X2-6400G PACKET BROKER

PRODUCT MANUAL

BRING CLARITY INTO YOUR NETWORKS

If you have any questions, you can contact us through our website:

www.profitap.com

or by email:

support@profitap.com

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

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

TABLE OF CONTENTS

INSTALLATION

1. UNPACKING & INSTALLATION

1.1 Unpacking

Carefully unpack all the items supplied with the X2-6400G and retain the packaging for later use:

- 1 x X2-6400G main unit
- 2 x C13 AC power cord
- 1 x RJ45 9-pin female serial adapter
- 1 x Rack mounting kit (including front & rear brackets and the necessary screws)
- Quick Start Guide

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

1.2 Installation as Standalone

The unit can be installed as a stand-alone 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 Installation in a Rack

The unit can be mounted in a standard 19″ (2U) rack using the **provided mounting brackets.**
a) Slide the main chassis into the desired rack location.
b) Secure the chassis using the **supplied screws.**
c) Make sure the rack is grounded properly.

2. HARDWARE OVERVIEW

X2-6400G is a high end versatile solution, designed for aggregation, advanced filtering and routing of multiple 40G/100G inputs, used in very high sustained bandwidth port monitoring and analysis scenarios.

The unit can be managed via CLI by connecting it to a computer, or via the X2-Manager web interface, after the initial CLI setup has been completed.

The unit features the following ports:

- **64 x** QSFP28 (40G/100G) ports, supporting optical transceivers, active optical cables or direct-attached 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
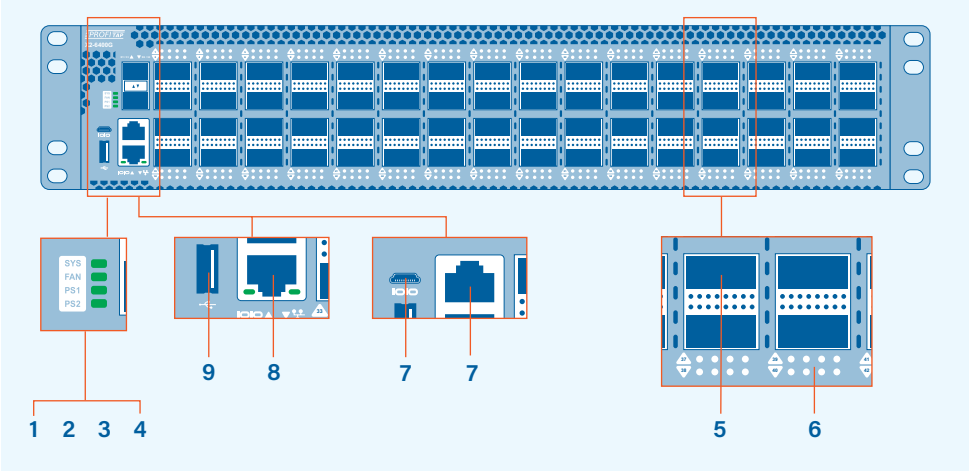
QSFP28 Modules support:
- 40G/100G speeds
- 4 x 10G SFP28 splits
- 4 x 25G SFP28 splits
- 2 x 50G SFP56 splits

They are also backward compatible with QSFP+ standards.

2.1 Technical and Electrical Specifications

- 2.2 GHz Intel Xeon quad-core 64-bit CPU
- 6.4 Tbps Barefoot ASIC
- Rigid metal enclosure, black oven painted
- 2 x 1200W, 100-240 VAC, 50-60 Hz, 80 Plus Platinum efficiency power supply (1 required for operation, 2 for redundancy) in redundant mode (100-240V / 50-60Hz).
- Typical power consumption: 730W
- Cooling : 4N + 1 redundant fans
- Operating temperature: 0°C to 45°C
- 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

2.2 Front View

1	System status LED	
2	Fan status LED	
3	PSU1 status LED	
4	PSU2 status LED	
5	QSFP28 port (1–64)	

6 QSFP28 port activity led. Led behavior is explained in detail in chapter 2.4

7 Serial management port

8 Ethernet management port

9 USB port (firmware update port)

2.3 Rear View
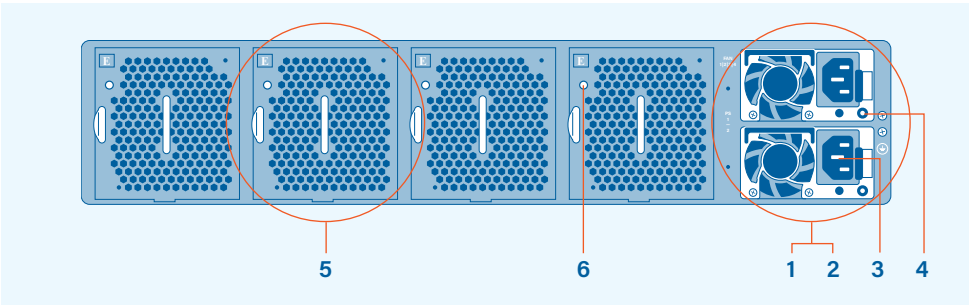
1 PSU1

2 PSU2

3 AC power connector (with Plug Retainer)

4 PSU status LED

5 Hot-swappable fan module

6 Fan status LED

2.4 Supported Cables and Transceivers

The following table describes the cables and transceivers supported by the X2-6400G Network Packet Broker:

DISTANCE	DESCRIPTION	NOTE
1 m	40/100G Direct Attach Copper (DAC) cable	QSFP28 to QSFP28
1 m	40/100G DAC Fanout cable	QSFP28 to 4 x SFP28
3 m	40/100G Direct Attach Copper (DAC) cable	QSFP28 to QSFP28
3 m	40/100G DAC Fanout cable	QSFP28 to 4 x SFP28
5 m	40/100G Direct Attach Copper (DAC) cable	QSFP28 to QSFP28
5 m	40/100G DAC Fanout cable	QSFP28 to 4 x SFP28
7–100 m	100G Direct Attach Copper (DAC) cable	QSFP28 to QSFP28 850nm, MMF
7–100 m	40/100G DAC Fanout cable	QSFP28 to 4 x SFP28
100 Gbps up to 100 m	100GBASE-SR4 QSFP28 Transceiver Optic (MPO)	QSFP28, 850nm, MMF
100 Gbps up to 10 km	100GBASE-LR4 QSFP28 Transceiver Optic (LC)	QSFP28, 1290–1310nm, SMF

2.5 LED Functionality

LED FUNCTION / STATE		MEANING / CONTROL
Power status LED for PSU1 and PSU2	OFF	Power is not supplied to the device.
	Green	PSU is operating normally.
	Orange	Signal issues: ⊙ PSU is present, but there is no electric current ⊙ Fan Lock ⊙ OTP: Over Temperature Protection ⊙ OCP: Over Current Protection ⊙ OVP: Over Voltage Protection ⊙ UVP: Under Voltage Protection
Fan status LED	OFF	Fans are not initialized
	Green	Fan is operating normally.
	Orange	Fan is faulty. Check the back of the unit to see which fan is the faulty one.
System status LED	Green	System is functioning properly.
	Orange	System warning.
Link/Speed LED mode for ports 1–32 (QSFP28)	OFF	No link established on the port.
	Green	Active link at 100 Gbps.
	Blinking Green	Data is transmitted at 100 Gbps.
	Yellow	Active link at 40 Gbps.
	Blinking Yellow	Data is transmitted at 40 Gbps.

3. 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.

The X2-6400G is equipped with status and activity LEDs. For more details on status LEDs color and coding, see chapter 2.5 LED Functionality chapter.

4. INITIAL ACCESS TO X2-6400G

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 must be used: 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.

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 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://assigned_IP.

X2-6400G can also be directly connected to a computer through its 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 only 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.

CONFIGURATION

1. WEB ADMINISTRATION

X2-6400G 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
- User Settings
- Administration

1.1 Device Status

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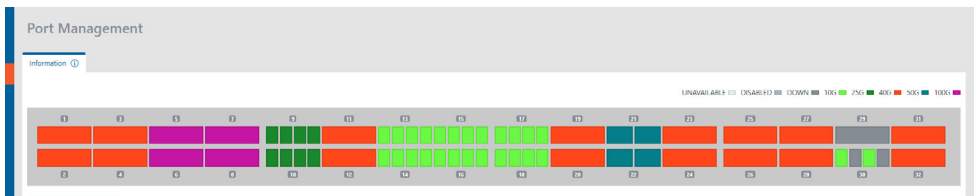
The following information is displayed:

- Revision information (model version, software/hardware revision, serial number)
- 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 (can be expanded for an improved view)
- Global device traffic statistics, with number of packets and octets for the inbound and outbound traffic.

1.2 Port Management

The Port 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 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 on the selected port: the current state of the port, the Tx and Rx bandwidth statistics and the SFP module information (if present)
- ◉ **Enable/Disable:** Allows the user to enable or disable a specific interface.
- ◉ **Speed:** Allows the user to change the port speed between 100G and 40G, or to split the port (2 x 50G, 4 x 25G, 4 x 10G) in order to use split cables.

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. Thus the port panel will allow the user to select more ports and change their state by choosing a new configuration from the <Set Multiple Ports> button.

The list of ports can be filtered via the filter button 🔽 to display only the ports matching the selected filter(s): port status, link status, speed, autonegotiation status.

1.3 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.

The Bandwidth Statistics allow 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). Statistics for the select ports can be downloaded via the Download Statistics button.

1.4 Traffic Management

The Traffic Management page allows the 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 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 tab displays the set of rules that is currently active and its details, including the filtered interfaces and the ones linked in load balancing. These details (name and description) can be changed using the <Edit> button, whereas the Rules and LAGs (Link Aggregation Groups) can be changed using the <Configure> button.

When Link Aggregation Group 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.

The Rule sets tab displays the list of existing set of rules (the active one being highlighted), allowing users logged in as administrators to create ⊕, configure ⚙, activate ☑ or delete 🗑 a rule set.

> ► *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 ➕ and defined ✏️

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

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 link aggregation 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.

Additionally, it's also possible to specify a **Priority class** for each rule. This feature can be used to define complex configurations, where the user wants to create exception cases within drop or allow filters. The device supports six priority classes and they are processed starting from '5' which has the highest priority to '0' for the lowest. Please note that within the same priority class, the rules dropping traffic will always have the priority over the one allowing it.

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

FILTER	DESCRIPTION
Ethernet Layer	Only frames matching MAC details configured in this section will be allowed to pass through (Source/ Destination MAC Address, Source/ Destination MAC Mask), with the possibility to select the packet type (IPv4, IPv6, ARP 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 Type setting is configurable only for IPv4/ IPv6, allowing the user to restrict the traffic to a specific type of L4 header (TCP, UDP, ICMP, IGMP). 'Any' allows filtering a custom EtherType or setting no filter for L3 headers.
TCP/ UDP Layer	When UDP/ TCP is selected in Protocol Type, only packets matching the Transport layer details configured in this section will be allowed to pass through. This can be done by clicking on the UDP/ TCP 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 allowed ports. After creating the group, in order to be activated, the desired filter needs to be selected by typing the respective group name in the Source/ Destination Ports Groups subsection. One or more groups are allowed.
VLAN Tags	Can be used for filtering as outer/ inner VLAN. This can be done by clicking on 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 respective group name in the Outer/ Inner VLAN ID subsection. The selections cannot overlap.

In the Advanced tab allows the configuration of some other options that can be applied on the traffic in outbound:

ACTION TYPE	DESCRIPTION
DROP/ACCEPT	the packet matching the specified filter can be dropped or accepted. Dropping is meant to be used when it is necessary to discard a subset of the traffic which is forwarded by a broader filter.
GTP IPv4/ IPv6 Filtering	this action allows the user to filter the IPv4/ IPv6 source/ destination addresses inside a GTP tunnel.
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 present, the outer VLAN TAG is removed. If both options are enabled at the same time, the board will replace the external VLAN ID tag with the one specified.
Slicing	Truncates the packet to the specified size between 64 and 9215 bytes.
ERSPAN Tunneling	De-Tunnel: strips ERSPAN encapsulation Tunnel: encapsulates packets using the specified ERSPAN tunneling settings

TRAFFIC DEDUPLICATION (LICENSE REQUIRED)

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

This feature can be controlled via the "Configure Deduplication" option 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. 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.

INGRESS RULE: 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 possible to have only a single rule for port and that these ports will be available only as input in other rules.

The available traffic manipulation options are:

ACTION TYPE	DESCRIPTION
VLAN Tag/Strip	This option will remove or add a VLAN tag to all traffic incoming in the selected port.
IPv4 Address	Allow the device interface to receive routed traffic in a IPv4 network.
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 Termination	Terminate and decapsulate an ERSPAN tunnel directed to the configured IPv4 address;
VXLAN Tunnel Termination	Terminate and decapsulate a VXLAN tunnel direccted to the configured IPv4 address and UDP port;

1.5 User Settings

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

- administrator - full control, limitless administration and system update

- user - create & set rules, aggregate and filter traffic and port configuration
- viewer - view only: settings, statistics, active rules

There is a minimum requirement for the passwords:

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

The **TACACS** tab allows adding one or more TACACS servers, and configuring the following details:

- priority (sets the order in which the servers will be taken into account, if more are added)
- login type (chap, login, pap)
- server hostname
- port
- secret key
- privilege mapping (translates the 15 privilege levels from TACACS into those of the viewers, users and admins; can be configured)

The **RADIUS** tab allows adding one or more RADIUS servers, and configuring the following details:

- Priority (sets the order in which the servers will be taken into account, if more are added)
- Server hostname
- Port
- Secret key
- Timeout (waiting time for response from the Radius server, can be set between one and 15 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 on the ➕ button. To apply the rule, click on the ✅ button.

- Fallback role (comes into place when there isn't a match between a user and a rule, with the 'none' option denying authentication access to any user)

1.6 Administration

The Administration section allows users with administrator rights to change system-related settings.
The Setup tab allows editing the administration contact details (name, phone, email), the system date and time and the network address.

> ► **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 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 chapter 4, chapter 4.1 for additional details).

The Firmware tab allows installing a new firmware on the board. The latest firmware version is available publicly at **https://x2series.profitap.com/img/**. The License information section displays the information related to the board license, and allows the installation of a new license.

The SNMP view can be used to control the device SNMPv3 service. This functionality allows the operators to monitor the state of the device and the interface traffic counters. The information can be accessed defining a specific user credentials. It's also possible to configure the device to emit traps to the requested sink servers. The SNMP MIB files are available from the GUI as well.

The Logs tab displays the system or application logs stored locally in the device. The system logs includes all logs coming from the OS components, while the application logs allow the user to view only the management plane ones. The logs display can be set to refresh automatically after a set amount of time. The logs can be downloaded via the Download button.

2. CLI ADMINISTRATION

After logging into the system, the user has access to all available commands, grouped into three 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** for available branches (or by hitting TAB from keyboards)
- ⊙ **.** returns to initial branch
- ⊙ **..** returns to previous branch

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.03
.configuration.interface.03.>
```

2.1 Configuration

The Configuration menu is used for the administration of all the interfaces (ports) in the system. The user first needs to select an interface (from 01 to 32) before administering it, e.g.:

```
.configuration.> interface.05
.configuration.interface.05.>
```

After this selection is made, there are 5 sub-menus that can be accessed:

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

speed.[value]   sets the port speed. Available values: 100G, 100G_FEC_RC, 2 x 50G, 40G, 4 x 10G, 4 x 25G, AUTONEG.

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.

statistics   Displays specified port statistics counters.

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.

2.2 Statistics

The Statistics menu is used for displaying or resetting network traffic related statistics. There are 2 sub-menus that can be accessed from here:

global [show/ reset] show: Displays information about the system temperature, PSU and FAN functionality. The only possible command under this submenu is show.
reset: resets the global statistics.

interface [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.

2.3 Status

The Status menu is used for displaying the status of the main functionalities and the system itself. There are 2 sub-menus that can be accessed from here.

device [show] Displays information about the system temperature, PSU and FAN functionality.

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

2.4 System

The System menu is used for administrative changes. There are 7 sub-menus that can be accessed from here.

date [set/show]   **set:** Allows the user to set the date and time
        show: Displays the date.

network [disable/ set/ status]   **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.

reboot   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.

syslog [application/ system]   **application/ system [reset]:** removes all syslogs from the application/ system.
        application/ system [show]: Displays all application/ system syslogs and their timestamps.

update [install]	**install:** Allows the user to update the system's firmware from a USB drive or from an URL address.
update [install]	**activate:** activates an existing login user.

block: prevents a certain user from login in.

edit: edits the details of an existing user (username, full name, email address and role).

new: creates a new user.

It needs specifying the username, full name, email and role details. Depending on the selected role, a user can have the following rights:

- admin - full control, limitless administration and system update
- user - creates & sets rules, aggregates and filters traffic
- viewer - (the default mode) has view rights only; can see the   settings, statistics and the active rules but is not able to take any action on anything.

passwd: followed by the desired user name changes the login password for a certain user.

remove: followed by the desired user name deletes a certain username from the user database.

show: followed by the desired user name displays all the information for that user: full name, email, role, and whether the user is active or not.

3. INTEGRATIONS

3.1 RESTful API Support

To integrate with tools, controllers and other IT systems, the X2-6400G offers programmatic access to the platform through HTTP RESTful API support.

The latest REST API documentation and examples can be accessed here:

https://x2series.profitap.com/api/

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.