# 9920 Software v21.2.2.2 Release Notes

## New Features, Bug Fixes, and Known Limitations

9039087-02 Rev AA
September 2025

## 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

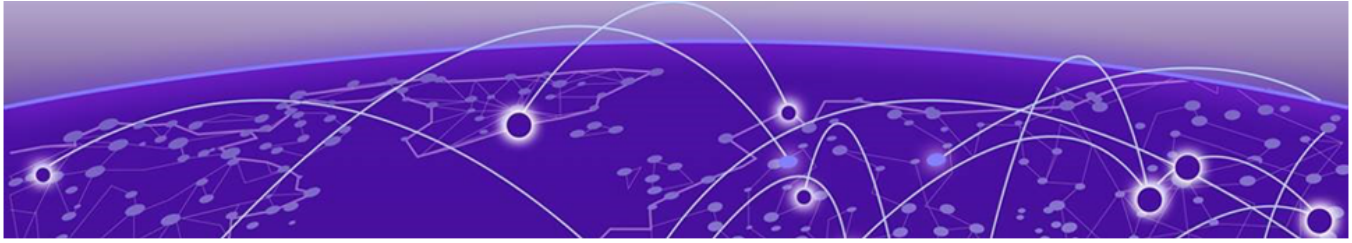
Extreme Networks® and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

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.

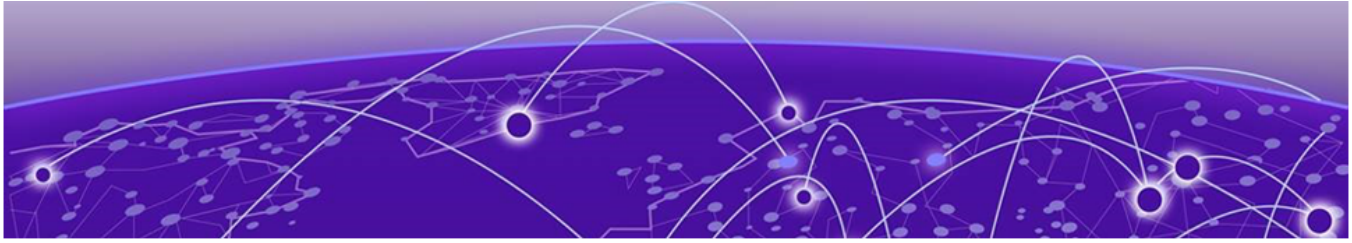
For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

## 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/

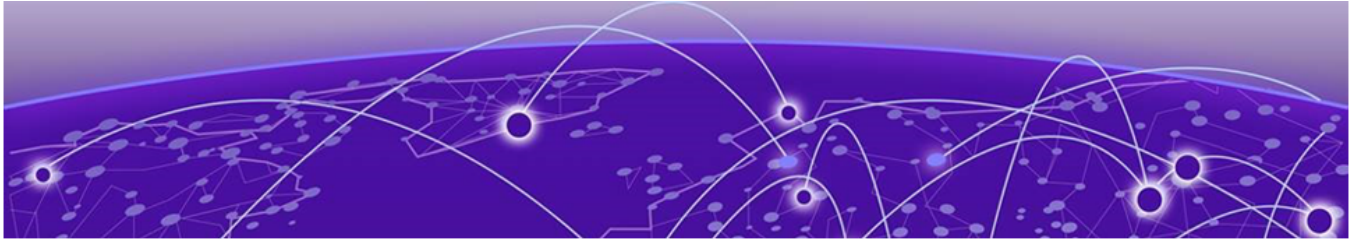


# Table of Contents



# Abstract

The release notes for Extreme Networks 9920 Software version 21.2.2.2 provides a comprehensive overview of defect fixes and operational updates for the 9920 network packet broker platform.



# Release Notes



The NPB software runs the NPB operating system and provides network packet broker functions.

## New in this Release

Version 21.2.2.2 of the Extreme 9920 software with the NPB application offers defect fixes.

For more information, see:

- *Extreme 9920 Software Configuration Guide, 21.2.2.0*
- *Addressed Issues*

## Commands

There are no new or modified commands in this release.

## Known Limitations

**Two cold start traps**

Occasionally, the trap receiver gets two SNMP cold start traps from the 9920 device, even though the 9920 device is reloaded only once.

**GRE tunnel encapsulation does not support MPLS packets**

When an MPLS packet is subjected to GRE encapsulation, the protocol ID in the GRE header is set to 0.

**Listener policy byte count is incorrect when truncation is enabled**

On Extreme 9920 devices, the byte count for truncated packets is the actual byte count seen by the egress ACL before truncation.

**GRE version-1 packets are not filtered with the 'network-id-type:NETWORK_ID_TYPE_GRE' rule**

The rule filters the GRE version-0 packets.

### Scale limitation of 2000 ingress groups is not achieved in a certain configuration

When both transport tunnels and ingress groups are configured, some of the non-transport ingress groups are not stored in the hardware table. Ingress groups that are not in the hardware table are not counted toward the scale limit.

### Filtering by the authentication header is not supported

You cannot configure ACLs for IP ESP (Encapsulating Security Payload) that filter for the authentication header.

### MAC ACL counters are incremented when traffic matches IPv4, IPv6, and MAC ACLs

If multiple matches, in different ACL types, are on permit rules, only the match in the highest-preference type is implemented. Lower-preference matches are ignored. The preference order is Layer 3 > Layer 2. The counters are incremented for all the matching ACLs because they indicate that a match is found.

### Matching packets based on IGMP group address for both IPv4 and IPv6 is not supported

You cannot configure ACL rules to match packets based on the IGMP group address for both IPv4 and IPv6.

### Transport tunnel termination is supported only for ERSPAN Type II

Transport tunnel termination considers only ERSPAN Type II headers for termination and does not consider any specific SPAN-ID to terminate and further classify the flows.

### Device links are not operational for 100G LR4 optic with FEC mode set to auto

To enable the links between Extreme 9920, SLX 9140, and SLX 9240 devices to be operational with 100GBASE-LR4 optics, configure one of the following

- Disable FEC on Extreme 9920 devices.
- Enable RS-FEC on SLX devices when the peer side FEC configuration is set to auto.

### IPv6 packets with extension headers cannot be matched, filtered, or forwarded

On Extreme 9920 devices, IPv6 packets with extension headers cannot be matched, filtered, or forwarded on standard TCP or UDP protocols.

### Multiple SNMP linkUp or linkDown traps are generated during SNMP upgrade

This situation occurs when you upgrade the SNMP service with the **`system service update`** command. These traps do not impact functionality and there is nothing you need to do.

### Overwriting of mirror sessions and packet capture due to ASIC behavior

A mirror session programmed at one stage will be overwritten by a subsequent stage if the packet matches an entry in the table. Onboard PCAP capture of ACL will overwrite packet capture of ingress interface and tunnel based captures.

### 100G-DR, FR optical transmission

The 100G-DR, FR uses a single laser and operates with PAM4 modulation at 53.125 Gb on the optical side. Since PAM4 encodes 2 bits per symbol, this results in a 100G transmission rate. Channels 2, 3, and 4 should remain inactive, so the tx, rx,

and txbias data will show proper values for channel 1, and either infinity or 0.00 for channels 2, 3, and 4.

## Addressed Issues

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

**Table 1: Defects closed with code changes**

| Issue ID | Description |
|---|---|
| NPB-6302 | When configuring ACL rules, the help text incorrectly displays the priority range as 1–65535 instead of the correct range of 1– 4095. |
| NPB-6326 | After ingress ACL processing, there is no egress traffic on most of the interfaces.<br>When one of the ports is in the Present state, the forwarding services (MS) are not initialized. |
| NPB-6338 | QSFP temperature failure results in slot2/LC2 reset by BMC. |
| NPB-6343 | Slot 5 is in faulty state after firmware and BMC upgrade. |
| NPB-6344 | If one of the slot is in the Present/Faulty state, egress rules are not programmed. |
| NPB-6345 | Slot 6 is in a faulty state after firmware and BMC upgrade. |
| NPB-6346 | Slot 7 is in a faulty state after firmware and BMC upgrade. |
| NPB-6347 | No egress traffic after firmware upgrade. |
| NPB-6349 | Port channels associated with the faulty card fail to come up after firmware and BMC upgrade. |

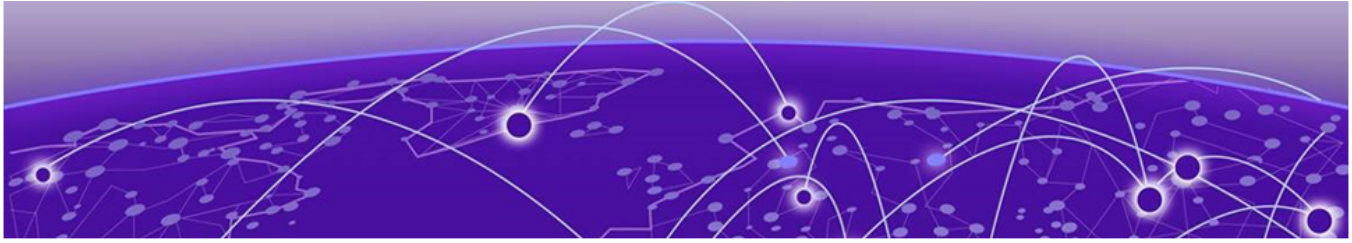
**Table 2: Defects closed without code changes**

| Issue ID | Description |
|---|---|
| NPB-6315 | All line cards restart randomly when there is voltage fluctuation.<br>Workaround:<br>Use the system slot command to bring up the line cards if they are in Present state. |
| NPB-6341 | Ingress Policy Match counters are not matching with the egress output counters.<br>The policy match includes both IPv4 and MAC ACL rules. If a packet matches both rules, it will be counted twice at the policy match stage. However, at the egress stage, the packet is counted only once. This explains the difference in counts. The system is functioning as designed. |
| NPB-6350 | When configured to remove the MPLS header, the system is also removing the IP header along with it.<br>The MPLS input traffic must include an inner Ethernet header immediately after the outer MPLS header. After correcting the input traffic stream, MPLS header removal works as expected. |

# Open Issues

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

| Issue ID | Description |
|---|---|
| NPB-5182 | Entity MIB item entPhysicalVendorType does not return any Vendor type OIDs, instead it just returns {0 0} when SNMP walk is performed. |
| NPB-5188 | "Link Fault Status" field in "Show interface ethernet" might show incorrect fault status. |
| NPB-5724 | LACP port-channel remains down after replaying the configuration with LACP rate as 'fast' in the member interfaces.<br>**Workaround:**<br>Reboot the system with the configuration applied, or set the LACP rate to normal. Once the port-channel is up, change it to lacp rate fast on member ports. |
| NPB-6285 | 100G-DR optics, tx, rx, and tx bias for 3 channels are showing wrong values. |
| NPB-6313 | For single lane optics, the show cli command displays the media information for all the lanes.<br>**Workaround:**<br>Consider data from the first lane only for single-lane optical modules. |
| NPB-6348 | QSFP detection fails after BMC upgrade.<br>**Workaround:**<br>Remove/insert affected QSFP. |



# 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.