CGS Tower Networks Ltd

# CGS User Guide for NPB I, NPB Ie, NPB Ie8, NPB II, NPB IIe, NPB III, and NPB IV

Release 5.1.1, June 2023

# Revision History

| Revision | Date | Description |
|---|---|---|
| 5.1.1 | June 6, 2023 | Added ability to change HTTP/HTTPS port numbers, see Working with the WebUI on p.51 |
| 5.1 | May 15, 2023 | Increased maximal number of filters in NPB IV to 12K, see Filter Resources on p.115 |
| 5.0 | February 10, 2023 | Added NPB IV support<br>Changed filter management<br>Added inline support in NPB Ie<br>Added support for modifying ARP and IPX heartbeats, see Heartbeat Profiles on p.150<br>Added LB operation mode in NPB III<br>Added support for stacking, see Stacking on p.181<br>Added NETCONF appendix, see Appendix 4 – NETCONF on p.227 |
| 4.7 | July 21, 2022 | Added inline graphical diagram, see Diagrams on p.177<br>Added inline load balancing failover actions and failover threshold, see Configuring Load Balancing Groups on p.165<br>Added privileges mapping for TACACS+, see Remote Users and Servers on p.190<br>Changed SNMP v2 traps behavior to support non default communities, see SNMP Trap Server on p.206 |
| 4.6 | March 28, 2022 | Added support for inline load balance groups in inline chain, see Inline Tool Chains on p.153<br>Added WebUI support for inline tool chains, see Inline Tool Chains on p.153<br>Enhanced SW upgrade syntax, see Upgrading to a New Image File on p.56 |
| 4.5 | December 1, 2021 | Added support for inline tool chains and inline tool load balancing groups, see Inline Tool Chains on p.153 and Inline Tool Load Balancing Groups on p.155<br>Added DNS resolving for external server hostnames, see Configuring DNS Servers on p.46<br>Added Ignore Bad CRC behavior, see Ignoring Bad CRC on p.81<br>Added multiple UDF window and GTP tunnel support in NPB Ie, see Working with UDF Windows on p.130<br>Added last login attempt information, see Active Sessions on p.194<br>Added Filter Duplication action, see Managing Filters on p.107<br>Added filter tags, see Defining Filters on p.105<br>Added Block ICMP request, see Blocking Incoming ICMP Requests on p.53<br>Added option to block dormant user logins, see Dormant Users on p.189 |

| Revision | Date | Description |
|---|---|---|
| 4.4 | July 1, 2021 | Added Inline support, see Heartbeat Profiles on p.150 and Inline Tools on p.148<br>Added Bidirectional filters support, see Defining Filters on p.105<br>Added MIB download support, see MIB Support on p.208<br>Added SSL certificate upload, see SSL Certificates on p.52<br>Added more speeds and breakout options to NPB Ie, see Port Configuration and Actions on p.75<br>Added more copper support to NPB Ie8, see Port Configuration and Actions on p.75<br>Added slicing support to NPB Ie, see Packet Slicing on p.145 |
| 4.2 | March 14, 2021 | Added IP interface support, see IP Interfaces on p.155<br>Added port line-code in NPB III, see Port Configuration on p.77<br>Added support for l2-l4-ipv6 mode in NPB I, see Filter Modes on p.112<br>Added copper support in NPB Ie<br>Added IPv6 support in UDF modes in NPB II and NPB III, see Filter Modes on p.112 |
| 4.0 | December 24, 2020 | Increased NPB Ie filters, see Filter Resources on p.115<br>Added MPLS parsing mode in NPB Ie, see MPLS Parsing Mode on p.95<br>Added GTP hash algorithms based on source and destination IPs and L4 ports, see Configuring Load Balancing Groups on p.165<br>Added double-tag (Q-in-Q) support, see Managing Tagged Traffic on p.90<br>Added 16 UDF windows in NPB II, see Working with UDF Windows on p.130 |
| | | Added support for NPB III<br>Added CPU, memory and disk status monitoring, see CPU, Memory, and Disk Status on p.61<br>Changed transceivers display commands and added transceiver read/write options, see Transceivers on p.61<br>Added Pre-emphasis support, see Pre-emphasis (NPB III) on p.83<br>Added IP list exact-match, see Using HW Exact Match Memory for IP Lists on p.127<br>Added gtp-ipv4-ipv6-hash tunnel, see Working with Tunnels on p.138<br>Added timestamp in NPB IIe and Ie8: For port configuration, see Timestamping (NPB Ie8 and NPB IIe) on p.88. For filter actions, see Timestamping on p.144.<br>Added 'delete by' filter actions, see Managing Filters on p.107<br>Added LB random algorithm in NPB III, see Configuring Load Balancing Groups on p.165<br>Added Audit log, see Audit Logs on p.70 |
| 3.5.2 | July 8, 2020 | Added GTP/L2TP high IPv6 address tunnel |

| Revision | Date | Description |
|---|---|---|
| 3.5.1 | June 24, 2020 | Added filter move actions, see Managing Filters on p.107<br>Added Cl108 FEC for 25G speed in NPB Ie8 and NPB IIe, see Table 14: Port Attributes<br>Added High Availability alarms, see Trap Support on p.209 |
| 3.5 | June 4, 2020 | Add Pseudo Random Bit Sequence (PRBS) support for ports, see Pseudo Random Binary Sequence (PRBS) on p.85<br>Changed copy action to be priority based, see Filter List on p.103<br>Added filter groups, see Filter Groups on p.103<br>Added GRE L2 support (NPB Ie8 and NPB IIe), see GRE Tunneling on p.162<br>Added High Availability monitored ports, see Monitored Ports on p.196<br>Added Slicing as filter operation, see Packet Slicing on p.145 |
| 3.1.1 | April 1, 2020 | Added Link Propagation support, see Link Propagation on p.84<br>Added Tx Laser Off support, see Port Configuration on p.77 |
| 3.1 | March 10, 2020 | Added NPB Ie8 support<br>Added support for multiple UDF patterns in filters, see Setting UDF Windows as Filter Classifiers on p.136<br>Added Dynamic Load Balancing support (NPB IIe), see Dynamic Load Balancing (NPB Ie8 and NPB IIe only) on p.170<br>Added XOR hash function, see Hash Functions on p.165<br>Added Section Load Balance Operation Mode on p.170 |
| 3.0 | August 15, 2019 | Added NPB Ie support<br>Added Section MPLS Stripping (NPB Ie, Ie8 and IIe only) on p.95<br>Added PPPoE tunnel support, see Working with Tunnels on p.138 |
| 2.6 | June 30, 2019 | Added on-site installation and activation, see Installing the NPB Software on p.22 and Activating the Device on p.23<br>Added Clear All Logs command, see Local Logs and Debug Reports on p.71<br>Added support for FEC Clause 91 algorithm, see Port Configuration - General on p.77<br>Added GRE and GTP IPv6 support for NPB IIe, see Working with Tunnels on p.138 |
| 2.5 | April 28, 2019 | Added NPB IIe UDF support<br>Added NPB IIe 50G speed support |
| 2.1 | March 2, 2019 | Added NPB IIe support<br>Added Section MAC Replacement on p.144<br>Added Section Added Section MPLS Stripping for NPB IIe<br>Added MPLS tunnel support in Section Working with Tunnels on p.138 |

| Revision | Date | Description |
|---|---|---|
| 2.0 | December 31, 2018 | Added Section High Availability on p.195<br>Added classifier negation support, see Using Negation on p.104<br>Added Section Port Groups on p.81<br>Added Section Port Groups on p.81<br>Added configurable absolute timeout, see Session Timeouts on p.42<br>Added Section Working with IP Lists on p.125<br>Added load balancing according to GTP inner IP<br>Added 2.5G speed support in NPB I |
| 1.3.6 | November 1, 2018 | Added 1G speed support in NPB II |
| 1.3.4 | October 18, 2018 | Added Section Changing SSH Settings on p.38<br>Added load balancing according to source or destination IP address<br>Added IF-MIB and SNMP-MIB-2 support |
| 1.3.1 | April 1, 2018 | Added filter copy action<br>Added filter session classifiers<br>Added Section Logical Operation between Classifiers (OR and AND) on p.121<br>Added Section Diagrams<br>Added Section Active Sessions |
| 1.2.3 | November 6, 2017 | Added copper auto negotiation and 10M/100M support |
| 1.2.2 | September 28, 2017 | Added Section Virtual Load Balance<br>Added inner IP classifiers in Section Working with Tunnels on p.138 |
| 1.2.1 | July 20, 2017 | Added missing WebUI sections |
| 1.2.1 | June 20, 2017 | Added the following sections:<br>Password Management<br>Changing the Login Banner<br>HTTPS/TLS Ciphers |
| 1.2 | May 2, 2017 | Added R1.2 content |
| 1.1.2.1 | February 27, 2017 | Added WebUI documentation |
| 1.1.2 | January 30, 2017 | Added Section Troubleshooting HW Failures<br>Added Section Alarm Operations<br>Updated Section Working with UDF Windows<br>Updated VLAN tag range in Section Ingress Operations<br>Updated Section Port Statistics<br>Updated and added contents to Appendix 3 – Port Counters |
| 1.1 | December 28, 2016 | Updated Section Working with NETCONF<br>Added Section Working with the WebUI<br>Added Section Location LED |

| Revision | Date | Description |
|---|---|---|
| 1.0 | December 2016 | Initial release |

# Disclaimer

PLEASE READ THESE LEGAL NOTICES CAREFULLY.

By using any of CGS Tower Networks Ltd. (the "Company") NPB I, NPB Ie, NPB Ie8, NPB II, NPB IIe, NPB III, NPB IV products you agree to the terms and conditions of usage set forth by CGS Tower Networks Ltd.

No licenses, express or implied, are granted with respect to any of the technology described in this manual. The Company retains all intellectual property rights associated with the technology described in this manual. This manual is intended to assist with installation of NPB I, NPB Ie, NPB Ie8, NPB II, NPB IIe, NPB III, NPB IV into your network.

## Trademarks

CGS Tower Networks Ltd and NPB I, NPB Ie, NPB Ie8, NPB II, NPB IIe, NPB III, NPB IV are trademarks of CGS Tower Networks Ltd. Additional company and product names may be trademarks or registered trademarks of the individual companies. Use of all trademarks requires the permission of the trademark owner.

## Additional Information

CGS Tower Networks Ltd reserves the right to make changes in specifications and other information contained in this document without prior notice. Effort have been made to ensure that the information in this document is accurate.

## Limitations on Warranty and Liability

CGS Tower Networks Ltd offers a limited warranty for all its products. IN NO EVENT, SHALL CGS Tower Networks Ltd. BE LIABLE FOR ANY DAMAGES INCURRED BY THE USE OF THE PRODUCTS (INCLUDING BOTH HARDWARE AND SOFTWARE) DESCRIBED IN THIS MANUAL, OR BY ANY DEFECT OR INACCURACY IN THIS MANUAL ITSELF. THIS INCLUDES BUT IS NOT LIMITED TO LOST PROFITS, LOST SAVINGS, AND ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT, even if CGS Tower Networks Ltd has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

CGS Tower Networks Ltd. warrants this device to be in good working order for a period of ONE YEAR from the date of purchase from CGS Tower Networks Ltd or an authorized CGS Tower Networks Ltd reseller.

Should the unit fail anytime during the said ONE YEAR period, CGS Tower Networks Ltd will, at its discretion, repair or replace the product or refund amounts that you paid for the product. This warranty is limited to defects in workmanship and materials and does not cover damage from accident, disaster, misuse, abuse or unauthorized modifications.

In order to make a claim under the warranty, or if you have a problem and require service, please call the number listed at the end of this section and speak with our technical service personnel. They may provide you with an RMA number, which must accompany any returned product. Return the product in its original shipping container (or equivalent) insured and with proof of purchase. The Company shall not be obligated to honor warranty claims that do not follow the procedure set forth herein.

The limited warranty set forth in Section 1 shall not apply in the event that a breach of such warranty results from the product or device, being (a) used other than in accordance with this manual or other published guidelines, (b) modified, repaired, serviced, maintained or altered by anyone other than the Company without the prior written approval of the Company in each instance; for the avoidance of doubt, the modification of any software embedded in the products shall result in the immediate voiding of the limited warranty; (c) damaged by causes beyond the reasonable control of the Company, such as a fire, flood or earthquake. The warranties do not apply (a) to consumable parts, such as batteries, that are designed to diminish over time, (b) to cosmetic damage, such as scratches and dents or (c) to defects caused by normal wear and tear and the normal aging of the product. The warranties extend only to you and do not extend to any other individual or entity. The warranties shall be voided if any serial number shall be removed or defaced.

## Additional Information

THE WARRANTY AND REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, EXPRESS OR IMPLIED. No CGS Tower Networks Ltd reseller, agent, or employee is authorized to make any modification, extension, or addition to this warranty.

CGS Tower Networks Ltd is always open to any comments or suggestions you may have about its products and/or this manual.

Send correspondence to

CGS Tower Networks Ltd

15 Hamelacha St. Rosh Haayin,

Israel, 4809136

Telephone: +972 (3) 6166026

Fax: +972 (3) 6166026

E-mail: info@cgstowernetworks.com / URL: www.cgstowernetworks.com

# Contents

# Introduction

## Product Overview

The CGS-NPB series introduces the next generation appliances providing network visibility that enables Cyber Security, Big Data analytics and monitoring tools deployed in high-end data centers and branch offices. The CGS-NPB appliances address the market requirement to reduce the cost, complexity and footprint of high-end network visibility solutions. The CGS-NPB series leverages a powerful state of the art platform combined with CGS innovative software, resulting in the most reliable, scalable, modular Packet Broker that support 1G, 10G, 25G, 40G, 50G, 100G, and 400G ports and multiple interfaces (Optical, Copper, DAC).

The CGS-NPB series includes aggregation, replication, filtering, stacking, and load balancing that enable and optimize the benefits of the tools. Additional advanced features with deep packet inspection capabilities that optimize network traffic management are available in a powerful data center ready 1RU server.

This document describes the NPB I, NPB Ie, NPB Ie8, NPB II, NPB IIe, NPB III, and NPB IV switching devices.

**Note:**
Throughout this document, unless stated otherwise, NPB I refers to NPB I, NPB Ie, and NPB Ie8, and NPB II refers to both NPB II and NPB IIe.

To give a general reference, the following figures provide a general view for NPB I and II. Other devices are similar.

**Figure 1: NPB I and NPB II Front Panels**

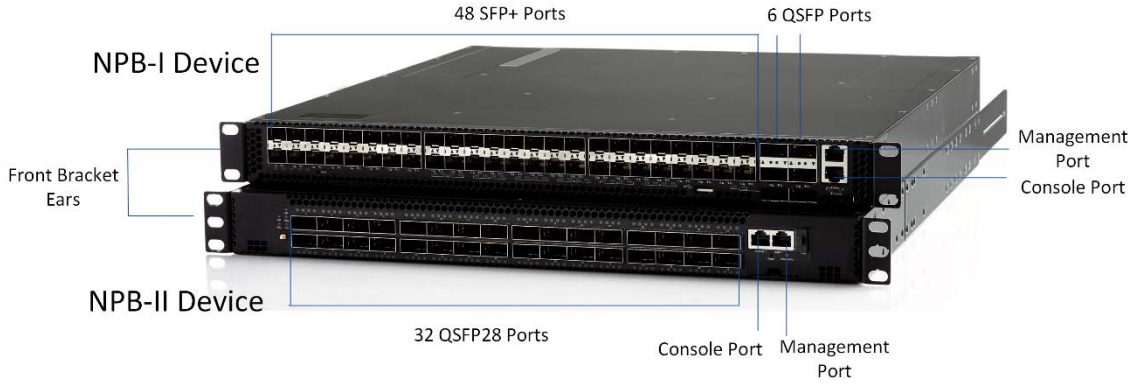


**Figure 2: NPB I Rear Panel**

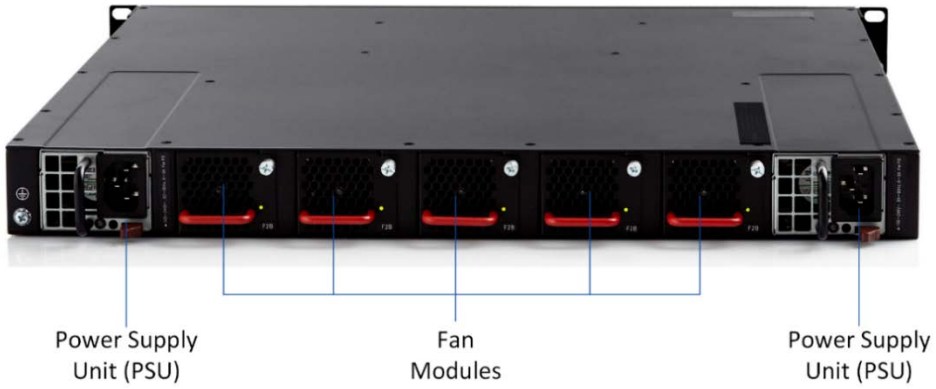
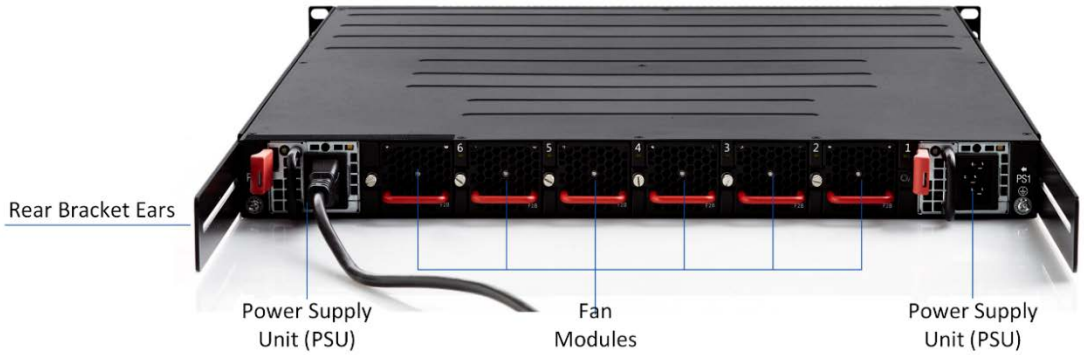



**Figure 3: NPB II Rear Panel**




## Key Features

- High density and compact 1RU form factor that saves rack space, power consumption and cooling (NPB IV is 2RU)
- CGS-NPB I: 48(SFP+) x 10M/100M/1G/2.5G/10G + 6(QSFP) x 10G/40G; each QSFP can breakout to 4 x 1G/2.5G/10G
- CGS-NPB Ie: 48(SFP+) x 10M/100M/1G/2.5G/10G + 6(QSFP28) x 1G/10G/25G/40G/50G/100G; each QSFP can breakout to 4 x 1G/10G/25G or 2 x 50G
- CGS-NPB Ie8: 48(SFP28) x 1G/10G/25G + 8(QSFP28) x 1G/10G/25G/40G/50G/100G; each QSFP28 can breakout to 4 x 1G/10G/25G or 2 x 50G
- CGS-NPB II: 32(QSFP28) x 1G/10G/25G/40G/100G; each QSFP28 can breakout to 4 x 1G/10G/25G
- CGS-NPB IIe: 32(QSFP28) x 1G/10G/25G/40G/50G/100G; each QSFP28 can breakout to 4 x 1G/10G/25G or 2 x 50G
- CGS-NPB III: 32(QSFP28 or QSFP-DD) x 10G/25G/40G/50G/100G/200G/400G; each QSFP-DD can breakout to 4 x 10G/25G/50G/100G or 2 x 40G/100G
- CGS-NPB IV: 40(QSFP28) x 40G/100G, or 20(QSFP28) ports, which can breakout to 4 x 10G/25G
- Cost effective data center ready platform
- High end platform with superior reliability, redundancy, modularity and scalability
- Aggregation, replication, filtering, timestamping, slicing, and load balancing

- Ingress and egress packet manipulations
- MPLS stripping
- Tunneled traffic filtering
- GRE tunneling
- Inline service chains
- High availability

## Use Cases

- Aggregation of TAP/SPAN network traffic to a centralized location where tools are deployed
- Optimize tools performance by filtering network traffic
- Load balance traffic according to tools capacities
- L1/L2 Matrix switch for testing environment (many to one, one to many, forwarding)
- MPLS stripping to enable monitoring of MPLS networks
- Service chaining in inline deployments

## Features and Benefits

**Table 1: NPB Features**

| Features | Benefits |
|---|---|
| Compact form factor | High density compact 1RU form factor that saves rack space, energy consumption and cooling |
| Traffic flow management | Aggregation of 1G, 10G, 25G, 40G, 50G, and 100G network ports based on port, MAC, VLAN, IPv4/IPv6 and TCP/UDP mapping rules<br>Redirect network traffic to Cyber Security, Big Data Analytics and monitoring tools through output ports based on mapping rules |
| Filtering | Filter network traffic to the selected ports based on the requirements of the tools that connect to them |
| Connectivity | Wide range of transceivers, optics and cables that support 1G, 10G, 25G, 40G, 50G, and 100G for common switches including Cisco, Juniper, Ericsson, SPAN PORTS and TAPS |
| Management | Multiple modern management options including CLI, SNMP V3, WEB UI, Net CONF, and REST API that can be connected to any SDN controller based management platform<br>Remote network access through Telnet or SSH<br>Logging that includes AAA servers, event notification, syslog, and SNMP traps |
| High availability | Supports high availability clusters for continuous operation |

| Features | Benefits |
|---|---|
| Reliability | Supports hot/cold aisle with port-to-power and power-to-port airflow |
| Redundancy | N+1 redundant, hot-swappable fan modules<br>Hot-swappable, load-sharing, redundant AC/DC PSU |
| GRE tunneling | GRE termination allowing to send and receive data over L2/L3 GRE tunnels |
| Aggregation | Aggregates and redirects network traffic from selected ingress ports to egress ports for further processing |
| Filtering | Optimizes tools performance by filtering out unnecessary network traffic with conditional 5-tuple filtering (MAC address, EtherType, IP address, TCP Port, UDF) |
| Slicing | Slices matched traffic at a fixed position |
| Timestamping | Marks packets with ingress and egress timestamp |
| PRBS | Runs Pseudo Random Binary Sequence on the ports |
| Port labelling | Tracks packet path by adding VLAN tags that indicate its ingress port |
| MAC replacement | Conditional MAC address replacement |
| MPLS stripping | Conditional removal of MPLS headers to accommodate tools that cannot handle MPLS traffic |
| Service chaining | Deploys inline configurations |
| Load balancing | Distributes traffic among several output interfaces using hash function or round robin |
| Inline | Supports inline traffic with service chain solutions using heartbeat monitoring |

# Installation

This chapter will walk you through the first installation process of the NPB device. It covers the following stages:

1. Unpacking and Installation
2. Verifying Device Operation Using LEDs
3. Working with the CLI

## Unpacking and Installation

The installation contains the following stages:

1. Preparation
2. Unpacking, Mounting, and Grounding
3. Identifying Your Device
4. Installing the Transceiver Modules
5. Powering the Device

### Preparation

Before starting the installation of your NPB device, make sure you have the following information available:

- IP address to be assigned to each NPB device you are about to install
- Netmask and default gateway IP address

To enable power redundancy, make sure you have two power sources.

### Unpacking, Mounting, and Grounding

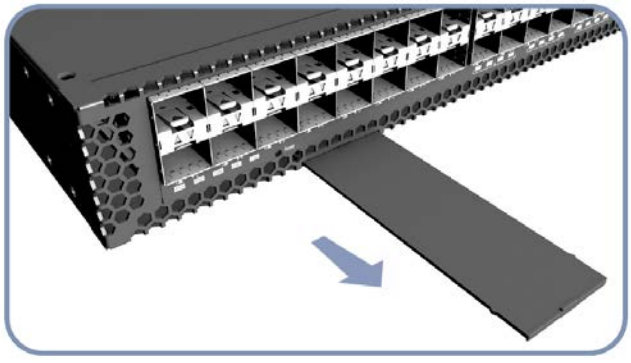
For information about unpacking, mounting, and grounding the device, consult the Quick Start Guide included. For more information, consult manufacturer documentation or CGS support.

### Identifying Your Device

Identify your device's MAC address and serial number as indicated on the product label. This information may be required when contacting CGS support.

The product label is located on the luggage tray, which can be pulled out from the front panel:

**Figure 4: NPB Luggage Tray Shown for NPB I**



## Installing the Transceiver Modules

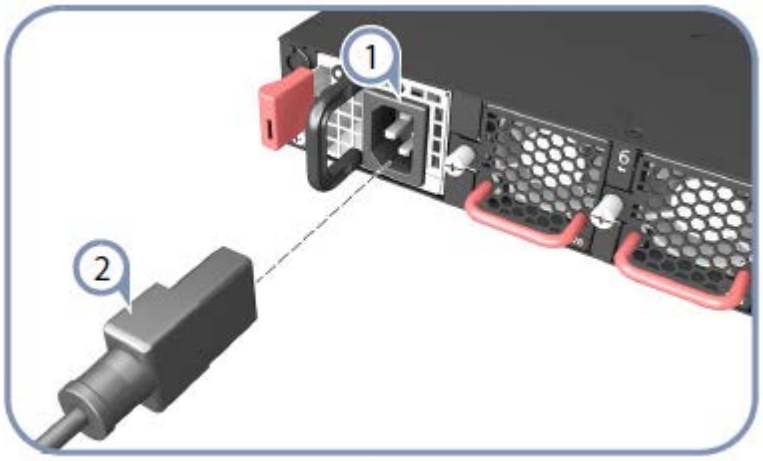
To install the SFP, SFP+ and QSFP transceivers (shipped separately), remove the temporary plug from the front panel ports, if there is one, and connect the corresponding transceiver module instead. You can connect one transceiver to each physical port of the NPB device.

## Powering the Device

The NPB device includes two Power Supply Units (PSU) to enable power redundancy.

To power your device, connect an external AC power source to one of the two PSU modules using the provided AC cord. If you wish to use the NPB device power redundancy, connect another AC cord to the second PSU module.

**Figure 5: Powering the Device**




# Installing the NPB Software

If the device was shipped without NPB software installed, the software can be installed using a USB storage device (Disk on Key). Perform the following steps:

1. Contact CGS to obtain the latest software image available for your device.
2. Burn the image to a USB stick.
3. Power down the device.
4. Connect the USB stick to the device.
5. Power up the device.
6. The installation process starts automatically and reboots the device when completed.
7. Remove the USB stick.

The device now is ready for activation as described in the next section.

## Activating the Device

To activate the NPB, a license must be installed. If the device installation was done on the user site as described above, a license must be installed manually by the user. Licenses are issued per machine and cannot be transferred between machines.

If no valid license is found, the system is not active and provides very limited functionality. In this case, the following indications are present when trying to access the system from CLI and WebUI:

**Figure 6: System License Not Valid Notice from the CLI**

```
SYSTEM LICENSE IS NOT VALID,
Use the ‘system license’ menu, consult the user
guide for more details
```

**Figure 7: System License Not Valid Notice from the WebUI**


To display the current license and its status from the CLI, use the following command:

```
NPB# show system license
```

To display the current license and its status using WebUI, select **System – Details** in the Navigation panel.

To install a license, perform the following steps:

1. Generate your machine's fingerprint. A fingerprint is an ASCII string that contains the information needed to generate a license for the machine. To generate a fingerprint from the CLI, use the following command:

   ```
   NPB# system license generate-fingerprint
   ```

   The Web UI generates the fingerprint automatically. Select **System – Details** in the Navigation panel, and click **Copy To Clipboard** to copy its value.

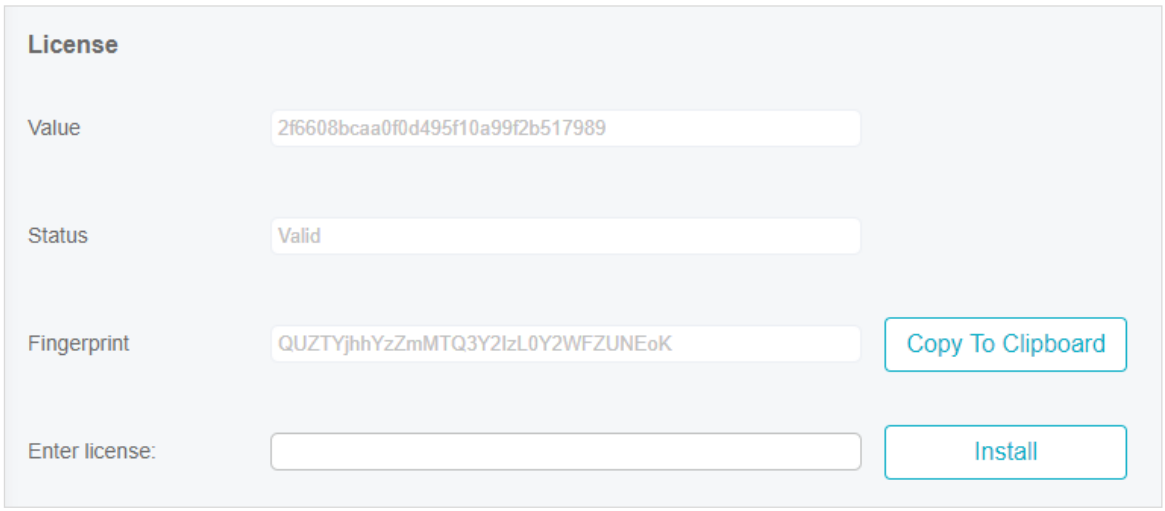
2. Contact CGS support with the fingerprint to obtain a license for your machine.
3. Install your license using the following CLI command:

   ```
   NPB# system license install <license-key>
   ```

   Or click **System – Details** in the Navigations panel, enter the license key, and click **Install.**

4. Verify that the license was installed successfully by displaying its status as described above.

**Figure 8: Installing License Using WebUI**




# Connecting and Integrating into the Network

After powering up the device, it can be connected and integrated into the network. There are two ways to do this:

- Via console port

Access the device through the console port, set its IP address, netmask, and default gateway according to your network requirements, and then access it through SSH.

- Via management port using default settings

Define a temporary network (usually just a laptop) according to the default management settings of the device and connect through SSH to set its IP address, netmask, and default gateway.

Once the IP address, netmask and default gateway are configured, the device can be accessed remotely through an SSH session.

## Connecting to the Device using the Console Port

To access the device through the console port, perform the following steps:

1. Connect the provided RJ45 console cable to the front-panel console port on one side and to a local PC running a terminal emulation SW on the other side.
2. Configure the SW to use the following settings:

| | |
|---|---|
| Baud rate | 115200 bps |
| Data bits | 8 |
| Stop bit | 1 |
| Parity | None |
| Flow control | None |

3. Connect to the local CLI using username: **`admin`** and password: **`admin`**.
4. Now, you can set the IP address and other management settings as described in Section Initial Device Configuration on p.44.

Once the device IP address is configured, you can connect the device to the network using the front-panel management port and access it remotely by SSH. Refer to Section Connecting to the Device using SSH on p.25.

### Connecting to the Device Using Default Management Interface Settings

The NPB device is shipped with the following default management interface configuration:

Address: 192.168.1.1

Netmask: 255.255.255.0

Gateway: 192.168.1.2

Configure a temporary network to work with the default settings above and connect to the device's front panel management port, using SSH as described in the next section to change the default IP setting to your network settings.

### Connecting to the Device using SSH

Once the device is connected to the network using the front-panel management port, it can be accessed remotely by SSH.

1. Open any SSH client on a PC that is connected to the network and can reach the device.
2. Open an SSH session to the device IP, using username: **`admin`** and password: **`admin`**.

## Verifying Device Operation Using LEDs

Check the LEDs on the front panel to verify proper operation. These LEDs are also useful for troubleshooting and for checking system hardware status.

**Figure 9: NPB I LEDs**

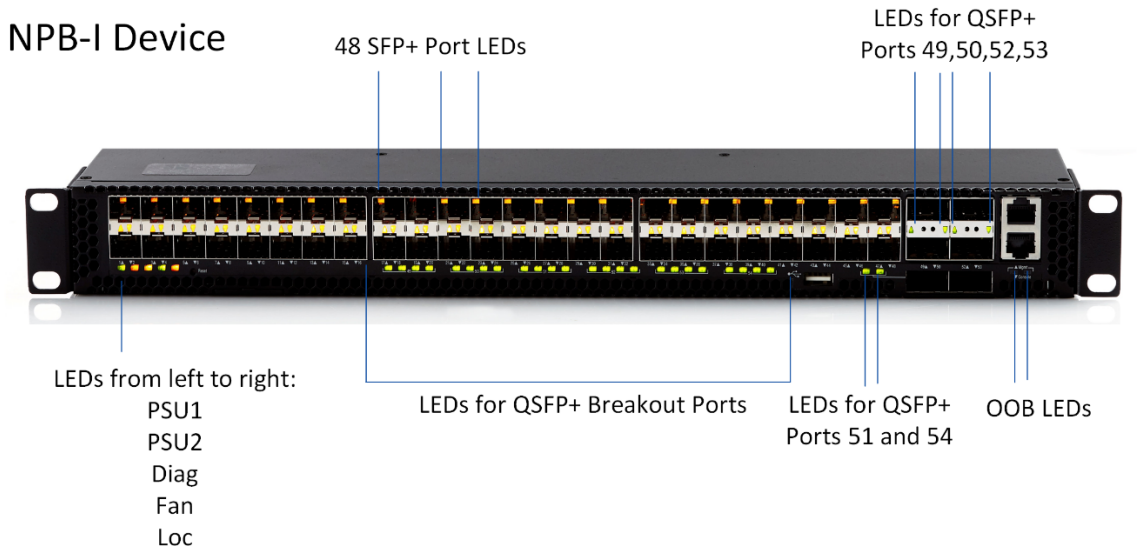


**Table 2: NPB I Front Panel LED Definitions**

| LED Name | LED Description | State |
|---|---|---|
| PSU1 | Indicates the status of Power Supply 1 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| PSU2 | Indicates the status of Power Supply 2 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| Diag | Indicates system diagnostic test results | Green – Normal<br>Amber – Fault detected |
| FAN | Indicates the status of the system fans | Green – All fans operational<br>Amber – One or more fan fault |
| LOC | Indicates a selected switch to help locate it in the Data Center | Amber flashing – Location function activated by management<br>Off – Function not active |
| SFP+ Port LEDs | Each SFP+ port has one LED (built into SFP+ cage) to indicate port status | On – Link is up. Flashing indicates activity.<br><br>Off – No link |
| QSFP Port LEDs | Each QSFP port has one LED to indicate port status | On – Link is up. Flashing indicates activity.<br>Off – No link |
| QSFP Breakout LEDs | Each QSFP has four LEDs to indicate the status of the individual 10G ports | On – Link is up. Flashing indicates activity.<br>Off – No link |
| Out Of Band (OOB) LEDs | 2 LEDs:<br>One indicates link status of 10/100/1000 management port.<br>The other indicates activity. | Green – Port has a link / is active<br>Off – No link / not active |

**Figure 10: NPB Ie Front Panel LEDs**

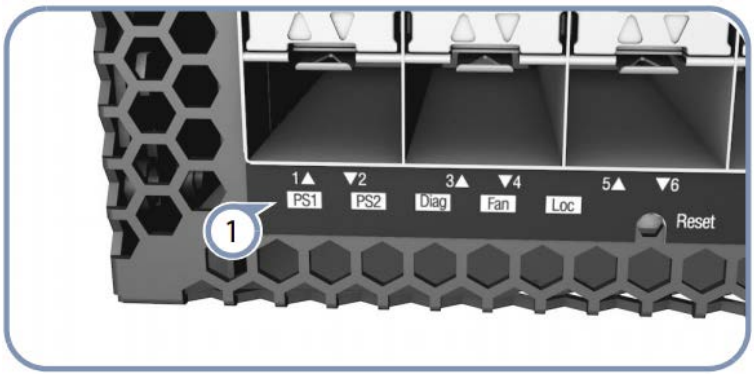



**Table 3: NPB Ie Front Panel LED Definitions**

| LED Name | LED Description | State |
|---|---|---|
| PS1 | Indicates the status of Power Supply 1 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| PS2 | Indicates the status of Power Supply 2 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| Diag | Indicates system diagnostic test results | Green – Normal<br>Amber – Fault detected |
| FAN | Indicates the status of the system fans | Green – All fans operational<br>Amber – One or more fan fault |
| LOC | Indicates a selected switch to help locate it in the Data Center | Amber flashing – Location function activated by management<br>Off – Function not active |
| SFP+ Port LEDs | Each SFP+ port has one LED (built into SFP+ cage) to indicate port status | Green – 10G<br>Amber – 1G<br>Off – no link |
| QSFP28 Port LEDs | Each QSFP28 port has one LED to indicate port status | Green – 100G<br>Blue – 40G<br>Off – no link |
| Out Of Band LED | Indicates the link status of the management port | Green – 1G link<br>Yellow – 10/100 link<br>Flashing – Indicates activity |

**Figure 11: NPB Ie8 Front Panel LEDs**

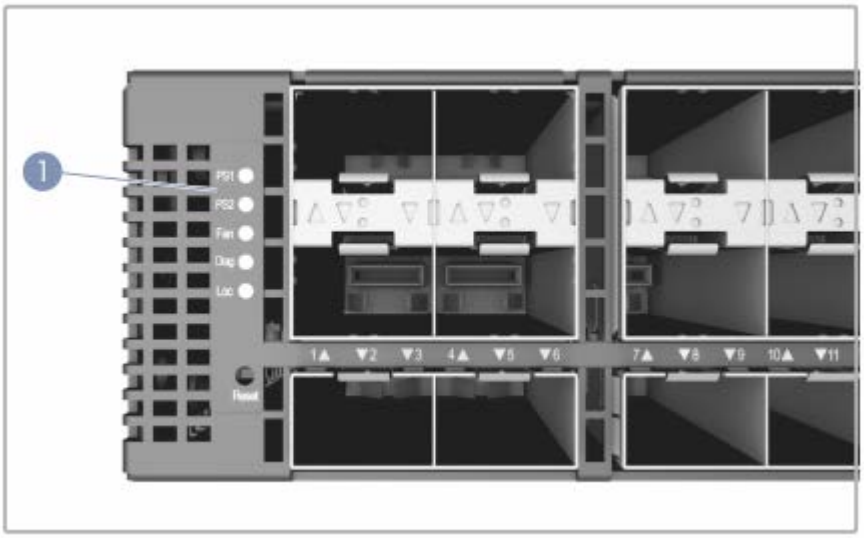



**Table 4: NPB Ie8 Front Panel LED Definitions**

| LED Name | LED Description | State |
|---|---|---|
| PS1 | Indicates the status of Power Supply 1 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| PS2 | Indicates the status of Power Supply 2 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| Diag | Indicates system diagnostic test results | Green – Normal<br>Amber – Fault detected |
| FAN | Indicates the status of the system fans | Green – All fans operational<br>Amber – One or more fan fault |
| LOC | Indicates a selected switch to help locate it in the Data Center | Green flashing – Location function activated by management<br>Off – Function not active |
| SFP+ Port LEDs | Each SFP+ port has one LED (built into SFP+ cage) to indicate port status | Green 1G/10G/25G<br>Off – no link |

| LED Name | LED Description | State |
|---|---|---|
| QSFP28 Port LEDs | LED 1 | Yellow – 1G/10G/25G<br>Blue – 40G<br>Green – 50G/100G<br>Off – not present |
| | LED 2-4 | Yellow – 1G/10G/25G<br>Green – 50G<br>Off – not present |
| Out Of Band LED | Indicates the link status of the management port | Green – 1G link<br>Yellow – 10/100 link<br>Flashing – Indicates activity |

**Figure 12: NPB II Front Panel LEDs**

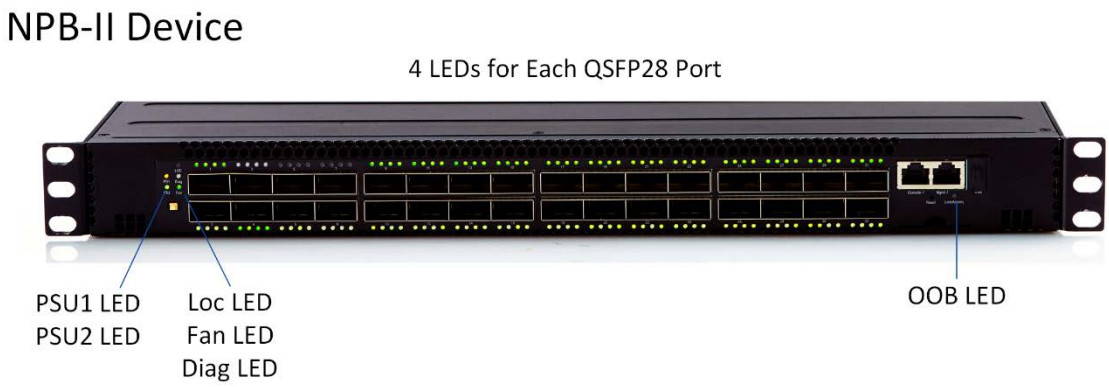



**Table 5: NPB II Front Panel LED Definitions**

| LED Name | LED Description | State |
|---|---|---|
| PSU1 | Indicates the status of Power Supply 1 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| PSU2 | Indicates the status of Power Supply 2 | Green – Normal<br>Amber – Fault detected<br>Off – No Power |
| Diag | Indicates system diagnostic test results | Green – Normal<br>Amber – Fault detected |
| FAN | Indicates the status of the system fans | Green – All fans operational<br>Amber – One or more fan fault |

| LED Name | LED Description | State |
|---|---|---|
| LOC | Indicates a selected switch to help locate it in the Data Center | Blue – Location function activated by management<br>Off – Function not active |
| QSFP28 Port LEDs | LED 1 | Blue – 100G<br>Yellow – 50G<br>Orange – 40G<br>Pink – 25G (white in breakout)<br>Green – 10G<br>White – 1G<br>Off – not present |
| | LED 2-4 | Yellow – 50G<br>White – 25G/1G<br>Green – 10G<br>Off – not present |
| Out Of Band LED | Indicates link status of 10/100/1000 management port | Green – 1G link<br>Yellow – 10/100 link<br>Flashing – Indicates activity |

### Example

In Figure 13, the LEDs indicate the following situation:

- Port 1 – Not Active – Link Down
- Port 2 – Active – Speed 10G
- Port 3 – Active – Speed 25G
- Port 4 – Active – Speed 40G
- Port 5 – Active – Speed 100G
- Port 6 – Active – Breakout 4x10G
- Port 7 – Active – Breakout 4x25G

When LEDs are flashing, there is active traffic on the corresponding port.

**Figure 13: Port Status LED Example**

**Figure 14: NPB IIe Front Panel LEDs**


**Table 6: NPB IIe Front Panel LED Definitions**

| LED Name | LED Description | State |
|---|---|---|
| PSU1 | Indicates the status of Power Supply 1 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| PSU2 | Indicates the status of Power Supply 2 | Green – Normal<br>Amber – Fault detected<br>Off – No Power |
| Diag | Indicates system diagnostic test results | Green – Normal<br>Amber – Fault detected |
| FAN | Indicates the status of the system fans | Green – All fans operational<br>Amber – One or more fan fault |
| LOC | Indicates a selected switch to help locate it in the Data Center | Blue flashing – Location function activated by management<br>Off – Function not active |
| QSFP28 Port LEDs | LED 1 | Blue – 100G<br>Purple – 50G<br>Red – 40G<br>White – 25G<br>Green – 10G/1G<br>Off – not present |
| | LED 2-4 | Purple – 50G<br>White – 25G<br>Green – 10G/1G<br>Off – not present |
| Out Of Band LED | Indicates link status of 10/100/1000 management port | Green – 1G link<br>Yellow – 10/100 link<br>Flashing – Indicates activity |

**Figure 15: NPB III Front Panel LEDs**

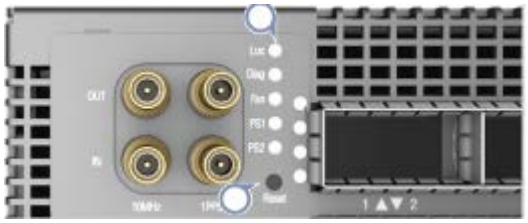


**Table 7: NPB III Front Panel LED Definitions**

| LED Name | LED Description | State |
|---|---|---|
| PSU1 | Indicates the status of Power Supply 1 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| PSU2 | Indicates the status of Power Supply 2 | Green – Normal<br>Amber – Fault detected<br>Off – No Power |
| Diag | Indicates system diagnostic test results | Green – Normal<br>Amber – Fault detected |
| FAN | Indicates the status of the system fans | Green – All fans operational<br>Amber – One or more fan fault |
| LOC | Indicates a selected switch to help locate it in the Data Center | Red flashing – Location function activated by management<br>Off – Function not active |
| QSFP-DD Port LEDs | LED 1 | Blue – 400G/200G/4x100/50G/4x50G<br>Green – 100G/10G/4x10G<br>Purple – 40G<br>Amber – 25G/4x25G<br>Off – not present |
| | LED 2 | Green – 200G/4x100G/50G/40G<br>Off – not present |
| | LED 3-4 | Green – 4x100G<br>Off – not present |
| Out Of Band LED | Indicates link status of management port | Green – 1G link<br>Flashing – Indicates activity |

**Figure 16: NPB IV Front Panel LEDs**

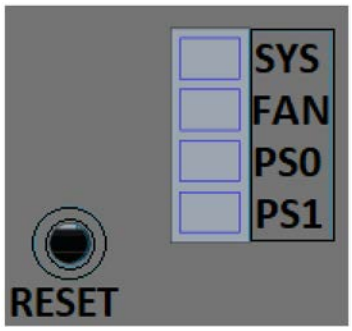



**Table 8: NPB IV Front Panel LED Definitions**

| LED Name | LED Description | State |
|---|---|---|
| SYS | Indicates the system status | Green – Host CPU is up<br>Amber – Power is up, but Host CPU is not up<br>OFF – No power |
| FAN | Indicates the fan status | Green – All fans operational<br>Amber – One or more fan fault<br>OFF – No fans present, or fans are not initialized |
| PS0 | Indicates the status of Power Supply 0 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| PS1 | Indicates the status of Power Supply 1 | Green – Normal<br>Amber – Fault detected<br>Off – No power |
| QSFP 28 Port LEDs | Indicates port link status | Green – Link is up<br>Flashing – Indicates activity |
| Out Of Band LED | Indicates link status of management port | Green – 1G link<br>Flashing – Indicates activity |

# Working with the CLI

This section introduces the NPB CLI functionality. It gives a general overview on the CLI modes of operation, and describes how to get help and how to use general and useful commands.

## CLI Modes

The CLI operates in two different modes:

- Operational mode allows the user to view the device configuration and to perform operations that do not change the device configuration, for example, to change CLI session settings.
- Configuration mode allows the user to change the device configuration.

When starting a CLI session, the user is logged in to Operational mode. To switch to Configuration mode, use the **`config`** command:

```
NPB# config
Entering configuration mode terminal
NPB(config)#
```

To switch back to Operational mode, use the **end** command:

```
NPB(config)# end
NPB#
```

The change is indicated in the CLI prompt.

### Configuration Mode

Once in Configuration mode, the user can change the device configuration. The changes done in the Configuration mode have no effect until they are "committed" using the **`Commit`** command. Commit operations are first validated and then can have atomic success or fail. Changes that have not yet been committed are called "pending changes".

You can view the set of pending changes using the **`show configuration`** command.

In the example below, the CLI flow sets the CLI idle timeout to 10 minutes:

```
NPB(config)# system cli session idle-timeout 10m
NPB(config)# show configuration
system cli session idle-timeout 10m NPB(config)# commit
Commit complete.
NPB(config)# show configuration
% No configuration changes found.
NPB(config)#
```

Note how, before the commit, the change is still pending and can be observed using the **`show configuration`** command, while the same command does not show the change after the commit, as it is no longer pending.

## CLI Help

To view the list of available commands at any state, use either the **?** character or the tab key, for example:

```
NPB(config)# system ?
Possible completions:
  aaa                 AAA settings
  alarms              Alarm operations
  cli                 Cli settings
  config-files        Configuration files actions
  details             Display system details
  factory-default     Restore factory default
  hw                  Control hw features
  interface           Interfaces configuration
  log                 System log level
  netconf             Netconf settings
  restconf            Restconf settings
  security            System security
  snmp                SNMP settings
  sw-upgrade          Software upgrade setting and activation
  syslog              Syslog settings
  time-and-date       Time and date settings
  user-mgmt           User authentication settings
  webui               Webui settings
```

To get help on a specific command, use the **help** command followed by the requested command name, for example:

```
NPB(config)# help system cli session idle-timeout
Help for command: system cli session idle-timeout

Maximum idle time before terminating a CLI session. Default
is PT30M, ie 30 minutes.
```

## CLI Useful Commands

This section includes a list of commonly used CLI commands. Use **?** or the tab key to see possible completions for each command.

**Note:**
Some of the commands are available only in either Operational or in Configuration mode. Some are available in both.

### | (pipe)

The **|** character can be used to redirect command output into a set of redirect commands for analyzing the returned data. These commands can be chained to achieve more complex processing.

The list of redirect commands varies from command to command and can be displayed using the **?** character. For example, for the **`show ports`** command:

```
NPB# show ports | ?
Possible completions:
  append        Append output text to a file
  begin         Begin with the line that matches
  best-effort   Display data even if data provider is unavailable or
                continue loading from file in presence of failures
  count         Count the number of lines in the output
  csv           Show table output in CSV format
  de-select     De-select columns
  display       Display options
  exclude       Exclude lines that match
  include       Include lines that match
  linnum        Enumerate lines in the output
  match-all     All selected filters must match
  match-any     At least one filter must match
  more          Paginate output
  nomore        Suppress pagination
  notab         Suppress table output
  repeat        Repeat show command with a given interval
  save          Save output text to a file
  select        Select additional columns
  sort-by       Select sorting indices
  tab           Enforce table output
  until         End with the line that matches
```

### alias

The **`alias`** command creates aliases for commonly used commands. It, for example, enables replacing the **`show system snmp`** command with the alias **`SNMP`** for easier use:

```
NPB(config)# alias SNMP expansion "show system snmp"
```

### do

The **do** command lets you run Operational mode commands from within Configuration mode.

### id

The **`id`** command displays information about the user that is currently logged in.

**no**

The **no** command returns fields to their default values or deletes elements.

**show running-config**

The **`show running-config`** command displays the currently running configuration.

**show**

The **show** command displays status and configuration of certain features.

**top**

The **`top`** command returns the user to the top level in Configuration mode. If followed by a command, the command is executed as if it was entered at the top level of the Configuration mode.

**who**

The **who** command displays information regarding the currently open sessions.

## CLI Keyboard Shortcuts

Table 9 list some useful CLI keyboard shortcuts.

**Table 9: CLI Keyboard Shortcuts**

| Shortcut | Action |
|---|---|
| **Move Commands** | |
| Ctrl-b or Left Arrow | Move the cursor back one character |
| Esc-b or Alt-b | Move the cursor back one word |
| Ctrl-f or Right Arrow | Move the cursor forward one character |
| Esc-f or Alt-f | Move the cursor forward one word |
| Ctrl-a or Home | Move the cursor to the beginning of the command line |
| Ctrl-e or End | Move the cursor to the end of the command line |
| **Delete Commands** | |
| Ctrl-h, Delete, or Backspace | Delete the character before the cursor |
| Ctrl-d | Delete the character following the cursor |
| Ctrl-k | Delete all characters from the cursor to the end of the line |
| Ctrl-u or Ctrl-x | Delete the whole line |
| Ctrl-w, Esc-Backspace, or Alt-Backspace | Delete the word before the cursor |
| Esc-d or Alt-d | Delete the word after the cursor |
| Ctrl-y | Insert the most recently deleted text at the cursor |

| Shortcut | Action |
|---|---|
| **Scroll and Search Commands** | |
| Ctrl-p or Up Arrow | Scroll backward through the command history |
| Ctrl-n or Down Arrow | Scroll forward through the command history |
| Ctrl-r | Search the command history in reverse order |
| **Case Commands** | |
| Esc-c | Capitalize the word at the cursor, that is, make the first character uppercase and the rest of the word lowercase |
| Esc-l | Change the word at the cursor to lowercase |
| Esc-u | Change the word at the cursor to uppercase |
| **Miscellaneous Commands** | |
| Ctrl-c | Abort a command/Clear line |
| Ctrl-l | Redraw the screen |
| Ctrl-z | Exit configuration mode |

## Changing the Login Banner

To modify the CLI Login banner, use the following CLI command:

```
NPB(config)# system cli banner "<new banner>"
```

Use the standard escaped characters \n, \r and \t for new line, carriage return, and tab.

To return to the default banner, use the following command:

```
NPB(config)# no system cli banner
```

## Changing SSH Settings

The NPB supports the following SSH Message Authentication Code (MAC) and encryption algorithms.

MAC: hmac-md5, hmac-sha1, hmacsha2-256, hmac-sha2-512, hmac-sha1-96, hmac-md5-96

Encryption: aes128-gcm@openssh.com, chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes256-cbc, 3des-cbc

By default, all algorithms are used.

To modify the set of used algorithms from the CLI, use the following commands:

```
NPB(config)# system cli ssh mac <algorithm-list>
NPB(config)# system cli ssh encryption <algorithm-list>
```

where **`algorithm-list`** is a list of comma-separated algorithms from the sets above.

To return to the default setting, use the following command:

```
NPB(config)# no system cli ssh mac
NPB(config)# no system cli ssh encryption
```

# Working with the WebUI Application

## Getting Started

The NPB device provides a Web UI application that can be used to configure and monitor the device using a web browser.

To set up the WebUI application for use, perform the following steps:

1. Assign an IP address to the NPB.
2. Enable the WebUI interface using the CLI.
3. Point your browser to the device's IP, using Port 8008 for an HTTP connection or Port 8888 for an HTTPS connection.
   For example: http://192.168.1.10:8008
4. When the Login page is displayed, log in using one of the NPB defined users.

The NPB WebUI application is compatible with Chrome and Firefox internet browsers on Windows 7, Windows 10, and Ubuntu 14 (or higher) operating systems.

**Figure 17: WebUI Login Page (NPB II)**


Upon successful login, you are redirected to the WebUI home page as shown in Figure 18.

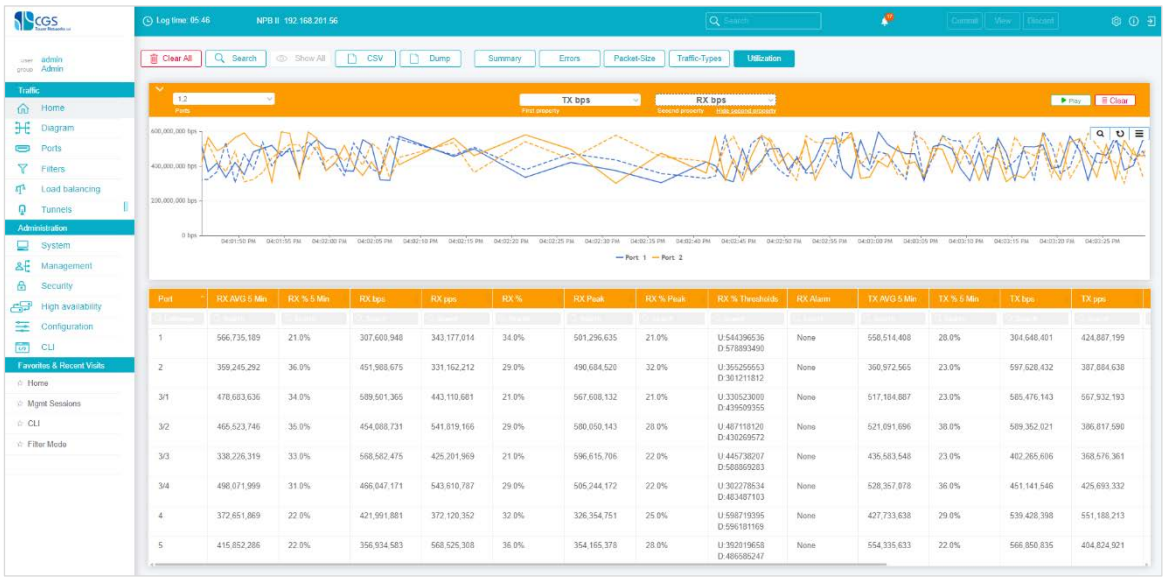
## WebUI Overview

The NPB WebUI application is an intuitive and easy-to-use graphical interface. This section describes its main design concepts. Specific operations are described throughout this document in the relevant sections.

WebUI pages contain the following elements:

- Navigation panel on the left
- Status bar on top
- Main panel in the central area
- Extension panel on the right (optional)

**Figure 18: Port Configuration Page (Main WebUI Page)**



## Navigation Panel

The area on the left is called the Navigation panel. It contains direct links to all the WebUI pages, grouped into categories referred to as Navigation Items (e.g. Ports, Filter and System).

At the very top of the Navigation panel appears the username and the group of the user that is currently logged in.

The Navigation panel remains accessible also when accessing other WebUI pages. It can be collapsed to get more space for the other panels.

## Status Panel

The blue bar at the top of the page is referred to as the Status panel. It contains the following information (left to right):

- Time passed since login
- Device IP and model
- Search tool for WebUI pages (Note that the tool does not search the content of the pages)
- Alarm indication – indicates the number of unviewed new alarms; clicking it leads to the alarm page
- Commit and Discard buttons for committing or discarding pending changes
- Settings, Info and Logout widgets

**Figure 19: Status Bar**

### Main Panel and Extension Panel

The content of the central area is set according to the selected page. By default, the application opens on the Port Configuration page.

In many WebUI pages, the information is displayed in a table with clickable lines. The table lines contain the main attributes of each element. Where relevant, clicking the line opens an extension panel on the right, which enables viewing and editing the full set of attributes of the selected element. Extension panels can be dragged to any location on the screen by clicking and dragging the panel's top bar.

In some tables, it is possible to configure multiple lines. To select multiple lines, mark their checkboxes while holding the Ctrl key, click while holding the Shift Key, or 'click and drag' to mark a range of lines.

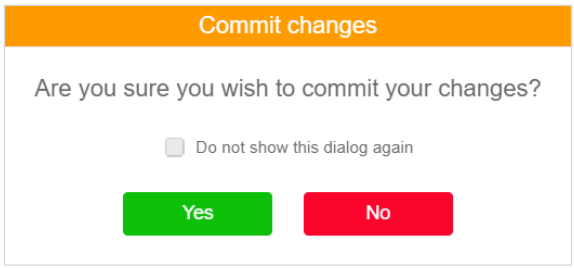
**Note:**

All changes done in the WebUI are considered 'pending' until they are committed (see Section Configuration Mode on p. 34 for details on pending changes).

Changes done in an extension panel usually require clicking the panel's **Apply** button to be populated to the table (after clicking **Apply**, they are still pending!).

To commit the pending changes, click the **Commit** button on the Status panel. You can view the changes before committing by clicking **View Changes** in the confirmation dialog.

**Figure 20: Commit Changes Dialog**




Some tables include search and sort capabilities as shown below (for the alarm table).

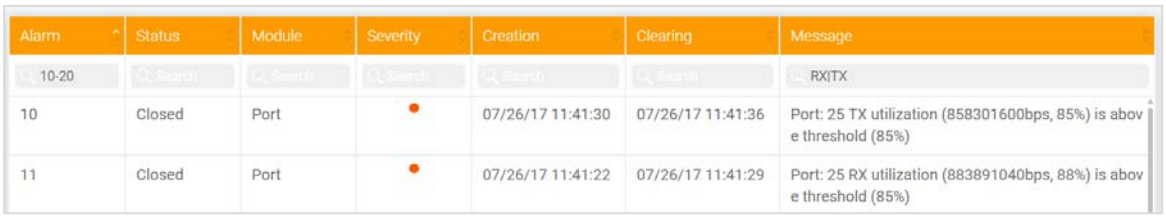
**Figure 21: Example of Search and Sort Capabilities in Tables**


To sort according to a specific column, click the header; a highlighted ˅ or ^ symbol indicates an active column sort.

To search a specific column, use the search box below the column name. The index column is searched numerically using a specific value or a range expression. Non-index columns are searched by regular expressions. Statistics columns can be searched with comparison operators such as ">100" and "<= 99".

For example, to display alarms with an ID in the range 10 to 20 that include either 'RX' or 'TX' in their message, use the numeric range expression '10-20' in the Alarm column (which is the index column of this table) and the regular expression 'RX|TX' in the Message column:

**Figure 22: Example of a Search in a Table**



| Alarm | Status | Module | Severity | Creation | Clearing | Message |
|---|---|---|---|---|---|---|
| 10-20 | | | | | | RX\|TX |
| 10 | Closed | Port | | 07/26/17 11:41:30 | 07/26/17 11:41:36 | Port: 25 TX utilization (858301600bps, 85%) is above threshold (85%) |
| 11 | Closed | Port | | 07/26/17 11:41:22 | 07/26/17 11:41:29 | Port: 25 RX utilization (883891040bps, 88%) is above threshold (85%) |

To clear the current search, click the **Show All** button above the table.

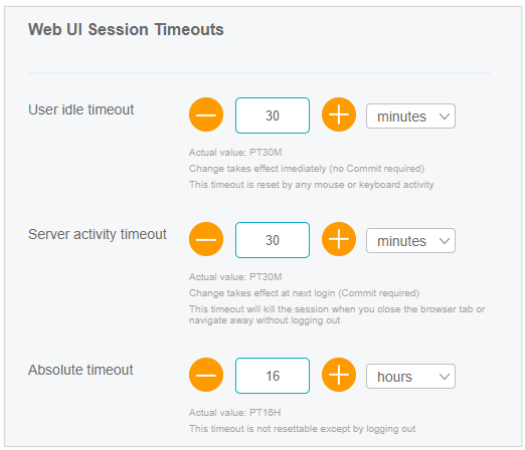
### Session Timeouts

For security considerations, the NPB WebUI application maintains session timeouts as listed below. When any of these timeouts expires, the session is terminated.

- User Idle timeout:
  Timer resets upon user activity (mouse or keyboard). Changing the value of this timeout takes effect immediately for the current session (no commit is required). Default setting is 30 minutes.
- Server Activity timeout:
  Timer resets upon server activity. This timeout will close a session if the session is not active, but the user has not logged out, e.g. when closing the browser without logging out or when the user is active in a different application but not in WebUI. Changing the value of this timeout takes effect at next login (commit is required). Default setting is 30 minutes.
- Absolute timeout:
  Timer resets only upon logout. This timeout will close a session regardless of its activity. Changing the value of this timeout takes effect at next login (commit is required). Default setting is 16 hours.

To change the session timeouts, select **Management – General settings** in the Navigation panel.

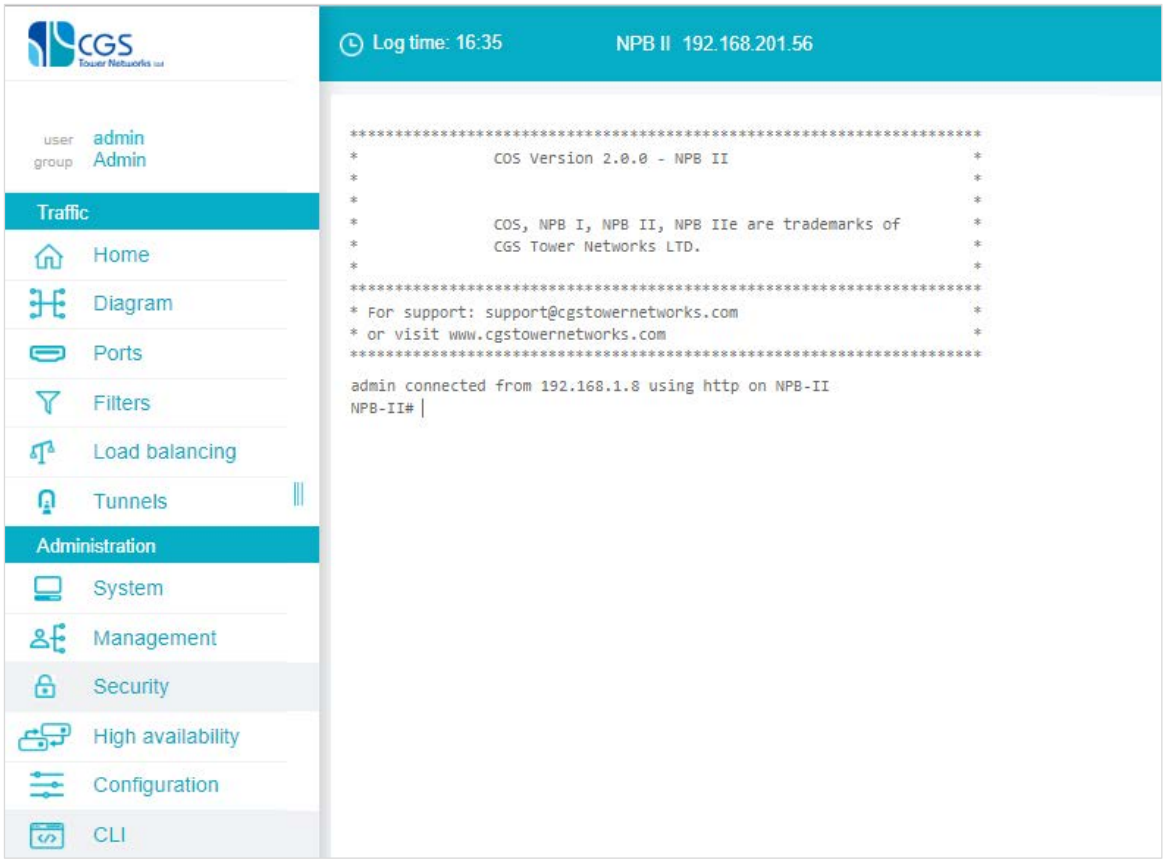
**Figure 23: Session Timeouts**



### Embedded CLI

The WebUI application contains an embedded CLI connection, which can be used as a regular CLI interface. To use it, click **CLI** on the Navigation panel.

**Figure 24: Embedded CLI Connection**



# System Settings

## Initial Device Configuration

### Setting IP Address

To access the NPB device remotely, you need to configure its IP address so it will meet your network requirements. This can be done either through the console port using CLI or through the management port as described in Section Connecting and Integrating into the Network on p.24.

The NPB device supports a single management interface named **eth0**. This interface supports the IPv4 and IPv6 protocols. Addresses can be assigned statically or using DHCP.

To set an IPv4 address from the CLI, use the following command:

```
NPB(config)# system interface eth0 ipv4-address <device-ip> ipv4-
gateway <gateway-ip> ipv4-mask <mask>
```

For example:

```
NPB(config)# system interface eth0 ipv4-address 192.168.10.10 ipv4-
gateway 192.168.0.1 ipv4-mask 255.255.255.0
```

To set an IPv6 address from the CLI, use the following command:

```
NPB(config)# system interface eth0 ipv6-address <device-ip> ipv6-
gateway <gateway-ip> ipv6-prefix-len <prefix-length>
```

For example:

```
NPB(config)# system interface eth0 ipv6-address 2610:20:6F15:15::27
ipv6-gateway 2610:20:6F15:15::0000 ipv6-prefix-len 64
```

To set an IP using DHCP from the CLI, use the following command:

```
NPB(config)# system interface eth0 dhcp enable
```

### Configuring the Management Interface

Table 10 lists the configurable management interface parameters.

**Table 10: Configurable Management Interface Parameters**

| Name | Description | Possible Values |
|---|---|---|
| DHCP | DHCP admin status | enable/disable, default is **disable** |
| duplex | Duplex mode | full/half/auto, default is **auto** |
| speed | Speed | 10M/100M/1000M/auto, default is **auto** |
| route | Specifies the routing path for this interface | See how to set interface routing below |

| Name | Description | Possible Values |
|---|---|---|
| ipv4-address | IPv4 address | Valid IPv4 address |
| ipv4-gateway | IPv4 default gateway | |
| ipv4-mask | IPv4 network mask | Valid IPv4 netmask |
| ipv6-address | IPv6 address | Valid IPv6 address |
| ipv6-gateway | IPv6 default gateway | |
| ipv6-prefix-len | IPv6 prefix length | 0-128 |

To set management port parameters from the CLI, use the following command:

```
NPB(config)# system interface eth0 dhcp|duplex|speed <value>
```

The NPB supports the configuration of routing paths per system interface. The paths define which next hop to use to reach a specific subnet. When traffic is sent out from the NPB to an external Syslog or SNMP server for example, the interface used for sending the traffic is selected based on these paths.

To set a routing path from the CLI, use the following command:

```
NPB(config)# system interface <if-name> route <name> to
<subnet>/<cidr> via <next-hop-ip>
```

To delete a routing path from the CLI, use the following command:

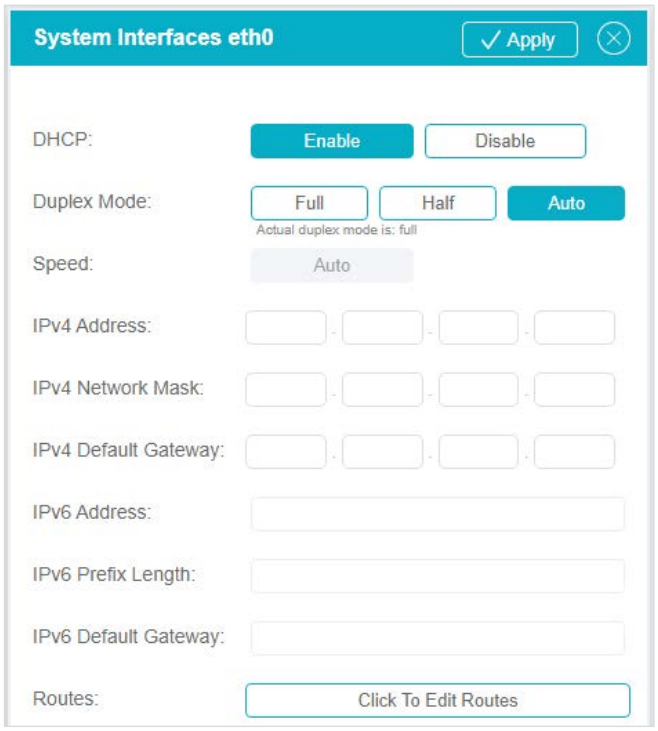
```
NPB(config)# no system interface <if-name> route <name>
```

To display management interface settings from the CLI, use the following command:

```
NPB# show system interface [eth0]
```

To configure the management interface using the WebUI application, select **System – Interfaces** in the Navigation panel. Click the eth0 interface line, and use the extension panel to set the required values. Note that changing the management interface parameters (e.g. its IP address) may disconnect the current WebUI session.

**Figure 25: Configuring Management Interface from WebUI**




**Note:**
NPB III supports only auto speed setting. Make sure that the far end is configured to work with auto negotiation.

## Configuring DNS Servers

The NPB supports name resolution using a list of DNS servers. The servers on the list are used to resolve configured external servers' hostnames, such as Syslog server.

To set the list of DNS servers from the CLI, use the following command:

```
NPB(config)# system dns nameservers <list-of-servers-ip-addresses>
```

More than one entry can be given separated by spaces inside a pair of square brackets. For example:

```
NPB(config)# system dns nameservers [ 192.168.1.1 192.201.10.10 ]
```

To clear the list of DNS servers from the CLI, use the following command:

```
NPB(config)# no system dns nameservers
```

To set the list of DNS servers from the WebUI, select **System - Interfaces** in the Navigation panel. Use the **DNS Servers** button above the table.

## Time and Date Settings

The NPB device supports two types of time and date sources:

- Local - When local source is selected, the device's time is set according to a value supplied locally.
- NTP based - When NTP source is selected, the device uses the NTP protocol to sync its clock with the provided NTP servers.

### Setting a Local Time Source from the CLI

To set the local time zone from the CLI, use the following command:

```
NPB(config)# system time-and-date time-zone <time-zone-name>
```

To set a local time source from the CLI, use the following command:

```
NPB(config)# system time-and-date current-time-and-date <time-and-date>
```

For example:

```
NPB(config)# system time-and-date current-time-and-date "10/10/2016 10:00:01"
```

### Setting NTP Servers as a Time Source from the CLI

The NBP device supports up to four NTP servers. Setting the NTP servers involves the following parameters:

**Table 11: NTP Server Parameters**

| Name | Description | Possible Values |
|---|---|---|
| address | NTP server name or IP address | Valid IPv4 address |
| authentication-type | Authentication method to use in NTP messages | md5/none/sha/sha1, default is **none** |
| keyid | Unique symmetric key ID for NTP authentication | 1-65534 |
| key-value | Symmetric key for NTP authentication | string |
| polling | Activate NTP polling | enable/disable, default is **enable** |
| poll-max-interval | Maximum polling intervals in seconds as a power of two | 10-17, default is 10 (=1024 sec.) |
| poll-min-interval | Minimal poll intervals in seconds as a power of two | 3-10, default is 6 (=64 sec.) |

To set NTP time source from the CLI, first enable NTP, then set the NTP servers parameters:

```
NPB(config)# system time-and-date ntp admin enable
NPB(config)# system time-and-date ntp server <server-id> address
<name-or-address> authentication-type md5|none|sha|sha1 [key-value
<key-value> keyid <key-id>] [polling enable|disable] [poll-max-
interval <interval>] [poll-min-interval <interval>]
```

To display the current time and date configuration from the CLI, use the following command:

```
NPB# show system time-and-date
System Time and Date
============================
Time          11:32:48
Date          10/11/16
Timezone      America/New_York
Source        NTP

System NTP configuration
=================================================================
Admin         Enabled
Status        Synchronized to NTP server 216.229.0.179 at stratum 2,
correct within 157 ms
ID# Server Address  Polling  Min Interval  Max Interval  Authentication
===  ==============  ========  ==========  ==========  =============
1    129.6.15.28    Enabled        6            16        MD5
2    129.6.15.30    Disabled       6            10        None
3    216.229.0.179  Enabled        6            11        None
4    24.56.178.140  Enabled        6            10        None
```

**Note:**
NTP synchronization may take several minutes. You can show the synchronization status using **`do show system time-and-date`**. In the example above, the status is **`Synchronized`…**

### Managing Time and Date Settings from the WebUI

To manage time and date settings from the WebUI, select **System - Date and Time** in the Navigation panel. Use the **Local** and **NTP** buttons to configure the relevant details:

**Figure 26: Setting a Local Time Source from the WebUI**

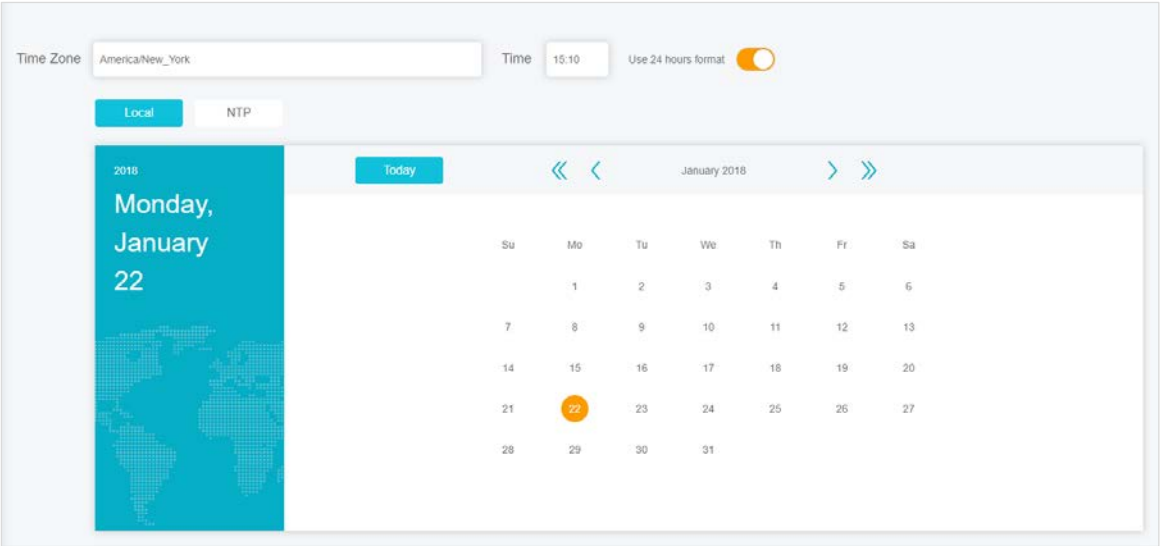
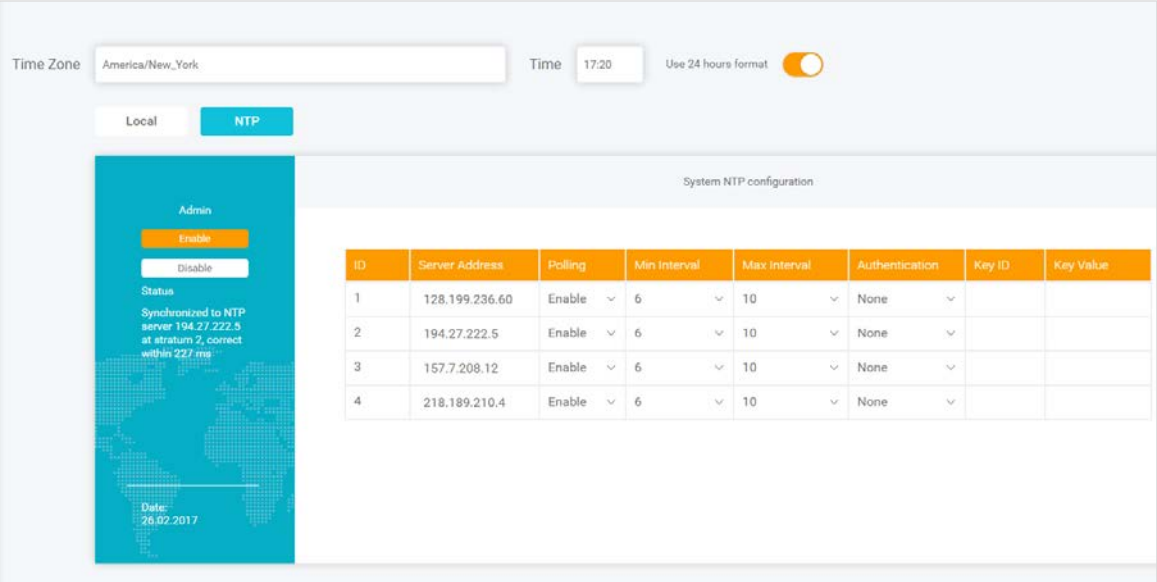


**Figure 27: Setting NTP Servers as a Time Source from the WebUI**




NTP server tables are editable inline. You can see the current NTP status next to the server table.

## Configuring Terminal for Using the Console Port

To access the device using the console port, configure your terminal to work with a baud rate of 115200 bps, 8 data bits, 1 stop bit, no parity, no flow control.

# Management Interfaces

This section describes the various management interfaces supported by the NPB device.

## Customizing the CLI

This section describes how to customize the CLI session. For a description of the CLI concepts and structure, refer to Section Working with the CLI on p.34.

Table 12 lists the configurable CLI attributes.

**Table 12: Configurable CLI Attributes**

| Command | Description | Possible Values |
|---|---|---|
| `NPB(config)# system cli session idle-timeout` | Sets an idle timeout after which the session is terminated | Duration using the following syntax: nYnMnDnHnMnS. E.g. 10 min and 30 sec. is expressed as 10m30s |
| `NPB# history` | Sets the size of the command history list | 1-1000, default is 1000 |
| `NPB# timestamp` | Logs the timestamp of every CLI command as it is entered | Enable/disable, default is disable |

| Command | Description | Possible Values |
|---|---|---|
| `NPB# paginate` | If paginate is **`false`**, the CLI pauses after each page it prints to the screen, waiting for user intervention to continue | true/false, default is **`false`** |
| `NPB# screen-length` | Sets the number of rows per screen | 1-32000, default is 82 |
| `NPB# screen-width` | Sets the number of characters per row | 1-512, default is 80 |
| `NPB# show-defaults` | When set to **`true`**, the configuration display includes the default value of every configured field | true/false, default is **`false`** |

## Working with SNMP

The NPB device supports both SNMP v2c and SNMP v3. SNMP users have read access and limited write access on the device based on their authorization. By default, the SNMP agent is not running and must be explicitly activated for each SNMP version.

To activate the SNMP agent from the CLI, use the following command:

```
NPB(config)# system snmp v2c|v3 true|false
```

For a full description of the NPB support of SNMP, refer to Section SNMP on p. 205.

## Working with NETCONF

The NPB device fully supports the NETCONF protocol. However, NETCONF support is disabled by default.

To activate NETCONF from the CLI, use the following command:

```
NPB(config)# system netconf enabled|disabled
```

By default, NETCONF uses Port 830. To use a different port, use the following command from the CLI:

```
NPB(config)# system netconf port <port-number>
```

To configure NETCONF using the WebUI, select **Management – General settings** in the Navigation panel.

## Working with RESTCONF

The NPB device fully supports the RESTCONF protocol. RESTCONF support is disabled by default.

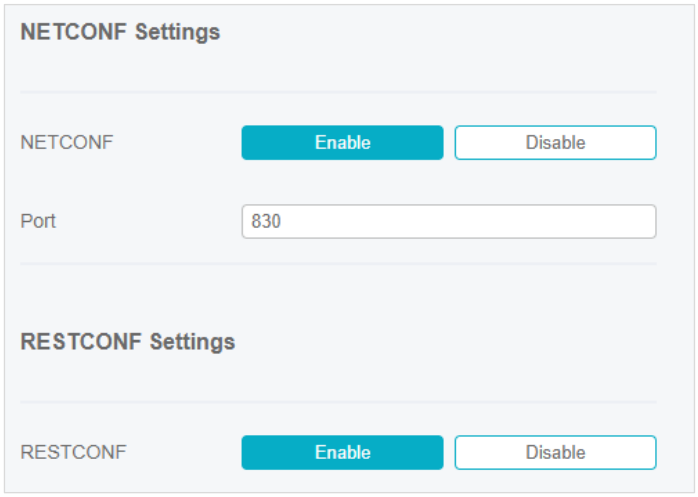
To activate RESTCONF from the CLI, use the following command:

```
NPB(config)# system restconf enabled|disabled
```

RESTCONF uses the WebUI ports, that is, Port 8008 for HTTP and Port 8888 for HTTPS.

To configure RESTCONF using the WebUI, select **Management – General settings** in the Navigation panel.

**Figure 28: Configuring NETCONF and RESTCONF using the WebUI**




## Working with the WebUI

To use the NPB WebUI application, point your browser to the device IP, using Port 8008 for HTTP or Port 8888 for HTTPS. For example: *https://192.168.100.100:8888*

These ports are configurable as explained below.

By default, WebUI HTTP access is disabled and HTTPS is enabled. To enable or disable WebUI access per protocol from the CLI, use the following command:

```
NPB(config)# system webui http|https enabled|disabled
```

To change the HTTP and HTTPS ports from the CLI, use the following command:

```
NPB(config)# system webui http|https port <port>
```

To change the HTTP and HTTPS ports from the WebUI, select **Management – General Settings** in the Navigation panel and use the **Web UI Settings** section.

### SSL Certificates

The NPB provides a default SSL certificate. For security reasons, it is highly recommended to replace the default certificate with your organization's certificate.

To create and upload a certificate file, perform the following steps:

1. Use a pair of private key and certificate signed by your organization. Do not use password-protected private keys. For details on how to create such a pair, see for example: https://jamielinux.com/docs/openssl-certificate-authority/create-the-root-pair.html
2. Create a pem file that contains the private key and the certificate. For example, on Linux, use the following command: `cat key.pem cert.pem > key_cert.pem`
3. Upload the pem file to the device as described below. This operation overwrites the currently installed certificate with the new certificate. A system reboot is required to install the new certificate.

To upload a certificate from the CLI, use the following command:

```
NPB# system webui https certificate import remote-url <remote-url>
[username <username> password <password>]
```

For example:

```
NPB# system webui https certificate import remote-url
scp://192.168.10.10/config/key_cert.pem username admin password 1234
```

To revert to the default certificate, use the following command:

```
NPB# system webui https certificate remove
```

To upload a certificate using the WebUI, select **Management – General settings** in the Navigation panel.

### HTTPS/TLS Ciphers

The NPB supports the following set of ciphers when establishing a HTTPS/TLS connection:

TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_AES_128_CCM_SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384, ECDH-ECDSA-AES256-GCM-SHA384, ECDH-RSA-AES256-GCM-SHA384, ECDH-ECDSA-AES256-SHA384, ECDH-RSA-AES256-SHA384, DHE-RSA-AES256-GCM-SHA384, DHE-DSS-AES256-GCM-SHA384, DHE-RSA-AES256-SHA256, DHE-DSS-AES256-SHA256, AES256-GCM-SHA384, AES256-SHA256, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES128-SHA256, ECDHE-RSA-AES128-SHA256, ECDH-ECDSA-AES128-GCM-SHA256, ECDH-RSA-AES128-GCM-SHA256, ECDH-ECDSA-AES128-SHA256, ECDH-RSA-AES128-SHA256, DHE-RSA-AES128-GCM-SHA256, DHE-DSS-AES128-GCM-SHA256, DHE-RSA-AES128-SHA256, DHE-DSS-AES128-SHA256, AES128-GCM-SHA256, AES128-SHA256, ECDHE-ECDSA-AES256-SHA, ECDHE-RSA-AES256-SHA, DHE-RSA-AES256-SHA, DHE-DSS-AES256-SHA, ECDH-ECDSA-AES256-SHA, ECDH-RSA-AES256-SHA, AES256-SHA, ECDHE-ECDSA-DES-CBC3-SHA, ECDHE-RSA-DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, EDH-DSS-DES-CBC3-SHA, ECDH-ECDSA-DES-CBC3-SHA, ECDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, ECDHE-ECDSA-AES128-SHA, ECDHE-RSA-AES128-SHA, DHE-RSA-AES128-SHA, DHE-DSS-AES128-SHA, ECDH-ECDSA-AES128-SHA, ECDH-RSA-AES128-SHA, AES128-SHA, EDH-RSA-DES-CBC-SHA, and DES-CBC-SHA

By default, the entire set is used.

To modify the set of supported ciphers from the CLI, use the following command:

```
NPB(config)# system webui https ciphers <cipher-list>
```

where **`cipher-list`** is a list of colon-separated ciphers from the set above.

To return to the default set, use the following command:

```
NPB(config)# system webui https ciphers DEFAULT
```

or:

```
NPB(config)# no system webui https ciphers
```

# Access Control Lists

## Overview

Access control lists (ACL) are used to restrict remote access to the device's management interface. With ACL, the exact set of IP addresses that are allowed to access each of the management interfaces (CLI, WebUI, SNMP, and NETCONF) is explicitly defined. Traffic arriving from non-authorized IPs is dropped. If no ACL is attached to an interface, traffic is not restricted.

## Blocking Incoming ICMP Requests

By default, the system answers ICMP echo requests (pings) destined to its IP interfaces. It is possible to change this behavior and ignore incoming ICMP echo requests.

To block or unblock incoming ping requests from the CLI, use the following command:

```
NPB(config)# [no] system security block-incoming-ping
```

To block or unblock incoming ping requests from the WebUI, select **Security – Access Control Lists** in the Navigation panel.

## Access Control List Configuration

To configure an ACL, you need to define control lists and then attach them to one or more of the management interfaces. The same list can be attached to several interfaces (e.g. CLI and WebUI) and several lists can be attached to a single interface. Up to 16 different lists are supported; each list can contain up to 16 entries; each entry can be either a single IP or an IP range.

To define a new ACL from the CLI, use the following command:

```
NPB(config)# system security acl <name> ip <ipv4-address>[/<ipv4-
subnet>]|<ipv6-address>[/<ipv6-net-mask>]|<ip-address-range>
```

More than one IP entry can be given using the [ ] syntax, separated by spaces inside a pair of square brackets. For example:

```
NPB(config)# system security acl myacl1 ip [ 192.168.100.10
192.168.100.20 ]
```

**Note:**
The spaces after the opening and before the closing square bracket are important! Missing spaces will cause a syntax error.

To add an IP to the current entries in an existing context, use the **ip** command without square brackets. For example:

```
NPB(config)# system security acl myacl1
NPB(config-acl-myacl1)# ip 192.168.100.30
```

To overwrite IP entries in an existing context, use the [ ] syntax. For example:

```
NPB(config)# system security acl myacl1
NPB(config-acl-myacl1)# ip [ 192.168.100.40 ]
```

In this case, IP 192.168.100.40 overwrites the entire list of entries. Of course, you can specify several IPs in the square brackets.

To remove an entry from an ACL list using the CLI, use the following command:

```
NPB(config)# no system security acl <name> ip <ipv4-address>[/<ipv4-
subnet>]|<ipv6-address>[/<ipv6-net-mask>]|<ip-address-range>
```

To delete an entire ACL list from the CLI, use the following command:

```
NPB(config)# no system security acl <name>
```

To attach an ACL list to a management interface from the CLI, use the following command:

```
NPB(config)# system <if-name> security acl <acl-name>
```

Where <if-name> is one of the following: **cli, snmp, netconf, webui**

To detach an ACL list from a management interface using the CLI, use the following command:

```
NPB(config)# no system <if-name> security acl [<acl-name>]
```

Where <if-name> is one of the following: **cli, snmp, netconf, webui**

**Example:**

In this example, 2 ACL lists are created: one with IPv4 addresses and another with IPv6 addresses. The first list is attached to the SNMP management interface, and both lists are attached to the WebUI and NETCONF management interfaces. Note the use of the [ ] syntax:

```
NPB(config)# system security acl my-ipv4-acl ip [ 192.168.1.20/
255.255.0.0 192.200.10.100-192.200.10.127 192.250.10.100 ]
NPB(config-acl-my-ipv4-acl)# exit
NPB(config)# system security acl my-ipv6-acl ip [
fe00::8eea:1bff:fe34:ce1b fe80::8eea:1bff:fe34:ce1b/64 ]
NPB(config-acl-my-ipv6-acl)# exit

NPB(config)# system snmp security acl my-ipv4-acl

NPB(config)# system webui security acl my-ipv4-acl
NPB(config)# system webui security acl my-ipv6-acl

NPB(config)# system netconf security acl my-ipv4-acl
NPB(config)# system netconf security acl my-ipv6-acl
```

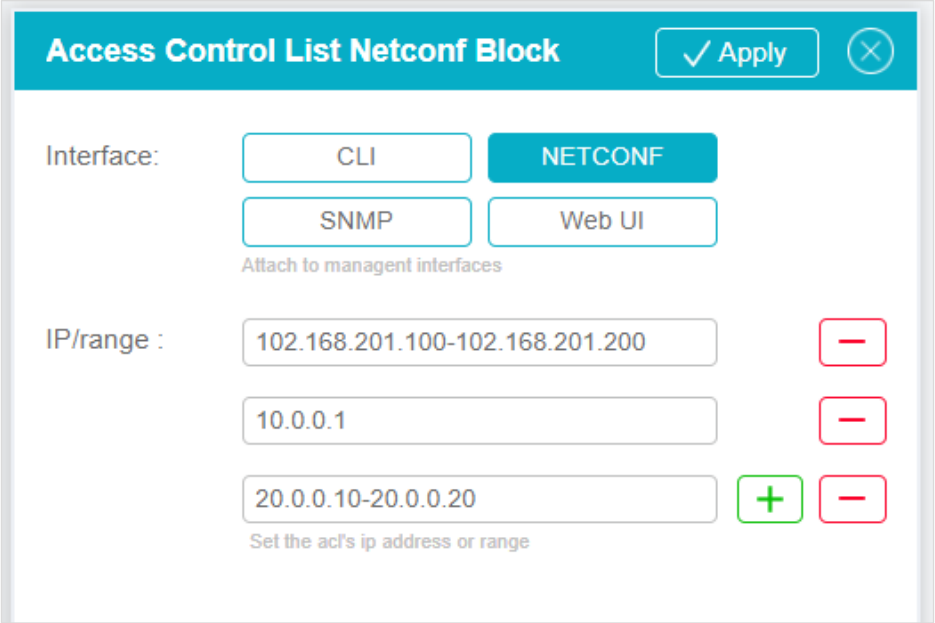
To manage ACL lists using the WebUI, select **Security – Access Control Lists** in the Navigation panel.

To create a new list, click **Add**. To remove an existing list, select the list, and click **Delete**.

To filter the displayed lists according to the management interface they are bound to, use the management interface buttons at the top of the window.

To set and modify list parameters, use the extension panel.

**Figure 29: Access Control List Configuration**




## Viewing ACL Configuration and Statistics

To see the configured ACL along with their statistics from the CLI, use the following command:

```
NPB(config)# show system security acl
```

To see the ACL attached to each management interface along with their statistics from the CLI, use the following command:

```
NPB(config)# show system <if-name> security
```

Where <if-name> is one of the following: **`cli`**, **`snmp`**, **`netconf`**, **`webui`**

To clear all ACL counters from the CLI, use the following command:

```
NPB(config)# system security clear-stats
```

To clear ACL counters for a specific ACL from the CLI, use the following command:

```
NPB(config)# system security acl <name> clear-stats
```

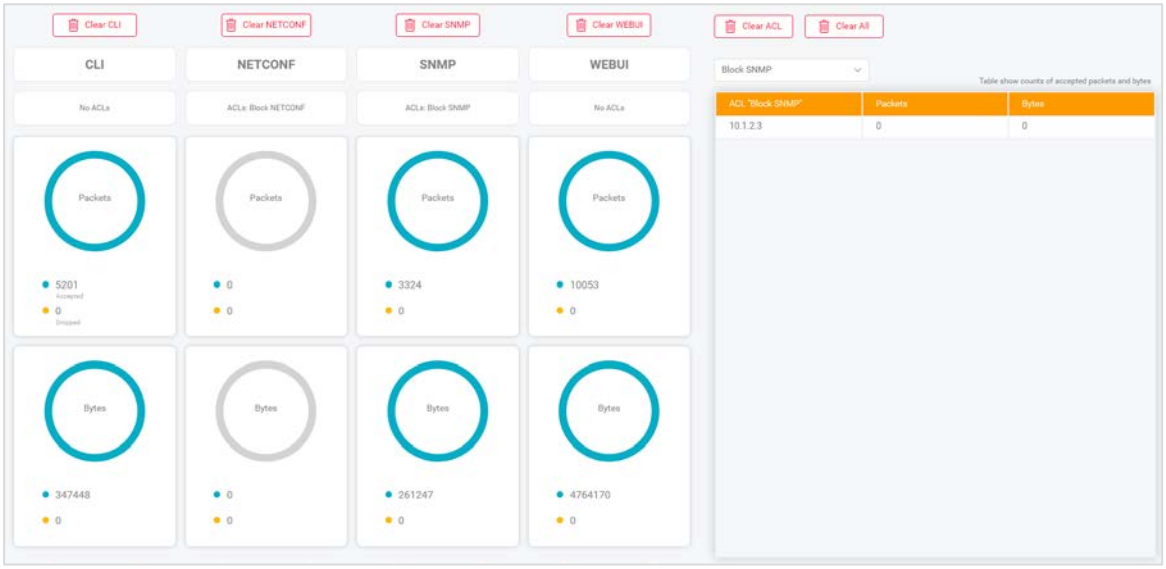
To clear ACL counters for a specific management interface from the CLI, use the following command:

```
NPB(config)# system <if-name> security clear-stats
```

Where <if-name> is one of the following: **`cli`**, **`snmp`**, **`netconf`**, **`webui`**

To view and clear ACL statistics using the WebUI, select **Security – Statistics** in the Navigation panel. Statistics are shown per managed interface on the left and per ACL list in the table on the right.

**Figure 30: ACL Statistics using the WebUI**




# SW Upgrade

## Overview

The NPB device contains two memory banks named **bank-a** and **bank-b** that can hold one NPB SW image each. The current application is always running from one bank, while the other bank is idle.

When upgrading, a new image is downloaded into the bank, on which the current application is not running. The image is validated, and after successful validation, the user can set this bank to be the "Next Boot Bank", that is, after a reboot, the device will boot from this bank.

To ensure that the NPB will always contain a valid image, it is not allowed to start a SW upgrade process when **`Next Boot Bank`** is not set to the currently running bank.

SW images can be loaded to the device by browsing your local files (WebUI only) or by using FTP, TFTP, SCP, HTTP, and HTTPS file transfer protocols.

## Upgrading to a New Image File

To upgrade the SW image from the CLI, use the following command:

```
NPB(config)# system sw-upgrade start [username <user>][password
<pass>] remote-url <file-name>
```

This command starts the file download to the device. Use the following command to stop the download operation:

```
NPB(config)# system sw-upgrade stop
```

To set the next boot bank from the CLI, use the following command:

```
NPB(config)# system sw-upgrade boot-bank version|[bank-a|bank-b]
```

To switch the boot bank to the nonactive bank from the CLI, use the following command:

```
NPB(config)# system sw-upgrade switch-boot-bank
```

To display the upgrade status from the CLI, use the following command:

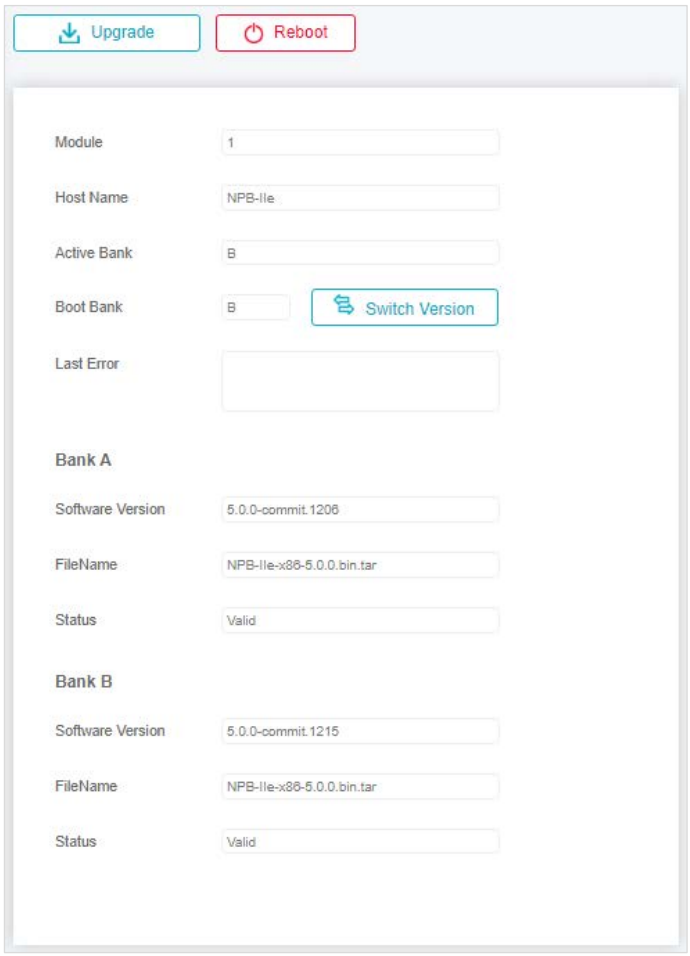
```
NPB# show system sw-upgrade
```

To upgrade the SW image using the WebUI, proceed as follows:

1. Select **Configuration – SW Upgrade** in the Navigation panel, and click the Upgrade button to upgrade the image.
2. In the popup window, enter the file's parameters or select a local file, and click **Next**.
3. Click the **Switch Version** button to set the boot bank.
4. Click the **Reboot** button to reboot.

This page also contains information regarding the installed version and the valid and next boot bank. To switch between boot banks, use the **Switch Version** button.

**Figure 31: Upgrading the SW Image Using the WebUI – Configuration**



**Note:**
The file download operation is separated from setting the next-boot-bank and from system reboot. This allows the user to download a new image file but still use the running image after system reboot until he wishes to perform the upgrade.

# Configuration Files

## Overview

Configuration files are human-readable XML files that contain the configurable data of the NPB device. The NPB device allows the user to store a set of configuration files locally. This allows the user an easy and intuitive way to manage his configurations, to perform backup and restore operations, and to move his configuration from one device to another.

Configuration files are created on demand for the NPB or downloaded using a set of file transfer protocols. Once a configuration file is stored locally, it can be renamed, viewed, and deleted.

To apply a configuration file, that is, to make the content of the file the active configuration for the NPB device, use the load and commit commands.

**Note:**
Applying a configuration file replaces the current configuration, that is, if the file contains a configurable element that already exists on the current running configuration, it will replace the running configuration.

## Importing and Exporting Configuration Files

To import a configuration file from the CLI, use the following command:

```
NPB# system config-files import local-file <file-name> remote-url
<url> [username <user-name> password <password>]
```

For example:

```
NPB# system config-files import local-file NPB-config-1 remote-url
scp://192.168.10.10/config/NPB-config-1.xml username admin password
1234
```

To export a configuration file from the CLI, use the following command:

```
NPB# system config-files export local-file <file-name> remote-url
<url> username <user-name> password <password>
```

For example:

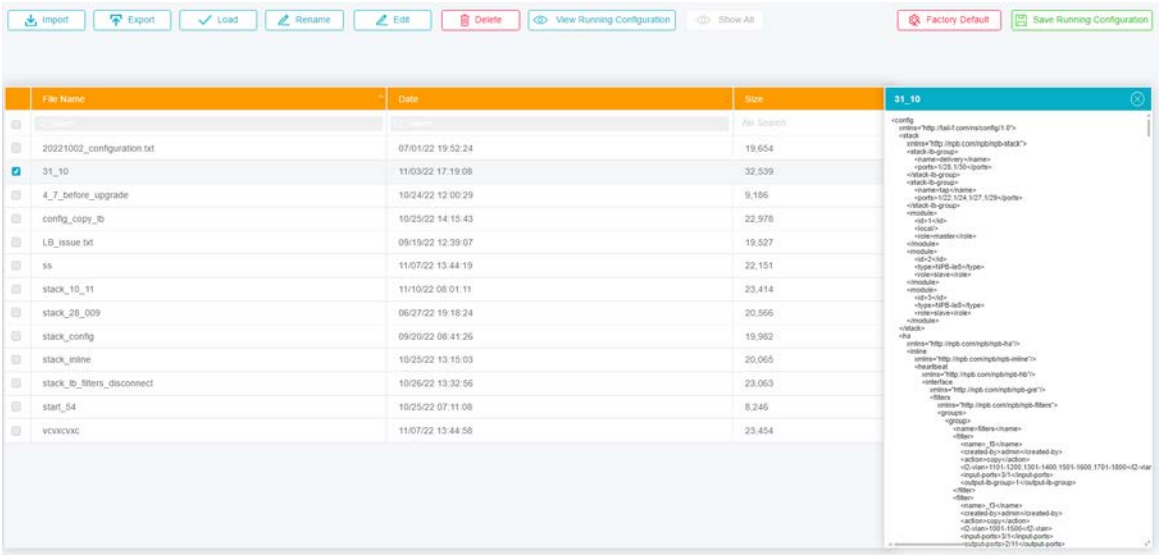
```
NPB# system config-files export local-file NPB-config-1.xml remote-
url scp://192.168.10.10/config/NPB-config-1 username admin password
1234
```

To import or export configuration files using the WebUI, select **Configuration – Files** in the Navigation panel.

To export a file, click its name and click **Export**.

To import a file, click **Import.** In the displayed popup window, enter the file parameters or select a local file. Imported files can be edited using the **Edit** button.

**Figure 32: Importing or Exporting Configuration Files using the WebUI**




**Note:**
The total memory capacity for configuration files is limited. If you have reached this limitation when trying to import, you can delete a locally stored file (as described below) or overwrite it by using its name as the local-file parameter.

## Saving the Currently Running Configuration

To store the current configuration locally in a file from the CLI, use the following command:

```
NPB(config)# system config-files save local-file <file-name>
```

To perform this operation using WebUI, click **Save To File** on the Configuration screen and enter the local file name in the displayed popup window.

**Note:**
The total memory capacity for configuration files is limited. If you have reached this limitation when trying to save, you can delete a locally stored file (as described below) or overwrite it by using its name as the local-file parameter.

## Applying a Configuration File

Applying a configuration file, that is, making its content the running configuration, consists of two operations:

1. First, load the content of the file.
2. After this stage, the configuration changes can be reviewed. If the load is successful and the changes are as required, commit the configuration.

The NPB supports two load methods, replace and merge. When using replace, the content of root level elements in the file replaces the content in the device. When using merge, the content of root level elements in the file is merged with the content in the device. The default method is replace.

To apply configuration file from the CLI, use the following command:

```
NPB(config)# system config-files load local-file <file-name> [merge]
```

To review the configuration changes to be committed from the CLI, use the following command:

```
NPB(config)# show configuration
```

For example, the following flow demonstrates the load and commit of a configuration file that disables NTP:

```
NPB(config)# system config-files load local-file no-ntp.xml
Loading.
6.29 KiB parsed in 0.22 sec (28.37 KiB/sec)
Done.
NPB(config)# show configuration
system time-and-date
 no ntp admin enable
!
NPB(config)# commit
Commit complete.
```

To apply a configuration file using the WebUI, proceed as follows:

1. Select the requested file from the list (its content is displayed on the right) and click **Load**.
2. To review the configuration changes, click **Commit** in the Status panel, and in the appearing Commit Changes Dialog, click **View Changes**. The changes are displayed in a separate window. Closing it brings you back to the Commit Changes dialog.
3. Click **Yes** to commit the changes or **No** to discard the changes.

## Managing Local Configuration Files

Local configuration files can be viewed, renamed, and deleted.

To perform these operations from the CLI, use the following commands:

```
NPB# system config-files rename local-file <file-name> new-name <new-file-name>
NPB# system config-files delete local-file <file-name>
NPB# system config-files view local-file <file-name>
```

To perform these operations from the WebUI, select the file name. The file content is displayed in the viewing panel on the right. Click **Rename** or **Delete** depending on your need.

# System HW Peripherals

## CPU, Memory, and Disk Status

The NPB constantly measures the CPU load, the memory consumption, and the disk usage.

To display these values from the CLI, use the following command:

```
NPB# show system status
```

To display these values from the WebUI, select **System - Status** in the Navigation panel, and click **Performance**.

**Figure 33: Displaying CPU, Memory, and Disk Status using WebUI**


## Transceivers

The NPB device reflects to the user the optical transceivers information as read from the transceivers on-board I2C. This allows the user to review the status and specifications of the transceivers used.

In addition, to detect potential issues, the device periodically monitors the status of the connected transceivers and raises an alarm if an error condition is detected, that is, when the transceivers' temperature, voltage, current, or power have crossed the manufacturer's pre-defined thresholds.

For a complete description of the alarms and traps used, see Section Syslogs on p.65 and Section SNMP Trap on p.206.

To display the transceiver status from the CLI, use the following command:

```
NPB# show transceivers [ddm <id>]
```

To read the transceiver EEPROM from the CLI, use the following command:

```
NPB# transceivers read ddm-id <port-number> address <address> [page
<page-number>]
```

To write the transceiver EEPROM from the CLI, use the following command:

```
NPB# transceivers write ddm-id <port-number> address <address> [page
<page-number>] value <new-value>
```

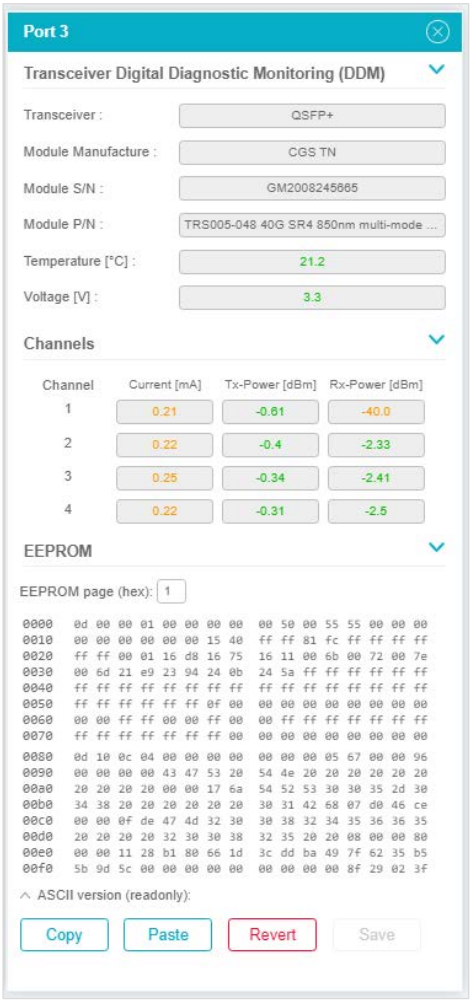
Page number is optional and set to 0 if not given.

EEPROM values are updated periodically. To trigger an update explicitly from the CLI, use the following command:

```
NPB# transceivers scan
```

To manage the transceivers using WebUI, select **Ports - Transceivers** in the Navigation panel. Click any transceiver in the list to open its extension panel.

**Figure 34: Transceivers Extension Panel**



## Other HW Components

The NPB device contains a set of swappable PSU panels, a set of fan panels, and a set of on-board temperature sensors.

The status of these components can be displayed. In addition, to detect potential issues, the device periodically monitors the status of these components and raises an alarm if an error condition is detected, for example, if the temperature crossed a pre-defined threshold.

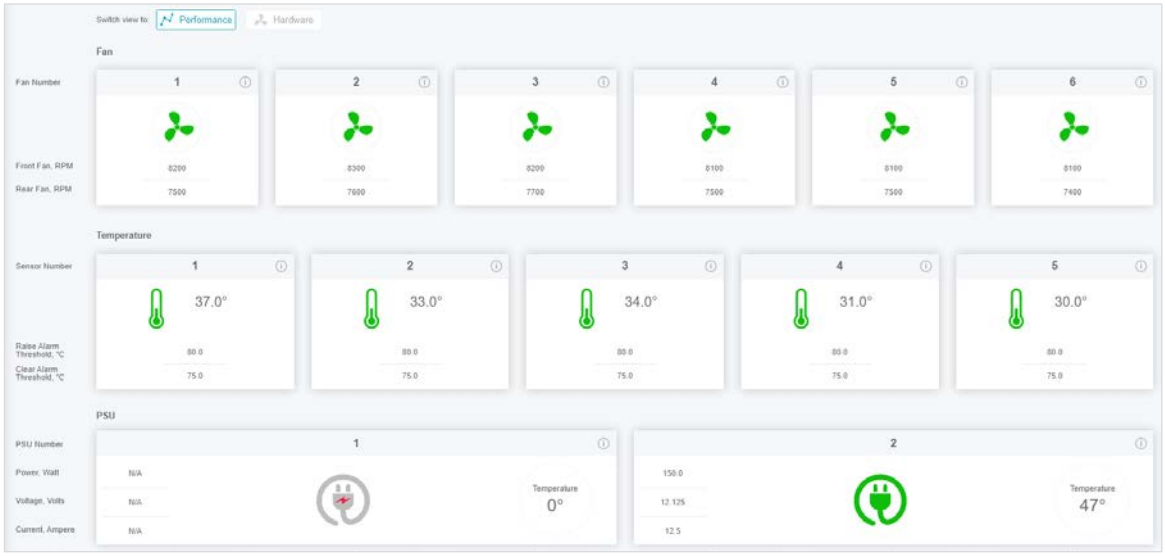
For a complete description of the alarms and traps used, see Section Syslogs on p.65 and Section SNMP Trap on p.206.

To display the HW components status from the CLI, use the following command:

```
NPB# show system hw-status [fan|psu|temperature-sensors]
```

To display the HW components status using the WebUI, select **System – Status** in the Navigation panel, and click **Hardware**. Additional information for each component is displayed when hovering over the Info symbol:

**Figure 35: Displaying HW Components Status using the WebUI**




### Troubleshooting HW Failures

The NPB device detects HW failures as listed in Table 13. Meaning and possible solutions are listed for each error condition.

**Table 13: Troubleshooting HW Components**

| Error Condition | Meaning | Possible Solution |
|---|---|---|
| Fan not present | Fan module has been removed or stopped functioning. | Replace/install fan module. |
| Fan status failure | Fan is not functioning. | Make sure that the fan can rotate freely. Replace fan module if needed. |

| Error Condition | Meaning | Possible Solution |
|---|---|---|
| PSU not present | PSU module has been removed. | The device can function with only one PSU present (without power redundancy).<br>For power redundancy, install a second PSU and connected it to an external AC power source. |
| PSU bad power | PSU is not connected to a power source or is not functioning. | Connect PSU to an external AC power source.<br>Replace/install PSU module if needed. |
| PSU bad temperature | PSU temperature is high due to a PSU internal fan issue. | Disconnect/replace/install the PSU module. |
| High temperature alarm | The temperature sensors detect high temperature (above 80°C). | Make sure that the fans are working. Replace malfunctioning fan modules as needed. Make sure the device is installed in a properly ventilated area. Alarm will be cleared when the temperature drops under 75°C. |

### Location LED

The Location (LOC) LED is located on the front panel. It can be used to easily locate the physical device on the rack.

To turn the Location LED on, off or to make it blink from the CLI, use the following command:

```
NPB(config)# system hw location-led on|off|[blink]
```

**Note:**
NPB IV does not have a Location LED.

# Logs, Alarms, and Debug Reports

The NPB device supports various logging capabilities to allow the user an easy way to monitor and audit the device operation. In addition, the device supports the generation of debug reports that can be used to trace down issues. All the information logged in memory is protected against memory exhaustion by file rotation.

## Syslogs

The NPB device is fully compliant with the Syslog standard, allowing the user to set local files, local users, and remote servers as logging destinations. The logs to be send to each destination are defined according to the standard Syslog severity and facilities. Local Syslogs files are rotated over time.

Configuring Syslog from the CLI consists of two steps:

1. Define a rule for every remote-server, local user or local file destination.
2. Add a set of selectors to each rule. The selector defines the set of severities and facilities to be logged by the rule.

To configure a Syslog rule for a remote server, local file, or lists of local users respectively, use the following command:

```
NPB(config)# system syslog rule <rule-name> action type remote-
machine remote-machine-settings name < server-name-or-ip> port
<remote-server-port> transport TCP|UDP|RELP

NPB(config)# system syslog rule <rule-name> action type local-file
local-file-settings immediate-sync true|false

NPB(config)# system syslog rule <rule-name> action type local-user
local-user-settings users <list-of-users>
```

To add a selector to a rule from the CLI, use the following command:

```
NPB(config-rule-1)# selectors <selector-id> facility-list <list of
facilities> priority <priority> [comparison same|same_or_higher]
[ignore true|false]
```

where <list of facilities> and <priority> are according to the standard Syslog definitions:

| | |
|---|---|
| Possible facilities | all, auth, authpriv, cron, daemon, ftp, kern, local0, local1, local2, local3, local4, local5, local6, local7, lpr, mail, news, security, syslog, user, uucp |
| Possible priorities | all, emerg, alert, crit, err, warning, notice, info, debug, none |

**`ignore`** parameters can be used for inversed selection, that is, to ignore a given list and to log everything else.

If the **`comparison`** parameter is set to **`same`**, only the specified priority will be logged. If it is set to **`same_or_higher`** (which is the default), the specified priority and all higher priorities will be logged.

As an example, let's assume we want to define the following Syslog configuration:

- Send all Syslogs of priority **`critical`** (but not any other priority) that occurred in all facilities to this remote server: IP = 192.168.10.10 through Port 514 using UDP protocol.
- Send all Syslogs of priority **`error`** or above for the facilities: kern, security and auth to this remote server: IP = 192.168.10.20 through Port 601 using TCP protocol.
- Log locally all Syslogs with priority **`critical`** and above from all facilities and all Syslogs with priority **`warning`** from facility kern. Note that for this configuration, we need two selectors.

In CLI, this will look as follows:

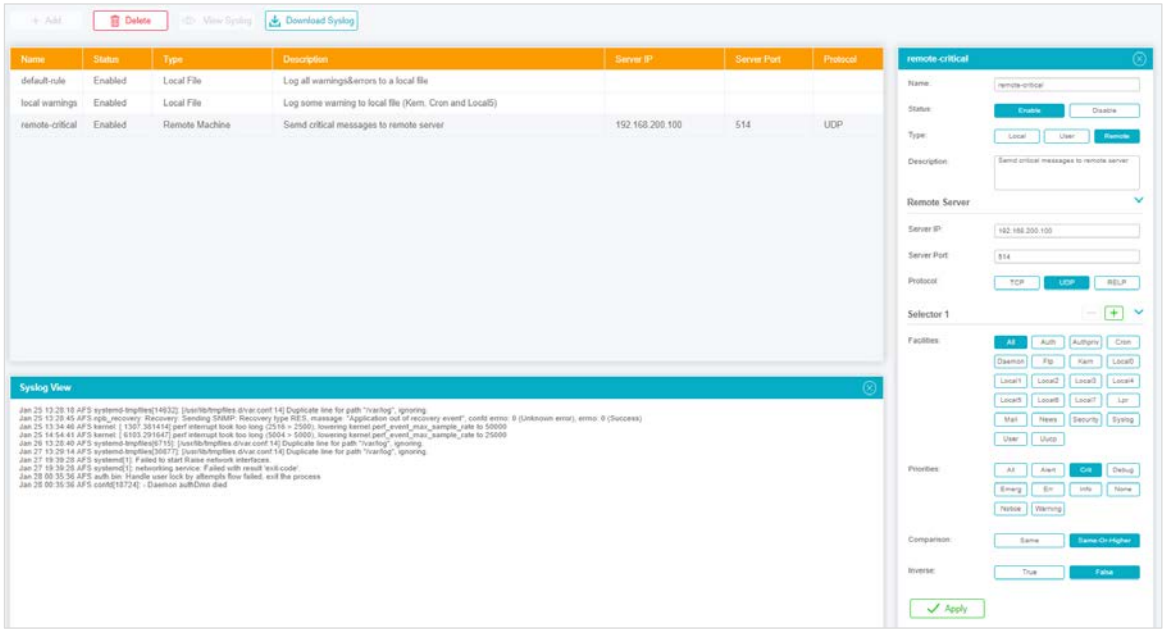
```
NPB(config)# system syslog rule remote-crit action type remote-
machine remote-machine-settings name 192.168.10.10 port 514 transport
UDP
NPB(config-rule-remote-crit)# selectors 1
NPB(config-rule-remote-crit)# selectors 1 facility-list all priority
crit comparison same

NPB(config)# system syslog rule remote-err action type remote-machine
remote-machine-settings name 192.168.10.20 port 601 transport TCP
NPB(config-rule-remote-err)# selectors 1 facility-list kern priority
err
NPB(config-selectors-1)# facility-list auth
NPB(config-selectors-1)# facility-list security

NPB(config)# system syslog rule local-rule action type local-file
NPB(config-rule-local-rule)# selectors 1 facility-list all priority
crit
NPB(config-rule-local-rule)# selectors 2 facility-list kern priority
err comparison same_or_higher
```

To display the content of the local Syslog file from the CLI, use the following command:

```
NPB# show syslog dump|head <lines>|last <lines>|tail
```

To manage Syslog rules using the WebUI, select **System – Syslog** in the Navigation panel. Current rules are shown in a table.

**Figure 36: Managing Syslog Rules using the WebUI**




To edit an existing rule, click the line in the table and change configurations in the extension panel as required.

To add a new rule, click **Add** to add a line to the table, then click the line, configure the new rule in the extension panel, and click **+Create** to apply your configuration.

Using the Rules extension panel on the right, you can perform the following actions:

- Select the rule type
- Enter remote server details if needed
- Set the selectors. Selectors can be added or removed by clicking the **+** or **-** buttons.

To display the content of the local syslog file, click **View Syslog**.

To download the content of the local syslog file, click **Download Syslog**.

## Alarms

The NPB generates alarms in case of noteworthy events or if it detects an error condition. The alarms are forwarded to the Syslog daemon and are logged according to the Syslog configuration. They are also sent as an SNMP trap if an SNMP trap server was configured.

This section describes the Syslog format and functionality of the alarms. For a list of the supported alarms and for a description of the SNMP traps, see Section SNMP on p. 205.

The NPB alarms can be "stateful" or "stateless":

- A stateful alarm indicates an error condition that may be cleared later. An example is the high-temperature alarm that can be cleared when the temperature drops.
- A stateless alarm indicates an event that is not considered an error and therefore will not be cleared. An example is a **`link up`** event on one of the ports.

The format of alarm messages is defined as follows:

- Each alarm has a unique ID.
- The alarm Syslog message has the following format:

  ID: <id>, <Module>, <Severity>, <Type>, <Message>

  Where:

  | | |
  |---|---|
  | <id> | is a unique alarm ID |
  | <Module> | states the system module that reported the alarm: PORT, HW, BCM, FLTR, SYS |
  | <Severity> | states the Syslog severity of the alarm message: INFO, MIN, MJR, CRIT |
  | <Type> | is one of the following strings: ACT (Active), RES (Resolved), EVT (Event) |
  | <Message> | is a free text containing the alarm's details |

- Alarms Syslog messages use the facility **`Local-0`**.
- Stateful alarms contain 2 messages: one with type ACT for raising the alarm and one with type RES for clearing the alarm. These messages have the same unique ID.
- State-less alarms contain one message of type EVT.

**Note:**
To filter Syslog alarms and forward them to a remote server, use the Syslog facility **`Local-0`** and the Syslog severity you wish to filter when configuring a Syslog rule.
See Section Syslogs on p.65 for more info on Syslog rules.

The following example shows a stateless message that the link status of Port 3 has changed to down:

```
ID: 102, PORT, INFO, EVT, Port: 3 link status is down
```

### Alarm Operations

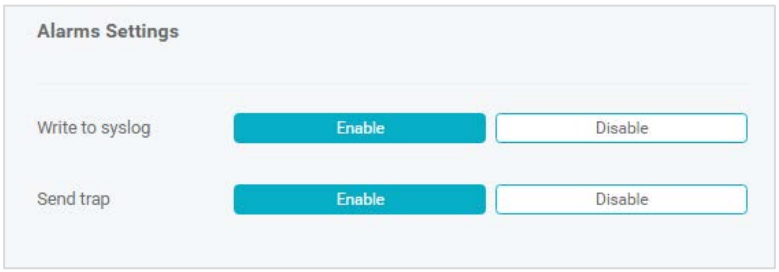
The user can control if NPB alarms are distributed as Syslog messages, SNMP traps, both, or none.

To set alarms distribution methods from the CLI, use the following command:

```
NPB(config)# system alarms syslog|trap enabled|disabled
```

To set alarm distribution methods using the WebUI, select **Management – General settings** in the Navigation panel. Alarms settings are on the right:

**Figure 37: Setting Alarm Distribution Methods using the WebUI**




The NPB device keeps track of the last 512 alarms and events in the alarm history list.

To view the alarm history list sorted according to last update time from the CLI, use the following command:

```
NPB# show system alarms | sort-by last-updated
```

It is possible to clear all non-active alarms (that is, alarms that have been resolved and events) from the history list. It is also possible to regenerate all active alarms (alarms that were not resolved yet) in the history list. This is useful when a new trap server is to be propagated with the current NPB active alarms.

To clear non-active alarms from the alarm history list from the CLI, use the following command:

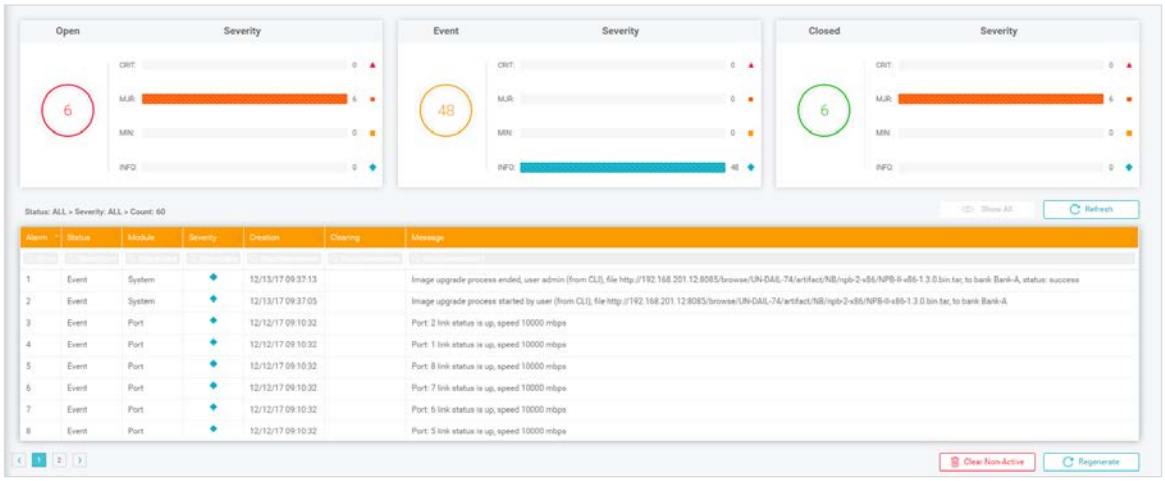
```
NPB# system alarms clear
```

To regenerate all active alarms in the alarm history list from the CLI, use the following command:

```
NPB# system alarms regenerate
```

To view and manage alarms using the WebUI, select **System – Alarms** in the Navigation panel. This page displays the current alarm history.

**Figure 38: Viewing and Managing Alarms using the WebUI**



Alarms can be filtered according to status and severity. For example:

To view only closed alarms, click the green circle in the panel marked **Closed** on the right.

To view only closed alarms of Major severity, click the **MAJ** bar in this panel.

The current display filter is shown above the list, e.g. "Status: CLOSED > Severity: MJR > Count: 28"

**Note:**
Filtering according to severity is possible only within alarms of the same status, not for alarms with a different status.

To view all alarms, click **Show All Alarms**.

To clear non-active alarms from the alarm history list, click **Clear Non-Active**.

To regenerate all active alarms in the alarm history list, click **Regenerate**.

## Audit Logs

The NPB device can maintain an auditing log containing information regarding users logging and configuration changes. Audit messaging uses the syslog logging mechanism. Messages can be saved locally and remotely, using a remote syslog server. See Section Syslogs on p.65 for more details about syslog configuration. Auditing is disabled by default.

To enable or disable auditing from the CLI, use the following command:

```
NPB# system audit enabled|disabled
```

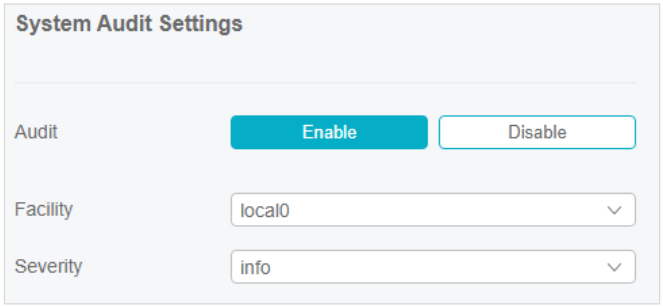
By default, auditing messages use the local0 facility and info severity.

To set auditing messages severity and facility from the CLI, use the following command:

```
NPB# system audit syslog facility <facility> severity <severity>
```

To configure auditing from the WebUI, select **Management – General settings** from the Navigation panel.

**Figure 39: System Audit Settings**



## Local Logs and Debug Reports

The NPB device logs information during its operations. This logged data can be used to monitor and audit the device as well as a source of information for tracing issues. The device can work in two pre-defined profiles that dictate the type and amount of data being collected:

- Use the Normal profile for regular operation, when trying to track down an issue.
- Use the Debug profile when more detailed information is needed.

Using the Debug profile does not affect the device's functionality and performance, but may slow down management operations. In addition, since there is a limitation on the total amount of memory consumed by the log files, using the Debug profile will exhaust the memory much faster, thus rotating the files more frequently. Therefore, it is best to use Debug mode for a limited time only.

Debug reports are used for collecting all log files and uploading them to a remote server. Optionally, the files can be encrypted prior to being transferred.

To set a log profile from CLI:

```
NPB(config)# system log level [debug|normal]
```

To generate a debug report from the CLI, use the following command:

```
NPB# system tools generate-debug-report local-file <local-file-name>
[recovery-info] [confd-detailed] remote-url <remote-url> [username
<user-name> password <password>] [encrypt-pwd <password-for-
encrypting-report>]
```

The **`recovery-info`** and **`confd-detailed`** parameters are optional. If present, the last system-recovery info and the management engine logs are added to the report. If the encryption option is used, the report includes the CLI history.

To clear all locally stored logs from the CLI, use the following command:

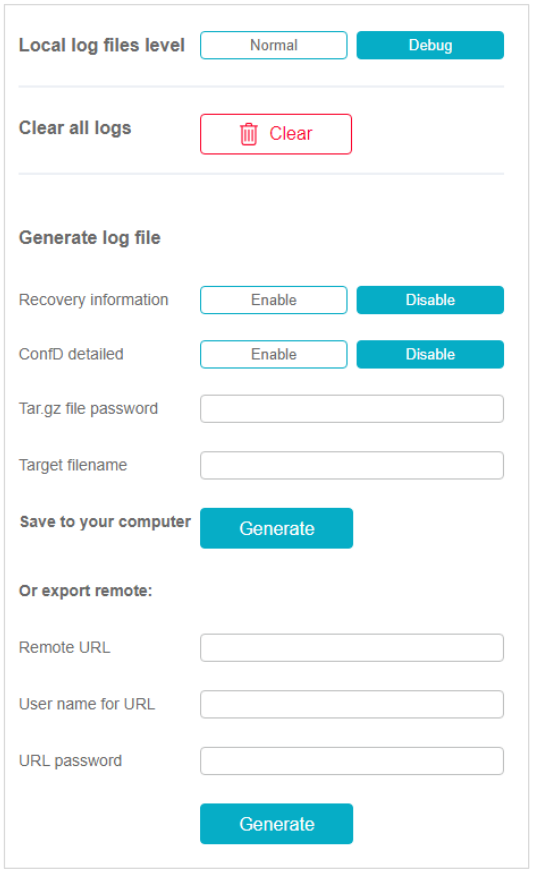
```
NPB# system log clear
```

To clear all locally stored logs and other debug information from the CLI, use the following command:

```
NPB# system log clear all
```

To set a log profile, to delete all logs, and to generate a debug report using the WebUI, select **Management – Tools** in the Navigation panel. The log profile settings are in the center of the page. The debug report generation settings are below it.

**Figure 40: Setting a Log Profile and Generating a Debug Report using the WebUI**




**Note:**
Only users with **admin** permissions can apply these operations. Refer to Section Users on p.147 for more details.

# Additional System Operations

## Viewing System Details

The NPB can display various system details, such as device model and serial number, SW and HW versions, and system uptime.

To view the system details from the CLI, use the following command:

```
NPB# show system details
```

To view the system details using the WebUI, go to **System – Details** in the Navigation panel.

## System Reboot

It is possible to reboot the system at any given time. The running configuration will still be used after reboot. The system will boot from the image present in the memory bank defined as **`next-boot bank`**.

To reboot the system from the CLI, use the following command:

```
NPB# system reboot
```

To reboot the system using the WebUI, click **Reboot** on the Configuration screen.

## Restore Factory Default

It is possible to restore the device's factory defaults, that is, to delete all information entered by the user and all logged data. To preserve connectivity to the device, the management interface's settings are kept.

To restore factory default from the CLI, use the following command:

```
NPB(config)# system factory-default
```

To restore factory default using the WebUI, click **Factory Default** on the Configuration screen.

**Note:**
The factory-default command will take affect after system reboot. It is **highly recommended** to reboot the system prior to any other change because any changes performed after this command will be lost.

## System Hostname and Description

It is possible to change the system's host name and description. The system host name is reflected in the CLI prompt in the next CLI session.

To change the host name from the CLI, use the following command:

```
NPB(config)# system details hostname <new-name>
```

To change the description from the CLI, use the following command:

```
NPB(config)# system details description <description>
```

To change the system host name and description using the WebUI, go to **System – Details** in the Navigation panel.

## Ping

The device supports sending ICMP ping using the management interface to check network connectivity.

To use ping from the CLI, use the following command:

```
NPB# system tools ping <ip> count <num-of-message> size <size-of-each-message>
```

To use ping using the WebUI, go to **Management – Tools** in the Navigation panel. Enter the required parameters and click **Send**. The output is displayed on the right.

To stop the Ping process, click **Stop**.

**Figure 41: Start Ping using the WebUI**

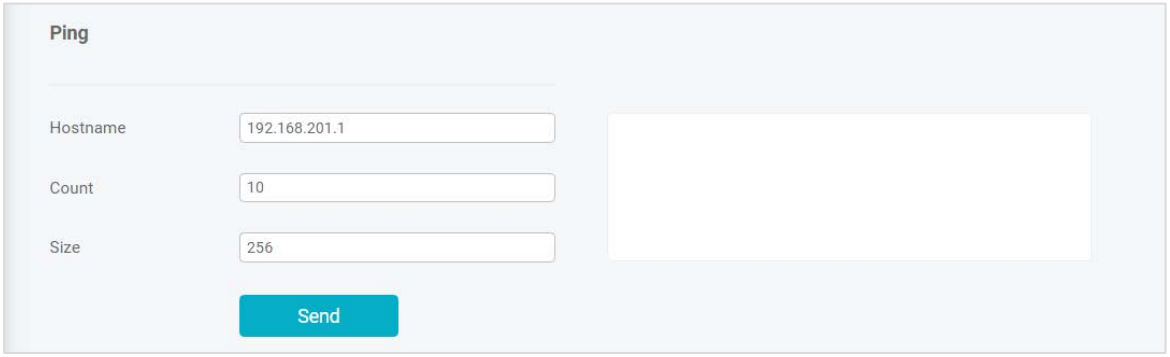
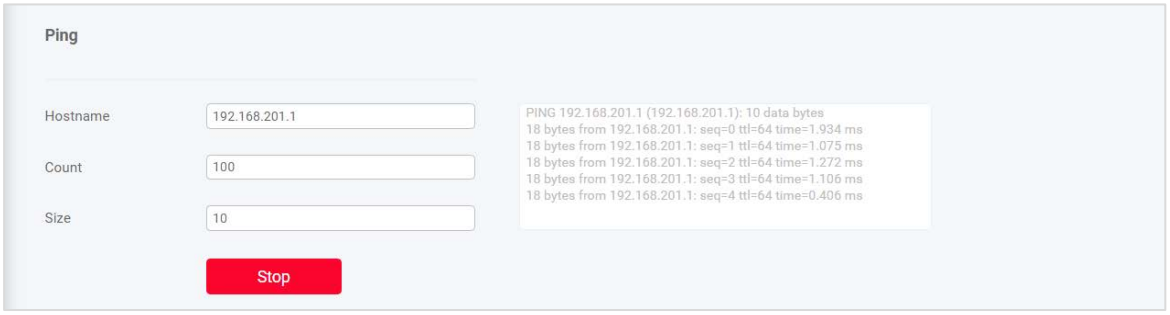



**Figure 42: Stop Ping using the WebUI**



# Port Configuration and Actions

## Overview

The NPB devices contain a set of physical ports as described below:

| | |
|---|---|
| NPB I | A total of 54 ports:<br>• 48 SFP+ ports, each supporting 10M/100M/1000M copper or 1 GbE/2.5 GbE/10 GbE<br>• 6 QSFP ports, each supporting 1 GbE/2.5 GbE/10 GbE/40 GbE or 4x1 GbE/4x2.5 GbE/4x10 GbE |
| NPB Ie | A total of 54 ports:<br>• 48 SFP+ ports, each supporting 10M/100M/1000M copper or 1 GbE/2.5 GbE/10 GbE<br>• 6 QSFP28 ports, each supporting 1 GbE/10 GbE/40 GbE/ 50 GbE/100 GbE or 2x50GbE/4x1 GbE/4x10 GbE/4x25 GbE |
| NPB Ie8 | A total of 56 ports:<br>• 48 SFP28 ports, each supporting 1G/10G copper, or 1 GbE/10 GbE/25 GbE<br>• 8 QSFP28 ports, each supporting 1 GbE/10 GbE/25 GbE/40 GbE/ 50 GbE/100 GbE or 2x50 GbE/4x1 GbE/4x10 GbE/4x25 GbE |
| NPB II | A total of 32 QSFP28 ports, each supporting 1GbE/10 GbE/25 GbE/40 GbE/ 100 GbE or 4x1 GbE/4x10 GbE/4x25 GbE |
| NPB IIe | A total of 32 QSFP28 ports, each supporting 1 GbE/10 GbE/25 GbE/40 GbE/ 50 GbE/100 GbE, or 2x50 GbE/4x1 GbE/4x10 GbE/4x25 GbE |
| NPB III | A total of 32 QSFP28/QSFP-DD ports, each supporting 10 GbE/25 GbE/ 40 GbE/50 GbE/100 GbE/200 GbE/400 GbE or 2x40 GbE/2x100 GbE/4x10 GbE/4x25 GbE/4x50 GbE/4x100 GbE |
| NPB IV | A total of 40 QSFP28 ports, each supporting 40 GbE/100 GbE, or 20 QSFP28 ports, each supporting 4x10 GbE/4x25 GbE |

By default, the ports admin status is set to **`disable`**, and the speed is set to 10G. Some physical ports can be split into several logical ports each as described below. The device collects traffic statistics and utilization statistics on all of its ports constantly. The user can configure the device to raise an alarm and to send an SNMP trap if a utilization threshold has been crossed (or cleared).

### Numbering Scheme

The NPB ports numbering scheme is straightforward and follows the front-panel numbering. For NPB IV, some limitations apply – see Section NPB IV Ports Numbering on p.77.

NPB ports can be of two types:

- QSFP+/QSFP28/QSFP-DD ports can either function as one logical port or be split into two or four logical ports. This operation is called **`port breakout`**.
- SFP+ ports can only function as one logical port.

Port numbering for QSFP+/QSFP28/QSFP-DD ports that function as one logical port and for SFP ports is identical to the front-panel numbering.

Port numbering for QSFP+/QSFP28 ports that were split into two or four logical ports consists of 2 parts:

<physical-port-id>/<logical-port-id>

For example, after splitting QSFP Port 4 into four logical ports, the existing IDs of the logical ports will be:

4/1, 4/2, 4/3, 4/4

Note that there will be no "Port 4" in this situation.

After merging the four logical ports back into one port, the single existing port ID will be 4.

Following the description above, the NPB port numbering schemes are as follows:

- For NPB I:

  1,2,3 … 48, 49[/1, /2, /3, /4] … 54[/1, /2, /3, /4]

  This means: Ports 1 to 48 cannot be split into several logical ports. Ports 49 to 54 can optionally be split into four logical ports.

- For NPB Ie:

  1,2,3 … 48, 49[/1, /2[, /3, /4]] … 54[/1, /2[, /3, /4]]

  This means: Ports 1 to 48 cannot be split into several logical ports. Ports 49 to 54 can optionally be split into two or four logical ports.

- For NPB Ie8:

  1,2,3 … 48, 49[/1, /2[, /3, /4]] … 56[/1, /2[, /3, /4]]

  This means: Ports 1 to 48 cannot be split into several logical ports. Ports 49 to 56 can optionally be split into two or four logical ports.

- For NPB II, NPB IIe, and NPB III:

  1[/1, /2[, /3, /4]] … 32[/1, /2[, /3, /4]]

  This means: All ports (1 to 32) can optionally be split into two (NPB IIe only) or four logical ports.

- For NPB IV:

  1[/1, /2, /3, /4] … 20[/1, /2, /3, /4], 21, 22 … 40

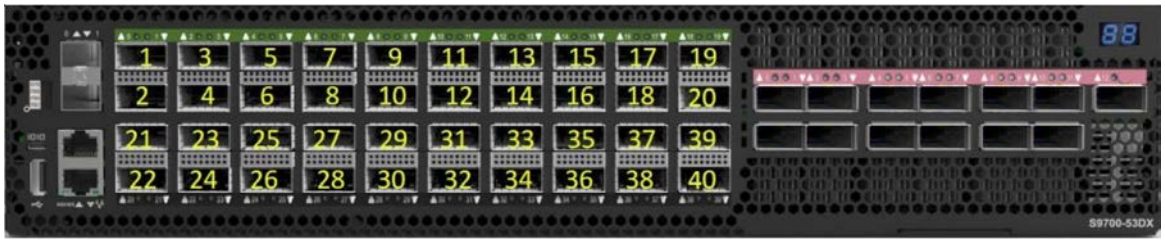
This means: The first 20 ports can optionally be split into four logical ports, see Section NPB IV Ports Numbering on p.77.The Breakout operation is described in detail later in this chapter.

### NPB IV Ports Numbering

In NPB IV, the following limitations apply:

- Front panel numbering is different from the system numbering:
  While the front panel numbering starts with 0, the system numbering starts with 1 like in other NPB devices. Therefore, System Port 1 is marked on the front panel as Port 0, System Port 2 is marked as Port 1 and so forth. See Figure 43 below.
- Ports in the same column (e.g., ports 3, 4, 23, and 24) must be configured to use two speed values out of the following options: 40 Gbps (either as 1x40 or 4x10), 4x25 Gbps, or 100 Gbps.
- Configuring a breakout on a port in the 1st or 2nd rows (ports 1-20) disables the matching port in the same column in the 4th or 3rd rows respectively. For example, configuring breakout on Port 1 (1st row) disables Port 22 (4th row), configuring breakout on Port 14 (2nd row) disables Port 33 (3rd row).

**Figure 43: NPB IV System Port Numbering**




# Port Configuration

## General

The NPB device allows the user to configure many of the port attributes, as shown below:

**Table 14: Port Attributes**

| Name | Description | Possible Values |
|---|---|---|
| port-name | Port's name | Free text (max. 48 characters) |
| description | Port's description, when loopback mode is not **`simplex`** | Free text (max. 140 characters) |
| tx-description | Port's Tx description when loopback mode is **`simplex`** | Free text (max. 140 characters) |
| rx-description | Port's Rx description when loopback mode is **`simplex`** | Free text (max. 140 characters) |
| admin | Administrative status | Enable/disable |

| Name | Description | Possible Values |
|---|---|---|
| tx-laser | Sets the transmitter laser status in the fiber connectors | on/off<br>Default is **on**. |
| fec | Port's FEC setting,<br>Configuration must match the far-end FEC setting. | disable – Disable FEC<br>enable – Use standard FEC algorithm (FC and RS clause 74)<br>cl91 – Use RS clause 91 FEC algorithm<br>cl108 – Use RS clause 108 FEC algorithm<br>RS 272 – Use Reed-Solomon 272 FEC algorithm<br>RS 544 – Use Reed-Solomon 544 FEC algorithm<br>RS 544 2xN – Use Reed-Solomon 544 2xN FEC algorithm<br><br>Default is **`disable`**.<br>Refer to Forward Error Correction (FEC) Support on p.81 |
| txfir | Set the port Tx Finite Impulse Response values (Pre-emphasis) | Refer to Pre-emphasis (NPB III) on p.83 |
| controlled ports | Sets the current port as monitor and defines its control ports | Refer to Section Link Propagation on p.84 |
| prbs | Port's PRBS setting | Refer to Section Pseudo Random Binary Sequence (PRBS) on p.85 |
| mode | Port's loopback mode | Refer to Section Port Loopback Options on p.84 |
| speed | Port's configured speed | 10M / 100M / 1G / 2.5G / 10G / 25G / 40G / 50G / 100G / 200G / 400G<br>The set of valid speed values depends on the port type and its breakout status |
| line-code | Port's line code, valid only in NPB III for 4x50G, 50G, and 100G speeds. | nrz (No-Return-to-Zero)<br>pam4 (Pulse-Amplitude Modulation-4)<br>Default is **`nrz`**<br>Refer to Section Port Breakout on p.88 |
| copper-autoneg | Port's auto negotiation setting. Applicable for copper transceivers only (NPB I, NPB Ie, NPB Ie8) | Enable/disable<br>Default is **`disable`** |

| Name | Description | Possible Values |
|---|---|---|
| copper-duplex | Port's duplex setting. Applicable for copper transceivers only (NPB I, NPB Ie, NPB Ie8) | Half/full<br>Default is **`full`** |
| double-tag | Set the behavior of double tagged traffic handled by the port (ingress and egress) | Refer to Managing Tagged Traffic on p.90 |
| egress-action | Action to take on egress traffic | Refer to VLAN Tagging Actions on p.91 |
| ingress-action | Action to take on ingress traffic | Refer to VLAN Tagging Actions on p.91 |
| vlan | VLAN tag to use according to action | Refer to VLAN Tagging Actions on p.91 |
| mpls-remove | Sets the MPLS labels removal mode | Refer to MPLS Stripping (NPB Ie, Ie8 and IIe only) on p.95 |
| Rx and Tx timestamp | Adds a timestamp trailer | Refer to Timestamping (NPB Ie8 and NPB IIe) on p.88 |
| utilization-alerts | Port's utilization alerts settings | Refer to Port Utilization on p.98 |

To change the port configuration from the CLI, use the following command:

```
NPB(config)# ports port <port-id> <parameter> <value> ...
```

For example:

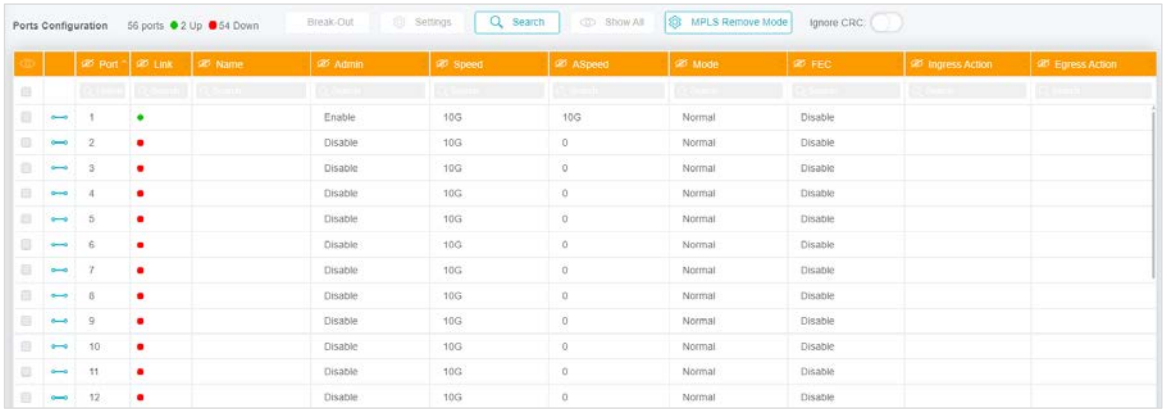
```
NPB(config)# ports port 1 admin enable fec enable
```

To display the port configuration from the CLI, use the following command:

```
NPB# show ports [port <port-id>]
```

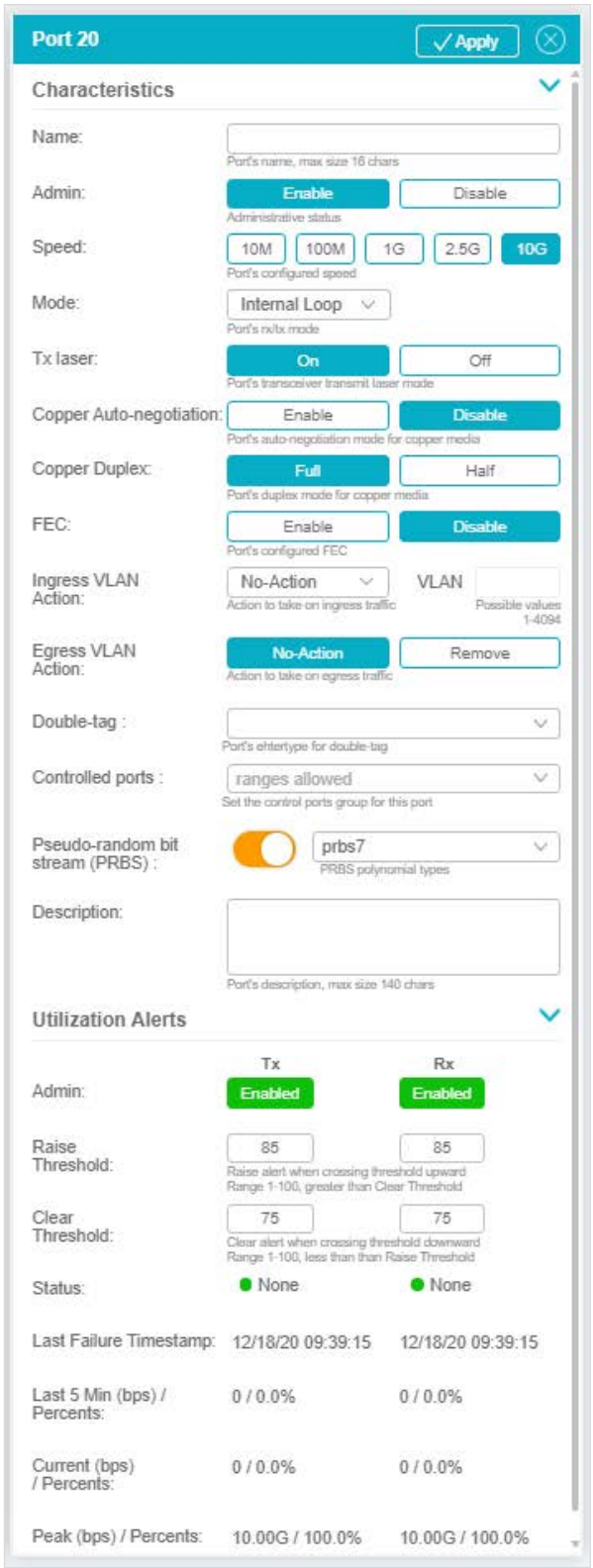
To view and configure port settings using the WebUI, select **Ports – Configuration** in the Navigation panel. The main table displays all available ports along with their basic attributes.

**Figure 44: Viewing and Configuring Port Settings using the WebUI**



To view more attributes or to configure a specific port, click one of the lines, and use the extension panel on the right to view and set ports parameters. To configure multiple lines, click the checkboxes next to the lines you want to edit, and click the **Settings** button above the table.

**Figure 45: Advanced Configuration using the Extension Panel**



## Forward Error Correction (FEC) Support

The NPB devices support several FEC algorithms that can be configured per port. Table 15 specifies the FEC support in each speed per device.

**Table 15: FEC Support per Device**

| Device | Clause74 (Enabled) | Clause91 | Clause108 | RS-272 | RS-544 | RS-544-2XN |
|---|---|---|---|---|---|---|
| NPB I | 1,2.5,10,40 | | | | | |
| NPB Ie | 1, 2.5,10,25,40, 50,100 | 100 | | | | |
| NPB Ie8 | 1,10,25,40,50,100 | 40,50,100 | 25* | | | |
| NPB II | 1,10,25,40,100 | 100 | | | | |
| NPB IIe | 1,10,25,40,50,100 | 40,50,100 | 25* | | | |
| NPB III | 10,25,40 | 25*,50,100 | | 200 | 50,100,200 | 400 |
| NPB IV# | 10,25,100 | 100 | 25 | | | |

* When using 25G speed, NPB Ie8 and NPB IIe using Clause 108 are interoperable with NPB III using Clause91.

# All ports in the same column must use the same FEC value.

## Ignoring Bad CRC

By default, the NPB drops packets that were received with a bad CRC. This behavior can be changed so that the CRC is ignored. Note that in this case, CRC is not re-calculated for transmitted packets, so modified packets are sent with their original (now wrong) CRC.

To set ignoring bad CRC behavior from the CLI, use the following command:

```
NPB(config)# ports [no] ignore-crc
```

To set ignoring bad CRC behavior from the WebUI, select **Ports – Configuration** in the Navigation panel and click **Ignore CRC** above the table.

## Port Groups

The NPB allows the user to group ports into logical groups and use these groups wherever ports can be used, for example in filters and load balancing definitions.

Collecting similar entities into groups makes the system configuration less error-prone and easier to maintain as modifications are done on the group (e.g. adding or removing ports) instead of all the places where its members are used.

To create a group from the CLI, use the following command:

```
NPB(config)# ports group <group-name> ports <group-members>
[description <description>]
```

For example:

```
NPB(config)# ports group Firewall-ports ports 1,2,3-6 description
"the set of ports connected to the firewall"
```

To delete a group from the CLI, use the following command:

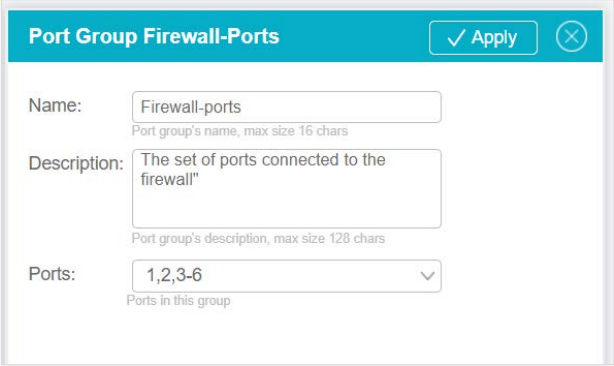
```
NPB(config)# no ports group <group-name>
```

To use the group from the CLI, just insert its name wherever a port ID is expected. It can be combined with other ports. The following example uses the Firewall-ports from the example above as a part of a filter's input ports classifier:

```
NPB(config)# filters filter f1 input-ports 10,12,Firewall-ports,20-21
```

To manage groups using the WebUI, select **Ports – Ports Groups** in the Navigation panel. Click an existing group to update it, or click **Add** to add a new one. Set the relevant parameters in the extension panel.

**Figure 46: Port Group Extension Panel**




The groups will be available in WebUI fields where a port is required.

## NPB Ie8 Speed Limitation

In NPB Ie8, Ports 1 to 48 are grouped into groups of four ports each. The speed of all ports in the same group must be either 25G or a mix of non-25G speeds (e.g. 1G or 10G).

The grouping of the ports is listed below.

**Table 16: Grouping of Ports in NPB Ie8**

| | | |
|---|---|---|
| 1, 2, 3, 6 | 16, 17, 19, 21 | 32, 34, 35, 36 |
| 4, 5, 7, 9 | 20, 22, 23, 24 | 37, 38, 39, 42 |
| 8, 10, 11, 12 | 25, 26, 27, 30 | 40, 41, 43, 45 |
| 13, 14, 15, 18 | 28, 29, 31, 33 | 44, 46, 47, 48 |

The following CLI command displays the port groups:

```
NPB-Ie8# show ports phy-info
```

To view port grouping using the WebUI, select **Ports – PHY info** in the Navigation Panel.

## Pre-emphasis (NPB III)

In NPB III, it is possible to shape the electrical signal by configuring the pre-emphasis coefficients per speed.

To set pre-emphasis coefficients from the CLI, use the following command:

```
NPB(config)# ports port <id> txfir 4x100|100G|200G|400G <lane-id>
main|post|pre coeff <coefficient-value>
```

Where **`lane-id`** is in the range 0-7, and **`coefficient-value`** is in the range -256-+256.

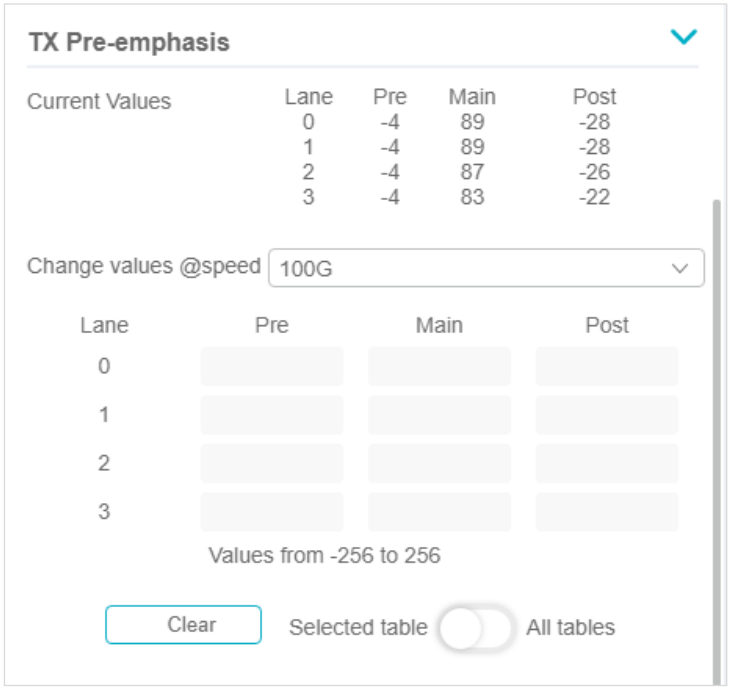
To reset pre-emphasis coefficients to their default values from the CLI, use the following command:

```
NPB(config)# ports port <id> no txfir 4x100|100G|200G|400G <lane-id>
main|post|pre
```

Where **`lane-id`** is in the range 0-7, and **`coefficient-value`** is in the range -256-+256.

To set pre-emphasis coefficients from the WebUI, select **Ports – Configuration** in the Navigation panel. Click one of the ports, and use the extension panel.

**Figure 47: Pre-emphasis**



## Link Propagation

The NPB device supports link propagation by logically pairing a control and a monitored port, whenever the link status of the monitored port is changed. This change is propagated to the control port. A monitor port can be paired to several control ports. In this case, link changes are propagated to all control ports.

When a control port link is down due to a monitored link being down, its link status is displayed as **`forced down`**.

To set link propagation from the CLI, use the following command:

```
NPB(config)# ports port <monitor-port-id> set-controlled-ports
<controlled ports>
```

For example, to set Port 1 as a monitor port with Ports 2, 3, 4, and 10 as its control ports:

```
NPB(config)# ports port 1 set-controlled-ports 2-4,10
```

To unset link propagation from the CLI, use the following command:

```
NPB(config)# ports port <monitor-port-id> no set-controlled-ports
```

To set link propagation from the WebUI, fill the **Controlled Port** field in the monitor port's extension panel.

## Port Loopback Options

Each port can be set to work in one of several supported loopback modes. This is handy when a port is used to manipulate traffic internally without sending the traffic externally or to enable Tx connectivity regardless of the Rx status (simplex). The supported loopback modes are listed in Table 17.

**Table 17: Loopback Options**

| Option Name | Description |
|---|---|
| loopback-MAC | Loopback of outgoing Tx back to Rx in the MAC parallel interface |
| loopback-internal | Loopback of outgoing Tx back to Rx in the PHY serial interface (not supported in NPB III) |
| loopback-external | Loopback of incoming Rx to Tx without any processing (not supported in NPB Ie8, IIe, and III) |
| simplex | Forces link up regardless of Rx connectivity<br>Use this state when connecting only Tx link to the port or when Tx and Rx are connected to different devices |
| normal (default) | Regular full duplex link |

Note that both MAC and internal loopback modes redirect ***outgoing*** traffic back to the device, each at a different place. This can be used to trace down packet error issues. The traffic reenters the device and is processed normally as if it was received from the network.

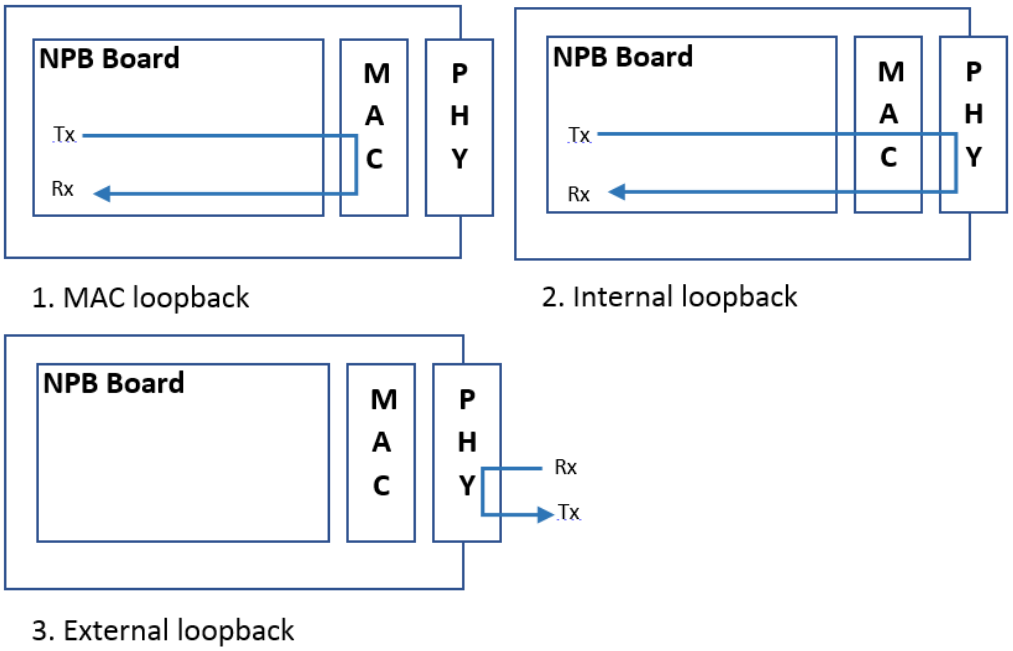
**Note:**
In NPB IV, loopback-internal and loopback-external are not supported for breakout ports.

To set loopback mode from the CLI, use the following command:

```
NPB(config)# ports port <id> mode normal|simplex|loopback-
MAC|loopback-external|loopback-internal
```

To set loopback mode from the WebUI use the port's extension panel.

**Figure 48: Loopback Types**




## Pseudo Random Binary Sequence (PRBS)

NPB ports support link error detection using the generation and receiving of PRBS. When enabled, the port transmits a sequence of bits while trying to detect the same sequence in the received traffic. Comparing the sent and received sequences allows error detection in the optical component connected to the port. PRBS can be used by one port (using a loopback cable) or by two connected ports. When using two ports, make sure that both ports enable PRBS using the same polynomial type.

To enable PRBS, set the port's **`admin`** state to **`enable`**.

Note the following behaviors when PRBS is enabled for a port:

- Its link and LED indications do not reflect the actual link status.
- Non-PRBS counters are not incremented.
- The ports cannot transmit or receive traffic that is not part of the PRBS.

**Note:**
Verify that ports with PRBS enabled are not used as filter input or output ports.

PBRS status can be one of the following:

- Down: No link or received PRBS could not be detected.
- Loss: Received PRBS lost bit stream synchronization.
- Lock: Received PRBS synchronized successfully.

When PRBS status is **lock**, PRBS testing takes place, and detected errors are reported.

The NPB supports the following PRBS polynomial types:

**Table 18: PRBS Polynomial Types**

| Type | Polynomial |
|---|---|
| PRBS7 (default) | $1 + x^6 + x^7$ |
| PRBS9 | $1 + x^5 + x^9$ |
| PRBS11 | $1 + x^9 + x^{11}$ |
| PRBS15 | $1 + x^{14} + x^{15}$ |
| PRBS23 | $1 + x^{18} + x^{23}$ |
| PRBS31 | $1 + x^{28} + x^{31}$ |
| PRBS58 | $1 + x^{39} + x^{58}$ |

Table 19 lists the bit rate used for Bit Error Rate (BER) calculation per supported port speed.

**Table 19: Bit Rate for BER Calculation**

| Port Speed (Gb) | Bit Rate |
|---|---|
| 1 | 1.03125 |
| 2.5 | 2.578125 |
| 10 | 10.3125 |
| 20 | 20.625 |
| 40 | 41.25 |
| 25 | 25.78125 |
| 50 | 51.5625 |
| 100 | 103.125 |

Table 20 lists the number of lanes and lane speeds used by PRBS per supported port speed.

**Table 20: Bit Rate for BER Calculation**

| Port Speed (Gb) | Lane Settings |
|---|---|
| 10 | 1x10 |
| 4x10 | 4x10 |
| 25 | 1x25 |
| 4x25 | 4x25 |
| 40 | 4x10 |
| 50 | 2x25 |
| 2x40 | 8x10 |
| 4x50 | 4x2x25 |
| 100 | 4x25 |
| 2x100 | 8x25 |
| 4x100 | 4x2x50 |
| 200 | 8x25 |
| 400 | 8x50 |

**Note:**
PRBS is not supported in NPB Ie and IV.

To set PRBS from the CLI, use the following command:

```
NPB(config)# ports port <id> prbs enable|disable [type prbs7|prbs9|
prbs11|prbs15|prbs23|prbs31|prbs58]
```

To set PRBS using the WebUI, use the port's extension panel.

To display PRBS statistics from the CLI, use the following command:

```
NPB# show port-statistics prbs [port <port-id>]
```

To display PRBS statistic using the WebUI, select **Home** in the Navigation panel and use the PRBS button.

See Section Port Statistics on p.99 for more information. See Appendix 3 – Port Counters on p.220 for details on the counters displayed.

# Timestamping (NPB Ie8 and NPB IIe)

NPB Ie8 and NPB IIe support packet timestamping by the port. Packets can be timestamped upon receiving, transmitting, or both. Each timestamp is added as a trailer to the packet. A configurable ID can be used in the trailer to identify the timestamping port.

**Table 21: Timestamp Trailer Structure**

| First Bit Position | Width in Bits | Description |
|---|---|---|
| 0 | 48 | 48-bit UTC timestamp (18 bits for seconds and 30 bits for nanoseconds).<br>The timestamp value represents the time passed since midnight. Midnight time is set, based on the date and time configuration, see Section Time and Date Settings on p.47 |
| 48 | 8 | Unused |
| 56 | 23 | ID in the range 0 – 8388607, default is 0 |
| 79 | 1 | 0: Rx timestamping<br>1: Tx timestamping |
| 80 | 32 | Unused |

To set port timestamping from the CLI, use the following command:

```
NPB(config)# ports port <id> rx-timestamp enable|disable [rx-
timestamp-id <rx-id>] tx-timestamp enable|disable [tx-timestamp-id
<tx-id>]
```

To set port timestamping from the WebUI, select **Ports – Configuration** in the Navigation panel. Click one of the ports, and use the extension panel.

# Port Breakout

QSFP+, QSFP28, and QSFP-DD physical ports can be split into two or four logical ports. This operation is called "ports breakout".

When splitting a physical port, the user can set the speed of the newly created logical ports. All sub-ports of the same main port use the same speed. Possible speed values are according to the port's type.

Breakout ports are created with their admin status disabled. Thus, before they can be used, the admin status must be changed **`enable`**.

The opposite operation of port breakout is merging the logical ports back into one logical port. This will deactivate the breakout ports and create a new port with admin status **`disable`** and the speed set to 10G.

Each logical port created by a port breakout acts as an independent port. This means that:

- Its attributes can be set independently without affecting the other logical ports (except for the speed attribute, which is set as a part of the breakout operation).
- Its statistics and utilization are collected independently.
- It can be used in filters configuration (filters are described in Section Filtering on p.145).

To perform a port breakout from the CLI, use the following command. Note the speed value in the **map** parameter.

```
I:   ports breakout port <port-id> enabled map 4x1|4x2.5|4x10
Ie:  ports breakout port <port-id> enabled map 4x1|4x10|4x25|2x50
Ie8: ports breakout port <port-id> enabled map 4x1|4x10|4x25|2x50
II:  ports breakout port <port-id> enabled map 4x1|4x10|4x25
IIe: ports breakout port <port-id> enabled map 4x1|4x10|4x25|2x50
III: ports breakout port <port-id> enabled map 2x40|2x100|4x10|4x25
|4x50|4x100 [line-code nrz|pam4]
IV:  ports breakout port <port-id> enabled map 4x10|4x25
```

**Note:**
In NPB III, a line code value can be set when mapping is 4x50. For more details, see line code in Section Port Configuration on p.77.

**Note:**
For NPB IV breakout limitations, see NPB IV Ports Numbering on p.77.

To undo a port breakout from the CLI, use the following command:

```
NPB(config)# ports breakout port <port-id> disabled
```

where <port-id> is the ID of the logical port.

To perform a port breakout using the WebUI, select **Ports – Configuration** in the Navigation panel. The Breakout button is located at the left end of each line. Hovering above it displays the available breakout options. Clicking it allows you to set the port breakout as needed. To breakout multiple lines, click the checkboxes next to the lines you want to breakout, and click the Breakout button above the table.

**Figure 49: Ports 1 and 2 without Breakout**


**Figure 50: Hovering over Port 1 to Show Breakout Options**

**Figure 51: Split Port Dialog**

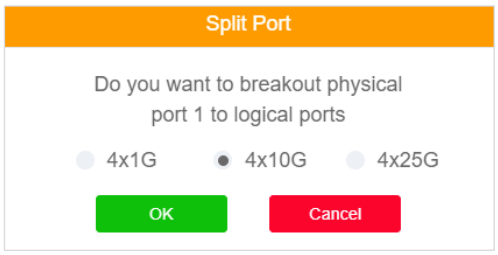
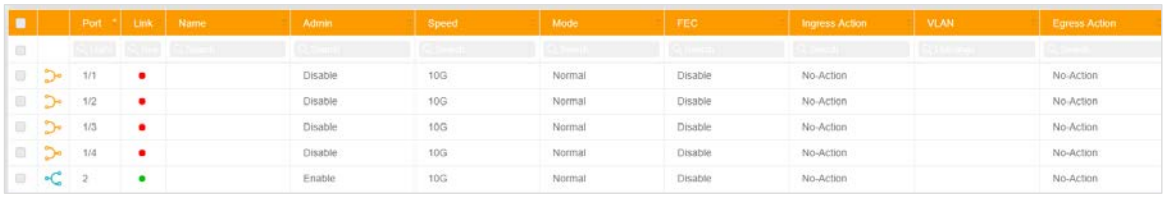
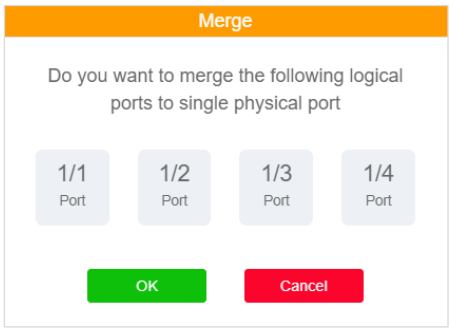



**Figure 52: Port 1 after Breakout**




To undo the Port 1 breakout, click one of the breakout ports (1/1-1/4) to display the Merge dialog. Click **OK** to merge the breakout ports back into a single physical port.

**Figure 53: Merging Breakout Ports Back into Single Physical Port**




# Managing Tagged Traffic

The NPB device supports the configuring of a double-tag (Q-in-Q) EtherType value per port. When set, packets that use this EtherType are treated differently than packets that do not. Supported double-tag EtherType values are the standard 8100, 9100, and 88A8. This configuration has the following effects:

- EtherType set on egress:
  By default, when transmitting a tagged packet, the device overwrites its outermost EtherType to 8100. Configuring double-tag EtherType on the egress port causes the device to use this EtherType when overwriting. Configuring double-tag EtherType on the ingress port limits the overwriting to packets with this EtherType or with EtherType 8100.

- Filter's VLAN classifier:
  By default, the l2-vlan classifier is matched against all traffic. Configuring double-tag EtherType on the ingress port causes only traffic with this EtherType value to be matched against the l2-vlan classifier. Other traffic is considered a non-match for the filter.
- Filter L3, L4 and UDF classifiers:
  By default, these classifiers are matched against all traffic. Configuring double-tag EtherType on the ingress port causes only traffic with this EtherType to be matched against these classifiers. Other traffic is considered a non-match for the filter.
- Port's Add and Replace ingress actions and filter's set-vlan action:
  By default, EtherType 8100 is used. Configuring double-tag EtherType on the egress port causes the device to use this EtherType instead.

To configure a double-tag EtherType value from the CLI, use the following command:

```
NPB(config)# ports port <id> double-tag 8100|88a8|9100
```

To configure a double-tag EtherType value using the WebUI, select **Ports – Configuration** in the Navigation panel. Click one of the ports and use the extension panel.

# VLAN Tagging Actions

## Overview

The NPB supports various VLAN related operations at the port level in both ingress and egress direction. This is useful to mark the incoming port of the traffic so this information can be used by a tool that receives traffic aggregated from several input ports. As the port mark is in some cases kept internal and not returned to the network, the VLAN tag should be removed in the egress direction.

VLAN tags are added as the outermost tag and become part of the packet. If the packet already contains a VLAN tag, this tag became the inner tag.

For example: Incoming traffic from Ports 1, 2, and 3 is aggregated into Port 4, which is connected to a monitor tool that should take different actions based on the input port. If the traffic on ingress Ports 1, 2, and 3 is tagged with different VLANs (say 1001, 1002, and 1003), the tool can use this tag and perform the actions based on it. If the traffic is returned to the network, an egress operation should be configured on the egress port to remove these tags.

## Ingress Operations

The following VLAN operations can be configured for the ingress direction:

**Table 22: Ingress Operations**

| Name | Description |
|---|---|
| Add | Adds a new VLAN tag as an outermost tag.<br>To use this operation, configure the new **`vlan`** value for the port. |
| Remove | For tagged packets, removes outermost tag (not supported in NPB III) |
| Replace | For tagged packets, replaces the incoming tag with a new VLAN tag.<br>For untagged packets, NPB Ie, Ie8, IIe, and IV add a new VLAN tag. NPB III does not modify the packet.<br>To use this operation, configure the new **`vlan`** value for the port. |
| No action | Does not modify VLAN tags (default) |

To configure a VLAN ingress operation from the CLI, use the following command:

```
NPB(config)# ports port <port-id> ingress-action add|no-
action|remove|replace
```

If the action requires a VLAN value (i.e. Add and Replace), configure it as follows:

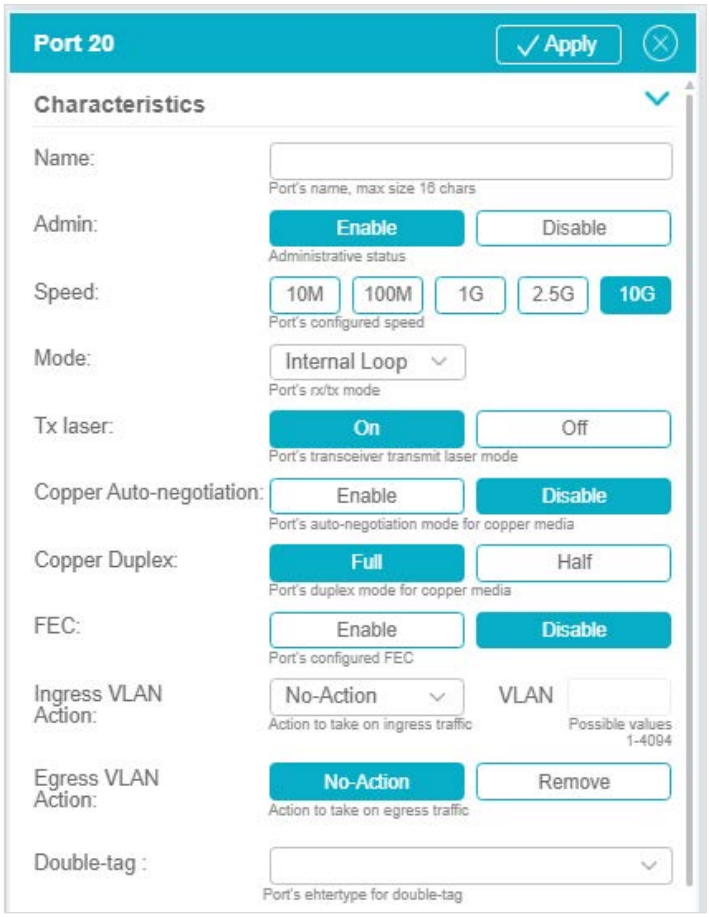
```
NPB(config)# ports port <port-id> vlan <vlan-id>
```

**Note:**
The NPB device supports ingress packets with up to 2 VLAN tags in the range 1..4094.

**Note:**
VLAN operations are not supported on ports that are bound to interfaces (e.g. GRE tunnels).

To configure a VLAN ingress operation using the WebUI, select **Ports – Configuration** in the Navigation panel. Click one of the ports and use the extension panel to set the required ingress operation and the VLAN value if needed.

**Figure 54: Configuring a VLAN Ingress Operation using the WebUI**




## Egress Operations

The following VLAN operations can be configured for the egress direction:

**Table 23: Egress Operations**

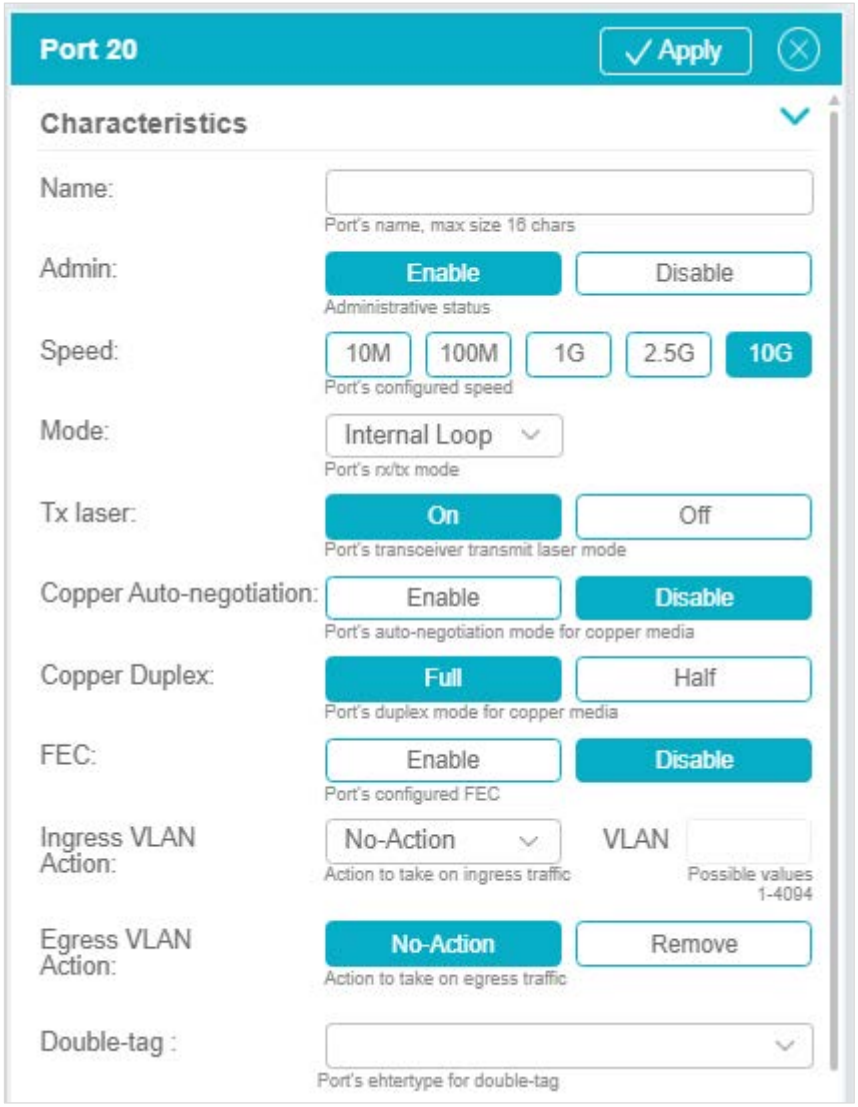
| Name | Description |
|---|---|
| Remove | For tagged packets, removes outermost tag (NPB I, NPB Ie8, NPB II, NPB IIe, and NPB III only) |
| Add | NPB III only, when packet is untagged |
| Replace | NPB III only |
| No action | Does not modify VLAN tags (default) |

To configure a VLAN egress operation from CLI, use the following command:

```
NPB(config)# ports port <port-id> egress-action no-action|remove
```

To configure a VLAN egress operation using the WebUI, select **Ports – Configuration** in the Navigation panel. Click one of the ports, and use the extension panel to set the required egress operation.

**Figure 55: Configuring a VLAN Egress Operation using the WebUI**



# MPLS Stripping (NPB Ie, Ie8 and IIe only)

The NPB Ie, Ie8, and IIe devices support MPLS label stripping as a port ingress action. Stripping is supported for L2 MPLS (with or without pseudo-wire) and L3 MPLS. When applied, all MPLS labels found in the packet are removed (up to 2 VLAN tags and 9 labels in NPB Ie / 7 labels in NPB Ie8 and IIe). Other headers are modified as described below. MPLS labels are detected according to the standard MPLS EtherTypes 0x8847 and 0x8848. MPLS payload is detected based on the first nibble of the payload.

## MPLS Stripping in NPB Ie

NPB Ie supports several global MPLS parsing modes. These modes are used when prior knowledge regarding the MPLS type is available. The MPLS stripping mode is defined per port. Table 24 lists the global parsing modes while Table 25 lists the MPLS stripping modes.

### MPLS Parsing Mode

The MPLS protocol format is hard to parse correctly without having some prior knowledge of the MPLS network. By default, NPB Ie uses heuristics parsing to get an educated guess about the MPLS format. It is possible to configure a specific MPLS type if the format is known.

**Table 24: MPLS Parsing Modes**

| Mode | Description | When to Use |
|---|---|---|
| none | No MPLS parsing | MPLS traffic is not parsed |
| heuristics | MPLS parsing is done heuristically. The parser makes an educated guess regarding the MPLS internal structure. | For MPLS traffic of an unknown type or of several types |
| eth-heuristics | MPLS parsing is done heuristically. The parser makes an educated guess regarding the MPLS internal structure, assuming no pseudowire exists. | For MPLS traffic of an unknown type or of several types that do not include pseudowire |
| eth-over-mpls | MPLS parsing assumes Ethernet over MPLS format (L2 MPLS). | MPLS traffic of L2 MPLS format is stripped. |
| pseudowire | MPLS parsing assumes pseudowire format. | MPLS traffic that uses pseudowire is stripped. |

To configure the global MPLS stripping mode from the CLI, use the following command:

```
NPB(config)# ports mpls remove-mode none|heuristics|eth-
heuristics|eth-over-mpls| pseudowire
```

**Note:**
Changing the global MPLS parsing mode requires a system reboot.

### MPLS Stripping Modes

The MPLS stripping mode is defined per port and dictates which type of MPLS traffic is stripped by the port.

**Table 25: MPLS Stripping Modes in NPB Ie**

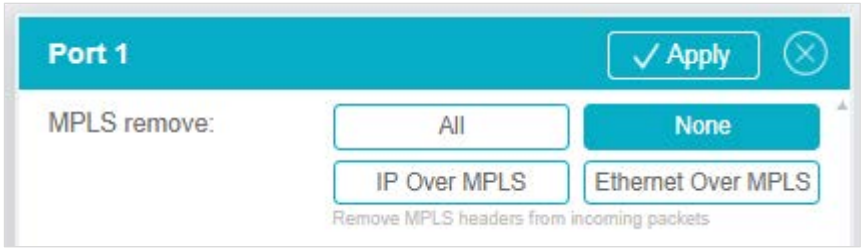
| Name | Description | When to Use |
|---|---|---|
| none | Does not remove MPLS labels | When no MPLS stripping is required by the port |
| eth-over-mpls | Removes MPLS labels if the MPLS payload is Ethernet.<br>In this case, the outer L2 header and the optional pseudowire are removed. | When global parsing mode is set to heuristic, and only MPLS L2 stripping is required by the port |
| ip-over-mpls | Removes MPLS labels if the MPLS payload is IP.<br>In this case, the original outer L2 MAC addresses are preserved, VLAN headers, if present, are removed, and an EtherType header is set according to the payload's IP version. | When global parsing mode is set to heuristic, and only MPLS L3 stripping is required by the port |
| all | Removes MPLS labels for both Ethernet and IP as described above. | When MPLS stripping of all MPLS traffic is required by the port |

To configure an MPLS Remove action from CLI, use the following command:

```
NPB(config)# ports port <port-id> mpls-remove all|eth-over-mpls|ip-over-mpls|none
```

To configure an MPLS Remove action using the WebUI, select **Ports – Configuration** in the Navigation panel. Click one of the ports, and use the extension panel to set the required egress operation.

**Figure 56: Configuring MPLS Remove Action using the WebUI in NPB Ie**



**Note:**
In NBP Ie, MPLS stripping has the following effects:
Each packet that performs MPLS stripping consumes double bandwidth from the switch.
The total number of filters is reduced from 12,500 to 10,000.

## MPLS Stripping in NPB Ie8 and IIe

In NPB Ie8 and IIe, the MPLS stripping mode is defined globally. Once defined, MPLS stripping can be enabled or disabled per port. Table 26 lists the MPLS stripping modes.

**Table 26: MPLS Stripping Modes in NPB Ie8 and IIe**

| Name | Description |
|---|---|
| none | Does not remove MPLS labels |
| eth-over-mpls | Removes MPLS labels if the MPLS payload is Ethernet with no control word. In this case, the outer L2 header is removed. |
| pwcw-over-mpls | Removes MPLS labels if the MPLS payload is Ethernet and a control word is used. In this case, the outer L2 header and the pseudo-wire are removed. |
| ip-over-mpls | Removes MPLS labels if the MPLS payload is IP. In this case, the original outer L2 MAC addresses are replaced with configurable MAC addresses, VLAN headers, if present, are removed, and an EtherType header is set according to the payload's IP version. |
| all | Removes MPLS labels if payload is either Ethernet with control word or IP. |

To configure an MPLS Remove action from the CLI, use the following command:

```
NPB(config)# ports mpls remove-mode all|eth-over-mpls| pwcw-over-
mpls|ip-over-mpls|none
```

To configure the MAC addresses to be used in ip-over-mpls mode from the CLI, use the following command:

```
NPB(config)# ports mpls l3-src-mac <mac>
NPB(config)# ports mpls l3-dst-mac <mac>
```

To set a MPLS Stripping action per port from the CLI, use the following command:

```
NPB(config)# ports port <port-id> mpls-remove enable|disable
```

To configure an MPLS Remove action using the WebUI, select **Ports – Configuration** in the Navigation panel and click the **MPLS Remove Mode** button.

To set MPLS stripping per port, use the port extension panel.

# Port Utilization

The NPB device constantly monitors its ports utilization and can raise and clear alarms and SNMP traps based on user-defined thresholds. The thresholds are set as a percentage of the overall port speed. The user can:

- Configure different thresholds for Rx and Tx traffic
- Turn alarms and trap generation on or off

This functionality is handy when ports are assumed to be underutilized. When this assumption is no longer valid, the user gets an alarm and can take the required actions.

To set port utilization alarm admin status from the CLI, use the following command:

```
NPB(config)# ports port <port-id> utilization-alerts rx|tx admin
enable|disable
```

To set port utilization alarm thresholds from the CLI, use the following command:

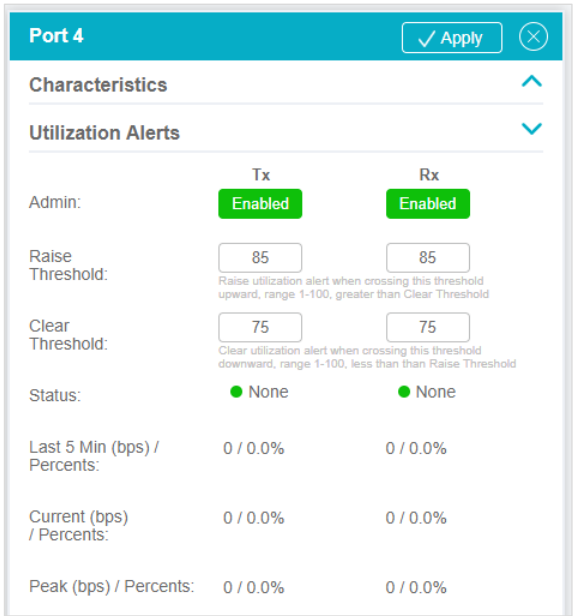
```
NPB(config)# ports port <port-id> utilization-alerts rx|tx clear-
threshold|
raise-threshold <threshold-value-in-percentage>
```

To display ports utilization figures alongside alarm threshold and current status, use the following command:

```
NPB# show port-statistics utilization [port <port-id>]
```

To set port utilization alarm thresholds using the WebUI, select **Ports – Configuration** in the Navigation panel. Click one of the ports and use the extension panel to set the thresholds admin state and values.

**Figure 57: Setting Port Utilization Alarm Thresholds using the WebUI**



## Port Statistics

The NPB device collects various statistics regarding the traffic it processes. These statistics are collected per port and can provide an efficient way to monitor and trace the device operation. The set of port statistics is divided into several categories as listed below:

| | |
|---|---|
| errors | Statistics regarding error conditions in the network and physical layers |
| packet-size | Counters count how many packets have been received and transmitted for each defined packet size |
| summary | Summary of the most commonly used statistics, for example received and transmitted packets and bytes and port utilization |
| traffic-types | Counters according to received and transmitted packets types |
| utilization | Utilization statistics |
| actions | Counters per port actions |
| prbs | PRBS statistics |
| fec | FEC statistics |
| queues | Port Tx queue settings and statistics (NPB Ie only) |

To display port statistics from the CLI, use the following command:

```
NPB# show port-statistics [errors|packet-size|summary|traffic-
types|utilization|actions|prbs|fec|queues] [port <port-id>]
```

When no specific category is given, all categories are displayed. When no specific port is given, all ports are displayed.

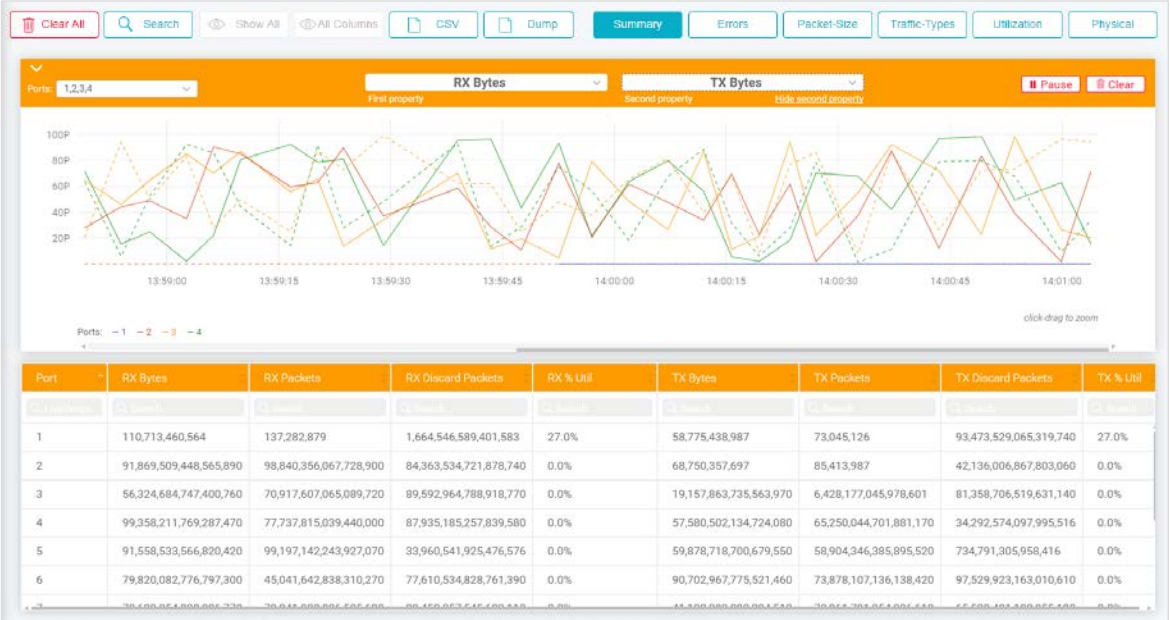
Statistics can be cleared on request. All statistics for all ports are cleared simultaneously.

To clear port statistics from the CLI, use the following command:

```
NPB# port-statistics clear
```

To view and clear port statistics using the WebUI, select **Home** in the Navigation panel. This page is divided into a graphical representation and a table representation as shown below.

**Figure 58: Viewing and Clearing Port Statistics using the WebUI**




Select the required counter category using the category buttons in the top row. The counters of the selected category appear in the table.

To use live graphs, select the ports you want to monitor and the counters you wish to display. Up to 2 counters of the selected category can be displayed simultaneously. You can click and drag the graph area to zoom in or out.

Click **Pause** to hold monitoring but keep the recorded values. The **Pause** button turns into **Play**, which you can click to resume monitoring.

Click **Clear** to clear the display. This means that you clear the recorded value history.

Click **CSV** in the top row to export the current table values to CSV file format. This includes the current values for all the counters on all the ports, but no history.

Click **Dump** to export the values displayed in the graph. This includes the history of the plotted graph, that is, all recorded values for the selected ports for up to two counters.

Click **Clear All** to clear all statistics.

## Port Tx Queues (NPB Ie Only)

NPB Ie dedicates 6GB of memory for port Tx queues. This allows the system to absorb Tx micro-bursts without packet drops. The memory is divided into 3 million buffers, with each buffer having the size of up to 2Kbytes. Buffers are assigned automatically to ports based on the transmitted traffic.

To check the status of the current queues from the CLI, use the following command:

```
NPB# show port-statistics queues
```

To view queue status using the WebUI, select the Queues category button on the home page.

See Appendix Queues on p.226 for a description of the buffer queue counters.

**Note:**
Due to the burstiness nature of the buffer allocation, the queue info is accurate only for the microsecond in which it was collected.
There are additional aspects of Tx queue allocations that are beyond the scope of this document. For more information, contact CGS support.

# Filtering

## Overview

Traffic filtering allows the user to manipulate traffic that arrives to the NPB device according to a set of criteria. Traffic matching the criteria can be redirected, copied, or dropped. This allows the user to aggregate traffic to an external tool, to drop specific traffic, to offload its tools by filtering out non-relevant data, and to support many other use cases.

This chapter describes the NPB filtering capabilities and explains how filters are configured and managed.

### Filter Concepts

In the most basic form, each filter consists of the following concepts:

| | |
|---|---|
| Inputs and outputs: | Lists of input and optionally output entities that define the filter's scope |
| Classifiers: | A set of matching criteria that is matched against incoming traffic |
| Actions: | Action to take in case there is a match |

These concepts are further described below.

#### Inputs and Outputs

Each filter contains an input list and optionally an output list. List entities are given either by stating valid ports IDs or by using higher level objects, such as port groups, GRE interfaces, and Load-Balance Groups, that contain a list of ports as part of their internal definition. The two types can be combined.

- The input list defines the set of ports, on which the filter criteria is applied.
- The output list defines the set of ports, to which matching traffic is passed, based on the filter's action.

The syntax of an explicit port list is a list of valid port IDs separated by commas. Ranges can be expressed using the hyphen mark. For example:

1, 2, 3/1 – 4/4, 10-20

When using port groups, GRE tunnels, or load balancing groups, the name or ID is used. For example: **`gre10.`** Refer to Port Groups on p.81, GRE Tunneling on p.162 and Configuring Load Balancing Group on p.165 for more details on those entities.

If the action is other than **`drop`**, an output list must be configured.

### Classifiers

The NPB device supports a wide range of classifiers from L2 to L4, including MPLS, L2TP, GTP and GRE tunnels, and User Defined Fragments (UDF). Each filter can contain many classifiers, covering several layers. Traffic is considered matching if all classifiers are matched based on the logical operation defined for the filter (AND or OR). See later on this section for more details.

### Actions

The NPB device supports several types of actions to be applied in case the incoming traffic matches:

| | |
|---|---|
| Redirect | Traffic from the set of input ports that matches the filter's criteria is aggregated, processed, and redirected to the list of output ports. |
| Copy | Traffic from the set of input ports that matches the filter's criteria is aggregated, processed, and a copy is redirected to the list of output ports. |
| Drop | Traffic from the set of input ports that matches the filter's criteria is dropped. In this case, there is no need to configure an output list. |

**Note:**
Traffic that is not matched by any filter is dropped.

**Note:**
Filters with a copy action cannot modify the traffic (e.g. by using VLAN editing operations). If the matched traffic was modified by other rules, the redirected copy reflects these changes.

# Filter Management

## Filter List

All configured filters are stored in an ordered filter list, which is divided into filter groups. The filter list is traversed as follows:

- Filters are handled according to their position in a first-match manner.
- If there is a match, the actions defined for the matching filter take place, and the traffic is processed accordingly. If the action is other than **copy**, list traverse stops. If the action is **copy**, list traversal continues.
- If no matching filter was found, the traffic is dropped.

## Filter Groups

The filter list is constructed of filter groups. This allows organizing filters in a flexible way, based on functionality and user's permissions. Filter groups do not affect the way the filter list is traversed as described above. Only users with admin permissions can create, delete, or modify filter groups. Non-admin users can create, delete, or modify filters within the groups, based on the group's permission level.

Each filter group has the following attributes:

**Table 27: Filter Group Attributes**

| Name | Description | Possible Values |
|---|---|---|
| name | Group name | Free text |
| description | Group description | Free text |
| permission | Sets the group permission level<br>Only users with higher or equal permissions than the defined value can edit the group's filters. | admin or oper<br>Default is **oper** |
| continue-only | If set, this group can contain only filters with a **copy** action | set or unset<br>Default is **unset** |

Up to 99 groups are supported.

To create a new group from the CLI, use the following command:

```
NPB(config)# filters groups add name <new-group-name> [description
<description>] [permissions admin|oper] [continue-filters-only]
```

By default, newly created groups are located as the last group in the list. To insert a new group at a specific place from the CLI, use the following command:

```
NPB(config)# filters groups insert before-group <existing-group-name>
name <new-group-name> [description <description>] [permissions
admin|oper] [continue-filters-only]
```

To rename a group from the CLI, use the following command:

```
NPB(config)# filters groups rename group <name> to <new-name>
```

To delete a specific group or all groups from the CLI, use one of the following commands:

```
NPB(config)# filters groups delete group <group-name>
NPB(config)# filters groups delete all
```

**Note:**
Deleting a filter group deletes all its filters.

To display the filter groups from the CLI use the following command:

```
NPB# show filters groups [group <name> [filter <name]]
```

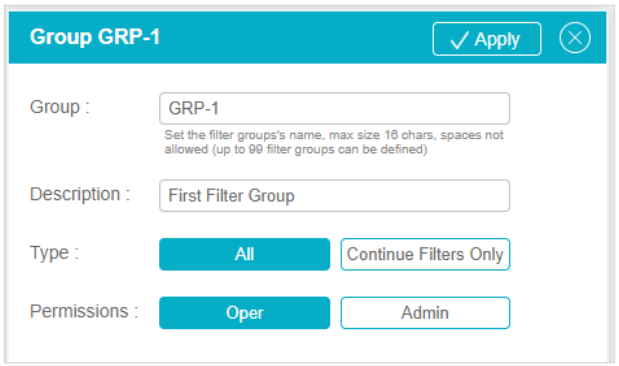
To manage filter groups using the WebUI, select **Filter – Groups** in the Navigation panel. All configured groups are displayed in the main table.

Use the **Add**, **Insert**, or **Delete** buttons to perform group operations.

Use the checkbox next to each line to indicate which line you wish to delete or insert above.

Select one of the configured lines to update the group using the extension panel.

**Figure 59: Filter Group Extension Panel**




## Defining Filters

Each filter contains a set of attributes that defined its operation. Table 28 shows the list:

**Table 28: Filter Attributes**

| Name | Description | Possible Values |
|---|---|---|
| name | Filter name | Free text, auto generated if not given. |
| description | Filter description | Free text |
| admin | Administrative status | Enable/disable, default is **`enable`** |
| bidirectional | Sets the filter as bidirectional. Setting a bidirectional filter is logically equivalent to adding a second filter using same classifiers and actions with the input and output ports switched. | set or not set,<br>Default is **`not set`** |
| tags | User-defined textual tags attached to the filter | Up to 5 free-text tags |
| action | Filter action | redirect/copy/drop |
| operator | Logical operation between classifiers | and/or, default is **and**<br>See Section Logical Operation between Classifiers (OR and AND) on p.121 |
| not | Set the list of classifiers to negate | A list of valid classifiers<br>Default is empty set. See Section Negating Classifiers on p.122 |
| input-ports | Input ports list | |

| Name | Description | Possible Values |
|---|---|---|
| output-ports | Output ports list, valid when action is redirect or copy | List of ports separated by commas, range can be specified using hyphen |
| input-interface | Input interface | Valid interface name (e.g. gre1)<br>See Section GRE Tunneling on p.162 |
| output-interface | Output interface, valid when action is redirect or copy | |
| output-lb-group | Output load balancing group, valid when action is redirect or copy | Up to 8 valid load balancing group IDs<br>See Section Load Balancing on p.163 |
| set-virtual-lb | Sets virtual load balancing VLAN tags | Valid VLAN range<br>See Section Virtual Load Balance on p.175 |
| set-virtual-lb-source | Sets virtual load balancing source value to deduce VLAN tag | **`primary`** or **`secondary`**, default is **`primary`**<br>See Section Virtual Load Balance on p.175 |
| vlan-set-outer | Sets or replaces outermost VLAN tag | Valid VLAN tag |
| classifiers | Filter classifiers | See Section Layers 2, 3 and 4 Filter Classifiers on p.117 |

### Filter Name and Priority

Filters are identified by their name as given upon creation. If no name was given, the system automatically generates one. Filter names are unique and do not change when performing filter actions.

The filter list is ordered by priority and managed in a compact form, that is, the first filter in the list has priority 1, and all other filters have subsequent priorities without any gaps. This implies that, when a filter is deleted, all filters below it in the list are pushed up. The same applies for filter insertion: if a filter is inserted, all filters below it are pushed down.

In addition to this global priority, each filter has an internal priority within its group. Actions in other groups do not affect this internal priority, while actions within a group affect it in the compact manner described above.

### Managing Filters

Filters can be created, renamed, deleted, edited, duplicated, and moved.

Filters are created within filter groups. A default group named **`filters`** is created automatically by the system. This group can be removed once other groups are created.

After creating filter groups (or using the default group), filters can be created inside the groups.

When creating a new filter, the user must define its input and output lists and its basic action. This is enough to create a functioning filter. However, in most use cases, additional classifiers and actions are required.

**Note:**
For brevity, the syntax given below does not include all possible options. An action and an input interface are mandatory.

#### Managing Filters from the CLI

To create a new filter and add it to the bottom of the filter group, use the following command:

```
NPB(config)# filters groups group <group-name> add [name <new-filter-name>] ...
```

To create a new filter and insert it before a specific filter given by name, use the following command:

```
NPB(config)# filters groups group <group-name> insert filter <before-name> [name <new-filter-name>]
```

To create a new filter and insert it before a specific filter given by priority, use the following command:

```
NPB(config)# filters groups group <group-name> insert priority <before-priority> [name <new-filter-name>]
```

To rename a filter, use the following command:

```
NPB(config)# filters groups group <group-name> rename filter <name> to <new-name>
```

To delete all filters of a group, use the following command:

```
NPB(config)# filters groups group <group-name> delete all
```

To delete a filter or several filters from a group based on name or priority, use the following command:

```
NPB(config)# filters groups group <group-name> delete filter <name>|priority <priority>
```

To delete a filter or several filters from a group based on given criteria, use the following command:

```
NPB(config)# filters groups group <group-name> delete by name <name> input-ports <ports> output-ports <ports>
```

To delete a filter or several filters from a group by a given priority range, use the following command:

```
NPB(config)# filters groups group <group-name> delete range <form-
id>-<to-id>
```

To move a filter based on name or priority, use the following command:

```
NPB(config)# filters groups group <group-name> move filter
<name>|priority <priority> before <filter-name>|before-priority
<priority>|up|down|top|bottom
```

To duplicate a filter based on name or priority, use the following command:

```
NPB(config)# filters groups group <group-name> duplicate filter
<name>|priority <priority> [before <filter-name>|before-priority
<priority>|bottom]
```

Filters can be moved or duplicated only within their group.

Changes in the filter priorities are considered pending changes after entering every CLI command, and sequential commands that use priority must take them into account. If you are making changes that involve many filter deletions and insertions, it is recommended to commit often.

### Syntax Abbreviations

The following two aliases are defined and can be used to simplify the filter group syntax:

```
fgroup: filters groups group
dgroup: filters groups group <last-created-group-name>
```

Example:

Instead of:

```
NPB(config)# filters groups group group1 add name filter1 ...
```

It is possible to use:

```
NPB(config)# fgroup group1 add name filter1 ...
```

If **`group1`** is the latest created group, the following alternative is identical:

```
NPB(config)# dgroup add name filter1 ...
```

When there is only one filter group configured (either the default group or another), the group name can be omitted from the CLI syntax.

Example:

If **`group1`** is the only configured group, the following syntax can be used:

```
NPB(config)# filters add name filter1 ...
```

When using the CLI, filter attributes can be set upon creation or, once a filter was created, by entering its context. For example, create a filter and configure its inputs, outputs, and actions:

```
NPB(config)# filters add input-ports 1,2 output-ports 3,4 action
redirect
```

The same result can be achieved by first creating a filter and then configure its attributes by entering its context:

```
NPB(config)# filters filter f1
NPB(config-filter-f1)# input-ports 1,2 output-ports 3,4 action
redirect
```

To display the filter list from the CLI, use one of the following commands:

```
NPB# show filters [filter <name>]
NPB# show filters tags [tag <tags-list>]
```

### Managing Filters from the WebUI

To manage filters using the WebUI, select **Filter – Rules** in the Navigation panel. All configured filters and groups are displayed in the main table. You can narrow your view using the filter group buttons above the table.

Use the **Add**, **Insert**, **Duplicate, Move, Delete**, or **Delete By** buttons to perform filter operations.

Use the checkbox next to each line to indicate which line you wish to delete or insert above.

When adding a new filter where multiple filter groups are defined, use the Choose Filter Group popup window to select the group in which the new filter is created. Select one of the configured lines to update the filter using the extension panel.

Click a section header to expand or collapse that section.

To configure multiple lines, click the checkboxes next to the lines you want to edit and click the **Settings** button above the table.

**Figure 60: Managing Filters using the WebUI**

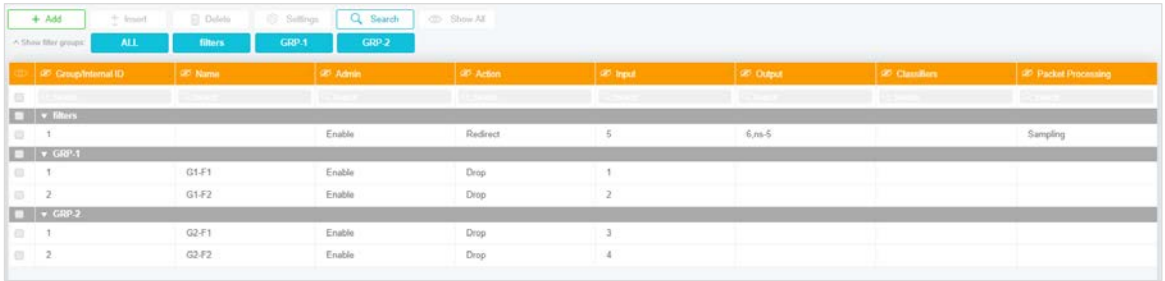
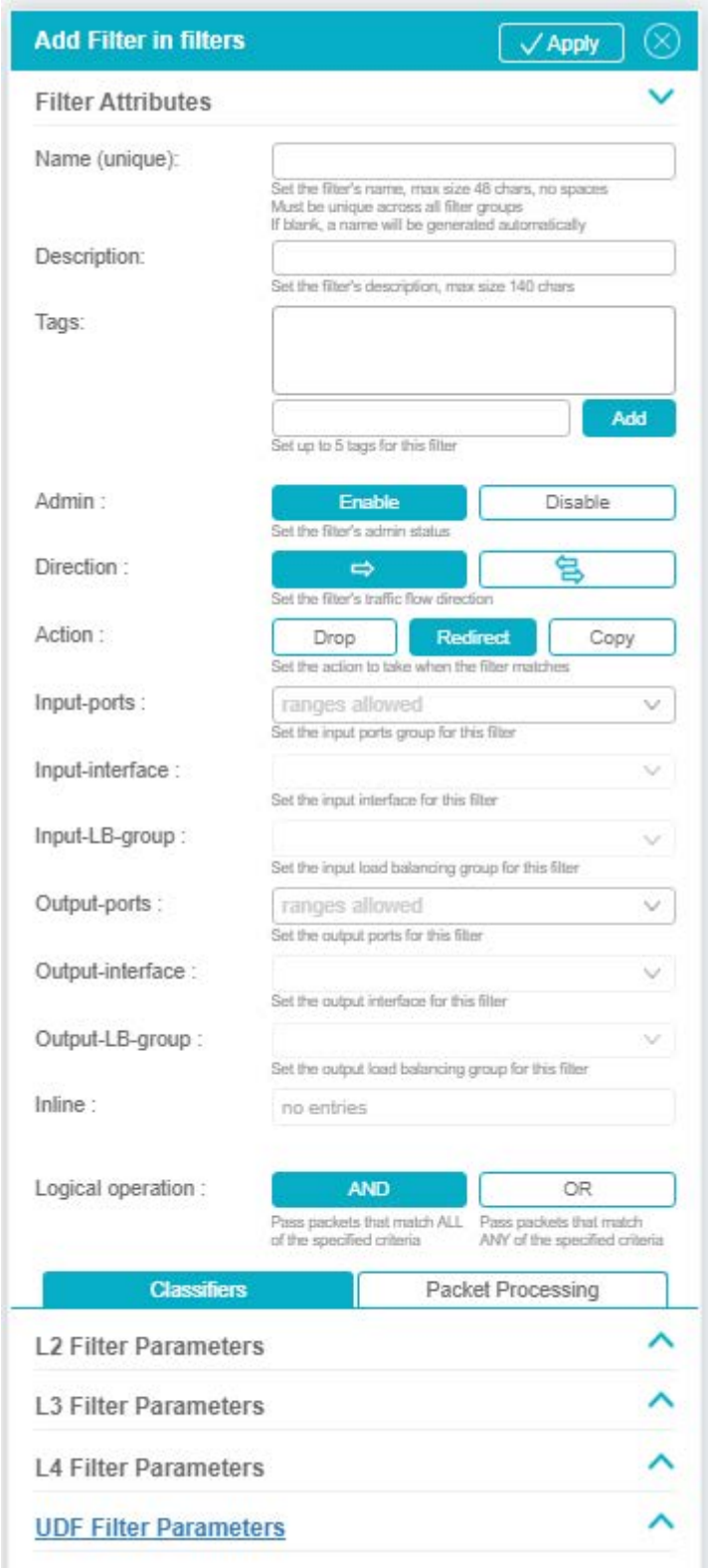


**Figure 61: Using the Filter Extension Panel**



To search the filter list, either use the Per Column search box, or click **Search** (see Figure 60: Managing Filters using the WebUI). Using the Search button will open a search template. Fill in the search criteria and click **Search** in the top bar of the template. Filters that match the search will appear in the table. Click **Clear** in the top bar of the template to clear the search.

## Filters and Port Operations

In general, port operations take place prior to filter processing. This means, for example, that if a port in the filter input ports list is configured to add a VLAN tag on ingress, this VLAN tag is visible to the filter and filtering according to it will yield a match although the VLAN was not part of the original packet.

An exception to this rule is the **`remove`** ingress action. When a VLAN tag is removed by the port, it is still visible to the filter classifiers, allowing the user to filter according to it.

## Filter Statistics

The NPB device constantly collects statistics regarding the number of packets and bytes that were matched for every active filter. For both packets and bytes, the current total and the current rate are provided. This gives the user an easy way to monitor the filter list operation and to validate if the filter definition is appropriate for his needs.

To display filters statistics from the CLI, use the following command:

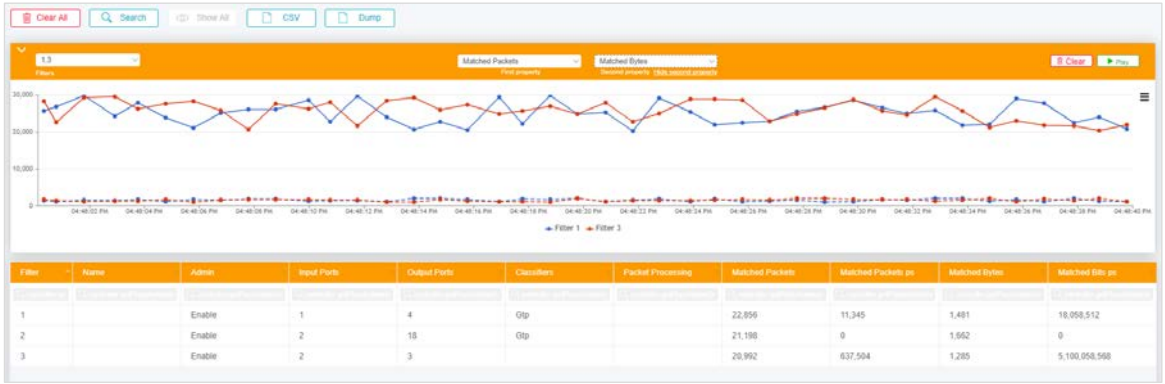
```
NPB# show filters stats [ group <name>]
```

To clear filter statistics (for all filters) from the CLI, use the following command:

```
NPB# filters clear-statistics
```

To view and clear filters statistics using the WebUI, select **Filter – Statistics** in the Navigation panel. This page is divided into a graphical representation and a table representation as shown below.

**Figure 62: Filter Statistics using WebUI**



To use live graphs, select the filters you want to monitor and the counters you wish to display. Up to 2 counters can be displayed simultaneously. You can click and drag the graph area to zoom in or out.

Click **Pause** to stop updating the graph but keep recording values. The **Pause** button turns into **Play.** When you click **Play**, the values that were recorded get added to the graph.

Click **Clear** to clear the display. This means that you clear the recorded value history.

Click **CSV** in the top row to export the current table values to CSV file format. This includes the current values for all the counters on all the filters, but no history.

Click **Dump** to export the values displayed in the graph. This includes the history of the plotted graph, that is, all recorded values for the selected filters for up to two counters.

Click **Clear All** to clear all statistics.

## Filter Modes

Prior to configuring any filters, configure the filter engines mode of operation to optimize the HW resources allocated for filtering. Table 29 lists the supported modes. Table 30 lists the supported classifiers in each mode. Tunnel classifiers are described in more details in Section Working with Tunnels on p.138.

**Table 29: Filter Modes**

| Mode | Supporting Devices | Description |
|---|---|---|
| l2-l4-ipv4 | All except NPB IV | Supports Layer 2, Layer 3, and Layer 4 classifiers with IPv4 addressing |
| l3-l4-ipv4-ipv6-mpls | All except NPB IV | Supports Layer 3 and Layer 4 classifiers with IPv4/IPv6 addressing and MPLS labels |
| l3-l4-ipv4-udf | All | Supports Layer 3 and Layer 4 classifiers with IPv4 addressing and UDF |
| l4-udf | NPB I, Ie and IV | Supports limited Layer 3 and Layer 4 classifiers and UDF |
| l2-l4-ipv6 | NPB I, Ie8, II, IIe, and III | Supports Layer 2, Layer 3, and Layer 4 classifiers with IPv6 addressing |
| l3-l4-ipv4-udf-vlb | NPB I, Ie8, II, IIe, and III | Supports Layer 3 and limited Layer 4 classifiers with IPv4 addressing, UDF, and virtual load balancing |
| l2-l4-ip-udf | NPB IV | Supports Layer 2, Layer 3, and Layer 4 classifiers with IPv4/IPv6 addressing and limited UDF |
| l3-l4-ipv4-ipv6 | NPB IV | Supports Layer 3, and Layer 4 classifiers with IPv4/IPv6 addressing |

**Table 30: Filter Mode Classifiers**

| Classifier | l2-l4-ipv4 | l3-l4-ipv4-ipv6-mpls | l3-l4-ipv4-udf | l4-udf | l2-l4-ipv6 | l3-l4-ipv4-udf-vlb | l2-l4-ip-udf | l3-l4-ipv4-ipv6 |
|---|---|---|---|---|---|---|---|---|
| Input interface (GRE or IP) | I, Ie8, II, IIe, III | I, II, III | I, Ie8, II, IIe, III | I | Ie8, IIe | Ie8, IIe | | |
| Inline | I, Ie8, II, IIe, III | I, II, III | I, Ie8, II, IIe, III | I | Ie8, IIe | Ie8, IIe | | |
| MAC | All | | | | All | | IV (for non IPv6 traffic) | |
| EtherType | All | I, Ie8, II, IIe, III | Ie, Ie8, II, IIe, III, IV | I | All | II, III | IV | |
| MPLS labels | | All | | | | | | |
| VLAN | All | All | All | All | I, II, III | All | IV | IV |
| Inner VLAN | I, Ie, Ie8, II, IIe | | | | | | IV | |
| L3 packet length | I, Ie8, II, IIe | I, Ie8, II, IIe | I, Ie8, II, IIe | I | I | Ie8, II, IIe | | |
| L3 protocol | All | All | All | All | All | All | IV | IV |
| L3 DSCP | All | I, Ie8, II, IIe, III | I, II, III, IV | I | | | IV | |
| IP fragmentation | All | I, Ie8, II, IIe, III | Ie, Ie8, II, IIe, III | Ie, Ie8, II, IIe, III | | Ie8, II, IIe, III | | |
| IPv4 address (source, destination, session) | All | All | All | | All | All | IV | IV |
| IPv6 address (source, destination, session) | | All | | | All | | IV (upper 80 bits) | IV |
| L4 port (source, destination) | All | All | All | All | All | All | IV | IV |

| Classifier | l2-l4-ipv4 | l3-l4-ipv4-ipv6-mpls | l3-l4-ipv4-udf | l4-udf | l2-l4-ipv6 | l3-l4-ipv4-udf-vlb | l2-l4-ip-udf | l3-l4-ipv4-ipv6 |
|---|---|---|---|---|---|---|---|---|
| TCP flag classifiers | All | I, Ie8, II, IIe, III | I | | | | IV | |
| UDF | | | All | All | | All | IV | |
| GTP, L2TP, PPPoE, and GRE tunneling | | | All | All | | All | | |
| MPLS tunneling | | | Ie8, II, IIe, III | All | | II, III | | |
| GTP message type | | | I, II, III | All | | I, II, III | | |
| GTP TEID | | | I, II, III | All | | I, II, III | | |
| Tunnel protocol | | | All | All | | All | | |
| Tunnel IPv4 address | | | All | All | | All | | |
| Tunnel IPv6 address | | | Ie8, II, IIe, III | All | | Ie8, IIe, II, III | | |
| Tunnel L4 ports | | | All | All | | All | | |
| Virtual load balancing | I, Ie8, II, IIe8, III | I, Ie8, II, IIe8, III | | | | All | | |

To see the list of supported classifiers from the CLI, use the following command:

```
NPB# show filters mode
```

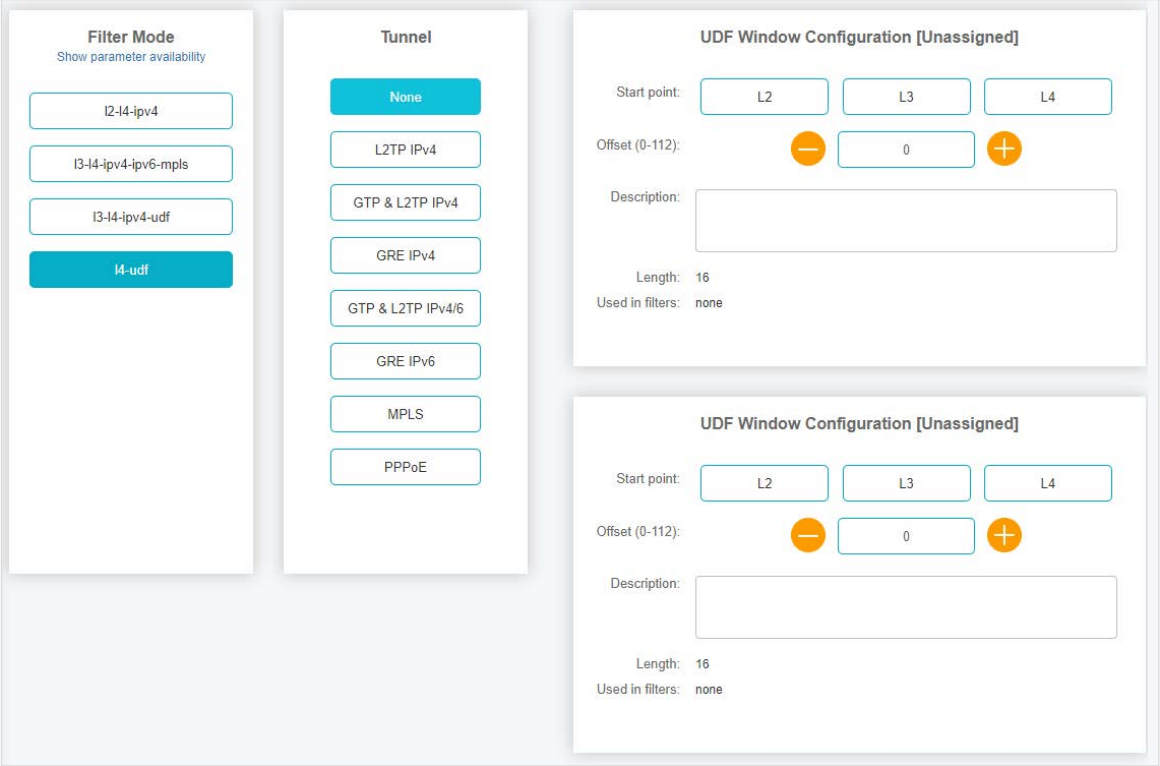
To set the filter mode from the CLI, use the following command:

```
NPB(config)# filters mode l2-l4-ipv4|l3-l4-ipv4-ipv6-mpls|l3-l4-ipv4-
udf|l4-udf|l2-l4-ipv6|l3-l4-ipv4-udf-vlb|l2-l4-ip-udf|l3-l4-ipv4-ipv6
```

**Note:**
Delete all filters and commit before changing the filter mode.

To set the filter mode using the WebUI, select **Filter – Mode** in the Navigation panel. Select the mode on the left to define additional mode-specific parameters. The list of supported classifiers per mode can be displayed by clicking **Show classifiers availability** in the **Filter Mode** section.

**Figure 63: Setting the Filter Mode using the WebUI**




# Filter Resources

The NPB device allocates HW resources for filter handling. This limits the maximal number of filters and the maximal number of ranges that can be used in filter classifiers (this applies to L2 VLAN, L4 port, and packet length classifiers). Internal filters reflect the number of resources used to support the user-defined filters. The number of internal filters used is affected by the filter's complexity, the type and number of classifiers used, and the logical operations between them.

In some devices, a dedicated memory can be used for exact match IP lists. For more information, see Using HW Exact Match Memory for IP Lists on p.127.

Table 31 lists the available resources for each product:

**Table 31: Filter Resources**

| Product | Maximal Number of Internal Filters | Maximal Number of HW Exact Match Filters | Maximal Number of Ranges |
|---|---|---|---|
| NPB I | 8191 | N/A | 32 |
| NPB Ie | 12,288 | N/A | 24 (L4 ports only) |
| NPB Ie8 | 3070 | 110,000 | 32 |

| Product | Maximal Number of Internal Filters | Maximal Number of HW Exact Match Filters | Maximal Number of Ranges |
|---|---|---|---|
| NPB II | 1023 | 15,000 | 32 |
| NPB IIe | 3070 | 110,000 | 32 |
| NPB III | 1023 | 40,000 | 0 |
| NPB IV | 12,288 | N/A | Per filter mode:<br>l2-l4-ip-udf: 29<br>l4-udf: 0<br>l3-l4-ipv4-udf: 18<br>L3-l4-ipv4-ipv6: 0 |

To show the status of filter resources from the CLI (this example is for NPB II), use the following command:

```
NPB# show filter-memory
```

To show the status of filter resources using the WebUI, select **Filter – Rules** in the Navigation panel. Filters resources are displayed at the bottom:

**Figure 64: Showing the Status of Filter Resources using the WebUI**


## Port Aggregation

Port aggregation is used to aggregate all traffic from the input ports and redirect it to all ports in the output ports list. This is useful to aggregate a set of underutilized ports into a tool connected to another port.

**Note:**
Incorrect port aggregation may over-utilize the input or output ports. It is up to the user to configure the network correctly in that sense.

Port aggregation can be set in all filter modes.

To create a port aggregation filter from the CLI, use the following command:

```
NPB(config)# filters add input-ports <input-ports-list> output-ports
<output-ports-list> action redirect
```

**Note:**
This command adds a new rule at the bottom of the list. Of course, a **`filter insert`** command can be used to insert at a specific position. Also, an existing filter can be modified to achieve the same results as described above.

To manage filters using the WebUI, select **Filter – Rules** in the Navigation panel. Create a new filter or update an existing one as described in Section Managing Filters from the WebUI on p.109.

Set input and output lists as needed and set the action to **redirect**.

## Layers 2, 3 and 4 Filter Classifiers

The NPB device supports a wide range of network related classifiers in Layer 2, 3 and 4. This allows the user to filter according to attributes in the packet's headers and to offload tools by providing them only with data they need.

**Note:**
The set of available classifiers depends on the filter mode. For example, IPv6 classifiers are available only if the mode is set to l3-l4-ipv4-ipv6-mpls.

Table 32: Layers 2 to 4 Classifiers lists the classifiers for Layers 2 to 4.

**Table 32: Layers 2 to 4 Classifiers**

| Name | Description | Possible Values |
|---|---|---|
| l2-dmac | Destination MAC address | 6 hexadecimal octets, separated by ":"<br>For example:<br>AA:A1:A0:BB:B1:B0 |
| l2-smac | Source MAC address | |
| l2-dmac-mask | Destination MAC address mask | |
| l2-smac-mask | Source MAC address mask | |
| l2-ethertype | Layer 2 Ether Type value | 4 hexadecimal digits<br>For example: 8100 |
| l2-vlan | VLAN or VLAN range value | A comma-separated list of valid VLAN IDs (1-4094). A range can be defined using a hyphen. |
| l2-inner-vlan | Inner VLAN value. If 0 is used, untagged packets will be considered as matched | A comma-separated list of valid VLAN ID (0-4095) |
| l2-inner-vlan-mask | Inner VLAN mask; valid only if l2-inner-vlan contains a single VLAN tag | 3 hexadecimal digits<br>For example: 01F |
| l3-dscp | Differentiated Services field value in IP header | Valid DSCP value (1-63) |

| Name | Description | Possible Values |
|---|---|---|
| l3-frag | Filter according to IP fragmentation attributes | Any: Packets containing any IP fragments<br>First: Packets containing a first IP fragment<br>None or first: Packets containing no IP fragments or a first IP fragment<br>Not first: Packets containing a non-first IP fragment<br>None: Packets that do not contain IP fragments<br><br>Note that supported options vary between devices and filter modes. |
| l3-pkt-len | L3 total length, including L3 header | Valid packet length (1-65535) or a valid range of lengths using '-' |
| l3-ipv4-addr | IPv4 address (source or destination) | A comma-separated list of valid IPv4 addresses with an optional mask or CIDR. For example: 1.0.0.1, 10.0.0.1/255.255.255.0, 20.0.0.1/32 |
| l3-ipv4-dst-addr | Destination IPv4 address | |
| l3-ipv4-src-addr | Source IPv4 address | |
| l3-ipv4-session | IPv4 session (source or destination). Sessions contain a pair of IPv4 addresses and a L4 port. | A comma-separated list of valid IPv4 sessions. A valid session consists of a pair of valid IPv4 addresses with an optional mask or CIDR followed by a ':', and a valid L4 port number.<br>For example: 1.0.0.1:8080, 10.0.0.1/255.255.255.0:409, 20.0.0.1/32:5680 |
| l3-ipv4-dst-session | IPv4 destination session. Sessions contain a pair of IPv4 addresses and a L4 port. | |
| l3-ipv4-src-session | IPv4 source session. Sessions contain a pair of IPv4 addresses and a L4 port. | |
| See note regarding session classifiers below this table | | |
| l3-ipv6-addr | IPv6 address or network (source or destination) | A comma-separated list of valid IPv6 addresses with an optional mask or CIDR.<br>For example: 2001:db8:0:0:1::1, 2002:db8:0:0:1::1/1::1, 2003:db8:0:0:1::1/32 |
| l3-ipv6-dst-addr | Destination IPv6 address or network | |
| l3-ipv6-src-addr | Source IPv6 address or network | |
| l3-ipv6-session | IPv6 session (source or destination). Sessions contain a pair of IPv6 addresses and a L4 port. | |

| Name | Description | Possible Values |
|---|---|---|
| l3-ipv6-dst-session | IPv6 destination session. Sessions contain a pair of IPv6 addresses and a L4 port. | A comma-separated list of valid IPv6 sessions. A valid session consists of a pair of valid IPv6 addresses with an optional mask or CIDR surrounded with [ ], followed by a ':', and a valid L4 port number. For example: [2001:db8:0:0:1::1]:8080, [2002:db8:0:0:1::1/1::1]:409, [2003:db8:0:0:1::1/32]:5680 |
| l3-ipv6-src-session | IPv6 source session. Sessions contain a pair of IPv6 addresses and a L4 port. | |
| Regarding IPv6 classifiers in NPB IV, see Note Regarding Session Classifiers on p.120 | | |
| l3-protocol-number | IP protocol number | See http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml for the complete list |
| l4-port | Source or destination L4 port or range of ports | A single valid port number with 4 hexadecimal mask or a comma-separated list of valid Layer 4 ports and port ranges (use hyphen to define range) |
| l4-dport | Destination L4 port or range of ports | |
| l4-sport | Source L4 port or range of ports | |
| l4-tcpflag-ack | TCP Packet Acknowledge flag (ACK) | No value is used. These classifiers are either present or not. To remove one of them from the CLI, use the **no** command. For example: **`no l4-tcpflag-ack`** |
| l4-tcpflag-fin | TCP flag to close connection (FIN) | |
| l4-tcpflag-psh | TCP Priority flag (PSH) | |
| l4-tcpflag-rst | TCP Reset flag (RST) | |
| l4-tcpflag-syn | TCP flag to open connection (SYN) | |
| l4-tcpflag-urg | TCP Urgent flag (URG) | |

**Note:**
In NPB IV, when using the l2-l4-ip filter mode, IPv6 classifiers are matched against the upper 80 bits only.

### Note Regarding Session Classifiers

A packet matches a session classifier if the IP/port pair in the packet matches the IP/port pair in the relevant directions. For example:

**Table 33: Session Filter Classifier Example**

| Classifier | Value | Matched Traffic |
|---|---|---|
| l3-ipv4-session | 1.0.0.1:8080 | Source IP is 1.0.0.1 and source port is 8080<br>OR<br>Destination IP is 1.0.0.1 and destination port is 8080<br>(but not Source IP 1.0.0.1 and Destination Port 8080) |
| l3-ipv4-dst-session | 1.0.0.1:8080 | Destination IP is 1.0.0.1 and destination port is 8080 |
| l3-ipv4-src-session | 1.0.0.1:8080 | Source IP is 1.0.0.1 and source port is 8080 |

## Setting Filter Classifiers

When using the CLI, filter classifiers can be set when creating the filter or, for an existing filter, by entering its context. The following example shows how to set the classifiers **`l2-vlan`** and **`l3-ipv4-addr`** when creating the filter:

```
NPB(config)# filters add input-ports 1,2,3,4 action drop l2-vlan 1020
l3-ipv4-addr 127.0.0.1/32
```

Alternatively, this is how to set the same values by entering a context for existing Filter 1:

```
NPB(config)# filters filter f1
NPB(config-filter-f1)# l2-vlan 1020
```

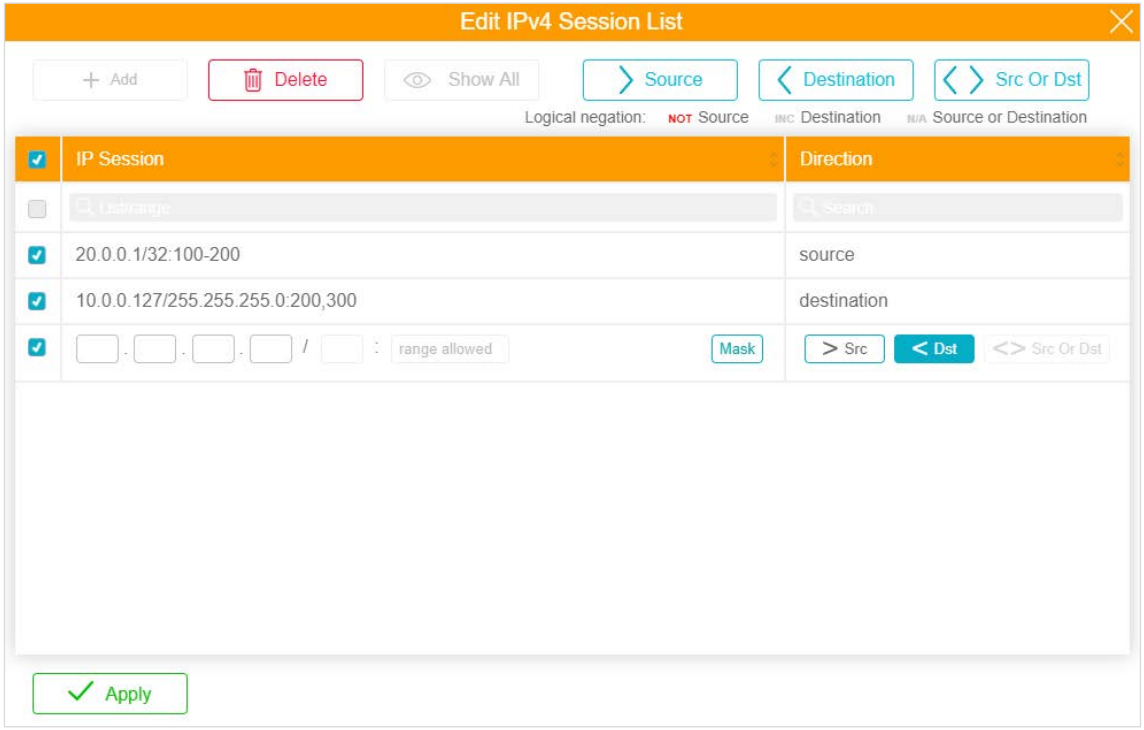
To set Layer 2, 3 and 4 classifiers using the WebUI, proceed as follows:

1. Select **Filter – Rules** in the Navigation panel.
2. Click an existing filter to update it, or use the **+ Add** or **± Insert** buttons to add a new one.
3. In the extension panel, select the Classifiers tab, if present, use **L2 Filter Parameters**, **L3 Filter Parameters** or **L4 Filter Parameters**, and set the relevant parameters.

To set address and session lists, click the relevant **Edit List** button in the L3 Filter Parameters section, and use the popup windows to insert the required information. For each address/session, specify its direction: destination, source, or both. Directions can also be set for all checked lines using the global buttons above the table. Use the **CIDR** and **Mask** buttons to toggle CIDR and mask notations.

**Note:**
The relation between all addresses with the same direction is OR. The relation between different directions is according to the filter's logical operation.

**Figure 65: Setting IP Session List using the WebUI**




## Logical Operation between Classifiers (OR and AND)

A filter can contain many classifiers of different types. In addition, some classifiers can have multiple values. The logical relation between the different classifiers can be set to be either OR or AND.

**Note:**
The logical relation within a multivalued classifier is always OR, i.e. multivalued classifiers are considered a match if at least one of their value matches the packet.

When the filter's logical relation is set to AND (default), a packet is considered to match the filter only if all different classifiers match individually. For multivalued classifiers, it is sufficient for only one value to match.

When the filter's logical relation is set to OR, a packet is considered to match the filter if at least one of the classifiers match.

**Examples**

Logical operation: AND
Classifiers: vlan = 200; source IP address = 200.0.0.1; destination IP address = 100.0.0.1

Matched traffic: vlan=200 ***and*** source IP address = 200.0.0.1 ***and*** destination IP address = 100.0.0.1

Logical operation: AND
Classifiers: vlan = 200, 300; source IP address = 200.0.0.1; destination IP address = 100.0.0.1

Matched traffic: vlan={200 ***or*** 300} ***and*** source IP address = 200.0.0.1 ***and*** destination IP address = 100.0.0.1.

**Note:**
vlan is a multivalued classifier, therefore at least one of its values will be considered a match regardless of the logical operation value.

Logical operation: OR
Classifiers: vlan = 200; source IP address = 200.0.0.1; destination IP address = 100.0.0.1

Matched traffic: vlan = 200 ***or*** source IP address = 200.0.0.1 ***or*** destination IP address = 100.0.0.1

Logical operation: AND
Classifiers: vlan = 200; IP address = 100.0.0.1

Matched traffic: vlan = 200 ***and*** {source IP address = 100.0.0.1 ***or*** destination IP address = 100.0.0.}.

**Note:**
Here, the OR operation between source and destination addresses is part of the classifier definition.

## Negating Classifiers

Some of the classifiers can be used with negation. When negation is set for a classifier, all values that are not equal to the classifier's configured values are considered a match. Negation can be combined with the OR and AND logical filter operations. The set of classifiers that support negation is listed below.

**Table 34: Classifiers that Support Negation**

| Type | Classifiers |
|---|---|
| Layer 2 | MAC source and destination addresses, Ethertype, VLAN, and inner VLAN |
| Layer 3 | Protocol number, IPv4 and IPv6 source and destination addresses, sessions and lists |
| Layer 4 | Source and destination ports |
| Tunnels | Inner protocol number, IPv4 and IPv6 source and destination addresses and lists, Layer 4 source and destination ports |

Note the following when using negation:

- When a classifier is negated, the absence of this classifier in the packet is considered a match. For example, negating VLAN 100 matches all traffic with VLAN different from 100 as well as all untagged traffic.
- To limit the matched traffic in a way that it only contains the classifier, additional classifiers can be used. For example, to match only traffic with an IP address different from 100.1.1.10 (but not non-IP traffic) use the l3-ip classifier in addition to negating the IPv4 classifier.
- When using masks, negation is done on the combination of a mask and a value. For example, negating a source MAC with value **`aa:bb:cc:dd:ee:ff`** and mask **`00:00:00:00:00:ff`** will match any source MAC with LSB different from ff.

### Examples

Classifiers: vlan = 200
Negated classifiers: vlan

Matched traffic: Tagged traffic with vlan **!=** 200 and untagged traffic

Classifiers: vlan = 200,300
Negated classifiers: vlan

Matched traffic: Tagged traffic with (vlan **!=** 200 **and** vlan **!=** 300) and untagged traffic

Logical operation: AND
Classifiers: l3-ip, vlan = 200, source IP address = 200.0.0.1
Negated classifiers: vlan, source IP address

Matched traffic: Tagged IP traffic with (vlan **!=** 200 **and** source IP address **!=** 200.0.0.1) and untagged IP traffic with source IP address **!=** 200.0.0.1

Logical operation: OR
Classifiers: vlan = 200, source IP address = 200.0.0.1
Negated classifiers: vlan, source IP address
Matched traffic: vlan **!=** 200 **or** IP address **!=** 200.0.0.1 **and** untagged traffic **and** non-IP traffic.
E.g. only traffic that includes both vlan=200 and source IP address = 200.0.0.1 will **not** be matched.

To set the list of negated classifiers from the CLI, proceed as follows.

To add a classifier to the list, use the following command:

```
NPB(config-filter-<name>)# not <classifier>
```

Example:

```
NPB(config-filter-f1)# not l2-vlan
```

**Note:**
Classifiers must be set for the filter before they can be negated.

To remove a classifier from the list, use the following command:

```
NPB(config-filter-<name>)# no not <classifier>
```

Example:

```
NPB(config-filter-f1)# no not l2-vlan
```

To clear the list, use the following command:

```
NPB(config-filter-<name>)# no not
```

To replace the current set of classifiers with a new set, state the new set of classifiers, separated by spaces inside a pair of square brackets:

```
NPB(config-filter-<name>)# not [ <classifier> <classifier> ...]
```

Example:

```
NPB(config-filter-f1)# not [ l2-vlan l3-ipv4-address ]
```

**Note:**
The spaces after the opening and before the closing square bracket are important! Missing spaces will cause a syntax error.

To set the list of negated classifiers from the WebUI, toggle the INC/NOT label appearing next to each classifier that supports negation.

**Figure 66: Negating L2 VLAN Value 100 from the WebUI**

- without negation, VLAN value that equals 200 is considered a match


- with negation, VLAN values different from 200 are considered a match

# Working with IP Lists

IP lists allow the definition and manipulation of IP addresses using txt files. This is useful when the list of IPs is too big to be handled manually, especially when it is automatically generated as a txt file by a security tool (for example, dynamic generation of an IP black list). In such cases, it is convenient to keep the txt file format and not to convert the list into the standard classifiers. Typically, in such cases, NETCONF will be used to populate the new IP list files into the system.

The content of IP lists can serve as source, destination, or both directions classifiers. Both IPv4 and IPv6 are supported.

## Defining IP Lists

IP lists are defined by text files. The file can contain either IPv4 or IPv6 addresses. Each line contains one valid IP address, optionally followed by a net mask.

For example:

```
1.2.3.4/16
10.0.0.1/24
```

Table 35 details the IP list attributes.

**Table 35: IP List Attributes**

| Name | Description | Possible Values |
|---|---|---|
| Name | IP list name | Free text |
| Description | IP list description | Free text |
| Use HW | When enabled, the IP list uses the dedicated exact-match memory, see Using HW Exact Match Memory for IP Lists on p.127.<br>When disabled, the IP list uses the internal filter resources. | enable, disable<br>Default is **`disable`** |

To set an IP list from the CLI, use the following command:

```
NPB(config)# filters ip-list <name> [description <description>] [use-hw enable|disable]
```

To delete an IP list from the CLI, use the following command:

```
NPB(config)# no filters ip-list <name>
```

To import an IP list file into an IP list from the CLI, enter the list context and use the following command:

```
NPB(config-ip-list-<name>)# import remote-url <url> [username <user-name> password <password>]
```

For example:

```
NPB(config)# filters ip-list MY_IP_LIST
NPB(config-ip-list-MY_IP_LIST)# import remote-url
scp://192.168.10.10/config/my-ip-list username admin password 1234
```

To manage IP lists using the WebUI, proceed as follows:

1. Select **Filter – IP lists** in the Navigation panel.
2. Click an existing list to update it, or click **Add** to add a new list.
3. In the IP list extension panel, enter the name of the list and an optional description, and click **Apply**.
4. Use the **Import** button to import an IP list file. (You do not need to click **Apply** again; just commit the change.)

**Figure 67: IP List Table**

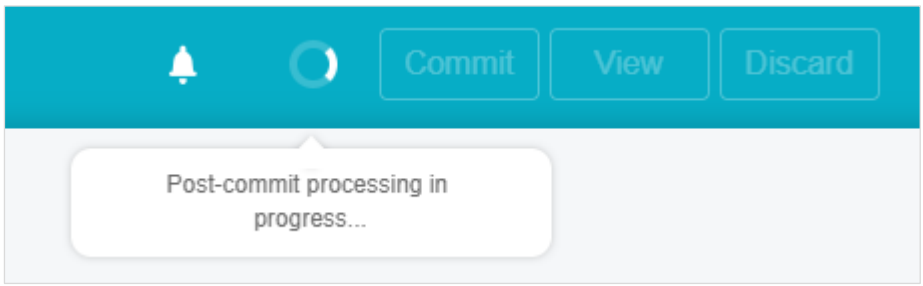

**Figure 68: IP List Extension Panel**


**Note:**
IP lists are compiled in the background after the Commit operation has returned. Therefore, when changing an existing list or loading a new one, the change will take effect only after the Commit operation has completed. Failures in IP list compilation are not reflected by the Commit operation status.

To check the status of the IP list background compilation from the CLI, use the **`show filter-memory`** command.

In the WebUI, the status is reflected next to the Commit button on the top bar. Hover above it to see the details, as shown in Figure 69 below.

**Figure 69: Background Processing Status**




## Using HW Exact Match Memory for IP Lists

In NPB Ie8, II, IIe, and III, it is possible to use a dedicated memory in the HW for IP lists. This significantly extends the number of IPs in a list.

Four types of lists can be supported:

- IPv4 source IPs – Each line contains an IPv4 address without masking.
- IPv4 destination IPs – Each line contains an IPv4 address without masking.
- IPv6 source IPs – Each line contains an IPv6 address without prefix. Only the 8 MSB (Most Significant Bytes) are matched.
- IPv6 destination IPs – Each line contains an IPv6 address without prefix. Only the 8 MSB are matched.

Up to 2 IP list types can be used according to the device. Table 36 lists the different capabilities per device:

**Table 36: IP List Types per Device**

| Device | Number of Types | Total Number of IPs | Supported in Filter Modes |
|---|---|---|---|
| NPB Ie8 | 2 | 110,000 | l2-l4-ipv4.<br>In other modes when mpls-remove-mode = all\|l3 |
| NPB II | 2 | 15,000 | l2-l4-ipv4, l2-l4-ipv6, l3-l4-ipv4-ipv6-mpls |
| NPB IIe | 2 | 110,000 | l2-l4-ipv4.<br>In other modes when mpls-remove-mode = all\|l3 |
| NPB III | 1 | 40,000 | 2-l4-ipv4, l2-l4-ipv6, l3-l4-ipv4-ipv6-mpls,<br>l3-l4-ipv4-udf |

To set an IP list to use the dedicated HW memory, use the **Use HW** option when configuring the IP list.

**Note:**
A list's type is determined based on its content (IPv4 or IPv6) and its usage as a filter classifier (source or destination).

### Setting IP Lists as Filter Classifiers

To set an IP list as a filter classifier from the CLI, use one of the following commands according to the direction of the classifier (source, destination, or both):

```
NPB(config-filter-<name>)# l3-ip-src-list <ip-list-name>
NPB(config-filter-<name>)# l3-ip-dst-list <ip-list-name>
NPB(config-filter-<name>)# l3-ip-list <ip-list-name>
```

To unset an IP list as a filter classifier, use one of the following commands:

```
NPB(config-filter-<name>)# no l3-ip-src-list <ip-list-name>
NPB(config-filter-<name>)# no l3-ip-dst-list <ip-list-name>
NPB(config-filter-<name>)# no l3-ip-list <ip-list-name>
```

To set an IP list as a filter classifier using the WebUI, go to the Filters extension panel – **L3 filter parameters** and click **Source IP list, Destination IP list**, or **IP list**.

**Note:**
IP list classifiers (source, destination, both) cannot be combined with other IP classifiers unless the filter's logical operation is OR.

IP list classifiers cannot be combined with the IP source list and the IP destination list classifiers unless the filter's logical operation is OR.

## MPLS Filtering

MPLS (Multi-Protocol Label Switching) is a packet forwarding technique used in high-performance telecommunication networks. It uses labels rather than network addresses to for packet forwarding. As the name suggests, MPLS can be used to encapsulate various network protocols.

The NPB device supports filtering according to MPLS labels. Up to four labels can be used. Filtering according to MPLS labels is supported in **`l3-l4-ipv4-ipv6-mpls`** filter mode only.

Table 37 lists the classifiers for MPLS filtering.

**Table 37: MPLS Filtering Classifiers**

| Name | Description | Possible Values |
|---|---|---|
| l2-mpls-label1 | First MPLS label value | Decimal value in the range 0-1048578 |
| l2-mpls-label2 | Second MPLS label value | |
| l2-mpls-label3 | Third MPLS label value | |
| l2-mpls-label4 | Fourth MPLS label value | |
| l2-mpls-label1-mask | First MPLS label mask | Hexadecimal value in the range 0x00000-0xFFFFF |
| l2-mpls-label2-mask | Second MPLS label mask | |
| l2-mpls-label3-mask | Third MPLS label mask | |
| l2-mpls-label4-mask | Fourth MPLS label mask | |

When a value is set for any of the 4 MPLS positions, the NPB will verify that there is a valid label at this position and that its value matches the configured value and mask. Leaving a field empty means that the position is not checked for valid labels.

To match all labels, use label = 0 and mask = 0.

For example, the following setting will match traffic with 2 or more labels, with an MPLS label of 100 in the first position and an MPLS label of 200 in the second position:

```
l2-mpls-label1 = 100
l2-mpls-label1-mask = FFFFF
l2-mpls-label2 = 200
l2-mpls-label2-mask = FFFFF
```

As the third position is left empty, it can either contain an MPLS label or not.

Adding the following settings forces the third position to contain a valid MPLS label with any value:

```
l2-mpls-label3 = 0
l2-mpls-label3-mask = 0
```

**Note:**
The protocol encapsulated within the MPLS tunnel cannot be deterministically deduced and is known only at the MPLS end nodes. Therefore, it is not possible to use classifiers beyond the last MPLS label (e.g. L3 and L4 classifiers).

# Advanced Filter Classifiers

## Overview

To examine specific areas inside the packet that are not part of the supported L2 to L4 headers, we need more advanced classifiers. The NPB device supports User Defined Fragment (UDF) filtering that can be used in such cases. UDF allows the user to define a "window" in the incoming packet that will be matched against the UDF classifiers of the filter. UDF windows are defined globally for the entire system. The number of UDF windows is product-dependent as described below.

A common use case for this feature is when the traffic undergoes L4 tunneling and the user wishes to filter according to the tunnel's inner headers (e.g. the inner IPs or ports). The NPB device provides predefined configurations for the two most common tunnel types, which are GTP and L2TP.

**Note:**
To use the UDF feature, set the filter mode to one of the UDF modes: **`l4-udf`**, **`l3-l4-ipv4-udf`**, or **`l3-l4-ipv4-udf-vlb`**.

## Working with UDF Windows

The NPB UDF feature provides the user maximal flexibility to handle proprietary data or when filtering according to non-standard fields is required. UDF is available only if the filter mode is set to one of the UDF modes (**`l4-udf, l3-l4-ipv4-udf, l3-l4-ipv4-udf-vlb`**).

A UDF window is a fixed-sized segment that starts at a specific offset from a given starting point. UDF windows are defined globally for the entire system. Each of the global UDF windows can be configured separately. Overlaps are allowed.

Table 38 lists the global UDF window attributes.

**Table 38: Global UDF Window Attributes**

| Parameter | Description | Possible Values |
|---|---|---|
| name | UDF window name | Free text, up to 32 characters |
| description | UDF window description | Free text, up to 128 characters |
| start point | UDF window starting point.<br>The UDF window itself starts **`offset`** bytes beyond **`start point`**. | NPB I, Ie, II, III, and IV: l2, l3, l4<br>NPB Ie8, IIe: l2, l3, l4, vlan, mpls<br><br>Default is **`l2`**. |
| offset | The UDF window starts **`offset`** bytes beyond **`start point`**. | The maximal supported offset depends on the start-point and length fields.<br>In NPB Ie, the maximal offset is 50 bytes.<br>In NPB Ie8 and IIe, in l2 format the maximal offset is 62 or 60 according to the format length.<br>NPB IV: up to 50 bytes<br><br>Note that in all products, only the first 128 Bytes of each packet are visible to UDF.<br><br>Must be even, default is 0 |
| length | UDF window length | Product-dependent, see Table 39 |
| format | Specify the format of the packets this UDF is applied to<br>Valid for NPB Ie8 and IIe only | See Section UDF Formats (NPB Ie8 and IIe Only) on p.131 |

The size of the UDF windows differs per product as listed in Table 39.

**Table 39: UDF Window Sizes**

| Device | UDF Mode | Num. of UDF Windows | UDF Window Sizes |
|---|---|---|---|
| NPB I | l3-l4-ipv4-udf, l3-l4-ipv4-udf-vlb | 2 | One window of 8 bytes and one window of either 8 or 16 bytes |
| | l4-udf | 2 | Two windows of either 8 or 16 bytes |
| NPB Ie | l3-l4-ipv4-udf | 9 | Each window can be 2-16 bytes long. Maximal total windows size is 19 bytes. |
| | l4-udf | 16 | Each window can be 2-16 bytes long. Maximal total windows size is 32 bytes. |
| NPB II | All | 16 | Each window can be 2-16 bytes long. Maximal total windows size is 32 bytes. |
| NPB Ie8 and NPB IIe | All | According to selected format | Each window can be 2-28 bytes long. Maximal total windows size is according to the selected format. |
| NPB III | All | 16 | Each window can be 2-32 bytes long. Maximal total windows size is 32 bytes. |
| NPB IV | All | 16 | Each window can be 2-16 bytes long. Maximal total windows size is 32 bytes. |

**Note:**
UDF cannot be used in filters that use the **copy** action.

### UDF Formats (NPB Ie8 and IIe Only)

In NPB Ie8 and IIe, each UDF window defines the type of packets it is applied to. Packets that are not of this type are never considered a match for the UDF. This mechanism eliminates false positive matching. In each filter, only one UDF of a given format can be used. The list of supported formats is shown in Table 40.

**Table 40: Supported UDF Formats**

| Format Name | Description of Matched Packets | Start Point | Maximal Size in Bytes |
|---|---|---|---|
| l2 | L2 header is present | Start of L2 header | 4 |
| l3-all | L3 header is present | Start of L3 header | 4 |

| Format Name | Description of Matched Packets | Start Point | Maximal Size in Bytes |
|---|---|---|---|
| l3-ipv4-frag-non-opt | L3 is fragmented IPv4 without options | Start of L3 header | 10 |
| l3-ipv4-frag-with-opt | L3 is fragmented IPv4 with options | Start of L3 header | 4 |
| l3-ipv4-non-opt | L3 is non fragmented IPv4 without options | Start of L3 header | 12 |
| l3-ipv4-with-opt | L3 is non fragmented IPv4 with options | Start of L3 header | 6 |
| l3-ipv6 | L3 is IPv6 | Start of L3 header | 8 |
| l3-known-non-ip | L3 is a known, non-IP protocol | Start of L3 header | 28 |
| l3-unknown | L3 is unknown | Start of L3 header | 4 |
| l4-all | L4 header is present | Start of L4 header | 16 |
| l4-tcp | L4 is TCP | Start of L4 header | 16 |
| l4-udp | L4 is UDP | Start of L4 header | 16 |
| l4-sctp | L4 is SCTP | Start of L4 header | 16 |
| l4-unknown | L4 is unknown | Start of L4 header | 16 |
| mpls-all | At least on MPLS label is present | Start of MPLS labels | 12 |
| mpls-one-label | Exactly one MPLS label is present | Start of MPLS label | 12 |
| mpls-two-label | Exactly two MPLS labels are present | Start of MPLS labels | 12 |
| mpls-three-label | Exactly three MPLS labels are present | Start of MPLS labels | 12 |
| mpls-four-label | Exactly four MPLS labels are present | Start of MPLS labels | 12 |
| mpls-more-then-four-label | More than four MPLS labels are present | Start of MPLS labels | 12 |
| vlan-all | One or more VLAN tags are present | 14 bytes beyond start of L2 header | 12 |
| vlan-double | Exactly two VLAN tags are present | 14 bytes beyond start of L2 header | 12 |

| Format Name | Description of Matched Packets | Start Point | Maximal Size in Bytes |
|---|---|---|---|
| vlan-single | Exactly one VLAN tag is present | 14 bytes beyond start of L2 header | 12 |
| gre-all | All GRE traffic types as described below | Start of GRE header | 16 |
| gre-l3-header-4-bytes | L3 GRE with GRE header length of 4 bytes | Start of GRE header | 16 |
| gre-l3-header-8-bytes | L3 GRE with GRE header length of 8 bytes | Start of GRE header | 16 |
| gre-l3-header-12-bytes | L3 GRE with GRE header length of 12 bytes | Start of GRE header | 16 |
| gre-l3-header-16-bytes | L3 GRE with GRE header length of 16 bytes | Start of GRE header | 16 |
| gre-l3-header-20-bytes | L3 GRE with GRE header length of 20 bytes | Start of GRE header | 16 |
| gre-l2-header-4-bytes | L2 GRE with GRE header length of 4 bytes | Start of GRE header | 16 |
| gre-l2-header-8-bytes | L2 GRE with GRE header length of 8 bytes | Start of GRE header | 16 |
| gre-l2-header-12-bytes | L2 GRE with GRE header length of 12 bytes | Start of GRE header | 16 |
| gre-l2-header-16-bytes | L2 GRE with GRE header length of 16 bytes | Start of GRE header | 16 |
| gre-l2-header-20-bytes | L2 GRE with GRE header length of 20 bytes | Start of GRE header | 16 |

The Supported UDF Formats table can be displayed in CLI, using the following command:

```
NPB-IIe# show filters udf-window formats-info
```

In WebUI, use the **Format Info** button in the **User Defined Filters** section.

### Setting UDF Windows

To set a UDF window from the CLI, use the following command:

NPB I, Ie, II, III, and IV:

```
NPB(config)# filters udf-window udf <name> [description
<description>] length <length> [start-point l2|l3|l4] [offset
<offset>]
```

NPB Ie8 and IIe:

```
NPB(config)# filters udf-window udf <name> [description
<description>] length <length> [start-point l2|l3|l4|vlan|mpls]
[offset <offset>] format <format>
```

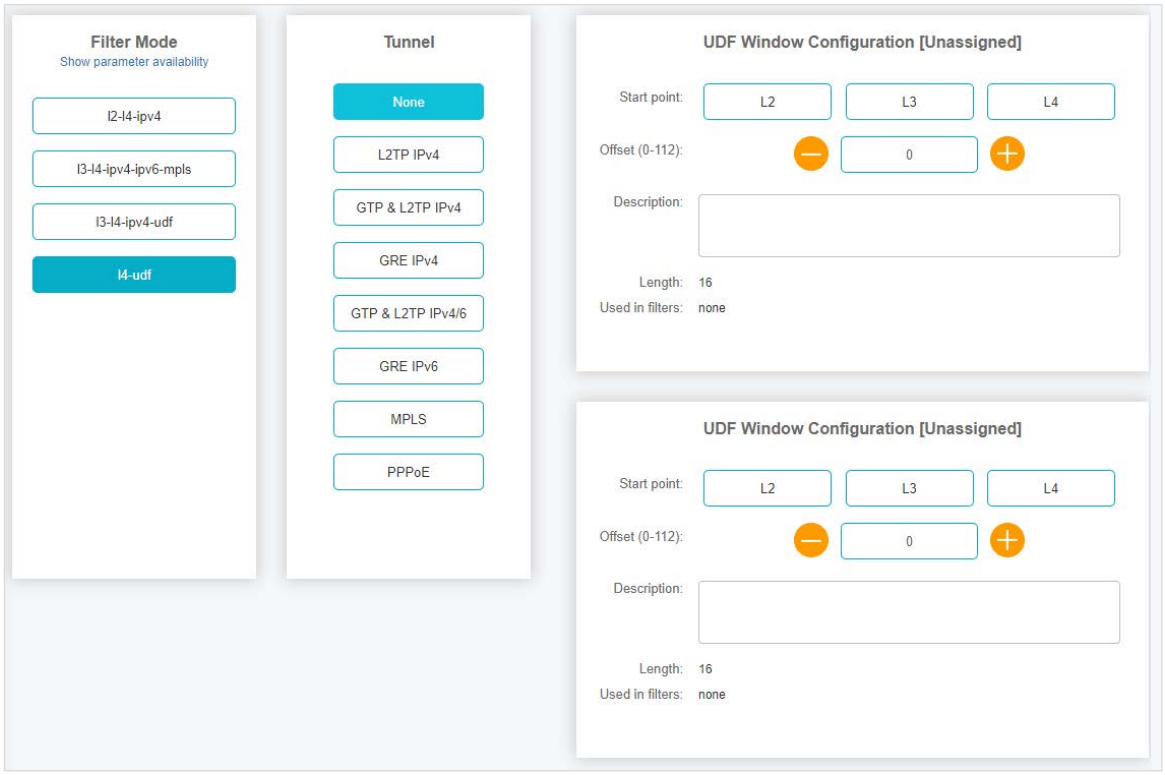
To display the configured UDF window from the CLI, use the following command:

```
NPB# show filters udf-window [udf <name>]
```

To manage UDF windows using the WebUI, select **Filter – Globals** in the Navigation panel. Select one of the UDF modes on the left and select the tunnel type. Use **None** if no tunnel support is required. Tunnels are described later in this chapter.

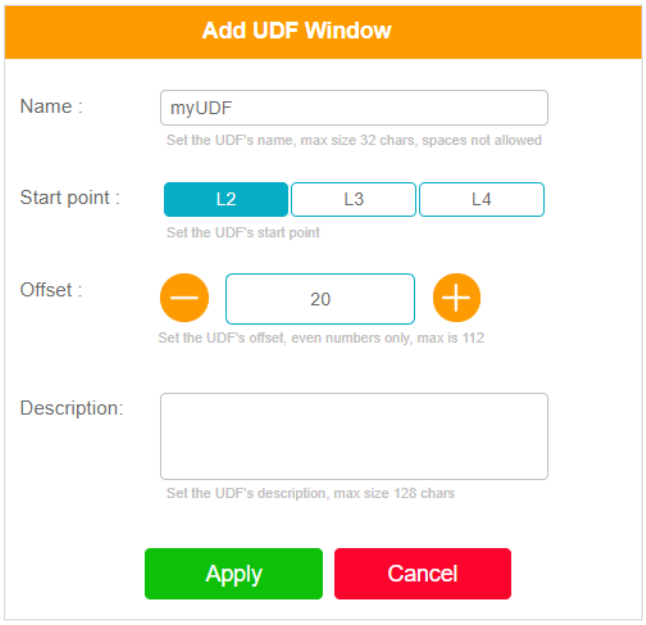
NPB I allows to set the UDF parameters for each window in the **Filter – Globals** screen as shown in Figure 70.

**Figure 70: Managing UDF Windows using the WebUI**



Click on one of the windows, and fill in the parameters in the popup:

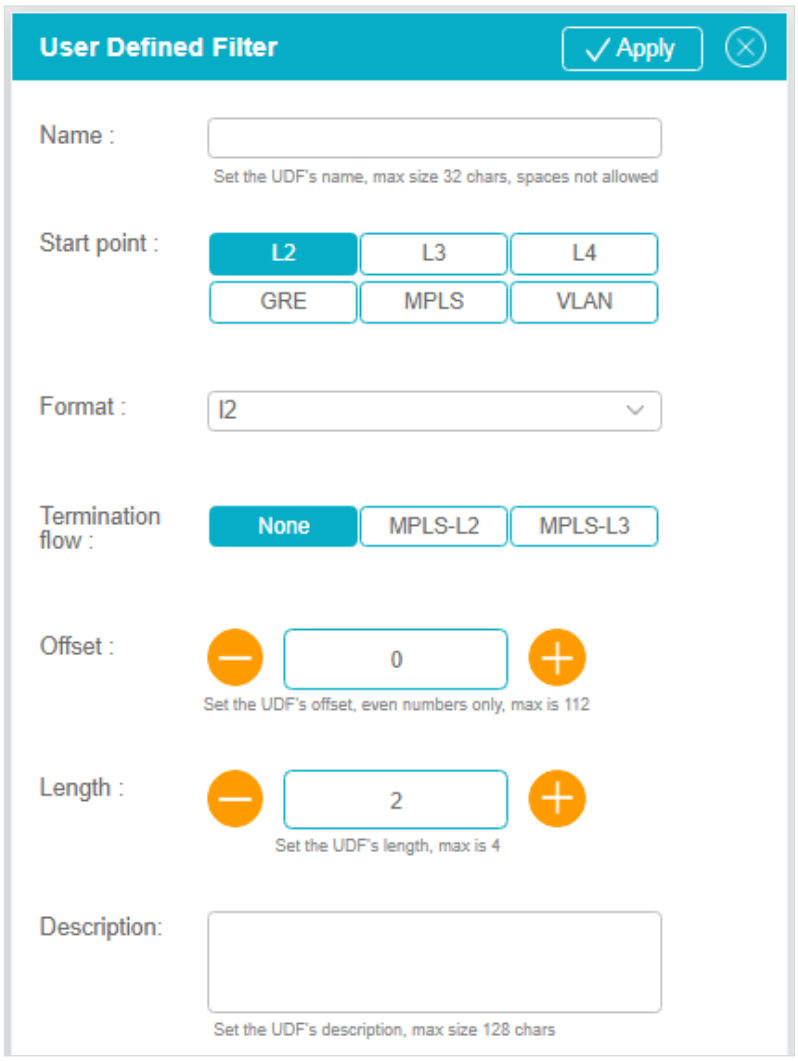
**Figure 71: Defining UDF Window Parameters**



In NPB Ie, Ie8, II, IIe, III and IV, UDF windows are managed as follows:

1. Select **Filter – User Defined Filters** in the Navigation panel.
2. Click an existing window to update it, or click **Add** to add a new window.
3. Set the relevant parameters in the UDF window extension panel.

**Figure 72: NPB Ie8 and IIe UDF Extension Panel**




### Setting UDF Windows as Filter Classifiers

Once defined, UDF windows can be used as filter classifiers. UDF classifiers are considered to match an incoming packet if the packet's content at the relevant segment matches one or more of the pattern and mask pairs configured for the UDF. If formats are used, the packet must be of the exact format specified. (This feature is applicable for NPB Ie8 and IIe only.)

Table 41 lists the UDF filter classifiers.

**Table 41: UDF Filter Classifiers**

| Name | Description | Possible Values |
|---|---|---|
| Pattern | Pattern to match in UDF window | Hexadecimal digits according to the UDF window size, 2 digits per byte. Pattern and mask must have equal lengths. |
| Mask | Optional mask for UDF window pattern | |

To set a UDF classifier from the CLI, use the following command:

```
NPB(config-filter-<name>)# udf <udf-name> pattern <pattern>[/mask
<mask>][,pattern <pattern>[/mask <mask>] [...]
```

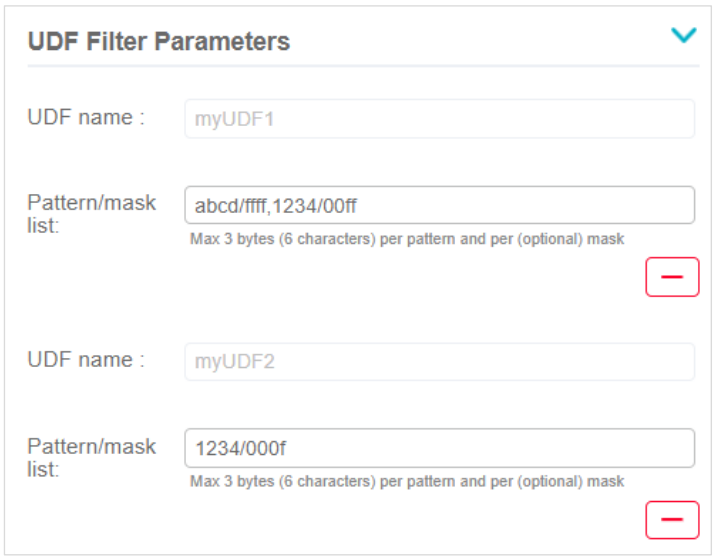
To set UDF classifiers in the WebUI, use the Classifiers tab in the filter extension panel:

1. In the **UDF Filter Parameters** panel, fill the UDF name, pattern, and mask.

   Use a slash '/' to add a mask to a specific pattern and a comma ',' to separate between pairs (similar to the CLI syntax).

2. Click **+** or **–** to add or remove more UDFs to this filter.

**Figure 73: Setting UDF Classifiers**




### UDF Limitations

Pay special attention to these two cases:

- If the packet's length is shorter than the defined window and pattern, the packet is not considered a match.
- If the UDF window and pattern exceeds the packet's 128 first bytes, the packet is not considered a match.

As an example, consider the following UDF window and pattern configuration:

| | |
|---|---|
| Starting point: | Layer 4 |
| Offset: | 100 |
| Pattern: | ABCD (length is 2) |

If the position of the pattern's last byte (L4 + 100 + 2) is beyond the packet boundaries or beyond the packet's first 128 bytes, the packet is not considered a match.

## Working with Tunnels

The NPB device supports predefined configurations for GRE, GTP, L2TP, MPLS, and PPPoE tunnel types. This allows the user to configure classifiers for these tunnels without having to deal with their exact packet structure. This mechanism uses the UDF windows described earlier.

Only after the tunnel type is selected at the system level, it is possible to add its classifiers.

Table 42 lists the supported tunnels:

**Table 42: Supported Tunnels**

| Tunnel | Devices | Tunnel Classifiers | Notes |
|---|---|---|---|
| GTP | NPB Ie8/IIe | GTP<br>IPv4 address | |
| GTP | NPB<br>Ie/II/III/IV | GTP<br>Protocol number<br>IPv4 address<br>L4 ports | |
| L2TP | All | L2TP<br>IPv4 address<br>L4 ports<br>Protocol number | |
| GTP and L2TP IPv4 | NPB<br>I/Ie/II/IV | GTP<br>GTP message type<br>GTP TEID<br>L2TP<br>IPv4 address<br>L4 ports<br>Protocol number | |
| gtp-ipv4-and-ipv6-src-msb | NPB Ie8/IIe | GTP<br>IPv4 address<br>IPv6 source address | IPv6 source address coverage depends on GTP header format. |
| gtp-ipv4-ipv6-dst-msb | NPB Ie8/IIe | GTP<br>IPv4 destination address<br>IPv6 address | IPv4 destination address and IPv6 address coverage depend on GTP header format. |

| Tunnel | Devices | Tunnel Classifiers | Notes |
|---|---|---|---|
| GTP and L2TP IPv4/6 | NPB I/Ie/II/IV | GTP<br>L2TP<br>IPv4/6 address<br>L4 ports (in IPv4)<br>Protocol number (in L2TP) | IPv6 source address coverage depends on GTP header format. |
| GTP and L2TP High IPv4/6 | NPB II | GTP<br>L2TP<br>IPv4/6 address<br>L4 ports (in IPv4)<br>Protocol number (in L2TP) | IPv6 destination address coverage depends on GTP header format, MSB part is always covered. |
| GTP and L2TP Hash IPv4/6 | NPB II | GTP<br>L2TP<br>IPv4/6 address<br>L4 ports (in IPv4)<br>Protocol number (in L2TP) | IPv6 destination address coverage depends on GTP header format, reduces the chance of false positive by verifying GTP and IP versions |
| GRE IPv4 | All except NPB I | GRE<br>IPv4 address<br>L4 ports<br>Protocol number | |
| GRE IPv6 | NPB II | GRE<br>IPv4 address<br>IPv6 address<br>L4 ports<br>Protocol number | |
| GRE IPv6 | NPB Ie8/IIe | GRE<br>IPv4 address<br>IPv6 address<br>Protocol number | IPv6 source and destination addresses coverage is 12 and 4 bytes respectively (MSB) |

| Tunnel | Devices | Tunnel Classifiers | Notes |
|---|---|---|---|
| MPLS | All | MPLS<br>L2<br>L3 (IPv4) | An MPLS tunnel, not being a L3 tunnel, does not add any new classifiers. The regular L2 and L3 classifiers are applied to the tunneled payload. MPLS supports only IPv4 classifiers.<br>In NPB Ie8 and IIe, IP fragments and protocol classifiers are not supported.<br><br>In NPB I, II and IV, a combination of up to 3 MPLS and VLAN headers is supported (i.e. 3 MPLS labels, or 2 MPLS labels and one VLAN header, or one MPLS label and 2 VLAN headers).<br>In NPB Ie8 and IIe, up to 5 MPLS labels and 3 VLANs are supported. |
| PPPoE | All | L3 (IPv4)<br>L3 (IPv6 in NPB II and NPB III)<br>L4 ports<br>Protocol number | A PPPoE tunnel, not being a L3 tunnel, does not add any new classifiers. The regular classifiers are applied to the tunneled payload. PPPoE supports only IPv4 classifiers. |

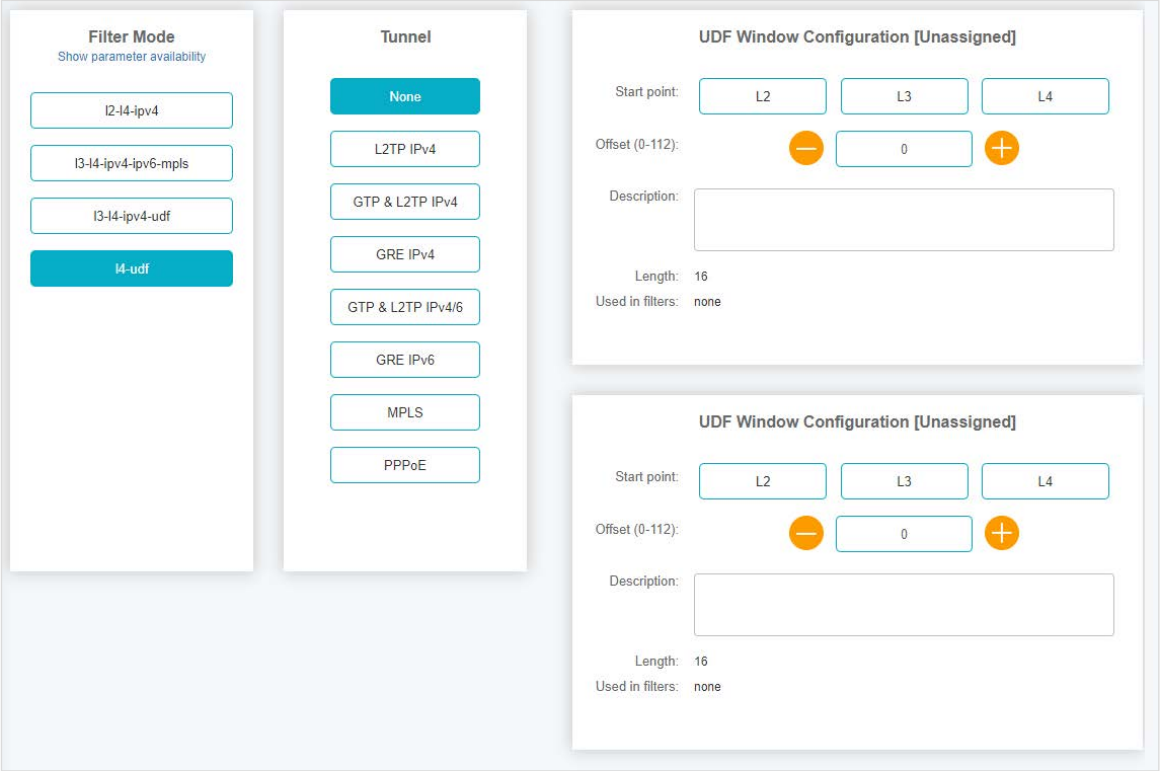
To set the tunnel type from the CLI, use the following command:

```
NPB(config)# filters udf-window tunnel none|gre|gre-ipv6|gtp-
l2tp|gtp-l2tp-ipv4-ipv6|gtp-l2tp-ipv4-ipv6-high| gtp-l2tp-ipv4-ipv6-
hash|gtp-ipv4-and-ipv6-src-msb|gtp-ipv4-ipv6-dst-msb|l2tp|mpls|pppoe
```

To set the tunnel type using the WebUI, select **Filter – Mode** in the Navigation panel. Select the UDF mode on the left, and select the tunnel type (GTP, L2TP, GRE, MPLS, or PPPoE).

**Note:**
The UDF windows used by the tunnel and their details are displayed after the tunnel is selected. In Figure 74 for example, the second UDF is used by L2TP with a predefined start point set to L4 and an offset that equals 28.

**Figure 74: Setting the Tunnel Type using the WebUI**




**Note:**
Tunnels use one or more UDF windows. UDF windows that are not being used by the tunnel can still be used independently as described in Section Working with UDF Windows on p.130.

Once the tunnel type has been set, filters can be configured to work with the selected tunnels, using the set of classifiers listed in Table 43. The availability of classifiers is set according to the tunnel type as described in Table 42: Supported Tunnels.

**Table 43: GTP, L2TP, and GRE Filter Classifiers**

| Name | Description | Possible Values |
|---|---|---|
| gtp-msg-type | GTP message type value | 1-255 |
| gtp-teid | GTP tunnel endpoint ID value | 8-digit hexadecimal value |
| gtp-teid-mask | GTP tunnel endpoint ID mask | |

| Name | Description | Possible Values |
|---|---|---|
| tunnel-protocol-number | IPv4 protocol number | For the complete list, see http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml |
| tunnel-ipv4-addr | Inner source or destination IPv4 | A comma-separated list of valid IPv4 addresses with an optional mask or CIDR. For example: 1.0.0.1, 10.0.0.1/255.255.255.0, 20.0.0.1/32 |
| tunnel-ipv4-dst-addr | Inner destination IPv4 | |
| tunnel-ipv4-src-addr | Inner source IPv4 | |
| tunnel-ipv6-addr | Inner source or destination IPv6 | A comma-separated list of valid IPv6 addresses with an optional mask or CIDR. For example: 2001:db8:0:0:1::1, 2002:db8:0:0:1::1/1::1, 2003:db8:0:0:1::1/32 |
| tunnel-ipv6-dst-addr | Inner destination IPv6 | |
| tunnel-ipv6-src-addr | Inner source IPv6 | |
| tunnel-l4-port | Inner source or destination port | A comma-separated list of valid Layer 4 ports |
| tunnel-l4-sport | Inner source port | |
| tunnel-l4-dport | Inner destination port | |

To configure tunnel filter classifiers from the CLI, first set the system-level setting as described above, then set the filter tunnel type:

```
NPB(config-filter-<name>)# tunnel-gre|tunnel-l2tp|tunnel-gtp-l2tp
```

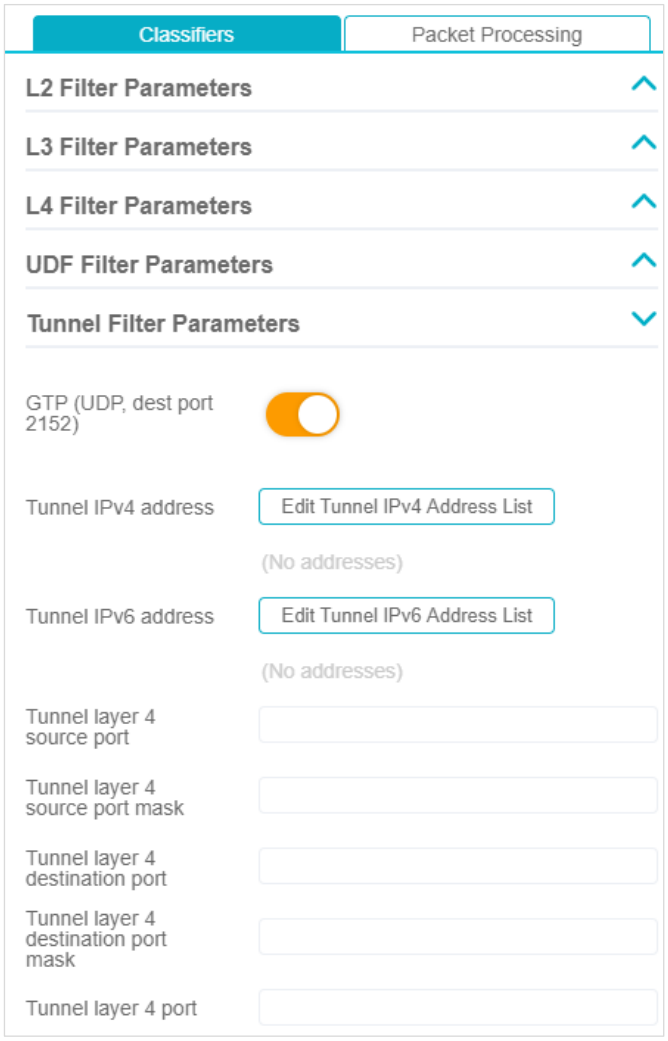
After setting the tunnel type, all tunneled traffic will be matched. The filter can be further refined using additional classifiers.

Tunnel classifiers are set using the CLI as any other classifier, e.g. in the filter context:

```
NPB(config-filter-<name>)# tunnel-ipv4-src-addr 127.0.0.1
```

To set tunnel classifiers using the WebUI, use the Classifiers tab in the filter extension panel. Select **Tunnel Filter Parameters** and fill in the relevant parameters. Use other **Filter Parameters** sections to add more classifiers.

**Figure 75: Setting Tunnel Classifiers (L2TP)**




### GTP and L2TP Packet Recognition

The NPB device recognizes the tunnel type as follows:

| | |
|---|---|
| GTP | IP protocol is UDP, destination port is 2152 |
| L2TP | Destination port is 1701 |
| GRE | IP protocol is 43 |

# Advanced Filter Actions

The NPB supports a set of advanced actions per filter that can be applied on the matched traffic. Advanced actions can be combined. The following list presents the set of NPB advanced actions:

- Timestamping (NPB Ie8 and NPB IIe)
- MAC address replacement
- VLAN editing
- Packet slicing (NPB Ie, NPB Ie8, NPB IIe, and NPB III)

## Timestamping

NPB Ie8 and NPB IIe support timestamping of packets matched by the filter. The timestamp value reflects the received time and is added as a trailer to the packet. Filter timestamping overwrites the port Rx timestamp if present.

For a description of the timestamp trailer refer to Section Timestamping (NPB Ie8 and NPB IIe) on p.88. Filter timestamping uses ID 0.

To set filter timestamping from the CLI, use the following command:

```
NPB(config-filter-<name>)# set-timestamp
```

To clear filter timestamping from the CLI, use the following command:

```
NPB(config-filter-<name>)# no set-timestamp
```

To set a timestamping action using the WebUI, use **Timestamp** in the Packet Processing tab in the filter extension panel.

## MAC Replacement

The NPB supports the replacement of MAC addresses.

To set a source and destination MAC replacement action from the CLI, use the following commands:

```
NPB(config-filter-<name>)# smac-replace <new-source-mac>
```

```
NPB(config-filter-<name>)# dmac-replace <new-destination-mac>
```

To clear a MAC replacement action from the CLI, use the following command:

```
NPB(config-filter-<name>)# no smac-replace|dmac-replace
```

To set a source and destination MAC replacement action using the WebUI, use **MAC replace** on the Packet Processing tab in the filter extension panel.

**Note:**
MAC replace is not supported in NPB Ie and IV.

## VLAN Editing

The NPB device supports a Set Outer VLAN operation. For untagged packets, the given VLAN tag is added. For tagged packets, the given VLAN tag replaces the outermost VLAN tag.

This operation can be combined with port-ingress VLAN editing. The outcome of the port ingress operation is visible at the filter processing stage. For example, using an Add ingress action with VLAN tag 100 and applying a Set Outer VLAN filter action with VLAN tag 200 results in replacing VLAN 100 (set at ingress) with VLAN 200.

To set VLAN editing from the CLI, use the following command:

```
NPB(config-filter-<name>)# vlan-set-outer <vlan-id>
```

To clear VLAN editing from the CLI, use the following command:

```
NPB(config-filter-<name>)# no vlan-set-outer
```

To set VLAN editing using the WebUI, use **VLAN Action** on the Packet Processing tab in the filter extension panel.

**Note:**
VLAN editing is not supported in NPB Ie and IV.

## Packet Slicing

NPB Ie, NPB Ie8, NPB IIe, and NPB III support packet slicing. When set, matched packets are sliced after a predefined number of bytes. Packet content is not modified except for the Ethernet CRC value

Table 44 lists supported slicing sizes per device.

**Table 44: Packet Slicing Size per Device**

| Device | Supported Slice Values | Limitations |
|---|---|---|
| NPB Ie | 64 (sliced at 45, padded with zeros till 64), 109, 173 | The total number of different output ports in filters using packet slicing is limited to 14. |
| NPB Ie8 | 192 | |
| NPB IIe | 192 | |
| NPB III | 214 | |

To set a packet slicing action from the CLI, use the following commands:

```
NPB(config-filter-<name>)# set-slice <slice-value>
```

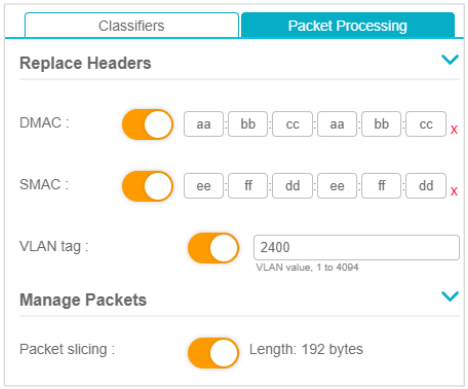
To clear a packet slicing action from the CLI, use the following command:

```
NPB(config-filter-<name>)# no set-slice
```

To set a packet slicing action using the WebUI, use **Slicing** on the Packet Processing tab in the filter extension panel.

**Note:**
The amount of output ports in all filters that are using the packet slicing operation is limited to four in NPB Ie8, NPB IIe, and NPB III. A slice action cannot be used if the filter output contains load balancing groups or tunnel interfaces.

**Figure 76: Setting a Slicing Action using the WebUI**



# Inline Solution

Security and monitoring tools can be connected inline to the network, meaning that traffic arriving from the network is directed through the tool and back to the network. Placing the NPB between the network and the tools provides the following advantages:

- Allows protection against tool failures
- Reduces tool overload by classifying the traffic before sending it to tool
- Enables sharing tools amongst different networks
- Enables load balancing traffic over several tools

The NPB supports 3 types of inline solutions:

- Inline tool – represents a single tool connected to the NPB
- Inline load balance group – represents a group of inline tools connected to the NPB. Traffic is distributed between the group members.
- Tool chain – represents an ordered chain of inline tools and inline load balance groups connected to the NPB. Traffic flows from the network to the first element of the chain, then to the second element, and so on, until it reaches the last element, from which it is redirected back to the network.

These solutions are described later in this section.

To define an inline solution, perform the following steps:

1. Connect the tool to one or two NPB ports. These are called *tool* **`port-a`** and **`port-b`**.
2. Connect the network to one or two NPB ports. These are called *network* **`port-a`** and **`port-b`**.
3. Optionally, create one or more heartbeat profiles and configure the external tools to return heartbeat messages seen on *tool* **`port-a`** to *tool* **`port-b`** (and vice versa if the solution is bidirectional).
4. Create one or more inline tools, attach heartbeat profiles to them, and set their port-a and port-b parameters to the ports to which you connected the tool.
5. Group several inline tools into inline load balance groups if needed.
6. Create an inline tool chain that contains the inline tools and inline load balance groups in the required order. This step is optional when using a single tool or a single load balance group as these can be used directly, without a chain.
7. Create a filter that uses the inline solution, set the *network* **`port-a`** and **`port-b`** as the filter's input and output ports. Set the filter as **`bidirectional`** if needed.

The solution's components are described in detail below.

# Inline Tools

An inline tool represents an external tool that is connected inline to the NPB. The inline tool status is based on the status of the NPB physical links it is connected to (*tool* **port-a** and **port-b**) and, if configured, on the tool's health as reported by its heartbeat profile. Upon failover, the action set in the **failover-action** parameter is applied. When the tool is recovered, traffic is redirected to it again.

The NPB supports up to 64 inline tools. Each inline tool contains the following attributes:

**Table 45: Inline Tool Attributes**

| Name | Description | Possible Values |
|---|---|---|
| name | Inline tool name | Free text, up to 32 characters |
| description | Inline tool description | Free text, up to 128 characters |
| heartbeat-profile | Heartbeat profile to use for detecting the tool status | Valid heartbeat profile name |
| port-a<br>port-b | **port-a** and **port-b** are the physical interfaces to which the inline tool is connected.<br>If **port-b** is not given, it is assumed that the tool is connected only to **port-a**. In this case, heartbeat messages sent on **port-a** are expected to be received back on **port-a**. | Valid port ID |
| failover-action | Action to take in case of failover | **nw-down** – forces the network ports to be down<br>**nw-drop** – drops traffic received on network input port<br>**nw-bypass** – redirects traffic from network input port to network output port<br>**tool-bypass** – bypasses the tool by redirecting traffic from one network port to the other<br>**tool-drop** – drops all traffic destined to the tool<br>Default is **tool-bypass** |

Inline tools can be placed into Failed mode manually. This is useful to simulate failures or to take the inline tool offline for maintenance.

**Note:**
When several tools share the same ports, the user must make sure that each tool is using a different heartbeat message, for example by using different custom messages or ARP messages with different target IPs. Failing to do so may result in wrong failure indications.

**Note:**
Inline tools are not supported in NPB Ie.

To set an inline tool from the CLI, use the following command:

```
NPB(config)# inline tool <name> [description <description>] port-a
<port-id> [port-b <port-id>] [heartbeat-profile <profile-name>]
[faileover-action nw-down|nw-drop|nw-bypass|tool-bypass|tool-drop]
```

To delete an inline tool from the CLI, use the following command:

```
NPB(config)# no inline tool <name>
```

To place an inline tool into Failed mode from the CLI, use the following command:

```
NPB(config)# inline tool <name> force-failover
```

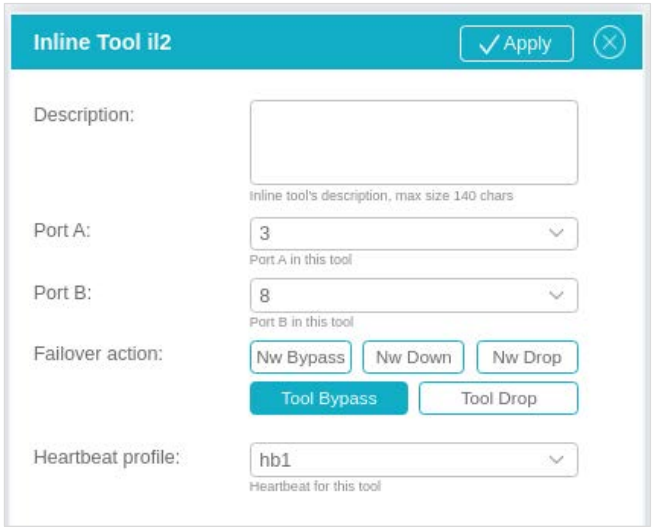
To place an inline tool back into Normal mode from the CLI, use the following command:

```
NPB(config)# inline tool <name> clear-failover
```

To manage inline tools using the WebUI, proceed as follows:

1. Select **Inline – Tools** in the Navigation panel.
1. Click an existing tool to update it, or use the **Add** button to add a new one.
2. Set the relevant parameters in the extension panel.
3. To delete a line, use the checkbox next to the line you wish to delete, and use the **Delete** button.
4. To place a tool in/out of Failed mode, use the **Force Failover** and **Clear Failover** buttons above the table

**Figure 77: Inline Tool Extension Panel**




## Heartbeat Profiles

Heartbeat profiles are used for monitoring inline tools and detect their health status. Heartbeat messages sent to a tool's interface are expected to be received back on its other interface (*tool* **`port-a`** and **`port-b`**). Normally, messages are expected to be received back without any modifications. However, when using an ARP request message, an ARP reply is accepted as well. Failing to receive these packets indicates that the tool has failed. The NPB keeps sending heartbeat messages to failed tools to detect their recovery.

The NPB supports up to 32 heartbeat profiles. Each heartbeat profile contains the following attributes:

**Table 46: Heartbeat Profile Attributes**

| Name | Description | Possible Values |
|---|---|---|
| name | Profile name | Free text, up to 32 characters |
| description | Profile description | Free text, up to 128 characters |

| Name | Description | Possible Values |
|---|---|---|
| direction | Specifies the direction of the heartbeat messages | **a-b** – Messages are sent from **port-a** and are expected to be received on **port-b**.<br>**b-a** – Messages are sent from **port-b** and are expected to be received on **port-a**.<br>**bidirectional** – Messages are sent from **port-a** and from **port-b** and are expected to be received on **port-b** and **port-a** respectively<br>Default is **bidirectional** |
| pkt-format | Heartbeat messages format. In all formats, the device MAC is used as source MAC. | **arp** – use gratuitous ARP message format<br>**ipx** – use IPX message format<br>**custom** – use a proprietary message format<br>Default is **ipx** |
| pkt-pattern | Custom message pattern; valid when **pkt-format** is **custom**. The device MAC is used as source MAC. | Hexadecimal stream, up to 512 characters long. Each two characters stand for one byte. |
| arp-target-ip | Target IP to use in ARP messages. Valid when **pkt-format** is **arp.** | Valid IPv4 address<br>Default is 0.0.0.0 |
| ipx-dst-address | Destination address to use in IPX messages. Valid when **pkt-format** is **ipx.** | Valid IPX address (12 bytes hex string)<br>Default is 00000102000000003040001 |
| interval | The number of milliseconds to wait between sending subsequent heartbeat packets | 30-5000 (msec)<br>Default is 1000 |
| timeout | The number of milliseconds to wait for a transmitted packet to be received back | 20-3000 (msec)<br>Default is 500 |
| Retry | The number of timed-out packets before announcing a failover | 0-5<br>Default is 3 |
| recovery-count | The number of successfully received packets before recovering from a failover | 1-120<br>Default is 3 |

**Note:**
Heartbeat profiles are not supported in NPB Ie.

To set a heartbeat profile from the CLI, use the following command:

```
NPB(config)# heartbeat profile <name> [description <description>]
[pkt-format ipx|arp|custom] [pkt-pattern <hex-pattern>] [arp-target-
ip <address>] [ipx-dst-address <address>] [interval <time>] [timeout
<time>] [retry <num>] [recovery-count <num>] [direction a-b|b-
a|bidirectional]
```

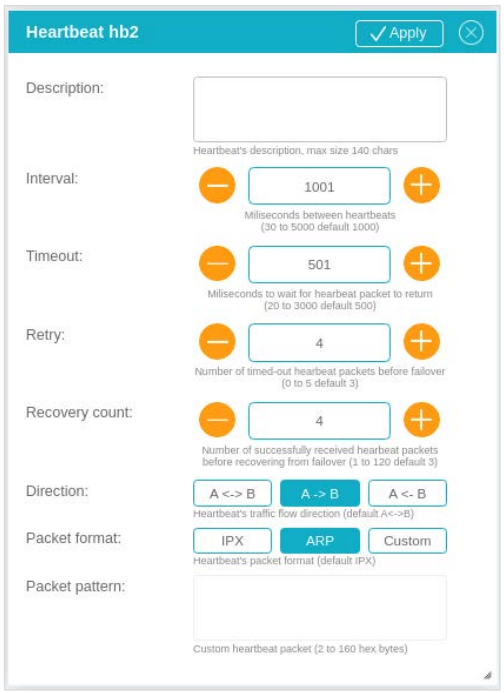
To delete a heartbeat profile from the CLI, use the following command:

```
NPB(config)# no heartbeat profile <name>
```

To manage heartbeat profiles using the WebUI, proceed as follows:

1. Select **Inline – Heartbeats** in the Navigation panel.
2. Click an existing profile to update it, or use the **Add** button to add a new one.
3. Set the relevant parameters in the extension panel.
4. To delete a line, use the checkbox next to the line you wish to delete, and click **Delete**.

**Figure 78: Heartbeat Profile Extension Panel**




# Inline Tool Load Balancing Groups

Network traffic can be load-balanced across several inline tools, using an inline load balancing group.

Load balance capabilities, such as hashing and standby, as described in Section Load Balancing on p.163, are supported for inline load balance groups.

Failover actions are applied only in case a tool has failed and there is no available standby tool in the group that can replace it. Two layers of failover actions are supported:

- Global failover for the entire group
- Failover per tool

If the group's failover action is **`per-tool`**, the failed tool's failover action is applied. Otherwise, the group's failover action is applied.

To configure inline load balancing, see Section Load Balancing on p.163.

## Inline Tool Chains

Network traffic can be redirected to an ordered chain of inline tools and inline load balance groups. Ingress traffic is redirected to the first element in the chain. Received traffic from that element is then redirected to the second element and so on. In case of inline load balancing groups, traffic is distributed across the group's active members. Traffic received from the last element is redirected back to the network.

Failover actions are applied when any of the tools fails. Two layers of failover actions are supported:

- Global failover for the entire chain
- Failover per tool

If the chain's failover action is **`per-tool`**, the failed tool's failover action is applied. Otherwise, the chain's failover action is applied.

**Note:**
If the failed tool is a member of an inline load balance group, this group failover action is applied as described above.

To create an inline tool chain from the CLI, use the following command:

```
NPB(config)# inline toolchain <name> [description <description>]
tools <comma separated list of tool names or lbg ids>
```

The ID of a load balance group is prefixed with lb_, for example: lb_1.

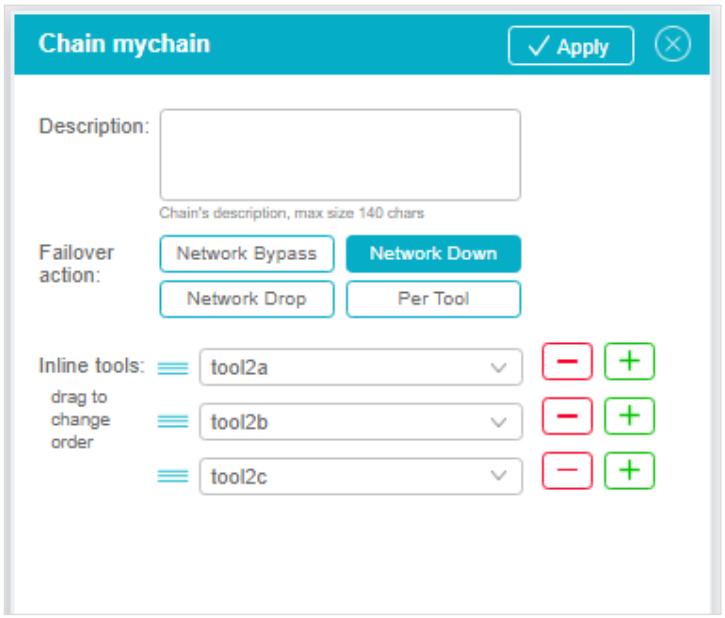
To delete an inline tool chain from the CLI, use the following command:

```
NPB(config)# no inline toolchain <name>
```

To manage an inline tool chain using the WebUI, proceed as follows:

1. Select **Inline - Chain** in the Navigation panel.
2. Click an existing chain to update it, or use the **Add** button to add a new one.
3. Set the relevant parameters in the extension panel.
4. To delete a line, use the checkbox next to the line you wish to delete, and use the **Delete** button.

**Figure 79: Managing an Inline Tool Chain**




## Inline Filters

Inline networks and Inline solutions are associated using filters. This allows the user to control which traffic is forwarded to which tools by using the filter's classifiers and to apply filter actions as needed.

Set *network* **`port-a`** and **`port-b`** as the filter's input and output ports. Set the filter as **`bidirectional`** if network traffic is bidirectional.

For more details on creating filters and on filter classifiers and actions, see Section Filtering on p.102.

To set an inline filter from the CLI, use the following command:

```
NPB(config)# filters filter <name> input-ports <port-id> output-port
<port-id> action redirect inline <tool-name|lb-id|chain-name>
[bidirectional]
```

Make sure to prefix the load balance group ID with **`lb_`**.

To unset an inline filter from the CLI, use the following command:

```
NPB(config)# filters filter <name> no inline
```

To manage inline filters from the WebUI, select **Filters – Rules** in the Navigation panel and use the filter's extension panel.

# IP Interfaces

NPB supports the configuration of IP interfaces over physical ports. IP interfaces allow you to assign IP addresses to the port and to connect it to an IP network.

An IP interface behaves as follows:

- Sends ARP request to discover the gateway MAC address
- Replays to ARP requests for its IP address
- For outgoing traffic, replaces the destination MAC addresses with the gateway's MAC address and the source MAC address with the NPB's MAC address.
- For incoming traffic, handles only traffic destined to its MAC address and optionally to its IP address

**Note:**
Ip interfaces are not supported in NPB Ie and NPB IV.

## Configuring IP Interfaces

IP interfaces contain the following parameters.

**Table 47: IP Interface Parameters**

| Name | Description | Possible Values |
|---|---|---|
| id | Interface ID | 1-99 |
| name | Interface name | Free text |
| description | Interface description | Free text |
| bind-port | NPB port that is bound to the interface; a port can be bound to several IP interfaces | Valid port ID |
| bind-ip | When set, the interface handles only IP traffic destined to it. This option must be enabled if several interfaces use the same bind-port | enable or disable<br>Default is **`disabled`** |
| ipv4-address | The interface IPv4 address | Valid IPv4 address |
| ipv4-gateway | The default gateway IPv4 address | |

Usually, the gateway's MAC address is discovered by sending ARP requests. It is possible to trigger a renewal of the address or to set it manually. When setting manually, no ARP requests are sent until a renewal of the address is triggered explicitly.

To create an IP interface from the CLI, use the following command:

```
NPB(config)# interface ip <id> ipv4-address <ipv4-address> ipv4-
gateway <gw-address> bind-port <port-id> [name <name>] [description
<description>] [bind-ip enable|disable]
```

To renew the gateway MAC address from the CLI, use the following command:

```
NPB(config)# interface ip <id> reset-gw-mac
```

To set the gateway MAC address manually from the CLI, use the following command:

```
NPB(config)# interface ip <id> set-gw-mac <mac>
```

To delete an IP interface from the CLI, use the following command:

```
NPB(config)# no interface ip <id>
```

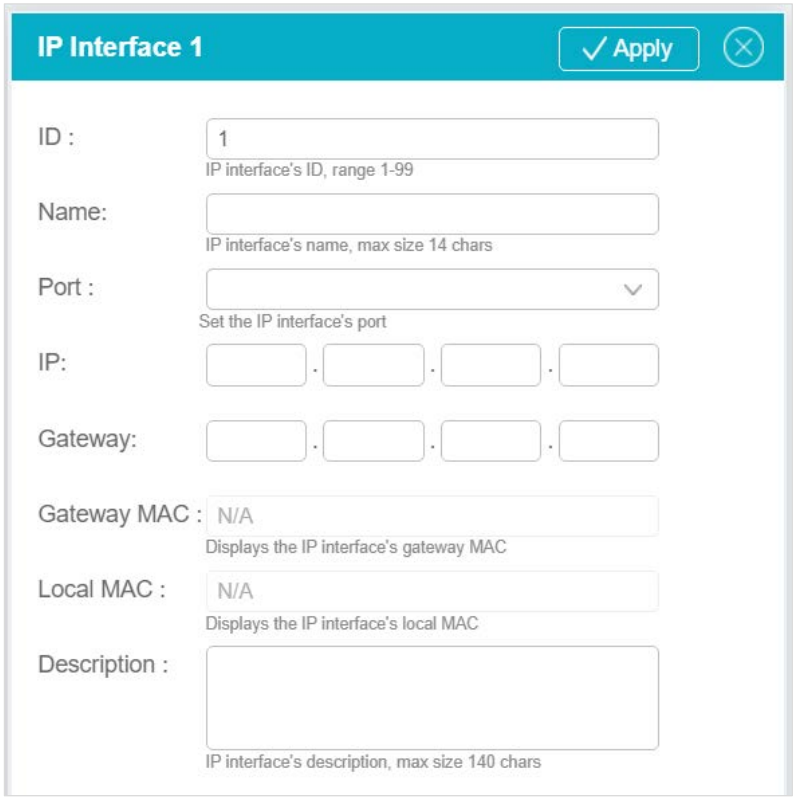
To display all configured IP interfaces from the CLI, use the following command:

```
NPB# show interface ip [<id>]
```

To manage IP interfaces using the WebUI, proceed as follows:

1. Select **Interfaces – IP** in the Navigation panel.
2. Click an existing interface to update it, or use the **Add** button to add a new one.
3. Set the relevant parameters in the extension panel.
4. To delete a line, use the checkbox next to the line you wish to delete, and use the **Delete** button.
5. To set or renew the gateway MAC address, click **Gateway MAC** above the table.

**Figure 80: IP Extension Panel**




Gateway MAC is discovered by the NPB device using ARP messages. Its value is displayed only after successful address resolution.

## IP Interfaces and Filters

IP interfaces can be used as filter input and output. Only traffic for which the destination MAC equals the interface MAC and (optionally) the destination IP equals the interface IP are received by the interface.

**Note:**
Ports that are bound to IP interfaces cannot be used as input or output ports directly.

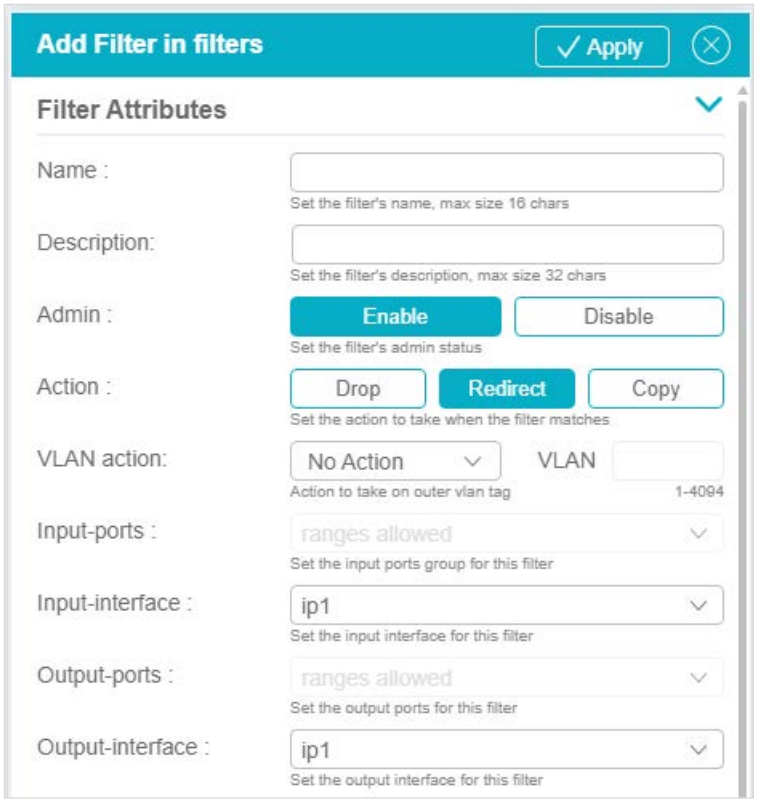
To set IP interfaces as input or output when configuring a filter from the CLI, use the **`input-interface`** and **`output-interface`** commands followed by **`ip<id>.`** For example:

```
NPB(config-filter-1)# input-interface ip1 output-interface ip2
```

See Section Filtering on p.102 for more details on CLI syntax.

To set an IP interface as a filter output or input interface using the WebUI, select **Filters – Rules** in the Navigation panel. Use the **Input Interface** and **Output Interface** options.

**Figure 81: Setting an IP Interface as Filter Output or Input Interface using the WebUI**



# GRE Tunneling

The Generic Routing Encapsulation (GRE) protocol is used to encapsulate one network layer protocol within another network layer protocol.

The NPB supports L2 and L3 GRE tunnels termination, allowing the user to tunnel traffic to a remote peer over the network. GRE tunnels contain a local GRE interface defined on the NPB and a remote peer defined at a routable location. Local GRE interfaces act as Layer 3 entities with respect to MAC and IP addresses resolution.

Incoming traffic arriving at the GRE interface is decapsulated, i.e. its external IP and GRE headers are stripped before entering the NPB device. Outbound traffic on a GRE interface is encapsulated with GRE headers. All VLAN tags are removed, and non-L3 traffic (e.g. ARP) is dropped.

The combination of VLAN editing and GRE Tunneling is not supported. Ports that act as GRE interfaces cannot perform VLAN editing operations.

Table 48 details the GRE support per device.

**Table 48: GRE Support per Device**

| Device | GRE Type | Maximal Number of Incoming GRE Tunnels | Maximal Number of Outgoing GRE Tunnels | Limitations |
|---|---|---|---|---|
| NPB I | L3 | 99 | 99 | |
| NPB Ie8 | L2 | 99 | 4 | Only one interface (in or out) can be bound to a single physical port. |
| NPB II | L3 | 99 | 99 | |
| NPB IIe | L2 | 99 | 4 | Only one interface (in or out) can be bound to a single physical port. |

# Configuring GRE Interfaces

GRE interfaces contain local and peer information and are bound to one of the NPB ports. A port can be bound to several GRE interfaces.

**Table 49: GRE Interface Parameters**

| Name | Description | Possible Values |
|---|---|---|
| id | Interface ID | 1-99 |
| name | Interface name | Free text |
| description | Interface description | Free text |
| bind-port | NPB port that is bound to the interface | Valid port ID |
| ipv4-address | IPv4 address of the local GRE tunnel termination point | Valid IPv4 address |
| ipv4-peer | IPv4 address and optionally a subnet of the remote GRE tunnel termination point or points. Only traffic arriving from this subnet is accepted by the GRE interface. | Valid IPv4 address with an optional netmask or CIDR |
| ipv4-gateway | IPv4 address of the default gateway for sending traffic to the remote peer. If not given, the peer's address acts as a gateway. | Valid IPv4 address |

The gateway's MAC address is discovered by sending ARP requests to the gateway or peer address. If a peer subnet is given, ARP is sent to its address part. It is possible to trigger a renewal of the address or to set it manually. When setting manually, no ARP requests are sent until a renewal of the address is triggered explicitly.

To create a GRE interface from the CLI, use the following command:

```
NPB(config)# interface gre <id> ipv4-address <local-address> ipv4-
peer <peer-address>[/<mask>|<cidr>] ipv4-gateway <gw-address> bind-
port <port-id> [name <name>] [description <description>]
```

To renew the gateway MAC address from the CLI, use the following command:

```
NPB(config)# interface gre <id> reset-gw-mac
```

To set the gateway MAC address manually from the CLI, use the following command:

```
NPB(config)# interface gre <id> set-gw-mac <mac>
```

To delete a GRE interface from the CLI, use the following command:

```
NPB(config)# no interface gre <id>
```

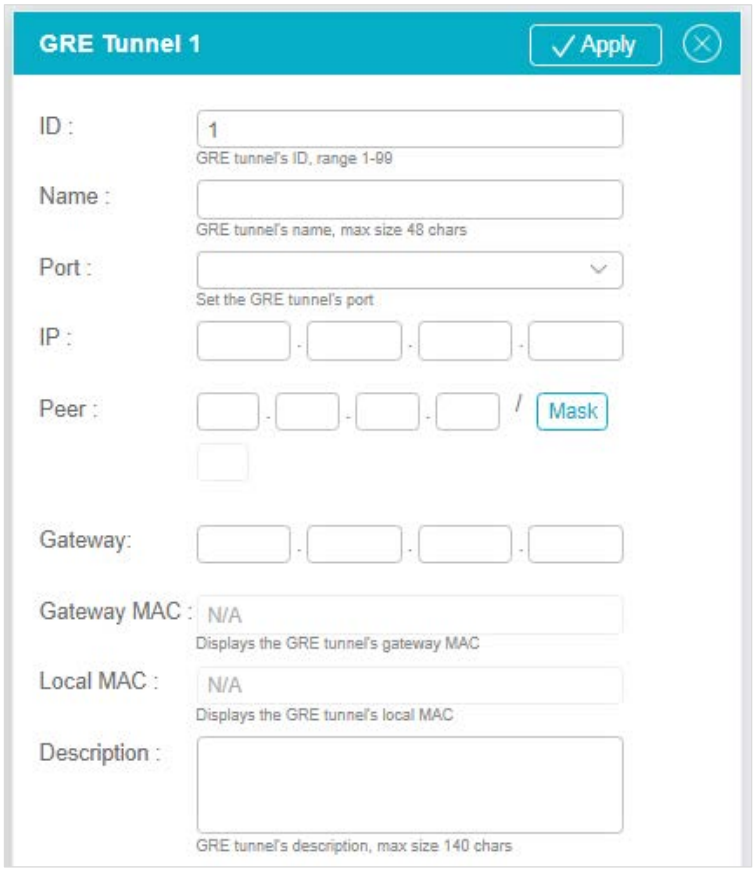
To display all configured GRE interfaces from the CLI, use the following command:

```
NPB# show interface gre [<id>]
```

To manage GRE tunnels using the WebUI, proceed as follows:

1. Select **Interfaces – GRE** in the Navigation panel.
2. Click an existing tunnel to update it, or use the **Add** button to add a new one.
3. Set the relevant parameters in the extension panel.
4. To delete a line, check the box next to the line you wish to delete, and click **Delete**.
5. To set or renew the gateway MAC address, click **Remote MAC** above the table.

**Figure 82: GRE Extension Panel**




Gateway MAC is discovered by the NPB device using ARP messages. Its value is displayed only after successful address resolution.

## GRE and Filters

GRE traffic entering the device on a GRE bound port is decapsulated. Therefore, GRE headers are not visible to the filter classifiers and cannot be used as matching criteria.

In GRE traffic entering the device on a non-bound port, GRE headers are visible to the filter classifiers and can be used as matching criteria, e.g. if the filter tunnel type is GRE or if UDF is used.

**Note:**
Ports that are bound to GRE interfaces cannot be used as input or output ports directly.

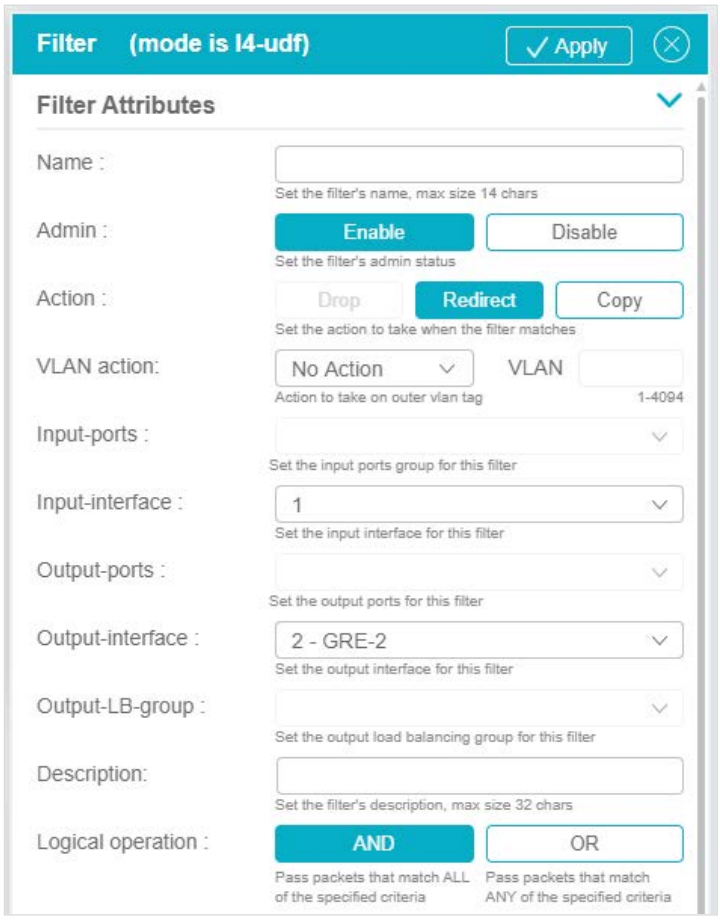
To set GRE interfaces as input or output ports when configuring a filter from the CLI, use the **`input-interface`** and **`output-interface`** commands followed by **`gre<id>.`** For example:

```
NPB(config-filter-1)# input-interface gre1 output-interface gre2
```

See Section Filtering on p.102 for more details on CLI syntax.

To set a GRE tunnel as a filter output or input interface using the WebUI, select **Filters – Rules** in the Navigation panel. Use the **Input Interface** and **Output Interface** options:

**Figure 83: Setting a GRE Tunnel as Filter Output or Input Interface using the WebUI**



# Load Balancing

Load balancing groups are used to distribute traffic among a set of ports, interfaces, or inline tools based on a predefined hash function. The hash function is designed to yield even distribution while sending packets that belong to the same flow to the same port ('flow stickiness').

Once defined, load balancing groups can act as filter output or as an inline solution, causing matched traffic to be distributed between its members according to a global hash function or in a round-robin manner.

To define and use load balancing groups, perform the following steps:

1. Set the global hash function parameters.
2. Define load balancing groups and set their set of members.
3. Use load balancing groups as filter output or inline solution. All traffic matched by the filter will be distributed between the group members as defined.

These 3 steps are described below.

## Configuring the Global Hash Function

The load balancing hash function is defined globally and provides the optimal distribution based on a set of selected headers.

### Hash Keys

Including a header in the hash function causes all flows with identical values in this header to be directed to the same port, thus ensuring stickiness with regards to this header. For example, including the source IP address, destination IP addresses, source L4 port, destination L4 port, and IP protocol headers (a.k.a. the 5 Tuple) ensures that all traffic that belongs to a certain TCP or UDP flow is directed to the same output port.

Supported hash keys are:

- Input port
- Source MAC address
- Destination MAC address
- VLAN tag value
- Ethertype value
- Source IP address (IPv4 and IPv6)
- Destination IP address (IPv4 and IPv6)
- Source and destination IP address combined (IPv4 and IPv6)
- IP protocol number
- UDP and TCP source port
- UDP and TCP destination port
- UDP and TCP source and destination ports combined
- MPLS labels
- GTP Tunnel Endpoint IDentifier (TEID)

In addition, the following values can be used as abbreviations:

- 5 Tuple – Source and destination IP addresses, source and destination ports, and IP protocol number
- 4 Tuple – Source and destination IP addresses, and source and destination ports
- All Layer 2 – Source and destination MAC address, VLAN tag, and EtherType value

By default, the global hash function uses '5 Tuple' as key.

**Note:**
Ethertype and VLAN tag are not supported in NPB Ie.

The following L2 hash keys can be combined with the input port, VLAN, and MPLS hash keys, but not with higher layer keys:

- Source and destination MAC
- Source and destination ports
- EtherType

To add a header to the hash function from the CLI, use the following command:

```
NPB(config)# lb hash hash [in-port] [5-tuple] [4-tuple] [smac] [dmac]
[vlan] [ethertype] [ip-src-addr] [ip-dst-addr] [ip-addr] [ip-
protocol-number] [l4-sport] [l4-dport] [l4-port] [l2-all] [mpls]
[gtp-id]
```

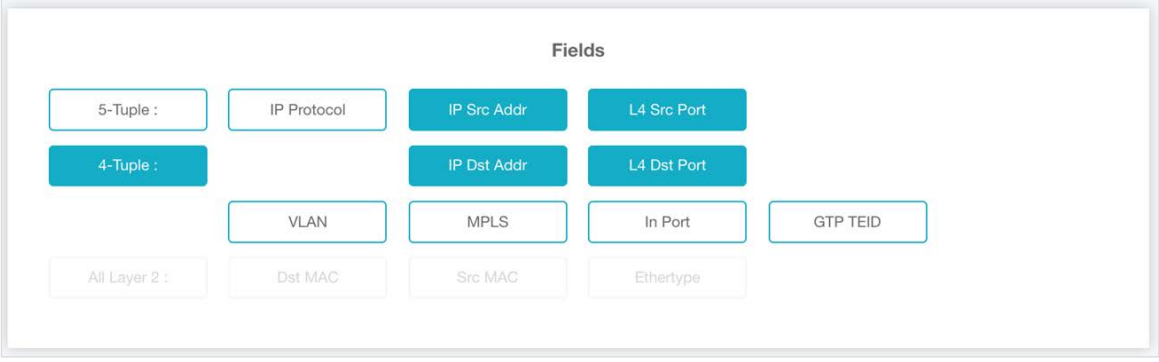
To replace the current set of headers with a new set, state the new set of headers, separated by spaces inside a pair of square brackets. For example, to overwrite the existing set with the set of L4 ports and MPLS, use the following command:

```
NPB(config)# lb hash hash [ l4-port mpls ]
```

**Note:**
The spaces after the opening and before the closing square bracket are important! Missing spaces will cause a syntax error.

To set the hash function keys using the WebUI, select **Load balancing – Hash** in the Navigation panel.

**Figure 84: Setting Hash Function Keys using the WebUI**



### Hash Functions

The NPB device supports two hash functions, CRC32 and XOR. The CRC32 function uses a hash key of 32 bits and can be used as symmetric or asymmetric. The XOR function uses a hash key of 16 bits and is always symmetric. Normally, CRC32 yields a better distribution, and it is used by default. Use XOR when CRC32 yields a non-even distribution and symmetry is acceptable.

To set the hash function from the CLI, use the following command:

```
NPB(config)# lb hash func crc32|xor
```

**Note:**
The XOR hash function is not supported in NPB Ie.

The CRC32 load balancing hash function can be defined as symmetric or asymmetric. A symmetric function directs both directions of a L3 flow to the same port, so that swapping the source and destination IP addresses and ports yields the same hash result. An asymmetric function does not guarantee this behavior.

By default, the function is symmetric.

To set the symmetry from the CLI, use the following command:

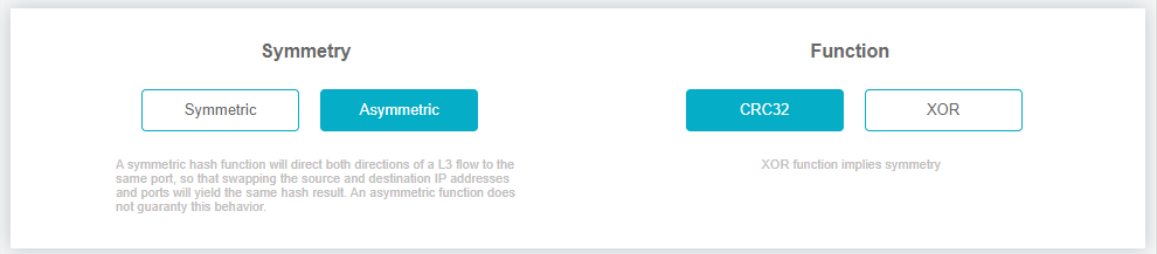
```
NPB(config)# lb hash symmetric disable|enable
```

To display the global load balancing configuration from the CLI, use the following command:

```
NPB# show lb hash
-------------------------------------------------------------------
                      LB Hash
-------------------------------------------------------------------
Hash                 [ 5-tuple ]
Symmetric            Disabled
Function             XOR
```

To set the hash function using the WebUI, select **Load balancing – Hash** in the Navigation panel.

**Figure 85: Setting Hash Function Symmetry using the WebUI**




## Configuring Load Balancing Groups

The NPB device supports up to 99 load balancing groups (64 in NPB IV). Load balancing capabilities can be tuned using the Load Balance Operation mode. Refer to Section Load Balance Operation Mode on p.170 for a full description of the capabilities and restrictions.

Table 50 lists the load balancing group parameters.

**Table 50: Load Balancing Group Parameters**

| Name | Description | Possible Values |
|---|---|---|
| Load balancing group ID | Group ID | 1 – 99 in all devices except NPB IV<br>1– 64 in NPB IV |
| name | Group name | Free text |
| description | Group description | Free text |
| algorithm | Group distribution algorithm | **hash** – distributes packets according to the globally defined hash function<br>**hash-dlb** – distributes packets using dynamic load balancing, see Section Dynamic Load Balancing (NPB Ie8 and NPB IIe only) on p.170 (NPB Ie8 and NPB IIe only)<br>**hash-gtp-ip** – distributes packets according to the GTP inner IP in a symmetric manner<br>**hash-gtp-src** – distributes packets according to a configurable number of bits taken from the GTP source inner IP suffix and source inner L4 ports suffix. The number of bits is set by the hash-gtp-size parameter.<br>**hash-gtp-dst** – distributes packets according to a configurable number of bits taken from the GTP destination inner IP suffix and destination inner L4 ports suffix. The number of bits is set by the hash-gtp-size parameter.<br>**src IP** – distributes packets according to the source IP address, not supported for MPLS traffic (NPB I, NPB Ie8, NPB II, and NPB IIe only)<br>**dest IP** – distributes packets according to the destination IP address not supported for MPLS traffic (NPB I, NPB Ie8, NPB II, and NPB IIe only)<br>**round robin** – distributes packets in a cyclic order (NPB Ie, NPB Ie8, NPB II, and NPB IIe only)<br>**random** – distributes packets randomly (NPB III only)<br>Default is **hash.** |

| Name | Description | Possible Values |
|---|---|---|
| dlb- inactivity | Dynamic Load Balancing inactivity timeout in microseconds | 16 – 32,000<br>Default is 10,000.<br>NPB Ie8 and IIe only, see Section Dynamic Load Balancing (NPB Ie8 and NPB IIe only) on p.170 |
| outputs | List of output ports, interfaces, or inline tools<br>The elements in this list are the group's members. | List of valid ports, port groups, interfaces, interface groups, or inline tools, separated by commas. Range can be specified using hyphens.<br>Members must be of the same type (ports, interfaces, or inline tools).<br>GRE interface IDs are prefixed with **`gre`** (e.g. gre1). Inline tool names are prefixed with **`tool`**_ (e.g. tool_mytool). |
| standby | List of group members that act as standby members for this group. Standby members replace failed members. | List of group members, separated by commas. Range can be specified using hyphens. |
| standby-failover | Sets the standby behavior in case a member returns to be active after a failure.<br>Standby members can either continue to act as an active member, placing the original member in the standby list, or they can return to the standby list, letting the recovered member return to its position as an active member. | **`active`** – The standby member continues to act as the active member, while the recovered member acts as a standby.<br>**`standby`** – The recovered member becomes active, the standby member returns to be standby.<br>Default is **`standby.`** |
| failover-holdtime | Time in msec to wait before considering a previously failed member to be stable enough to be reintroduce into the group | 0 – 10,000<br>Default is 0. |
| failover-action | Sets the group failover action for inline groups | One of the valid inline tool failover actions, see Section Inline Tools on p.148<br>Or:<br>**`lb-bypass`** – Bypass the inline group.<br>**`lb-drop`** – Drop traffic forwarded to the inline group.<br>**`per-tool`** – Applies the failed tool's failover action<br>Default is **`per-tool`**. |

| Name | Description | Possible Values |
|---|---|---|
| failover-threshold | Sets the number of failed tools that triggers the failover action. Zero means all tools. Valid only if **`failover-action`** is not **`per-tool`**. | 0 - Number of configured members<br>Default is zero. |
| overload | Sets the behavior when an active member changes state to down and no standby member were configured or are available | **`drop`** – The member stays in the group. All traffic directed to it is dropped until a standby port is available.<br>**`re-hash`** – The member leaves the group. Traffic is rehashed between remaining group members. When a standby member becomes available, it joins the group, and traffic is rehashed again.<br>Default is **`re-hash.`** |
| hash-gtp-size | Sets the number of internal filters to be used to implement GTP hashing; valid only if algo is **`hash-gtp-ip`**, **`hash-gtp-src`**, or **`hash-gtp-dst`**, must be set to 0 otherwise | 0, 64, 256, 1024<br>1024 is not supported in NPB II and NPB III |

**Note:**
In NPB IV, ports that are members in a load balancing group (as outputs or standbys) cannot be used as a filter's input ports. The entire load balance group can be set as a filter's input using the CLI.

To set a load balancing group from the CLI, use the following command:

```
NPB(config)# lb group <id> outputs <output-list>  [name <name>]
[description <description>] [algo hash|hash-dlb|hash-gtp-ip|hash-gtp-
src|hash-gtp-src|ip-src-addr|ip-dst-addr|round-robin|random][dlb-
inactivity <timeout>][standby <ports-list>] [standby-failover
active|standby][failover-action <nw-bypass|nw-down|nw-drop|lb-
bypass|lb-drop|per-tool>][failover-threshold <threshold>][failover-
holdtime <timeout>][overload drop|re-hash][ hash-gtp-size
0|64|256|1024]
```

To delete a load balancing group from the CLI, use the following command:

```
NPB(config)# no lb group <id>
```

Once defined, load balancing groups can be edited by entering a CLI context:

```
NPB(config)# lb group <id>
```

For example:

```
NPB(config)# lb group 1
NPB(config -group-1)# algo round-robin
```

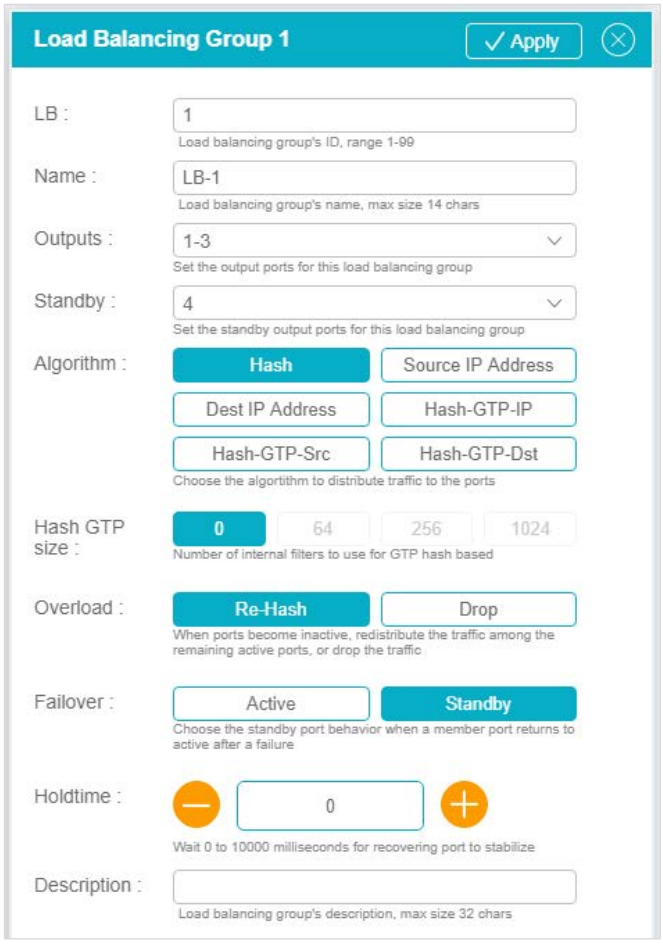
To display the current load balancing groups from the CLI, use the following command:

```
NPB# show lb group [group-id]
```

**Note:**
This command displays the current set of active ports, which may be different from the configured set if standby ports have replaced active ports.

To manage load balancing groups using the WebUI, select **Load balancing – Groups** in the Navigation panel. Use the **Add** and **Delete** buttons to create and remove groups. Use the extension panel to set the group's parameters.

**Figure 86: Load Balancing Groups Extension Panel**



### Dynamic Load Balancing (NPB Ie8 and NPB IIe only)

Dynamic Load Balancing (DLB) hashing takes into consideration the output ports utilization when selecting an output port for a specific flow. This may reduce the chance of packet drops in cases where the traffic is not evenly distributed. Dynamic Load Balancing, like simple hashing, does not split flows. Once an output port has been selected for the flow, it is kept as long as the flow is active (regardless of port utilization). However, a specific flow's output port is not predictable as it depends on the load of the output ports when the decision is made.

The DLB inactivity timeout is the time interval after which an idle flow is assumed to be inactive. A new packet with the same flow keys (e.g. 5-tuple) is considered a new flow and may use a different output port.

To set dynamic load balancing from the CLI, use the following command:

```
NPB(config)# lb group <id> algo hash-dlb [dlb-inactivity <interval>]
```

To set dynamic load balancing from the WebUI, use the load balancing group extension panel.

### Consistent Load Balancing (NPB IV only)

Consistent load balancing is designed to reduce traffic rehashing in case of failed and recovered members to a minimum:

- When a member fails, traffic rehashing is performed only for the traffic handled by that member.
- When a member is recovered, hashing is performed only for the relative amount of traffic required to reach an ideal distribution.

NPB IV automatically applies consistent load balancing.

## Load Balance Operation Mode

NPB I, Ie8, II, and IIe support two modes for working with load balancing groups as filter outputs. The **Advanced** mode allows full feature support, but introduces limitations when mixing load balance groups and ports as outputs. The **Basic** mode does not introduce such limitations, but supports a reduced set of features. The default mode is **Advanced**.

**Note:**
Releases older than R3.1 use only the Advanced mode.
NPB Ie and IV support only the Basic mode.

The differences between the two modes are as follows.

Basic mode:

- Load balance groups and ports can be mixed as outputs in the same filter.
- Several load balance groups can be used as outputs of the same filter.
- Traffic cannot be sent directly to a port that is a member in a load balance group.
- A port cannot be a member in more than one load balance group.
- Only hash algorithm is supported.
- Filter copy operation is supported when the filter has a load balance group as its output.

Advanced mode:

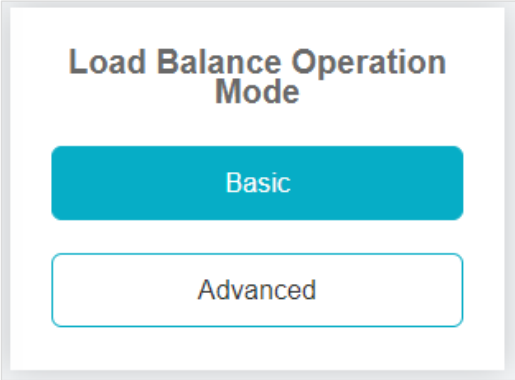
- When mixing load balance groups and ports as filter outputs, the following global restriction holds:
  When configuring a filter with several load balance groups or with a mix of load balance groups and ports, each output except for the first load balance group is marked as a *mixed resource*. The number of mixed resources in the system is limited to 4. A group that is marked as mixed resource in several filters is counted only once.
- Traffic can be sent directly to a port that is a member in a load balance group.
- A port can be a member in more than one load balance group.
- Both hash and round-robin algorithms s are supported.
- Support for filter copy operation is limited when the filter has a load balance group as its output. Copy is not supported when the mixed resources limitation is violated internally when creating the internal filters required for the copy operation.
- In NPB III, only a single output load balance group can be configured per filter.

To set the Load Balance Operation mode from CLI, use the following command:

```
NPB(config)# filters lb-oper-mode advanced|basic
```

To set the Load Balance Operation mode from the WebUI, select **Filters – Globals** in the Navigation panel, and select the required mode.

**Figure 87: Selecting Load Balance Operation Mode**




NPB Ie supports a single operation mode with the following limitation:

- A port cannot be a member in more than one load balance group.

# Setting Load Balancing Group as Filter Output

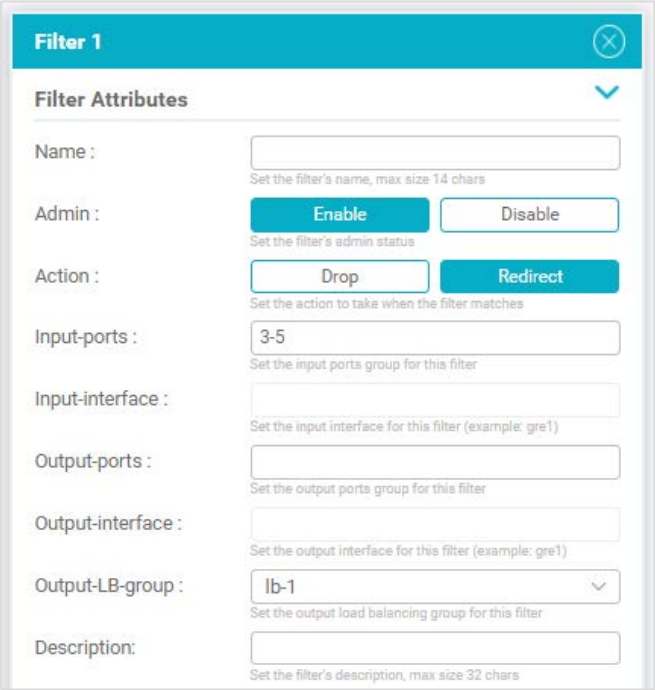
Once defined, a load balancing group can be used as a filter output.

To set a load balancing group as a filter output from the CLI, use the **`redirect`** action with the **`output-lb-group`** option:

```
NPB(config)# filters add action redirect output-lb-group <group-id>
```

To set a load balancing group as a filter output using the WebUI, select **Filters – Rules** in the Navigation panel. Use the **Redirect** action with the **Output-LB-group** option:

**Figure 88: Setting Load Balancing Group as Filter Output using the WebUI**




It is possible to define several load balancing groups as a filter output. It is also possible to combine load balancing groups and output ports. In this case a copy of each matched packet is redirect to every output port and to every load balancing group.

The maximal number of load balancing groups per filter is 7.

# Predicting Load Balancing Outbound Port

The NPB prediction tool allows the user to predict the load balance outbound port that will be assigned to a specific packet. This tool is helpful when new traffic is about to be added to an existing configuration as knowing in advance the port or ports to which this traffic will be redirected can help, for example, to avoid port overloading.

To use the prediction tool from the CLI in NPB I, use the following command:

```
NPB(config)# lb info show in-port <input-port-id> lb-id <lb-group-id>
[l2-dmac <dest-MAC>] [l2-ethertype <ethertype>] [l2-smac <src-MAC>]
[l2-vlan <vlan>] [l3-ipv4-dst-addr <ipv4-dest>] [l3-ipv4-src-addr
<ipv4-src>] [l3-ipv6-dst-addr <ipv6-dest>] [l3-ipv6-src-addr <ipv6-
src>] [l3-protocol-number <protocol>] [l4-dport <l4-dest-port>] [l4-
sport <l4-src-port>]
```

To use the prediction tool from the CLI in NPB Ie8, NPB II, NPB IIe and NPB III, use the following command:

```
NPB(config)# lb info show in-port <input-port-id> [l2-dmac <dest-
MAC>] [l2-ethertype <ethertype>] [l2-smac <src-MAC>] [l2-vlan <vlan>]
[l3-ipv4-dst-addr <ipv4-dest>] [l3-ipv4-src-addr <ipv4-src>] [l3-
ipv6-dst-addr <ipv6-dest>] [l3-ipv6-src-addr <ipv6-src>] [l3-
protocol-number <protocol>] [l4-dport <l4-dest-port>] [l4-sport <l4-
src-port>] [pkt <packet-data>]
```

**Note:**
Use the **pkt** option to provide packet data (up to 80 bytes). If **pkt** is used with additional fields, the values of these fields overwrite the relevant packet data.

The output of the command is the load balance group ID and the port number to which the given packet will be redirected under the current configuration.

**Note:**
Load Balancing Prediction is not supported in NPB Ie and NPB IV.

To use the prediction tool using the WebUI, select **Load Balancing – Hash** in the Navigation panel:

**Figure 89: Using the Prediction Tool using the WebUI – on NPB I**

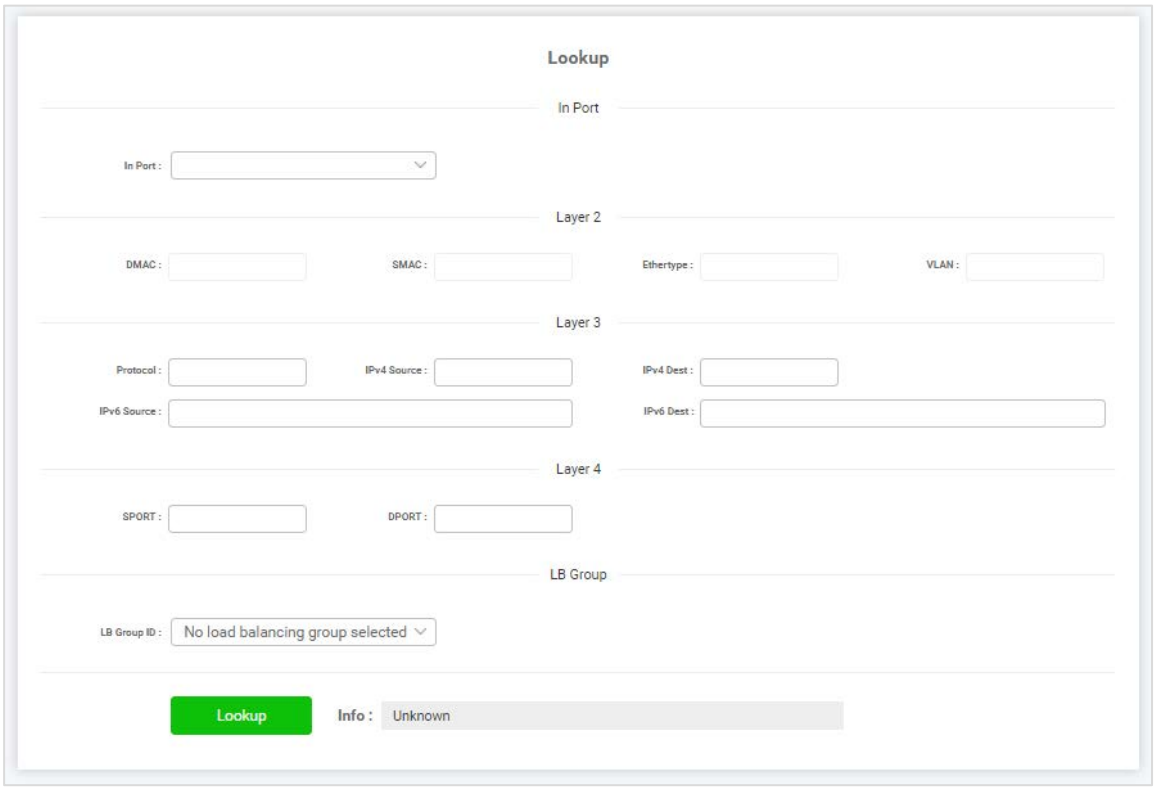
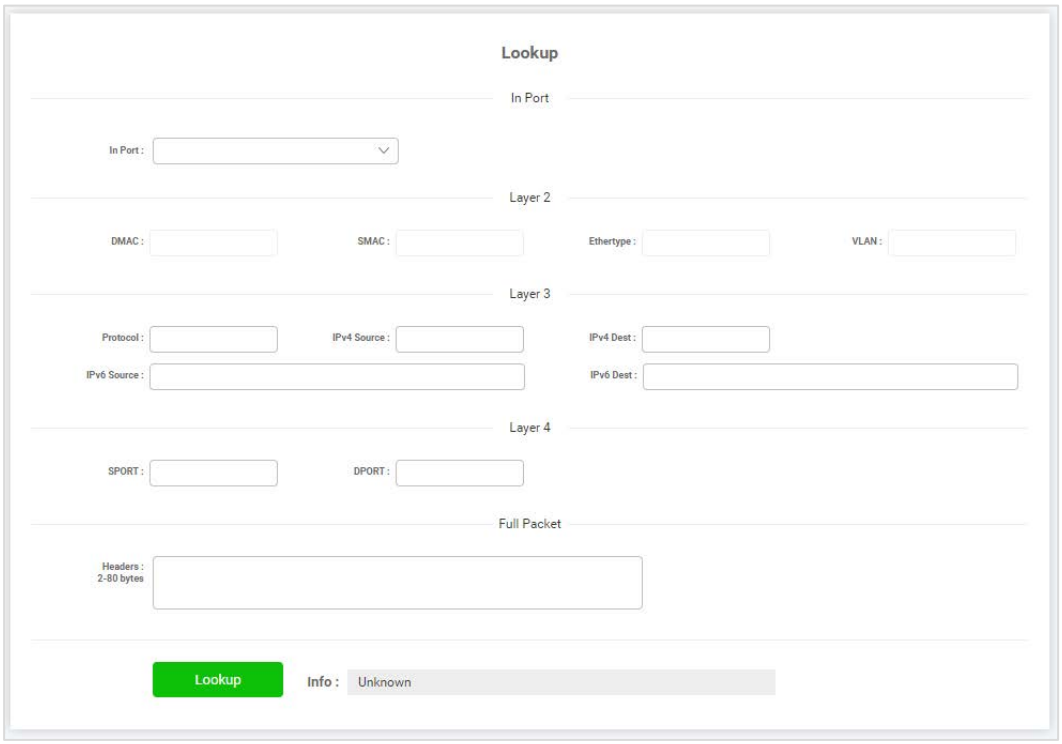



**Figure 90: Using the Prediction Tool using the WebUI – on NPB Ie8, II, and IIe**



# Virtual Load Balance

Virtual Load Balancing allows VLAN tagging of outbound packets according to the global hash function results. The VLAN tag for each packet is selected from a given range of tags according to the hash function result and the VLB source as shown in Table 51.

**Table 51: VLAN Tag Selection according to VLB Source**

| Source | Description |
|---|---|
| Primary | When used with a load balance group as an output destination, this option provides an additional level of distribution which is correlated with the load balance distribution.<br>When used without load balance group as an output destination, this option mimics the load balance distribution. |
| Secondary | Provides an additional level of distribution which is not correlated with the load balance distribution |

The default source is **`primary`**.

Virtual load balancing is configured per filter as a filter classifier.

To set virtual load balancing from the CLI, use the following command in a filter context:

```
NPB(config-filter-1)# set-virtual-lb <vlan-range>
```

The range size defined by **`vlan-range`** must be 2, 4, 8, 16, 32, 64, 128, 256, or 512.

To set a virtual load balancing source from the CLI, use the following command in a filter context:

```
NPB(config-filter-1)# set-virtual-lb-source primary|secondary
```

To set virtual load balancing from the WebUI, use the Packet Processing tab in the filter's extension panel. See Section Managing Filters on p.107.

**Note:**
Virtual load balancing consumes one filter resource per VLAN tag. E.g. a range of 8 VLAN tags consumes 8 filter resources

**Note:**
Virtual load balancing is not supported in NPB Ie.

## Virtual Load Balance Example

This example assumes a virtual load balance range of 101-104 and a load balancing group of 2 ports (1,2). There are three cases:

### 1. Source is primary, using a load balancing group as output

VLAN tags are correlated with the load balance distribution. Each port uses a subset of the range:

**Table 52: VLB Example 1**

| Port | VLAN Tags on Outbound Traffic (Even Distribution) | |
|---|---|---|
| 1 | 101 | 102 |
| 2 | 103 | 104 |

### 2. Source is secondary, using a load balancing group as output

VLAN tags are not correlated with the load balance distribution. Each port uses the entire range:

**Table 53: VLB Example 2**

| Port | VLAN Tags on Outbound Traffic (Even Distribution) | | | |
|---|---|---|---|---|
| 1 | 101 | 102 | 103 | 104 |
| 2 | 101 | 102 | 103 | 104 |

### 3. Source is either primary or secondary, redirecting to port 1

VLAN tags are not correlated with the load balance distribution. Port 1 uses the entire range. If the source is primary, the VLAN tags mimic the distribution of a load balance group with 4 ports:

**Table 54: VLB Example 3**

| Port | VLAN Tags on Outbound Traffic (Even Distribution) | | | |
|---|---|---|---|---|
| 1 | 101 | 102 | 103 | 104 |

# Diagrams

The NPB supports an interactive, graphical interface to view and manage ports, filters, load balance groups, and inline solutions.

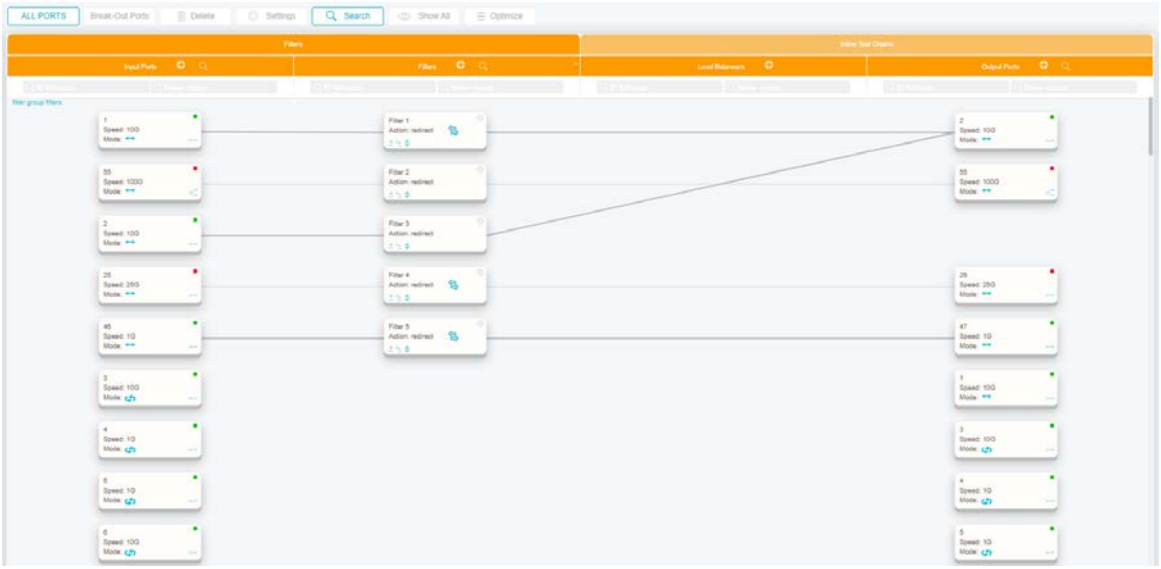
This interface allows you to:

- View the current filter and inline solution configurations graphically in a single glimpse
- Create new objects, such as filters, load balancing groups, inline tools, and inline chains
- Move objects
- Set connectivity easily by drawing lines between objects

To use the diagram function, select **Diagram** in the Navigation panel.

The diagram page contains a Filters section and an Inline Tool Chains section. To switch between the sections, use the tabs in the upper part of the diagram.

**Figure 91: Diagram**




## Filters Diagram

The Filters diagram contains the system's filters, ports, and load balance objects and allows you to manipulate them using a graphical canvas.

Two lists of ports are displayed on both sides of the canvas: input ports are on the left, and output ports are on the right. These lists contain all the ports, interfaces, and groups configured in the system. Filters and load balance groups are displayed between these two lists. Relations between objects are displayed using lines.

Each object contains icons that reflect its configuration and state. Hovering over an object displays full descriptions.

Clicking an object opens its extension panel on the right. Use the panel to edit the object's attributes.

To create a new port group, a GRE tunnel, or an IP interface, click the Input/Output Ports **+** icon in the diagram header bar.

To create a new load balance group, click the Load Balancer **+** icon in the diagram header bar.

To add a new filter, do one of the following:

- Use the Filters **+** icon in the diagram header bar.
- Drag a line from an input port directly to a load balancer or output port.
- To insert a new filter at a particular position, click the **+** icon in the lower left corner of any filter symbol.
- To duplicate a filter, click the **++** icon in the lower left corner of any filter symbol.

To move an existing filter, click the up/down arrows in the lower left corner of any filter symbol.

To open the port or filter search template, click the magnifying glass icon in the Input/Output Ports or Filter columns. The search templates can also be opened by clicking the **Search** button above the table.

The following buttons appear above the diagram:

- **Ports/Ports & Groups** – This button enables you to view both ports and port groups, or just the ports, or just the port groups. The button does not appear if no port groups are defined. When you are viewing just the ports or just the port groups, the button appears in solid blue to alert you that you are not seeing the entire configuration. When no port groups are defined, the button is named **ALL PORTS.** Clicking it adds a new entry that represents all of the device's ports.
- **Break-Out I/F** – This button enables you to view interfaces as individual component symbols. The button appears in solid blue when you are in this viewing mode. When the button is off (and the interfaces are invisible), you make connections to GRE tunnels using the ports that the tunnels are bound to.

  Note: When **Break-Out I/F** is on, you can still open the interface extension panel by clicking the interface name in the port symbol, but you cannot connect the port's interface by dragging a line from the port symbol. The line must be dragged from the interface's own symbol.

- **Break-Out Ports** – This button sets the merge/break-out state of selected ports (e.g., a single 40G port vs. four 10G ports). The break-out state of individual ports can also be set by clicking the break-out icons at the right side of the port symbols.
- **Delete** - Select ports, filters, load balancers, and interconnect lines by clicking or ctrl-clicking them; then click **Delete** to delete the selected objects. Click **Commit** to commit the changes, as usual.
- **Settings** – Select one or more ports or filters, and click **Settings** to configure them.
- **Search** – This button opens up the port and filter search template extension panels. The search templates can also be opened by clicking the magnifying glass icon in the Input/Output Ports or Filter columns.
- **Show All** and **Optimize** – The diagram supports sorting and searching in a manner similar to the table. Click **Show All** to remove all search criteria. Click **Optimize** to return to the default sort, which puts the filters in priority order and auto-places the load balancers and ports for a clean layout.

- **Save Position** and **Return Position** – When creating a new filter, the diagram automatically places it in its position. This may cause an automatic scroll up. Use this button to return to the filter's original vertical scrolling location. Or mark a vertical scroll position by clicking Save Position and return there by clicking Return Position.
- **Refresh** – This button, which is visible only when the Auto Refresh setting is off, causes the diagram data to be re-loaded and the diagram to be re-drawn.

## Inline Tool Chains Diagram

The Inline Tool Chains diagram contains the system's inline objects and allows you to manipulate them using a graphical canvas.

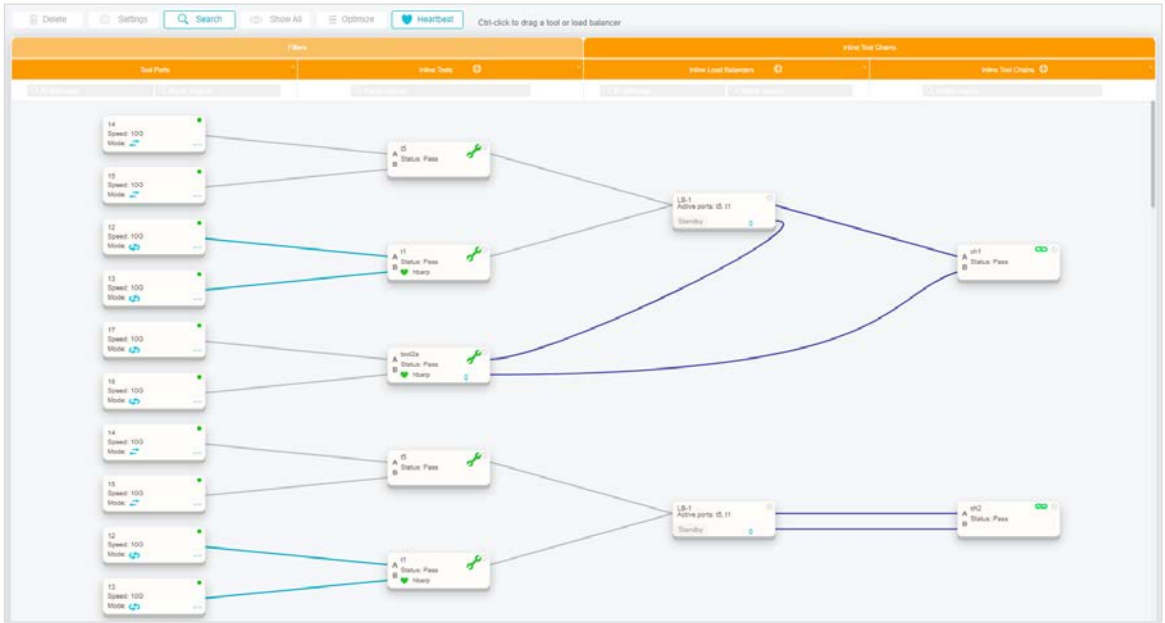
Four columns are displayed:

- Tool ports
- Inline tools
- Inline load balancers
- Inline tool chains

As in the Filters diagram, each object contains icons that reflect its configuration and state. Hovering over an object displays the full description, and clicking an object opens its extension panel on the right. Use the panel to edit the object's attributes.

Dark blue lines indicate the connections of inline tools and load balancers in an inline tool chain. They can be viewed as visualizing the traffic flow through the chain. The gray lines connecting the ports, tools, and load balancers indicate configuration, but not traffic flow through the chain.

**Figure 92: Inline Tool Chains Diagram**



The extension panels can be used to configure inline tool chains and load balancers. However, many operations can also be accomplished graphically:

- To create a tool, inline load balancer, or inline tool chain, click the **+** icon in the relevant column.
- To create an inline tool, draw a line between two ports.
- To create an inline load balancer, draw a line between two inline tools.
- To create a heartbeat profile, draw a line between two inline tools.
- To create an inline tool chain, draw a line between two inline tools and/or load balancers.
- To add an inline tool to an existing inline load balancer or tool chain, ctrl-click-drag the tool and drop it onto the inline load balancer or tool chain. Or: draw a line from the tool to these objects.
- To remove an inline tool or load balancer from a tool chain, ctrl-click-drag it and drop it in an empty area of the diagram.
- To move a tool within a chain, use one of the following options:
    - Use the up/down arrows at the tool symbol.
    - Or: ctrl-click-drag the tool and drop it on the tool at the target position.
    - Or: draw a line from a tool to the tool at the target position.

It is valid to use a tool or inline load balancer in more than one inline tool chain at the same time. The inline tool chain diagram represents the configuration by duplicating the symbols for the shared tool or inline load balancer, along with the tools and ports that connect to it, so that each inline tool chain is shown as a separate entity.

When you select a duplicated inline load balancer, tool, or port, all instances of that item become selected to highlight the fact that any configuration changes you make to that item (other than its position or inclusion in the inline tool chain) apply in all inline tool chains where the item is used.

As no port can be used simultaneously in both a filter and an inline tool, ports are shown only in the diagram to which they apply. In other words, inline tool ports are hidden in the Filters diagram, and ports connected to filters are hidden in the Inline Tool Chains diagram. Unconnected ports appear in both diagrams. Likewise, load balancers are shown only in the diagram to which they apply.

The buttons above the diagram and the search boxes behave as explained in the Filters diagram section. The **Heartbeat** button navigates to the **Inline > Heartbeats** page.

# Stacking

A stack is two or more NPB devices that are connected physically and act as a single managed device. Each device in the stack has a unique module ID, which is used to identify this device and its ports. One of the stack devices acts as its master device and manages the entire stack. Other devices support only limited configuration options and are referred to as "normal" devices.

Devices in the stack are physically connected using "stack load balancing ports". These ports are used for the internal stack traffic and form the stack's backbone. They cannot be used for other purposes. The set of stack ports is given as part of the stack creation and reflects the actual physical connections. Physical connections between two devices are reflected in the configuration of stack load balancing ports in each device.

**Note:**
Generally, stack load balancing groups are defined symmetrically, that is, all group members in one device are connected to another device. However, when working in a spine-leaf topology, a stack load balancing group defined in a leaf can include ports that are connected to several spines.

**Note:**
It is not recommended to use breakout ports as stack load balance ports. If this is required, contact CGS support for information.

The stack is managed as a single entity using the master device's management interfaces. Port notation is enhanced to include the port's module ID:

<module-ID>/<port-id>[/<breakout-channel>]

For example, Port 10 in Device 4 is identified as Port 4/10 when not breakout is defined, and as Ports 4/10/1, 4/10/2, 4/10/3, and 4/10/4 when breaking out into 4 channels.

A stack can contain up to 100 devices with a total of up to 2,048 ports.

**Note:**
Stacking is supported on NPB I, Ie8 and IIe only.

Some of the system behavior is affected when using a stack. These changes are:

- In many commands, module IDs can be specified to limit the command's scope to specific modules only.
  For example, to reboot modules 2, 3, 4 and 7 from the CLI, use the following command:

  ```
  NPB(config)#system reboot module 2-4,7
  ```

- SW upgrade can be performed for the entire stack or only for specific modules. See detailed description below.
- All stack devices must have a valid license. Fingerprint generation and license installation are performed from the master.

- The two ports of an inline tool and all ports of an inline load balancer must reside on the same physical device.
- Alarms generated by the stack devices are collected and handled by the master device. Each alarm contains the module ID of the generating device. In addition, the stack generates alarms that reflects its status.
- All stack devices share the master's user-management configuration.
- ACL rules are applied by the master to all other devices. ACL statistics can be obtained per device.
- HTTP certificates are populated by the master to all other devices.
- Time and date are managed by the master and populated to all other devices.
- System status (temperature sensors, PSUs, and fans) are collected and displayed by the master for each of the devices.

## Stack Creation and Deletion

To configure a stack, perform the following steps:

1. Plan the physical topology of the stack and determine the required backbone throughput. Although a spine-leaf topology is recommended for most cases, the topology can be flexible as long as each device is reachable from the master device. Assign a unique module ID for each device, and select one device to be the master (can be any of the devices).
2. Physically connect the stack devices based on the stack topology (using network cables).
3. Log in into the master device, set its role, its module ID, and configure its stack load balancing ports in accordance with the physical cabling.
4. Log in into each of the other devices, set their roles, their module IDs, and configure their stack ports in accordance with the physical cabling.
5. It is possible to add devices to the stack using the master device. In this case, the device ports can be pre-configured before the physical device is added.

**Note:**
Before adding a device to the stack, make sure to return it to its factory default. See Restore Factory Default on p.73.
When a device is added to the stack, its current configuration is deleted and its load balance mode is set to **`basic`**.

To remove a device from the stack, delete its stack configuration.

**Note:**
As a best practice, save the device's current configuration before adding it to a stack, if it is possible that you may want to restore the configuration after removing the device from the stack.

## Stack Management Using the CLI

To set a device to be the master device using that device's CLI, use the following command (<mid> means the module's ID number):

```
NPB(config)# stack module <mid> role master local
```

To set a device to be a stack member that is not the master using that device's CLI, use the following command:

```
NPB(config)# stack module <mid> role normal local
```

To set the device stack load balancing ports, use the following command:

```
NPB(config)# stack stack-lb-group <group-name> ports <list of ports, - and , can be used>
```

Repeat this command for each set of ports physically connected to a remote device on both ends of the connection. Each remote device connected to this device is assigned a separate stack-lb-group.

**Note:**
In the `stack stack-lb-group command`, you do not specify which device this stack-lb-group connects to. You only configure the ports; the stack itself discovers the topology (which devices connect to which other devices).

To pre-configure a non-master device from the master device, use the following command:

```
NPB(config)# stack module <mid> role normal type <device-type>
```

To connect to the CLI of another device in the stack from the master device, use the following command:

```
NPB# stack connect module <mid>
```

To run remote CLI commands on other devices in the stack from the master device's CLI, use the following command:

```
NPB# stack cli-command <command> module <list of mids or 'all'>
```

The command includes entering config mode and commit if needed.
For example, to disable SNMP V3 on modules 1-4 and 9, use the following command:

```
NPB# stack cli-command "config; system snmp v3 false; commit" module 1-4,9
```

To remove the stack configuration, use the following command:

```
NPB(config)# no stack module <mid>
```

To see the stack configuration, use the following command:

```
NPB# show stack [module <mid>]
```

## Stack Management Using the WebUI

To create a stack using the WebUI, select **Stack – Modules** in the Navigation panel. Use the **Add** and **Delete** buttons to add and remove modules. Use the extension panel to set the module's parameters.

**Figure 93: Creating Stack Using WebUI**

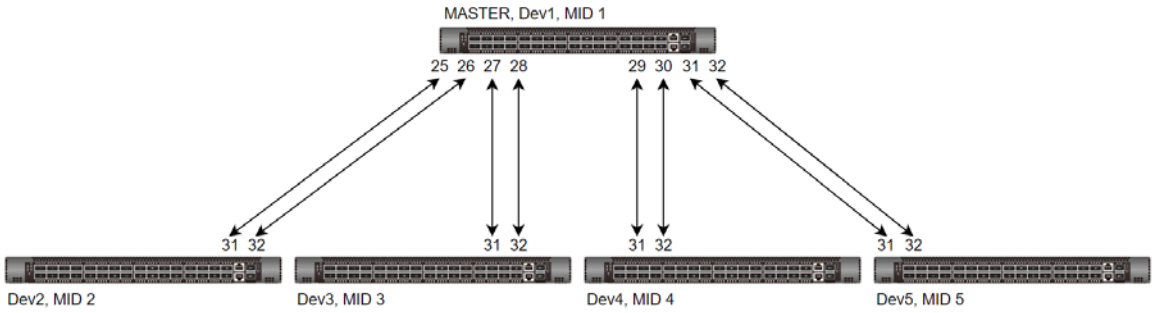

To define the module's stack load balancing port groups using the WebUI, select **Stack – Ports** in the Navigation panel. Use the **Add** and **Delete** buttons to add and remove groups. Use the extension panel to set the group's parameters.

## Stack Creation Example

This example shows the construction of a stack of five devices using a spine leaf topology. For convenience, the spine device is set as the master. A stack backbone link speed of 200G is desired, therefore, two 100G ports are defined as stack load balance groups on each device for each physical connection.

The diagram below shows the stack topology with Dev1 as the master, the assigned module IDs, the stack load balancing port assignments, and the physical cabling.

**Figure 94: Example: Stack of Five Devices Using a Spine Leaf Topology**



To configure this stack from the CLI, use the following commands:

In the master device (Dev1)

```
stack module 1 role master local
stack stack-lb-group name2 ports 1/25, 1/26
stack stack-lb-group name3 ports 1/27, 1/28
stack stack-lb-group name4 ports 1/29, 1/30
stack stack-lb-group name5 ports 1/31, 1/32
```

In Dev2:

```
stack module 2 role normal local
stack stack-lb-group name1 ports 2/31, 2/32
```

In Dev3:

```
stack module 3 role normal local
stack stack-lb-group name1 ports 3/31, 3/32
```

In Dev4:

```
stack module 4 role normal local
stack stack-lb-group name1 ports 4/31, 4/32
```

In Dev5:

```
stack module 5 role normal local
stack stack-lb-group name1 ports 5/31, 5/32
```

## Stack Topology Diagram

The WebUI application provides a topology diagram that displays the configured stack. The diagram allows you to observe the stack devices, links connectivity and status, and to rearrange the entities on the canvas. It does not allow you to configure the stack entities (for example, to add or remove devices).

To display the stack topology diagram, select **Stack – Topology** in the Navigation panel.

- Drag and drop a device to relocate it.
- Click on a link to see information on its ports and status.
- Clink on a device to see information about its role and connectivity.
- Device and link colors indicate their connectivity status.
- Use the buttons above the table to search for a specific device by module IP or hostname.

**Figure 95: Stack Topology Diagram**


## Stack SW Upgrade

Stack SW upgrade is similar to the standalone process as described in Section SW Upgrade on p.56. Upgrade can be performed on all or some of the modules as described below.

To upgrade the stack images from the CLI, use the following command:

```
NPB(config)# system sw-upgrade start [user <user>] [pass <pass>]
[module <list of mids or 'all'>] remote-url [ <url> <url> … ]
```

**Note:**
The lists of URLs contain the images for all the given device types.
Example: If the module types are NPB I, NPB II, and NPB IIe, three URLs are provided, one for each type. This command automatically loads the correct images for the devices based on their type.

To switch or change the boot bank from the CLI, use the following command:

```
NPB(config)# system sw-upgrade boot-bank [bank-a|bank-b] [version
<version>] [module <list of mids or 'all'>]

NPB(config)# system sw-upgrade switch boot-bank [module <list of mids
or 'all'>]
```

To reboot the modules, use the following command:

```
NPB(config)# system reboot [module <list of mids or 'all'>]
```

To manage stack upgrade using the WebUI, select **Configuration – SW Upgrade** in the Navigation panel. Select the required devices and click **Upgrade** or **Switch Version**.

# Users

The NPB device supports user management for both local and remote users. RADIUS and TACACS+ are supported as AAA remote servers.

When a user attempt to login to the system, the local and remote account lists are queried according to a configurable order. Once logged in, the user is assigned to one of the predefined authorization groups. This allows a role-based user authorization where each user has a different set of permissions according to his group.

The device is preconfigured with three authorization groups: **`read-only`**, **`oper`** and **`admin`**, and with one local user named **`admin`** who is a member of the **`admin`** group.

This section describes the NPB users management, users authentication and users authorization support.

## Local Users

Local users are users that are defined locally on the device, that is, their login authentication does not involve accessing remote AAA servers. The **`admin`** user predefined on the device cannot be deleted or modified. Additional local users can be added and deleted by users in the **`admin`** group.

To add or update local users from the CLI, use the following command:

```
NPB(config)# system aaa username <user-name>
```

When creating a new user, the device prompts for password and group.

To change local user password from the CLI, use the following command:

```
NPB(config)# system aaa username <user-name> change-password
```

To reset local user password from the CLI, use the following command:

```
NPB(config)# system aaa username <user-name> reset-password
```

This action changes the user's password to a new randomly generated password.

To delete a local user from the CLI, use the following command:

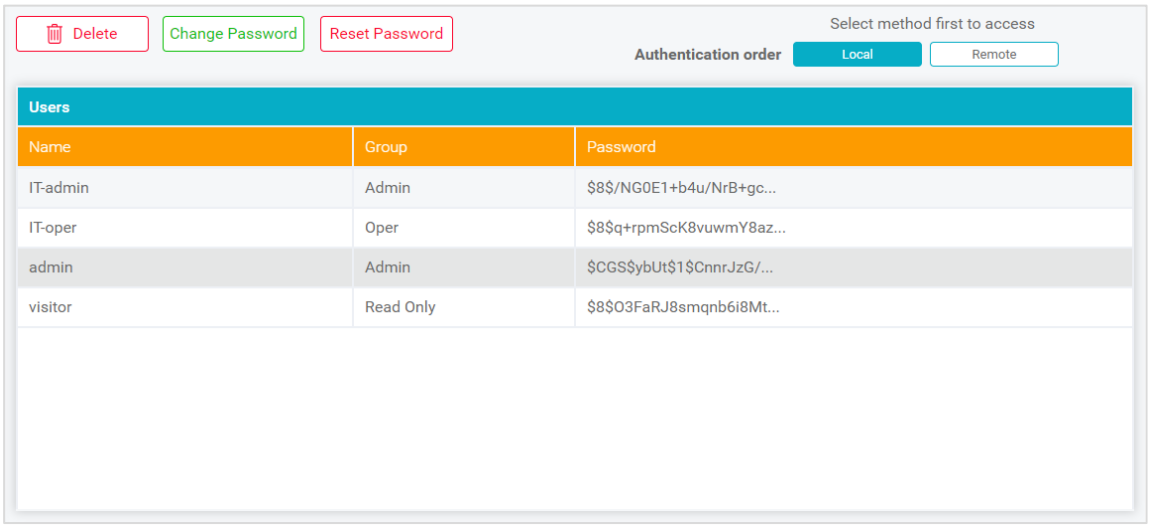
```
NPB(config)# no system aaa username <user-name>
```

To display local users from the CLI, use the following command:

```
NPB# show system aaa
system aaa
Username        Password        Group       Status
=============== =============== =========== =======
admin           $1$1T4NiuT5$DB Admin       OK
IT-MGR          $1$ORpLfhDD$Vv Oper        OK
Visitor         $1$K9PZSWJF$w0 Read Only   Locked
```

To configure local users using the WebUI, select **Management – Users** in the Navigation panel. Local users are displayed in the Users table.

**Figure 96: Configuring Local Users using the WebUI**



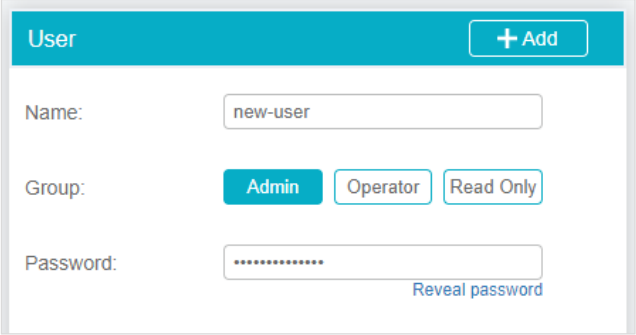

To update user information, select the user in the list, update the information in the extension panel, and click **Update**.

To change or reset a user's password, click **Change Password** or **Reset Password** on top of the screen.

To delete a user, select the user in the list, and click **Delete**.

To add a new user, double-click the admin user, fill in the new user's details in the extension panel and click **Add**.

**Figure 97: Adding New User**



## Password Management

To protect against unauthorized access, the NPB enforces the following limitations upon the password selection for local users:

- Passwords must start with a digit or a letter.
- Passwords must be at least 8 characters long.
- Passwords must contain at least one character from each of the following groups:
  - Lower-case letters
  - Upper-case letters
  - Digits
  - Special characters of the set !#$%&')(*+,-./:;<=>?@[\]^_`{|}~
- Passwords must not contain the user name nor the reversed user name.
- New passwords must differ from the five last passwords used

Passwords must be changed according to the following rules:

- Every 30 days
- Only 7 days after the last change

Users who are members in the **admin** group can change and reset passwords for all local user in the system. Other users can only change their own password. The predefined **admin** user's password can be reset only by the **admin** user itself.

Failing to enter the correct password for 3 times will block the user for 5 minutes.

# Dormant Users

Dormant users are local users that did not attempt to login to the device for a predefined number of days (up to 1000 days). It is possible to block the next login attempts of such users. Admin user intervention is required to reactivate such users.

To block or unblock dormant users from the CLI, use the following command:

```
NPB(config)# system aaa [no] block-dormant <days>
```

An admin user can delete all dormant users from the CLI, using the following command:

```
NPB(config)# system aaa dormant-delete-all
```

An admin user can reactivate a specific dormant user from the CLI, using the following command:

```
NPB(config)# system aaa username <name> reactivate
```

To configure dormant user behavior using the WebUI, select **Management – Users** in the Navigation panel. Use the buttons above the table to set the blocking time, and to delete or reactivate dormant users.

# Remote Users and Servers

Remote users are users that are defined on a remote server such as RADIUS and TACACS+. To authenticate such users, a connection to the remote server must be established.

The NPB device supports both RADIUS and TACACS+ as remote AAA servers.

Remote users get their authorization (group assignment) from the remote server.

- For Radius users, this is done using the server-reply message.
- For TACACS+ users, this is done using the priv_lvl AV pair. The mapping between privileges and groups is configurable, by default it is: admin = 1, oper = 3, read-only = 5

See Section Groups on p. 191 for more details about user groups.

To configure a remote AAA server from the CLI, use the following command:

```
NPB(config)# system user-mgmt remote-server <server-id> address
<server-name-or-address> auth-method radius|tacacs key <server-key>
[port <port-number>] [admin enable|disable]
```

When no port number is given, the default ports are used (1812 for RADIUS, 49 for TACACS+). When no **admin** value is given, the server is created with **admin** enabled.

To set TACACS+ privileges from the CLI, use the following command:

```
NPB(config)# system user-mgmt tacacs admin-priv-level <level> oper-
priv-level <level> read-only-priv-level <level>
```

The system supports up to five AAA servers. The AAA servers' access order is according to their location in the list.

To remove an AAA remote server from the list from the CLI, use the following command:

```
NPB(config)# no system user-mgmt remote-server <server-id>
```

To configure AAA remote servers using the WebUI, select **Management – Users** in the Navigation panel.

**Figure 98: Configuring AAA Remote Servers using the WebUI**


AAA remote servers are displayed in the AAA Servers table.

Use the extension panel to add, delete, or update remote servers.

Use the TACACS+ button above the table to set TACACS+ privileges mapping.

## User Authentication

The order in which user authentication is performed can be configured. By default, local users are checked before remote users. The order in which the remote servers are accessed is according to their position in the list.

To set the authentication order from the CLI, use the following command:

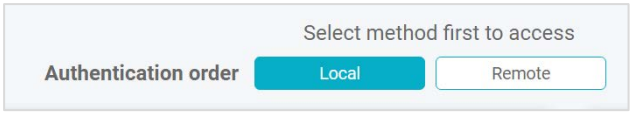
```
NPB(config)# system user-mgmt auth-order local-first|remote-first
```

The authentication order is displayed as part of the **`show system user-mgmt`** command:

```
NPB# show system user-mgmt
```

To configure the user authentication order using the WebUI, select **Management – Users** in the Navigation panel. Click either **Local** or **Remote** to set the first authentication method.

**Figure 99: Configuring User Authentication Order using the WebUI**




## Groups

After a successful user authentication, the user is assigned to a group that dictates the user privileges and permissions. The NPB device supports three predefined groups as described below. A user that is not explicitly assigned to a group is considered to be in the **`read-only`** group.

**Table 55: Permissions according to User Groups**

| Permissions | User Group | | | Notes |
|---|---|---|---|---|
| | Read-only | Operators (oper) | Administrators (admin) | |
| Read-only permissions | X | X | X | |
| Port settings | | X | X | |
| Filter settings | | X | X | |
| Load balancing groups | | X | X | |
| GRE tunneling | | X | X | |
| Self-user management (change his own password) | | X | X | Operator users can set their own password |
| Configuration files management | | X | X | |

| Permissions | User Group | | | Notes |
|---|---|---|---|---|
| | Read-only | Operators (oper) | Administrators (admin) | |
| Management interface settings (mgmt. port, SNMP) | | | X | |
| High Availability | | | X | |
| ACL management | | | X | |
| Local and remote users management | | | X | |
| Session management and CLI parameters | | | X | |
| System tools (reboot, factory default, hostname, debug reports) | | | X | |
| Logs and syslogs | | | X | |
| SW upgrade | | | X | |

**Note:**
If the same user is configured as both local and remote but with a different group assignment for each, he will get the permissions of the least privileged group. Such cases are hard to maintain and should be avoided for security reasons.

## Example: Working with Free-RADIUS and TAC-plus

The example below demonstrates the configuration of free-RADIUS and TAC-plus servers to work with the NPB device. Refer to free-RADIUS documentation for more details.

Assuming we want to define the following user on the RADIUS server:

User: npb-user

Password: npb-password

Group: Oper

The AAA server's IP, port and key are as follows:

IP: 192.168.200.200

Port: 120

Server key: npb-AAA-key

The IP of the NPB device is as follows:

NPB IP: 192.168.10.10

To configure the NPB device with the RADIUS parameters, use the following CLI command:

```
NPB(config)# system user-mgmt remote-server 1 auth-method radius
address 192.168.200.200 port 120 key npb-AAA-key
```

To configure the NPB device with the TACACS+ parameters, use the following CLI command:

```
NPB(config)# system user-mgmt remote-server 2 auth-method tacacs
address 192.168.200.200 port 120 key npb-AAA-key
```

## Free-RADIUS Configuration

To configure the free-RADIUS server, perform the following steps:

1. Add the user to the **users** file (/etc/freeradius/users):

```
"npb-user"
      Cleartext-Password:= "npb-password"
      Reply-Message = "oper"
```

2. Add the NPB device as an authenticated client to the **client.conf** file (/etc/freeradius/clients.conf)

```
client NPB {
      ipaddr = 192.168.10.10
      secret = npb-AAA-key
}
```

3. You may need to restart the RADIUS service for it to reload the configuration.

## TAC-plus Configuration

To configure the TAC-plus server, perform the following steps:

1. Create a group for **oper** users by editing the configuration file (/etc/tacacs+/tac_plus.conf), note that the priv_lvl for oper users is 3:

```
group = oper {
      default service = permit
      service = ppp
      protocol = ip {
            priv_lvl = 3
      }
}
```

2. Create the user, and add it to the oper group (same file):

```
user = npb-user {
      name = "NPB Oper User"
      member = oper
      pap = cleartext npb-password
}
```

3. You may need to restart the TAC-plus service for it to reload the new configuration.

# Active Sessions

It is possible to see currently logged-in users and interact with them using messages. It is also possible for the **admin** user to log off other users.

To see all active users from the CLI, use the following command:

```
NPB# who
```

To log off a user or a session from the CLI, use the following command:

```
NPB# logout user|session <user-name>|<session-id>
```

To send a message to all or some active users from the CLI, use the following command:

```
NPB# send all|<user-name> "<message>"
```

For example:

```
NPB# send admin "Hi, Admin user"
```

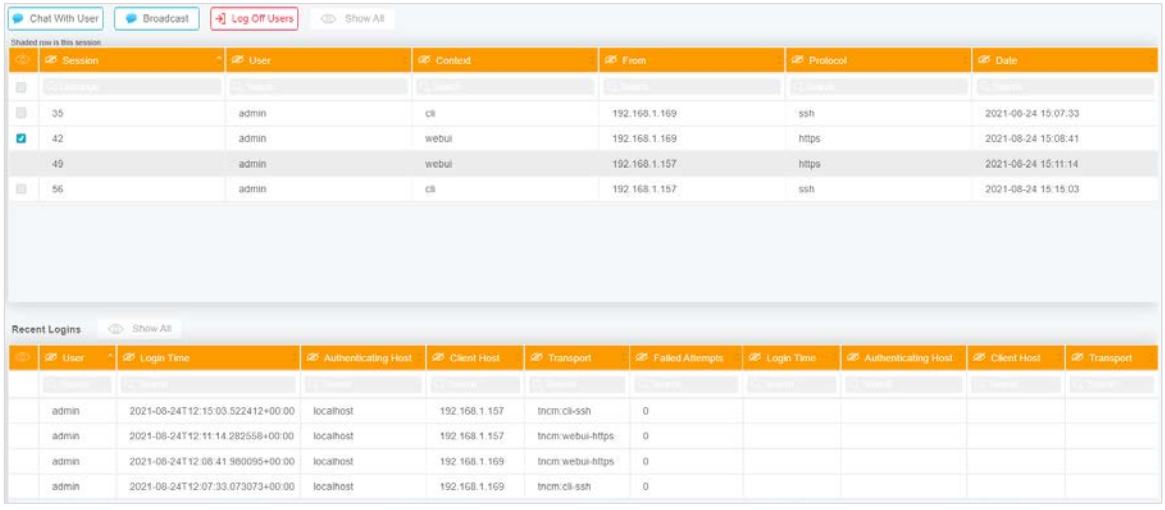
To see recent login attempts from the CLI, use the following command:

```
NPB# show last-logins
```

To handle logged-in users using the WebUI, select **Management – Sessions** in the Navigation panel. The following actions are available:

- You can have a chat session with another logged-in user by selecting the user and clicking **Chat with User**.
- You can send a message to all logged in users by clicking **Broadcast**.
- Users with admin privileges can log off users by selecting them and clicking **Log Off Users.**
- The row representing your current session is highlighted in gray.
- Recent login attempts are displayed in the bottom table

**Figure 100: Handling Users in Active Session**



# High Availability

## Overview

The NPB provides High Availability (HA) support to allow continuous operation in case a machine is down due to maintenance or a fault condition. HA is based on a cluster of two machines that are configured identically. One machine acts as the active machine and the other as passive. When the active machine's health level is inferior compared to the passive machine's level, a switchover occurs, and the passive machine takes control.

NPB supports two modes of high availability:

- Active-Active: In this mode, the ports on the passive machine behave the same as the ports in the active machine. This means that traffic that enters the passive machine is processed and redirected normally. If this is not desirable, it is up to the user to direct traffic only to the active machine.
- Active-Standby: In this mode, the ports on the passive machine are in Standby mode. This means that their link is forced to be down. Traffic cannot enter the device. In this mode, the user can redirect traffic to both devices, knowing it will only be processed by the active machine.

## HA Operation

HA mode of operation is defined as follows:

- HA is based on a cluster of two identical NPB machines running the same SW image.
- When HA is enabled, one of the machines is elected as active (master) and the other as passive (slave).
- The initial role of each machine is configurable.
- Only the active machine can be configured. The passive machine acts as read-only.
- Both machines can be accessed normally using their management IP address. In addition, an optional Virtual IP (VIP) address can be configured that always leads to the currently active machine.
- All configuration changes done on the active machine are automatically replicated to the passive machine.
- Both machines are running a periodic health check algorithm exchanging information regarding their status. This information is used to detect cases where a switchover is required.
- Switchover occurs in the following cases:
    - The active machine is no longer available.
    - The health level of the active machine is inferior compared to the passive machine's.
    - Both machines have the same health level, but the currently passive machine is to become active (e.g. due to a Revert Failover mode as described below).
- Upon switchover, the passive machine becomes active, and the VIP points to it. In case of Active-Standby mode, the ports are taken out of Standby mode.

- The two machines can be coupled by configuring each with the IP address of its peer, or by associating the same cluster ID to both.
- When the passive machine is not available, the commits made in the active machine are not synced. The commits are synced as soon as the passive machine is up again. The number of unsynced commits can be shown using the CLI or WebUI as explained below.

## Monitored Ports

It is possible to define a set of ports to be monitored by the HA module on both machines. If any of these ports change their link status to down in the active machine, while the monitored ports are up in the passive machine, a switchover may occur depending on other setting and conditions, e.g. the hysteresis parameter.

When working in Active-Standby mode, monitored ports admin state is kept enabled in the standby device, so link changes can be detected. Traffic received on these ports is dropped.

## HA Conflicts

HA conflicts may occur when the two machines are configured independently or when the HA settings on both machines mismatch. When a conflict is detected, data replication stops until the conflict is resolved.

The NPB provides two methods for conflict resolution:

- Use primary – The machine that was set as primary is defined as the new active machine.
- Resolve manually – The user manually sets one of the machines as active.

After the conflict has been resolved, data replication starts again, replicating the active machine's configuration into the passive machine and overwriting the existing configuration on that machine.

## Managing HA

Table 56 provides a list of the HA settings.

**Table 56: HA Settings**

| Name | Description | Possible Values |
|---|---|---|
| admin | Activates and deactivates HA | enabled, disabled<br>Default is **`disabled`** |
| Mode | Sets the HA mode, must be configured identically on both machines | active-active, active-standby<br>Default is **`active-standby`** |
| Role | The initial role of the machine, must be configured differently on each machine | primary, secondary |

| Name | Description | Possible Values |
|---|---|---|
| monitored ports | The set of ports monitored by the HA module | List of ports or port groups separated by commas. Ranges can be specified using hyphens. |
| peer IP | Sets the IP address of the other machine in the HA cluster | Valid IPv4 address |
| cluster ID | Sets the cluster ID for this machine, must be configured identically on both machines and on no more than two machines | Integer number |
| virtual IP | Sets the virtual IP used for the cluster; this IP always points to the current active machine | Valid IPv4 address |
| failover mode | Sets the behavior when a machine is available again after a failover. The machine can either **revert** to its original role or **retain** its current state. Note that reverting may cause additional switchovers. Must be configured identically on both machines | revert, retain<br>Default is **`retain`** |
| conflict resolve mode | Sets the method in which conflicts are resolved. See Section HA Conflicts on p.196 above. | use-primary, manual<br>Default is **`use-primary`** |
| resolve-conflict | Manually sets the role of the machine to be either active (master) or passive (slave). Valid only when a conflict occurs and the Conflict Resolve mode is manual. See Section HA Conflicts on p.196 above. | be-master\|be-slave |
| Hysteresis | Sets the minimal time to wait between consequent switchovers | 0 – 3,600 seconds<br>Default is 10 seconds |

## Managing HA using the CLI

To enable or disable HA from the CLI, use the following command (no commit is needed, action takes place immediately):

```
NPB(config)# ha enabled|disabled
```

To set the HA mode, use the following command:

```
NPB(config)# ha mode active-active|active-standby
```

To set the VIP address, use the following command:

```
NPB(config)# ha virtual-ip <ip>
```

To set HA attributes, use the following command (no commit is needed, action takes place immediately):

```
NPB(config)# ha set cluster-id <id>|peer-ip <ip> role
primary|secondary
```

To set a list of monitored ports, use the following command:

```
NPB(config)# ha monitored-ports <list of port-ids and port groups>
```

To unset the list of monitored ports, use the following command:

```
NPB(config)# no ha monitored-ports
```

The following optional attributes can be set only when HA is disabled:

```
NPB(config)# ha [conflict-resolve-mode manual|use-primary] [failover-
mode retain|revert] [hysteresis <interval in sec>]
```

To resolve a conflict, use the following command (no commit is needed, action takes place immediately):

```
NPB(config)# ha resolve-conflict be-master|be-slave
```

To review the conflict in a diff like notation, use the following command:

```
NPB# ha show-conflict password <password>
```

Where password is the current user's password on the peer machine

To review the current HA status, use the following command:

```
NPB# show ha
```

## Managing HA using the WebUI

When HA is enabled, the HA icon is displayed on the status bar with an indication of the current synchronization status. The notification bubble can display the following: A number inside the bubble indicates the number of unsynced commits. U means Unconnected, C means Conflict, and S means not-Synced. Hovering on the icon reveals more details about the current HA status

**Figure 101: HA Status using WebUI**



When accessing a machine that is in Slave state, the Commit button is greyed out and indicates **Slave**.

To use the High Availability feature , select **High Availability - Configuration** from the Navigation panel, or click the HA icon in the Status bar, and set the relevant parameters.

The Resolve Conflict section appears only when there is a conflict. To show the conflict details, click **Show Conflict**. To resolve a conflict, click **Be Master** or **Be Slave** buttons to set this machine as Master or Slave.

**Figure 102: HA Settings – Showing a Conflict**

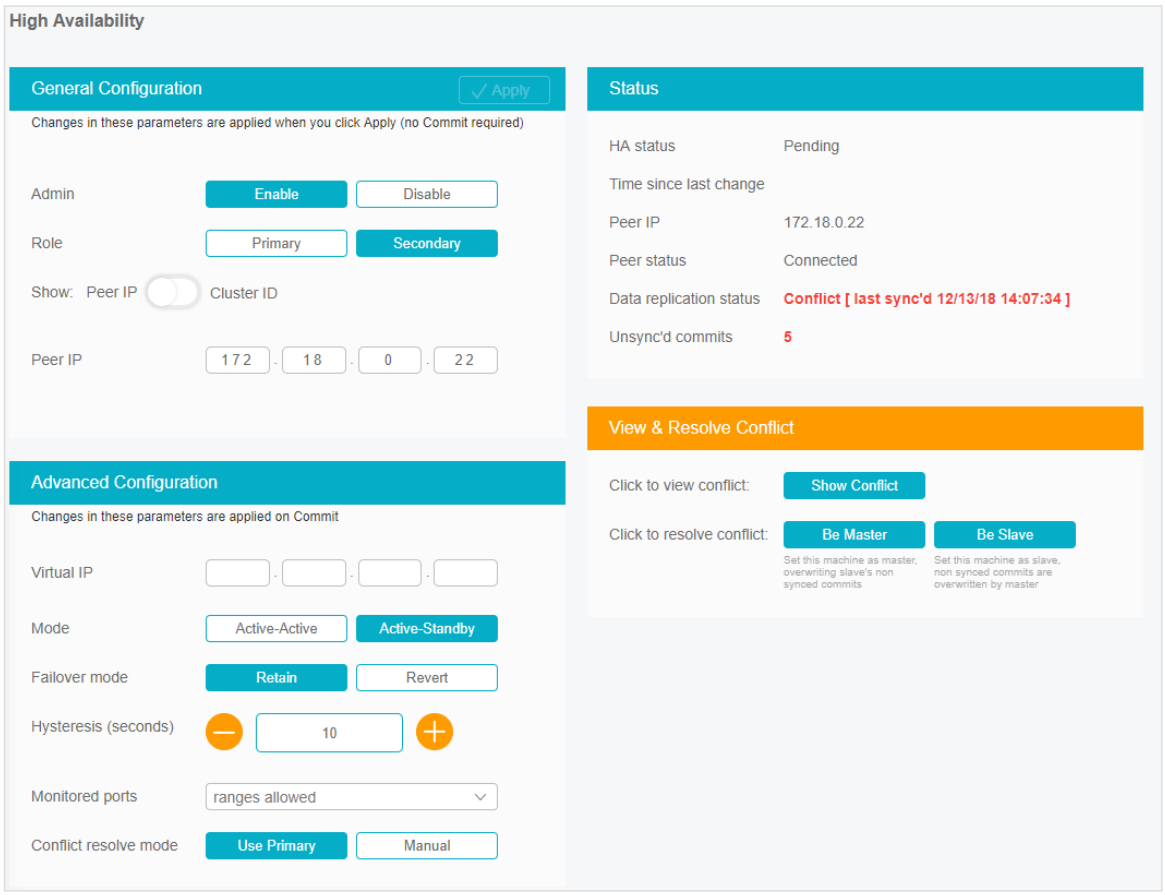
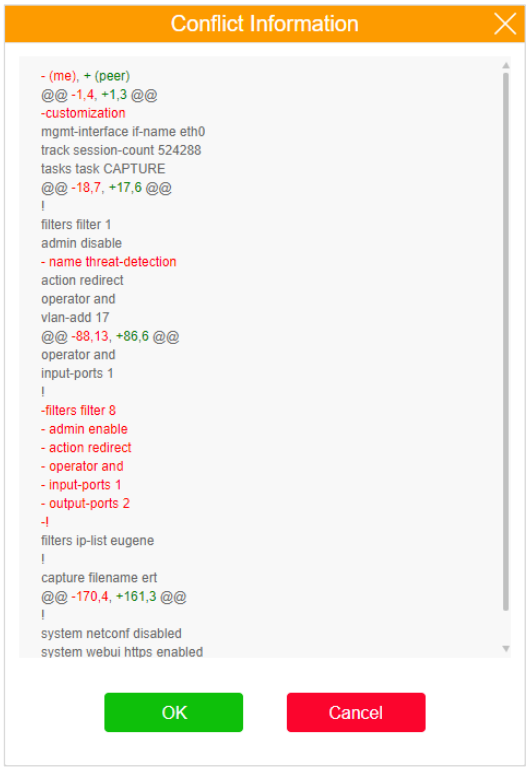



**Figure 103: Show Conflict Output Example**



## Setting HA Cluster

This section describes how to set two machines (A and B) as a HA cluster.

Make sure before starting the procedure that the SW image installed on both machines is identical.

In addition, it is recommended that the HA settings for Resolve Conflict mode and Failover mode are identical on both machines. Otherwise, a conflict may occur.

It is also recommended that both machines share the same time-and-date setting (either by using the same NTP server or by setting the local clock manually to the same value).

In the steps below, Machine A is set as primary. This may be convenient if there is a configuration on A that you want to replicate to B.

To set setting a HA cluster, perform the following steps:

1. In Machine A, set the HA Mode parameter to be **`active-active`** or **`active-standby`**.
2. In Machine A, set the HA role to be either **`primary`** or **`secondary`**.
3. In Machine A, set the Cluster ID or Peer-IP address (IP address of Machine B).
4. In Machine A, set the VIP address for the cluster (optional, can be done at any stage).
5. In Machine A, change the default settings for Failover mode, Conflict Resolve mode and hysteresis if needed (optional).
6. In Machine B, set the opposite role.
7. If you used a Cluster ID in Machine A, set the same Cluster ID in Machine B. Otherwise, in Machine B, set IP address of Machine A as the peer-ip address.
8. The VIP and optional settings set in Machine A will be replicated to Machine B once HA syncs.
9. Commit all changes in Machines A and B.
10. In Machine A, set HA to enabled.
11. In Machine B, set HA to enabled.
12. Use the CLI or WebUI to monitor the HA status. If the two devices have connectivity, Machine A is defined as active and Machine B as passive.

Once synced, you can use the active device's IP address or the VIP (if configured) to access the active device.

# SNMP

## Overview

This section describes the NPB support of SNMP (Simple Network Management Protocol). The NPB SNMP agent supports SNMP v2c read and write communities, SNMP v3 users, and acts as an SNMP trap sender. This section also provides a description of CGS proprietary MIB supported by the NPB device.

## General SNMP Configuration

### SNMP Agent

The NPB device runs an SNMP agent that can be accessed from the user's SNMP client, using a configurable port. This connection can be used for standard SNMP actions (walk, get, set, etc.). Each such action is considered an atomic transaction that may be fully committed or rejected, that is, if several values have been changed in a single transaction and the transaction was rejected, the entire transaction will not be committed.

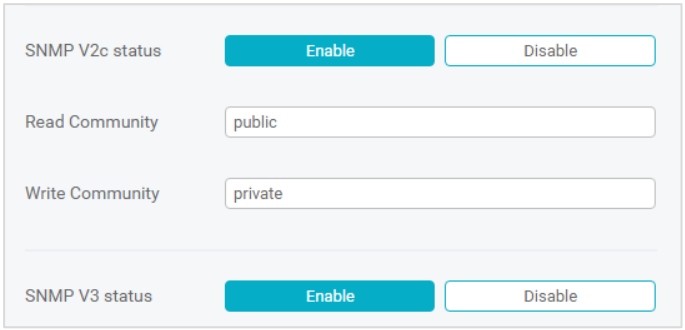
By default, the SNMP agent is not active. To use it, it must be explicitly activated for each SNMP version.

To activate the SNMP agent from the CLI, use the following command:

```
NPB(config)# system snmp v2c|v3 true|false
```

To activate the SNMP agent using the WebUI, select **Management – General settings** in the Navigation panel. Click either **Enable** or **Disable** next to each SNMP version.

**Figure 104: Activating the SNMP Agent using the WebUI**



## General Configuration

SNMP has a set of general attributes that can be configured. Table 57 lists these attributes.

**Table 57: SNMP Attributes**

| Name | Description | Possible Values |
|---|---|---|
| v2c | SNMP v2c status | true/false, default is **`false`** |
| v3 | SNMP v3 status | true/false, default is **`false`** |
| port | SNMP agent port | UDP port, default is 161 |
| sys-contact | System contact | Free text |
| sys-location | System location | |
| sys-name | System name | |
| read-community | SNMP v2c read community name | Free text, default is **`public`**<br>See SNMP V2 Communities |
| write-community | SNMP v2c write community name | Free text, default is **`private`**<br>See SNMP V2 Communities |
| v3-username | SNMP v3 users settings | Refer to Section SNMP V3 Users on p.205 |
| trap-server | SNMP trap servers settings | Refer to Section SNMP Trap on p.206 |
| engine-id | ID of the SNMP agent engine, used for the authorization of SNMP transaction. This value is not configurable and identifies the specific NPB device | Not configurable |

To set the general SNMP configuration from the CLI, use the following command:

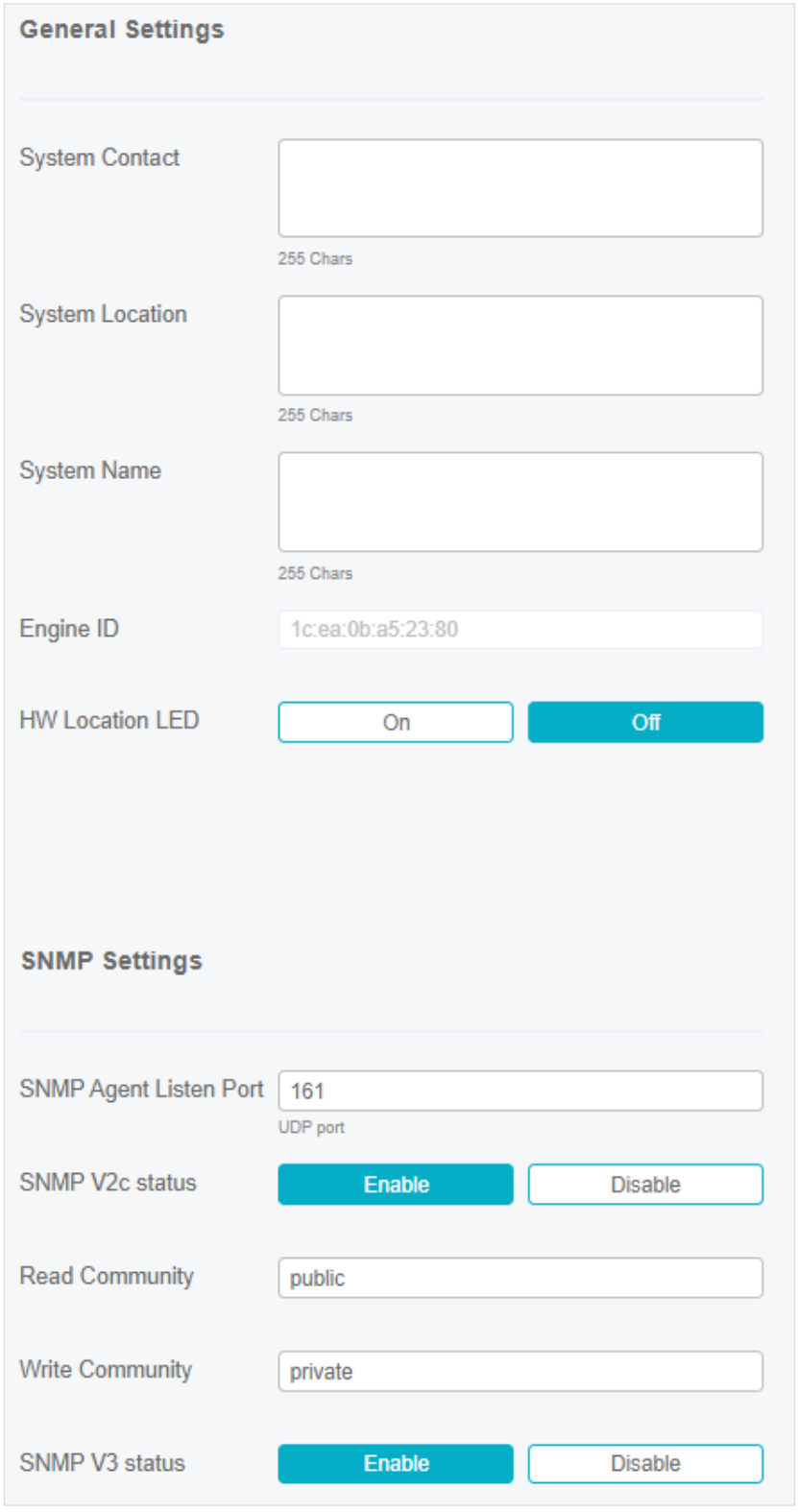
```
NPB(config)# system snmp [v2c true|false] [v3 true|false] [port
<port>] [sys-name <name>] [sys-contact <contact>] [sys-location
<location>]
```

To display SNMP settings from the CLI, use the following command:

```
NPB# show system snmp
```

To set the general SNMP configuration using the WebUI, select **Management – General settings** in the Navigation panel.

**Figure 105: Setting SNMP General Configuration using the WebUI**



# SNMP Communities and Users

## SNMP V2C Communities

SNMP v2c community names are used as passwords for read-only and read-write users. By default, the passwords are **`public`** and **`private`** but they can be changed for security reasons.

The NPB device grants write community users operator privileges, that is, these users can perform all actions that are exposable to SNMP that a CLI user who is a member of the operators group (**`oper`**) can do.

The NPB device grants read community users read-only privileges, that is, these users can perform all actions that are exposable to SNMP that a CLI user who is a member of the **`read-only`** group can do.

To change SNMP v2c community names from the CLI, use the following command:

```
NPB(config)# system snmp read-community|write-community <name>
```

To change SNMP v2c community names using the WebUI, select **Management – General settings** in the Navigation panel.

## SNMP V3 Users

The NPB device supports both USM and VACM users as defined by SNMP. The user privileges are set according to the authentication access property of the user.

The NPB device grants users with read-write authentication access operator privileges, that is, these users can perform all actions that are exposable to SNMP that a CLI user who is a member of the operators group (**`oper`**) can do.

The NPB device grants users with read-only authentication access **`read-only`** privileges, that is, these users can perform all actions that are exposable to SNMP that a CLI user who is a member of the **`read-only`** group can do.

SNMP V3 users have the following parameters:

**Table 58: SNMP V3 User Parameters**

| Name | Description | Possible Values |
|---|---|---|
| v3-user-name | User name | Free text |
| auth-access | User authorization access | Read-only/read-write |
| auth-pass | SNMP authentication password | String |
| auth-protocol | SNMP authentication protocol | MD5/SHA/none |
| priv-pass | SNMP privacy password | String |
| priv-protocol | SNMP privacy protocol | AES-128/DES/none |

To define an SNMP v3 user from the CLI, use the following command:

```
NPB(config)# system snmp v3-username <user-name> auth-access read-
only|read-write auth-protocol MD5|SHA|none auth-pass <auth-password>
priv-protocol AES-128|DES|none priv-pass <priv-password>
```

To remove an SNMP v3 user from the CLI, use the following command:

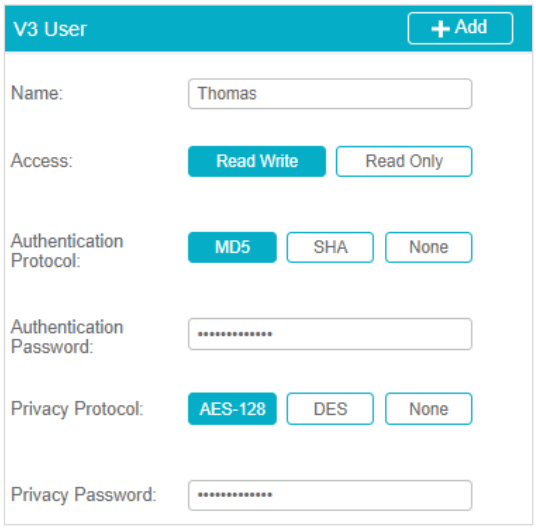
```
NPB(config)# no system snmp v3-username <user-name>
```

To display SNMP v3 users from the CLI, use the following command:

```
NPB# show system snmp v3-username
```

To manage SNMP v3 users using the WebUI, select **Management – SNMP** in the Navigation panel. SNMP v3 users are displayed in the V3 Users table. Use the extension panel to add, delete, or update users.

**Figure 106: SNMP v3 Users Extension Panel**




## SNMP Trap Server

Table 59 lists the parameters of the SNMP trap server.

**Table 59: SNMP Traps Parameters**

| Name | Description | Possible Values |
|---|---|---|
| name | Trap server name | Free text |
| address | Trap server IP address | Valid IPv4 address |
| port | Trap server listen port | Valid UDP port, default is 162 |
| admin | Trap server status | Disable/enable, default is enable |
| trap-ver | Trap version | v2c-trap/v3-trap |

| Name | Description | Possible Values |
|---|---|---|
| community | SNMP v2c community that is used for sending traps to the server | Valid v2c community |
| v3-user | SNMP v3 user that is used for sending traps to the server | Configured v3 user name |

To add a v2c trap server from the CLI, use the following command:

```
NPB(config)# system snmp trap-server <name> address <address> [admin
enable|disable] [port <port-number> trap-ver v2c-trap community
<community-name>
```

To add a v3 trap server from the CLI, use the following command:

```
NPB(config)# system snmp trap-server <name> address <address> [admin
enable|disable] [port <port-number> trap-ver v3-trap v3-user <user-
name>
```

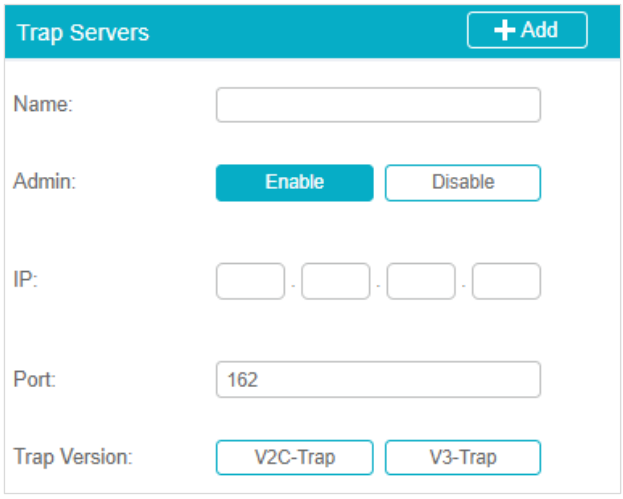
**Note:**
The v3 user name must refer to an existing v3 user.

To display the SNMP trap server configuration from the CLI, use the following command:

```
NPB# show system snmp trap-server
```

To manage SNMP trap servers using the WebUI, select **Management – SNMP** in the Navigation panel. SNMP trap servers are displayed in the Trap Servers table. Use the extension panel to add, delete, or update servers.

**Figure 107: SNMP Trap Servers Extension Panel**



# MIB Support

The NPB device uses the following OID as a root for all proprietary MIBs:

| | |
|---|---|
| NPB I | so(1).org(3).dod(6).internet(1).private(4).enterprises(1).cgs(47477).npb(100).npb-1(1)<br>1.3.6.1.4.1.47477.100.1 |
| NPB Ie | so(1).org(3).dod(6).internet(1).private(4).enterprises(1).cgs(47477).npb(100).npb-1e(5)<br>1.3.6.1.4.1.47477.100.5 |
| NPB Ie8 | so(1).org(3).dod(6).internet(1).private(4).enterprises(1).cgs(47477).npb(100).npb-1e8(6)<br>1.3.6.1.4.1.47477.100.6 |
| NPB II | so(1).org(3).dod(6).internet(1).private(4).enterprises(1).cgs(47477).npb(100).npb-2(2)<br>1.3.6.1.4.1.47477.100.2 |
| NPB IIe | so(1).org(3).dod(6).internet(1).private(4).enterprises(1).cgs(47477).npb(100).npb-2e(4)<br>1.3.6.1.4.1.47477.100.4 |
| NPB III | so(1).org(3).dod(6).internet(1).private(4).enterprises(1).cgs(47477).npb(100).npb-3(7)<br>1.3.6.1.4.1.47477.100.7 |
| NPB IV | so(1).org(3).dod(6).internet(1).private(4).enterprises(1).cgs(47477).npb(100).npb-4(8)<br>1.3.6.1.4.1.47477.100.8 |

The NPB device supports the following MIBs:

**Table 60: Supported MIBs**

| MIB Name | Description |
|---|---|
| SNMP-MIB2 | Standard SNMP MIB-2 (RFC 1213) |
| IF-MIB | Standard Interface Group MIB (RFC 2863) |
| NPB-SYSTEM | NPB system configuration |
| NPB-PORTS | NPB ports management |
| NPB-FILTERS | NPB filters management |
| NPB-LB | NPB load balancing groups management |
| NPB-GRE | NPB GRE tunneling management |
| NPB-HA | NPB high availability |
| NPB-INLINE | NPB inline solution management |
| NPB-HB | NPB heartbeat management |
| NPB-STACK | NPB stacking management |
| NPB-TRAPS | NPB traps configuration |

NPB MIBs can be extracted from the device as a tar file.

To extract the MIB files using CLI, use the following command:

```
NPB# system snmp export remote-url <url> [username <username>]
[password <password>]
```

For example:

```
NPB# system snmp export remote-url scp://192.168.10.10/config/
username admin password 1234
```

To extract the files using the WebUI, select **System – SNMP** in the Navigation panel.

## Trap Support

The NPB device supports the following types of traps:

**Table 61: Supported Traps**

| Name | Description | Variable Binding |
|---|---|---|
| Reboot completed | System has powered up after an expected reboot | Image name, current SW bank |
| Unexpected shutdown | System has powered up after an unexpected reboot | Image name, current SW bank |
| Port connectivity | Port status has changed from up to down or vice versa | Port number, port speed if the port is up |
| Port utilization | Port utilization has crossed a threshold | Port number, utilization figures |
| Transceivers | Transceiver temperature, voltage, or current have crossed a threshold | Transceiver number and status |
| Load balancing active port state change | Status of the load-balancing active port has changed from up to down or vice versa | Load-balancing group ID, port ID and state |
| Load balancing standby port event | Load-balancing standby port has replaced a failed active port | Load-balancing group ID, standby port ID, and failed port ID |
| Image installation started | Image installation process has started | User name and interface (CLI, WebUI, SNMP, or NETCONF), image name, target bank |
| Image installation completed | Image installation process has been completed | User name and interface (CLI, WebUI, SNMP or NETCONF), image name, target bank, status |
| Running image has changed | System powered up with a new image for the first time | Old and new image names, active SW bank |

| Name | Description | Variable Binding |
|---|---|---|
| High Availability status has changed | A High Availability switchover occurred, the connection to the peer has changed, or the data replication status has changed. | Status (master, slave, pending), connection status, data replication state, cluster id and peer id |
| HW (PSU, fans, temperature sensors) | An on-board HW component reported an error condition | HW component type and status |
| Recovery | Recovery event occurred | None |

NPB TRAP files are delivered with the NPB software.

# Appendix 1 – HW Specifications

## NPB I HW Specifications

### Ports

| | | |
|---|---|---|
| Switch ports: | 48 x SFP+ | Each supports 1 GbE or 10 GbE |
| | 6 x QSFP | Each supports 1x40 GbE or 4 x 1/10 GbE |
| Management ports: | 1 x RJ-45 serial console | |
| | 1 x RJ-45 100/1000BASE-T management | |
| | 1 x USB Type A storage | |

### Physical and Environmental

| | |
|---|---|
| Dimensions (WxDxH): | 44.3 x 47.3 x 4.34 cm (17.4 x 18.6 x 1.71 in) |
| Weight: | 8.5 kg (18.74 lb), with two installed PSU modules |
| Fans: | Hot-swappable 4+1 redundant fans |
| Operating temperature: | 0°C to 40°C (32°F to 104°F) |
| Storage temperature: | -40°C to 70°C (-40°F to 158°F) |
| Operating humidity: | 5% to 95% non-condensing |

### LEDs

| | |
|---|---|
| QSFP/SFP+ Port LEDs: | Link Status, Activity, Rate |
| Ethernet Management Port LED: | Link Status, Activity |
| Console Port LED: | Link Status |
| System LEDs: | Diagnostic, Locator, PSU and Fan Status |

### Power

| | |
|---|---|
| PSUs: | 2 redundant, load-sharing, hot-swappable AC or -48V DC |
| Input voltage: | 90V to 264V AC at 50-60 Hz. -48 to -72V DC. |
| Input current: | Max 6 A@100/120V AC, 3 A@ 200/240V AC,10 A@ -72V DC |
| PSU efficiency: | Up to 93% for AC PSUs |
| Power input option: | 12V DC |
| Max power: | 282W, without pluggable optics |

# NPB Ie HW Specifications

## Ports

| | | |
|---|---|---|
| Switch ports: | 48 x SFP+ | Each supports 1 GbE or 10 GbE |
| | 6 x QSFP28 | Each supports 40 GbE or 100 GbE |
| Management ports: | 1 x RJ-45 serial console | |
| | 1 x RJ-45 100/1000BASE-T management | |
| | 1 x USB Type A storage | |

## Physical and Environmental

| | |
|---|---|
| Dimensions (WxDxH): | 44 x 54.8 x 4.4 cm (17.32 x 21.57 x 1.73 in) |
| Weight: | 9.34 kg (20.59 lb), with two installed PSU modules |
| Fans: | Hot-swappable 5+1 redundant fans |
| Operating temperature: | 0°C to 40°C (32°F to 104°F) |
| Storage temperature: | -40°C to 70°C (-40°F to 158°F) |
| Operating humidity: | 5% to 95% non-condensing |

## LEDs

| | |
|---|---|
| QSFP28/SFP+ Port LEDs: | Link Status, Activity, Rate |
| Ethernet Management Port LED: | Link Status, Activity |
| Console Port LED: | Link Status |
| System LEDs: | Diagnostic, Locator, PSU and Fan Status |

## Power

| | |
|---|---|
| PSUs: | 2 redundant, load-sharing, hot-swappable AC or -48V DC |
| Input voltage: | 100V to 240V AC at 50-60 Hz; -48V to -72V DC |
| Input current: | Max 6 A@100/120V AC, 3 A@ 200/240V AC, 10 A@ -72V DC |
| PSU efficiency: | Up to 93% for AC PSUs |
| DC output: | 5V DC @ 4 A, 12V DC @ 52.9 A |
| Power input option: | 48V DC, 100V to 240V AC |
| Max power: | 360W, without pluggable optics |

# NPB Ie8 HW Specifications

## Ports

| | | |
|---|---|---|
| Switch ports: | 48 x SFP28 | Each supports 1 GbE, 10 GbE, or 25GbE |
| | 8 x QSFP28 | Each port supports 1x10/40/100 GbE or 4 x 1/10/25 GbE or 2x 50 GbE per port using splitter cables. |
| Management ports: | 1 x RJ-45 serial console | |
| | 1 x RJ-45 100/1000BASE-T management | |
| | 1 x USB Type A storage | |

## Physical and Environmental

| | |
|---|---|
| Dimensions (WxDxH): | 43.8 x 53.6 x 43.5 cm (17.26 x 21.1 x 1.71 in.) |
| Weight: | 10 kg (22.05 lb), with two installed PSUs |
| Fans: | Hot-swappable 5+1 redundant fans |
| Operating temperature: | 0°C to 45°C (32°F to 113°F) |
| Storage temperature: | -40°C to 70°C (-40°F to 158°F) |
| Operating humidity: | 5% to 95% non-condensing |

## LEDs

| | |
|---|---|
| QSFP28/SFP+ Port LEDs: | Link Status, Activity, Rate |
| Ethernet Management Port LED: | Link Status, Activity |
| Console Port LED: | Link Status |
| System LEDs: | Diagnostic, Locator, PSU and Fan Status |

## Power

| | |
|---|---|
| PSUs: | 2 redundant, load-sharing, hot-swappable AC or -48V DC |
| Input voltage: | 100V to 240V AC at 50-60 Hz; -36V to -72V DC |
| Input current: | Max 7.8A@100/120V AC, 3.8A@200/240V AC, 16A@ -36 to -72V DC |
| PSU efficiency: | Up to 93% for AC PSUs |
| DC output: | 5V DC @ 3A, 12V DC @ 54A |
| Power input option: | 48V DC, 100V to 240V AC |
| Max power: | 650W, without pluggable optics |

# NPB II HW Specifications

## Ports

| | |
|---|---|
| Switch ports: | 32 x QSFP28 ports<br>Each port supports 1x10/40/100 GbE or 4 x 10/25 GbE per port using splitter cables. |
| Management ports: | 1 x RJ-45 serial console |
| | 1 x RJ-45 100/1000BASE-T management |
| | 1 x USB Type A storage |

## Physical and Environmental

| | |
|---|---|
| Dimensions (WxDxH): | 43.8 x 51.5 x 4.35 cm (17.3 x 20.3 x 1.7 in) |
| Weight: | 10 kg (23 lb), with two installed PSU modules |
| Fans: | Hot-swappable 4+1 redundant fans |
| Operating temperature: | 0°C to 45°C (32°F to 113°F) |
| Storage temperature: | -40°C to 70°C (-40°F to 158°F) |
| Operating humidity: | 5% to 95% non-condensing |
| Operating altitude: | 0 to 10,000 feet |

## LEDs

| | |
|---|---|
| QSFP 28 Port LEDs: | Link Status, Activity, Rate |
| Ethernet Management Port LED: | Link Status, Activity |
| Console Port LED: | Link Status |
| System LEDs: | Diagnostic, Locator, PSU and Fan Status |

## Power

| | |
|---|---|
| PSUs: | 2 redundant, load-sharing, hot-swappable AC or -48V DC |
| Input voltage: | 90V to 240V AC at 50-60 Hz. -36V to -72V DC |
| Input current: | Max 6 A@100/120V AC, 3 A@ 200/240V AC,10 A@ -72V DC |
| PSU efficiency: | Up to 93% for AC PSUs |
| Power input option: | 12V DC |
| Max power: | 350W, without pluggable optics |
| Typical power: | 310W, without pluggable optics |

# NPB IIe HW Specifications

## Ports

| | |
|---|---|
| Switch ports: | 32 x QSFP28 ports<br>Each port supports 1x10/40/100 GbE or 4 x 10/25 GbE or 2x 50 GbE per port using splitter cables. |
| Management ports: | 1 x RJ-45 serial console |
| | 1 x RJ-45 100/1000BASE-T management |
| | 1 x USB Type A storage |

## Physical and Environmental

| | |
|---|---|
| Dimensions (WxDxH): | 44.25 x 47.3 x 4.39 cm (17.42 x 18.62 x 1.73 in) |
| Weight: | 10.87 kg (23.96 lb), with two installed PSU modules |
| Fans: | Hot-swappable 4+1 redundant fans |
| Operating temperature: | 0°C to 45°C (32°F to 113°F) |
| Storage temperature: | -40°C to 70°C (-40°F to 158°F) |
| Operating humidity: | 5% to 95% non-condensing |
| Operating altitude: | 0 to 10,000 feet |

## LEDs

| | |
|---|---|
| QSFP 28 Port LEDs: | Link Status, Activity, Rate |
| Ethernet Management Port LED: | Link Status, Activity |
| Console Port LED: | Link Status |
| System LEDs: | Diagnostic, Locator, PSU and Fan Status |

## Power

| | |
|---|---|
| PSUs: | 2 redundant, load-sharing, hot-swappable AC or -48V DC |
| Input voltage: | 100V ~240V AC. -36V ~-72V DC |

# NPB III HW Specifications

## Ports

| | |
|---|---|
| Switch ports: | 32 x QSFP-DD ports<br>Each port supports 1x10/25/40/50/200/100/400 GbE<br>or 4 x 10/25/50/100 GbE per port using splitter cables. |
| Management ports: | 1 x RJ-45 serial console |
| | 1 x RJ-45 1000BASE-T management |
| | 1 x USB Type A storage |

## Physical and Environmental

| | |
|---|---|
| Dimensions (WxDxH): | 43.84 x 53.6 x 4.31 cm (17.25 x 21.1 x 1.69 in) |
| Weight: | 11.06 kg (24.38 lb), with two installed PSU modules |
| Fans: | Hot-swappable 5 + 1 redundant fans |
| Operating temperature: | 0°C to 45°C (32°F to 113°F) |
| Storage temperature: | -40°C to 70°C (-40°F to 158°F) |
| Operating humidity: | 5% to 95% non-condensing |

## LEDs

| | |
|---|---|
| QSFP DD Port LEDs: | Link Status, Activity, Rate |
| Ethernet Management Port LED: | Link Status, Activity |
| System LEDs: | Diagnostic, Locator, PSU and Fan Status |

## Power

| | |
|---|---|
| PSUs: | 2 redundant, load-sharing, hot-swappable AC or -48V DC |
| Input voltage: | 100V ~240V AC. -36V ~-72V DC |

# NPB IV HW Specifications

## Ports

| | |
|---|---|
| Switch ports: | 40 x QSFP28 ports<br>Each port supports 1x40/100 GbE.<br>First 20 ports support 4 x 10/25 GbE. (In this case, ports 21-40 are non-active.) |
| Management ports: | 1 x RJ-45 serial console |
| | 1 x RJ-45 1000BASE-T management |
| | 1 x USB Type A storage |

## Physical and Environmental

| | |
|---|---|
| Dimensions (WxDxH): | 43.6 x 76.2 x 8.76 cm (17.17 x 30 x 3.45 in) |
| Weight: | 26.7 kg (58.9 lbs.) |
| Fans: | Hot-swappable 3 + 1 redundant fans |
| Operating temperature: | 0°C to 45°C (32°F to 113°F) |
| Storage temperature: | -40°C to 70°C (-40°F to 158°F) |
| Operating humidity: | 5% to 85% non-condensing |

## LEDs

| | |
|---|---|
| QSFP DD Port LEDs: | Link Status, Activity, Rate |
| Ethernet Management Port LED: | Link Status, Activity |
| System LEDs: | Power, system status, fan status, PSU status |

## Power

| | |
|---|---|
| PSUs: | Hot swappable, 1+1 redundant PSU |
| Input voltage: | 200V ~ 240V, 12.5A, 50Hz ~ 60Hz AC. -40V ~ -72V, 60A ~ 33A DC.<br>Typical power: 750 Watts (no transceiver) |

# Appendix 2 – Recovery

The NPB device constantly monitors the status of its SW components. In the very rare occasion that a severe error condition is detected, the built-in recovery mechanism is activated.

The goal of the recovery mechanism is the following:

- Allow the user to take action to resolve the error condition when possible
- Apply pre-defined logic to resolve the error condition when user intervention is not possible
- Protect the user data and configuration
- Notify the user that a severe error occurred, by sending an SNMP trap
- Collect logs and other information to allow CGS support to perform a root cause analysis for the issue

There are two types of recovery modes: manual and automatic.

## Manual Recovery

In this state, user intervention is possible through a set of CLI commands.

The user can do any of the following:

- Validate the images in the boot banks
- Upload new firmware
- Change the boot bank
- Back up the configuration and database
- Delete the current configuration and database
- Reset to factory defaults
- Reboot

**Note:**

Operational CLI commands are blocked at this state until the recovery is resolved.

The CLI commands syntax is as follows:

```
NPB# recovery
Possible completions:
  bank              Bank images operations
  database          Configuration database operations
  factory-default   Restore factory default
  mgmt-port-info    Get management port information
  reboot            System reboot
NPB# recovery bank
Possible completions:
  get-current-boot    Get the current boot bank
  get-next-boot       Get the next boot bank
  load-image          Load image to boot bank
  set-next-boot       Set boot bank
  validation-boot     Validate boot bank status
  validation-second   Validate second bank status
```

```
NPB# recovery database
Possible completions:
  backup   Backup configuration database
  delete   Delete configuration database
```

## Automatic Recovery

In this state, the system is in a position where a severe error was detected and no user intervention is possible. In this case, an automatic procedure is activated.

The automatic procedure runs the following steps. After each step, a test is performed to check whether the error condition was resolved.

1. Reboot the device.
2. Switch boot-bank and reboot again.
3. Delete the current database and reboot again.
4. Return the device to factory defaults and reboot again.

After the system is recovered, it is recommended to check the Syslog file to review the changes done by the Automatic Recovery mechanism. The System will present a special recovery banner at this stage.

To mark that the system is recovered and to return to the normal banner, use the following command from the CLI:

```
NPB # system system-recovery-solved
Have you solved the system recovery issue? [yes,NO] yes
```

# Appendix 3 – Port Counters

This section describes the ports statistics counters supported by the device.

Refer to Section Port Statistics on p.99 on how to display and clear statistics.

## Summary

| Counter Name | Description | Source |
|---|---|---|
| RX Bytes | The total number of octets received on the port, including framing characters | RFC 1213 |
| RX Packets | The number of packets received on the port | RFC 1213 |
| RX Discard Packets | The number of inbound packets which were chosen to be discarded even though no errors had been detected. | RFC 1213 |
| RX % Util | Current received bandwidth as percentage of the maximal port's bandwidth | CGS |
| TX Bytes | The total number of octets transmitted out on the port, including framing characters | RFC 1213 |
| TX Packets | The number of packets transmitted out on the port | RFC 1213 |
| TX Discard Packets | The number of outbound packets which were chosen to be discarded even though no errors had been detected | RFC 1213 |
| TX % Util | Current transmitted bandwidth as percentage of the maximal port's bandwidth | CGS |

## Utilization

| Counter Name | Description | Source |
|---|---|---|
| RX AVG 5 Min | Average received throughput in Mbps during the last 5 minutes | CGS |
| RX % 5 Min | Average received throughput during the last 5 minutes expressed as a percentage of the maximal port's capacity | CGS |
| RX Mbps | Current received throughput in Mbps | CGS |
| RX % | Current received throughput expressed as a percentage of the maximal port's capacity | CGS |
| RX Peak | Peak received throughput in Mbps since last statistics clearance | CGS |
| RX % Peak | Peak received throughput since last statistics clearance expressed as a percentage of the maximal port's capacity | CGS |
| RX % Thresholds | Received utilization alarm thresholds (Up and Down) expressed as a percentage of the maximal port's capacity | CGS |

| Counter Name | Description | Source |
|---|---|---|
| RX Alarm | Current received alarm status | CGS |
| TX AVG 5 Min | Average transmitted throughput in Mbps during the last 5 minutes | CGS |
| TX % 5 Min | Average transmitted throughput during the last 5 minutes expressed as a percentage of the maximal port's capacity | CGS |
| TX Mbps | Current transmitted throughput in Mbps | CGS |
| TX % | Current transmitted throughput expressed as a percentage of the maximal port's capacity | CGS |
| TX Peak | Peak transmitted throughput in Mbps since last statistics clearance | CGS |
| TX % Peak | Peak transmitted throughput since last statistics clearance expressed as a percentage of the maximal port's capacity | CGS |
| TX % Thresholds | Transmit utilization alarm thresholds (Up and Down) expressed as a percentage of the maximal port's capacity | CGS |
| TX Alarm | Current transmit alarm status | CGS |

## Packet Sizes

| Counter Name | Description | Source |
|---|---|---|
| Undersized Packets | The number of packets received that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed | RFC 1757 |
| RX 64 Bytes | The total number of packets received that were 64 octets in length | RFC 1757 |
| TX 64 Bytes | The total number of packets transmitted that were 64 octets in length | RFC 1757 |
| RX 65 to 127 Bytes | The total number of packets received that were between 65 and 127 octets in length inclusive | RFC 1757 |
| TX 65 to 127 Bytes | The total number of packets transmitted that were between 65 and 127 octets in length inclusive | RFC 1757 |
| RX 128 to 255 Bytes | The total number of packets received that were between 128 and 255 octets in length inclusive | RFC 1757 |
| TX 128 to 255 Bytes | The total number of packets transmitted that were between 128 and 255 octets in length inclusive | RFC 1757 |

| Counter Name | Description | Source |
|---|---|---|
| RX 256 to 511 Bytes | The total number of packets received that were between 256 and 511 octets in length inclusive | RFC 1757 |
| TX 256 to 511 Bytes | The total number of packets transmitted that were between 256 and 511 octets in length inclusive | RFC 1757 |
| RX 512 to 1023 Bytes | The total number of packets received that were between 512 and 1023 octets in length inclusive | RFC 1757 |
| TX 512 to 1023 Bytes | The total number of packets transmitted that were between 512 and 1023 octets in length inclusive | RFC 1757 |
| RX 1024 to 1518 Bytes | The total number of packets received that were between 1024 and 1518 octets in length inclusive | RFC 1757 |
| TX 1024 to 1518 Bytes | The total number of packets transmitted that were between 1024 and 1518 octets in length inclusive | RFC 1757 |
| RX 1519 to 2047 Bytes | The total number of packets received that were between 1519 and 2047 octets in length inclusive | RFC 1757 |
| TX 1519 to 2047 Bytes | The total number of packets transmitted that were between 1519 and 2047 octets in length inclusive | RFC 1757 |
| RX 2048 to 4095 Bytes | The total number of packets received that were between 2048 and 4095 octets in length inclusive | RFC 1757 |
| TX 2048 to 4095 Bytes | The total number of packets transmitted that were between 2048 and 4095 octets in length inclusive | RFC 1757 |
| RX 4096 to 9216 Bytes | The total number of packets received that were between 4096 and 9216 octets in length inclusive | RFC 1757 |
| TX 4096 to 9216 Bytes | The total number of packets transmitted that were between 4096 and 9216 octets in length inclusive | RFC 1757 |
| RX 9217 to 16830 Bytes | The total number of packets received that were between 9217 and 16830 octets in length inclusive | RFC 1757 |
| TX 9217 to 16830 Bytes | The total number of packets transmitted that were between 9217 and 16830 octets in length inclusive | RFC 1757 |
| RX Oversized (Over MTU) | The total number of packets received that were longer than 1518 octets | RFC 1757 |
| TX Oversized (Over MTU) | The total number of packets transmitted that were longer than 1518 octets | RFC 1757 |

## Traffic Types

| Counter Name | Description | Source |
|---|---|---|
| Unknown Protocol | The number of packets received via the port with unknown or unsupported protocol | RFC 1213 |
| RX Unicast | The number of unicast packets received via the port | RFC 2233 |
| TX Unicast | The number of unicast packets transmitted via the port | RFC 2233 |
| RX Broadcast | The number of broadcast packets received via the port | RFC 2233 |
| TX Broadcast | The number of broadcast packets transmitted via the port | RFC 2233 |
| RX Multicast | The number of multicast packets received via the port | RFC 2233 |
| TX Multicast | The number of multicast packets transmitted via the port | RFC 2233 |

## Actions

| Counter Name | Description | Source |
|---|---|---|
| MPLS Remove | The number of packets received via the port that underwent MPLS removal | CGS |
| Slice | The number of packets transmitted via the port that were sliced | CGS |

## Errors

| Counter Name | Description | Source |
|---|---|---|
| RX Error Packets | The number of inbound packets that contained errors preventing them from being deliverable into the device | RFC 1213 |
| RX Fragments | The number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error) | RFC 1757 |
| RX Jabber | The number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error) | RFC 1757 |
| TX Error Packets | The number of outbound packets that could not be transmitted because of errors | RFC 1213 |

| Counter Name | Description | Source |
|---|---|---|
| RX Drop Events | The number of events in which packets were dropped by the device due to lack of resources<br>Note that this number is not necessarily the number of packets dropped. It is just the number of times this condition has been detected. | RFC 1757 |
| RX IP Errors | The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc. | RFC 1213 |
| Collisions | The best estimate of the total number of collisions on this interface | RFC 1757 |
| Late Collisions | The number of times that a collision is detected on the interface later than one slotTime into the transmission of a packet | RFC 2665 |
| Alignment Errors | The number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error) | RFC 1757 |
| RX MAC Errors | A count of frames for which reception on the interface failed due to an internal MAC sublayer receive error | RFC 2665 |
| Carrier Sense Errors | The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on the interface | RFC 2665 |
| Symbol Errors | • For an interface operating in half-duplex mode at 1000 Mb/s: the number of times the receiving media was non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that caused the PHY to indicate a Data Reception error or a Carrier Extend error on the GMII<br>• For an interface operating in full-duplex mode at 1000 Mb/s: the number of times the receiving media was non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that caused the PHY to indicate a Data Reception error on the GMII | RFC 2665 |

| Counter Name | Description | Source |
|---|---|---|
| Deferred Collisions | A count of frames for which the first transmission attempt on the interface was delayed because the medium was busy. This counter does not increment when the interface is operating in full-duplex mode. | RFC 2665 |
| Excessive Collisions | A count of frames for which transmission on the interface failed due to excessive collisions.<br>This counter does not increment when the interface is operating in full-duplex mode. | RFC 2665 |
| FCS Errors | A count of frames received on the interface that were an integral number of octets in length but did not pass the FCS check | RFC 2665 |
| TX MAC Erros | A count of frames for which transmission on the interface failed due to an internal MAC sublayer transmit error | RFC 2665 |
| Frame Too Long | A count of frames received on the interface that exceeded the maximum permitted frame size | RFC 2665 |
| Unknown OpCode | A count of MAC Control frames received on this interface that contained an opcode that is not supported by this device | RFC 2665 |

## PRBS

| Counter Name | Description | Source |
|---|---|---|
| Error bit total | The number of bit errors detected | CGS |
| Error bit rate | The number of bit errors detected out of the total number of bits sent, measured in $10^{-9}$ units | CGS |
| Run time | PRBS test duration time | CGS |
| Last lost time | Timestamp of the last lost synchronization event | CGS |
| Last error time | Timestamp of last error event | CGS |

## FEC

| Counter Name | Description | Source |
|---|---|---|
| FEC corrected | The number of FEC detected and corrected by the system | CGS |
| FEC uncorrected | The number of FEC detected but not corrected by the system | CGS |

## Queues

| Counter Name | Description | Source |
|---|---|---|
| Max memory | The maximal Tx buffer memory that can be assigned to the port | CGS |
| Memory usage | Current Tx buffer memory assigned to the port | CGS |
| Max BD | The maximal number of buffer descriptors that can be assigned to the port | CGS |
| BD usage | Current number of buffer descriptors assigned to the port | CGS |

# Appendix 4 – NETCONF

NETCONF (Network Configuration Protocol) provides a standard scripting mechanism to maintain and configure network devices. The NPB fully supports NETCONF as a management interface. This appendix provides a general introduction for working with NETCONF and a set of examples to be used as a reference.

## Introduction

To use NETCONF to manage the NPB device, some understanding of the underlying configuration schema is required. The NPB uses a single YANG schema for all its management interfaces (CLI, SNMP, NETCONF, RESTCONF, and WebUI), so usually the first step when constructing a NETCONF request is to be familiar with the equivalent CLI command.

There are two standard ways to communicate with the NPB using NETCONF: the first is by a NETCONF client, for example **`network-console`** (https://pypi.org/project/netconf-console), the second is by sending NETCONF data directly to the NETCONF port.

This document uses **`network-console`**, but all the examples can be used directly by using a single file as explained below.

To enable NETCONF on the device, see Section Working with NETCONF on p.50.

Once enabled, a simple connectivity test can be done by using the following command:

```
netconf-console -u <user> -p <password> --host=<host-ip> –hello
```

On successful activation, this command returns the device's capabilities.

**Note:**
For brevity, in the rest of this document, the `user`, `password` and `host` options are omitted.

NETCONF can be used for the following operations:

1. Retrieve the device's schema
2. Read data from the device
3. Configure the data
4. Run actions on the device

## Retrieving the Device's Schema

To construct a NETCONF request, some knowledge of the device management schema is required. The preferred way is to use the CLI syntax as a reference, but in some cases, a deeper understanding is needed. In these cases, the device's schema can be fetched from the device.

The schema is constructed from modules and submodules. To get the list of modules, use the following command:

```
netconf-console --get -x /modules-state
```

To get a schema of a specific module or submodule, use the following command:

```
netconf-console --get-schema=<module-or-submdl–name>
```

For example, use the following command to get all modules and submodules related to ports:

```
netconf-console --get -x /modules-state | grep ports
```

The result starts with the following lines. The ports main module is **`nb-ports.`** Its submodules are listed below it:

```
<name>npb-ports</name>
<namespace>http://npb.com/npb/npb-ports</namespace>
  <name>npb-ports-breakout-submdl</name>
  <name>npb-ports-common-p-submdl</name>
  <name>npb-ports-common-submdl</name>
```

## Reading Data

The device data can be divided into configured data and non-configured data.

- Configured data is data entered by the user as part of the device configuration, for example, filters, load balance groups and interfaces.
- Non-configured data is data provided by the device without being configured first by the user, for example, statistics, alarms and PSU status.

To read only configured data, use the following command:

```
netconf-console --get-config -x <XPATH>
```

To read configured and non-configured data, use the following command:

```
netconf-console --get -x <XPATH>
```

where XPATH is a valid XML path for the relevant element. As explained above, the XPATH can be deduced from the CLI syntax or by looking in the schema.

### Examples

Example 1: Reading the ports configured data

CLI syntax: `show ports, show running-config ports`

```
netconf-console --get-config -x /ports
```

Example 1.1: Reading Port 1 configured data

```
netconf-console --get-config -x /ports/port[1]
```

Example 1.2: Reading Port 1 admin status

```
netconf-console --get-config -x /ports/port[1]/admin
```

Example 1.3: Reading admin status for all ports:

```
netconf-console --get-config -x /ports/port/admin
```

Example 2: Reading the ports statistics

CLI syntax: `show port-statistics`

```
netconf-console --get -x /port-statistics
```

Example 2.1: Reading the summary statistics table

CLI syntax: `show port-statistics summary`

```
netconf-console --get -x /port-statistics/summary
```

Example 2.2: Reading the summary statistics table for Port 1

CLI syntax: `show port-statistics summary port 1`

```
netconf-console --get -x /port-statistics/summary/port[1]
```

Example 2.3: Reading the rx-octet value of the summary statistics table for Port 1

```
netconf-console –get -x /port-statistics/summary/port[1]/rx-octets
```

Example 2.4: Reading the rx-octet value of the summary statistics table for all ports

```
netconf-console --get -x /port-statistics/summary/port/rx-octets
```

## Configuring the Device

To configure the device, use the **`--edit-config`** command, which receives an XML file as its input. The XML syntax is defined in the NETCONF RFC. **`--edit-config`** automatically commits the changes before returning.

The **`--edit-config`** command syntax is as follows:

```
netconf-console --edit-config=<path-to-xml-file>
```

## Examples

Example 3: Creating a filter

CLI syntax:

```
filters groups group filters filter MY-FILTER input-ports 2 output-
ports 3 action redirect ; commit
```

NETCONF command:

```
netconf-console --edit-config=create-filter.xml
```

File content:

```
<filters xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://npb.com/npb/npb-filters">
   <groups>
         <group>
               <name>filters</name>
               <filter nc:operation="create">
                     <name>MY-FILTER</name>
                     <input-ports>2</input-ports>
                     <output-ports>3</output-ports>
                     <action>redirect</action>
               </filter>
         </group>
   </groups>
</filters>
```

Example 3.1: Disabling a filter's admin state

CLI syntax:

```
filters groups group filters filter MY-FILTER admin disable ; commit
```

NETCONF command:

```
netconf-console --edit-config=edit-filter.xml
```

File content:

```
<filters xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://npb.com/npb/npb-filters">
      <groups>
            <group>
                  <name>filters</name>
                  <filter>
                        <name>MY-FILTER</name>
                        <admin>disable</admin>
                  </filter>
            </group>
      </groups>
</filters>
```

Example 3.2: Deleting a filter

CLI syntax:

```
no filters groups group filters filter MY-FILTER ; commit
```

NETCONF command:

```
netconf-console --edit-config=delete-filter.xml
```

File content:

```
<filters xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns="http://npb.com/npb/npb-filters">
      <groups>
            <group>
                  <name>filters</name>
                  <filter nc:operation="delete">
                        <name> MY-FILTER</name>
                  </filter>
            </group>
      </groups>
</filters>
```

## Running Actions

To run actions on the device, use the **`--rpc`** command, which receives an XML file as its input. The XML syntax is defined in the NETCONF RFC. Actions that modify the database commit the changes automatically before returning. However, commit failures are not reflected to the caller. Therefore, it is recommended to read the database to verify the changes were committed successfully.

The **`rpc`** command syntax is as follows:

```
netconf-console --rpc=<path-to-xml-file>
```

To understand if an operation is an action, start with checking the CLI syntax. If it does not require a `commit`, then it is an action. Some actions however change the database and do require a `commit`. To identify this case, examine the schema. Actions names are prefixed with `action` or `tailf:action`.

For example, the CLI command `port-statistics clear` is an action as it does not require a `commit`. On the other hand, `filters ip-list import` is an action that changes the database and therefore does require a `commit`. To verify this, the schema can be examined as follows:

```
netconf-console --get -x /modules-state | grep filters

        <name>npb-filters</name>
        <namespace>http://npb.com/npb/npb-filters</namespace>
          <name>npb-filters-actions-submdl</name>
          <name>npb-filters-bcmbased-submdl</name>

netconf-console --get-schema=npb-filters | grep import | grep action
```

The result is:

```
tailf:action import {
```

Searching the schema for **`ip-list`** returns the following result:

```
tailf:action import {
            tailf:info "Import ip-list file from remote server";
```

### Examples

Example 5: Calling the filters Clear Statistics action

CLI syntax:

```
filters clear-statistics
```

NETCONF command:

```
netconf-console --rpc=clear-filter-stats.xml
```

File content:

```
<action xmlns="http://tail-f.com/ns/netconf/actions/1.0">
   <data>
         <filters xmlns="http://npb.com/npb/npb-filters">
               <clear-statistics></clear-statistics>
         </filters>
   </data>
</action>
```

## Using a Single File

It is possible to combine several actions in a single XML file and give it as a parameter to **`netconf-console`** using the following syntax:

```
netconf-console <xml-file>
```

### Examples

Example 6: Creating a load balancing group and 2 filters in a single file

NETCONF command:

```
netconf-console setup-create.xml
```

File content:

```
<?xml version="1.0" encoding="UTF-8"?>
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <capabilities>
         <capability>urn:ietf:params:netconf:base:1.0</capability>
   </capabilities>
</hello>
]]>]]>
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="1" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <edit-config xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
            <target>
                  <running/>
            </target>
            <config>
                  <lb xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
                  xmlns="http://npb.com/npb/npb-lb">
                        <group nc:operation="create">
                              <lb-id>10</lb-id>
                              <outputs>1,2</outputs>
                              <hash>ip-addr</hash>
                              <name>MY-LBG</name>
                        </group>
                  </lb>
                  <filters
                  xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0"
                  xmlns="http://npb.com/npb/npb-filters">
                        <groups>
                              <group>
                                    <name>filters</name>
                                    <filter nc:operation="create">
                                          <name>MY-FILTER1</name>
                                          <action>redirect</action>
                                          <input-ports>2</input-ports>
                                          <output-ports>1</output-ports>
                                    </filter>
                                    <filter nc:operation="create">
                                          <name>MY-FILTER2</name>
                                          <action>redirect</action>
                                          <input-ports>4</input-ports>
                                          <output-ports>3</output-ports>
                                    </filter>
                              </group>
                        </groups>
                  </filters>
            </config>
      </edit-config>
</rpc>
]]>]]>
<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="2" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <close-session/>
</rpc>
```

15 HaMelacha st. ▌ Rosh Haayin, Israel, 4809136
**Tel/Fax:** +972-3-6166026 ▌ **Email**: info@cgstowernetworks.com
www.cgstowernetworks.com