Extreme 9920 Software v21.2.1.0 Release Notes

New Features, Commands, and Known Issues

9038141-00 Rev AB
July 2024

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/

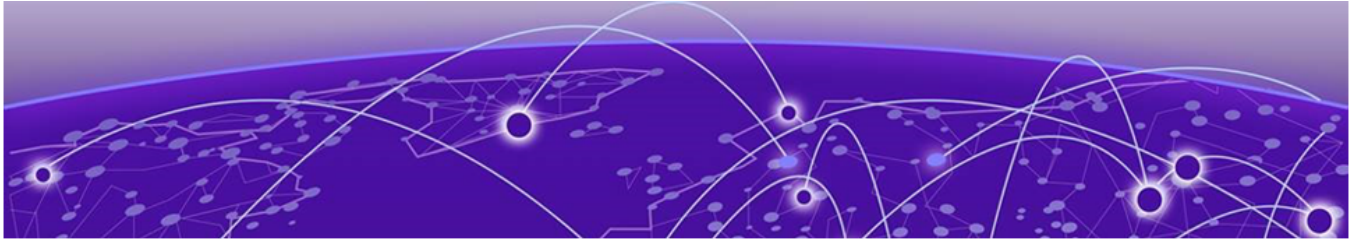
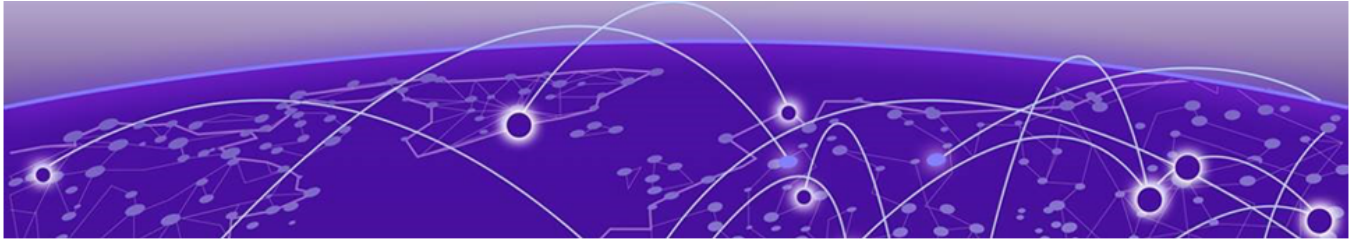


Table of Contents



Release Notes

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

Release Information

Release Date: July 2024

The release notes for Extreme Networks' Extreme 9920 software version 21.2.1.0 provide an overview of new features, command updates, known limitations, defect fixes, and open defects. Key updates include 400G line card support and the introduction of the "linecard" command. Known limitations cover issues such as GRE tunnel encapsulation and MAC ACL counters. Closed defects address problems like incorrect power supply recognition and port-channel traffic egress. Open defects include issues with SNMP walks and LACP port-channels. Support options and subscription details for product announcements are also provided.

New in this Release

Version 21.2.1.0 of the Extreme 9920 software with the NPB application offers 400G Line Card Support and offers defect fixes .

Table 1: Feature Updates

Feature	Description
400G Line Card Support	Extreme 9920 software supports 400G speed on the line card. For more information, refer to the *Extreme 9920 Software Configuration Guide, 21.2.1.0*.

For more information, refer to Defects Closed With Code Changes on page 6.

Commands

There is a new command introduced in this release.

New command

- linecard

For more information, refer to the *Extreme 9920 Software Command Reference, 21.2.1.0*.

Known Limitations

Note the following caveats that were disclosed in the NPB 21.1.2.0 release that is applicable for this release of the software as well.

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.

Defects Closed With Code Changes

The following defect was closed with code changes in this release of the software.

Parent Defect ID:	NPB-6196	**Issue ID:**	NPB-6196
Severity:	S3 - Moderate		
Product:	NPB	**Reported in Release:**	NPB 21.1.2.6
Symptom:	The traffic that was received at ingress was not egressing out of one of the port-channels.		
Condition:	The PRE.LAG table entry was not updated correctly in the hardware table for the port-channel where traffic was not egressing out.		

Parent Defect ID:	NPB-6232	**Issue ID:**	NPB-6232
Severity:	S3 - Moderate		
Product:	NPB	**Reported in Release:**	NPB 21.1.2.7
Symptom:	DC PSUs with part numbers other than 801116-00-01 and DPS-1600AB-22 D were recognized as AC power supplies. Thus, DC power supply 801116-00-AA displayed as an AC power supply.		
Condition:	DC PSUs with part numbers other than 801116-00-01 and DPS-1600AB-22 D were displayed as AC PSUs.		

Defects Closed Without Code Changes

The following defects were closed without code changes in the 21.2.1.0 release of the software.

Parent Defect ID:	NPB-6216	**Issue ID:**	NPB-6216
Reason Code:	Third Party Issue	**Severity:**	S2 - Major
Product:	NPB	**Reported in Release:**	NPB 21.1.2.5
Symptom:	On expiry of K3s client and server certificates which has a validity of one year, the microservices goes down.		
Workaround:	The certificates will get automatically renewed on performing a reboot of the device in the 2 months window before certificate expires or after the certificates expire.		

Open Defects

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

Parent Defect ID:	NPB-5182	**Issue ID:**	NPB-5182
Severity:	S2 - Major		
Product:	NPB	**Reported in Release:**	NPB 21.1.1.0
Symptom:	Entity MIB item entPhysicalVendorType does not return any Vendor type OIDs instead it just return {0 0} when SNMP walk is performed		
Condition:	The symptom always happens during SNMP walk of entPhysicalVendorType in the entity MIB.		
Workaround:	No workaround		
Recovery:	No recovery available		

Parent Defect ID:	NPB-5188	**Issue ID:**	NPB-5188
Severity:	S3 - Moderate		
Product:	NPB	**Reported in Release:**	NPB 21.1.1.0
Symptom:	"Link Fault Status" field in "Show interface Ethernet" might show incorrect fault status.		
Condition:	"no shutdown" on the Ethernet interface.		
Recovery:	No functional impact.		

Parent Defect ID:	NPB-5724	**Issue ID:**	NPB-5724
Severity:	S3 - Moderate		
Product:	NPB	**Reported in Release:**	NPB 21.1.2.0
Symptom:	LACP port-channel remains down after replaying the configuration with lacp rate as 'fast' in the member interfaces.		

Condition:	The issue is seen when the lacp configurations are replayed with the node in default-configs only when "lacp rate fast" is configured on member ports.
Workaround:	If you reboot the system with config, it will work properly or change the "lacp rate normal" and after the port-channel comes up again change it to "lacp rate fast" on member ports.
Recovery:	Disable and enable lacp in the global config mode. ('no protocol lacp' and 'protocol lacp')

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.