Extreme OS ONE Switching and Routing v22.2.2.0 Release Notes

New Features, Bug Fixes, and Known Limitations

9039559-00 Rev AA
April 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/

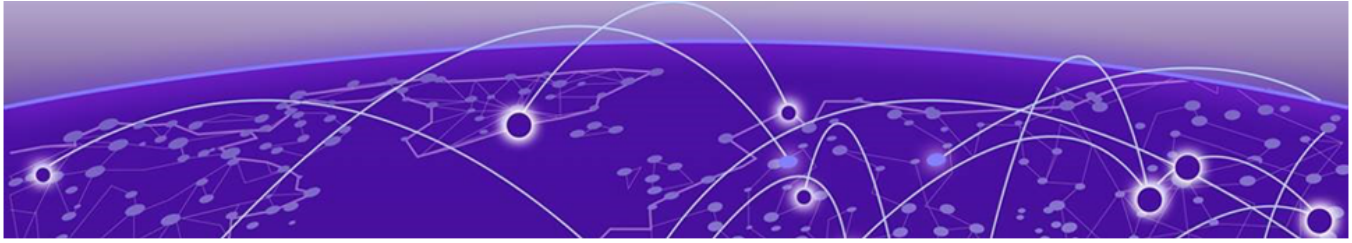
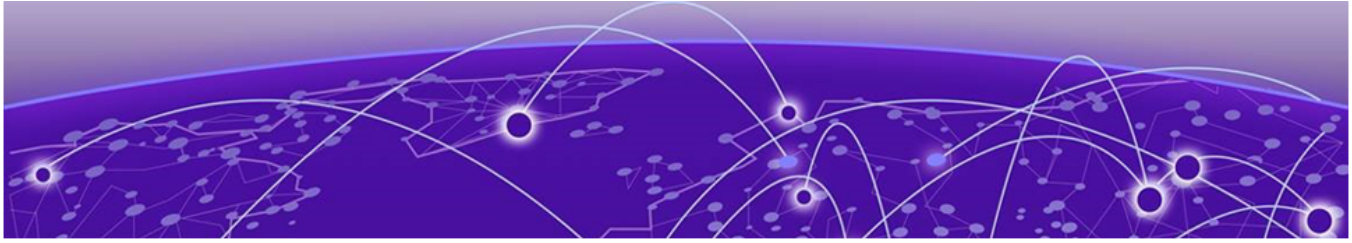
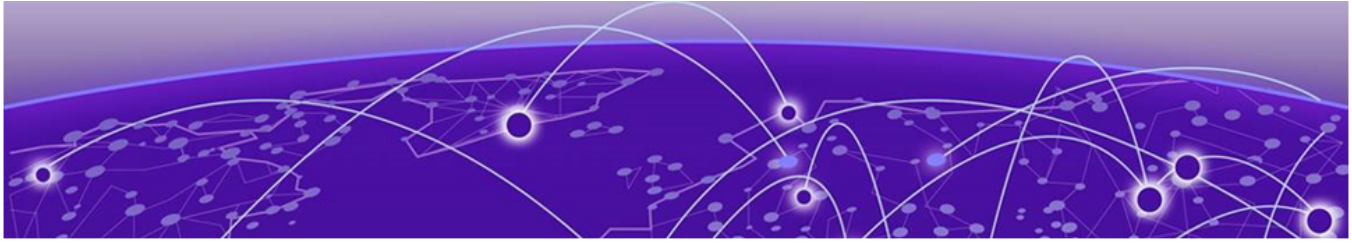


Table of Contents



Abstract

The Extreme OS ONE SR v22.2.2.0 Release Notes provides a comprehensive overview of essential updates, technical improvements, and known limitations for advanced IP fabric and data center environments. It highlights enhancements in configuration recovery, security, management interfaces, and network resiliency, with expanded protocol and hardware support. 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.

New in this Release

Extreme OS ONE Switching and Routing 22.2.2.0 introduces the following features and enhancements.

Table 1: New features in Extreme OS ONE Switching and Routing 22.2.2.0

Feature	Description
VRF and Source-Interface Support	Adds Virtual Routing and Forwarding (VRF) and source-interface configuration support for Manageability applications, including Rsyslog and Reliable Event Logging Protocol (RELP). This support is required for the majority of management application deployments and enables proper routing of management traffic across VRFs.
ICMP Rate Limiting	Rate limits Internet Control Message Protocol (ICMP) traffic on the Management port — either the out-of-band (OOB) port or the in-band Redundant Management Ethernet (RME) port — to prevent Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks. This feature provides the following capabilities: • Enable or disable the feature through the API or CLI. The feature is enabled by default. • Configure rate limit values for ICMP traffic in packets per second (pps) within a supported range. • Log statistics for ICMP traffic drops caused by rate limit breaches.
Limit maximum connections per IP address	Limits the number of HTTP connections per IP address on the Manageability plane using the connection tracking (ConnTrack) module in IP tables. This prevents connection exhaustion that can cause northbound applications, such as XCO, to experience connection failures when HTTP client connections are not closed properly.
Network Element Authentication Support	Introduces mutual authentication (mTLS) for machine-to-machine communication with external authentication servers. This feature provides the following capabilities: • Certificate import support for servers and clients that use mutual authentication. • ◦ Supported Server: gNMI ◦ Supported Clients: LDAPS, Syslog, RADIUS, and HTTPS for system firmware update
Strong password entropy	Extends password entropy enforcement with the following controls: • **History**: Checks new passwords against a configurable number of previously used passwords (range: 1 through 10, default: disabled) to prevent password reuse. • **Max-Sequence**: Rejects passwords that contain a configurable minimum number of consecutive sequential characters in the forward or reverse direction, for example, abc or cba (range: 1 through 10, default: disabled). • **Max-Repeat**: Rejects passwords that contain a configurable minimum number of repeated characters, for example, aaa or 222 (range: 1 through 10, default: disabled).

Table 1: New features in Extreme OS ONE Switching and Routing 22.2.2.0 (continued)

Feature	Description
RAS	Displays a Reliability, Availability, and Serviceability (RAS) warning message as a Message of the Day (MOTD) when a user starts a privileged shell through the start-shell command. The message alerts users that the shell is intended for additional troubleshooting with the assistance of Extreme GTAC, and that unsupported use may leave the system unstable or void official support.
ACL Based Mirroring	Enables traffic mirroring based on Access Control List (ACL) match criteria. This feature allows selective packet capture and monitoring of specific traffic flows that match defined ACL rules, supporting network visibility and troubleshooting in production environments.
QoS - Drop Precedence Support	Adds Drop Precedence support with configurable values (0 through 2) for the following Quality of Service (QoS) scenarios: • Default QoS maps • User-configured QoS maps • Layer 2 (L2) traffic using Priority Code Point (PCP) markings and Layer 3 (L3) traffic using Differentiated Services Code Point (DSCP) markings Supported on TD3, TD4, and J2-based platforms
ACL-based QoS marking	Supports Quality of Service (QoS) marking of ingress traffic based on ACL match criteria. In untrusted QoS deployments, such as Cloud Native Infrastructure as a Service (CNIS) environments, traffic arriving on access ports from server or compute nodes can be filtered and marked using the following match criteria: • MAC • VLAN • IP ACLs for IPv4 and IPv6 Traffic can be marked with a Drop Precedence, Traffic Class (TC) or DSCP, or PCP values.
Resilient Hashing	Implements Resilient Hashing (RH) for Equal-Cost Multi-Path (ECMP) load balancing on TD3, J2-based platforms to minimize flow disruption when ECMP group membership changes. This feature provides the following capabilities: • Per-VRF enable or disable configuration • Support for BGP and static routes for both IPv4 and IPv6 • VRF-level control of ECMP path count, with support for up to 128-way ECMP • Flow set table monitoring with RASlog, GNMI, and SNMP notification alerts when the table limit is exceeded

Table 1: New features in Extreme OS ONE Switching and Routing 22.2.2.0 (continued)

Feature	Description
MLAG Resiliency Enhancement	Extends Multi-Chassis LAG (MLAG) resiliency to handle I2C error conditions, which can trigger split-brain scenarios due to hardware communication failures. This enhancement builds on existing resiliency work that addressed HSLAgt crashes and kernel panics caused by Out-of-Memory (OOM) conditions.
QoS Scheduling	The Egress Port Scheduler determines which packets transmit first based on the scheduling mechanism applied on the egress queues to provide precise control over traffic prioritization.

Hardware Support

Extreme OS ONE Switching and Routing 22.2.1.0 and later releases support Extreme 8520, Extreme 8720, Extreme 8730, and Extreme 8820 hardware platforms.

Upgrade and Downgrade Considerations

This section provides information on supported upgrade paths, migration considerations, and compatible software versions.

Supported upgrade paths for Extreme OS ONE Switching and Routing 22.2.2.0 are:

- Release 22.2.0.0 to 22.2.1.0
- Release 22.2.1.0 to 22.2.2.0

Note

- Always back up configuration and enable maintenance mode before upgrading.
- Automatic rollback triggers if microservices fail to come up post-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 platform-specific SLX-OS image. Do not interchange images across platforms.

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

Supported FEC Modes

Table 2: 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 2: 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 3: 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
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 features 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 features are not supported: • Origination of Router Solicitation • IPV4 Router advertisement
List Key Values	Special characters such as @, #, $, *, [,] are not supported in list key values. Key-values containing these special characters are not accepted.
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 features are not supported: • Confed-AS • IPv6 Link-local Peering • Selection-Knobs (Default-Metric, Enforce-First-AS) • Route-Aggregation, Large Communities

Feature	Limitations and Restrictions
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.
GARP	Trailer bits are stripped off from GARP packets if suppress-arp and arp-snooping are enabled.
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. • Time zone changes will be effective after reload for timestamp change for the new trace logs of microservices. However, system clock is updated immediately. • 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. • The default rsyslog server does not function if any configured server is unreachable or has certificate-related issues. **Workaround:** ◦ Delete invalid configuration • Services such as LDAP, RADIUS, or rsyslog are disabled when the global minimum TLS version is set to 1.3 and the service-level minimum TLS version is set to 1.2. **Workaround:** ◦ Disable or enable logging remote server configuration.
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

Open Issues

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

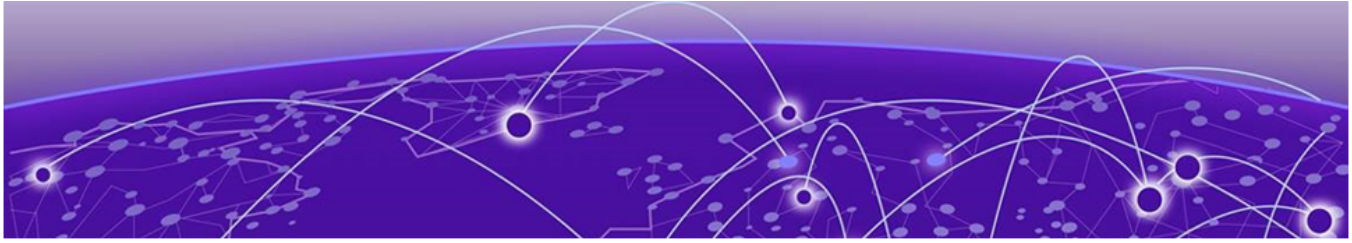
Issue ID	Description
TOS-33031	**Symptom:** A traffic drop might be observed when Resilient Hashing is applied on the ECMP Nexthop, and MLAG PO member interface goes down due to I2C Error condition. **Condition:** Occurs only on resilient hashed traffic flows that are redirected using the redirection rule on TD3 device. **Workaround** Disable the Resilent Hashing on the ECMP next-hop.
TOS-32522	**Symptom:** When the ISL underlay port-channel is de-configured and configured, and then shut/ no shut multiple times, the underlay reachability fails and the MLAG session goes down. **Condition:** Occurs when the ISL underlay port-channel is de-configured and configured, and then shut/ no shut multiple times. **Workaround:** Perform a shut/no shut of the MLAG underlay Port-Channel interface.

Acronyms and Abbreviations

Term	Definition
AAA	Authentication Authorization and Accounting
ACL	Access Control List
ARP	Address Resolution Protocol
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BIOS	Basic Input/Output System
BMC	Baseboard Management Controller
CLI	Command Line Interface
CNIS	Cloud Native Infrastructure as a Service
CRL	Certificate Revocation List
CoS	Classification of Service
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System

Term	Definition
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
DSCP	Differentiated Services Code Point
ECMP	Equal-Cost Multi-Path
EVPN	Ethernet Virtual Private Network
FEC	Forward Error Correction
GARP	Gratuitous Address Resolution Protocol
GRUB	GRand Unified Bootloader
gNMI	gRPC Network Management Interface
HTTP	HyperText Transfer Protocol
HWROT	Hardware Root of Trust
IAH	Integrated Application Hosting
ICMP	Internet Control Message Protocol
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LED	Light Emitting Diode
LFS	Link Fault Signaling
LLDP	Link Layer Discovery Protocol
MIB	Management Information Base
MLAG	Multi-Chassis LAG
MOTD	Message of the Day
mTLS	Mutual Transport Layer Security
ND	Neighbor Discovery
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
ONIE	Open Network Install Environment
OOB	Out of Band
OOBM	Out-of-Band Management
OOM	Out of Memory
PCP	Priority Code Point
PIC	Prefix Independent Convergence
PSU	Power Supply Unit
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAS	Reliability, Availability, and Serviceability

Term	Definition
RELP	Reliable Event Logging Protocol
RH	Resilient Hashing
RME	Redundant Management Ethernet
SCP	Secure Copy Protocol
SFTP	Secure File Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS	Terminal Access Controller Access Control System
TC	Traffic Class
TD4	Broadcom Trident 4–based platforms
TPVM	Third-Party Virtual Machine
TLS	Transport Layer Security
USB	Universal Serial Bus
VxLAN	Virtual Extensible LAN
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.