PROFITAP

XX series

XX-1800G rev. 2

XX-3200G rev. 2

NETWORK PACKET BROKERS

USER MANUAL

XX-Series rev. 2 software version: v1.2.0

If you have any questions, visit our Knowledge Base:

https://kb.profitap.com/

You can also contact us through our website:

https://www.profitap.com/contact-us/

Or directly by email:

support@profitap.com

For the latest documentation and software, visit our Resource Center:

https://resources.profitap.com/

TABLE OF CONTENTS

1. Overview **5**
1.1. Hardware Overview 5
1.1.1. XX-1800G rev. 2 5
1.1.2. XX-3200G rev. 2 5
1.2. Supported Cables and Transceivers 6
1.3. XX-1800G rev. 2 7
1.3.1. Package Contents 7
1.3.2. Installation as Standalone 7
1.3.3. Installation in a Rack 7
1.3.4. Technical and Electrical Specifications 7
1.3.5. Front View 8
1.3.6. Rear View 8
1.3.7. LED Functionality 9
1.4. XX-3200G rev. 2 11
1.4.1. Package Contents 11
1.4.2. Installation as Standalone 11
1.4.3. Installation in a Rack 11
1.4.4. Technical and Electrical Specifications 11
1.4.5. Front View 12
1.4.6. Rear View 12
1.4.7. LED Functionality 13
2. Connecting Power and Start-Up **15**
3. Initial Access **16**
3.1. Configuring the Ethernet Management Port 16
4. Web Administration **17**
4.1. Device Status 17
4.2. Port Management 18
4.3. Statistics 18
4.4. Traffic Management 19
4.4.1. Rule - Interfaces 19
4.4.2. Rule - Filters 20
4.4.3. Load Balancing Groups 20
4.4.4. Ingress Rules 20
4.5. Authentication 21
4.5.1. Users 21
4.5.2. TACACS+ 21
4.5.3. RADIUS 21
4.5.4. LDAP and LDAPS 22
4.5.5. Profitap Supervisor 22
4.5.6. Custom Authentication Configuration 23
4.6. Administration 23
4.6.1. Setup 23
4.6.2. Firmware 23
4.6.3. SNMP 24
4.6.4. Firewall 24
4.6.5. Logs 24
4.6.6. Support 24
5. Command Line Reference **25**
5.1. Configuration 25
5.2. Statistics 27

5.3. Status 27
5.4. System 28
6. Integrations **50**
6.1. RESTful API Support 50
6.2. Ansible Support 50
Legal **51**
Disclaimer 51
Copyright 51
Trademarks 51

1. Overview

1.1. Hardware Overview

1.1.1. XX-1800G rev. 2

XX-1800G is supplied with either 24 x 1/10/25G + 2 x 40/100G or 48 x 1/10/25G + 6 x 40/100G enabled ports, depending on the license:

- **XX-1800G-242-AC**: 24 x 1/10/25G SFP28, 2 x 40/100G QSFP28, 2 x AC PSUs
- **XX-1800G-486-AC**: 48 x 1/10/25G SFP28, 6 x 40/100G QSFP28, 2 x AC PSUs
- **XX-1800G-242-DC**: 24 x 1/10/25G SFP28, 2 x 40/100G QSFP28, 2 x DC PSUs
- **XX-1800G-486-DC**: 48 x 1/10/25G SFP28, 6 x 40/100G QSFP28, 2 x DC PSUs

The unit features the following ports:

- 48 x 1/10/25G SFP28 and 6 x 40/100G QSFP28 ports supporting optical transceivers, active optical cables or DAC cables to connect the ports to the hosts
- 1 x RJ45 Ethernet management port
- 1 x RJ45 serial management port to connect to a PC for the initial configuration
- 1 x USB port to load the configuration files or OS from a USB storage device

QSFP28 ports 53 and 54 support 4 x 10G and 4 x 25G splits via fanout cables.

1.1.2. XX-3200G rev. 2

XX-3200G is supplied with either 16 x 40/100G or 32 x 40/100G enabled ports, depending on the license:

- **XX-3200G-16-AC**: 16 x 40/100G QSFP28, 2 x AC PSUs
- **XX-3200G-32-AC**: 32 x 40/100G QSFP28, 2 x AC PSUs
- **XX-3200G-16-DC**: 16 x 40/100G QSFP28, 2 x DC PSUs
- **XX-3200G-32-DC**: 32 x 40/100G QSFP28, 2 x DC PSUs

The unit features the following ports:

- 32 x 40/100G QSFP28 ports supporting optical transceivers, active optical cables or DAC cables to connect the ports to the hosts
- 1 x 10G SFP+ management port
- 1 x RJ45 100/1000BASE-T management port
- 1 x RJ45 serial management port to connect to a PC for the initial configuration
- 1 x USB 3.0 Type A port to load the configuration files or OS from a USB storage device

QSFP28 ports support 4 x 10G and 4 x 25G splits via fanout cables, except port 32.

1.2. Supported Cables and Transceivers

Profitap XX-Series devices are not vendor locked to any specific brand of QSFP or SFP modules and cables. For optimal support, Profitap transceivers are recommended.

	XX-1800G rev. 2	XX-3200G rev. 2
1000BASE-T SFP Module	✔	
1000BASE-SX SFP Module	✔	
1000BASE-LX/LH SFP Module	✔	
10G SFP+ Direct Attach Cable	✔	
10G SFP+ Active Optical Cable	✔	
10GBASE-T SFP+ Module	✔	
10GBASE-SR SFP+ Module	✔	
10GBASE-LR SFP+ Module	✔	
25G SFP28 Direct Attach Cable	✔	
25G SFP28 Active Optical Cable	✔	
25GBASE-SR SFP28 Module	✔	
40G QSFP+ Direct Attach Cable	✔	✔
40G QSFP+ Active Optical Cable	✔	✔
40GBASE-SR4 QSFP+ Module	✔	✔
40GBASE-LR4 QSFP+ Module	✔	✔
40GBASE-PLR4 QSFP+ Module	✔	✔
40GBASE-SR-BD QSFP+ Module	✔	✔
40GBASE-SR-BD Rx only QSFP+ Module	✔	✔
100G QSFP28 Direct Attach Cable	✔	✔
100G QSFP28 Active Optical Cable	✔	✔
100GBASE-SR4 QSFP28 Module	✔	✔
100GBASE-LR4 QSFP28 Module	✔	✔
100GBASE-SR-BD QSFP28 Module	✔	✔
100GBASE-SR-BD Rx only QSFP28 Module	✔	✔

1.3. XX-1800G rev. 2

1.3.1. Package Contents

Carefully unpack all the supplied items and retain the packaging for later use.

- 1 x XX-1800G main unit
- 2 x C13 AC power cord
- 1 x USB 3.0 cable
- 1 x RJ45 female to 9-pin serial adapter
- 1 x rack mounting kit (brackets, adjustable mounting rail kit, screws, grounding kit)

Note: Please contact the supplier if any part is missing or damaged.

1.3.2. Installation as Standalone

The unit can be installed as a standalone unit.

To ensure proper heat dissipation and ventilation, leave at least 15 cm (6 inches) of space behind the unit and 5 cm (2 inches) in front.

1.3.3. Installation in a Rack

The unit can be mounted in a standard 19'' (1U) rack using the provided mounting brackets.

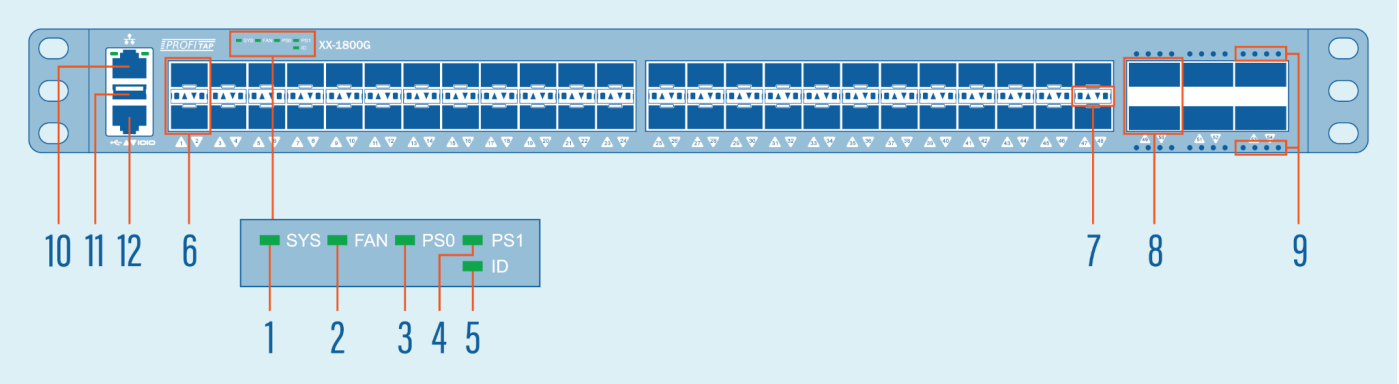
1. Slide the main chassis into the desired rack location.
2. Secure the chassis using the supplied screws.
3. Make sure the rack is grounded properly.

To install the switch without a shelf, use the included rack mount kit.

1.3.4. Technical and Electrical Specifications

- 1.6 GHz quad-core CPU
- 2.0 Tbps ASIC
- AC Model: 2 x 450 W, 100–240 VAC, 50–60 Hz, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy)
- DC Model: 2 x 450 W, -40–-60 VDC power supply (1 required for operation, 2 for redundancy)
- Typical/Max power draw: 108/380 W
- Cooling: 5 redundant (N+1) hot-swappable fans
- Operating temperature: 0°C to 45°C — 32°F to 113°F
- Operating humidity: 20% to 95%, non-condensing
- Non-operating/Storage temperature: -40 °C to 70 °C
- Non-operating/Storage relative humidity: 10% to 95%, non-condensing
- Dimensions (WxDxH): 440 x 440 x 44 mm — 17.32 x 17.32 x 1.73 in
- MTBF: 215,658 hours
- MTTR: 20 hours

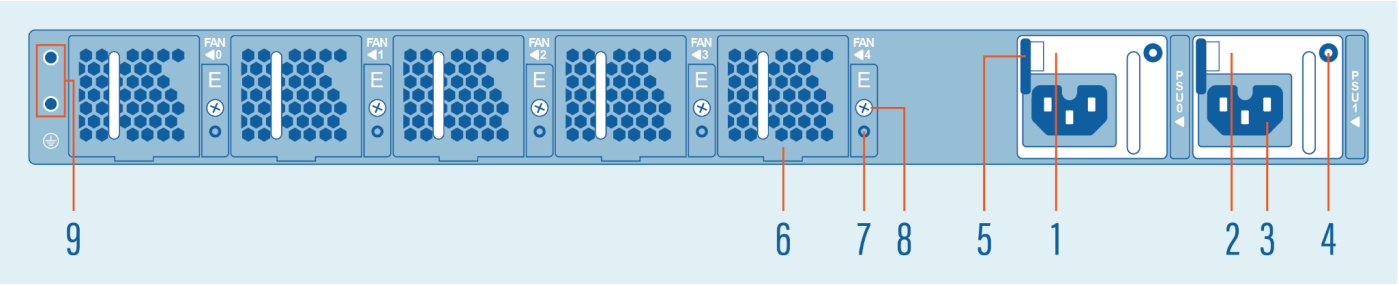
1.3.5. Front View



1	System status LED	7	SFP28 port activity LEDs
2	Fan status LED	8	40/100G QSFP28 ports (49–54)*
3	PSU0 status LED	9	QSFP28 port activity LEDs
4	PSU1 status LED	10	Ethernet management port
5	ID LED	11	USB port
6	1/10/25G SFP28 ports (1–48)	12	Serial management port

* 4x10G and 4x25G splits supported on ports 53–54.

1.3.6. Rear View



1	PSU0	6	Hot-swappable fan module
2	PSU1	7	Fan status LED
3	AC power connector	8	Fan module captive thumbscrew
4	PSU status LED	9	Grounding lug M4 screw holes
5	PSU release latch		

1.3.7. LED Functionality

LED Function	LED State	Description
PS0/PS1 status LED	Off	Power is not supplied to the PSU
	Green	PSU is operating normally
	Amber	PSU fault
PSU module LED	Off	No power input
	Green	Output ON and OK
	Blinking green (1/s)	PSU standby state input power present / Only +5VSB on.
	Blinking green (2/s)	Power supply firmware updating (bootloader mode).
	Red	Power supply critical event causing a shutdown, failure, over current, short circuit, over voltage, fan failure, and/or over temperature.
	Blinking red	DC power cord unplugged or DC power lost with a second power supply in parallel still with DC input power. Power supply DC present, 5VSB and 12V off via on/off control from system.
	Blinking green+red	Power supply warning events where the power supply continues to operate; high temp, high power, high current, and/or slow fan.
Fan status LED	Off	Fans are not initialized
	Green	Fans operating normally
	Amber	Fan fault: check rear of unit to see which fan is faulty
Fan module LED	Off	No input power
	Green	Fan operating normally
	Amber	Fan fault
System status LED	Off	No power
	Green	System operating normally
	Amber	Power is up but host CPU boot failed
SFP28 port LED	Off	No link
	Green	25G link

	Blinking green	25G activity
	Amber	10G link
	Blinking amber	10G activity
QSFP28 port LED	Off	No link
	Green	100G link
	Blinking green	100G activity
	Yellow	40G link
	Blinking yellow	40G activity

1.4. XX-3200G rev. 2

1.4.1. Package Contents

Carefully unpack all the supplied items and retain the packaging for later use.

- 1 x XX-3200G main unit
- 2 x C13 AC power cord
- 1 x RJ45 female to 9-pin serial adapter
- 1 x USB 3.0 cable
- 1 x rack mounting kit (brackets, screws, rail kit)
- 1 x grounding kit (ground lug, screws)

Note: Please contact the supplier if any part is missing or damaged.

1.4.2. Installation as Standalone

The unit can be installed as a standalone unit.

To ensure proper heat dissipation and ventilation, leave at least 15 cm (6 inches) of space behind the unit and 5 cm (2 inches) in front.

1.4.3. Installation in a Rack

The unit can be mounted in a standard 19’’ (1U) rack using the provided mounting brackets.

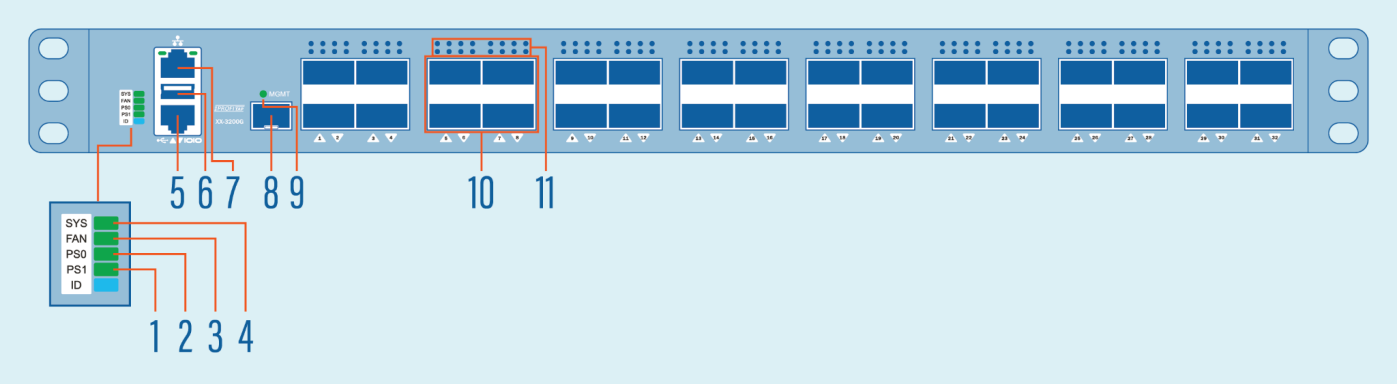
1. Slide the main chassis into the desired rack location.
2. Secure the chassis using the supplied screws.
3. Make sure the rack is grounded properly.

To install the switch without a shelf, use the included rack mount kit.

1.4.4. Technical and Electrical Specifications

- 1.6 GHz quad-core CPU
- 3.2 Tbps ASIC
- AC Model: 2 x 750 W, 100–240 VAC 50–60 Hz, 190–310 V HVDC, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy)
- DC Model: 2 x 750 W, -36–-72 VDC, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy)
- Typical power consumption: 190 W (no cables/transceivers)
- Cooling: 3 redundant (N+1) hot-swappable fans
- Operating temperature: 0°C to 45°C — 32°F to 113°F
- Operating humidity: 5% to 95%, non-condensing
- Storage temperature: -40°C to 70°C — -40°F to 158°F
- Dimensions (WxDxH): 440 x 480 x 44 mm — 17.32 x 18.9 x 1.73 in
- Weight: 7.5 kg — 16.5 lb
- MTBF: 230,870 hours

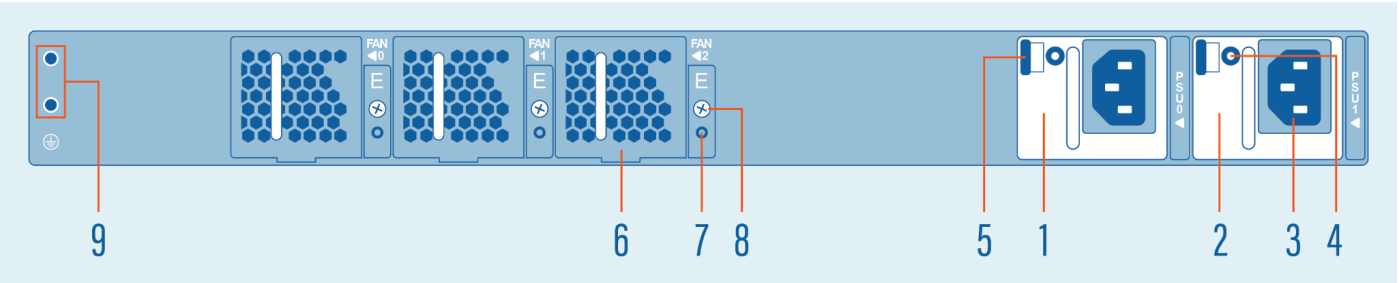
1.4.5. Front View



1	PSU1 status LED	7	Ethernet management port
2	PSU0 status LED	8	10G SFP+ management port (currently unused)
3	Fan status LED	9	10G SFP+ management port LED (currently unused)
4	System status LED	10	40/100G QSFP28 ports (1–32)*
5	Serial management port	11	QSFP28 port activity LEDs
6	USB port		

* 4x10G and 4x25G splits supported on ports 1–31.

1.4.6. Rear View



1	PSU0	6	Hot-swappable fan module
2	PSU1	7	Fan status LED
3	AC power connector	8	Fan module captive thumbscrew
4	PSU status LED	9	Grounding lug M4 screw holes
5	PSU release latch		

1.4.7. LED Functionality

LED Function	LED State	Description
PS0/PS1 status LED	Off	Power is not supplied to the PSU
	Green	PSU is operating normally
	Amber	PSU fault
PSU module LED	Off	No power input
	Green	Output ON and OK
	Blinking green (1/s)	PSU standby state input power present / Only +5VSB on.
	Blinking green (2/s)	Power supply firmware updating (bootloader mode).
	Red	Power supply critical event causing a shutdown, failure, over current, short circuit, over voltage, fan failure, and/or over temperature.
	Blinking red	DC power cord unplugged or DC power lost with a second power supply in parallel still with DC input power. Power supply DC present, 5VSB and 12V off via on/off control from system.
	Blinking green+red	Power supply warning events where the power supply continues to operate; high temp, high power, high current, and/or slow fan.
Fan status LED	Off	Fans are not initialized
	Green	Fans operating normally
	Amber	Fan fault: check rear of unit to see which fan is faulty
Fan module LED	Off	No input power
	Green	Fan operating normally
	Amber	Fan fault
System status LED	Off	No power
	Green	System operating normally
	Amber	Power is up but host CPU boot failed
QSFP28 port LEDs, 40G/100G mode	Off	No link
	Green	100G link

	Blinking green	100G activity
	Amber	40G link
	Blinking amber	40G activity
QSFP28 port LEDs, 4x10G/4x25G mode	Off	No link
	Green	25G link
	Blinking green	25G activity
	Amber	10G link
	Blinking amber	10G activity

2. Connecting Power and Start-Up

After ensuring all the necessary precautions have been taken during installation, the unit can be powered on. The system does not have a main switch: it powers up if one of the redundant power supplies is being connected to the main power.

The use of both power supplies is recommended to achieve a maximum fail-safe operation at all times.

The power supply modules are hot swappable: they can be exchanged or new modules can be added at all times under power, but data loss during the exchange must be taken into account.

XX-Series devices are equipped with status and activity LEDs. For more details on status LEDs color and coding, see chapters 1.3.7 (XX-1800G) or 1.4.7 (XX-3200G).

3. Initial Access

The unit's management port is initially set to DHCP, and can be accessed with the following default credentials:

- Username: **admin**
- Password: **Adminadmin1**

If the unit is deployed on a network without a DHCP server, it is possible to configure the unit's network settings by accessing it via the serial connection using the credentials above.

3.1. Configuring the Ethernet Management Port

To connect to the serial management interface, use the supplied cable and adapters, and any terminal software, with the following connection settings: 115200 baud rate, 8 bit, no parity, 1 bit stop.

Log in using the credentials in the previous section.

Edit the network configuration using the following command:

```
.system.network.set
```

Depending on user requirements, the IP can be set to either dynamic (DHCP) or static (custom IP). Please follow the instructions to configure the preferred option.

After the configuration is complete, the system is accessible through the network via SSH and web GUI at: `https://<ip_addr>`

XX-Series devices can also be connected directly to a computer through the Ethernet management port. In this case, manual IP policy must be applied to both the unit and the computer.

> **Note:** If the computer network interface is limited to 10/100 Mbps, a special twisted pair cable must be used instead of a normal patch cable.

For security reasons, an SSL certificate is pre-installed.

4. Web Administration

XX-Series devices can be administered either in CLI mode or via a web-based GUI, which is OS and platform independent.

Grouped by functionality, six menu tabs are displayed on the left side of the interface:

- Device Status
- Port Management
- Statistics
- Traffic Management
- Authentication
- Administration

4.1. Device Status

The **Information** tab in the **Device Status** menu displays details about the status of the device and the system administrator contact information:

- System information (model version, hardware and software revisions, serial number)
- Administrator information (name, phone number, email address)
- Date and time information
- Network details
- Global device traffic statistics, with number of packets and octets for the inbound and outbound traffic
- Sensors (air temperature measured in proximity of the fans block, system temperature measured within the forwarding plane chip, CPU temperature, PSU and fan status)
- Temperature readings for CPU, system and external air over time (can be expanded for an improved view)

4.2. Port Management

The **Port Management** page is a graphical representation of the system, providing detailed status information and allowing an easy configuration of each interface (port), as well as a more detailed view of the attached SFP modules. Besides the visual overview, the port information is also provided in a list view.

Configuration of a port is done by left-clicking on its graphical representation, thus exposing the following menu:

- **Port**: Shows the port number.
- **Status**: Displays additional information about the selected port: the current state of the port, the Tx and Rx bandwidth statistics, and the transceiver information (if present). This window also allows the port label to be changed, the port to be enabled or disabled, the port speed to be changed, and the port to be split.
- **Enable/Disable**: Allows the user to enable or disable a specific interface.
- **Speed**: Allows the user to change port speed, or to split the ports in order to use split cables. Note that for the SFP28 ports, the user cannot set individual port speeds, as these ports are grouped by 4 in the data plane. The interface will change the speed configuration in a consistent way, however it is the user's responsibility to make sure that the connected modules are capable of the selected speeds.

> **Note:** If the user wishes to change the configuration of a group of ports at the same time, this is possible using the *Manage Multiple* button, which allows the user to select multiple ports and change their state by choosing a new configuration from the *Set Multiple Ports* button.

The port list can be filtered via the *filter* button located at the top right corner of the list.

4.3. Statistics

The **Statistics** page displays specific statistics counters, either globally, or filtered by the interfaces selected.

The **Ports Statistics** tab displays traffic statistics for the selected interface(s). Clicking one or more interfaces will result in visually check-marking them and in adding new column(s) with their respective data stats. The *Reset Statistics* button will perform a reset of the hardware counters used in all the ports. Statistics for the select ports can be downloaded via the *Download Statistics* button.

The **Bandwidth Statistics** tab allows the user to compare the Tx and Rx bandwidth usage for each port, using bandwidth charts. The user can select the desired ports on the panel and see the bandwidth values plotted on the two charts on the screen. The value can be displayed in three different time ranges: one, three, and six hours.

4.4. Traffic Management

The **Traffic Management** page allows users logged in as administrators to create custom traffic aggregation, duplication and filtering rules, as well as enable load balancing for multiple interfaces, tailoring the way data flows on each port of the unit.

These custom settings are grouped into Rule Sets. Rule Sets can be managed and activated from the list in the Rule Sets tab. Only one Rule Set is active at any time.

The **Active** tab displays the Rule Set that is currently active, and its details, including the filtered interfaces, and the ones linked in load balancing. The Rule Set's name and description can be changed using the *Edit* button. The list of available rules can be filtered by name, input and output ports, priority class, and action type.

The **Rule Sets** tab displays the list of existing sets of rules (the active one being highlighted), allowing users logged in as administrators to:

-  Create a rule set
-  Clone a rule set
-  Configure a rule set
-  Activate a rule set
-  Rename a rule set
-  Delete a rule set

Multiple Rule Sets can be deleted by selecting one or more Rule Sets and pressing the *Delete Rule Sets* button, or exported by pressing the *Export Rule Sets* button. Previously exported Rule Sets can be imported by pressing the *Import Rule Sets* button.

> **Note:** Only one rule set can be active at a time.

A rule set needs to be composed of at least one rule in order to be taken into account and have any effect when applied. Rules can be added  , cloned  , modified  or deleted  .

> **Important:** Only data matching at least one of the defined rules will pass through, everything else will be dropped.

4.4.1. Rule - Interfaces

The first step in creating or editing a rule is defining the inbound and outbound interfaces.

The **Interfaces** tab allows defining the rule behavior (aggregation, replication), and using the load balancing groups in order to set the load-balance of the outbound traffic. Enabling the counter will display the amount of frames matching the defined rule.

The **Policy** option can be set to *Accept* or *Drop* the targeted traffic. Dropping is meant to be used when it is necessary to discard a subset of the traffic which is forwarded by a broader filter.

Additionally, a **priority class** can be specified for each rule. This feature can be used to define complex configurations, in which the user wants to create exception cases within drop or allow filters. The device

supports six priority classes, which are processed from 5 (highest priority) to 0 (lowest priority). Note that, within the same priority class, rules dropping traffic always have the priority over rules allowing traffic.

4.4.2. Rule - Filters

The **Filters** tab allows the user to configure the way in which traffic is targeted, according to specific rules related to its L2, L3 and L4 packet headers:

- **Ethernet Layer**
  Only frames matching MAC details configured in this section will be targeted (Source/Destination MAC Address, Source/Destination MAC Mask), with the possibility to select the **packet type** (IPv4, IPv6, ARP, TCP (IPv4/6), UDP (IPv4/6), SCTP (IPv4/6), Custom Protocol (IPv4/6), or any).

- **IPv4/IPv6 Layer**
  When IPv4/IPv6 is selected, the board will filter for any packet of those types. In order to filter for the IPv4/IPv6 details, the user needs to fill in the related fields (Source/Destination IP Address, Source/Destination IP Mask). The **Protocol** setting is only configurable for IPv4/IPv6, allowing the user to restrict the traffic to a specific type of L4 header (TCP, UDP, SCTP, ICMP, IGMP). *Any* allows filtering a custom EtherType or setting no filter for L3 headers.

- **TCP/UDP/SCTP Layer**
  When TCP/UDP/SCTP is selected in **Packet Type** or **Protocol**, only packets matching the transport layer details configured in this section will be filtered.

- **VLAN Tags**
  Can be used for filtering the first VLAN ID.

> **Note:** If multiple filter fields are configured, only packets matching all filters will be targeted.

4.4.3. Load Balancing Groups

When **Load Balancing Group** is enabled for a group of interfaces, it is important to remember that when a port is inserted in one of these groups, it cannot be used in additional rules and will be displayed as unavailable in the port layout. Additionally, in order to have a consistent behavior of the load balancing group, all of the interfaces belonging to that group **must** operate at the same speed.

The traffic is load balanced using the L3 and L4 fields to make sure to distribute the traffic flows consistently in the output ports.

4.4.4. Ingress Rules

Users can define specific traffic manipulation rules to be performed on the interface ingress pipeline. Note that these operations will be performed before the filter and action engine described above. Users should ensure that the configured ingress rules don’t impact the functionality of the other rules.

Each Rule Set can include an independent set of ingress rules associated to each port. Note that it is only possible to have a single rule per port, and that these ports will only be available as input in other rules.

The available traffic manipulation option is:

- **VLAN Tag**: Adds a VLAN tag to all traffic incoming in the selected port.

4.5. Authentication

4.5.1. Users

The **Users** tab allows users logged in as administrators to add new users or edit existing users and their privilege levels. Depending on the selected role, the user has the following privileges:

- **administrator**: full control, limitless administration and system update;
- **user**: create and set rules, aggregate and filter traffic, and port configuration;
- **viewer**: view only: settings, statistics, active rules.

The minimum requirements for the passwords are as follows:

- 8 characters;
- one letter uppercase;
- one letter lowercase;
- one digit.

4.5.2. TACACS+

The **TACACS+** tab allows adding up to three TACACS+ servers, and configuring the following details:

- priority (sets the order in which the servers will be taken into account, if more are added, with a lower number corresponding to a higher priority);
- login type (chap, login, pap);
- server hostname;
- port;
- secret key;
- timeout (waiting time for response from the TACACS+ server, can be set between 1 and 3 seconds);
- privilege mapping (translates the 15 privilege levels from TACACS+ into those of the viewers, users and admins; can be configured).

4.5.3. RADIUS

The **RADIUS** tab allows adding up to three RADIUS servers, and configuring the following details:

- priority (sets the order in which the servers will be taken into account, if more are added, with a lower number corresponding to a higher priority);
- server hostname;
- port;
- secret key;
- timeout (waiting time for response from the RADIUS server, can be set between 1 and 3 seconds);
- privilege mappings count (allows adding one or more rules for users. These rules are integer or string **type** attributes, requiring a **name** and a **value**. During authentication, the system checks if a user matches the rules. If there is a match between a user and a rule, then a **role** is applied for the user);

  Note: To add a new rule, click the  button. To apply the rule, click the  button.
- fallback role (comes into effect when there isn't a match between a user and a rule, with the 'none' option denying authentication access to *any* user).

4.5.4. LDAP and LDAPS

The **LDAP** tab offers the possibility to configure one or more LDAP servers for user authentication. In order to set up the LDAP access, the following settings are required:

- server hostname or address;
- server port: (default 389 for LDAP and 636 for LDAPS);
- priority (sets the order in which the servers will be taken into account, if more are added, with a lower number corresponding to a higher priority);
- timeout (waiting time for response from the LDAP server, can be set between 1 and 3 seconds);
- base DN (base distinguished name): this is the base DN used to query the LDAP servers for its information (example: `ou=people,dc=example,dc=com`);
- user DN (user distinguished name): DN parameter used to query for the usernames. (example: `uid`);
- LDAP version: it is possible to configure both LDAP Version 2 and Version 3 servers;
- privilege mappings count (allows adding one or more rules for users. These rules are integer or string **type** attributes, requiring a **name** and a **value**. During authentication, the system checks if a user matches the rules. If there is a match between a user and a rule, then a **role** is applied for the user);

  Note: To add a new rule, click the  button. To apply the rule, click the  button.
- fallback role (comes into place when there isn't a match between a user and a rule, with the 'none' option denying authentication access to *any* user);
- TLS mode: the user can select whether the server requires TLS (for LDAPS), and if they wish to enforce strict TLS session validation. Note that if this option is set to "strict", the user will likely need to import a private CA certificate on the device (*Administration* > *Setup* GUI page).

4.5.5. Profitap Supervisor

Profitap Supervisor can be used as a centralized authentication facility for all XX-Series and X2-Series packet brokers.

This feature can be enabled in the Supervisor when registering the device. The centralized manager will automatically register in the device as an authentication facility. From this moment on, the device will query the Supervisor to verify, using its authentication configuration, if the credentials used for login are valid. This feature allows the user to define the whole authentication configuration for all Profitap NPBs in a single point and have it being used across the whole fleet of packet brokers.

In the **Profitap Supervisor** tab, it is possible to visualize if any Supervisor has been registered with the device and eventually modify the address, port and registration token. Note that the Supervisor is already performing the registration process automatically and these settings shouldn't require any manual change.

When disabling the Profitap Supervisor from this GUI, the device will stop reaching to the Supervisor for authentication.

4.5.6. Custom Authentication Configuration

XX-Series devices allow users to not only define multiple authentication methods, but also to configure how the different methods are used by the device. Clicking the *Configure Authentication* button on any tab of the *Authentication* page allows users to see the list of available authentication methods and change their priority and activation strategy.

For each method, one of the following strategies can be selected:

- **Enable**: The method is activated and will be used to authenticate users;
- **Disable**: The method is not active and its configuration will be ignored;
- **Restrict**: A restricted authentication method is activated only if all higher priority methods are failing access. In the case of RADIUS, TACACS+, LDAP, and Supervisor methods, this means that no server is responding (or no server is programmed). If only one of the registered RADIUS/TACACS+/LDAP servers replies with a rejection, the following restricted methods will be skipped. Note that “Local Users” are always available, meaning that any “restrict” method after that will never be activated.

All authentication methods and their configured priority and activation strategy apply to all login methods: Serial CLI, SSH CLI, GUI, HTTPS RestAPI, and Ansible.

4.6. Administration

The **Administration** section allows users with administrator privileges to change system-related settings.

4.6.1. Setup

The **Setup** tab allows editing the administration contact details (name, phone, email), the system date and time, and the network configuration. This view can also be used to regenerate or replace the GUI HTTPS certificate, and import custom CA certificates.

> **Note:** In case the IP is set from static to DHCP, the new IP must first be discovered or allocated by the gateway (using a MAC address table). Also, disabling the network interface will make the web interface unavailable, in which case a serial connection to the unit must be established in order to reactivate the network interface (see chapter 5.1).

The *Configuration Backup / Restore* section allows you to backup all of the user settings, and to restore them from a previous backup. The backup package will be encrypted with the provided passphrase. Use the toggle options to select which settings to export or import.

4.6.2. Firmware

The **Firmware** tab allows the installation of a new firmware on the device. The latest firmware version is available publicly at https://npb.profitap.com/.

The *License Information* section displays the information related to the device license, and allows the license to be updated.

4.6.3. SNMP

The **SNMP** tab can be used to control the device's SNMP (v2c/v3) service. This functionality allows the operators to monitor the state of the device and the interface's traffic counters. The information can be accessed after having defined SNMP user credentials. It is also possible to configure the device to emit traps to the requested sink servers. The SNMP MIB files are also available from the GUI.

4.6.4. Firewall

The **Firewall** tab provides the ability to configure the device management service access control list. The IP address ranges that are allowed to access the various device services (HTTP, HTTPS, SSH, SNMP) can be defined here.

The ACL operates in allowlist (or whitelist) mode, meaning that addresses not covered by ALLOW rules are automatically rejected.

WARNING: If all entries are removed and the configuration is saved, management interface services won't be accessible anymore. In order to regain access, the serial CLI will need to be used, and the necessary ALLOW entry added.

4.6.5. Logs

The **Logs** tab displays the system and application logs stored locally on the device. The system logs include all logs coming from the OS components, while the application logs allow the user to view only the management plane ones. The Syslog tab can also be used to configure remote collectors for the device logs. This can be done by clicking the *Remote Servers* button and using the view that appears to configure the remote logging server details.

4.6.6. Support

The **Support** tab provides access to support files located on the device: the user manual (this document), product datasheet, REST API documentation, and Ansible library.

5. Command Line Reference

After logging into the system, the user has access to all available commands, grouped into four menus, as follows:

- Configuration
- Statistics
- Status
- System

Each menu can be selected by typing its name in the console, e.g.:

```
.> configuration
```

Useful commands to navigate the console:

- ***ls*** or ***help*** to list available branches (or by hitting TAB from keyboards)
- **.** returns to the initial branch
- **..** returns to the previous branch
- CTRL+D cancels a running command

Commands residing in cascading menus can also be executed from any location, outside their normal context menu, using the [**.**] prefix, provided the path and the command name is known, e.g.:

```
.status.device.> .configuration.interface.01
.configuration.interface.01.>
```

5.1. Configuration

The **Configuration** menu is used for the administration of all the interfaces (ports) in the system. An interface must first be selected (from 01 to 32, 56 or 64 depending on the model) before configuring it:

```
.configuration.> interface.01
.configuration.interface.01.>
```

The following commands are available:

```
.configuration.interface.01.enable
```

```
Enables the selected interface.
```

```
.configuration.interface.01.disable
```

```
Disables the selected interface.
```

```
.configuration.interface.01.label [show/set/reset]
```

show displays the port label.

set sets the port label.

reset resets the port label.

```
.configuration.interface.01.show
```

Displays the configuration associated with the selected interface and its current status regarding the link, whether it is enabled or not, speed and duplex mode.

```
.configuration.interface.01.speed [value]
```

Sets the port speed. Available values (depending on the port): 1G, 10G, 25G, 40G, 100G, 100G_FEC_RS, 2x50G, 4x10G, 4x25G, AUTONEG.

```
.configuration.interface.01.statistics
```

Displays statistics counters for the specified port.

```
.configuration.interface.01.transceiver.show
```

Displays information about the SFP/QSFP transceiver present in the interface. Key metrics here are the Tx and Rx dB levels which can offer insight on whether the fiber lines are experiencing faults or even intrusion attempts.

5.2. Statistics

The **Statistics** menu is used for displaying or resetting network traffic related statistics.

```
.> statistics
```

The following commands are available:

```
.statistics.global [show/reset]
```

show displays the following global statistics: bytes received, bytes sent, packets received, packets sent.

reset resets the global statistics.

```
.statistics.interface [port_number/all] [show/reset]
```

show displays the full statistics for a specified interface, or, if *all* is selected, displays the full statistics for all interfaces.

reset resets the full statistics for a specified interface, or, if *all* is selected, resets the full statistics for all interfaces.

5.3. Status

The **Status** menu is used for displaying the status of the main functionalities and the system itself.

```
.> status
```

The following commands are available:

```
.status.device.show
```

Displays general information about the device and device status.

```
.status.interface [port_number/all] [show/transceiver.show]
```

show displays the configuration associated with the selected interface and its current status regarding link speed.

transceiver.show displays information about the SFP/QSFP transceiver present in the interface, and about all ports.

5.4. System

The **System** menu is used for administrative changes.

```
.> system
```

The following commands are available:

```
.system.aaa.tacacs+ [add/config/show]
```

Configure remote authentication for the TACACS+ protocol.

```
.system.aaa.tacacs+.add --hostname [hostname or IPv4/IPv6 address] --login-type
[login/chap/pap] --min-admin-level [0–15] --min-user-level [0–15] --port
[0–65535] --priority [1–3] --secret [string] --timeout [1–3]
```

Adds a TACACS+ server.

Option	Parameter	Description	Example
--hostname	hostname or IPv4/IPv6 address	The TACACS+ server's hostname or IP address.	--hostname 10.10.10.1
--login-type	login/chap/pap	The type of login used in the server.	--login-type login
--min-admin-level	0–15	Value that defines what priv_lvl is requested for a user to be granted admin privileges.	--min-admin-level 5
--min-user-level	0–15	Value that defines what priv_lvl is requested for a user to be granted normal privileges.	--min-user-level 5
--port	0–65535	The port for the connection to the TACACS+ server. Default expected port is 49.	--port 49
--priority	1–3	The server priority in the user selection within the device. A server with a lower value have higher priority, so their users will be selected first in case of duplicates. There cannot be 2 specified servers sharing the same priority.	--priority 1

--secret	string	Key string used to encrypt the communication between the server and the client.	--secret key123
--timeout	1–3	Waiting time for response from the server, in seconds.	--timeout 1

```
.system.aaa.tacacs+.config --priority [1–5] --setting [enable/disable/restrict]
```

General settings for the TACACS+ authentication method.

Option	Parameter	Description	Example
--priority	1–5	Sets the priority of the TACACS+ authentication method. Lower value represents higher priority, meaning this method will be called before lower priority methods.	--priority 1
--setting	enable/disable /restrict	Enables, disables, or restricts the method. Restrict means the method will only be used if all higher priority methods are failing.	--setting enable

```
.system.aaa.tacacs+.show
```

Displays information about the current TACACS+ configuration. If one or more entries exist, they will be listed here. Existing entries can be configured using their current priority number as identifier (between 1 and 3).

```
.system.aaa.tacacs+.[1–3] [edit/remove/show]
```

Configure an existing TACACS+ entry using its priority number as identifier (between 1 and 3).

edit edits the entry using the same options as the *tacacs+.add* command shown above.

remove deletes the entry.

show displays information about this entry.

```
.system.aaa.radius [add/config/show]
```

Configure remote authentication for the RADIUS protocol.

```
.system.aaa.radius.add --attribute_name [string] --attribute_type [string or
integer] --attribute_value [string or integer] --fallback_role
[none/admin/user/viewer] --hostname [hostname or IPv4/IPv6 address] --operator
['<', '<=', '=>', '>', '==', '!='] --port [0–65535] --priority [1–3] --role
[none/admin/user/viewer] --secret [string] --timeout [1–3]
```

Adds a RADIUS server.

Option	Parameter	Description	Example
--attribute_name	string	Privilege map entry name.	--attribute_name entry1
--attribute_type	string (str) or integer (int)	Privilege map entry type.	--attribute_type int
--attribute_value	string or integer	Privilege map entry value.	--attribute_value 23
--operator	'<', '<=', '=>', '>', '==', '!='	Privilege map entry value comparison operator.	--operator '=='
--role	none/admin/user/viewer	Privilege map entry role.	--role admin
--fallback_role	none/admin/user/viewer	Comes into effect when there isn’t a match between a user and a rule, with the 'none' option denying authentication access to any user.	--fallback_role none
--hostname	hostname or IPv4/IPv6 address	The RADIUS server's hostname or IP address.	--hostname 10.10.10.1
--port	0–65535	The port for the connection to the RADIUS server. Default expected port is 1812.	--port 1812
--priority	1–3	The server priority in the user selection within the device. A server with a lower value have higher priority, so their users will be selected first in case of duplicates. There cannot be 2 specified servers sharing the same priority.	--priority 1
--secret	string	Key string used to encrypt the	--secret key123

		communication between the server and the client.	
--timeout	1–3	Waiting time for response from the server, in seconds.	--timeout 1

```
.system.aaa.radius.config --priority [1–5] --setting [enable/disable/restrict]
```

General settings for the RADIUS authentication method.

Option	Parameter	Description	Example
--priority	1–5	Sets the priority of the RADIUS authentication method. Lower value represents higher priority, meaning this method will be called before lower priority methods.	--priority 1
--setting	enable/disable /restrict	Enables, disables, or restricts the method. Restrict means the method will only be used if all higher priority methods are failing.	--setting enable

```
.system.aaa.radius.show
```

Displays information about the current RADIUS configuration. If one or more entries exist, they will be listed here. Existing entries can be configured using their current priority number as identifier (between 1 and 3).

```
.system.aaa.radius.[1–3] [edit/privilege-map/remove/show]
```

Configure an existing RADIUS entry using its priority number as identifier (between 1 and 3).

edit edits the entry using the same options as the *radius.add* command shown above (with the exception of privilege map-specific options).

privilege-map edits the privilege map for this entry.

remove deletes the entry.

show displays information about this entry.

```
.system.aaa.radius.[1–3].privilege-map [add/delete/edit/show]
```

Configure the privilege map of the specified RADIUS entry.

add adds an entry to the privilege map of the specified RADIUS entry using the same privilege map-specific options as the *radius.add* command shown above (*--attribute_name*, *--attribute_type*, *--attribute_value*, *--operator*, *--role*).

delete removes the entry specified with the *--index* option (e.g. *--index 1* to remove the entry with index number 1).

edit edits an entry using the same privilege map-specific options as the *radius.add* command shown above (*--attribute_name*, *--attribute_type*, *--attribute_value*, *--operator*, *--role*), in addition to the *--index* option (e.g. *--index 1* to edit the entry with index number 1).

show displays the current privilege map entries and their index numbers.

```
.system.aaa.ldap [add/config/show]
```

Configure remote authentication for the LDAP protocol.

```
.system.aaa.ldap.add --attribute_name [string] --attribute_type [string or
integer] --attribute_value [string or integer] --base_dn [string] --fallback_role
[none/admin/user/viewer] --hostname [hostname or IPv4/IPv6 address] --operator
['<', '<=', '>=','>','==','!=','=~'] --port [0–65535] --priority [1–3] --role
[none/admin/user/viewer] --timeout [1–3] --tls_usage [none/lenient/strict]
--user_dn [string] --version [2/3]
```

Adds an LDAP server.

Option	Parameter	Description	Example
--attribute_name	string	Privilege map entry name.	--attribute_name entry1
--attribute_type	string (str) or integer (int)	Privilege map entry type.	--attribute_type int
--attribute_value	string or integer	Privilege map entry value.	--attribute_value 23
--base_dn	string	Base DN used to query the LDAP servers for its information.	--base_dn ou=people,dc=example,dc=com
--fallback_role	none/admin/user/viewer	Comes into effect when there isn't a match between a user and a rule, with the	--fallback_role none

		'none' option denying authentication access to any user.	
--hostname	hostname or IPv4/IPv6 address	The LDAP server's hostname or IP address.	--hostname 10.10.10.1
--operator	'<', '<=', '=>', '>', '==', '!='	Privilege map entry value comparison operator.	--operator '=='
--port	0–65535	The port for the connection to the LDAP server. Default expected port is 389 for LDAP and 636 for LDAPS.	--port 389
--priority	1–3	The server priority in the user selection within the device. A server with a lower value have higher priority, so their users will be selected first in case of duplicates. There cannot be 2 specified servers sharing the same priority.	--priority 1
--role	none/admin/user/viewer	Privilege map entry role.	--role admin
--timeout	1–3	Waiting time for response from the server, in seconds.	--timeout 1
--tls_usage	none/lenient/strict	Select whether the server requires TLS (for LDAPS), and whether to enforce strict TLS session validation. **None:** TLS is not used for server communication. Data is transmitted in plain text without encryption. **Lenient:** TLS is used for secure server communication, but the connection doesn't require a valid, trusted SSL/TLS certificate. **Strict:** TLS is used for secure server communication, and the connection requires a valid, trusted SSL/TLS certificate.	--tls_usage strict

		Note that if this option is set to “strict”, the user will likely need to import a private CA certificate on the device.	
--user_dn	string	DN parameter used to query for the usernames.	--user_dn uid=john.doe
--version	2/3	LDAP version.	--version 3

.system.aaa.ldap.config --priority [1–5] --setting [enable/disable/restrict]

General settings for the LDAP authentication method.

Option	Parameter	Description	Example
--priority	1–5	Sets the priority of the LDAP authentication method. Lower value represents higher priority, meaning this method will be called before lower priority methods.	--priority 1
--setting	enable/disable/restrict	Enables, disables, or restricts the method. Restrict means the method will only be used if all higher priority methods are failing.	--setting enable

.system.aaa.ldap.show

Displays information about the current LDAP configuration. If one or more entries exist, they will be listed here. Existing entries can be configured using their current priority number as identifier (between 1 and 3).

.system.aaa.ldap.[1–3] [edit/privilege-map/remove/show]

Configure an existing LDAP entry using its priority number as identifier (between 1 and 3).

edit edits the entry using the same options as the *ldap.add* command shown above (with the exception of privilege map-specific options).

privilege-map edits the privilege map for this entry.

remove deletes the entry.

show displays information about this entry.

```
.system.aaa.ldap.[1–3].privilege-map [add/delete/edit/show]
```

Configure the privilege map of the specified LDAP entry.

add adds an entry to the privilege map of the specified LDAP entry using the same privilege map-specific options as the *ldap.add* command shown above (*--attribute_name*, *--attribute_type*, *--attribute_value*, *--operator*, *--role*).

delete removes the entry specified with the *--index* option (e.g. *--index 1* to remove the entry with index number 1).

edit edits an entry using the same privilege map-specific options as the *ldap.add* command shown above (*--attribute_name*, *--attribute_type*, *--attribute_value*, *--operator*, *--role*), in addition to the *--index* option (e.g. *--index 1* to edit the entry with index number 1).

show displays the current privilege map entries and their index numbers.

```
.system.aaa.supervisor [config/deactivate/edit/show]
```

Configure the Supervisor authentication method.

```
.system.aaa.supervisor.config --priority [1-4] --setting
[enable/disable/restrict]
```

General settings for the Supervisor authentication method.

Option	Parameter	Description	Example
--priority	1–4	Sets the priority of the Supervisor authentication method. Lower value represents higher priority, meaning this method will be called before lower priority methods.	--priority 1
--setting	enable/disable /restrict	Enables, disables, or restricts the method. Restrict means the method will only be used if all higher priority methods are failing.	--setting enable

```
.system.aaa.supervisor.deactivate
```

Deactivates Supervisor authentication.

```
.system.aaa.supervisor.edit --hostname [hostname or IP address]
--registration-token [string]
```

Changes the Supervisor hostname or IP address and registration token.

```
.system.aaa.supervisor.show
```

Displays information about the current configuration of the Supervisor authentication method.

```
.system.aaa.users [config/new/edit/remove/show]
```

Configure the Local Users authentication method.

```
.system.aaa.users.config --priority [1-4] --setting [enable/restrict]
```

General settings for the Local Users authentication method.

Option	Parameter	Description	Example
--priority	1–4	Sets the priority of the Local Users authentication method. Lower value represents higher priority, meaning this method will be called before lower priority methods.	--priority 1
--setting	enable/restrict	Enables or restricts the method. Restrict means the method will only be used if all higher priority methods are failing.	--setting enable

```
.system.aaa.users.new --email [email] --enable [true/false] --full_name
[full_name] --password [password] --role [admin/user/viewer] --username
[username]
```

Creates a new user account using the specified information.

Option	Parameter	Description	Example
--email	string	The user's email address.	--email new@user.it
--enable	true/false	Enable or disable this user for local authentication.	--enable true

--full_name	string	The user's full name. Doesn't support spaces.	--full_name New_User
--password	string	The user account's password. Requires 8 characters, one letter uppercase, one letter lowercase, one digit.	--password Password1
--role	admin/user/ viewer	The user account's privileges. **admin:** full control, limitless administration and system update; **user:** create and set rules, aggregate and filter traffic, and port configuration; **viewer:** view only: settings, statistics, active rules.	--role admin
--username	string	The user account's unique name.	--username newuser

```
.system.aaa.users.edit [username] --email [email] --enable [true/false]
--full_name [full_name] --password [password] --role [admin|user|viewer]
--username [newusername]
```

Edits the specified user account. All options are optional.

```
.system.aaa.users.remove [username]
```

Deletes the specified user account.

```
.system.aaa.users.show [username]
```

Displays information about the specified user account.

```
.system.aaa.show
```

Lists the authentication methods, whether they are enabled, disabled or restricted, and their priority.

```
.system.date.set --date [YYYY-MM-DD] --servers [server1,server2,...] --time
[HH:MM:SS] --timezone [timezone] --type [user/ntp]
```

Configures the device's date and time settings.

Option	Parameter	Description	Example
--date	YYYY-MM-DD	Sets the date manually if *--type* is set to *user*.	--date 2008-10-31
--servers	server1,server2,...	The list of NTP servers used to set the date and time if *--type* is set to *ntp*.	--servers 0.pool.ntp.org,1.pool.ntp.org,2.pool.ntp.org
--time	HH:MM:SS	Sets the time manually if *--type* is set to *user*.	--time 01:23:45
--timezone	timezone	The time zone used to set the time if *--type* is set to *ntp*. Use *.system.date.show_available_timezones* to display the list of available time zones.	--timezone Europe/Amsterdam
--type	user/ntp	Selects whether the date and time are to be set manually or using NTP servers.	--type ntp

```
.system.date.show
```

Displays the NTP status, time zone, date, time, and configured NTP server(s).

```
.system.date.show_available_timezones
```

Lists available timezones to be used for setting a new date.

```
.system.firewall [append/emplace/insert/remove/show]
```

Configure the management interface's firewall.

```
.system.firewall.append --active [true/false] --address [ip address] --label
[string] --mask [0–128] --policy [allow/drop] --services [snmp,ssh,http,https]
```

Adds a firewall record at the end of the list.

Option	Parameter	Description	Example
--active	true/false	Sets whether or not this entry is enabled.	--active true
--address	ip address	The source IPv4 or IPv6 address.	--address 1.1.1.1
--label	string	The label for this entry.	--label fwentry1
--mask	0–128	The CIDR mask.	--mask 32
--policy	allow/drop	Sets whether to allow or drop traffic from the specified source IP address and service(s).	--policy allow
--services	snmp/ssh/http/https	The services targeted by this entry.	--services snmp,ssh,http,https

```
.system.firewall.emplace --active [true/false] --address [ip address] --label
[string] --mask [0–128] --policy [allow/drop] --priority [integer] --services
[snmp,ssh,http,https]
```

Adds a firewall record into a specific priority place in the list. See the *append* command above for an explanation of the options. The only difference is the addition of the *--priority* option, which takes an integer parameter, e.g. *--priority 1*.

```
.system.firewall.insert --active [true/false] --address [ip address] --label
[string] --mask [0–128] --policy [allow/drop] --services [snmp,ssh,http,https]
```

Adds a firewall record at the beginning of the list. See the *append* command above for an explanation of the options.

```
.system.firewall.remove --priority [integer]
```

Removes a firewall entry by specifying its priority. See the *show* command below for finding an entry's priority.

```
.system.firewall.show
```

Displays the list of current firewall entries and their priority.

```
.system.network [disable/set/status]
```

Configure the management interface's network settings.

```
.system.network.disable
```

Disables the Ethernet management port. The serial management port will still be operating. After issuing the command, the user must confirm it [yes].

Note: If connected through the Ethernet management port, after issuing the *disable* command, the session will be lost.

```
.system.network.set --type [disable/dhcp/static/dhcp_v4/dhcp_v6/eui-64] --ip
[static IPv4 address] --prefix [IPv4 CIDR prefix] --gateway [gateway IPv4
address] --dns [first DNS IPv4 address] --dns2 [second DNS IPv4 address] --ip_v6
[static IPv6 address] --prefix_v6 [IPv6 CIDR prefix] --gateway_v6 [gateway IPv6
address] --dns_v6 [first DNS IPv6 address] --dns2_v6 [second DNS IPv6 address]
--hostname [device hostname]
```

Sets the management interface's network settings.

Option	Parameter	Description	Example
--type	disable/dhcp/static/dhcp_v4/dhcp_v6/eui-64	**disable** disables the management interface. **dhcp** sets the IP acquisition mode to DHCP IPv4/IPv6. **static** sets the IP acquisition mode to STATIC IPv4/IPv6. **dhcp_v4** sets the IP acquisition mode to DHCP IPv4. **dhcp_v6** sets the IP acquisition mode to DHCP IPv6. **eui-64** sets the IP acquisition mode to STATIC IPv6 EUI-64.	--type dhcp

--ip	IPv4 address	Sets the management interface's IPv4 address, if *--type* is set to *static*.	--ip 127.0.0.1
--prefix	IPv4 CIDR prefix	Sets the management interface's IPv4 CIDR prefix, if *--type* is set to *static*.	--prefix 24
--gateway	IPv4 address	Sets the management interface's gateway's IPv4 address, if *--type* is set to *static*.	--gateway 192.168.1.1
--dns	IPv4 address	Sets the management interface's first DNS's IPv4 address, if *--type* is set to *static*.	--dns 8.8.8.8
--dns2	IPv4 address	Sets the management interface's second DNS's IPv4 address, if *--type* is set to *static*.	--dns2 8.8.8.8
--ip_v6	IPv6 address	Sets the management interface's IPv6 address, if *--type* is set to *static* or *eui-64*.	--ip_v6 ::1
--prefix_v6	IPv6 CIDR prefix	Sets the management interface's IPv6 CIDR prefix, if *--type* is set to *static*.	--prefix_v6 64
--gateway_v6	IPv6 address	Sets the management interface's gateway's IPv6 address, if *--type* is set to *static* or *eui-64*.	--gateway_v6 FE80::1
--dns_v6	IPv6 address	Sets the management interface's first DNS's IPv4 address, if *--type* is set to *static* or *eui-64*.	--dns_v6 2001:4860:4860::8888
--dns2_v6	IPv6 address	Sets the management interface's second DNS's IPv4 address, if *--type* is set to *static* or *eui-64*.	--dns2_v6 2001:4860:4860::8888
--hostname	string	Sets the management interface's hostname.	--hostname hostname

.system.network.status

Displays the network parameters of the unit: IP mode, hostname, link status, IP, mask, gateway, DNS, and MAC.

.system.license.install --insecure [true/false] --url [license file url]

Installs a new license on the device.

Option	Parameter	Description	Example
--insecure	true/false	Specifies whether the license URL uses a secure connection.	--insecure false
--url	URL	The URL of the new license to install on the device (HTTP/HTTPS/FTP). If server credentials are required, they need to be passed as part of the url in the form `ftp://user:password@server/file`. If the username or password include special characters that cannot be expressed in the URL format, they will need to be replaced with their entity codes (e.g `@` will be `%40`). A list is available at https://dev.w3.org/html5/html-author/charref	--url ftp://user:password@server/file

.system.reboot --force [true/false]

Reboots the system, keeping all configurations intact. After issuing the command, the user must confirm it [yes].

Note: Rebooting the unit will temporarily disrupt the data flow.

Option	Parameter	Description	Example
--force	true/false	Optional. If set to *true*, the system will reboot without asking for confirmation.	--force true

.system.snmp.communities [add/delete/edit/show]

Configure SNMP v2c communities.

```
.system.snmp.communities.add --active [true/false] --name [name]
```

Adds an SNMP community.

Option	Parameter	Description	Example
--active	true/false	Sets the new community as active or inactive.	--active true
--name	string	Sets the new community's name.	--name community1

```
.system.snmp.communities.edit --active [true/false] --id [id] --name [name]
```

Edits the community specified by the *--id* option.

Option	Parameter	Description	Example
--active	true/false	Sets the specified community as active or inactive.	--active true
--id	integer	Specifies the id of the community to edit.	--id 21
--name	string	Set the new name of the specified community.	--name community1

```
.system.snmp.communities.delete --id [id]
```

Deletes the community specified by the *--id* option.

```
.system.snmp.communities.show --id [id]
```

Displays details about the community specified by the *--id* option, or about all communities if *--id* isn't used.

```
.system.snmp.enable
```

Enables the SNMP service.

```
.system.snmp.disable
```

Disables the SNMP service.

```
.system.snmp.state
```

Displays the state of the SNMP service.

```
.system.snmp.trapsinks [add/edit/delete/show]
```

Configure SNMP trapsinks.

```
.system.snmp.trapsinks.add --active [true/false] --community [community] --host
[hostname] --name [name] --port [port] --user [user] --version [v2c/v3]
```

Adds an SNMP trapsink.

Option	Parameter	Description	Example
--active	true/false	Sets the new trapsink as active or inactive.	--active true
--community	string	The trap receiver community, if *--version* is set to *v2c*.	--community community1
--host	hostname or IPv4/IPv6	The trap receiver hostname or IP address.	--host 11.11.11.11
--name	strong	Sets the new trapsink's name.	--name trapsink1
--port	integer	The trap receiver port.	--port 161
--user	string	The trap receiver user, if *--version* is set to *v3*.	--user snmpuser1
--version	v2c/v3	The SNMP version for the new trapsink.	--version v2c

```
.system.snmp.trapsinks.edit --active [true/false] --community [community] --host
[hostname] --id [id] --name [name] --port [port] --user [user] --version [v2c/v3]
```

Edits the SNMP trapsink specified by the *--id* option.

Option	Parameter	Description	Example
--active	true/false	Sets the specified trapsink as active or inactive.	--active true
--community	string	The trap receiver community, if	--community

		--version is set to *v2c*.	community1
--host	hostname or IPv4/IPv6	The trap receiver hostname or IP address.	--host 11.11.11.11
--id	integer	Specifies the id of the trapsink to edit.	--id 10
--name	strong	Sets the trapsink's new name.	--name trapsink1
--port	integer	The trap receiver port.	--port 161
--user	string	The trap receiver user, if *--version* is set to *v3*.	--user snmpuser1
--version	v2c/v3	The SNMP version.	--version v2c

```
.system.snmp.trapsinks.delete --id [id]
```

Deletes the SNMP trapsink specified by the *--id* option.

```
.system.snmp.trapsinks.show
```

Displays configured SNMP trapsinks.

```
.system.snmp.users [add/edit/delete/show]
```

Configure SNMP v3 users.

```
.system.snmp.users.add --active [true/false] --auth [md5/sha] --auth_pass [auth
passphrase] --priv [des/aes] --priv_pass [priv passphrase] --security
[noauth/auth/priv] --username [username]
```

Adds an SNMP user.

Option	Parameter	Description	Example
--active	true/false	Sets the new user as active or inactive.	--active true
--auth	md5/sha	The algorithm for user authentication (*--security* set to *auth* or *priv*).	--auth sha
--auth_pass	string	The passphrase for user authentication (*--security* set to *auth* or *priv*).	--auth_pass userpwd1
--priv	des/aes	The encryption protocol (*--security*	--priv des

		set to *priv*).	
--priv_pass	string	The encryption passphrase (*--security* set to *priv*).	--priv_pass userpwd2
--security	noauth/auth/priv	Selects the requested security policy. Note that requests sent by `noauth` users will be performed in clear over the network.	--security priv
--username	string	Sets the new user's name.	--username user1

```
.system.snmp.users.edit --active [true/false] --auth [md5/sha] --auth_pass [auth passphrase] --id [id] --priv [des/aes] --priv_pass [priv passphrase] --security [noauth/auth/priv] --username [username]
```

Edits the SNMP user specified by the *--id* option.

Option	Parameter	Description	Example
--active	true/false	Sets the specified user as active or inactive.	--active true
--auth	md5/sha	The algorithm for user authentication (*--security* set to *auth* or *priv*).	--auth sha
--auth_pass	string	The passphrase for user authentication (*--security* set to *auth* or *priv*).	--auth_pass userpwd1
--id	integer	Specifies the id of the user to edit.	--id 12
--priv	des/aes	The encryption protocol (*--security* set to *priv*).	--priv des
--priv_pass	string	The encryption passphrase (*--security* set to *priv*).	--priv_pass userpwd2
--security	noauth/auth/priv	Selects the requested security policy. Note that requests sent by `noauth` users will be performed in clear over the network.	--security priv
--username	string	Sets the specified user's new name.	--username user1

```
.system.snmp.users.delete --id [id]
```

Deletes the SNMP user specified by the *--id* option.

```
.system.snmp.users.show --id [id]
```

Displays details about the user specified by the *--id* option, or about all users if *--id* isn't used.

```
.system.syslog.application.show
```

Displays all application logs and their timestamps.

```
.system.syslog.system.show
```

Displays all system logs and their timestamps.

```
.system.syslog.servers [add/edit/delete/show]
```

Configure remote syslog servers to send logs to.

```
.system.syslog.servers.add --active [true/false] --hostname [hostname] --port [port] --priority [alert/emerg/crit/error/warning/notice/info/debug] --protocol [tcp/udp] --type [system/app/both]
```

Adds a remote syslog server entry.

Option	Parameter	Description	Example
--active	true/false	Sets the new server as active or inactive.	--active true
--hostname	hostname or IPv4/IPv6	The server's hostname or IP address.	--hostname 1.1.1.1
--port	integer	The server port through which to connect.	--port 5454
--priority	alert/emerg/crit/error/warning/notice/info/debug	The type of logs to send. From *alert* (send only the highest priority logs) all the way down to *debug* (send everything).	--priority debug
--protocol	tcp/udp	The protocol used for sending the logs.	--protocol tcp
--type	system/app/both	The log source: *system* sends OS components logs, *app* sends management plane logs, *both* sends both.	--type both

```
.system.syslog.servers.edit --active [true/false] --hostname [hostname] --id [id]
--port [port] --priority [alert/emerg/crit/error/warning/notice/info/debug]
--protocol [tcp/udp] --type [system/app/both]
```

Edits the remote syslog server entry specified by the *--id* option.

Option	Parameter	Description	Example
--active	true/false	Sets the server as active or inactive.	--active true
--hostname	hostname or IPv4/IPv6	The server's hostname or IP address.	--hostname 1.1.1.1
--id	integer	Specifies the id of the entry to edit.	--id 22
--port	integer	The server port through which to connect.	--port 5454
--priority	alert/emerg/crit/error/warning/notice/info/debug	The type of logs to send. From *alert* (send only the highest priority logs) all the way down to *debug* (send everything).	--priority debug
--protocol	tcp/udp	The protocol used for sending the logs.	--protocol tcp
--type	system/app/both	The log source: *system* sends OS components logs, *app* sends management plane logs, *both* sends both.	--type both

```
.system.syslog.servers.delete --id [id]
```

Deletes the remote syslog server specified by the *--id* option.

```
.system.syslog.servers.show
```

Displays the list of remote syslog servers.

```
.system.update.install --insecure [true/false] --url [system package url]
```

Installs a new device firmware from a URL.

Option	Parameter	Description	Example
--insecure	true/false	Specifies whether the firmware package URL uses a secure connection.	--insecure false
--url	URL	The URL of the firmware package to install on the device (HTTP/HTTPS/FTP). If server credentials are required, they need to be passed as part of the url in the form `ftp://user:password@server/file`. If the username or password include special characters that cannot be expressed in the URL format, they will need to be replaced with their entity codes (e.g `@` will be `%40`). A list is available at https://dev.w3.org/html5/html-author/charref	--url ftp://user:password@server/file

6. Integrations

6.1. RESTful API Support

To integrate with tools, controllers and other IT systems, the XX-Series rev. 2 offers programmatic access to the platform through HTTP RESTful API support.

The latest REST API documentation and examples can be downloaded from the GUI's *Support* tab.

6.2. Ansible Support

XX-Series rev. 2 devices can be also controlled and configured using ansible playbooks. The necessary libraries and example playbooks are available in the web GUI's *Support* tab or in our resource center.

Legal

Disclaimer

The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranty of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes in the content thereof without obligation of the manufacturer to notify any person of such revision or changes.

Copyright

Trademarks

The trademarks mentioned in this manual are the sole property of their owners.

Profitap HQ B.V.
High Tech Campus 84
5656AG Eindhoven
The Netherlands
sales@profitap.com
www.profitap.com