPng learned routes—maximum number of RIPng routes.	Summit X670-G2, X460-G2, X770, X450-G2 ExtremeSwitching X440-G2, X620	3,000 N/A
Spanning Tree (maximum STPDs)—maximum number of Spanning Tree Domains on port mode EMISTP.	Summit X450-G2, X770, X670-G2, X460-G2, and ExtremeSwitchingX620 ExtremeSwitching X440-G2	64 32

Table 4: Supported Limits (continued)

Metric	Product	Limit
Spanning Tree PVST+—maximum number of port mode PVST domains. Note: • Maximum of 10 active ports per PVST domain when 256 PVST domains are configured. • Maximum of 7 active ports per PVST domain when 128 PVST domains are configured.	Summit X770, X670-G2, and ExtremeSwitching X620 Summit X460-G2, X450-G2, and ExtremeSwitching X440-G2	256 128
Spanning Tree—maximum number of multiple spanning tree instances (MSTI) domains.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620 ExtremeSwitching X440-G2	64 32
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.	Summit X770, X670-G2 Summit X460-G2, X450-G2 ExtremeSwitching X440-G2 ExtremeSwitching X620	500 600 256 600
Spanning Tree—maximum number of VLANs on all MSTP instances.	Summit X770 Summit X670-G2 Summit X460-G2, X450-G2 ExtremeSwitching X440-G2 ExtremeSwitching X620	1,024 1,000 1,024 512 1,024
Spanning Tree (802.1d domains)—maximum number of 802.1d domains per port.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	1
Spanning Tree (number of ports)—maximum number of ports including all Spanning Tree domains.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620 ExtremeSwitching X440-G2	4,096 2,048
Spanning Tree (maximum VLANs)—maximum number of STP-protected VLANs (dot1d and dot1w).	Summit X770, and ExtremeSwitching X620 Summit X670-G2 Summit X460-G2, X450-G2 ExtremeSwitching X440-G2	1,024 560 600 500
SSH (number of sessions)—maximum number of simultaneous SSH sessions.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8
Static MAC multicast FDB entries—maximum number of permanent multicast MAC entries configured into the FDB.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	1,024

Table 4: Supported Limits (continued)

Metric	Product	Limit
Syslog servers—maximum number of simultaneous syslog servers that are supported.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	4
Syslog targets—maximum number of configurable Syslog targets.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	16
Telnet (number of sessions)—maximum number of simultaneous Telnet sessions.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8
Virtual routers—maximum number of user-created virtual routers that can be created on a switch.	Summit X460-G2, X670-G2, X770, X450-G2 ExtremeSwitching X440-G2, X620	63 N/A
Virtual router forwarding (VRFs)—maximum number of VRFs that can be created on a switch. Note: * Subject to other system limitations.	Summit X460-G2, X670-G2, X770, X450-G2 ExtremeSwitching X440-G2, X620	960 * N/A
Virtual router protocols per VR—maximum number of routing protocols per VR.	Summit X460-G2, X670-G2, X770, X450-G2 ExtremeSwitching X440-G2, X620	8 N/A
Virtual router protocols per switch—maximum number of VR protocols per switch.	Summit X460-G2, X670-G2, X770, X450-G2 ExtremeSwitching X440-G2, X620	64 N/A
VLAN aggregation—maximum number of port-VLAN combinations on any one superVLAN and all of its subVLANs.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	1,000
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.)	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	4,094
VLANs—maximum number of port-specific tag VLANs.	Summit X770, X670-G2, X460-G2 ExtremeSwitching X440-G2, X620	4,093 N/A
VLANs—maximum number of port-specific tag VLAN ports.	Summit X460-G2 Summit X770, X670-G2 Summit X450-G2, and ExtremeSwitching X440-G2, X620	4,096 8,192 N/A
VLANs (Layer 2)—maximum number of Layer 2 VLANs.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	4,094

Table 4: Supported Limits (continued)

Metric	Product	Limit
VLANs (Layer 3)—maximum number of VLANs performing IPv4 and/or IPv6 routing. Excludes sub-VLANs.	Summit X460-G2, X770, X670-G2, X450-G2 ExtremeSwitching X440-G2, X620	2,048 510
VLANs (maximum active port-based)—maximum active ports per VLAN when 4,094 VLANs are configured with default license.	Summit X770, X670-G2, X460-G2, X450-G2, and ExtremeSwitching X440G2 ExtremeSwitching X620	32 16
VLANs (maximum active protocol-sensitive filters)—number of simultaneously active protocol filters in the switch.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	16
VLAN translation—maximum number of translation VLANs. Assumes a minimum of one port per translation and member VLAN.	Summit X770 Summit X670-G2 Summit X460-G2 Summit X450-G2 ExtremeSwitching X620 ExtremeSwitching X440-G2	103 63 53 51 15 47
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 ExtremeSwitching X620 ExtremeSwitching X440-G2	1,024 512 255
VLAN translation—maximum number of translation VLAN pairs in an L2-only environment.	Summit X460-G2 Summit X450-G2, X770, X670-G2 ExtremeSwitching X440-G2, X620	2,046 1,024 512
VRRP (v2/v3-IPv4) (maximum instances)—maximum number of VRRP instances for a single switch, with Advanced Edge license or higher. Note: These limits are applicable for Fabric Routing configuration also.	Summit X770, X670-G2, X460-G2, X450-G2 ExtremeSwitching X440-G2, X620	511 128

Table 4: Supported Limits (continued)

Metric	Product	Limit
VRRP (v3-IPv6) (maximum instances)—maximum number of VRRP instances for a single switch, with Advanced Edge license or higher. (VRRP-VRRPv3-IPv6) Note: These limits are applicable for Fabric Routing configuration also.	Summit X770, X670-G2, X460-G2, X450-G2 ExtremeSwitching X440-G2, X620	511 128
VRRP (v2/v3-IPv4/IPv6) (maximum VRID)—maximum number of unique VRID numbers per switch.	Summit X770, X670-G2, X460-G2, X450-G2 and ExtremeSwitching X440-G2, X620 Note: With Advanced Edge license or higher	255
VRRP (v2/v3-IPv4/IPv6) (maximum VRIDs per VLAN)—maximum number of VRIDs per VLAN.	Summit X770, X670-G2, X460-G2, X450-G2 and ExtremeSwitching X440-G2, X620 Note: With Advanced Edge license or higher	255
VRRP (v2/v3-IPv4/IPv6) (maximum ping tracks)—maximum number of ping tracks per VLAN.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2 Note: With Advanced Edge license or higher	8
VRRP (maximum ping tracks)—maximum number of ping tracks per VRRP Instance under 128 VRRP instances, with Advanced Edge license or higher.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8 (20 centisecond or 1 second hello interval)
VRRP (v3-IPv6) (maximum ping tracks)—maximum number of ping tracks per VRRP Instance under 128 VRRP instances, with Advanced Edge license or higher.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8 (20 centisecond or 1 second hello interval)
VRRP (v2/v3-IPv4/IPv6) (maximum iproute tracks)—maximum number of IP route tracks per VLAN.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8
VRRP (v2/v3-IPv4/IPv6)—maximum number of VLAN tracks per VLAN.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8

Table 4: Supported Limits (continued)

Metric	Product	Limit
VXLAN—maximum virtual networks. Note: Every VPLS instance/ PSTag VLAN reduces this limit by 1. Assumption is all BUM (broadcast/unknown-unicast/ multicast) FDB entries are pointing to the same set of RTEPs when all VNETs use explicit flooding. Depends on whether all VNETs use standard or explicit and the number of tenant VLAN ports.	Summit X670-G2, X770 Summit X460-G2, X450-G2, and ExtremeSwitching X440-G2, X620	2,048–4,000 N/A
VXLAN—maximum tenant VLAN plus port combinations Note: Every (VPLS/PSTag VLAN) + port reduces the limit by 1.	Summit X670-G2, X770 Summit X460-G2, X450-G2, and ExtremeSwitching X440-G2, X620	4,096 N/A
VXLAN—maximum static MAC to IP bindings. Note: Every FDB entry configured reduces this limit by 1	Summit X670-G2, X770 Summit X460-G2, X450-G2, and ExtremeSwitching X440-G2, X620	64,000 N/A
VXLAN—maximum RTEP IP addresses	Summit X670-G2, X770 Summit X460-G2, X450-G2, and ExtremeSwitching X440-G2, X620	512 N/A
VXLAN—maximum virtual networks with dynamic learning and OSPF extensions for VXLAN	Summit X670-G2, X770 Summit X460-G2, X450-G2, and ExtremeSwitching X440-G2, X620	4,000 N/A
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.	Summit X450-G2, and ExtremeSwitching X440G2, X620	10 with 100 DACLs
XNV authentication—maximum number of VMs that can be processed (combination of local and network VMs).	Summit X460-G2, X670-G2, X770 Summit X450-G2, and ExtremeSwitching X440-G2, X620	2,048 1,024

Table 4: Supported Limits (continued)

Metric	Product	Limit
XNV database entries—maximum number of VM database entries (combination of local and network VMs).	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	16,000
XNV database entries—maximum number of VPP database entries (combination of local and network VPPs).	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	2,048
XNV dynamic VLAN—Maximum number of dynamic VLANs created (from VPPs / local VMs).	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	2,048
XNV local VPPs—maximum number of XNV local VPPs.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	2,048 ingress 512 egress
XNV policies/dynamic ACLs—maximum number of policies/dynamic ACLs that can be configured per VPP.	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	8 ingress 4 egress
XNV network VPPs—maximum number of XNV network VPPs.[p]	Summit X450-G2, X460-G2, X670-G2, X770, and ExtremeSwitching X620, X440-G2	2,048 ingress 512 egress

[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 4,096.

[p] The number of XNV authentications supported based on system ACL limitations.

3 Open Issues, Known Behaviors, and Resolved Issues

Open Issues
Known Behaviors
Resolved Issues in ExtremeXOS 22.1

This chapter lists open software issues, limitations in ExtremeXOS system architecture (known issues), and resolved issues in ExtremeXOS.

Open Issues

The following are new open issues for supported features found in ExtremeXOS 22.1.

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

CR Number	Description
General	
xos0065183	Recreating a VPN VRF with same name after deleting it produces a BGP error.
xos0066006	When ICMP redirect is received and the new gateway ARP is not resolved, the redirect route becomes valid and is used. This results in traffic being dropped. This problem is more apparent when the redirection happens to a host on a different subnet because ExtremeXOS enables IP ARP checking by default. Workaround: Disable IP ARP checking for this foreign redirect.
xos0066067	When a configuration file (.xsf) saved in ExtremeXOS 21.1 is run on ExtremeXOS 22.1, all the configured MAC lists, primary and secondary shared-secrets in RADIUS and TACAS, and NMS shared-secrets are replaced with empty strings.
ACL	
xos0064027	Due to limitations in slice depth, Summit X460-G2 series switches cannot have 512 single-wide rules in a single slice, causing applications like policy to not attain full capacities. Consequently, Summit X460-G2 series switches are constrained to Summit X450-G2 rule limits.
NetLogin	
xos0065247	Unauthenticated clients in NetLogin get DHCP IP address using NetLogin-authenticated VLAN when private VLAN is configured and clients are in isolated VLAN.
OVSDB	

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

CR Number	Description
xos0065008	OVSDB schema is not cleared when changing configuration and rebooting. Workaround: In setups where OVSDB is used to manage and configure the ExtremeXOS switch as a VTEP, the VTEP schema database must be manually cleared using the command `disable ovsdb schema` when the active configuration of an ExtremeXOS switch is changed using the CLI command `use configuration`. Failure to do so might result in OVSDB using a stale VTEP schema database.
xos0065504	The command `show ovsdb schema` can become unresponsive when either ExtremeXOS or OVSDB are synchronizing data.
xos0064657, xos0064656	switch_fault_status and port_fault_status are not set in the hardware_vtep schema. In ExtremeXOS 22.1, for switch_port_status and port_fault_status (PSTAG-like scenarios), EMS receives a log message.
SNMP	
xos0066062	SNMP community strings that are stored as encrypted using the command `configure snmp add community community_string readonly | readwrite store-encrypted` do not work after you upgrade from an earlier version of ExtremeXOS to version 22.1.
xos0066070	XSF scripts with encrypted communities and v3 users created with earlier versions of ExtremeXOS do not work on ExtremeXOS 22.1. Additionally, after loading the script, SNMP access remains disabled in ExtremeXOS 22.1, even if it was enabled in an earlier version of ExtremeXOS. This occurs because SNMP is disabled by default in ExtremeXOS 22.1 and enabled by default in earlier versions. Workaround: There are two possible workarounds: • Manually enable snmp access using the command `enable snmp access`, and then reconfigure the SNMPv3 users and v2c encrypted communities using the commands `configure snmpv3 add useruser_name {authentication {md5 | sha }auth_password {privacy { des | aes}} priv_password` and `configure snmp add community [readonly | readwrite] community_stringstore-encrypted`. • Backup the switch's previous version's configuration using the `save configuration prevvers.cfg` command in the earlier ExtremeXOS version, and then after upgrading, use the configuration using the command `use configuration prevvers.cfg`. This enables SNMP access and configures v3 users. However, the encrypted v2c communities need to be reconfigured manually using the command `configure snmp add community [readonly | readwrite] community_stringstore-encrypted`. For example, if upgrading from ExtremeXO 21.1.1.4-patch1-5.xos to 22.1.1.5.xos, when in 21.1.1.4-patch1-5, issue the command `save configuration cfg_21_1_1_4_patch1-5.cfg`. Now, after upgrading to ExtremeXOS 22.1, issue the command `use configuration cfg_21_1_1_4_patch1-5`.

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

CR Number	Description
xos0066086	User-defined SNMPv3 users do not work after upgrading to ExtremeXOS 22.1 if the SNMPv3 default-users were disabled using the command `disable snmpv3 default-user` in ExtremeXOS 21.1 or earlier.
SSH	
xos0066027	After downloading certificates, the commands `show ssl trusted-ca` and `show ssl ocsp-signature-ca` fail to show any output. However, PKI validation that makes use of these certificates works.
xos0065712	When repeated login and logout is performed using SSH-PKI (SSH login using certificates) for about two days from eight terminals, memory leak occurs.

Known Behaviors

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

Table 6: Known Issues, Platform-Specific, and Feature Change Requests (CRs)

CR Number	Description
General	
xos0064095	With MVRP, when there is greater than 1,500 VLANs to be advertised, `process mrp died with signal 11` error occurs. Workaround: Use the `configure mrp ports timers` command to increase the periodic timer value of MRP to 5 seconds from the default of 1 second, which throttles MRP process.
SSH	
xos0064755	Turning FIPS mode off when Secure mode is on loses the cipher configuration.
VRRP	
xos0064219	When downgrading the ExtremeXOS image from 22.1 to an earlier version, if you have set up a greater number of VRRP VRIDs per VLAN than are supported in that earlier release, but that are supported in version 22.1 (maximum of 255), VRRP instances for all VRIDs are incorrectly enabled. Workaround: After downgrading the ExtremeXOS image, configure VRRP to have no more than the supported number of VRRP VRIDs per VLAN that are supported for the downgraded version.
xos0065724	Traceroute fails when the intermediate router is a VRRP gateway.
VXLAN	
xos0064227	When using VNI ID match condition, it is not possible to match ARP fields in inner packet.
xos0064837	Replace-DSCP does not work for terminating nodes.

Resolved Issues in ExtremeXOS 22.1

The following issues were resolved in ExtremeXOS 22.1. ExtremeXOS 22.1 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, ExtremeXOS 15.7.1, ExtremeXOS 16.1, ExtremeXOS 16.1.2, ExtremeXOS 16.1.3, and ExtremeXOS 21.1. For information about those fixes, see the release notes for the specific release.

Table 7: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) in 22.1

CR Number	Description
General	
xos0055511	While configuring STP (802.1d) with port-encapsulation mode as EMISTP where the L2PT-enabled VMAN and access VLAN have the same tag, the designated bridge is not accepting the L2PT tunneled BPDUs from the root bridge, and thus causes a loop (designated bridge also becomes a root bridge). This problem does not occur: • When the access VLAN's tag and the L2PT-enabled VMAN's tag are different. • Without any L2PT configured, with the same tag used for the access VLAN and provider-edge VMAN. • When using Per-VLAN Spanning Tree Plus (PVST+), regardless of same or different tags.
xos0058668	After rebooting DHCPv6, client remains in rebooting state.
xos0063183	Chalet's web login requires RADIUS Netlogin to be enabled for RADIUS authentication to succeed when only Mgmt-Access should be required.
xos0063331	VLAN IP address is unconfigured when modifying the VLAN name/port information from Chalet.
xos0063554	The following vulnerability in OpenSSL exists that impacts ExtremeXOS (CVE-2015-3197): A malicious client can negotiate SSLv2 ciphers that have been disabled on the server and complete SSLv2 handshakes even if all SSLv2 ciphers have been disabled, provided that the SSLv2 protocol was not also disabled via SSL_OP_NO_SSLv2. This issue affects OpenSSL versions 1.0.2 and 1.0.1.
xos0064043	Unable to use a configuration file that has been copied from an existing configuration file.
xos0064216	Unable to ping a destination which is reachable, if the destination is also present locally but disabled.
xos0064220	Calling-station-id attribute is missing in the RADIUS request for mgmt-access.
xos0064240	No log message appears by default when a BGP peer transitions to established or from the established state.
xos0064436	When adding ports to VLAN from Chalet, IPforwarding gets disabled for that VLAN.
xos0064446	Vulnerability CVE-2016-2108 Negative Zero.
xos0064447	Creation of user accounts through XML does not work.
xos0064459	Nettools process ends unexpectedly with signal 11 when processing router advertisement packets with DNSSL option.

Table 7: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) in 22.1 (continued)

CR Number	Description
xos0064682	Enabling egress VMAN CEP filtering on a CEP port sends a tagged packet, even though it should be forwarded as untagged.
xos0064722	Setting a CoS component IRL or IUB to none (0) in Policy manager (Extreme Management Center) should imply an interpretation by the platform of rate equivalent to "unlimited." However when "0" or "none" is enforced to a Summit Ingmeter this does not mean unlimited, but instead a literal 0 rate
xos0064863	Hostname is not getting resolved via DNS while initiating SSH/SCP/TFTP from switch.
xos0064890	Kernel oops occurs randomly when there is a lot of slow path forwarded traffic and continuous link flaps.
xos0064956	EDP neighbors are not displayed when remote mirroring is disabled or after unconfiguring a monitor port of remote mirroring.
xos0064960	Multicast traffic is forwarded through MVR receiver port in a VLAN even if there is no active receiver.
xos0065073	Kernel oops observed when IPv6 duplicate address detected in the switch.
Summit Family Switches	
xos0058437	For Summit X460 and X670-G2 series switches, the buffer for Weighted Random Early Detection (WRED) queues is incorrectly allocated at 10% of shared memory plus minimum guarantee, when it should be 100% of shared memory plus minimum guarantee.
xos0062972	Add Support for the following optics on Summit X670-G2 and X770 series switches: • 10329, 908618-10, 40Gb BiDi QSFP+ • Avago AFBR-79EBPZ-EX1 optic transceiver
xos0063433	On Summit X670 series switches, process rtmgr pid 1554 ends unexpectedly with signal 6 after disabling/enabling links in the active LSP path.
xos0064068	When booting with policy enabled or enabling policy after booting, the writing of policy rules is slow. This can also block the saving of the configuration.
xos0064232	On Summit X670-G2 and X770 series switches, after changing a VPWS service VLAN tag, traffic continues to be forwarded with the prior tag.
SummitStack	
xos0062753	System-health-check previously ran only on master and backup modules. As a result, any errors on the standby modules of the stack were not checked and reported. The system-health-check process now runs on all ‘operational’ or ‘alive’ modules in the stack, including standby modules.
xos0063743	On SummitStacks, after a save, and then reboot, the master node does not reboot and the following error "Timed out - HAL is not responding" appears.
xos0063788	The following error appears continuously in backup/standby nodes when node is put in the failed state due to a license/ExtremeXOS mismatch: `&ltErro:DM.Error&gt Slot-2: Node State[185] = FAIL (License Mismatch)`
xos0063919	On standby nodes, IP ARP refresh and Neighbor refresh are now disabled on VR-Mgmt. Primary and backup nodes use the configured enabled/disabled setting.

Table 7: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) in 22.1 (continued)

CR Number	Description
xos0064575	"Operation draining timed out" error message appears while saving the configuration in stacking switch.
ExtremeSwitching X440-G2 Series Switches	
xos0062583	Policy: Dynamic VLAN is not removed from backup slot after issuing `unconfigure policy maptable`.
xos0064964	Misleading fan failure may be reported on ExtremeSwitching X440-G2-12t and X440-G2-12p switches due to internal fans running at 0 RPM. Fans in these models may operate at 0 RPM if the system temperature is maintained without running the fans. This is normal operation.
ExtremeSwitching X620 Series Switches	
xos0062890	On ExtremeSwitching X620 series switches, 100 mbps SFPs (100FX, FX/LX, BASET) fail to link on reboot.
Summit X460-G2 Series Switches	
xos0063811	Summit X460-G2 series switches with ExtremeXOS 15.6 through 21.1, have the following limitations for SyncE input reference frequency: • Network clock does not lock with input SyncE source port 52 (both at 10G and 1G speed) on all 48-port models (X460-G2-48t, 48x and 48p). Note: For SyncE input at 10G, avoid port 52. • When the 10G ports operate at 1G speed, the network clock does not lock. Models with Ethernet BASE-T or Power over Ethernet (PoE) ports may lock on initial configuration, but do not lock after a save and reboot. Note: For SyncE input at 1G, use a 1G port, not a 10G port.
xos0063960	Several help options do not appear for the `show fdb` command.
xos0064472	SyncE clock switchover does not occur when the clock source ports medium are different. When the clock source configured on a fiber port is then unconfigured, and reconfigured, for another copper port, the clock status goes into holdover mode. After a reboot it gets locked.
xos0064713	In SummitStacks, memory leak happens in NetLogin process when continuous MAC authentication occurs leading to a backup node reboot.
Summit X670-G2 Series Switches	
xos0064568	After slot reboot, traffic drop occurs on VPLS service VLAN LAG port.
ACL	
xos0064170	When ClearFlow is enabled with around 4,000 rules with separate counters, the HAL process utilization almost always stays at 40%.
xos0064496	BGP route policy performs improper community delete operation.
xos0064523	Dynamic ACL rule is not removed properly when turning off packet capture.
xos0064573	ACL process ends unexpectedly after refreshing a policy with clear-flow rules.
BGP	

Table 7: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) in 22.1 (continued)

CR Number	Description
xos0064884	"remove-private-AS-numbers" setting in BGP is not preserved after switch reboot.
xos0065189	BGP secondary best path is not active when primary best path goes down.
MLAG	
xos0056368	Kernel errors occur after disabling sharing configuration on ISC ports of MLAG. For example: "exvlan: handleVsmKernelRequest:8545: handleVsmKernelRequest Invalid Ingress port: 1000008 got"
MPLS	
xos0063968	HAL process ends unexpectedly after changing/reverting service VLAN tag.
xos0064386	With L3VPN, deleting the user VR type VPN-VRF causes process rtmgr to end unexpectedly with signal 11.
Python	
xos0064122	The command `show tech-support` terminates prematurely when 40G or 100G optics are present in the switch.
Security	
xos0062721	With Policy enabled, UPM scripting is not executed on an authentication.
xos0061359	Policy has no PVID after unconfiguring the switch.
xos0062850	When upgrading ExtremeXOS to 15.7 or later releases, the web HTTP access is enabled even though it is disabled in the configuration.
xos0063190	Session timeout value is inappropriately overwriting the idle time-out value whenever both session timeout and idle timeout values are same, or the idle timeout value is 0.
xos0064029	Cannot delete prefixes for VLAN router advertisement messages after setting them.
xos0064334	With both dot1x and MAC enabled on same port and with default protocol order, UPM auth profile is executed only for MAC authentication; dot1x is not executed. Logoff profile is also executed only for MAC user and not for dot1x user.
SNMP	
xos0057212	SNMP traps not sent after changing or saving configuration, even though respective traps are enabled.
xos0064114	SNMP process ends unexpectedly with signal 6 after running the switch for a long time.
SSH	
xos0062368	Key based authentication happens for the users without the userS being bound to the key. Any user in the switch is authenticated provided the key is present.
xos0062431	Disabled accounts and locked out users can logon using keys.
xos0063347	IPv6 address is not supported in SCP client present in the device.
VLAN	
xos0063761	Traffic is not forwarded after disable/enable sharing when traffic ingressing port is part of both port specific tag (PSTag) and service VMAN (untagged port).

Table 7: Resolved Issues, Platform-Specific, and Feature Change Requests (CRs) in 22.1 (continued)

CR Number	Description
xos0062912	SNMP trap sent for link up/down status change does not include port instance.
xos0063837	After deleting pstag port from a VLAN that has two LAG ports added as untagged, an error message appears.
xos0064094	Removing subscriber VLAN from one PVLAN affects traffic in another PVLAN.
xos0064100	With policy enabled, switch reloads with kernel oops when deleting a port from a VLAN that also has the same port added to PSTag.
xos0064491	The configuration of a disabled VLAN without any ports does not appear in the output of the `show configuration` command.
xos0064909	Traffic loss occurs while changing and reverting the base VID of VLANs with PSTag ports.
xos0064910	The following error message occurs while changing tag value in VLANs having port-specific tag configured ports: `<Erro:Kern.MPLS.Error> MPLS bcm_esw_mpls_port_match_vlan_del failed`
VRRP	
xos0063346	With multiple (greater than two) VRRP instances and host-mobility enabled, FDB flush sent during topology change from other L2 protocols does not occur.