PROFITAP

XX-720G PACKET BROKER

INSTALLATION AND CONFIGURATION MANUAL

BRINGING CLARITY INTO NETWORKS.

ANYTIME. ANYWHERE.

For any questions, technical or otherwise, please contact our customer support through our website:

www.profitap.com

or by email:

info@profitap.com

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

http://www.profitap.com/resource-center/

TABLE OF CONTENTS

INSTALLATION

1. UNPACKING & INSTALLATION

1.1 Unpacking

Carefully unpack all the items supplied with the XX-720G and retain the packaging for later use:

- ◉ 1 x XX-720G main unit
- ◉ 2 x C13 AC power cord
- ◉ 1 x Mini-USB to RJ45 male serial cable
- ◉ 1 x Mini-USB to RJ45 female serial cable
- ◉ 1 x RJ45 female to 9-pin serial adapter
- ◉ 1 x rack mounting kit (including front & rear brackets and the necessary screws)
- ◉ 4 x rubber foot with adhesive patch
- ◉ Quick Start Guide flyer
- ◉ Installation and Configuration Manual booklet
- ◉ SFP modules not included (can be ordered separately)

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

1.2 Installation as Stand-alone

The unit can be installed as a stand-alone unit by attaching the provided rubber feet to the bottom panel of the switch, offering scratch protection and preventing slipping.

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 Installation in a Rack

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

a) Slide the main chassis into the desired rack location.

b) Secure the chassis appropriate rack screws.

c) Make sure the rack is grounded properly.

2. HARDWARE OVERVIEW

The XX-720G is an up-to-date versatile solution, designed for aggregation, filtering and routing of multiple 1G/10G/40G inputs, used in very high bandwidth port monitoring and analysis scenarios.
Depending on the offering, the unit can be supplied with either a limited number of enabled ports or with full functionality:

- XX-720G-242-AC: HD NPB, 24 x 10G cages + 2 x 40G cages, 2 power supplies (AC)
- XX-720G-486-AC: HD NPB, 48 x 10G cages + 6 x 40G cages, 2 power supplies (AC)
- XX-720G-242-DC: HD NPB, 24 x 10G cages + 2 x 40G cages, 2 power supplies (DC)
- XX-720G-486-DC: HD NPB, 48 x 10G cages + 6 x 40G cages, 2 power supplies (DC)

The unit can be managed via CLI by directly connecting it to a computer or by using the XX-Manager web interface, after the initial CLI setup has been completed.

The unit holds the following ports:

- 48 x SFP+ (1G/10G) ports and 6 x QSFP+ (40G) ports, supporting optical transceivers, active optical cables or direct-attached cables to connect the ports to the hosts
- 1 x Ethernet management port used to access the switch via an RJ45 Ethernet cable
- 1 x serial management port (mini-USB like) to connect to a PC for the initial configuration or for resetting the users
- 1 x USB port to load the configuration files or OS from a USB storage device

2.1 Technical and Electrical Specifications

- 2.4GHz Intel quad-core CPU
- 1280 Gbps ASIC
- Rigid metal enclosure, black oven painted
- AC model: 2 x 550W, 100-240 VAC, 50-60 Hz, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy)
- DC model: 2 x 800W, -40–-60 VDC, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy)
- Typical power: 285W
- Cooling: 4 redundant (N+1) hot-swappable fans
- Operating temperature: 0°C to 45°C
- Operating humidity: 20% to 95%, non-condensing
- Dimensions (DxWxH): 410 x 440 x 44 mm

2.2 Front View
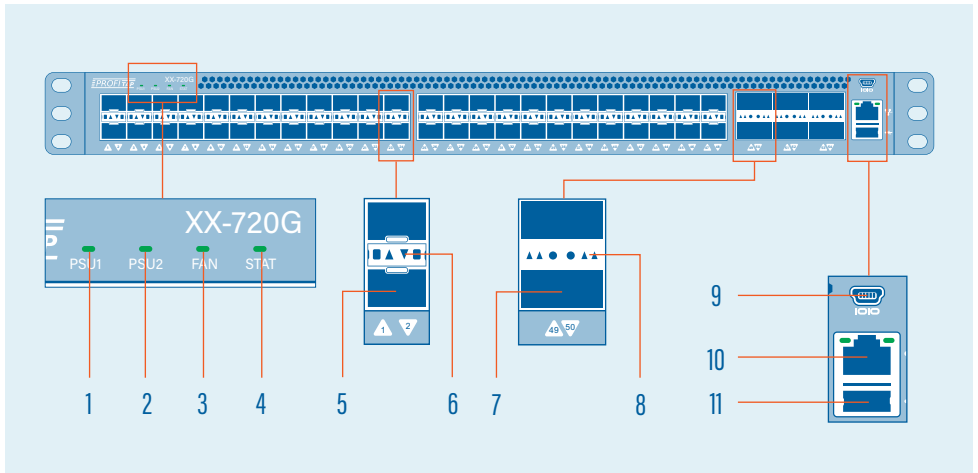
1	PSU1 status LED	**7**	QSFP+ port (49-54)
2	PSU2 status LED	**8**	QSFP+ port activity LED
3	Fan status LED	**9**	Serial management port
4	System status LED	**10**	Ethernet management port
5	SFP+ port (0-48)	**11**	USB port (firmware updating port)
6	SFP+ port activity LED		

2.3 Rear View
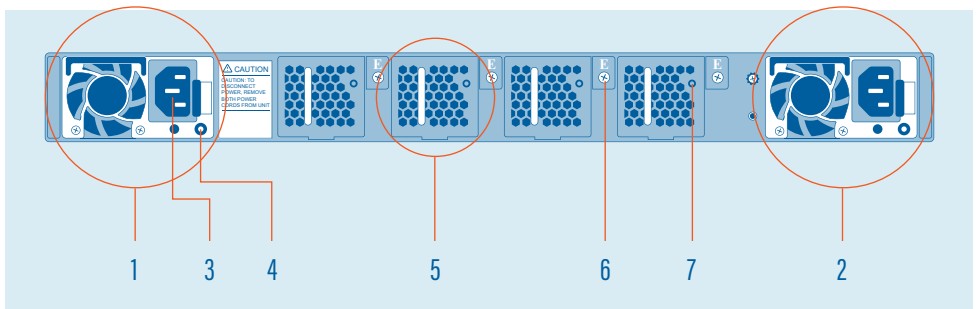
1	PSU1	**5**	Hot-swappable FAN module
2	PSU2	**6**	FAN module screw
3	AC Power Connector (with Plug Retainer)	**7**	FAN status LED
4	PSU status LED		

2.4 Supported Cables and Transceivers

The following table describes all cables and transceivers supported by the XX-720G Packet Broker.

DISTANCE	DESCRIPTION	NOTE
1m	1/10G Direct Attach Copper (DAC) cable	SFP+ to SFP+
	40G Direct Attach Copper (DAC) cable	QSFP+ to QSFP+
	40G DAC Fan Out cable	QSFP+ to 4x SFP+
3m	1/10G Direct Attach Copper (DAC) cable	SFP+ to SFP+
	40G Direct Attach Copper (DAC) cable	QSFP+ to QSFP+
	40G DAC Fan Out cable	QSFP+ to 4x SFP+
5m	1/10G Direct Attach Copper (DAC) cable	SFP+ to SFP+
	40G Direct Attach Copper (DAC) cable	QSFP+ to QSFP+
	40G DAC Fan Out cable	QSFP+ to 4x SFP+
7-100m	1/10G Direct Attach Copper (DAC) cable	SFP+ to SFP+
	40G Direct Attach Copper (DAC) cable	QSFP+ to QSFP+ 850nm, MMF
	40G DAC Fan Out cable	QSFP+ to 4x SFP+
10Gbps up to 20m	10GBASE-T Transceiver	SFP+
10-40Gbps up to 100m	10GBASE-SR SFP+ Transceiver Optic	SFP+, 850nm, LC
	40GBASE-SR4 QSFP+ Transceiver Optic (MPO)	QSFP+, 850nm, MM
10-40Gbps up to 10km	10GBASE-LR SFP+ Transceiver Optic	SFP+, 1310nm, LC
	40GBASE-LR4 QSFP+ Transceiver Optic (LC)	QSFP+, 1290-1310nm, SM

2.5 LED Functionality

LED FUNCTION / STATE		MEANING / CONTROL
Power LED status for PSU1 and PSU2	OFF	Power is not supplied to the device.
	Green	PSU is operating normally.
	Amber	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
Fan LED Status	Green	Fan is operating normally
	Amber	Fan is faulty. Check the back of the unit to see which fan is the faulty one.
System LED Status	Green	System is functioning properly
	Amber	System warning
Link/Speed LED mode for ports 0-48 (SFP+)	OFF	No link is established on the port
	Green	Active link @ 10Gbps
	Blinking Green	Data is transmitted @ 10Gbps
	Yellow	Active link @ 1Gbps
	Blinking Yellow	Data is transmitted @ 1Gbps
Link/Speed LED mode for ports 49-54 (QSFP+)	OFF	No link is established on the port
	Green	Active link @ 40Gbps

LED FUNCTION / STATE		MEANING / CONTROL
Link/Speed LED mode for port 49-54 (QSFP+)	Blinking Green	Data is transmitted @ 40Gbps

3. CONNECTING POWER AND START-UP

The system powers on when one of the power supplies is connected to the main power. The use of both power supplies is recommended to ensure fail-safe operation.

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.

The XX-720G is equipped with status and activity LEDs. For more details on status leds color and coding, please see 2.5 Led Functionality chapter.

4. INITIAL ACCESS TO XX-720G

The first-time access to the system can only be done through the serial connection, using the supplied cable and adapters. Using any terminal software, use the following connection settings: 115200 baud rate, 8 bit, no parity, 1 bit stop.

Login, using the following credentials:
- Username: profitap
- Password: profitap

Follow the prompt to create an administrator account. After creating the new admin user, the session will close. The factory default user (profitap) remains active for direct connections to the unit's serial management port.

To reset the users database, run the following command:

```
.> system.users.reset
```

4.1 Configuring the Ethernet Management Port

After logging in with the newly created admin account, the Ethernet management port can be configured by running the following command:

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

Depending on user's requirements, the IP can be set either dynamic (DHCP) or static (custom IP). Please follow the instructions for configuring the preferred option. After the configuration is complete, the system is accessible via SSH and **XX-Manager** (web-based interface) at https://assigned_IP.

XX-720G can also be directly connected to a computer through its Ethernet management port. In this case, manual IP policy must be applied for both the unit and the computer.

> ► **Note:** If the computer network interface is only 10/100Mbit capable, a twisted pair special cable must be used instead of a normal patch cable.

For security reasons, an SSL certificate is pre-installed. A new certificate can be generated or imported. See CLI Administration - System for more details.

CONFIGURATION

1. WEB ADMINISTRATION

The XX-720G can be administered either in CLI mode or in a graphical web-based interface, called XX Manager, which is OS and platform independent.

> ► Note: XX Manager can only administer and monitor a single XX-720G unit.

Grouped by functionality, there are six menu tabs displayed in the left side of the screen:

- ◉ Device Status
- ◉ Port Management
- ◉ Global Statistics

- ◉ Traffic Rules
- ◉ User Settings
- ◉ Administration

1.1 Device Status

The Device Status page displays the device status and sensors information.

> ► Note: Without logging in, this menu is the only one available.

The following information is displayed:

- ◉ Revision information (model number, sw/hw revision)
- ◉ Administrator information (user name, phone number, email address)
- ◉ Date and time information
- ◉ Network details
- ◉ Sensors (the air temperature is measured in proximity of the fans block, the system temperature is measured within the forwarding plane chip).
- ◉ Temperature readings for CPU, system and external air.

1.2 Ports Management

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

Configuration of a port is done by clicking on one of the port and select one of the following entries:

- ◉ **Status:** Displays additional information on the selected port: the current state of the port, the Tx and Rx bandwidth statistics and the SFP module information (if present).

    - ◉ VLAN tag: allows the user to set an additional header tag to the frames received through the current interface.

    > ► Note: Enabling or disabling tags will momentarily restart the filtering engine, resulting in a brief brake in the output flow.

- ◉ **Enable/Disable:** Allows the user to enable or disable a specific interface.
- ◉ **Speed:** Allows the user to set a specific speed for an individual port. Note that for the SFP+ ports, the user cannot set individual port speeds, given 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.
- ◉ **Split/Unsplit:** (Only for QSFP+ interfaces): this options allows the user to use the 40G interface as a combined set of 4xSFP+ ports. This is necessary in order to use split cables.

- **Reset:** Allows the user to reset the port configuration to the default state:
  - SFP+: Enabled @ 10G speed.
  - QSFP+: Enabled @ 40G speed.

1.3 Statistics

The Statistics page displays specific statistic counters either global or filtered by selected interfaces.

The Ports Statistics tab displays traffic statistics for selected interface(s). Clicking one or more interfaces will highlight them while new column(s) will be added with their respective data stats.

The Global Statistics tab displays global sent and received data as well as traffic rules related counters. The following units are used:

- Rx/Tx Bandwidth: bits per second (bps)
- Received/Sent Octets: number of frames or octets (counter)

The Charts tab displays traffic statistics for selected interface(s) in a graphical representations, highlighting the percentage in Rx and Tx bandwidth for each interface.

1.4 Traffic Rules

The Traffic Rules page allows the administrator logged in users to create custom traffic aggregation, duplication and filtering rules, as well as enable load balancing for multiple interfaces, therefore tailoring the way data flows on each port of the unit. These custom settings can be grouped into Rule Sets and depending on the requirements, a certain Rule Set can be selected as active from the list of existing Rule Sets. The Active Rule Set tab displays the rule-set that is currently active and its details, including the filtered interfaces and the ones linked in load balancing.

The Rules Sets tab displays the list of existing rule-sets, (highlighting the active one), allowing administrator logged in users to activate, configure, delete or create new rule-sets. Only one rule can be active at a time:

- Creating a new rule-set is done by clicking ⊕ Add Rule Sets.
- activating a rule-set is done by clicking ☑
- configuring an existing rule-set is done by clicking ⚙
- renaming an existing rule-set is done by clicking ✏
- deleting an existing rule-set is done by clicking 🗑

After creating a rule-set (which at the beginning is just a name, with no defined rules), one or more rules can be then added, and load balancing can be enabled for two or more interfaces.

The rules define how the traffic will be processed by the packet broker. When creating a new rule, the user will be requested to define the behavior of the rule. The possible options are:

ALLOW: Only the traffic matching the defined filters will be forwarded;

EGRESS DROP: The traffic matching the defined filter will be removed from the stream.

The ports panel in the "Interfaces" tab will allow the user to define which ports need to be used as source for the traffic stream and which ports will work as output. Note that when selecting multiple input ports, the device will aggregate the traffic incoming from the interfaces.

When selecting multiple output ports, the device will replicate the traffic stream to the interfaces. The matching counter option can be used to start a counter monitoring the amount of packets that are matching the defined filter. These counters will be displayed in the Global Statistics tab.

The Filters tab allows configuring the device to only accept traffic responding to specific rules related to its L2, L3 and L4 packet content. In this section, a statistics counter can also be enabled to check how many packets pass the new filter.

FILTER	DESCRIPTION
Packet type	This selection will discard all other types of data but the selected one. Selecting Any Packet, allows all types of data passing through.
MAC Layer	Additional filter: only frames matching MAC details configured in this section will be allowed to pass through.
802.1q VLAN fields	Additional filter: only frames matching VLAN details configured in this section (having a VLAN tag in their header, added before entering the NPB) will be allowed to pass through.
IPv4 layer	Additional filter: only packets matching IPv4 details configured in this section will be allowed to pass through. Only available when Packet type selection is set to Any Packet or IPv4.

FILTER	DESCRIPTION
IPv6 layer	Additional filter: only packets matching IPv6 details configured in this section will be allowed to pass through. Only available when Packet type selection is set to Any Packet or IPv6.
EtherType	Additional filter: only frames matching EtherType details configured in this section will be allowed to pass through. Only available when Packet type selection is set to Any Packet.
Transport Layer	Additional filter: only packets matching Transport layer details configured in this section will be allowed to pass through. Not available when Packet type selection is set to ARP.

► **Note:** If multiple filter fields are configured, only those packets matching all filters will be allowed to pass through.

Mask: Allows a less granular filtering for the MAC, IPs and IDs, accepting packets from a broader region, but still following the same rules as Networking Subnet Mask.

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

The Import / Export tab allows users to import and export one or multiple rule sets, using a .json file as the storage medium. Once a rule set has been imported, the Rule Sets tab will be displayed, showing the additional imported rule sets.

Note: Rule sets names are unique, therefore trying to import rule sets having the same name as the ones already configured in the unit will give an error message. Exported rules should only be imported on XX-720G series network packet brokers.

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

By default, the load balancing port selection algorithm is taking into account all the information included up to Layer 4. This behaviour can be changed by clicking **⚙ Configure**

1.5 User Settings

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

- Admin - full control, limitless administration and system updating.
- User - create & set rules, aggregate and filter traffic.
- Viewer - view only: settings, statistics, active rules.
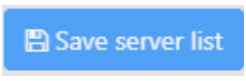
The XX-720G unit supports remote authentication, authorization and accounting services for networked access control through a centralized server, a protocol called TACACS+.

The Tacacs+ tab allows users to configure this type of access, functionality also available using the aaa command in CLI mode.

Tacacs+ servers can be edited, deleted or new ones added in the list of servers. Servers priority can also be changed here, by using the arrow buttons.
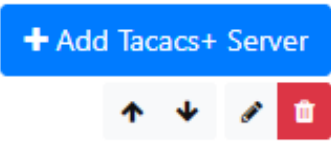
+ Add Tacacs+ Server

> ► Note: After changing the server priority order, users need to click the Save server list button for changes to take effect.

Save server list

Editing or adding a new Tacacs+ server require the following information:

Add Tacacs+ Server

Priority	Login type
1	pap

Hostname	Port
tacacs.profitap.com	49

Secret
••••••

Privilege mapping

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

■ Viewer privilege level ■ User privilege level ■ Admin privilege level
[0-4] [5-12] [13-15]

Confirm Cancel

hostname/port: represents the TACACS+ server hostname or IP address. The default expected port is 49.

login type: represents the type of login used in the server. Possible options are PAP,CHAP and LOGIN.

priority: represents the server priority (1-5) 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. Selecting 1 will configure the current server to be the first one used for authentication. Selecting 5 will configure the current server to be the last one used for authentication.

> ► Note: There cannot be 2 specified servers sharing the same priority.

secret: represents a key string used to encrypt the communication between the server and the client.

Privilege mapping: adjusting the slides modifies the access level granted for different user types:

- ◎ *admin privilege level:* represents a value between 15 and 0 that defines what priv_lvl is requested for an user in order to be granted admin privileges.
- ◎ *user privilege level:* represents a value between 15 and 0 that defines what priv_lvl is requested for an user in order to be granted normal privileges.

> ► Note: user privilege level must be smaller than the value used for admin minimum level.

- ◎ *viewer privileged user:* represents the access level below user privilege level.

> ► **Note:** Enabling TACACS+ server authentication applies for all login methods: serial, ssh and XX-Manager.

1.6 Administration

The Administration page allows users with administrator privileges to change system related settings.

The Setup tab allows editing the administration contact details, the system date and time and the network address.

> ► **Note:** In case the IP is set from static to dynamically allocated (DHCP), the unit address must first be discovered (by searching for its IP address or its hostname) or allocated by the gateway, using a mac allocation 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 chapters 4 and 4.1 for additional details).

The Update tab allows the system to be updated to a new version, from a locally stored update file. After the installation is complete, the system reboots.

Using the SNMP tab, the user will be able to configure the SNMP v1/v2c settings. In this view, the entire service can be set to enable/disable and the SNMP community entries for the GET/WALK requests and the TRAP sinks can be configured.

The Firewall tab includes the ACL setting to control which external addresses can use the device's services. The page includes the selection of the default firewall policies:

Whitelist (default): External requests not matching any ACL entry will be denied;

Blacklist: External requests not matching any ACL entry will be allowed.

In this GUI, it is also possible to define multiple ACL entries. These can be used to explicitly deny or allow external addresses to access the device's services.

The Syslog tab allows the user to view the state of the system logs. From this tab, it is also possible to configure a list of remote syslog servers.

2. CLI ADMINISTRATION

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, for example:

```
.> configuration
```

Useful commands to navigate the console:

- ◉ 'ls' or 'help' for available branches
- ◉ TAB also shows the available branches
- ◉ Ctrl+D cancels a command
- ◉ '.' returns to initial branch
- ◉ '..' returns to previous branch

Commands residing in cascading menus can also be executed from anywhere, outside their normal context menu, using the [.] prefix, provided the path and the command name is known, for example:

```
.status.device.> .configuration.interface.3
.configuration.interface.3.>
```

2.1 Configuration

The Configuration menu is used for administering all the interfaces (ports) in the system. The user first needs to select an interface (from 1 to 72) before administering it:

```
.configuration.> interface 5
.configuration.interface.5.>
```

After this selection is made, the following commands are available:

enable [on/off]   Enables or disables the selected interface.

reset   Deletes all configurations made for the selected interface and restores it to a default state. After issuing the command, the user must confirm it [yes / no].

speed [value]   Sets the port speed. Available values are: Auto, 1G/10G (for the SFP+ ports), 40G (for the QSFP+ ports).

split [on/off]   This option is only available for the QSFP+ interfaces (49-54). If set to on, the interface will be split into 4 interfaces totalling the original speed of the QSFP+ port before the split. If for example, the interface [50] needs to be split and its speed is set to 100G, the following 25G interfaces will be created after the split: 50.1, 50.2, 50.3, 50.4.

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

Tx_disable [parameter] Controls the state of the TX_DISABLE SFP feature, useful in scenarios where BiDi SFP and QSFP modules are used to only receive traffic from an optic tap.
show: Displays the current state of the TX_DISABLE functionality.
on: Stops the TX signal on the SFP module.
off: Restarts the TX signal on the SFP module.

vlan.[parameter] set: allows the user to set an additional header tag to the frames received on the selected interface, particularly useful for aggregation purposes where it's important to know the identity of frames coming from different interfaces which are then aggregated onto a single interface. If "Activate VLAN ID match check on INGRESS" is enabled by answering with "Y", all frames received through the selected interface will be dropped at the INGRESS level (before the routing stage), except those having this tag in their header.

> ► Note: enabling tags will momentarily restart the filtering engine and will have as effect a brief brake in the output flow.

show: Displays the tag status for the selected interface.
disable: Removes the tag on the selected interface. After issuing the command, the user must confirm it [yes / no].

> ► Note: enabling tags will momentarily restart the filtering engine and will have as effect a brief brake in the output flow.

transceiver   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.

2.2 Statistics

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

counter   Displays the counters enabled in 1.4 Traffic Rules -> Match Counter feature.

global.[show/reset]   Displays or resets the following global statistics: Bytes received, Bytes sent, packets received, packets sent.

interface.[show/reset].[interface]   Displays or resets the full statistics for a specified interface. If instead of an interface number, all parameter is used instead, full statistics will be displayed or reset for all interfaces.

> ► Note: The number of portID might exceed the expected number of 54, because the system counts the split interfaces individually.

2.3 Status

The Status menu is used for displaying the status of the main functionalities and the system itself. There are 4 sub-menus that can be accessed from here.

device   Displays information about the system temperature, PSU and FAN functionality. The only possible command under this submenu is list.

interface   show [interface]: displays the configuration associated with the selected interface and its current status regarding link, whether it is enabled or not, speed and duplex mode. vlan.show [interface]: displays the current VLAN TAGGING configuration for the selected interface.

2.4 System

The System menu is used for administrative changes. There are 11 sub-menus that can be accessed from here.

aaa   The XX-720G unit supports remote authentication, authorization and accounting services for networked access control through a centralized server, a protocol called TACACS+. The aaa menu allows users to configure this type of access.

add: It allows the user to add a new TACACS+ server, using the following details:
- ◉ server: represents the TACACS+ server hostname or IP address. The default expected port is 49. In case this

port is different, specify it using the following format:

```
hostname:port
```

- ⊙ **login type:** represents the type of login used in the server. Possible options are PAP,CHAP and LOGIN.

- ⊙ **priority:** represents the server priority (1-5) 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. Selecting 1 will configure the current server to be the first one used for authentication. Selecting 5 will configure the current server to be the last one used for authentication.

> ► **Note:** There cannot be 2 specified servers sharing the same priority.

- ⊙ **secret:** represents a key string used to encrypt the communication between the server and the client.

- ⊙ **admin minimum level:** represents a value between 15 and 0 that defines what priv_lvl is requested for an user in order to be granted admin privileges.

- ⊙ **user minimum level:** represents a value between 15 and 0 that defines what priv_lvl is requested for an user in order to be granted normal privileges.

> ► **Note:** this value needs to be smaller than the value used for admin minimum level.

Remove: allows removing one of the previously configured TACACS+ server entries.

Edit: allows modifying one of the previously configured TACACS+ server entries.

show: allows displaying the previously configured TACACS+ server entries.

> ► **Note:** Enabling TACACS+ server authentication applies for all login methods: serial, ssh and XX-Manager.

date

show: Displays the date.

set: Allows the user to set the date and time.

ntp_server: This command controls the list of NTP servers that the device can use to synchronize its clock.

add: Add a new NTP server;

edit: Edit an existing NTP server;

delete: Delete an existing NTP server;

disable: Disable an existing NTP server;

enable: Enable an existing NTP server;

show: Display the current available NTP servers.

time_mode [set/show]: Select how the system clock should be set. The "NTP" option will enable the NTP service to synchronize the clock from a network time server.

time_zone [set/show]: Control the timezone used by the device to display its time.

factory_reset	Should the system become corrupted or the main parameters need to be restored to their default values, this option resets the device to the factory state and reboots the system. After issuing the command, the user must confirm it [yes / no].

> ► **Warning:** In case of a factory defaults reset, all stored Rule Set data and the Users database will be deleted.

legal	Displays the Product Legal Information.
license	install: It allows users to install an advance license after their initial purchased one expired. The .lic license file can be uploaded to the unit from an USB drive or from an URL address.

> ► **Warning:** Please only use a genuine license file provided by Profitap. After uploading a new valid license, the unit reboots.

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 / no].

> ► Note: if connected through the Ethernet management port, after issuing the disable command, the session will be lost.

set: Allows the user to set the IP acquisition mode of the unit to either DHCP or STATIC. In case STATIC is selected, the user has to input the IPv4, network mask, gateway and DNS address.

	status: Displays the network parameters of the unit: IPmode,Link status, IP, Mask, Gateway and DNS.
network.acl	**policy [set/show]**: Controls the device's ACL firewall's default policy. This can be set as "Whitelist" (deny any request not matching) or "Blacklist" (allow any request not matching).
	rules: This set of commands allows the user to configure the ACL entries defining the source IPv4 addresses that can or cannot access the device's services.
	add: Create a new ACL entry on the device;
	delete: Delete an existing ACL entry on the device;
	disable: Disable an existing ACL entry on the device;
	edit: Modify an existing ACL entry on the device or its priority;
	enable: Enable an existing ACL entry on the device;
	show: Display the current ACL entries.
reboot	Reboots the system, keeping all configurations intact. After issuing the command, the user must confirm it [yes / no].

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

snmp	Allows the user to configure the Simple Network Management Protocol.
	community: (only designed for SNMP v1 and v2c) Allows users to add, delete or edit SNMP communities, used for establishing trust without standard credentials.
	disable/enable: Disables or enables the feature.
	show: Displays whether the feature is enabled or disabled.

trapsinks: (only designed for SNMP v1 and v2c) Allows the user to add, delete or configure hosts which SNMP notifications (traps) will be sent to.

`

ssl_cert

renew: It creates a new SSL certificate for the XX Manager web interface. After issuing the command, the user must confirm it [yes / no].

import: Allows the user to import a pre-generated SSL certificate and key to the device, required for the HTTPS web interface. After the command is issued, the user can upload from a chosen URL or from a USB device, first the new key and then the related certificate.

> ► Note: Both key and certificate files are expected to be in PEM format. After both files have been uploaded, the system checks their validity, replaces the current versions and restarts the web interface.

syslog

clean: Removes all syslogs from the system.

show: Displays all syslogs and their timestamps.

remote.config: Allows the user to input the network details of a remote server where syslogs would be sent to: protocol type (TCP/ UDP), IP/hostname, port number.

remote.disable: Disables this feature.

update

install: Allows the user to update the system's firmware from a USB drive or from an URL address.

users

activate: Activate an existing login user.

block: Prevent an existing user from login in.

edit: Edit the details of any existing user: username, full name, email address and role.

new: Creates a new user. The following properties will be required: username, full name, email, role (viewer [default], admin, user). Depending on the selected role, the user has the following privileges:

- ⊙ Admin - full control, limitless administration and system updating.
- ⊙ User - create & set rules, aggregate and filter traffic.
- ⊙ Viewer - view only: settings, statistics, active rules.

passwd: Specifying an user name as parameter [passwd user_name] will allow changing the login password for that user name.

show: Specifying an user name as parameter [print user_name] will display all the information for that user: full name, email, role and whether the user is active or not.

reset: This command will remove all registered users and replace them with the default user: profitap:profitap (username:password). After issuing the command, the session will close. After reconnecting, the user must login with the factory credentials (profitap:profitap) and add a new admin user.

rm: Specifying an user name as parameter [rm user_name] will result in deleting that username from the user database.

LEGAL

DISCLAIMER

The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties 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.