

# The logo for the X2 series, consisting of a large, stylized "X2" in a dark blue, bold font, followed by the word "series" in a smaller, italicized, dark blue font.

***X2-2000G***

***X2-2010G***

***X2-3200G***

***X2-6400G***

***NETWORK PACKET BROKERS***

***USER MANUAL***

X2-Series software version: v0.15.2 / x0.15.3

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](mailto:support@profitap.com)**

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

**<https://resources.profitap.com/>**

# TABLE OF CONTENTS

<b>1. Overview</b>	<b>5</b>
<b>1.1. Hardware Overview</b>	<b>5</b>
1.1.1. X2-2000G	5
1.1.2. X2-2010G	5
1.1.3. X2-3200G	6
1.1.4. X2-6400G	6
<b>1.2. Supported Cables and Transceivers</b>	<b>7</b>
<b>1.3. X2-2000G</b>	<b>8</b>
1.3.1. Package Contents	8
1.3.2. Installation as Standalone	8
1.3.3. Installation in a Rack	8
1.3.4. Technical and Electrical Specifications	8
1.3.5. Front View	9
1.3.6. Rear View	9
1.3.7. LED Functionality	10
<b>1.4. X2-2010G</b>	<b>11</b>
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
<b>1.5. X2-3200G</b>	<b>14</b>
1.5.1. Package Contents	14
1.5.2. Installation as Standalone	14
1.5.3. Installation in a Rack	14
1.5.4. Technical and Electrical Specifications	14
1.5.5. Front View	15
1.5.6. Rear View	15
1.5.7. LED Functionality	16
<b>1.6. X2-6400G</b>	<b>17</b>
1.6.1. Package Contents	17
1.6.2. Installation as Standalone	17
1.6.3. Installation in a Rack	17
1.6.4. Technical and Electrical Specifications	17
1.6.5. Front View	18
1.6.6. Rear View	18
1.6.7. LED Functionality	19
<b>2. Connecting Power and Start-Up</b>	<b>20</b>
<b>3. Initial Access</b>	<b>21</b>
3.1. Configuring the Ethernet Management Port	21
<b>4. Web Administration</b>	<b>22</b>
4.1. Device Status	22
4.2. Port Management	23
4.3. Statistics	23
4.4. Traffic Management	24
4.4.1. Rule - Interfaces	24
4.4.2. Rule - Filters	25
4.4.3. Rule - Advanced	26

4.4.4. Load Balancing Groups	27
4.4.5. Ingress Rules	27
4.4.6. Time Synchronization (X2-3200G, X2-6400G)	28
4.4.7. Traffic Deduplication	29
4.5. Authentication	30
4.5.1. Users	30
4.5.2. TACACS+	30
4.5.3. RADIUS	30
4.5.4. Profitap Supervisor	31
4.5.5. Custom Authentication Configuration	31
4.6. Administration	32
4.6.1. Setup	32
4.6.2. Firmware	32
4.6.3. SNMP	32
4.6.4. Firewall	32
4.6.5. Logs	32
4.6.6. Support	33
<b>5. Command Line Reference</b>	<b>34</b>
5.1. Configuration	34
5.2. Statistics	36
5.3. Status	36
5.4. System	37
<b>6. Integrations</b>	<b>56</b>
6.1. RESTful API Support	56
6.2. Ansible Support	56
<b>Legal</b>	<b>57</b>
Disclaimer	57
Copyright	57
Trademarks	57

# 1. Overview

## 1.1. Hardware Overview

**X2-Series** is a high-end versatile solution, designed for aggregation, advanced filtering and routing of multiple high speed inputs, used in very high sustained bandwidth port monitoring and analysis scenarios.

All models can be managed via CLI, or via the **X2-Manager** web interface.

**QSFP28 modules** support:

- 40G/100G speeds
- 4 x 10G SFP28 splits
- 4 x 25G SFP28 splits
- 2 x 50G SFP56 splits

They are also backward compatible with QSFP+ standards.

### 1.1.1. X2-2000G

X2-2000G is supplied with either 28 or 56 enabled ports, depending on the license:

- **X2-2000G-244:** 16 x 1/10/25G SFP28, 8 x 10/25G SFP28, 4 x 40/100G QSFP28
- **X2-2000G-488:** 16 x 1/10/25G SFP28, 32 x 10/25G SFP28, 8 x 40/100G QSFP28

The unit features the following ports:

- 16 x 1/10/25G SFP28, 32 x 10/25G SFP28, and 8 x 40/100G QSFP28 ports supporting optical transceivers, active optical cables or DAC cables to connect the ports to the hosts
- 1 x management port used to access the unit through an RJ45 Ethernet cable
- 1 x serial management port (RJ45) 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

### 1.1.2. X2-2010G

X2-2010G is supplied with either 28 or 56 enabled ports, depending on the license:

- **X2-2010G-244:** 24 x 10/25G SFP28, 4 x 40/100G QSFP28
- **X2-2010G-488:** 48 x 10/25G SFP28, 8 x 40/100G QSFP28

The unit features the following ports:

- 48 x 10/25G SFP28 and 8 x 40/100G QSFP28 ports supporting optical transceivers, active optical cables or DAC cables to connect the ports to the hosts
- 1 x management port used to access the unit through an RJ45 Ethernet cable
- 1 x serial management port (RJ45) 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

### 1.1.3. X2-3200G

X2-3200G is supplied with either 16 or 32 enabled ports, depending on the license:

- **X2-3200G-16-AC:** 16 x 40/100G QSFP28
- **X2-3200G-32-AC:** 32 x 40/100G QSFP28

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 management port used to access the unit through an RJ45 Ethernet cable
- 1 x serial management port (RJ45) 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
- 1 x 1G SFP port for PTPv2 time synchronization

### 1.1.4. X2-6400G

The unit features the following ports:

- 64 x 40/100G QSFP28 ports supporting optical transceivers, active optical cables or DAC cables to connect the ports to the hosts
- 1 x management port used to access the unit through an RJ45 Ethernet cable
- 2 x serial management ports (1 x RJ45, 1 x micro USB) 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
- 1 x 1G SFP port for PTPv2 time synchronization

## 1.2. Supported Cables and Transceivers

Profitap X2-Series devices are not vendor locked to any specific brand of QSFP or SFP modules and cables. For optimal support, Profitap transceivers are recommended.

	X2-2000G	X2-2010G	X2-3200G	X2-6400G
10G SFP+ Direct Attach Cable	✓	✓		
10G SFP+ Active Optical Cable	✓	✓		
25G SFP28 Direct Attach Cable	✓	✓		
25G SFP28 Active Optical Cable	✓	✓		
40G QSFP+ Direct Attach Cable	✓	✓	✓	✓
40G QSFP+ Active Optical Cable	✓	✓	✓	✓
100G QSFP28 Direct Attach Cable	✓	✓	✓	✓
100G QSFP28 Active Optical Cable	✓	✓	✓	✓
1000BASE-T SFP Module	✓			
1000BASE-SX SFP Module	✓			
1000BASE-LX/LH SFP Module	✓			
10GBASE-T SFP+ Module	✓	✓		
10GBASE-SR SFP+ Module	✓	✓		
10GBASE-LR SFP+ Module	✓	✓		
25GBASE-SR SFP28 Module	✓	✓		
40GBASE-SR4 QSFP+ Module	✓	✓	✓	✓
40GBASE-LR4 QSFP+ Module	✓	✓	✓	✓
40GBASE-PLR4 QSFP+ Module	✓	✓	✓	✓
40GBASE-SR-BD QSFP+ Module	✓	✓	✓	✓
40GBASE-SR-BD Rx only QSFP+ Module	✓	✓	✓	✓
100GBASE-SR4 QSFP28 Module	✓	✓	✓	✓
100GBASE-LR4 QSFP28 Module	✓	✓	✓	✓
100GBASE-SR-BD QSFP28 Module	✓	✓	✓	✓
100GBASE-SR-BD Rx only QSFP28 Module	✓	✓	✓	✓

## 1.3. X2-2000G

### 1.3.1. Package Contents

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

- 1 x X2-2000G main unit
- 2 x C13 AC power cord
- 1 x RJ45 female to 9-pin serial adapter
- 1 x USB/RJ45 adapter cable
- 1 x RJ45 cable
- 1 x rack mounting kit (front and rear brackets, screws)
- Quick start guide

**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.

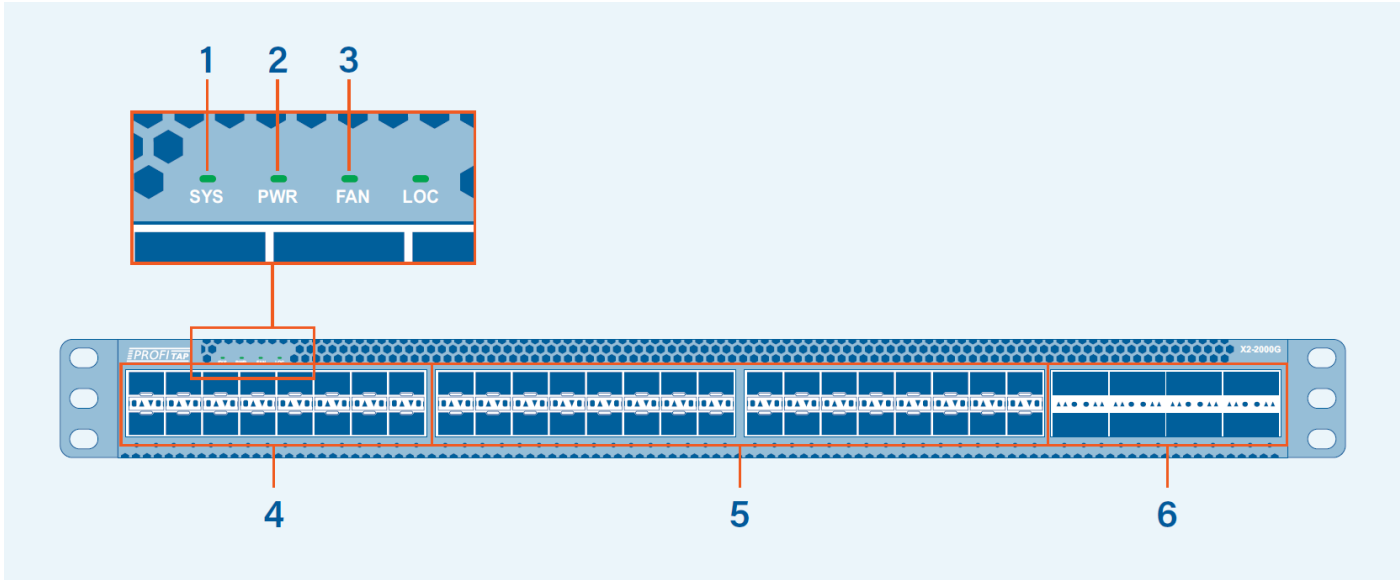
To install the switch without a shelf, use the included rack mount kit.

### 1.3.4. Technical and Electrical Specifications

- 2.2 GHz Intel Xeon quad-core 64-bit CPU
- 2.0 Tbps ASIC
- 2 x 850 W, 100-240 VAC, 50-60 Hz, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy)
- Typical power consumption: 600 W
- Cooling: 3N + 1 redundant fans
- Operating temperature: 0°C to 40°C — 32°F to 104°F
- Operating humidity: 10% to 90%, non-condensing
- Dimensions (WxDxH): 440 x 460 x 44 mm — 17.32 x 18.11 x 1.73 in
- Safety: FCC, CE, RoHS 6

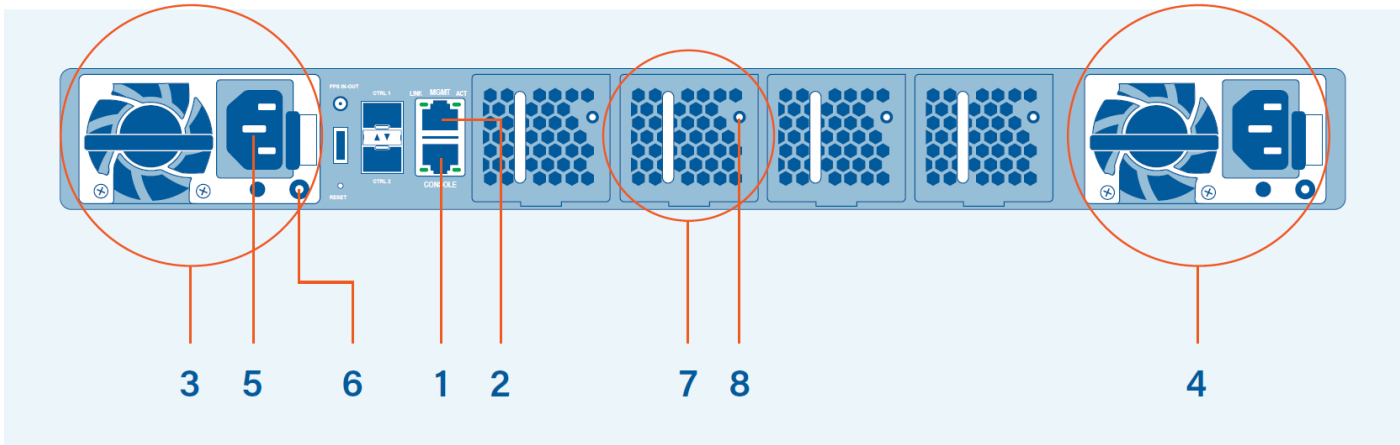


1.3.5. Front View



1	System status LED	4	1/10/25G SFP28 ports (1-16)
2	PSU status LED	5	10/25G SFP28 ports (17-48)
3	Fan status LED	6	40/100G QSFP28 ports (49-56)

1.3.6. Rear View



1	Serial management port	5	AC Power Connector (with Plug Retainer)
2	Ethernet management port	6	PSU status LED
3	PSU1	7	Hot swappable fan module
4	PSU2	8	Fan LED

### 1.3.7. LED Functionality

LED Function	LED State	Description
System status LED	Green	System operating normally
	Blinking green	System booting
	Red	System fault
PSU status LED	Green	PSU operating normally
	Red	PSU fault
	Off	No PSU installed
Fan status LED	Green	Fan operating normally
	Red	Fan fault: check rear of unit to see which fan is faulty
	Off	No fan installed
SFP28/QSFP28 port LED	Green	100G link
	Blinking green	100G activity
	White	50G link
	Blinking white	50G activity
	Amber	40G link
	Blinking amber	40G activity
	Blue	25G link
	Blinking blue	25G activity
	Purple	1G or 10G link
	Blinking purple	1G or 10G activity

## 1.4. X2-2010G

### 1.4.1. Package Contents

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

- 1 x X2-2010G main unit
- 2 x C13 AC power cord
- 1 x RJ45 female to 9-pin serial adapter
- 1 x USB/RJ45 adapter cable
- 1 x RJ45 cable
- 1 x rack mounting kit (front and rear brackets, screws)
- Quick start guide

**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.

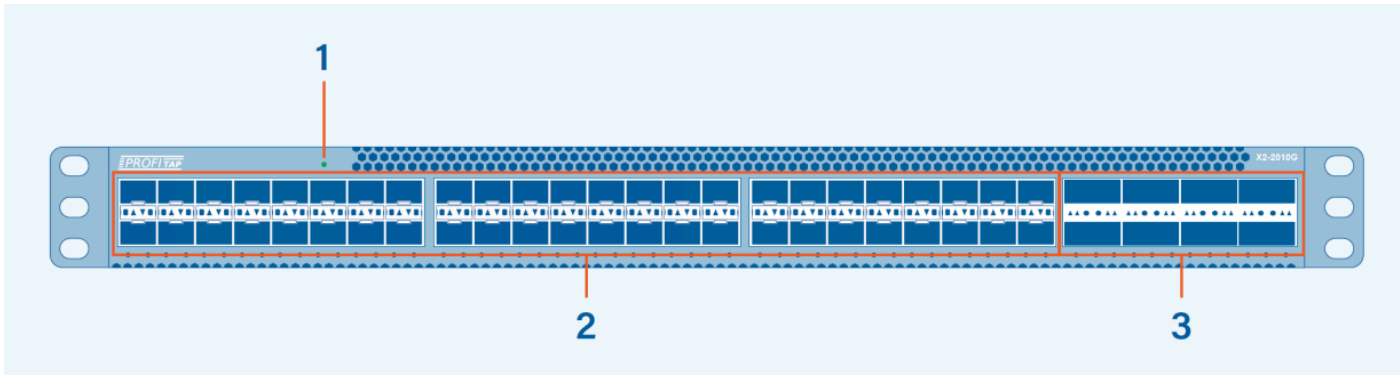
1. Slide the main chassis into the desired rack location.
2. Secure the chassis using the supplied screws.
3. Make sure the rack is grounded properly.

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

### 1.4.4. Technical and Electrical Specifications

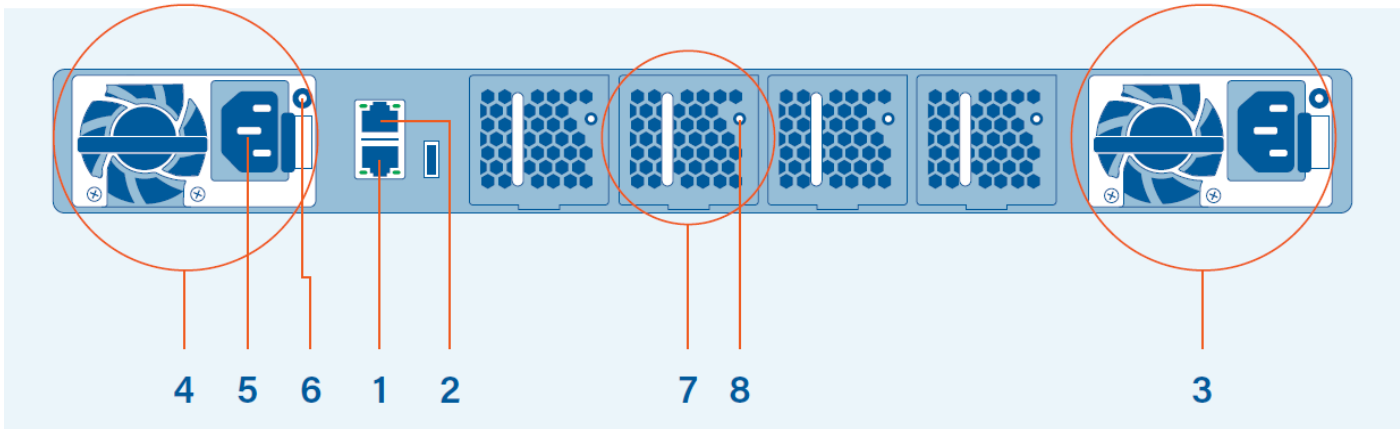
- 2.4 GHz Intel Xeon 8-core 64-bit CPU
- 2.0 Tbps ASIC
- 2 x 800 W, 100-240 VAC, 50-60 Hz, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy)
- Typical power consumption: 600 W
- Cooling: 3N + 1 redundant fans
- Operating temperature: 0°C to 40°C — 32°F to 104°F
- Operating humidity: 10% to 85%, non-condensing
- Dimensions (WxDxH): 440 x 485 x 44 mm — 17.32 x 19.09 x 1.73 in
- Safety: FCC, CE, RoHS 6

1.4.5. Front View



1	System status LED	3	40/100G QSFP28 ports (49-56)
2	10/25G SFP28 ports (1-48)		

1.4.6. Rear View



1	Serial management port	5	AC Power Connector (with Plug Retainer)
2	Ethernet management port	6	PSU status LED
3	PSU1	7	Hot swappable fan module
4	PSU2	8	Fan LED

### 1.4.7. LED Functionality

LED Function	LED State	Description
System status LED	Green	System operating normally
	Blinking green (0.5 Hz)	Bootloader execution
	Blinking green (4 Hz)	BIOS ready
	Amber	One of the PSUs is unpowered or caution event (ex: one FAN fail in OS)
	Red	Thermal trip or critical event (ex: two or more FANS fail in OS)
PSU status LED	Green	PSU operating normally
	Blinking green	PSU in standby mode
	Amber	PSU fault
	Off	AC cable not connected
Fan status LED	Green	Fan operating normally
	Red	Fan fault
	Off	Not connected
QSFP28 100G/40G mode status LED	Green	100G link
	Blinking green	100G activity
	Amber	40G link
	Blinking amber	40G activity
QSFP28 split out 25G mode status LED	Green	25G link
	Blinking green	25G activity
QSFP28 split out 10G mode status LED	Amber	10G link
	Blinking amber	10G activity
SFP28 25G mode status LED	Green	25G link
	Blinking green	25G activity
SFP28 10G mode status LED	Amber	10G link
	Blinking amber	10G activity

## 1.5. X2-3200G

### 1.5.1. Package Contents

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

- 1 x X2-3200G main unit
- 2 x C13 AC power cord
- 1 x RJ45 female to 9-pin serial adapter
- 1 x USB/RJ45 adapter cable
- 1 x RJ45 cable
- 1 x rack mounting kit (front and rear brackets, screws)
- Quick start guide

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

### 1.5.2. 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.

### 1.5.3. Installation in a Rack

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

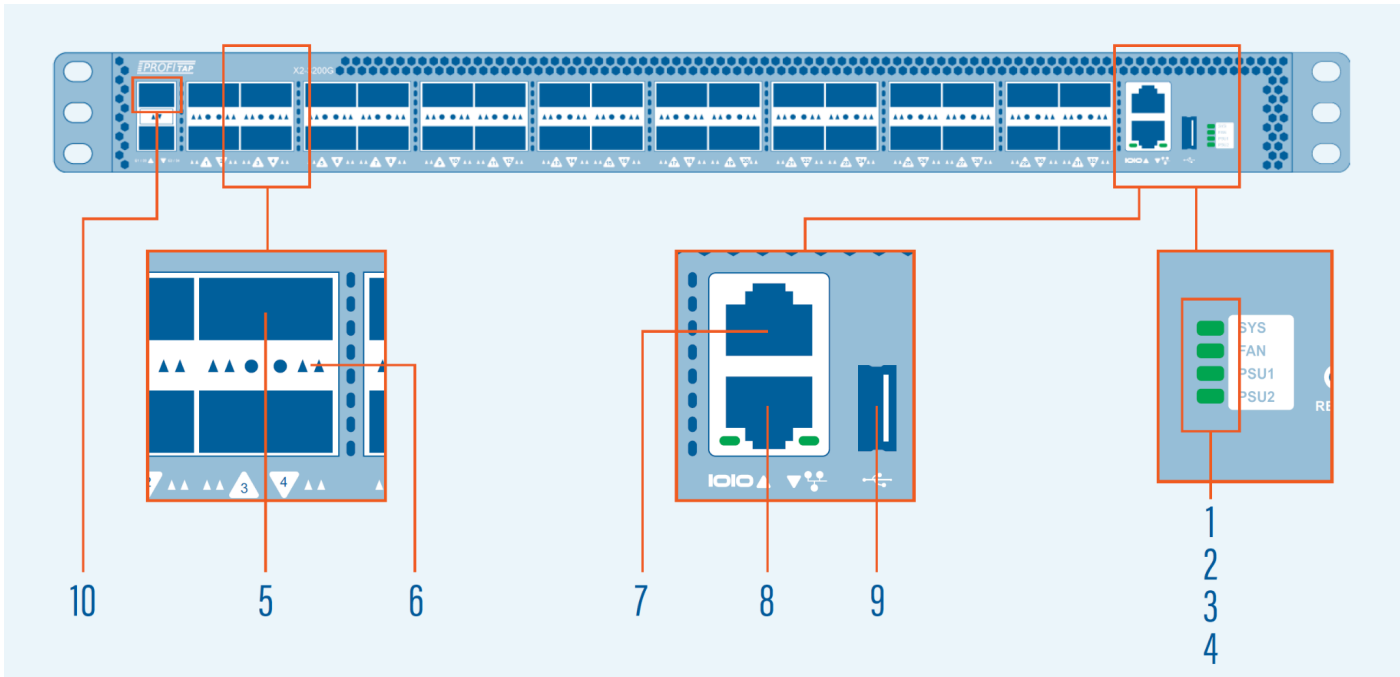
1. Slide the main chassis into the desired rack location.
2. Secure the chassis using the supplied screws.
3. Make sure the rack is grounded properly.

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

### 1.5.4. Technical and Electrical Specifications

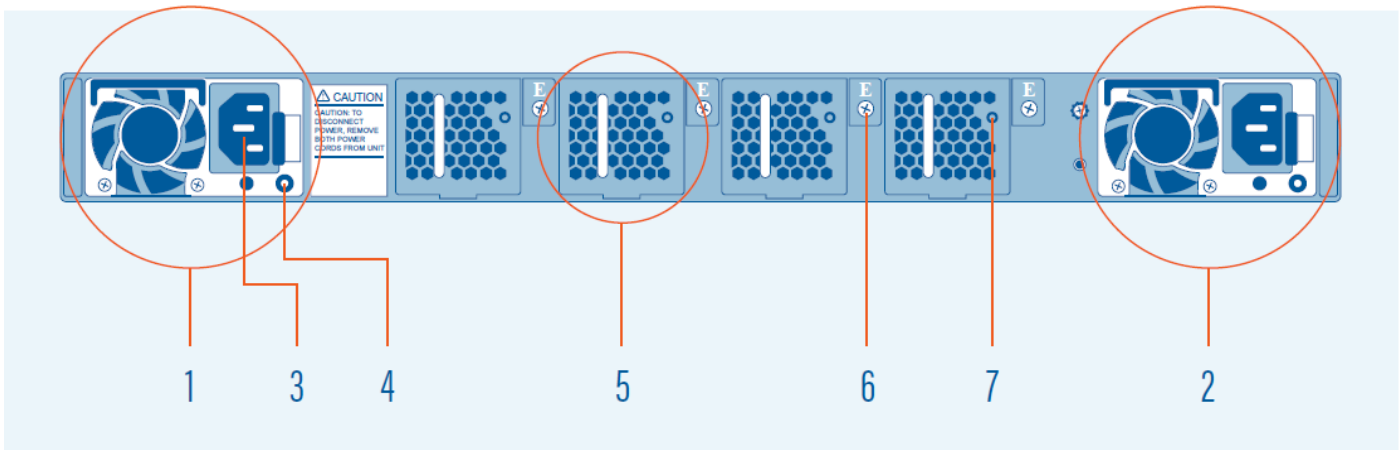
- 2.2 GHz Intel Xeon quad-core 64-bit CPU
- 3.2 Tbps ASIC
- Rigid metal enclosure, black oven painted
- 2 x 550 W, 100-240 VAC, 50-60 Hz, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy)
- Typical power consumption: 350 W
- Maximum heat dissipation: 1650 BTU/hr
- Cooling: 4N + 1 redundant fans
- Operating temperature: 0°C to 45°C — 32°F to 113°F
- Operating humidity: 20% to 95%, non-condensing
- Dimensions (WxDxH): 440 x 430 x 44 mm — 17.32 x 16.93 x 1.73 in
- Safety: FCC, CE, RoHS 6
- MTBF: 188423 hours

1.5.5. Front View



1	System status LED	6	QSFP28 port activity LED
2	Fan status LED	7	Serial management port
3	PSU1 status LED	8	Ethernet management port
4	PSU2 status LED	9	USB port
5	QSFP28 ports (1–32)	10	E1/33 time sync SFP port (1G)

1.5.6. Rear View



1	PSU1	5	Hot swappable fan module
2	PSU2	6	Fan module screw
3	AC power connector (with plug retainer)	7	Fan status LED
4	PSU status LED		

### 1.5.7. LED Functionality

LED Function	LED State	Description
System status LED	Green	System is functioning properly
	Orange	System warning
Fan status LED	Off	Fans not initialized
	Green	Fans operating normally
	Orange	Fan fault: check the back of the unit to see which fan is the faulty one
PSU1/PSU2 status LED	Off	Power is not supplied to the device
	Green	PSU is operating normally
	Orange	Signal issues: <ul style="list-style-type: none"> <li>- PSU is present, but no current is supplied</li> <li>- Fan Lock</li> <li>- OTP: Over temperature Protection</li> <li>- OCP: Over Current Protection</li> <li>- OVP: Over Voltage Protection</li> <li>- UVP: Under Voltage Protection</li> </ul>
QSFP28 port LED	Off	No link
	Green	100G link
	Blinking Green	100G activity
	Yellow	40G link
	Blinking Yellow	40G activity



## 1.6. X2-6400G

### 1.6.1. Package Contents

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

- 1 x X2-6400G main unit
- 2 x C13 AC power cord
- 1 x RJ45 female to 9-pin serial adapter
- 1 x USB/RJ45 adapter cable
- 1 x RJ45 cable
- 1 x rack mounting kit (front and rear brackets, screws)
- Quick start guide

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

### 1.6.2. 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.

### 1.6.3. Installation in a Rack

The unit can be mounted in a standard 19" (2U) rack using the provided mounting brackets.

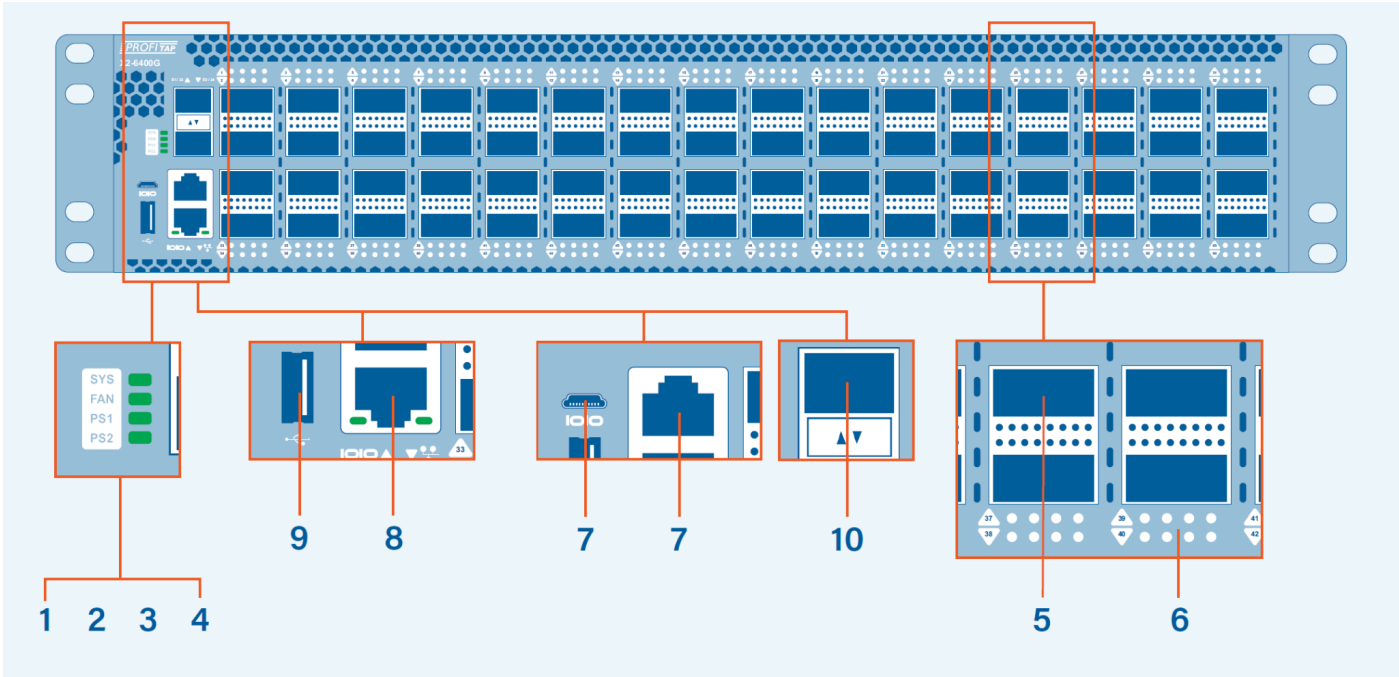
1. Slide the main chassis into the desired rack location.
2. Secure the chassis using the supplied screws.
3. Make sure the rack is grounded properly.

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

### 1.6.4. Technical and Electrical Specifications

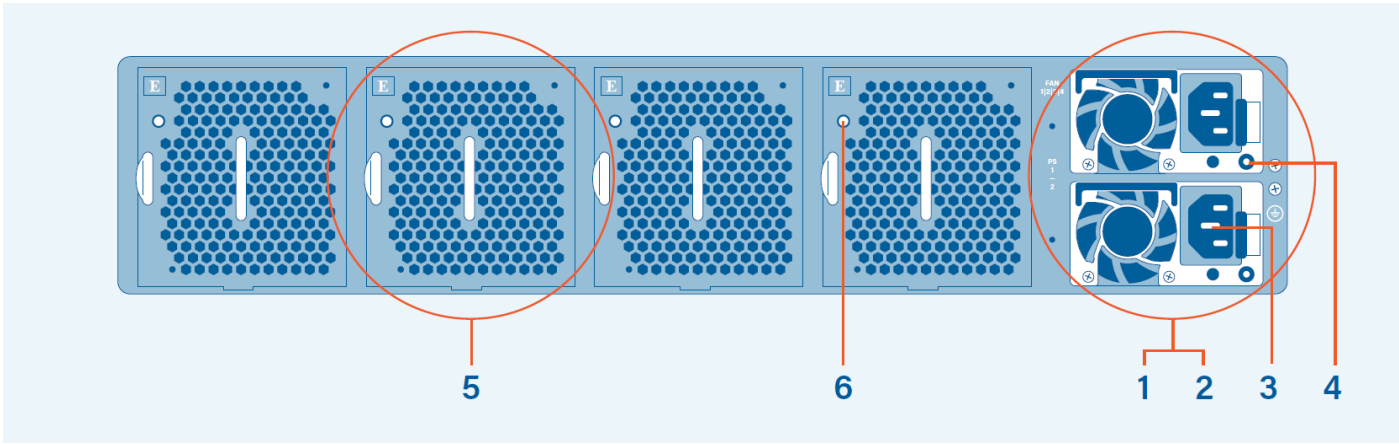
- 2.2 GHz Intel Xeon quad-core 64-bit CPU
- 6.4 Tbps ASIC
- Rigid metal enclosure, black oven painted
- 2 x 1200 W, 100-240 VAC, 50-60 Hz, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy)
- Typical power consumption: 730 W
- Cooling: 4N + 1 redundant fans
- Operating temperature: 0°C to 45°C — 32°F to 113°F
- Operating humidity: 20% to 95%, non-condensing
- Dimensions (WxDxH): 440 x 430 x 88 mm — 17.32 x 16.93 x 3.46 in
- Safety: FCC, CE, RoHS 6

1.6.5. Front View



1	System status LED	6	QSFP28 port activity LED
2	Fan status LED	7	Serial management port
3	PSU1 status LED	8	Ethernet management port
4	PSU2 status LED	9	USB port
5	QSFP28 ports (1–64)	10	E1/65 time sync SFP port (1G)

1.6.6. Rear View



1	PSU1	4	PSU status LED
2	PSU2	5	Hot swappable fan module
3	AC power connector (with plug retainer)	6	Fan status LED

### 1.6.7. LED Functionality

LED Function	LED State	Description
System status LED	Green	System is functioning properly
	Orange	System warning
Fan status LED	Off	Fans not initialized
	Green	Fans operating normally
	Orange	Fan fault: check the back of the unit to see which fan is the faulty one
PSU1/PSU2 status LED	Off	Power is not supplied to the device
	Green	PSU is operating normally
	Orange	Signal issues: - PSU is present, but no current is supplied - Fan Lock - OTP: Over temperature Protection - OCP: Over Current Protection - OVP: Over Voltage Protection - UVP: Under Voltage Protection
QSFP28 port LED	Off	No link
	Green	100G link
	Blinking Green	100G activity
	Yellow	40G link
	Blinking Yellow	40G 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.

**X2-Series** devices are equipped with status and activity LEDs. For more details on status LEDs color and coding, see chapters [1.3.7](#) (X2-2000G), [1.4.7](#) (X2-2010G), [1.5.7](#) (X2-3200G), or [1.6.7](#) (X2-6400G).

## 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

Connect through the serial port using the following settings: 115200 baud rate, 8 bit, no parity, 1 bit stop. Login 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 **X2-Manager** (web-based interface) at: **https://<ip\_addr>**

**X2-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

**X2-Series** devices can be administered either in CLI mode or in a graphical web-based interface called **X2-Manager**, 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:** 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.

The *Configure Filtering* button allows the filtering mode to be set to either *IPv6 Source and/or Destination Filtering* (default) or *MLPS Filtering*.

### 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. IPv6 Source and Destination Addresses filtering is only possible if the Rule Set is configured with *IPv6 Addresses Filtering* (*Configure Filtering* button on the Rule Set page).

- **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. This can be done by clicking the *L4 Ports Group Edit* button, creating a group, naming it, and deciding how the port group will appear, by listing the exact ports followed by comma, or by selecting a range of allowed ports. After creating the group, the desired filter needs to be selected by typing/selecting the group name in the **Source/Destination Ports Groups** subsection.

- **VLAN Tags**

Can be used for filtering as outer/inner VLAN. This can be done by clicking the *VLAN ID Group Configuration* button, creating a group, naming it, and deciding how the port group will appear, by listing the exact ports followed by comma, or by selecting a range of ports. After creating the group, in order to be activated, the desired filter needs to be selected by typing the group name in the **Outer/Inner VLAN ID** subsection. The selections cannot overlap.

- **MPLS Labels**

This section can be used to filter on MPLS labels. Up to six MPLS labels can be specified. Note that each label will match only with the one in the specified position. This option is only available if the Rule Set is configured with *MPLS Filtering* enabled (*Configure Filtering* button on the Rule Set page).

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

#### 4.4.3. Rule - Advanced

The **Advanced** tab allows the configuration of options that can be applied to the traffic in outbound, as well as advanced filtering:

- **Strip VLAN Tag/Add VLAN Tag**  
A VLAN header with the specified **VLAN ID** can be added. The new tag is always added externally. Packet EtherType fields are guaranteed to be updated automatically. If VLAN Strip is enabled, the outer VLAN tag is removed. If both options are enabled at the same time, the external VLAN ID tag will be replaced by the one specified.
- **Strip MPLS Tag**  
Remove either the outer MPLS label or all MPLS labels in all packets passing through the rule.
- **Slicing**  
Truncates the packets to the specified size (between 64 and 9215 bytes).
- **MAC Address Spoofing**  
This function allows the source and/or destination MAC addresses to be replaced with the specified ones.
- **Tunnel Filter**  
Filter traffic encapsulated in the following tunneling protocols:
  - GTP-IP;
  - VXLAN;
  - ERSPAN.
- **Tunnels Stripping**  
Allows the user to remove tunnel headers for the following protocols:
  - IP in IP;
  - GRE-TAP;
  - ERSPAN;
  - VXLAN;
  - Teredo.
- **Traffic Tunneling**  
Encapsulate the traffic passing through the rule in an ERSPAN type 2, ERSPAN type 3, or GRE tunnel. The address fields and optionally the tunnel VLAN used in the tunnel must be specified. If ERSPAN type 3 tunnel is selected, the packets will also include a nanosecond precision timestamp. It is also possible to truncate the tunneled traffic by specifying the maximum size for each packet in bytes.

#### 4.4.4. 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.

It is possible to change the traffic distribution strategy via the *Configure* button in the *Load Balancing Group* section of the Rule Set. In this view, it is possible to select between:

- **Round Robin:** Traffic will be distributed equally across all of the output ports;
- **Flow Hash:** Traffic will be distributed based on the selected headers fields.

Note that if *Flow Hash* is used with source AND destination options enabled for L3 or L4, the unit will make sure to distribute the traffic maintaining flow symmetry and consistency.

#### 4.4.5. Ingress Rules

On the X2-Series, 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 options are:

- **VLAN Tag:** Adds a VLAN tag to all traffic incoming in the selected port;
- **VLAN Strip:** Removes a VLAN tag from all traffic incoming in the selected port;
- **IPv4 Address:** Allows the device interface to receive routed traffic in an IPv4 network;
- **GRE-TAP Tunnel Stripping:** All incoming GRE-TAP traffic will be automatically stripped of the external tunnel;
- **GRE-TAP Tunnel Termination:** When enabled, users can associate a MAC and IPv4 Address to the selected interface. This will be available in the network and can be used to direct a GRE-TAP (Ethernet over GRE) tunnel in the NPB interface. The traffic will be decapsulated and processed further using the other user rules;
- **ERSPAN Tunnel Stripping:** All incoming ERSPAN traffic will be automatically stripped of the external tunnel;
- **ERSPAN Tunnel Termination:** Terminates and decapsulates an ERSPAN tunnel directed to the configured IPv4 address;
- **VXLAN Tunnel Stripping:** All incoming VXLAN traffic will be automatically stripped of the external tunnel;
- **VXLAN Tunnel Termination:** Terminates and decapsulates a VXLAN tunnel directed to the configured IPv4 address and UDP port.

#### 4.4.6. Time Synchronization (X2-3200G, X2-6400G)

This section can be used to configure the Time Synchronization port (see [1.5.5](#) for X2-3200G and [1.6.5](#) for X2-6400G). This interface only operates with 1G SFP modules.

The system works as a PTPv2 slave clock and will use the synchronized time to perform high quality nanosecond precision traffic timestamping for ERSPAN type 3 encapsulated traffic (see *Traffic Tunneling* in [4.4.3](#)).

Click the *Configure Time Synchronization* button to configure the MAC and IP address associated with the port. Information about the internal synchronization process and its performance is then available from the Rule Set page's *PTPv2 Time Synchronization* table.

The *System Synchronization State* section provides information about the current state of synchronization. The possible states are:

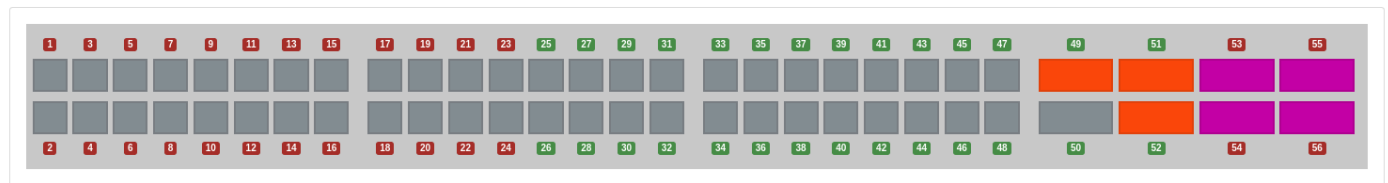
- **Inactive:** Synchronization port is disabled;
- **Freerun:** Synchronization has not completed correctly and the system is timestamping with its own clock rate;
- **Progress:** System is synchronizing against a local master clock and is trying to rearrange its clock frequency to follow the master;
- **Locked:** System is synchronized against the local master clock and the timestamping clock has an average error within  $\pm 500$  ns.

This view also provides information about the clock offset against the master clock and the time server's IP address.

#### 4.4.7. Traffic Deduplication

X2-Series NPBs are capable of performing traffic deduplication (license required). This feature is useful when the same packets are captured from different tapping points and aggregated in the packet broker.

Traffic Deduplication



■ Deduplication Hardware Table A [1-24 and 53-56]

■ Deduplication Hardware Table B [25-48 and 49-52]

✕ Cancel

✓ Confirm

This feature can be controlled via the *Configure Deduplication* button in the *traffic management* view. Clicking this button opens a new view, allowing the user to select the interfaces on which the device will check for duplicate packets. The deduplication configuration view displays different colors for ports wired to the different hardware tables that the device is using to compare the incoming packets. Only traffic incoming on ports wired to the same hardware table (i.e. ports displayed with the same color) is evaluated for deduplication.

Note that the traffic identification will happen in the interface **ingress**, using the following fields:

- IPv4/6: Source and Destination Addresses;
- IPv4/6: Protocol/Next Header field;
- IPv4 Identification;
- TCP/UDP/SCTP: Source and Destination ports (or relative offset in fragmented traffic);
- TCP/UDP/SCTP: Checksum.

## 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 level mappings (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. Profitap Supervisor

Profitap Supervisor can be used as a centralized authentication facility for all 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 X2-Series 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 X2-Series device will stop reaching to the Supervisor for authentication.

The Profitap Supervisor Authentication is supported for GUI, CLI, and REST API access.

#### 4.5.5. Custom Authentication Configuration

X2-Series products 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 either the *Users*, *TACACS+*, *RADIUS*, or *Profitap Supervisor* 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+, and Supervisor methods, this means that no server is responding (or no server is programmed). If only one of the registered RADIUS/TACACS+ 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.

## 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.

**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://x2series.profitap.com/img/> for X2-2010G, X2-3200G and X2-6400G, and at <https://x2series.profitap.com/x2-2000g/> for X2-2000G.

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 (v1/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 X2-Series 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

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

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

General settings for the TACACS+ authentication method.

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

```
.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.	
<code>--timeout</code>	1-3	Waiting time for response from the server, in seconds.	<code>--timeout 1</code>

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

General settings for the RADIUS authentication method.

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

```
.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.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

<code>--password</code>	string	The user account's password. Requires 8 characters, one letter uppercase, one letter lowercase, one digit.	<code>--password Password1</code>
<code>--role</code>	admin/user/viewer	The user account's privileges.  <b>admin:</b> full control, limitless administration and system update; <b>user:</b> create and set rules, aggregate and filter traffic, and port configuration; <b>viewer:</b> view only: settings, statistics, active rules.	<code>--role admin</code>
<code>--username</code>	string	The user account's unique name.	<code>--username newuser</code>

```
.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 <i>user</i> .	--date 2008-10-31
--servers	server1,server2,...	The list of NTP servers used to set the date and time if --type is set to <i>ntp</i> .	--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 <i>user</i> .	--time 01:23:45
--timezone	timezone	The time zone used to set the time if --type is set to <i>ntp</i> .  Use <code>.system.date.show_available_timezones</code> 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	<b>disable</b> disables the management interface.  <b>dhcp</b> sets the IP acquisition mode to DHCP IPv4/IPv6.  <b>static</b> sets the IP acquisition mode to STATIC IPv4/IPv6.  <b>dhcp_v4</b> sets the IP acquisition mode to DHCP IPv4.  <b>dhcp_v6</b> sets the IP acquisition mode to DHCP IPv6.  <b>eui-64</b> 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 <i>static</i> .	--ip 127.0.0.1

<code>--prefix</code>	IPv4 CIDR prefix	Sets the management interface's IPv4 CIDR prefix, if <code>--type</code> is set to <i>static</i> .	<code>--prefix 24</code>
<code>--gateway</code>	IPv4 address	Sets the management interface's gateway's IPv4 address, if <code>--type</code> is set to <i>static</i> .	<code>--gateway 192.168.1.1</code>
<code>--dns</code>	IPv4 address	Sets the management interface's first DNS's IPv4 address, if <code>--type</code> is set to <i>static</i> .	<code>--dns 8.8.8.8</code>
<code>--dns2</code>	IPv4 address	Sets the management interface's second DNS's IPv4 address, if <code>--type</code> is set to <i>static</i> .	<code>--dns2 8.8.8.8</code>
<code>--ip_v6</code>	IPv6 address	Sets the management interface's IPv6 address, if <code>--type</code> is set to <i>static</i> or <i>eui-64</i> .	<code>--ip_v6 ::1</code>
<code>--prefix_v6</code>	IPv6 CIDR prefix	Sets the management interface's IPv6 CIDR prefix, if <code>--type</code> is set to <i>static</i> .	<code>--prefix_v6 64</code>
<code>--gateway_v6</code>	IPv6 address	Sets the management interface's gateway's IPv6 address, if <code>--type</code> is set to <i>static</i> or <i>eui-64</i> .	<code>--gateway_v6 FE80::1</code>
<code>--dns_v6</code>	IPv6 address	Sets the management interface's first DNS's IPv4 address, if <code>--type</code> is set to <i>static</i> or <i>eui-64</i> .	<code>--dns_v6 2001:4860:4860::88 88</code>
<code>--dns2_v6</code>	IPv6 address	Sets the management interface's second DNS's IPv4 address, if <code>--type</code> is set to <i>static</i> or <i>eui-64</i> .	<code>--dns2_v6 2001:4860:4860::88 88</code>
<code>--hostname</code>	string	Sets the management interface's hostname.	<code>--hostname hostname</code>

## `.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	<p>The URL of the new license to install on the device (HTTP/HTTPS/FTP).</p> <p>If server credentials are required, they need to be passed as part of the url in the form <code>ftp://user:password@server/file</code>. 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. <code>`@`</code> will be <code>`%40`</code>). A list is available at <a href="https://dev.w3.org/html5/html-author/charref">https://dev.w3.org/html5/html-author/charref</a></p>	--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 <i>true</i> , 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 --version is set to v2c.	--community 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 ( <code>--security</code> set to <i>auth</i> or <i>priv</i> ).	--auth sha
--auth_pass	string	The passphrase for user authentication ( <code>--security</code> set to <i>auth</i> or <i>priv</i> ).	--auth_pass userpwd1
--priv	des/aes	The encryption protocol ( <code>--security</code> set to <i>priv</i> ).	--priv des
--priv_pass	string	The encryption passphrase ( <code>--security</code> set to <i>priv</i> ).	--priv_pass userpwd2

<code>--security</code>	<code>noauth/auth/priv</code>	Selects the requested security policy. Note that requests sent by `noauth` users will be performed in clear over the network.	<code>--security priv</code>
<code>--username</code>	<code>string</code>	Sets the new user's name.	<code>--username user1</code>

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

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

```
.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	<p>The URL of the firmware package to install on the device (HTTP/HTTPS/FTP).</p> <p>If server credentials are required, they need to be passed as part of the url in the form <code>ftp://user:password@server/file</code>. 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. <code>@`</code> will be <code>%40`</code>). A list is available at <a href="https://dev.w3.org/html5/html-author/charref">https://dev.w3.org/html5/html-author/charref</a></p>	--url ftp://user:password@server/file

## **6. Integrations**

### **6.1. RESTful API Support**

To integrate with tools, controllers and other IT systems, the X2-Series offers programmatic access to the platform through HTTP RESTful API support.

The latest REST API documentation and examples can be downloaded from the [X2-Manager's Support tab](#) or accessed at <https://x2series.profitap.com/api/>

### **6.2. Ansible Support**

X2-Series devices can be also controlled and configured using ansible playbooks. The necessary libraries and example playbooks are available in the [X2-Manager'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*

This publication, including all photographs and illustrations, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

## *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](http://www.profitap.com)

© 2024 Profitap — v2.3