Extreme OS ONE Switching and Routing v22.2.3.0 Release Notes

New Features, Bug Fixes, and Known Limitations

9041130-00 Rev AA
August 2026

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, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

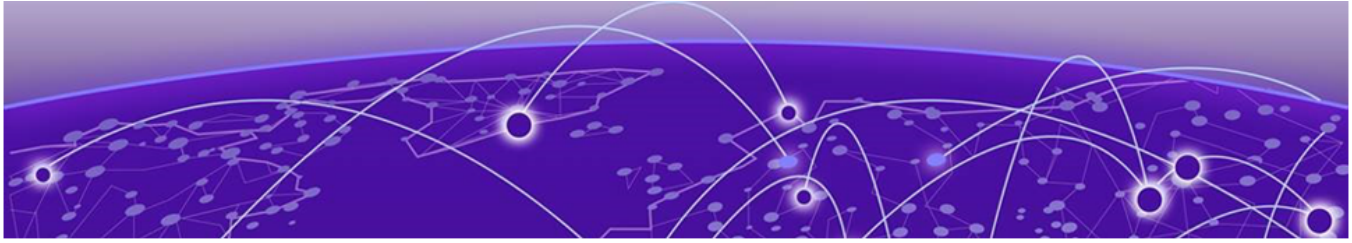
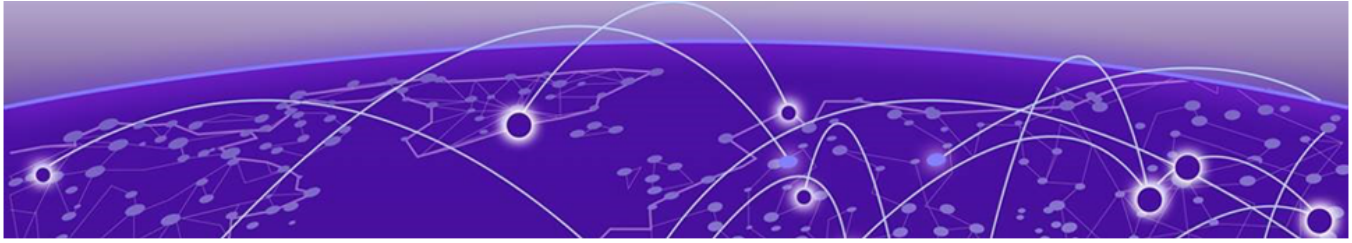
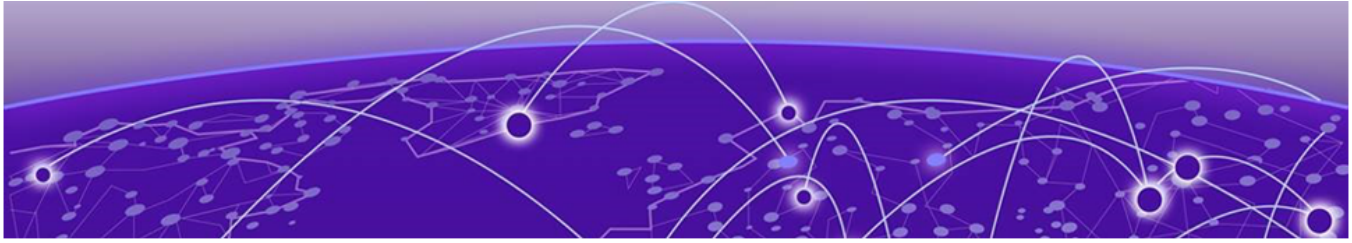


Table of Contents



Abstract

The Extreme OS ONE Switching and Routing v22.2.3.0 Release Notes provides a comprehensive overview of essential updates, technical improvements, and known limitations for advanced IP fabric and data center environments. The document provides guidance on deployment scenarios, configuration best practices, and troubleshooting, addressing open issues and restrictions relevant to network engineers and administrators.



Release Notes

Introduction to Extreme OS ONE

Extreme OS ONE is a cloud-native network operating system (NOS) based on a micro-services architecture. Key characteristics include:

- Modular and composable design for a simple software life-cycle management.
- API-first approach for management programmability.
- Data plane abstraction, supporting integration with multiple ASIC vendors and accelerating the introduction of new hardware platforms.
- Security-first principles that enhance responsiveness to vulnerabilities and minimize the attack surface.

Extreme OS ONE is a high-performance network operating system designed for data centers, service provider, and enterprise networking environments. Extreme OS ONE powers Extreme 8000 series devices.

For a complete set of Extreme OS ONE Switching and Routing documentation, see the https://supportdocs.extremenetworks.com/support/documentation/extreme-os-one-switching-and-routing-v22-2-3-0/.

New in this Release

Extreme OS ONE Switching and Routing 22.2.3.0 introduces the following features and enhancements.

Feature	Description
RoCE v2 Switch Stack - Priority-based Flow Control (PFC)	Priority-based Flow Control (PFC) under IEEE 802.1Qbb creates eight virtual priority queues, allowing congested RoCE v2 traffic to pause without affecting best-effort or control traffic mapped to the affected priority queue.
DCBX for RoCEv2 Signaling	Data Center Bridging Exchange (DCBX) enables directly connected network devices to discover, negotiate, and validate Data Center Bridging (DCB) configurations automatically.
RoCE v2 Switch Stack - Enhanced Transmission Selection (ETS)	Enhanced Transmission Selection (ETS) allocates dedicated bandwidth to specific traffic classes in a switch stack, preventing RoCE v2 storage and RDMA flows from starvation by background network traffic.
RoCE v2 Switch Stack - Congestion Notification (ECN)	Explicit Congestion Notification (ECN) marks packets when buffer queues fill up, enabling end hosts to reduce transmission rates proactively and avoid traffic loss or pause storms.
Azure Local LLDP Extensions	Link Layer Discovery Protocol (LLDP) support on physical top-of-rack switches enables Azure Local to perform automated topology discovery, diagnostics, and telemetry verification.
Remote Switch Port Analyzer (RSPAN)	Remote Switch Port Analyzer (RSPAN) enables monitoring and traffic capture from source ports distributed across multiple switches.
MLAG Resiliency Improvement for PS Failure, Disk Full triggers	Improves MLAG cluster resilience by detecting and handling hardware and software failure triggers such as PS failure & Disk full.
Multiple Spanning Tree Protocol (MSTP)	Multiple Spanning Tree Protocol (MSTP), defined in IEEE 802.1s, prevents network loops while enabling traffic load balancing across different VLANs. MSTP operates on instances rather than directly on VLANs, allowing multiple VLANs to be associated with the same instance or mapped to different instances.
BGP Large Communities	BGP Large Communities are 96-bit BGP path attributes defined in RFC 8092 that natively support 4-byte Autonomous System Numbers (ASNs) for flexible routing policy configuration.
BGP route aggregation	BGP route aggregation combines multiple smaller IP route prefixes into a single larger prefix announcement.
DHCP Relay IPv4	The DHCP Relay Agent centralizes IP address and network configuration distribution across multiple subnets or VLANs by intercepting local DHCP broadcast messages from clients and forwarding them as unicast traffic to remote DHCP servers.
VRRP (IPv4)	Virtual Router Redundancy Protocol (VRRP) enables multiple routers to share a single virtual IP address, providing a reliable default gateway for local devices.
Low level firmware packaging as part of the software package upgrade	Automates BMC and FireLight firmware updates during OS ONE Switching and Routing image installation on 8520/8720/8730 switches by bundling vendor firmware binaries in the image and triggering version-checked, pre-boot upgrades with user prompting, failure handling, and show version visibility into firmware sync status.

Feature	Description
SNMP Notification for Fan and PS failure and recovery events	Introduces extremePlatformMIB to enable SNMP monitoring of fan and power supply FRU status. Delivers fruStatusChanged trap notifications for every fan/PSU state transition (failure, recovery, insertion, removal).
SNMP MIB and Notification for Optical Transceivers	Introduces EXTREME-OPTICAL-MONITORING-MIB to enable SNMP polling of per-port and per-lane DDM sensor values (temperature, voltage, Tx/Rx power, Tx bias). Delivers trap notifications on threshold crossings and unqualified optic insertion.
SNMP Configurable Engine-id, SysDesc, Groups & Views	Allows configuration of SNMP Engine ID and System Description. Implements View-based Access Control Model (VACM) to configure views, groups, and associations with SNMPv1/v2c communities and SNMPv3 users, providing granular MIB access control.
SNMP Informs	Adds reliable SNMP notification delivery through SNMP Informs support (SNMPv2c/v3) with per-host configurable notify-type, remote engine ID for SNMPv3, and explicit enable command to prevent unintended trap transmission.
Support restriction of system internal IPv4/IPv6 subnet conflict within potential customer subnet	Allows operators to configure the internal IPv4/IPv6 address ranges used by the embedded K3S cluster, preventing conflicts with customer subnets. Changes take effect on the next system reboot.

Hardware Support

Extreme OS ONE Switching and Routing 22.2.3.0 and later releases support Extreme 8520, Extreme 8720, Extreme 8730, and Extreme 8820 hardware platforms.

Upgrade and Downgrade Considerations

For more information about firmware upgrade and downgrade, see *Extreme OS ONE Switching and Routing Deployment Guide*.

Upgrade from 22.2.2.0 to 22.2.3.0 using Full Install

For more information about full install, see *Extreme OS ONE Switching and Routing Command Reference Guide*.

Note

- Always back up the configuration and enable maintenance mode on reload before upgrading devices.
- Automatic rollback is triggered if microservices fail to come up after the upgrade.
- Standard firmware rollback reverts to the previous image.
- Upgrade device running with SLX-OS to 20.8.1 before attempting migration.
- Rollback to SLX-OS after OS ONE migration is not supported. Downgrade requires ONIE-based installation.
- Use a platform-specific SLX-OS image. Do not interchange images across platforms.

SLX-OS to OS ONE Migration

This procedure provides instructions to migrate supported platforms from **SLX-OS** to **OS ONE**.

Supported Migration Method

CLI-based migration method (Recommended for controlled upgrades)

Important

- Migration is **disruptive** and results in a **cold reboot**.
- Post-migration, a **System Firmware Commit** must be executed before the device is placed into use.

Limitations

- Third-Party Virtual Machine (TPVM) partition will be removed as part of the migration and cannot be recovered post-migration.
- Rollback to SLX-OS is not supported after migration is completed. Downgrade requires ONIE-based installation.
- Configuration migration is not supported. Manually reapply configuration after OS ONE installation.
- For SLX-OS to OS ONE 22.2.3.0 migration, executing a system firmware full-install after migration may render the device unusable. Full-install after migration is not recommended.
- Use system firmware upgrade for post-migration upgrades.
- OSOneSR-22.2.3.0.bin is the recommended build for migration. Firmware upgrade and firmware full-install function as expected in this release.

Install OS ONE on SLX Platforms

You can install OS ONE on SLX platforms.

Before You Begin

- Upgrade device running with SLX-OS to 20.8.1 before attempting migration
- Valid image is available on SCP/FTP/SFTP/TFTP server or USB
- Reachability to the image server
- Management VRF details (if applicable)
- Maintenance window approved (device reboot required)
- Back-up running configuration before migration

Note

- ONIE menu behavior may vary based on platform and BIOS version.
- When a full ONIE menu is present, **ONIE Rescue mode cannot be used** for ONIE-uninstaller.

About This Task

This method uses the **firmware download migrate** command and is supported from **SLX-OS 20.8.1 and later**.

Procedure

1. Log in to the device running **SLX-OS**.
2. Run the firmware migration command using the appropriate protocol.

   ```
   firmware download migrate <protocol> [options]
   ```

   SCP Example (with VRF):

   ```
   firmware download migrate scp user <username> password <password> host <host-ip>
   directory <image-path> use-vrf mgmt-vrf file <image-name>
   ```

3. Review all system-generated warnings carefully, including:
   - Hardware profile changes
   - MTU default reset warnings
   - Maximum-path restrictions
   - Confirmation that TPVM partition will be deleted
4. Type `y` and press `Enter` to proceed when prompted.

   ```
   Do you want to continue? [y/n]:
   ```

   The system performs the following:
   - Download the OS ONE image
   - Validate the image
   - Install the firmware
   - Automatically reboot the device

5. Perform the `Post-Migration Mandatory Actions`.
   a. Log in using default credentials:
      - Username: admin
      - Password: password
   a. Perform **System Firmware Commit**.

      ```
      system firmware commit
      ```

   b. Verify that OS ONE is correctly installed:

      ```
      show firmware
      ```

OS ONE to SLX-OS Migration

This procedure provides instructions to migrate supported platforms from **OS ONE** to **SLX-OS** using ONIE.

Supported Migration Method

ONIE Install (clean install using ONIE)

Important

- Migration is **disruptive** and may impact traffic during reboot.
- Configuration is erased during this process. Ensure a backup/restore plan is in place.

SLX-OS Image Selection (Mandatory)

Note
Use the correct image for the hardware platform. Do not interchange images.

SLX-OS Image File Name	Supported Platforms
`SLXOS_SWBD3200-20.8.1slxos20.8.11_231201_1030-ONIE.bin`	8720, 8520-48XT, 8520-48Y
`SLXOS_SWBD4200-20.8.1slxos20.8.1_231201_1030-ONIE.bin`	8820-40C, 8820-80C

Install SLX-OS on OS ONE Platforms

You can install SLX-OS on OS ONE platforms.

Before You Begin

- ONIE menu behavior may vary by platform/BIOS.
- Always verify platform-to-image mapping before installation.
- Reapply configuration after migration (backup/restore).

About This Task

Follow this procedure toi install SLX-OS on OS ONE platforms.

Procedure

1. Reboot into ONIE.
   a. Reboot from OS ONE CLI and press Esc within 5 seconds to enter GRUB.
   b. Select ONIE.

      If full ONIE menu is unavailable, use ONIE Rescue.
2. Ensure management connectivity on eth0/eth1 (DHCP or static).
3. Remove the existing OS ONE.

   ```
   onie-uninstaller
   ```

   This may take 20–30 minutes. The device reboots automatically.
4. Install the correct SLX-OS image using the supported methods.

   Replace `<SWBDxxxx>` with the mapped image for your platform.

   - HTTP / Wget

     ```
     onie-nos-install SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
     ```

   - TFTP

     ```
     tftp -g -r SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin <TFTP_Server_IP>
     onie-nos-install SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
     ```

   - FTP

     ```
     ftpget -u <username> -p <password> <Server-IP>
     SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin onie-nos-install
     SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
     ```

   - USB

     ```
     mkdir /mnt/usb
     ```

     ```
     mount /dev/sda1 /mnt/usb onie-nos-install /mnt/usb/
     SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
     ```

   - HTTP / Wget

     ```
     onie-nos-install SLXOS_<SWBDxxxx>-20.8.1slxos20.8.1_231201_1030-ONIE.bin
     ```
5. Perform post-installation validation.

   ```
   dhcp ztp cancel
   ```

   ```
   show version
   ```

Supported FEC Modes

Table 1: Extreme 8730 FEC Matrix

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
400G	400G DR4	RS-FEC	Auto, RS-FEC
400G	400G DAC	RS-FEC	Auto, RS-FEC
400G	400G SR8	RS-FEC	Auto, RS-FEC
400G	400G LR4	RS-FEC	Auto, RS-FEC
400G	400G LR4P	RS-FEC	Auto, RS-FEC
400G	400G AOC	RS-FEC	Auto, RS-FEC
400G	400G DR4X	RS-FEC	Auto, RS-FEC
400G	400G Fr4	RS-FEC	Auto, RS-FEC
100G	100G DAC	RS-FEC	Auto, RS-FEC, Disabled
100G	100G SR4	RS-FEC	Auto, RS-FEC, Disabled
100G	100G eSR4	RS-FEC	Auto, RS-FEC, Disabled
100G	100G 4WDM	Disabled	Auto, RS-FEC, Disabled
100G	100G CWDM	RS-FEC	Auto, RS-FEC, Disabled
100G	100G SWDM4	Disabled	Auto, RS-FEC, Disabled
100G	100G Dr	Disabled	Auto, RS-FEC, Disabled
100G	100G FR	Disabled	Auto, RS-FEC, Disabled
100G	100G AOC	RS-FEC	Auto, RS-FEC, Disabled
100G	100G LR4	Disabled	Auto, RS-FEC, Disabled
100G	100G LR4-Lite	RS-FEC	Auto, RS-FEC, Disabled
100G	100G ER4LT	Disabled	Auto, RS-FEC, Disabled
100G	100G Breakout Dr	Disabled	Auto, RS-FEC, Disabled
100G	100G Breakout FR	Disabled	Auto, RS-FEC, Disabled
100G	100G Breakout LR	Disabled	Auto, RS-FEC, Disabled
25G	Breakout DAC	RS-FEC	Auto, RS-FEC, FC-FEC, Disabled
25G	Breakout SR	Disabled	Auto, RS-FEC, FC-FEC, Disabled

Table 1: Extreme 8730 FEC Matrix (continued)

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
25G	Breakout AOC	Disabled	Auto, RS-FEC, FC-FEC, Disabled
25G	25G LR	Disabled	Auto, RS-FEC, FC-FEC, Disabled

Table 2: Extreme 8720, Extreme 8520, and Extreme 8820 FEC Matrix

Port Type	Media Type	Default FEC Mode	Supported FEC Modes
100G	100G DAC	RS-FEC	Auto, RS-FEC, Disabled
100G	100G SR4	RS-FEC	Auto, RS-FEC, Disabled
100G	100G eSR4	RS-FEC	Auto, RS-FEC, Disabled
100G	100G 4WDM	Disabled	Auto, RS-FEC, Disabled
100G	100G CWDM	RS-FEC	Auto, RS-FEC, Disabled
100G	100G SWDM4	Disabled	Auto, RS-FEC, Disabled
100G	100G Dr	Disabled	Auto, RS-FEC, Disabled
100G	100G FR	Disabled	Auto, RS-FEC, Disabled
100G	100G AOC	RS-FEC	Auto, RS-FEC, Disabled
100G	100G LR4	Disabled	Auto, RS-FEC, Disabled
100G	100G LR4-Lite	RS-FEC	Auto, RS-FEC, Disabled
100G	100G ER4LT	Disabled	Auto, RS-FEC, Disabled
100G	100G Breakout FR	Disabled	Auto, RS-FEC, Disabled
25G	Breakout DAC	RS-FEC	Auto, RS-FEC, FC-FEC, Disabled
25G	Breakout SR4	Disabled	Auto, RS-FEC, FC-FEC, Disabled
25G	Breakout AOC	Disabled	Auto, RS-FEC, FC-FEC, Disabled
25G	25G LR	Disabled	Auto, RS-FEC, FC-FEC, Disabled

Supported Optics

For a complete list of all supported optics, see Extreme Optics at https://optics.extremenetworks.com/ONE/

Limitations and Restrictions

This section documents the known issues, limitations, design choices, and restrictions identified as of this release. Workarounds are provided where applicable.

Feature	Limitations and Restrictions
ROCEv2	• QOS profiles are configurable on physical interfaces only, not on VEs. • DCBX operates per interface only, not per VLAN or per LAG member. • Headroom and PFC XOff/XOn configurations are not supported. • ECN counters increment on Q0 for any queue. • RoCEv2 over MLAG/EVPN is not supported.
MSTP	• MST region configuration and VLAN-to-Multiple Spanning Tree Instance (MSTI) mapping: The single CIST instance governs all VLANs on an MSTP-enabled port. • MSTI domains: The switch supports only Instance 0 (CIST). • Spanning Tree Protocol (STP) on Multi-Chassis Link Aggregation (MLAG) interfaces is not supported. • Boundary port behavior details beyond CIST-only interaction with STP and Rapid STP (RSTP) peers. • Bridge Protocol Data Unit (BPDU) Guard, Admin Edge Port (PortFast), and BPDU Filter are not supported. • Root Guard, Loop Guard, and Edge Guard are not supported. • Spanning Tree across VXLAN or EVPN overlays is not supported. • Per-VLAN STP (PVST) and Rapid PVST are not supported. • Default-mode bridge domain support is not supported. • MST Priority Vector cannot be configured through this interface. • MST timer parameters (Hello Time, Max Age, Forward Delay, and Max Hops) cannot be configured through this interface.
RSPAN	• Only one remote-span interface can be configured per mirror session. • A mirror session cannot simultaneously use local mirror destination ports and remote-span destinations. • MLAG interfaces cannot be configured as remote-span destinations. • VLAN IDs must be within the range 1–4094. • Remote-span is supported only on Ethernet, Internal, and Port-channel interfaces. • Overlapping VLAN bridge-domain and remote-span configurations are not supported.
BGP Large community	BGP Large community is not supported in EVPN routes.

Feature	Limitations and Restrictions
DHCP Relay	• DHCPv6 relay functionality is not supported. • DHCP Relay and Server functionality cannot be deployed on the same node. • Standard option 82 support is provided; vendor-based customization is not supported.
MLAG Resiliency — Disk Full Triggers	• If the rootfs size drops below 500 MB, the device may reboot. Clear rootfs space to restore CLI functionality. • Automatic tech support collection is not triggered when a disk full condition is detected.
VRRP	The following are not supported: • IP Prefix Reachability object tracking • Accept Mode • Extended VRRP • IPv6
Resilient Hashing (RH)	RH does not support changes to ECMP paths made by routing protocols. If a protocol such as BGP updates ECMP paths, RH cannot maintain flow consistency.
BFD	The following are not supported: • Authentication • Demand and Echo modes
BGP Events and Notifications	• Only IPv4 Standard MIB is supported • Only IPv6 Enterprise MIB is supported
SNMP Events and Notifications for BFD	• Standard MIB is not supported • Only Enterprise MIB is supported along with proprietary Extreme MIB.
L3 HW Resource Monitoring	• There is no alarm support. • The configuration to rate-limit the generation of events and traps through threshold monitoring is currently not available.
IPV6 RA RS	The following are not supported: • Origination of Router Solicitation • IPV4 Router advertisement
List Key Values	• "*" is not supported in list key values. • All printable ASCII characters are supported except with white space for the fields: group, groupname, view, read-view. • All printable ASCII characters are supported except "/" and "." for ssl-profile-id • All printable ASCII characters are supported except ": , /", and "," for username • Only alphanumeric and "-" are supported for hostname.

Feature	Limitations and Restrictions
SNMP	When snmpwalk is performed at the root, snmpwalk on all MIBs may end with the following message: "No more variables left in this MIB View (It is past the end of the MIB tree)". There are no issues when MIB OID is used for snmpwalk.
Static Routing	Proxy ARP/ND is not supported.
BGP Underlay	The following are not supported: • Confed-AS • IPv6 Link-local Peering • Selection-Knobs (Default-Metric, Enforce-First-AS)
L2 / L3 QoS (Broadcom Trident 4–based platforms - TD4)	Due to a hardware limitation of only four multicast queues, counters for unknown unicast and multicast traffic are mapped accordingly (Applicable for TD4). • Updating the default-traffic-class value overwrites the CoS 0 to TC (Traffic Class) mapping in hardware for default mode BD (Bridge Domain) members. • Egress L2 Remarking is always enabled in hardware. • To apply ingress QoS maps on VLAN Mode BD, configure QoS Maps under the Ethernet or Port-Channel interface. This ensures the configuration is looped through all LIFs (Logical Interfaces) under the interface and applied consistently. • Any QoS configuration applied directly to VLAN Mode BD LIFs is ignored. If the same LIF is moved to a Default Mode BD, the configuration is replayed. • The Trust DSCP setting is not effective unless a user-defined map is configured and attached to the L2 LIF. • If a specific QoS configuration exists on a LIF under an Ethernet or Port-Channel interface, the QoS Map from the parent interface is not applied until the specific configuration is removed from the LIF. • When QoS configuration is deleted from a LIF, the configuration from the parent Ethernet or Port-Channel interface is automatically applied to the LIF.
BGP Default route originate	Only the default-route-originate command method is supported on per peer-group. The redistribute/send-default-route and network commands are globally supported and applicable to all peer-groups. However, all three methods are not supported on a per peer-group basis.
Authentication, Authorization and Accounting (AAA)	Radius accounting for GNMI is not supported.

Feature	Limitations and Restrictions
Logging	• All system logs such as /var/auth/log are by default exported to the syslog server. • Filtering is not supported. • Forward Referencing to tls-profile-id is not supported: **Workaround:** 1. Import required ca certificate before configuring rsyslog server. 2. If rsyslog is already configured and a CA certificate is imported or rotated later, delete the `tls-profile-id` in the rsyslog configuration and reconfigure it or disable and enable it back.
Certificate Management	When using the certificate import or export command, if the password is provided inline, it is displayed in plain text on the screen. **Workaround:** As a workaround, use the interactive method to import or export the certificate. In this mode, the password is entered securely and is not displayed on the screen.
Port Operations	Advanced port QSFP28, ToD, and GNSS port on 8730 platform are not supported.
OOB (Management port)	• If the secondary port is active and the primary port is down, replugging the primary port and removing the secondary within 5 seconds does not trigger a change in active mode. • MTU settings are currently not supported for OOB management interfaces. • On 8730 platform mgmt 0, interface operates at a fixed speed of 10G. When interface mgmt 0 is up or down, the individual speeds of mgmt 1 and mgmt 2 are reflected on respective interfaces, extMgmt 1 and extMgmt 2.
Third-Party Virtual Machine (TPVM)	Hashed password configuration for TPVM/trusted peer is not supported
SNMP Groups & Views	Notify-View is not supported

Open Issues

The following defects are open in this release of the software.

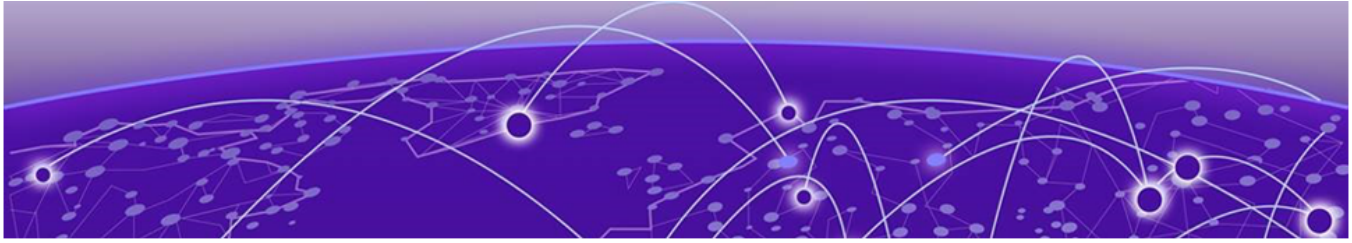
Issue ID	Description
TOS-35793	**Symptom:** In rare cases, changing the default admin password fails with the error message: *admin user password update failed*. The failure persists after copying the default configuration, preventing console login. **Condition:** The `history` attribute under **system → aaa → authentication → password-attributes** is configured to a non-zero value, and the **`copy default running-config`** command is subsequently executed. **Workaround:** Remove the `history` attribute before executing the **`copy default running-config`** command.
TOS-35600	**Symptom:** Tunnel traffic will be dropped as tunnel underlay nexthop not created successfully in hardware. **Condition:** The port-channel (PO) interface is removed while its member interfaces are still configured with the `channel-group` command. **Workaround:** Remove the `channel-group` configuration from all member interfaces before deleting the port-channel (PO) interface.
TOS-33819	**Symptom:** Control packets destined for the SAG IP might not be processed during CPU overload conditions, resulting in protocol flaps. **Condition:** This issue is specific to SAG IP configurations with MLAG. **Workaround:** Perform a shut/no-shut operation on the affected L3 or VE interface.
TOS-35552	**Symptom:** Informs are sent using the previous SNMPv3 user credentials instead of updated credentials. **Condition:** This issue occurs when an SNMPv3 user and a corresponding SNMPv3 inform host are configured, and the SNMPv3 user credentials or attributes (such as authentication method, privacy method, authentication password, or privacy password) are updated. Subsequent inform events are then sent using the previous credentials instead of the updated credentials. **Workaround:** Restart the SNMP server (disable and then re-enable it) on the configured VRF.

Issue ID	Description
TOS-33034	**Symptom:** Few Dynamic MAC entries not flushed after all front panel ports are brought down. **Condition:** Occurs only when continuous traffic is running during the trigger event. **Workaround:** Stop the traffic before shutting down all front panel ports. **Recovery:** Clear the dynamic MAC table associated with the affected bridge domain.
TOS-33031	**Symptom:** A traffic drop might be observed when Resilient Hashing is applied on the ECMP Nexthop, and MLAG PO member interface goes down due to I2C Error condition. **Condition:** Occurs only on resilient hashed traffic flows that are redirected using the redirection rule on TD3 device. **Workaround:** Disable the Resilient Hashing on the ECMP next-hop.

Acronyms and Abbreviations

Term	Definition
AAA	Authentication Authorization and Accounting
ACL	Access Control List
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BIOS	Basic Input/Output System
CLI	Command Line Interface
CNIS	Cloud Native Infrastructure as a Service
CoS	Classification of Service
DCBX	Data Center Bridging Capability Exchange
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
ECMP	Equal-Cost Multi-Path
ECN	Explicit Congestion Notification
ETS	Enhanced Transmission Selection
FEC	Forward Error Correction
GRUB	GRand Unified Bootloader

Term	Definition
gNMI	gRPC Network Management Interface
HTTP	HyperText Transfer Protocol
IAH	Integrated Application Hosting
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
MIB	Management Information Base
MLAG	Multi-Chassis LAG
mTLS	Mutual Transport Layer Security
ND	Neighbor Discovery
NTP	Network Time Protocol
ONIE	Open Network Install Environment
OOB	Out of Band
OOBM	Out-of-Band Management
PFC	Per-priority Flow Control
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RH	Resilient Hashing
RME	Redundant Management Ethernet
RSPAN	Remote Switch Port Analyzer
SCP	Secure Copy Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
TC	Traffic Class
TD4	Broadcom Trident 4–based platforms
TPVM	Third-Party Virtual Machine
TLS	Transport Layer Security
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
ZTP	Zero Touch Provisioning



Help and Support

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

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

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

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions 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 RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.

3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.