younctа

YOUNCTA

Customer Support

SWR 2.1.0

Feature & Configuration Guide for

Y-Packet 2

Author	S. Tucci
Date	03-08-2017
Group	Technical Support
Version	1
Revision	1

01	030817		A. GRECO	S. TUCCI
ED	**DATE**	**CHANGE NOTE**	**APPRAISAL**	**ORIGINATOR**

ADDITIONAL CONTRIBUTOR (S)

Contribution to this document has been given by:

- G. Corini
- A. Di Bacco

Table of content

TERMS, ACRONYMS AND ABBREVIATIONS

Acronym or term	Explanation
ATPC	Automatic Transmit Power Control
CA	Certificate Authority
CCDP	Co-Channel Dual Polarization
CoS	Class of Service (802.1p)
CSR	Certificate Signing Request
CT	Craft Terminal
DSCP	Differentiated Services Code Point
HSB	Hot Stand-By
IVL	Independent VLAN Learning
Jumbo Frame	Ethernet frame longer than 1522 bytes
ODU	Out Door Unit
OS	Operation System
PoE	Power over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RLA	Radio Link Aggregation
RTPC	Remote Transmit Power Control
SLAAC	Stateless Address Autoconfiguration
SNMP	Simple Network Management Protocol
SSM	Synchronization Status Messages
SWR	Software Release
VAC	Voltage Alternating Current
VDC	Voltage Direct Current
VID	VLAN ID
VLAN	Virtual LAN
XPIC	Cross Polarization Interference Cancellation

1 Product description

Y-Packet 2 is a High Capacity Microwave Radio system designed for reliable point-to-point transmission.
Y-Packet has been conceived using a full outdoor approach, and can be powered by either mains (110-220 VAC) or battery (-48 VDC).
Y-Packet 2 main features are listed below:

- Frequency bands : 2, 4L, 4U, 6U, 7, 8, 10.5, 11, 13, 15, 17, 18, 23, 24, 32, 38 GHz
- ETSI (7, 14, 28, 40, 56 MHz) radio channel
- ANSI (10, 20, 30, 40, 50, 60 MHz) radio channel
- Modulation Agility (4, 16, 32, 64,128, 256, 512, 1024, 2048 QAM)
- FEC coding for improved Rx threshold performance
- Adaptive Modulation configurable by Operator
- Digital pre-distorter for higher Tx power
- Transmitted power configurable and RTPC or ATPC
- Compact ODU
- System Types 1+0, 2+0 XPIC, 1+1 HSB, 2+0 RLA
- Traffic capacity from 8 to 417 Mbps L2 throughput in 1+0 configuration (up to 840 Mbps for 2+0 XPIC and/or RLA)
- FE/GE 100/1000BASE-T User Interface with auto-negotiation
- VDC power supply
- VLAN IEEE 802.1q Transparent, Trunk and Access mode
- QoS: management of eight priority queues according to IEEE 802.1Q or DSCP
- Rate Limiter for Ingress traffic
- User friendly web management interface: the Y-Terminal
- Double IPv4 stack, with Primary and Secondary Management Interfaces
- IPv4 and IPv6 stacks support
- NMS management capabilities (embedded SNMP agent)
- 3 NTP servers for timing
- Sync-E configurable on PoE/SFP ports, or on radio port
- Three classes of users: Admin, Read-Write, Read-Only

1.1 Main features at a glance

Following features have been developed in SWR 2.1.0.

Radio & Modem
Support for the 4L/U, 7, 8, 17, 18 GHz frequency band, with increased Tx power.

Management

Primary and Secondary Management interfaces on IPv4 and IPv6 stack; protocols HTTP and HTTPS for Web GUI interface. Management available also on NFC dedicated mobile application.

System Types

Support for 1+0 Unprotected configuration has been developed

SNMP Management

SNMP Management interface has been implemented into this SWR. A new SNMP page has been created on the Y-Terminal: here operator can set a list of SNMP Managers, who will receive SNMP alarm traps from the Y-Packet 2 equipment network. SNMP Managers can run on IPv4 and IPv6 stack. Also SNMP Community Strings can be set on this Y-Terminal page.

Radio Performances

On Radio Performances Y-Terminal page, operator can access a set of statistical counters available in the system to monitor the quality performances of the link.
Tx power, RSSI, as well as SNR are collected for local and remote radio equipment. For each of these values, the Maximum, Average and Minimum values are provided, with option to filter one type of counters only. In case of Adaptive Modulation working mode, also the seconds spent in each modulation are traced.
Historical Counters are stored, for the standard time intervals of 15 mins and 24 hours. For any of the data collected, an intuitive graphical representation is given for the Historical Counters, with opportunity to filter data or to adjust graphical view according to custom settings.

Statistics

On Statistics Y-Terminal page, operator can access a set of statistical counters available in the system to monitor traffic flowing through the system and its quality.
For each of the Y-Packet interfaces, namely PoE, SFP and Radio, Ethernet traffic statistics can be displayed.
Historical Counters are stored, for the standard time intervals of 15 mins and 24 hours. For any of the data collected, an intuitive graphical representation is given for the Historical Counters, with opportunity to filter data or to adjust graphical view according to custom settings.

Backup of equipment configuration

A basic Backup functionality has been implemented with SWR 2.1.0 official. At every change of configuration, and after that each new setting has been applied by user, a backup of equipment configuration will be stored. User doesn't even need to download configuration on local PC folder, as the backups are stored inside equipment memory.

2 Radio & Modem

At Y-Terminal **Radio & Modem** page, user can find all fields to setup for the radio link to be operational. Here following you can find details on how to configure each parameter.
Radio & Modem page offers opportunity to connect and configure both Local Radio and Remote Radio. Two different pages are displayed, one for each end point of the radio link.

In order to help customer distinguish on what end he is operating, the two pages have a different background color: white for the **Local Radio Port**, light blue for the **Remote Radio Port**. Both pages offer the same set of parameters to be configured.

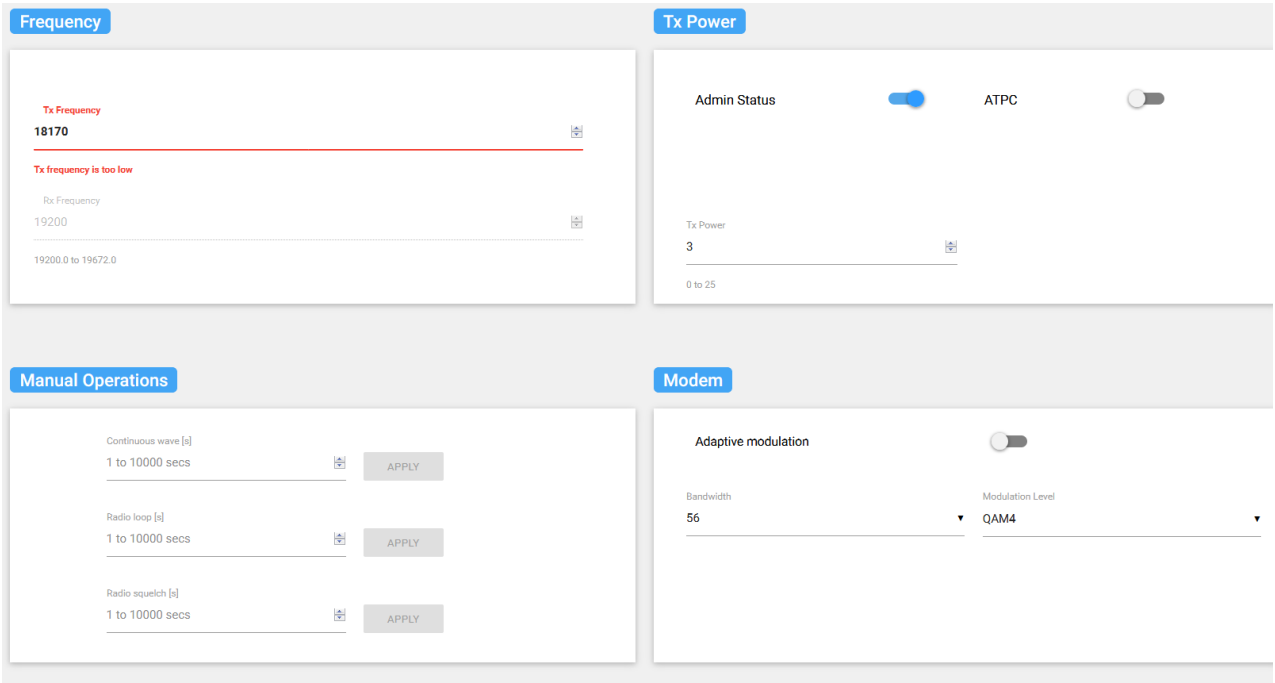
2.1 Frequency

On Y-Terminal **Radio & Modem** page, **Frequency** box, user can set the radio transmitter frequency by entering the desired value expressed as MHz. Tx Frequency must be set to a value between **Min Tx Frequency** and **Max Tx Frequency**.

Tx Frequency Min and Max allowed values are displayed just below each field. The **Tx Frequency** value can be written or just increased/decreased by means of a spinner-field.

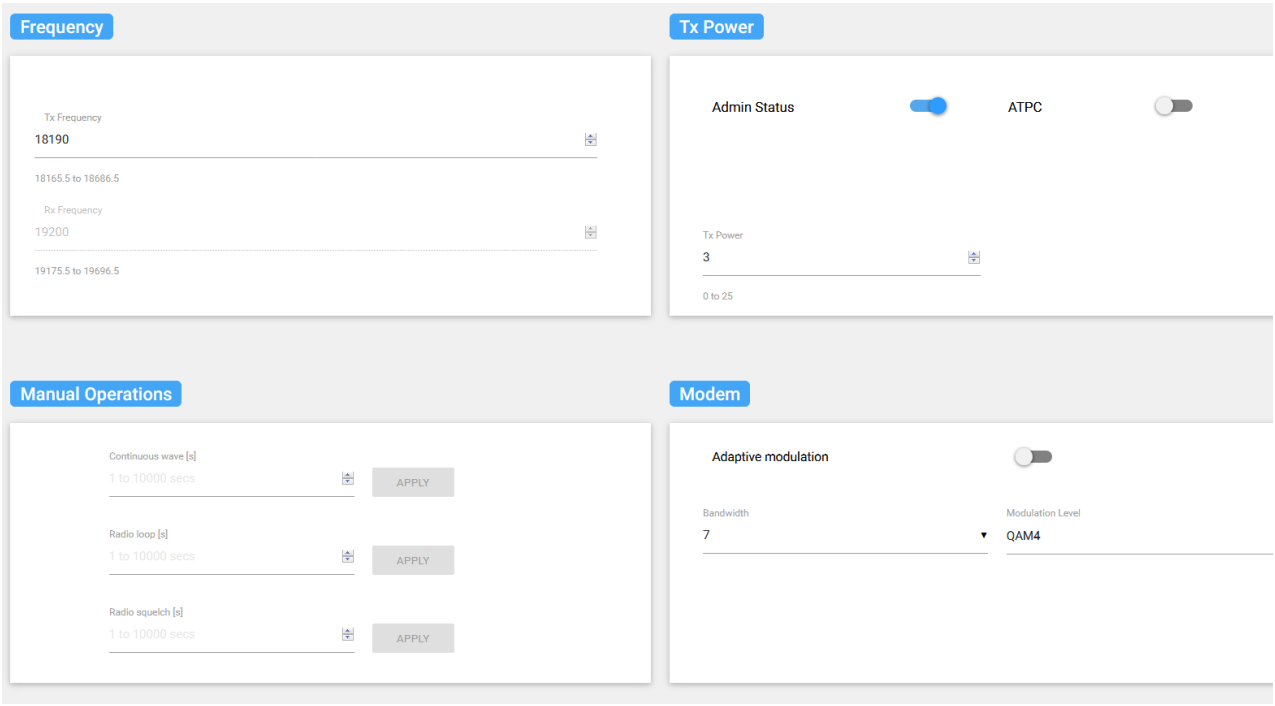
Min and Max Tx Frequency values depend on the value of **Bandwidth** set. Starting from the absolute Min and Max Tx Frequencies allowed on the equipment (written on the equipment labels) the Min and Max Tx Frequency values for each bandwidth will be calculated by adding/subtracting half the value of **Bandwidth** from the Min and Max absolute values.

! Before setting a different value of Bandwidth, the configured value of Tx Frequency shall be checked, to verify that it is inside the range of frequencies supported with new Bandwidth; in case it is not, a warning message appear as displayed in the picture below.

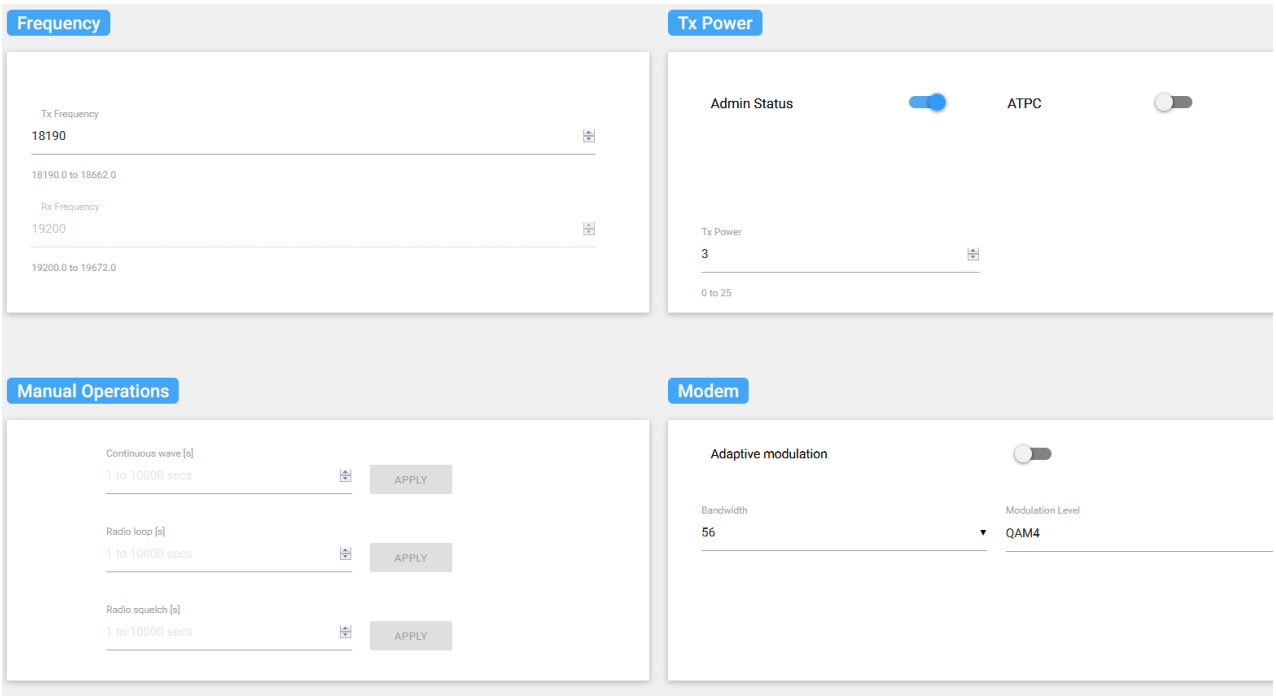


Picture 2.1 – Change of Bandwidth fails when Tx Frequency value is out of new range

Here below are reported two examples of Tx frequency ranges, respectively for 7 MHz and 56 MHz Bandwidth. It can be seen how the **Min Tx Frequency@7 MHz** is lower than **Min Tx Frequency@56 MHz**. In the same way, the **Max Tx Frequency@7 MHz** is higher than **Max Tx Frequency@56 MHz**.



Picture 2.2 – Min & Max Tx Frequency @ 7 MHz Bandwidth



Picture 2.3 – Min & Max Tx Frequency @ 56 MHz Bandwidth

Once set the Tx Frequency to any value in the allowed range, the Rx Frequency field will be automatically set, and displayed grey at Y-Terminal; this means that Rx Frequency is not editable for licensed bands, but instead automatically calculated on the basis of the equipment **Tx/Rx Spacing**.

Tx/Rx Spacing is the gap, expressed as MHz, between Tx and Rx frequency.

The Rx Frequency is calculated as follows:

! **Rx Frequency** = configured **Tx Frequency** + **Tx/Rx Spacing** for Low Band units

! **Rx Frequency** = configured **Tx Frequency** - **Tx/Rx Spacing** for High Band units

Example: **Tx/Rx Spacing** is 1010.00 MHz, and **Tx Frequency** set on Low Band unit is 17940,00 MHz; the resulting **Rx Frequency** will be 17940,00+1010.00=18950.00 MHz.

The above rule doesn't apply to Unlicensed Bands, where Rx Frequency field is editable and can be set independently from configured Tx Frequency; in this case, operator shall accurately check that it is set to the same value as Tx Frequency on the Far End. Also **Rx Frequency** Min and Max allowed values are displayed just below its field.

2.2 Tx Power

On Y-Terminal **Radio & Modem** page, **Tx Power** tab, user can configure the administrative and operational status of the radio interface, as well as transmission power levels and thresholds for ATPC mode. The available buttons and fields on **Tx Power** tab are:

Admin Status: it is the administrative status of the radio interface; it is changed by means of a switch button, and can have values ON or OFF

Tx Power: it is the fixed Tx power level (manual mode), expressed in dBm

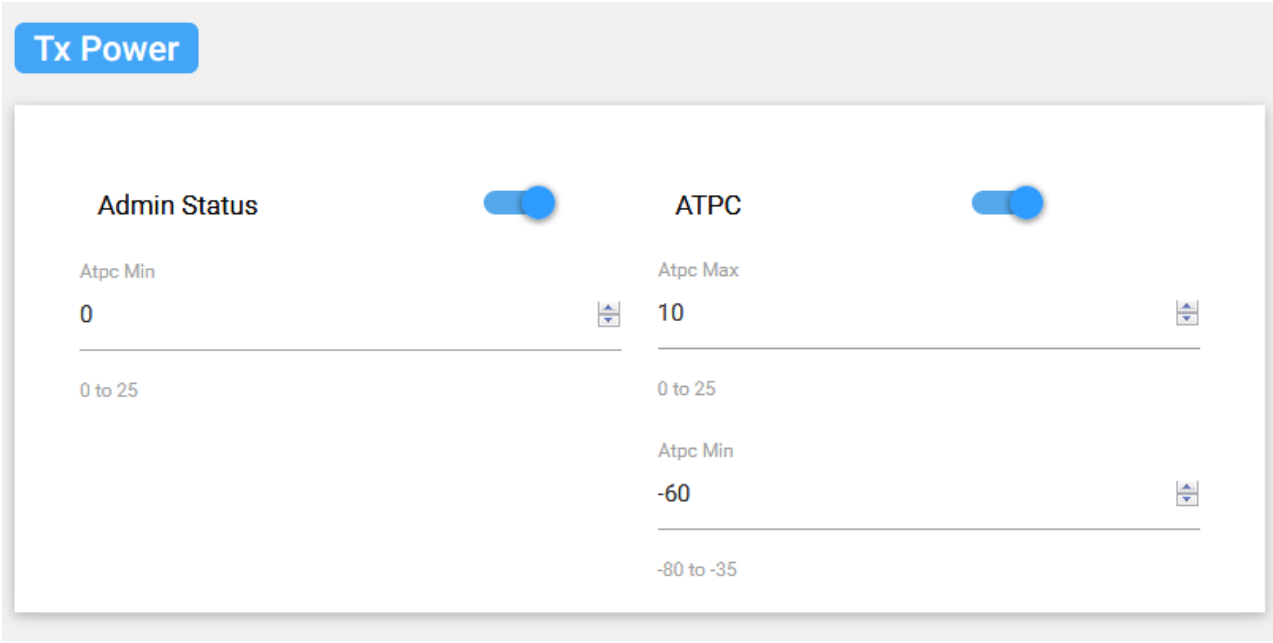
ATPC: it is the working mode of the radio interface in terms of Tx Power; it is changed by means of a switch button, and can have values ON or OFF.

Once ATPC is set to ON, the three following fields appear at the Y-Terminal **Tx Power** tab:

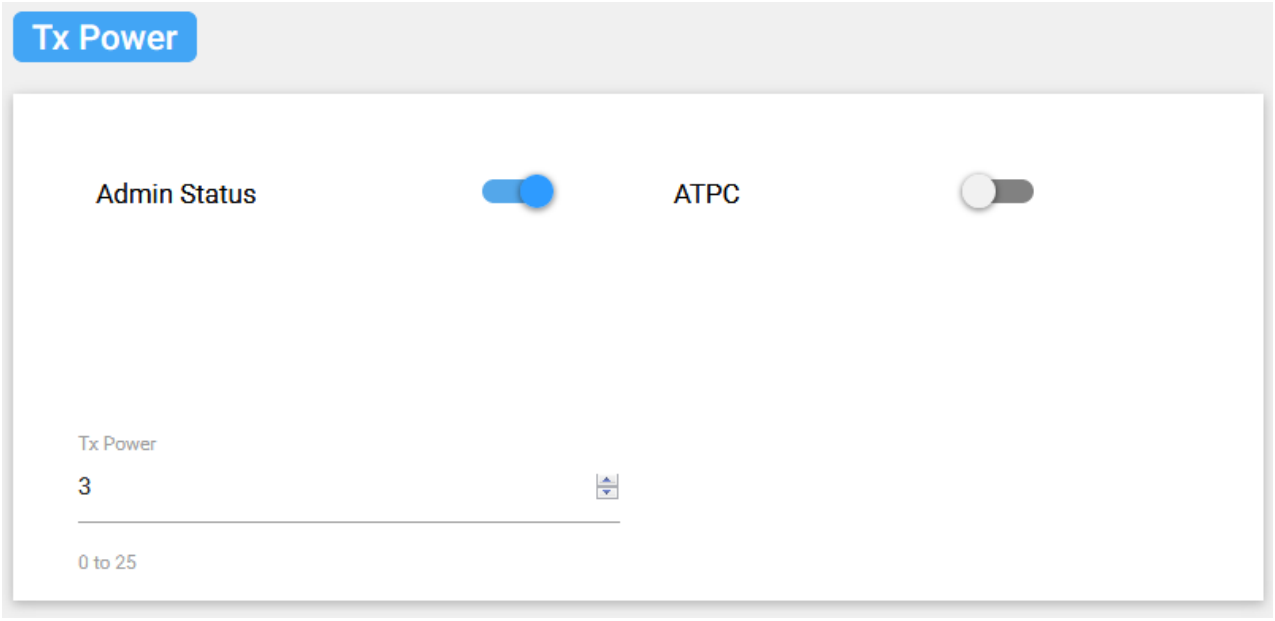
ATPC Min: it is the minimum transmission power level to be used by system when working in ATPC mode, expressed in dBm

ATPC Max: it is the maximum transmission power level to be used by system when working in ATPC mode, expressed in dBm

ATPC Target: it is the value of the Rx signal at Far End to be used as a target in ATPC mode, expressed in dBm



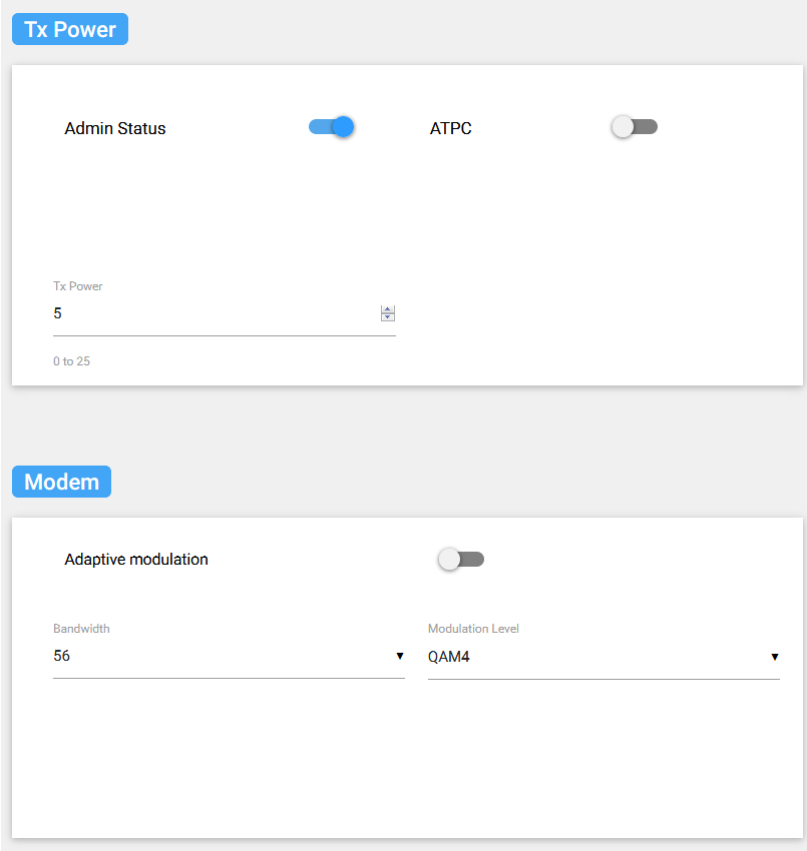
Picture 2.4 – Tx Power menu when ATPC is enabled



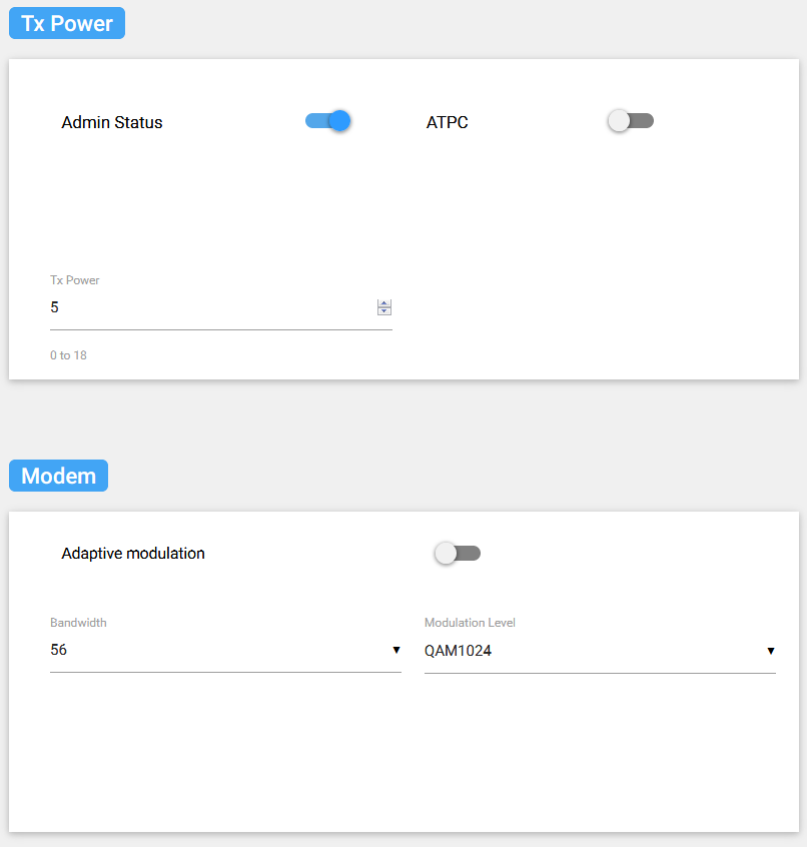
Picture 2.5 – Tx Power menu when ATPC is disabled

The following general guidelines apply to Tx Power, both for fixed and ATPC mode: Min and Max Tx Power values, which are allowed to be configured by user, depend on the value of modulation set. For each modulation selected, the **Min Tx Power** and **Max Tx Power** values will be displayed at Radio Capability box, on the left side of page.

Here below are reported two examples of Min and Max Tx Power, respectively for 4 QAM and 1024 QAM. It can be seen how the **Max Tx Power@4 QAM** is higher than **Max Tx Power@1024 QAM**.

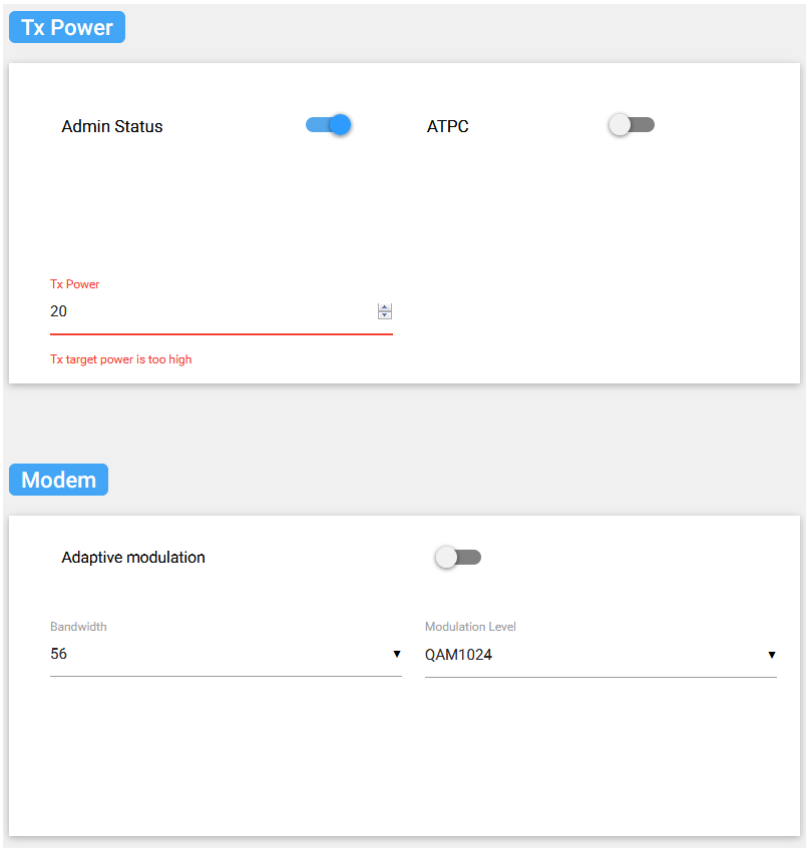


Picture 2.6 – Max Tx Power @ 4 QAM



Picture 2.7 – Max Tx Power @ 1024 QAM

! Before setting a different value of modulation, when working in Tx Power fixed mode, check the configured value of Tx Power, to verify that it is inside the range of values supported with new modulation. In case it is not, the new modulation is not applied, and the wrong Tx Power is notified to user.



Picture 2.8 – Error message when Tx Power is out of range

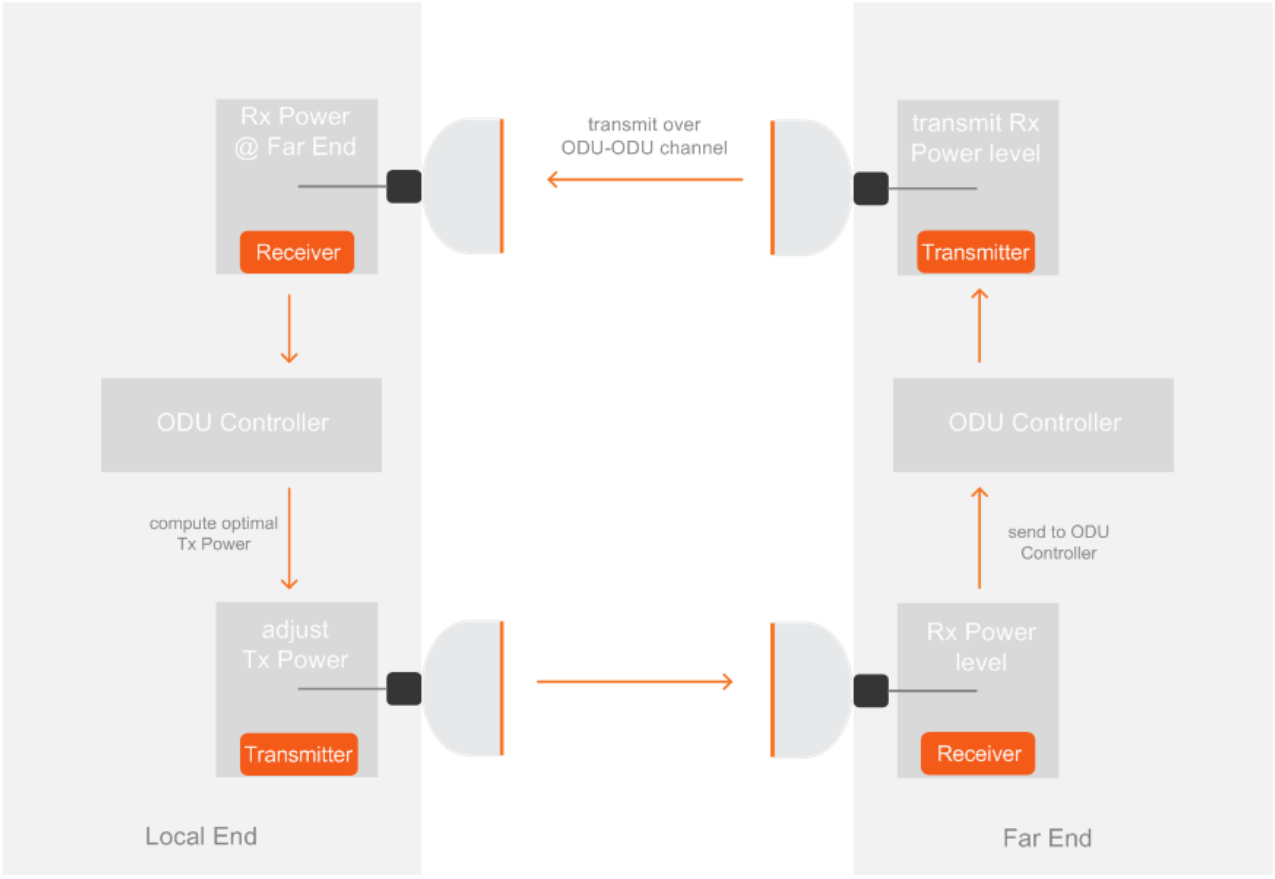
When ATPC mode is selected, the **ATPC Min**, **ATPC Max** and **ATPC Target** values shall be provided.

For ATPC to work properly, user shall carefully configure these values, in order to get optimal power management over the radio link. Automatic Transmit Power Control (ATPC) is a feature of a digital microwave radio link that adjusts transmitter output power based on the varying Rx signal level at the Far End receiver. When fading conditions occur, transmission power will be increased as needed, until the maximum is reached, and with the goal to keep the Rx signal level at Far End the closest to the ATPC Target value configured.

ATPC system is based on a control loop of the transmitted power between the local transmitter and the Far End receiver. Independent ATPC control systems are dedicated to each transmission direction. The information exchange uses a dedicated ODU-ODU service channel.

With reference to picture below, ATPC algorithm consists of the following steps:

- the receiver at Far End detects every 10ms the received power value, the ODU controller transmits this Rx power value to Local End via the ODU-ODU embedded channel
- the ODU controller on Local End, by comparing the received Rx power value with the configured **ATPC Target** value, computes the proper value of power to be transmitted. Then, the local transmitter in Local End adjusts its own transmitted power to the computed value



Picture 2.9 – ATPC power control loop

ATPC works differently depending if manual or automatic modulation mode is selected

! When manual modulation mode is selected: the equipment moves its transmission power between the **ATPC Min** and **ATPC Max** values, and takes the **ATPC Target** as the Rx power level to keep constant at the Far End. Thus, it is suggested that:

ATPC Min: it should be set to the lowest configurable Tx Power for the selected modulation

ATPC Max: it should be set to the highest configurable Tx Power for the selected modulation

ATPC Target: it should be set from 3 to 6 dBm higher than the BER 10^{-6} threshold for the selected modulation

! When automatic modulation mode is selected: the equipment moves its transmission power levels automatically, always taking the **ATPC Target** as the Rx power level to keep constant ate the Far End. Thus, it is suggested that:

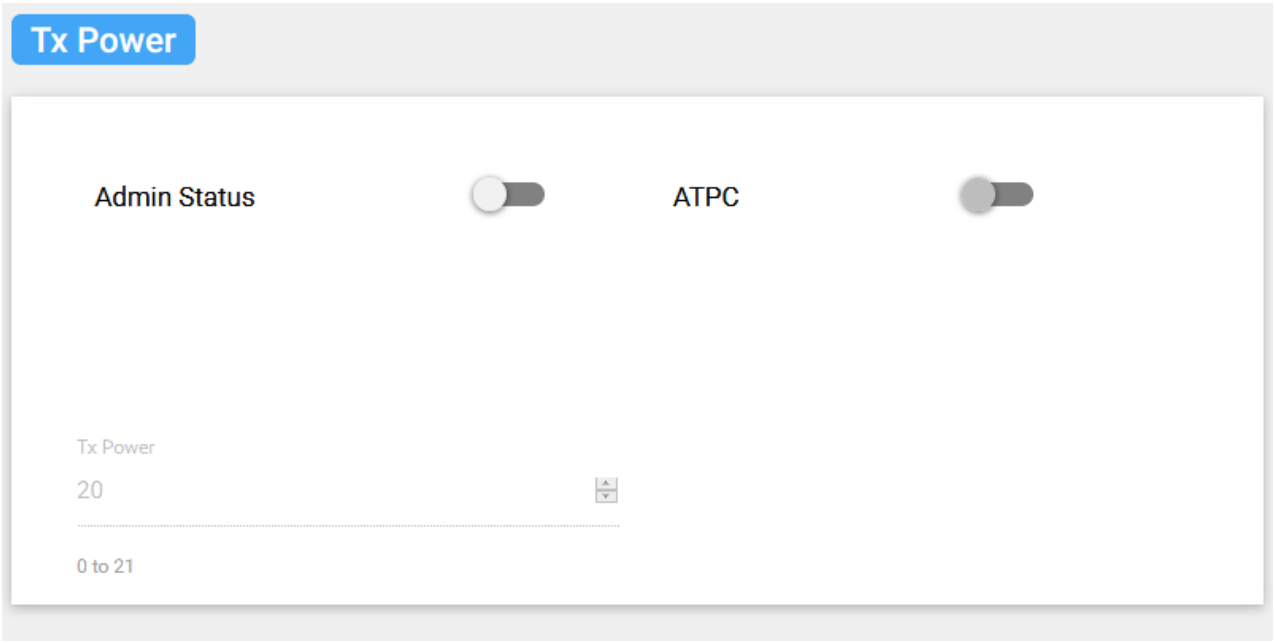
ATPC Target: it should be set from 3 to 6 dBm higher than the BER 10^{-6} threshold for the modulation chosen as **Max Modulation Level**

One of the first tasks that operator has to accomplish, to make the radio link operational, is to set the Radio interface Administrative Status. The Administrative Status for the radio interface can be configured in two possible states:

! **Off**: this is the default value, and shall of course be changed to Up in order to have connection between the equipment on the two sides of the radio link; the Administrative Status **Off** sets the state of the transmitter to off, so

no signal is transmitted. Although the transmitter is off, the receiver is always on, so operator must be aware of this when troubleshooting on the radio link.

! **On**: the Administrative Status of the transmitter is set to on, and it enables Tx as manual mode, with fix value of Tx power transmitted.

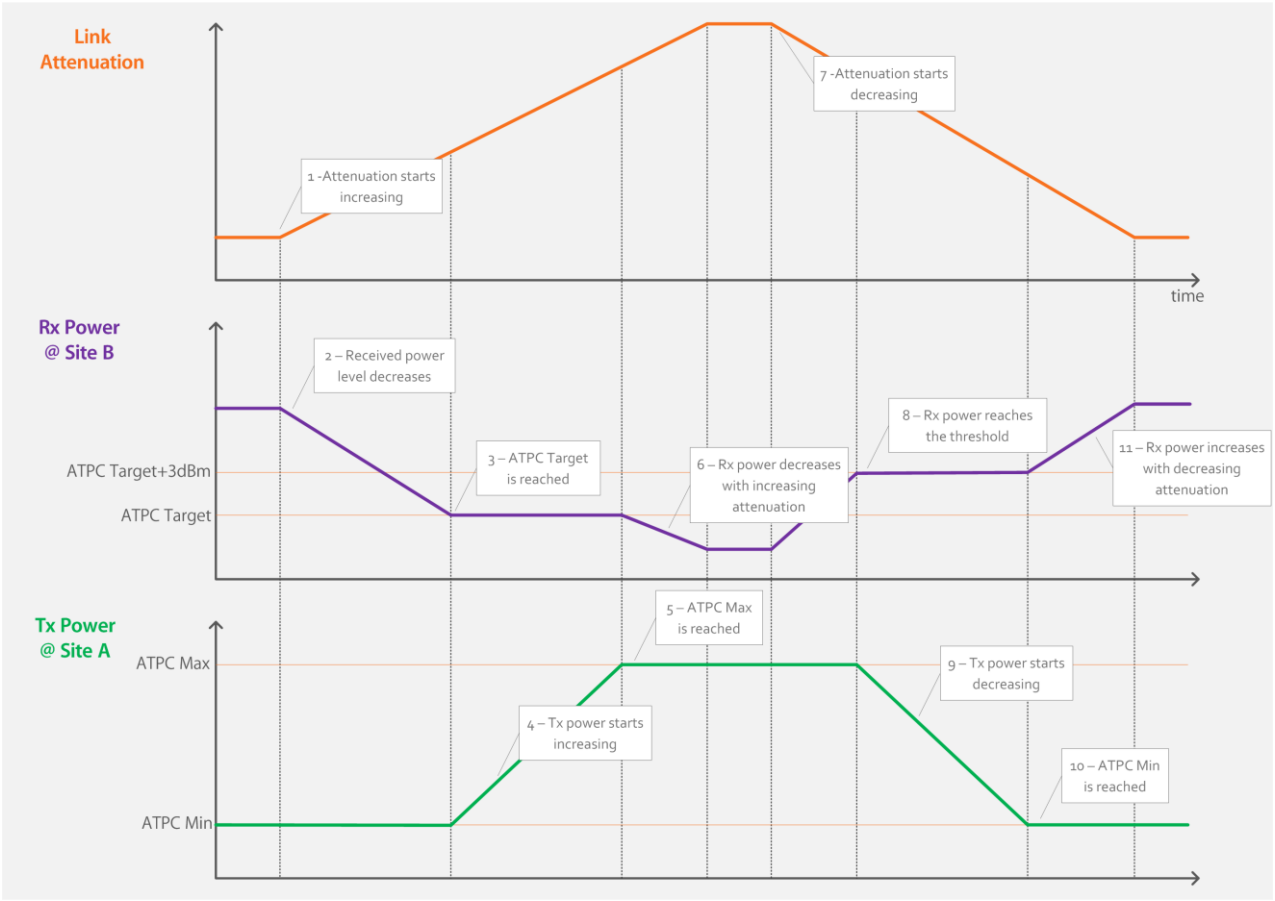


Picture 2.10 – Radio Interface Administrative Status set to Off

Configuration Example and Technical Hints – ATPC (Automatic Transmit Power Control)

In this case study we will analyse a simple unprotected link, where the Radio Administrative Status has been set to ATPC and the Modulation Mode to "manual". The radio link starts experiencing attenuation, so the system reacts by varying transmit power.

In the first phase, the attenuation is increasing, while in the second phase its level will start decreasing; we will see in both transitions how transmit power is used to compensate attenuation effects and achieve optimal link performance and reduced power consumption.



Picture 2.11 – ATPC power with varying attenuation on the radio link

With reference to the above picture, we will consider Site A as our local site, and Site B as the Far End.

Point 1: due to bad weather conditions, some attenuation starts being experienced over the radio link; this attenuation increases with time.

Point 2: Rx power level at Site B goes down, following attenuation; by means of the ODU-ODU channel, the ODU at Site B sends constantly its Rx power value to the ODU at Site A. The Rx power level at Site B decreases to a point where it reaches the **ATPC Target** level.

Point 3: as the **ATPC Target** level has been reached by ODU at Site B, it is the time for ODU at Site A to start reacting by adjusting its Tx power.

Point 4: in order to compensate the loss of Rx power due to attenuation, ODU A starts transmitting a higher power value. Starting from a Tx power value of **ATPC Min**, the Tx power is increased with the increasing attenuation.

Point 5: ODU at Site A reaches the maximum allowed Tx power level, **ATPC Max**.

Point 6: attenuation goes on increasing, so the Rx power level at Site B goes down; nevertheless, the ODU at Site A still transmits its maximum allowed Tx power, that is **ATPC Max**.

Point 7: attenuation starts decreasing.

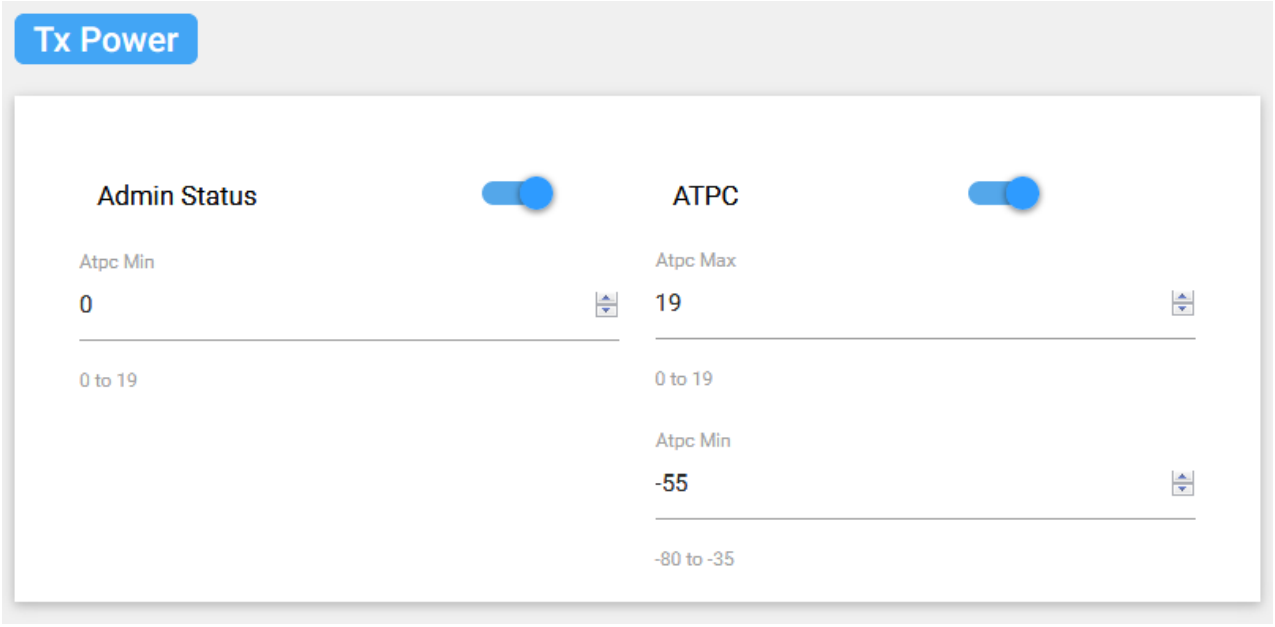
Point 8: Rx power value at Site B starts increasing again, following attenuation.

Point 9: starting from **ATPC Max,** ODU A starts reducing its Tx power value.

Point 10: the Tx power at ODU A reaches its minimum allowed value, **ATPC Min**.

Point 11: as attenuation decreases, the Rx power value at Site B goes up until it reaches its normal value.

Please see below a example of ATPC configuration on Y-Terminal. The ATPC is set to ON, the modulation is fixed 256 QAM. For this 18 GHz link, the 10^{-6} BER value @256 QAM is -61,5 dBm. The ATPC Target is chosen to be 6,5 dBm higher than the 10^{-6} BER value, so resulting in a -55 dBm. For the selected 256 QAM modulation, at 56 MHz bandwidth, the Min and Max allowed Tx values are respectively 0 dBm and 19 dBm, so the ATPC Min is set to 0 dBm and the ATPC Max to 19 dBm.



Picture 2.12 – Example of ATPC configuration

2.3 Manual Operations

Manual Operations are tools which can help operator to troubleshoot any malfunction that may be detected on the radio link. These are available at **Radio & Modem** Y-Terminal page, **Manual Operations** tab.

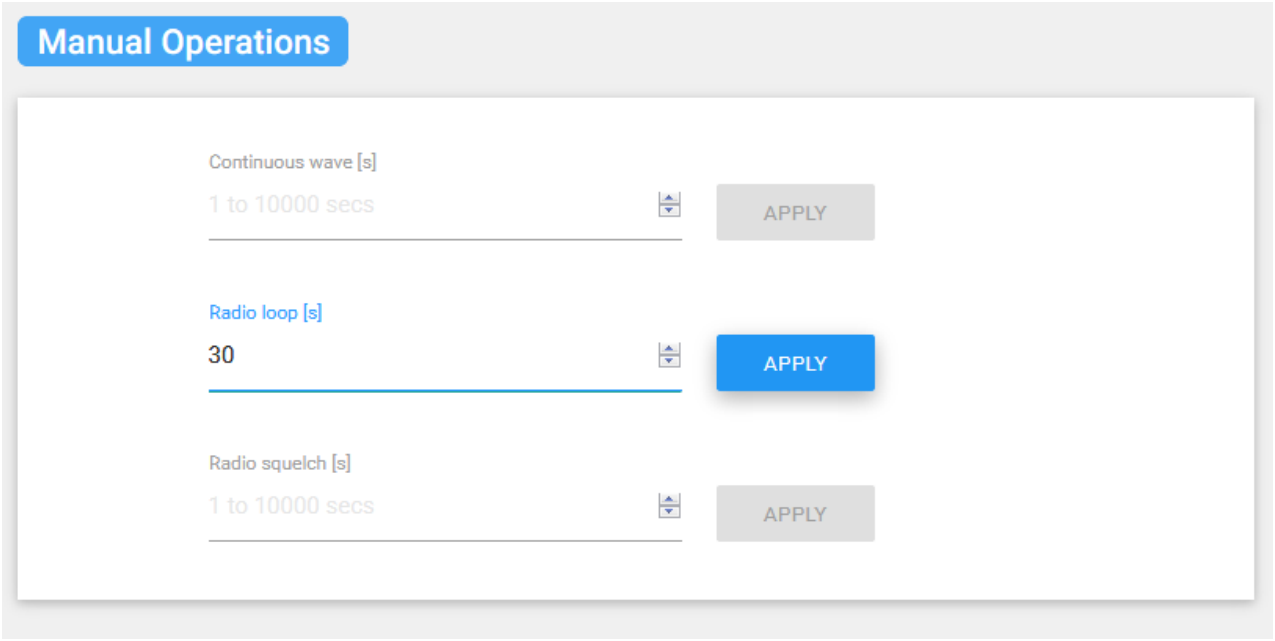
Purpose of Manual Operations is to detect possible failures at the radio interface and generally over the radio link; available manual Operations are:

CW Mode: Continuous Wave (un-modulated carrier). One tone is transmitted to the Tx frequency set.

Radio Loop: a RF loop can be set to verify if the transmitted signal is correctly received at the receiver of the ODU. OL Tx and Rx are automatically set to the same frequency in middle band and the amplifier of loop is switched on. Tx is also transmitted to the antenna.

Radio Squelch: the radio transmitter is squelched (set to off, so no signal is transmitted). Rf Tx chain power is switched off, and RF attenuator is set to maximum of attenuation.

Manual Operations have been implemented as timed operations, that allow user to enable the desired tool for a configurable time expressed in seconds. Once the duration in seconds has been inserted in the specific field, clicking on Apply will trigger the selected Manual Operation to be activated.

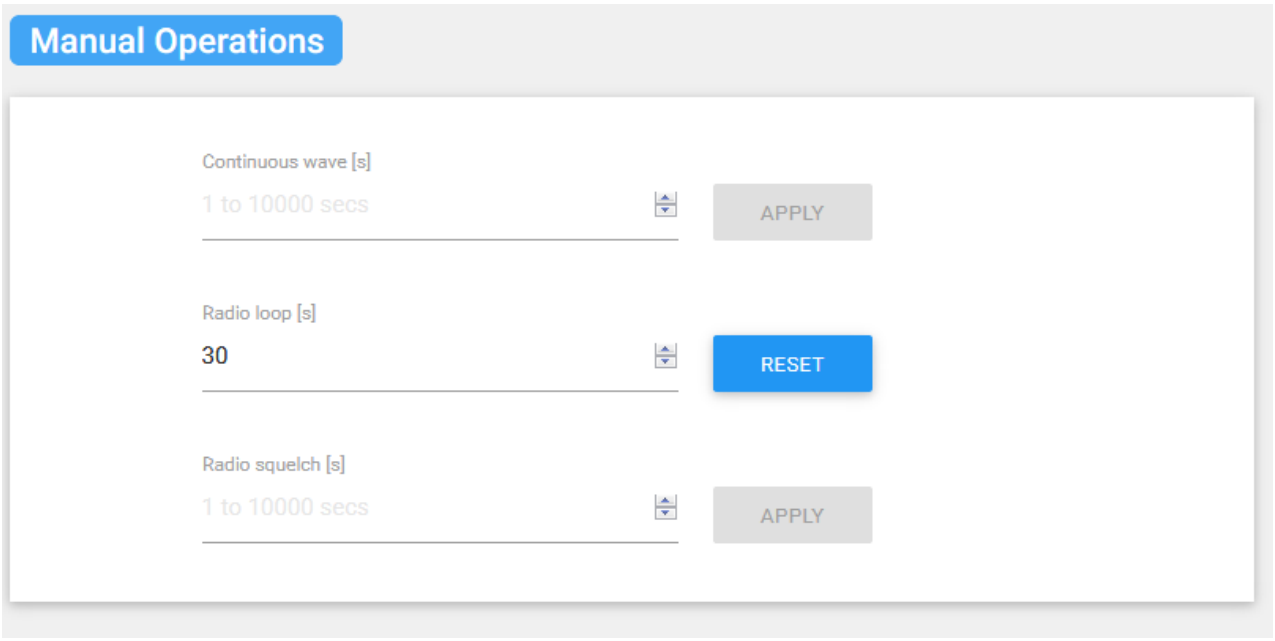


Picture 2.13 – Manual Operations: Radio Loop activated for 30 seconds

Manual Operations can be deactivated in two ways:

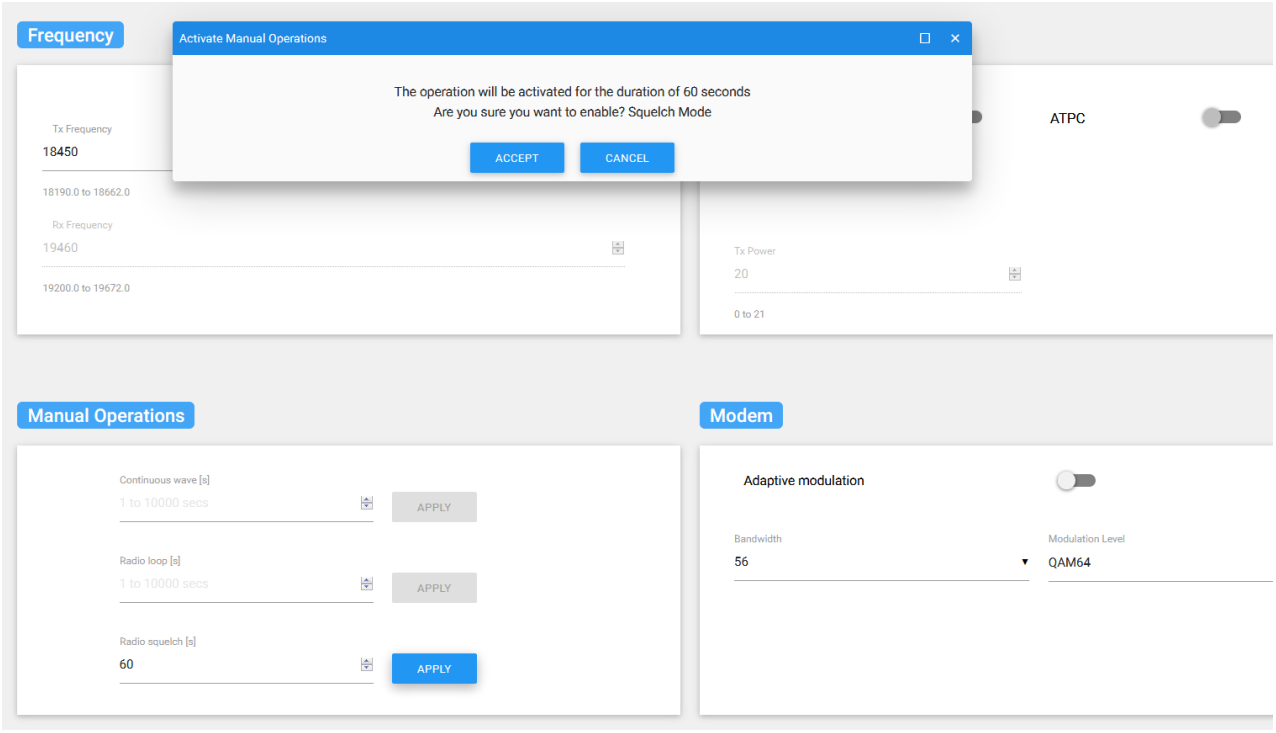
! automatically: at expiration of configured time, the timed operation will be automatically released by system

! manually: before expiry time, by clicking on Reset button, user will force the system to release the timed operation



Picture 2.14 – Radio Loop is reset manually

Manual Operations can cause disruption of traffic; for that reason, a warning message is displayed to user when activating one. Once confirmed by user, the timed operation is activated by system.



Picture 2.15 – Message of confirmation before activating Manual Operation

2.4 Modem

This section provides description of how Modem can be configured to provide enhanced handling of modulation and transmission bandwidth.

On Y-Terminal **Radio & Modem** page, **Modem** tab, user can configure following parameters:

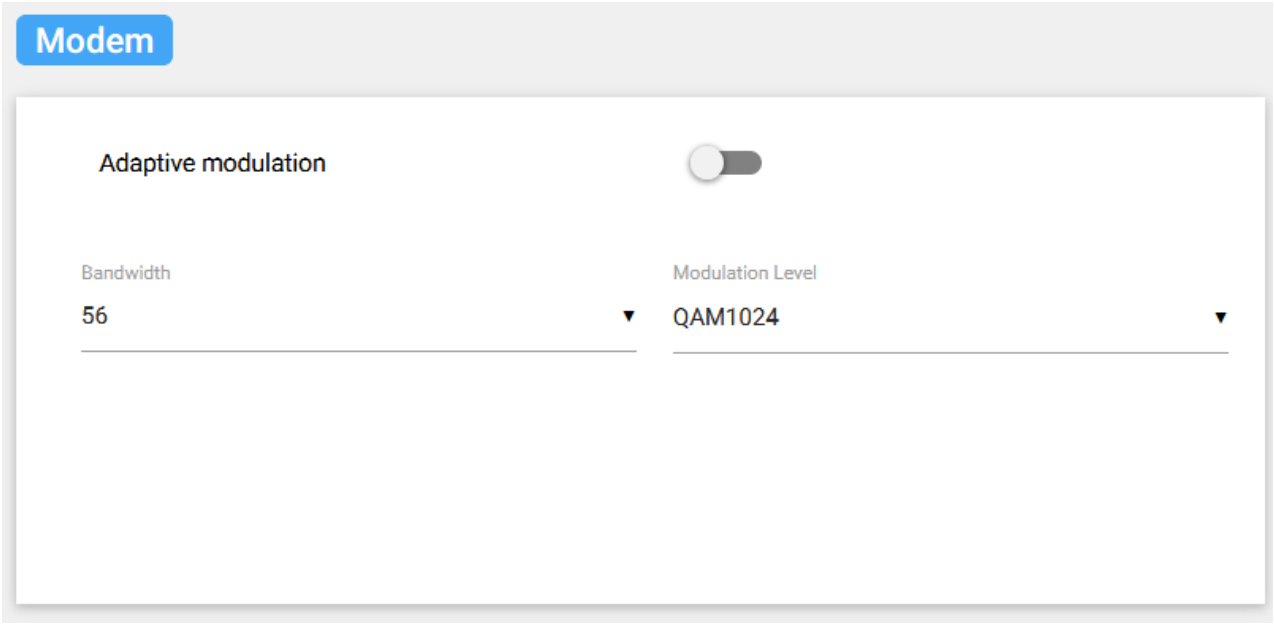
Adaptive modulation: it is changed by means of a switch button, and can have values ON or OFF

Bandwidth: it is the RF channel bandwidth; available values for ETSI standard are 7, 14, 28, 40, 56 MHz

Modulation Level: it defines the modulation index used in the manual mode (fixed)

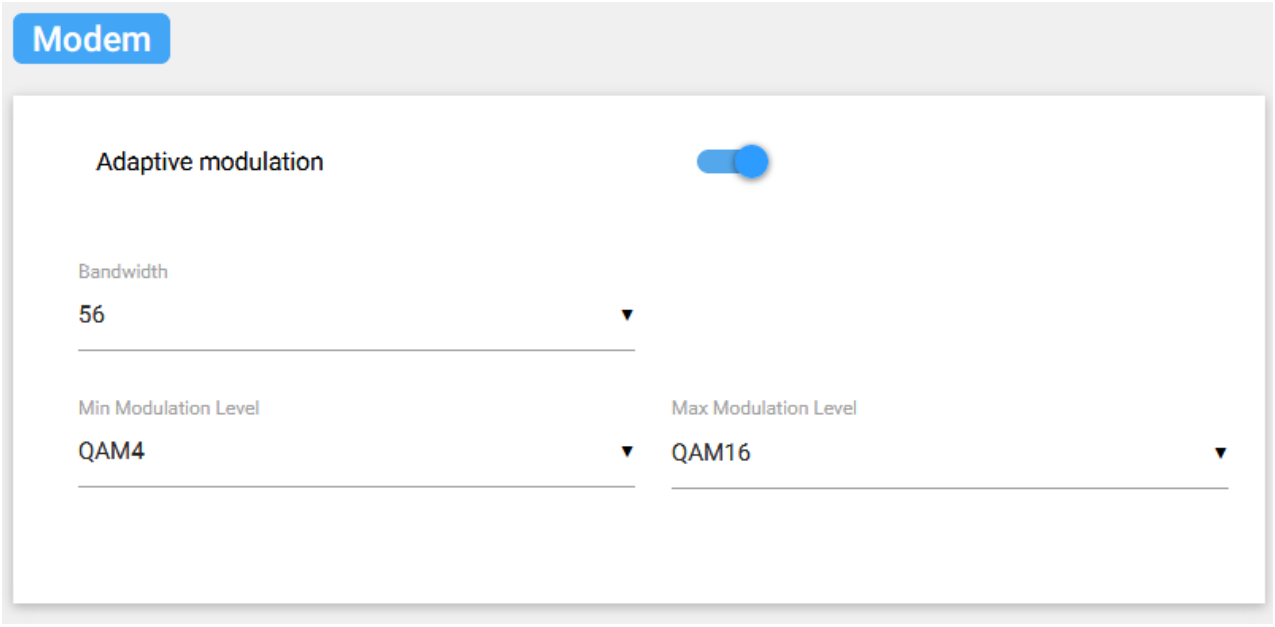
Min Modulation Level: it is displayed only when the adaptive modulation mode is set to ON; it defines the minimum modulation index to be used (among QAM4, QAM16, QAM64, QAM256, QAM 1024)

Max Modulation Level: it is displayed only when the adaptive modulation mode is set to ON; it defines the maximum modulation index to be used (among QAM4, QAM16, QAM64, QAM256, QAM 1024).



Picture 2.16 – Modem menu in case of Adaptive modulation OFF

To enable adaptive modulation, the Adaptive modulation switch shall be set to ON, then the thresholds of **Min** and **Max Modulation Level** shall be selected. Basing on possible fading or impairments that may occur on the radio link, the system will change modulation, moving between the minimum and the maximum modulation schemes selected.



Picture 2.17 – Modem menu in case of Adaptive modulation ON

Adaptive Modulation operates according to MSE thresholds, that indicate the quality of the signal received. Starting for example from 1024QAM, and degrading the Rx signal, then MSE threshold also degrades; once reached the threshold of MSE for modulation to be changed, the system is triggered for changing modulation to 256 QAM, and so on as far as MSE threshold goes down. Changes of modulation are error free.

3 Ethernet

In order to setup configuration over the Ethernet ports of Y-Packet 2 (one electrical PoE and one optical SFP), a dedicated **Ethernet** page is displayed at Y-Terminal.
Inside the **Ethernet** menu, two sub-pages will be displayed, where different types of configuration can be done on the ports.
For all details of configuration of Ethernet ports, please refer to paragraphs that follow.

3.1 Interfaces

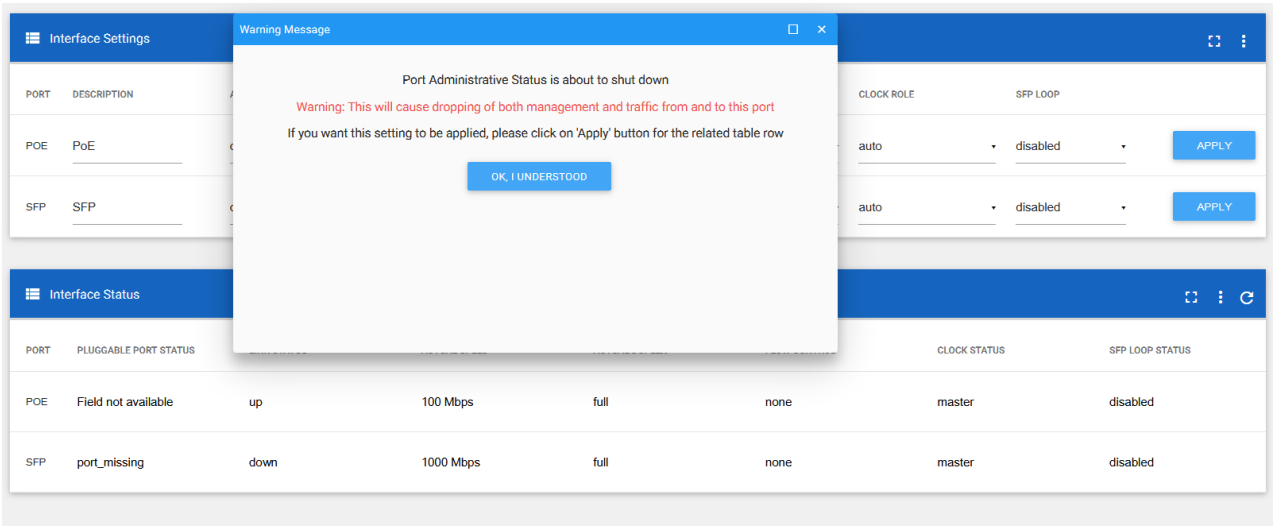
This chapter provides information about configuring the physical layer of Ethernet interfaces on Y-Packet 2. It includes the following sections: Administrative Status, Negotiation, Speed & Duplex, Flow Control and Clock Role.

Administrative Status

Each Ethernet port on Y-Packet 2 can be administratively set to enabled or disabled by means of the Y-Terminal. A scrolldown menu, with the “on” and “off” options, is displayed for **Admin Status**. At its default configuration, both

ports are set to administratively “on”; by selecting “on/off” from the scrolldown menu, user can change the **Admin Status**. Then, clicking on Apply button is required to apply the selected status.

In case user turns a port to “off” a warning message will be displayed, advising user that the port will be shut down, and consequently the connection to Y-Packet 2 will be lost on that port.



Picture 3.1 – Port Admin Status set to “off” on PoE

Clicking on “OK, I understood” the message popup window will be closed, and user will have to click again on Apply button in order to confirm operation and administratively shut down the port. Once that PoE port is set to administratively down, connection to equipment will be possible on SFP optical port only, until PoE is administratively set again to “on” through Y-Terminal interface.

The same procedure described above can be applied to SFP port.

A check is made by system, to avoid that both ports are shut down together, and connection to equipment permanently lost on Ethernet side. Thus, if one port is in “off” status, it will be not allowed to set also the other port to “off”.

Negotiation

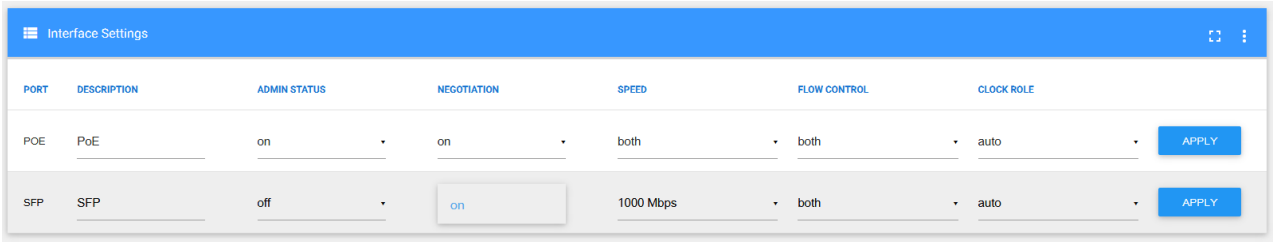
Fast Ethernet and Gigabit Ethernet interfaces use a connection-setup algorithm called autonegotiation. Autonegotiation allows the local and remote devices to configure compatible settings for communication over the link. Using autonegotiation, each device advertises its transmission capabilities and then agrees upon the settings to be used for the link.

At their default configuration, autonegotiation is enabled both for PoE and SFP ports.

The following guidelines should be followed regarding autonegotiation:

! If autonegotiation is disabled on one of the two peers in the Ethernet link, it must be disabled on the other peer. If one peer in the Ethernet link has autonegotiation disabled while the other peer has not, the link will not come up properly, often leading to duplex mismatch between the two link partners.

! Autonegotiation cannot be disabled on the optical SFP port.



Picture 3.2 – Negotiation can only be enabled on SFP port

Speed & Duplex

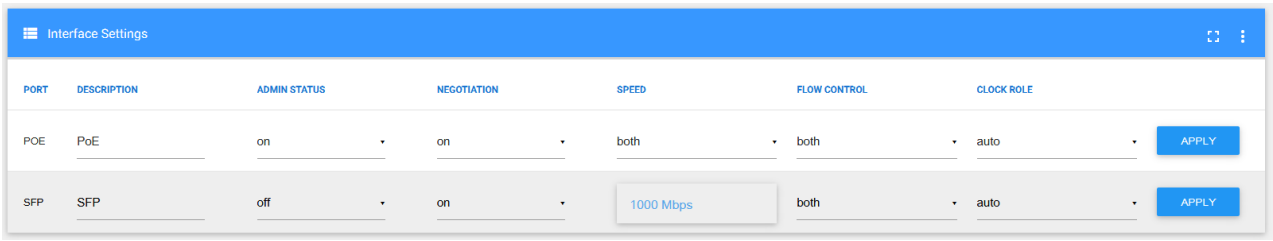
Speed and duplex configurations can be advertised using autonegotiation. However, on Y-Packet 2, the only possible configurations are:

! For PoE (RJ-45 copper interfaces):

in case **Autonegotiation** is set to "on", both 1000 Mbps and 100 Mbps can be advertised for speed, and full-duplex (FDX) mode (half-duplex mode is not used);

in case **Autonegotiation** is set to "off" (hard-coding), only 100 Mbps speed id supported, and full-duplex (FDX) mode (half-duplex mode is not used);

! For SFP (fibre interface): link speed is still negotiated, with 1000 Mbps capability only, and full-duplex (FDX) mode.

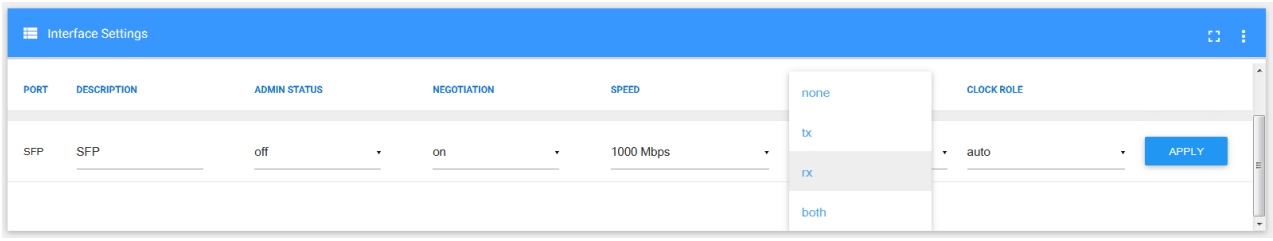


Picture 3.3 – Speed can only be 1000 Mbps on SFP port

Flow Control

The flow control used on PoE and SFP interfaces is implemented as a standard IEEE 802.3x Xon/Xoff mechanism. It consists of sending flow control pause frames with a value of pause time (quanta). When the total data rate ingressing the two Ethernet ports is higher than the maximum bandwidth available at the radio port, flow control mechanism is required to exploit maximum throughput on the radio interface while avoiding congestion and packet loss. Flow control can be independently activated or deactivated for ingress and/or egress traffic (Tx and/or Rx).

The resulting flow control operating mode is negotiated with the Ethernet link partner, and depends on the flow control settings on the negotiating peer.



Picture 3.4 – Flow Control settings on Y-Packet 2

Configuration Example and Technical Hints – Flow Control

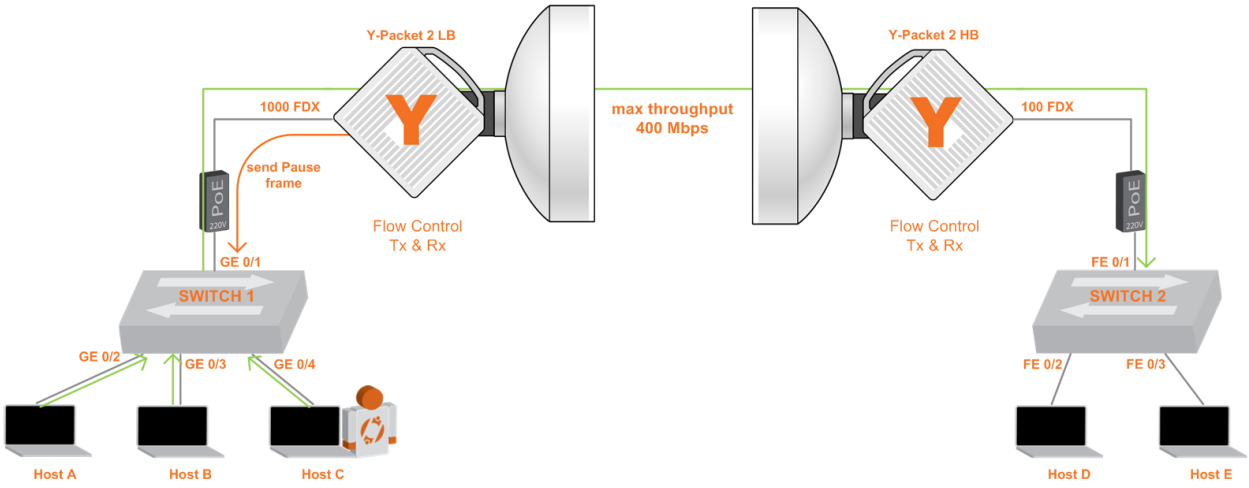
In this case study we will analyze two different cases, where the flow control is activated as Tx and Rx, and negotiated with link partner as both Tx and Rx.

In Case 1, the flow control starts working only as Tx: it is the Y-Packet 2 that sends Pause frames to the connected Switch, asking to pause transmission for a "quanta" of time. In Case 2, the flow control starts working as Rx, and Y-Packet 2 slows down its transmission upon receiving a Pause frame from the connected Switch.

Case 1

In this radio link, Y-Packet 2 LB has Flow Control enabled in both Tx and Rx, and it has negotiated with Switch 1, interface GE 0/1, an operating mode of Tx and Rx.

Switch 1 has three connected hosts, where: Host A is sending a rate of data traffic of 200 Mbps from interface GE 0/2, Host B is sending a rate of data traffic of 150 Mbps from interface GE 0/3, and Host C is sending both data traffic and management traffic, for a total rate of 250 Mbps, from GE 0/4.



Picture 3.5 – Y-Packet 2 sends Flow Control Pause frames to advertise sender to slow down transmission

All data and management traffic are forwarded through interface GE 0/1 of Switch 1 to Y-Packet 2 LB; all traffic flows have a L2 destination address such that Y-Packet 2 LB is sending this traffic over its radio interface. The radio link is

configured as Bandwidth 56 MHz, and Modulation 1024, thus reaching a maximum Layer 2 throughput of nearly 416 Mbps.

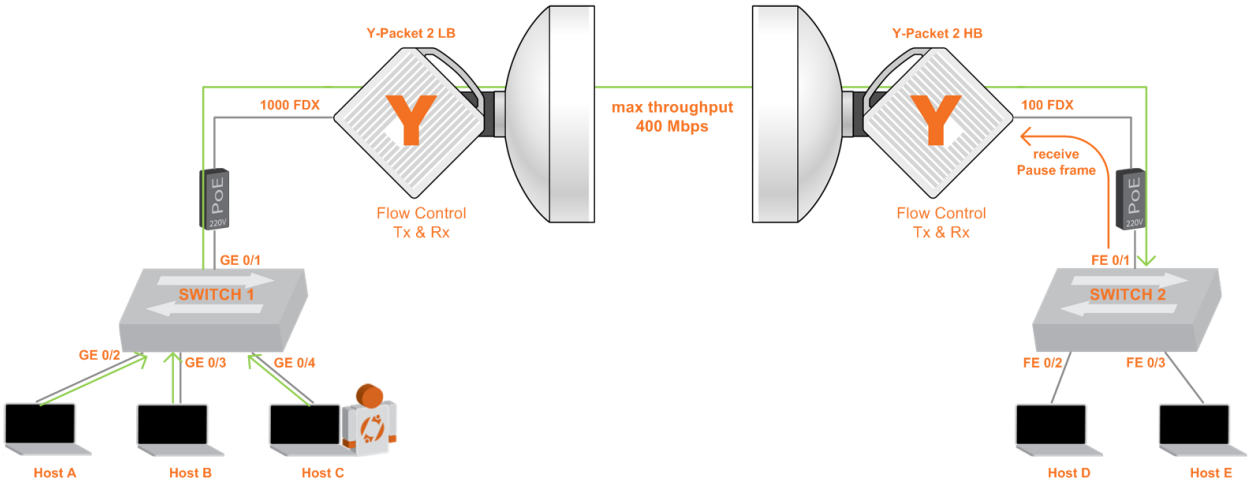
As the total amount of traffic coming from interface GE 0/1 of Switch 1 is 600 Mbps, it exceeds the maximum available bandwidth on the Y-Packet link; so, upon receiving this rate of traffic, Y-Packet 2 sends a flow control frame, to advertise Switch 1 to slow down its transmission due to lack of resources to send this rate over the radio interface. Y-Packet 2 will send a Pause frame, with a value of time, called "quanta", that Switch 1 shall be waiting without transmitting frames to Y-Packet 2.

Switch 1 receives these flow control frames and, as the flow control is active in Rx on Switch 1, it reacts by pausing transmission for the "quanta" received. At the expiry of this "quanta" time, Switch 1 will resume transmission, until again stopped by other possible Pause frames. The Pause frames mechanism will go on until the sending of data traffic (over the maximum allowed rate) is stopped: this has guaranteed that no packet drops be experimented during transmission, and the maximum available bandwidth on the radio link be exploited.

Case 2

In this radio link, Y-Packet 2 HB has Flow Control enabled in both Tx and Rx, and it has negotiated with Switch 2, interface FE 0/1, an operating mode of Tx and Rx. The speed negotiated on the interface is 100, and the duplex full.

On the other side of the radio link, Switch 1 has three connected hosts, where: Host A is sending a rate of data traffic of 100 Mbps from interface GE 0/2, Host B is sending a rate of data traffic of 75 Mbps from interface GE 0/3, and Host C is sending both data traffic and management traffic, for a total rate of 125 Mbps, from GE 0/4.



Picture 3.6 – Y-Packet 2 receives Flow Control Pause frames and slows down transmission

All data and management traffic are forwarded through interface GE 0/1 of Switch 1 to Y-Packet 2 LB; all traffic flows have a L2 destination address such that Y-Packet 2 LB is sending this traffic to Y-Packet 2 HB over its radio interface. The radio link is configured as Bandwidth 56 MHz, and Modulation 1024, thus reaching a maximum Layer 2 throughput of nearly 416 Mbps.

The total amount of traffic coming from interface GE 0/1 of Switch 1 is 300 Mbps, and it doesn't exceed the maximum available bandwidth on the radio; so, all traffic is sent to interface FE 0/1 on Switch 2.

As the maximum rate at Switch 2, interface FE 0/1, is 100 Mbps, FE 0/1 sends a flow control frame, to advertise Y-Packet 2 HB to slow down its transmission. Switch 2 will send a Pause frame, with a value of time, called “quanta”, that Y-Packet 2 HB shall be waiting without transmitting frames to Switch 2.

Y-Packet 2 HB receives these flow control frames and, as the flow control is active in Rx, it reacts by pausing transmission for the “quanta” received. At the expiry of this “quanta” time, Y-Packet 2 HB will resume transmission, until again stopped by other possible Pause frames. The Pause frames mechanism will go on until the sending of data traffic (over the 100 Mbps allowed rate on FE 0/1) is stopped: this has guaranteed that no packet drops be experimented during transmission.

3.2 Ethernet Test

The Ethernet Test can be used to measure the throughput to another Y-Packet 2 device, and thereby help to discover network bottlenecks on the radio link. When the Ethernet Test is started from the local equipment, it tests the available bandwidth on radio side, that is using the remote radio equipment as the host to send traffic to.

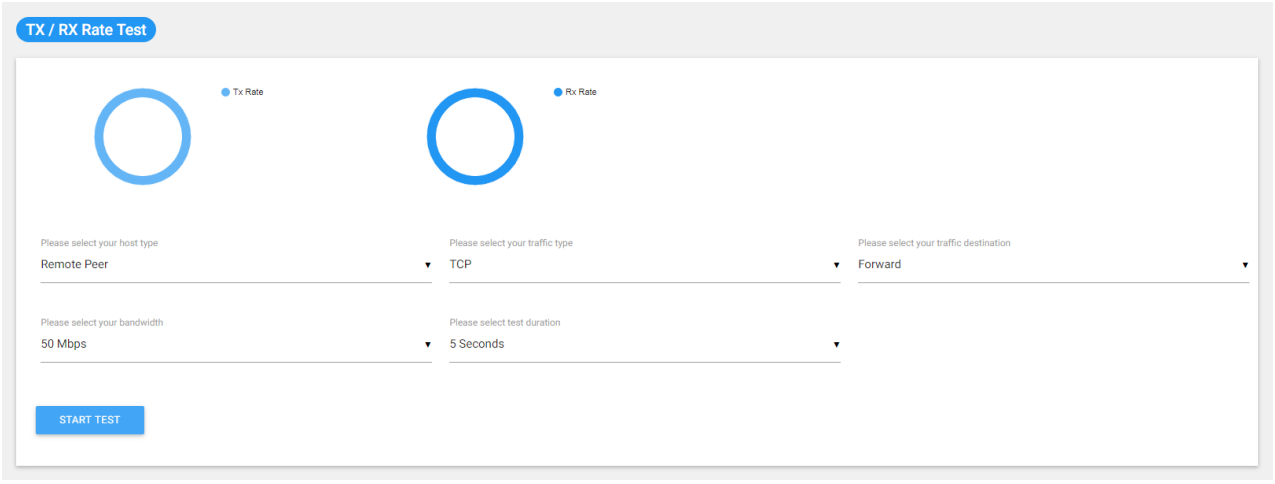
From Y-Terminal Ethernet page, Ethernet test section, user can configure a set of parameters before running the bandwidth test to its remote peer on the radio side. Configurable parameters are:

! **Traffic Type** : it can be TCP or UDP protocol type

! **Traffic Destination** : it can be Forward, Reverse or Both

! **Bandwidth** : it is the rate of simulated traffic that will be sent to/from the remote destination host

! **Test Duration** : it is the time the traffic test will last, expressed in seconds



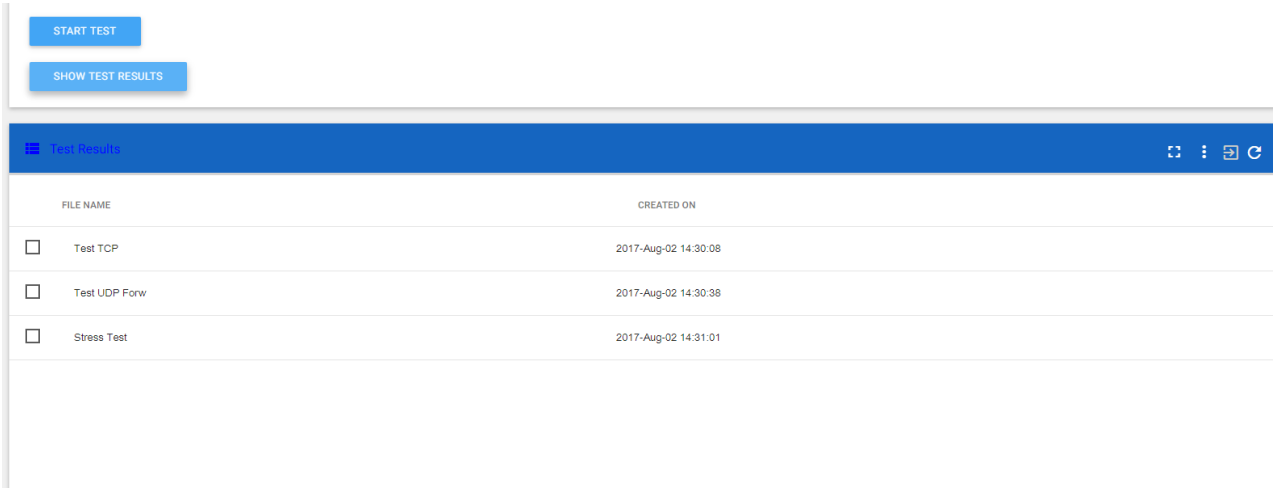
Picture 3.7 – Ethernet Test setup page

One important remark on the protocol selection: when choosing the TCP protocol, user shall be aware that the test uses the standard TCP algorithm with acknowledgments, and follows the TCP “sliding window” on how many

packets to send according to latency, dropped packets, and other features in the TCP. Statistics for throughput are calculated using the entire size of the TCP data stream.

Thus, when testing bandwidth performance, what we're actually testing is maximum TCP bandwidth at the transport layer (L4). Lots of applications use TCP as the transport protocol, include HTTP, SMTP, FTP, etc. Unlike UDP, TCP is a reliable, connection-oriented protocol with built-in mechanisms for connection established, acknowledgement, and termination. If your network is configured for QoS, you must make sure that the IPs or ports for these tests are configured for the highest priority QoS; otherwise, your results will not be accurate.

Clicking the **Start Test** button, the simulated traffic flow will be started, and automatically stopped at the end of the configured time duration. At the end of test, a **Show Test Results** new button will be displayed: clicking on it, a table will open, listing all test result files.

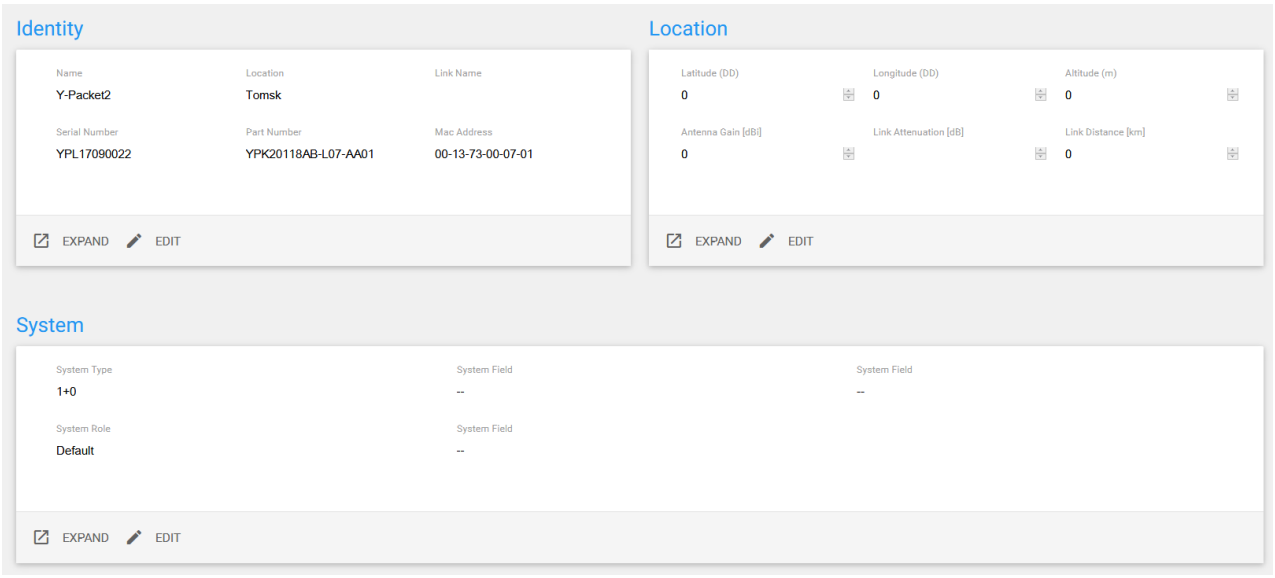


Picture 3.8 – Table with Ethernet Test result files

For each Test Result file, the file name and date of creation will be displayed. An **Export** icon is available in the table, to save the selected file(s) to local PC.

4 System Settings

This section describes how to configure general system settings on Y-Packet 2. On Y-Terminal **System Settings** page, **System** box, user can configure the link system type, as 1+0, 2+0 XPIC, RLA.



Picture 4.1 – System Settings page

Please read Chapter 5 for all details of configuration and operation of System Types. No description about system types is provided in this chapter.

4.1 Identity

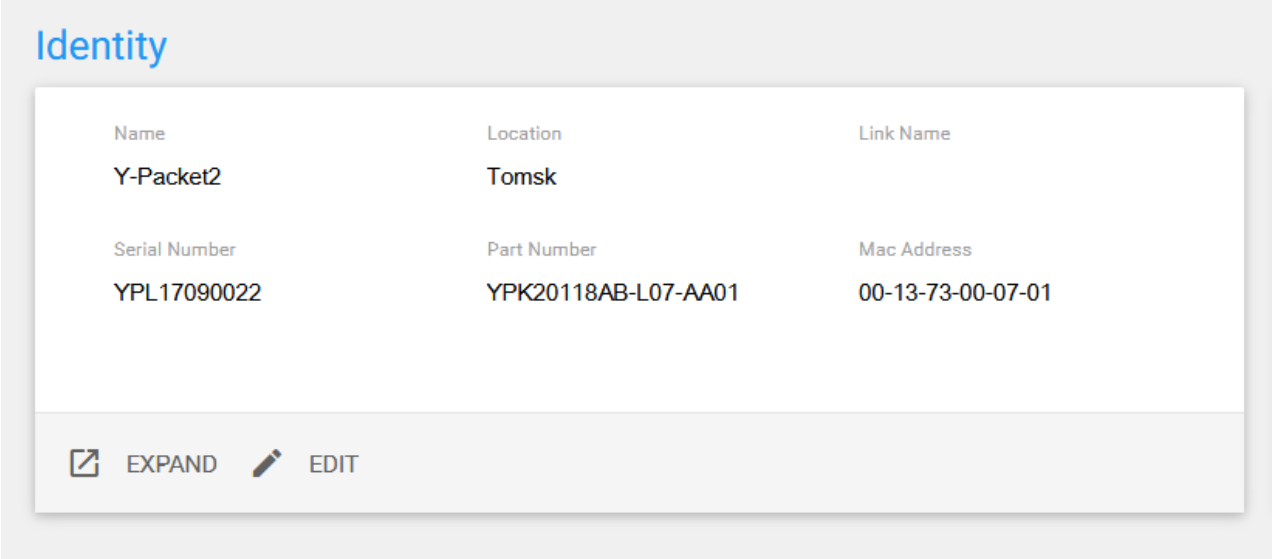
On Y-Terminal **System Settings** page, **Identity** box, user is can write some general labels used to identify the link.

Three available labels are provided to user, which are normally used to identify the link in the operator network. These are **Name, Location** and **Link Name**. One of these labels, the **Name**, is used in two ways:

- displayed on left-top of Y-Terminal page, as name for the web page, in the form <TabTitle> <System Name> (where <TabTitle> is embedded and cannot be changed by operator)
- used when operator performs a backup of configuration on equipment, from **Backup & Restore** Y-Terminal page. The backup filename will be in the form: "Backup_<System Name>_<Location Name>_<yyyy.mm.dd>_<hh.mm.ss>.zip".

In case the **Name** and/or **Location Name** contain blank spaces, these will be stripped in the backup filename.

Here below you find an example of **Identity** labels:



Picture 4.2 – Identity labels tab in Y-Terminal

To edit labels, user shall click on the **Edit** icon on bottom of Identity box, then insert the **Name**, **Location** and **Link Name** strings. Once inserted, clicking on **Save** will write the labels into equipment configuration, while a click on **Cancel** will close the edit window without applying the new settings.

When entering the Edit mode, only the editable fields will be displayed as underlined, while the others that are not underlined are fixed or set by system and thus cannot be edited.

On the same **Identity** box, the equipment HW info are also provided: these parameters uniquely identify each unit. Let's see how the HW info are built:

Serial Number

It is unique for each ODU. It has the form <Y><PP><yywwnnnn>, where:

<Y> stands for Y-Packet 2, and is common to all equipment series

<PP> stands for Place of Production, indicating where the equipment has been manufactured

<yywwnnnn> is: <yy> for year of production, <ww> for the week of production, <nnnn> the progressive number for that year and week of production.

Part Number

It is common to the all equipment of the same Frequency band, Sub-band and Tx-Rx Spacing. It has the form <YPK2><01><nn><AX><Lnn><AA01>, where:

<YPK2> stands for Y-Packet 2 and is common to all equipment series

<01> is currently fixed (reserved for future use) and is common to all equipment series

<nn> is a number that indicates the main frequency band; it is common to all equipment belonging to the same frequency band

<AX> indicates the sub-band: <X> is B for Low Band units, and C for High Band units; regardless of main frequency band, AB and AC refer always to the Low and High sub-bands for any frequency

<Lnn> indicates the frequency range covered with the equipment diplexer

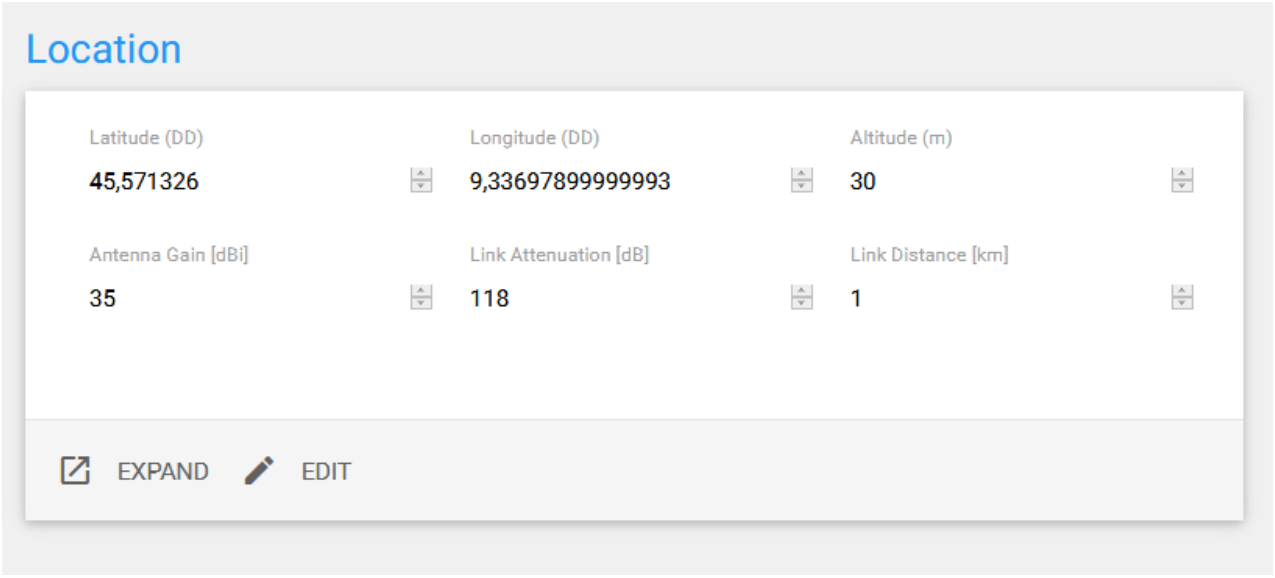
<AA01> refers to the HW version, it is fixed to AA01 and is common to any equipment

MAC Address

It has the standard MAC address format, where the first three bytes refer to the OUI, and the last three to each specific equipment.

4.2 Location

In order to locate the Y-Packet 2 once installed, user is provided a set of fields where he can exactly specify the GPS coordinates of the installation. GPS coordinates are expressed in terms of Latitude, Longitude and Altitude: the unit of measure is decimal degrees for Latitude and Longitude, so having the format like in the picture below:



Picture 4.3 –Location box in the Y-Terminal

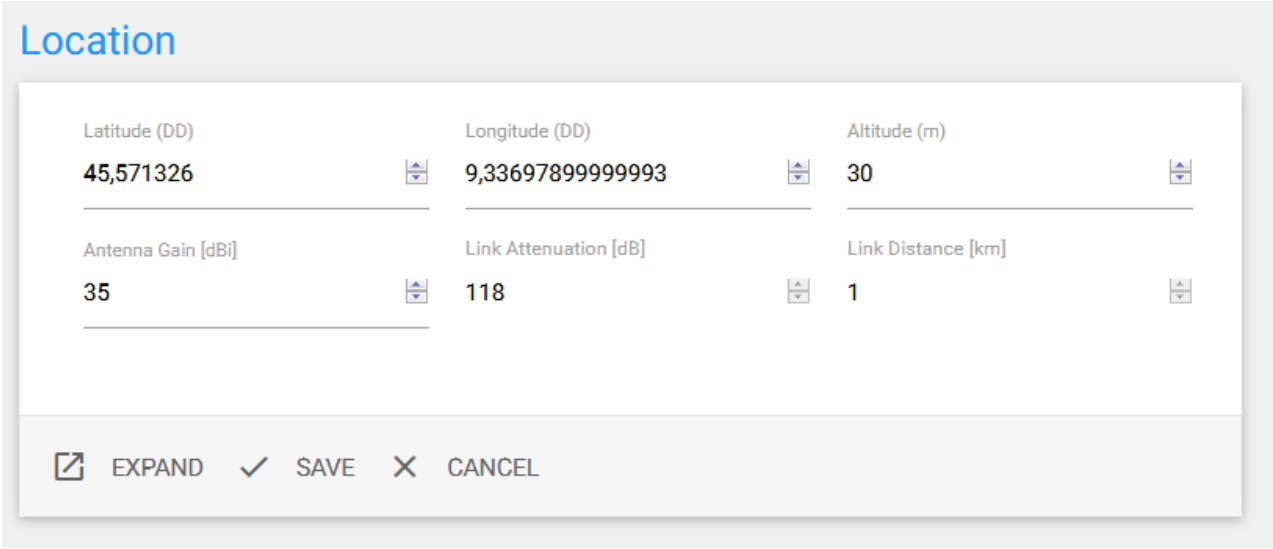
Another parameter that can be set at **Location** box is:

Antenna Gain: expressed as dBi, it shall be set equal to the value of the installed antenna gain. The system will use this value, together with the GPS coordinates, to calculate the link distance.

To edit GPS coordinates and Antenna Gain, user shall click on the **Edit** icon on bottom of Location box, then insert the desired values. Once inserted, clicking on **Save** will write values into equipment configuration, while a click on **Cancel** will close the edit window without applying the new settings.

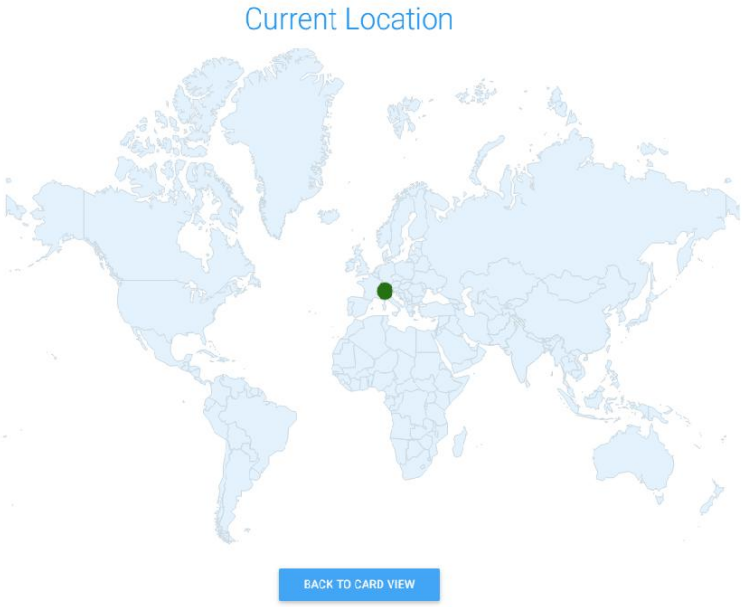
When entering the Edit mode, only the editable fields will be displayed as underlined, while the others that are not underlined are fixed or set by system and thus cannot be edited.

Based on Antenna Gain, GPS coordinates and RSSI values, also the **Link Attenuation** and **Link Distance** will be provided at the **Location** box. These values are retrieved and/or calculated by system, and thus cannot be edited.



Picture 4.4 –Editing fields in Location box: only the editable fields are underlined

The Location box can be expanded to show the exact location of the equipment on a map. Clicking on the **Expand** icon a map is displayed, where the equipment is located based on the Latitude and Longitude provided.



Picture 4.5 –Expanding the Location box the equipment is shown on a map

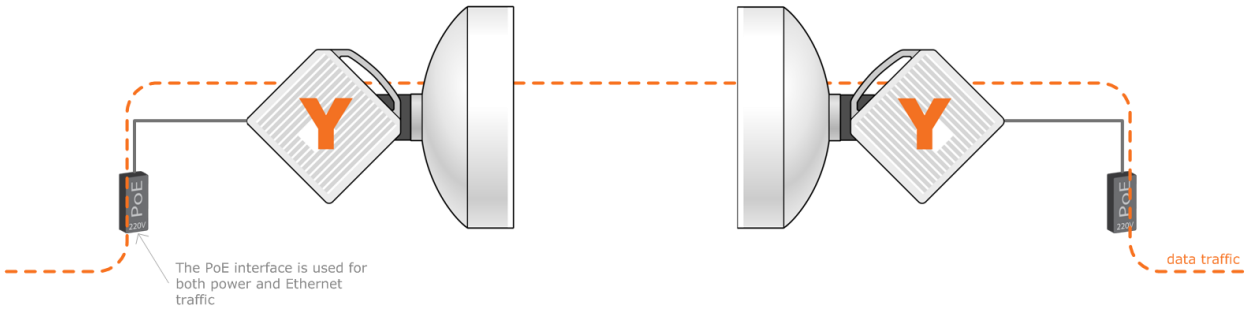
5 System Types

This section provides information on Y-Packet System Types and, where required, the procedures for related configuration.

5.1 1+0 Unprotected

This is the basic configuration of Y-Packet 2 radio link. It is an Unprotected configuration, requiring at each side of the link just one Y-Packet 2 ODU and one antenna.

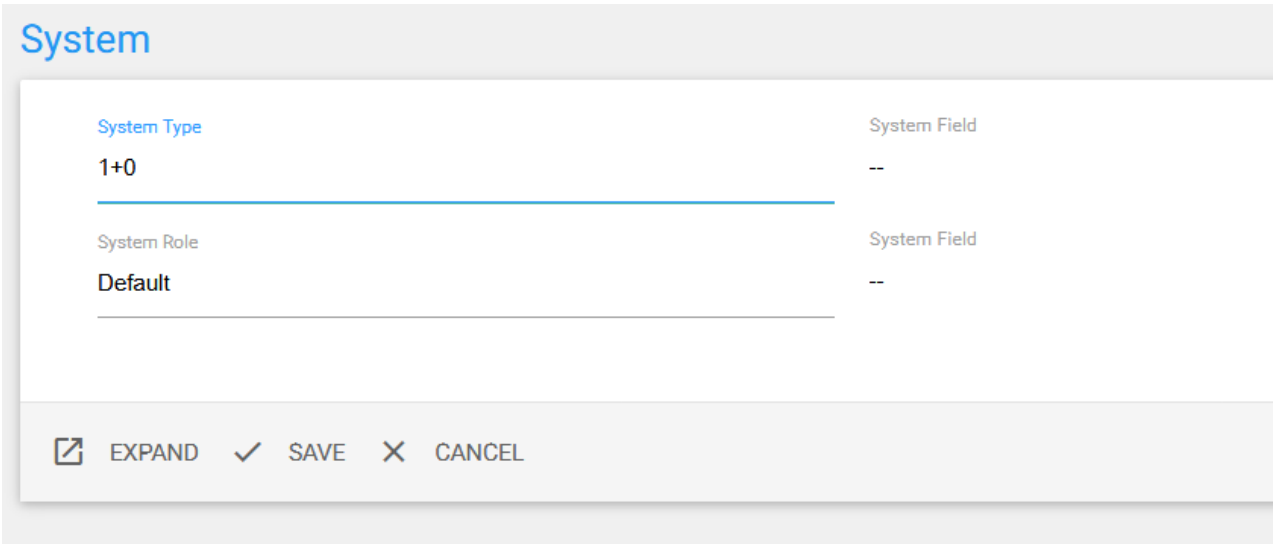
Please find below an example of 1+0 Unprotected link:



Picture 5.1 – Example of 1+0 Unprotected link

By default, the Y-Packet 2 is configured as 1+0 Unprotected, so no configuration at all is required for this kind of system type.

Please find below how to set the 1+0 Unprotected configuration at Y-Terminal **System Settings** page, **System** box.

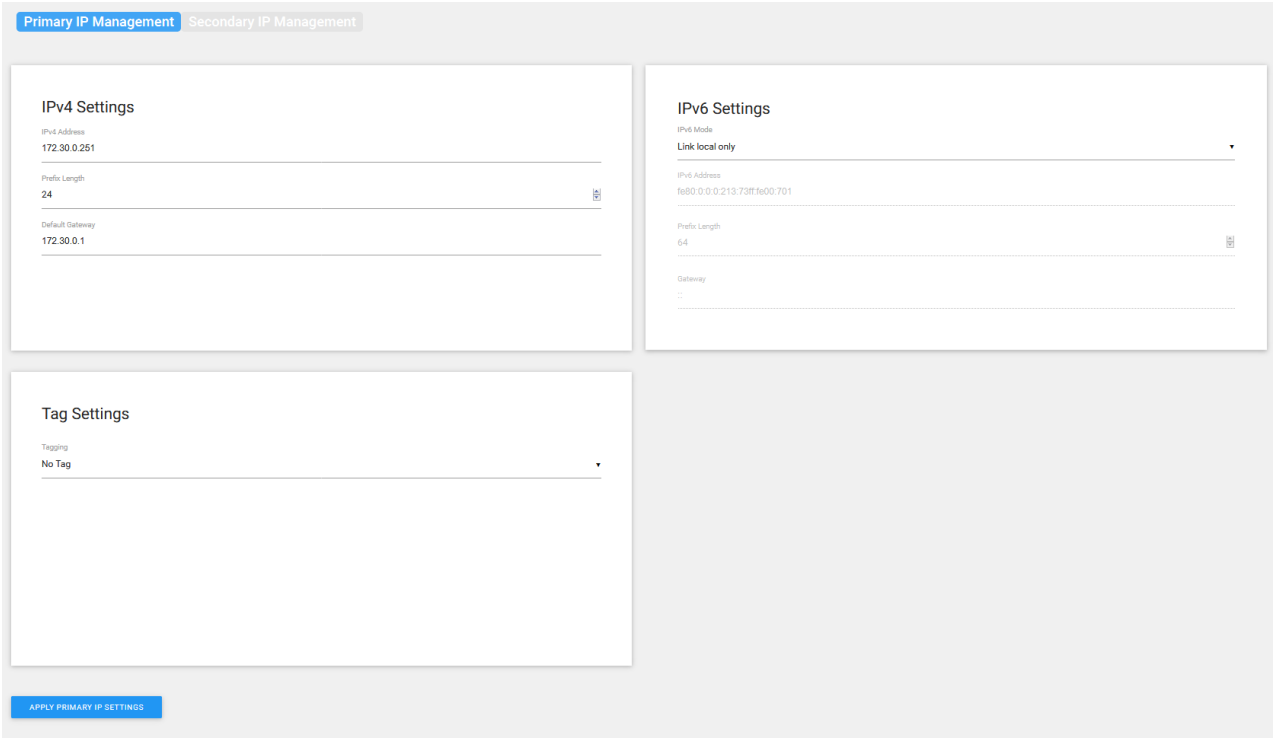


Picture 5.2 – Configuring 1+0 Unprotected system type at Y-Terminal

To edit System Type, user shall click on the **Edit** icon on bottom of **System** box, then choose "1+0" from scrolldown menu. Once selected, clicking on **Save** will write setting into equipment configuration, while a click on **Cancel** will close the edit window without applying the new setting.

6 Networking

This section explains how to configure network parameters on Y-Packet 2 in order to establish Layer 3 connectivity to Y-Terminal. In the first part we will explain how to configure IPv4 and IPv6, then we will explain how the Primary and Secondary management interfaces work. Here below you find the reference Y-Terminal **Networking** page, where all network parameters can be configured by user.



Picture 6.1 – Networking Y-Terminal page

6.1 Primary & Secondary Management Interfaces

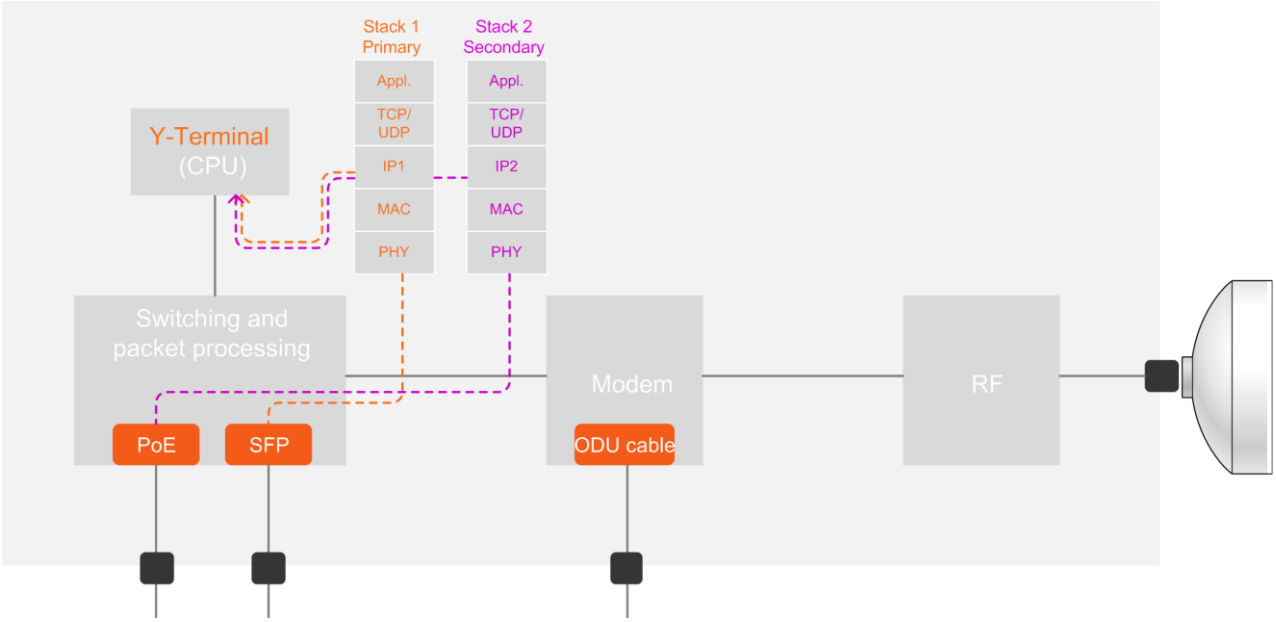
For management purposes, Y-Packet 2 uses two different TCP/IP stacks where the application services run, such as the Y-Terminal web interface. We will refer to these stacks as **Primary IP Management** and **Secondary IP Management**.

The double TCP/IP stack feature consists of two independent stacks, Stack 1 and Stack 2, sharing the same MAC address as well as the application layer services. Secondary IP Management uses Stack 2, and it has been implemented for local management only: it allows operator to perform management from a dedicated port, that is PoE port. By means of the Y-Terminal, PoE port can be configured as local management, and the Secondary IP Management assigned a dedicated IP address and VLAN ID. No access to Secondary IP Management is allowed from SFP optical port.

In case both SFP and PoE are configured as ordinary traffic ports, the Secondary IP Management interface is shut down, and only Primary IP Management can be reached, by any of the two Ethernet ports.

For a better understanding of how the Primary and Secondary Management work, pleased refer to the schemes below, where the two stacks are represented.

This picture describes the case of Secondary Management enabled, with the two Ethernet ports split on different stacks, Stack 1 and Stack 2.



Picture 6.2 – Connection to Y-Terminal when Secondary IP Management is enabled

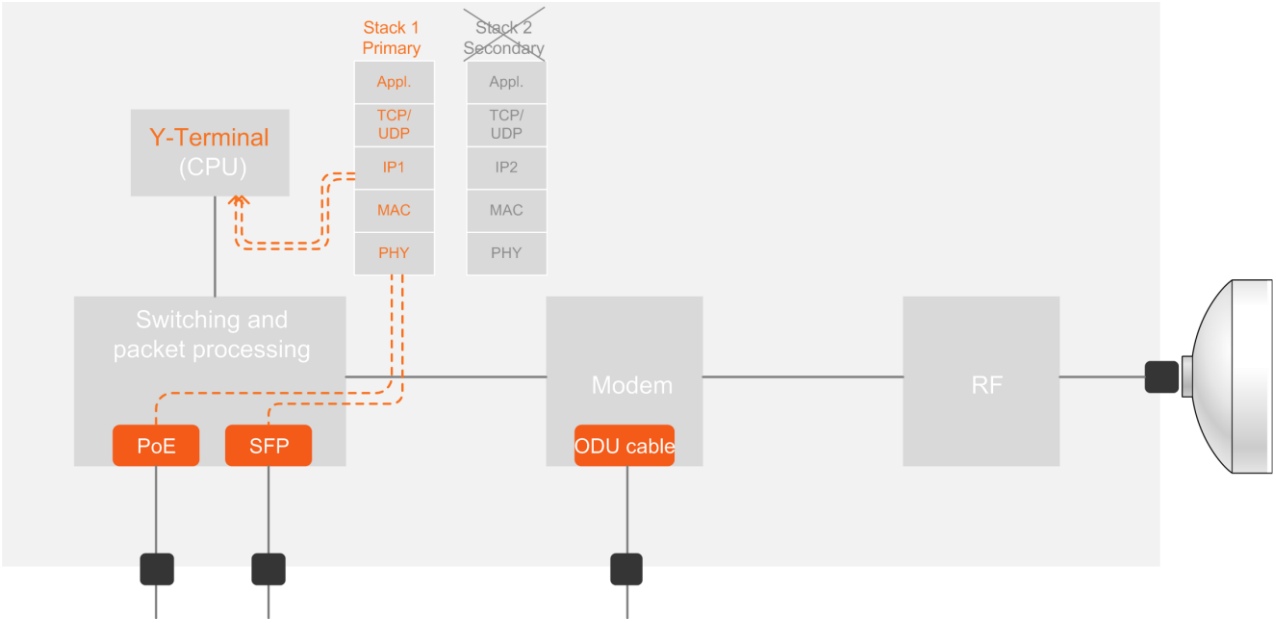
Secondary Management is enabled, so a user connected on PoE port will reach the Y-Terminal web management page on the Secondary IP Management only; access to Primary IP Management from PoE port is forbidden. The PoE is automatically configured by system to be used for management traffic only, so no data user traffic will be allowed on this port.

On the other hand, the SFP port is allowed to access to Primary IP Management only, and can forward both data user traffic and management traffic.

Secondary Management allows not only the management of local ODU, but management of the remote equipment also, as far as the Secondary IP Management has been enabled on the remote Y-Packet 2 as well.

Secondary IP Management doesn't use a gateway, so it can be reached on switched network only; one host trying to connect to a Y-Packet 2 cloud shall belong to the same IP subnet as the equipment network.

This second picture describes the case of Secondary IP Management disabled, where both Ethernet ports connect to Primary IP Management and the Secondary IP Management is shut down.



Picture 6.3 – Connection to Y-Terminal when Secondary IP Management is disabled

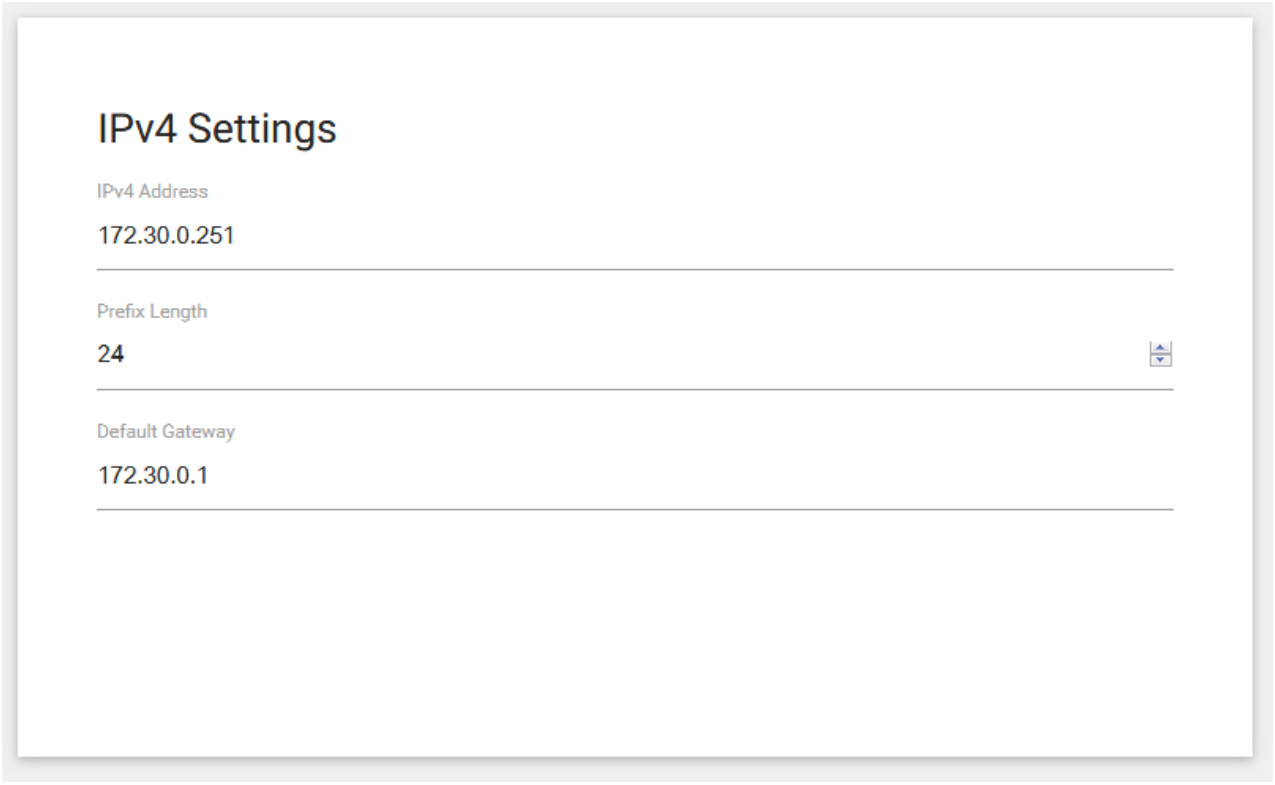
In this configuration, Secondary IP Management is shut down, so PoE and SFP can only connect to Y-Terminal on the Primary IP Management interface. Both port are allowed to forward data and management traffic.

6.2 IPv4 on Primary Management

In order to achieve Layer 3 connectivity to Y-Packet on **Primary IP Management**, IPv4 address shall be configured on the equipment. The IPv4 refers to management only, and has nothing to do with data traffic. The IPv4 address shall be assigned manually, as no dynamic assignment is supported.

Y-Terminal of any of the equipment is reached using its IPv4 address, that shall be defined uniquely in the network.

IPv4 settings for Primary IP Management can be configured at **Networking** Y-Terminal page, **Primary IP Management** tab, **IPv4 Settings** box.



Picture 6.4 – Configuration of IPv4 on Primary IP Management

At its factory default configuration, the units are preloaded with the following IPv4 addressing:

IPv4 Address: 172.30.0.251 for Low Band ODU, 172.30.0.252 for High Band ODU

Prefix Length: 24

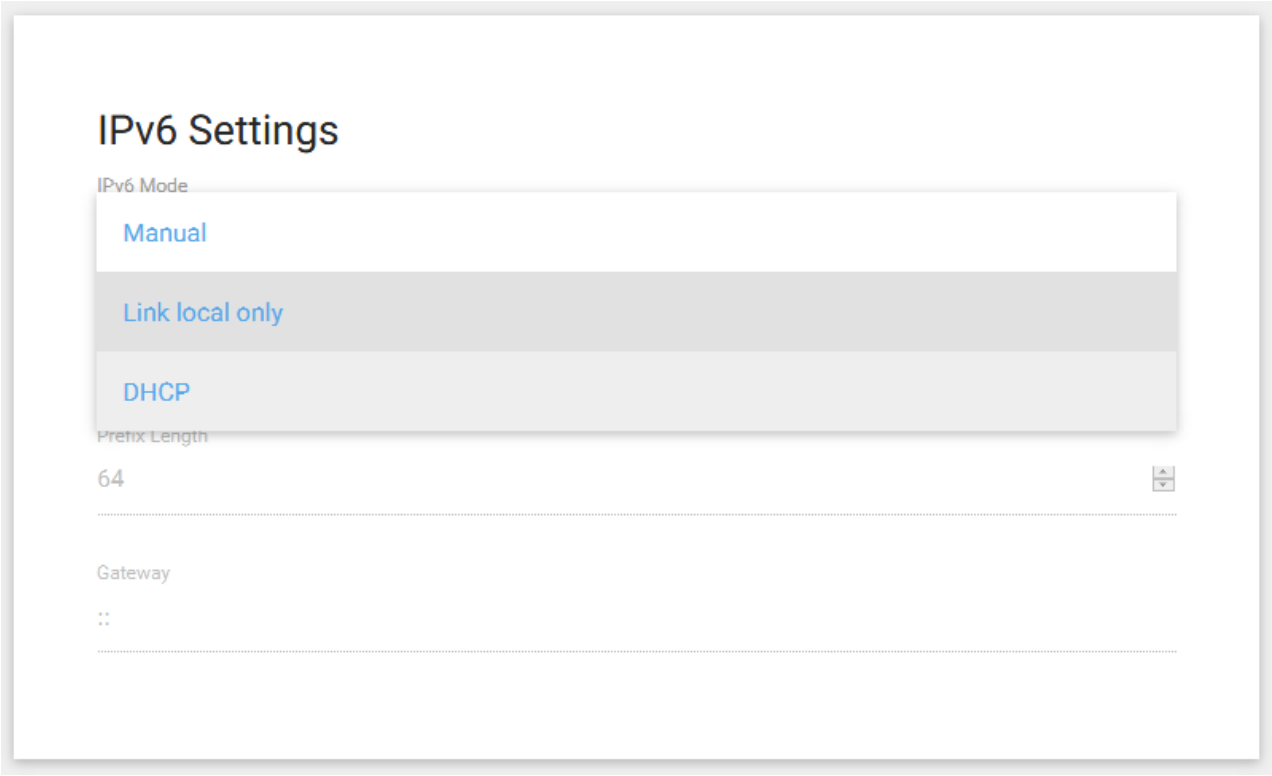
Default Gateway: 172.30.0.1

IPv4 address and Prefix Length can be changed, and any IP addressing (classful or classless) is supported. Primary IP Management interface uses a gateway, this means that it can be managed by hosts belonging to a different IP subnet, as long as the routing exists to the Y-Packet 2 network. The Default Gateway shall belong to the same IP subnet as the IPv4 address of the equipment.

6.3 IPv6 on Primary Management

In addition to IPv4, Y-Packet 2 supports, on Primary IP Management only, IPv6 network layer protocol. While IPv4 addresses have a 32-bit value, IPv6 addresses have a size of 128 bits: therefore, IPv6 has a vastly enlarged address space compared to IPv4. Support for IPv6 on Y-Packet 2 means that some application, mainly the Y-Terminal web management interface, can be run on IPv6. The IPv6 128-bit address can be either assigned manually or as stateless autoconfiguration (SLAAC).

IPv6 on Primary IP Management can be configured at **Networking** Y-Terminal page, **Primary IP Management** tab, **IPv6 Settings** box. IPv6 can be enabled by operator in one of the three available modes: **Link Local Only**, **Manual** or **DHCP**.



Picture 6.5 – Configuration of IPv6 Mode on Primary IP Management

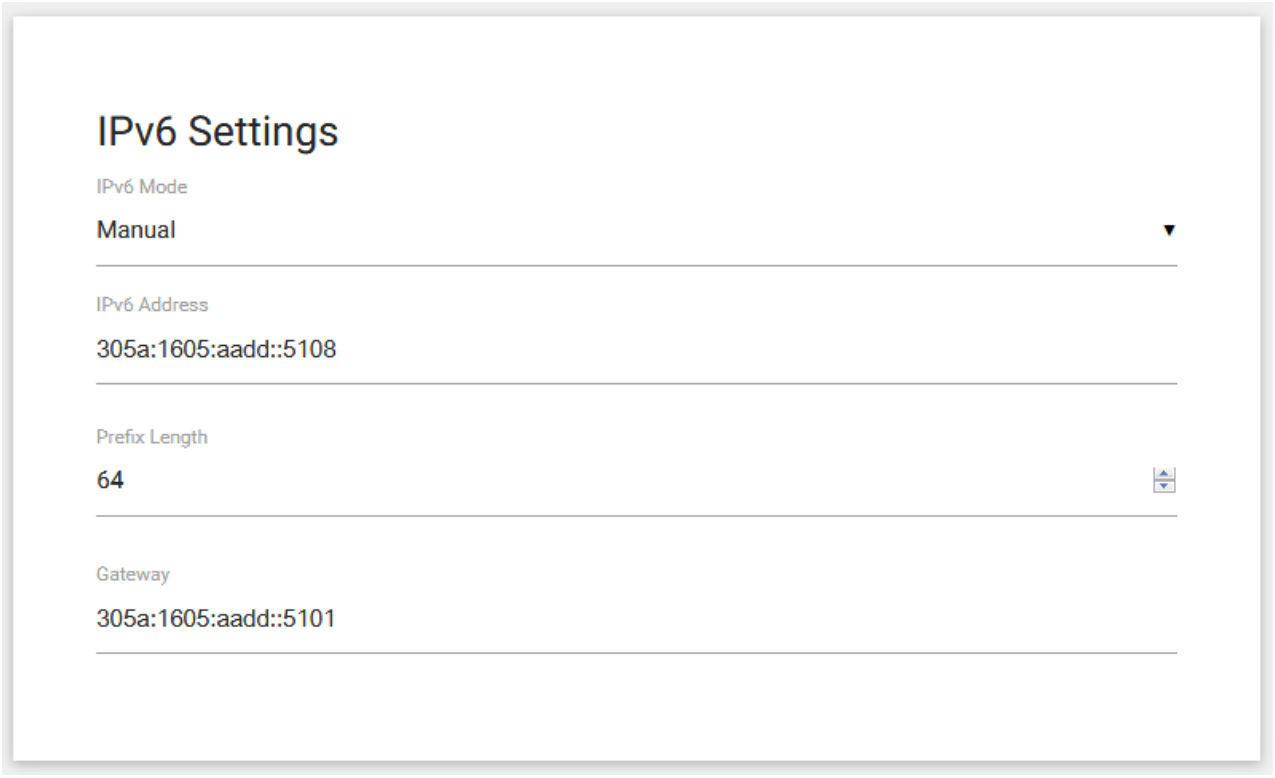
In Manual configuration the user shall set manually all 128 bits of the address as:

IPv6 Address: it is the 128 bits address of the Y-Packet 2, used for Layer 3 connectivity on IPv6 to management interface

Prefix Length: the net prefix of the IPv6 address, containing: the "routing prefix" combined with the "subnet id" in the first most significant 64 bits, and the "interface identifier" in the least significant 64 bits. The "interface identifier" is 64 bits either when the IPv6 address is automatically generated from the interface's MAC address using the modified EUI-64 format, or obtained from a DHCPv6 server, or also assigned manually

Gateway: it is the IPv6 address of the gateway, used for IPv6 routing

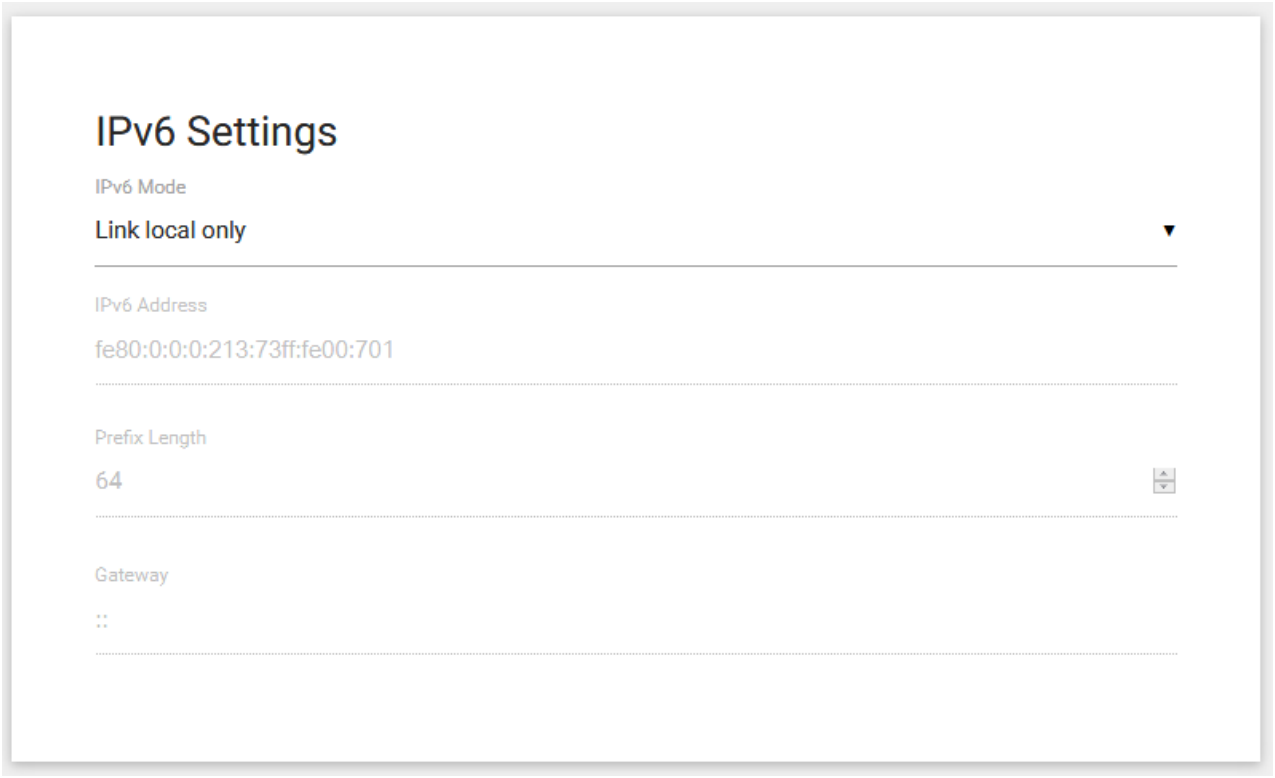
When IPv6 on Y-Packet 2 is configured in Manual mode, in addition to the manual IPv6 address the interface self assigns also a Link Local Only address.



Picture 6.6 – Configuration of IPv6 as Manual mode

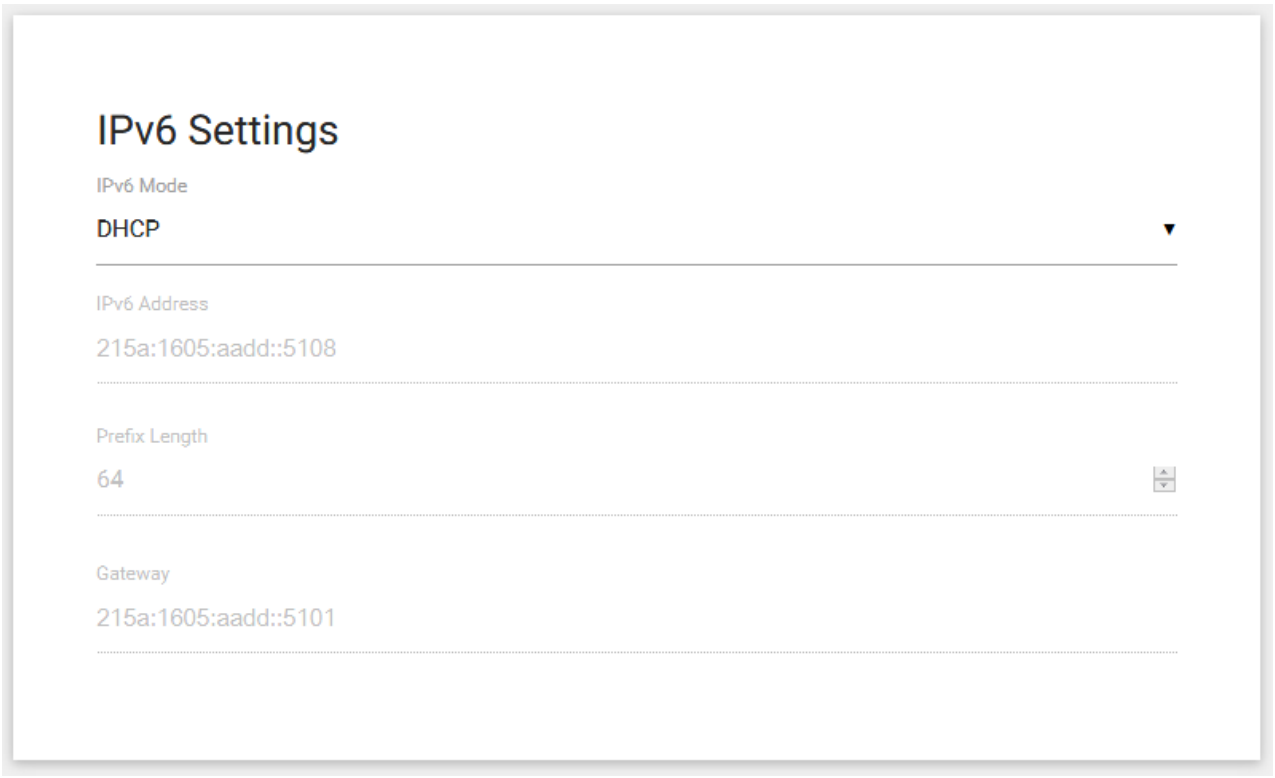
In SLAAC mode (stateless autoconfiguration), the host is capable of self assigning the IPv6, having prefix length fe80::/10 and the 64 rightmost set according to the EUI-64 bit identifier derived from the MAC address. Since the MAC is unique, the IPv6 is unique and its meaning is local: thereby it will not be routed. Within the SLAAC mode, Y-Packet 2 supports two different options, which are **Link Local Only** and **DHCP**.

In **Link Local Only** mode, the management interface shall self assign an IPv6 address according to the RFC 4291, but not changing the net prefix even if advertised by a router on the local area network: this means that any router advertisement shall be ignored. In the Link Local Only address, the 64 rightmost bits of the IPv6 address are the same for all hosts (fe80::/64 link-local address prefix), rendering them non-routable.



Picture 6.7 – Configuration of IPv6 as Link Local Only mode

In DHCP mode, the management interface shall listen to possible router advertisements to receive a IPv6 address and change its net prefix accordingly; in addition to IPv6 address assigned by router, the interface shall self assign also a Link Local Only address, as in RFC 4291. The default gateway shall be also acquired by means of advertisements from a local router.



Picture 6.8 – Configuration of IPv6 as DHCP mode

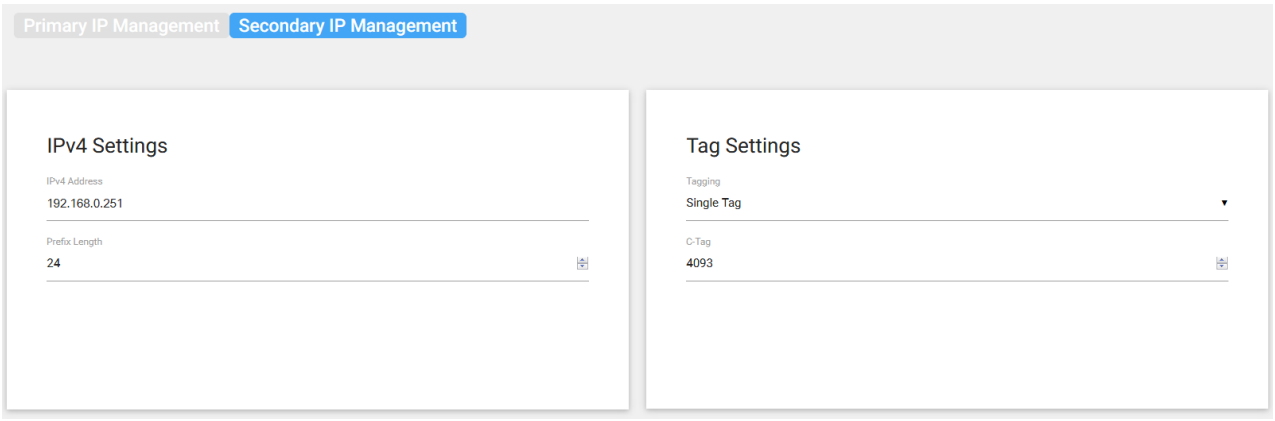
6.4 IPv4 on Secondary Management

In order to achieve Layer 3 connectivity to Y-Packet on **Secondary IP Management**, IPv4 address shall be configured on the equipment. The IPv4 refers to management only, and has nothing to do with data traffic. The IPv4 address shall be assigned manually, as no dynamic assignment is supported.

Please note that Secondary IP Management is reachable from PoE port only.

Y-Terminal of any equipment in a network is reached using its IPv4 address, that shall be defined uniquely in the network. Operator shall be aware that Secondary IP Management doesn't use a gateway, and is thus reachable by host belonging to the same IPv4 subnet only.

IPv4 settings for Secondary IP Management can be configured at **Networking** Y-Terminal page, **Secondary IP Management** tab, **IPv4 Settings** box.



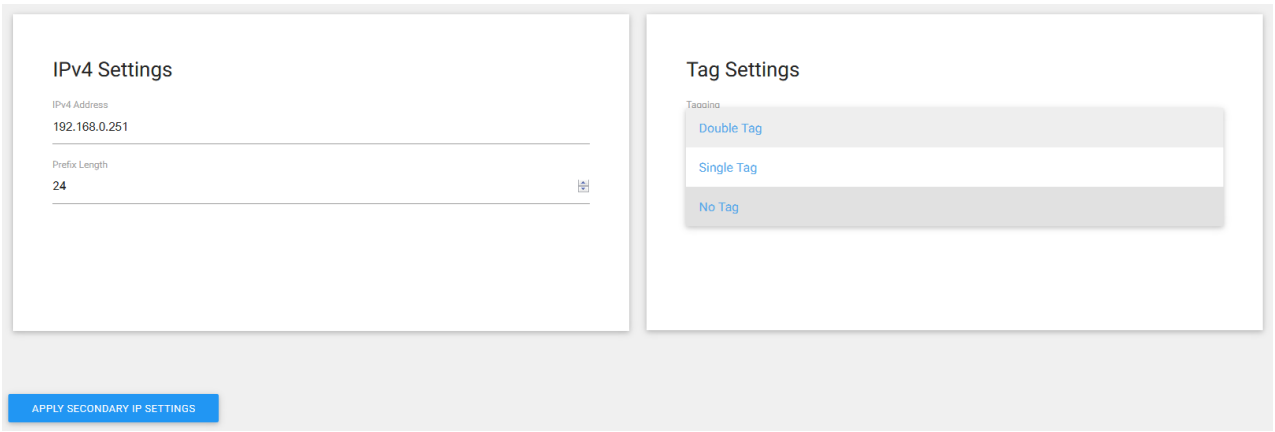
Picture 6.9 – Configuration of IPv4 on Secondary IP Management at factory default

At its factory default configuration, Secondary IP Management is preloaded with the following IPv4 addressing:

IPv4 Address: 192.169.0.1 for Low Band ODU, 192.169.0.2 for High Band ODU

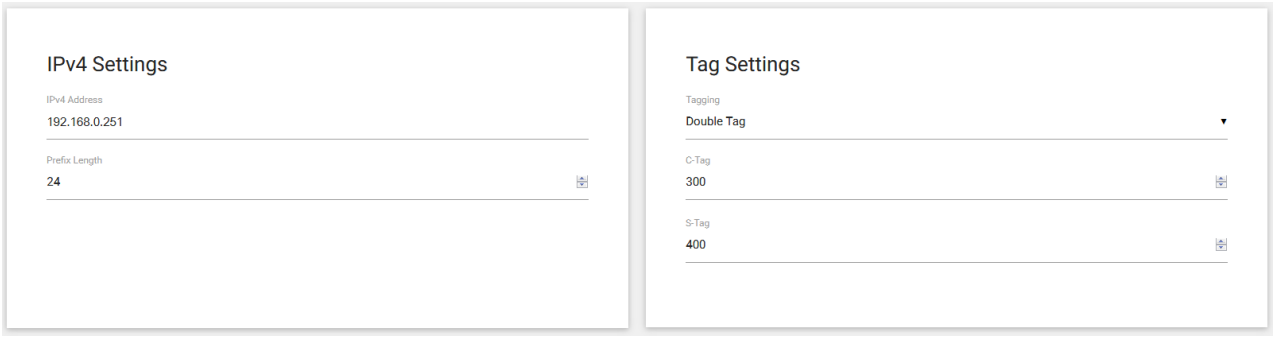
Prefix Length: 24

Tagging: No Tag

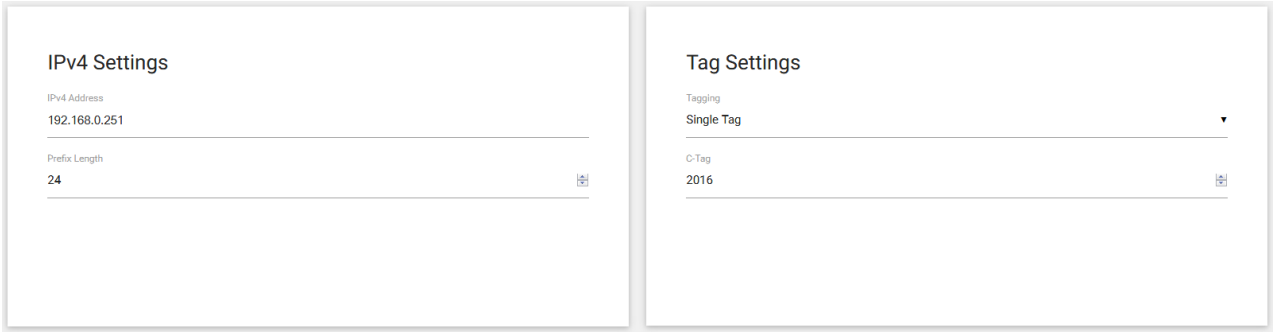


Picture 6.10 – Changing Tag Settings on Secondary IP Management

Please find below two possible changes for the Secondary IP Management: in the first case, the Tag Setting is set to Double Tag, and the C-Tag and S-Tag configured; in the second case it is Single Tag and the C-Tag shall be configured.



Picture 6.11 – Configuration of Tag Settings as Double Tag on Secondary IP Management



Picture 6.12 – Configuring C-Tag for Single Tag mode on Secondary IP Management

7 User Settings

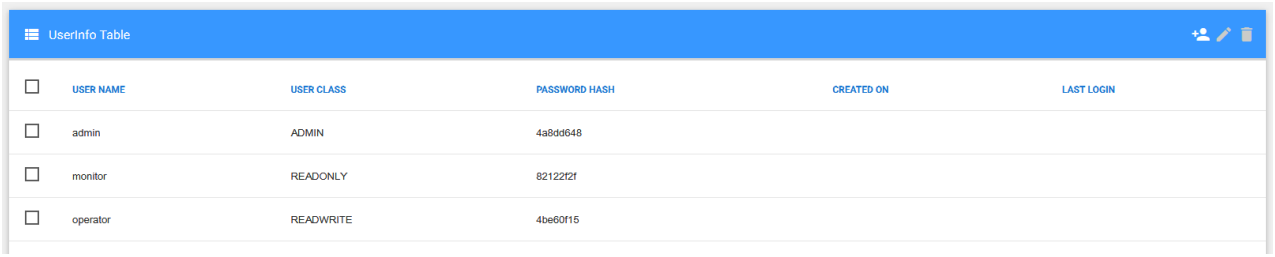
This section describes how access to Y-Terminal is organized, in terms of users and levels of user rights.

Three levels of users are implemented on Y-Packet 2: Admin, Operator and Monitor. On Y-Terminal **User Settings** page, customer can setup the desired configuration for users. For all what follows, we will consider to be logged in as Admin class users, as Admin users are the only ones who have the rights to create, modify, remove other users. The other two classes of users, Operator and Monitor, aren't even displayed the User Settings page in the Main Menu of Y-Terminal when logged in.

For details of rights associated to each level, please refer to following paragraphs.

At its factory default configuration, Y-Packet 2 comes with three built-in users: one has administrative rights (admin), the second has read-only rights (monitor) and the third (operator) has read-write rights.

The user with Admin rights is **admin**, and its password is **port_adm**; password can be changed, nevertheless this user cannot be deleted. The user with read-only rights is **monitor**, and its password is **port_mon**; password can be changed, and user can be deleted. The user with read-write rights is **operator**, and its password is **port_op**; password can be changed, and user can be deleted.

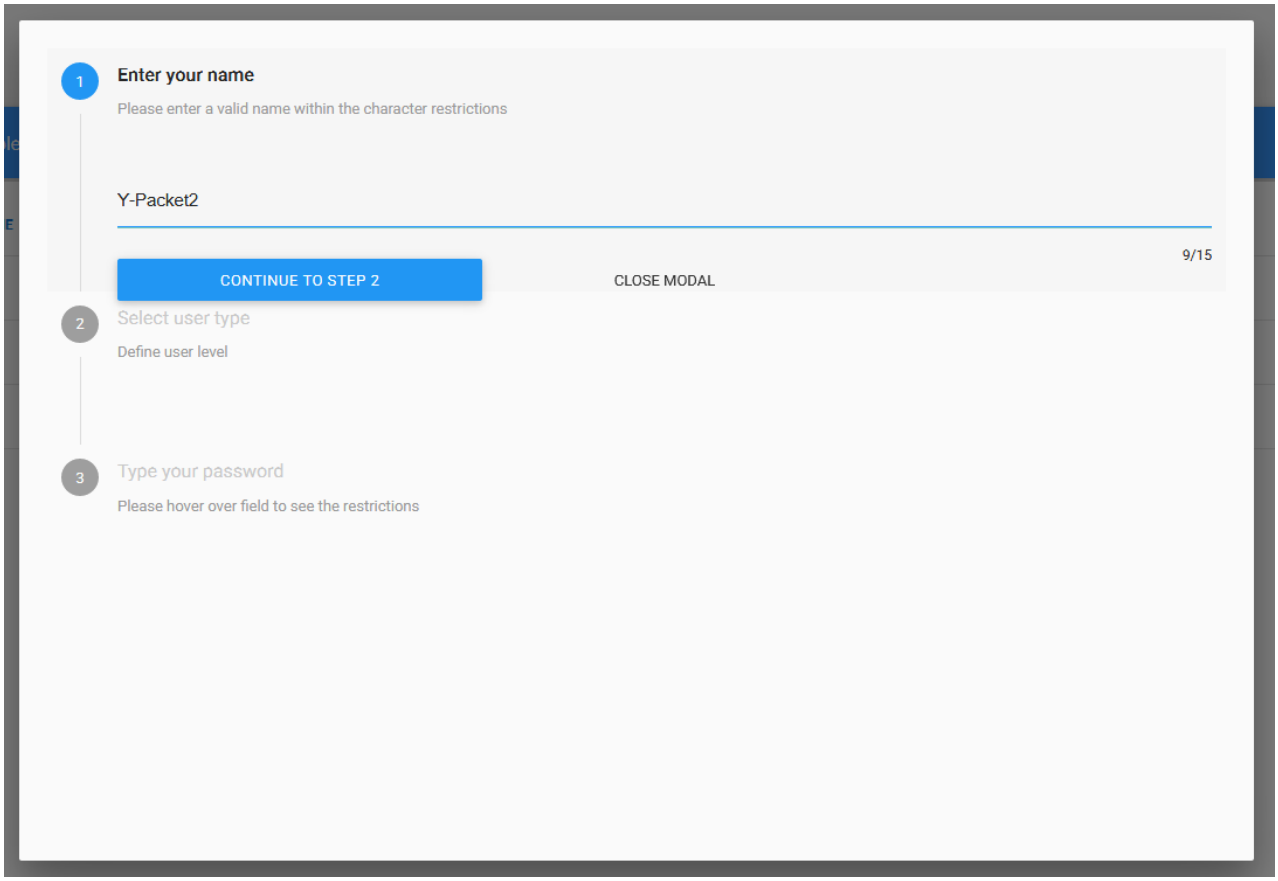


Picture 7.1 – Y-Terminal User Settings page, with the three default users

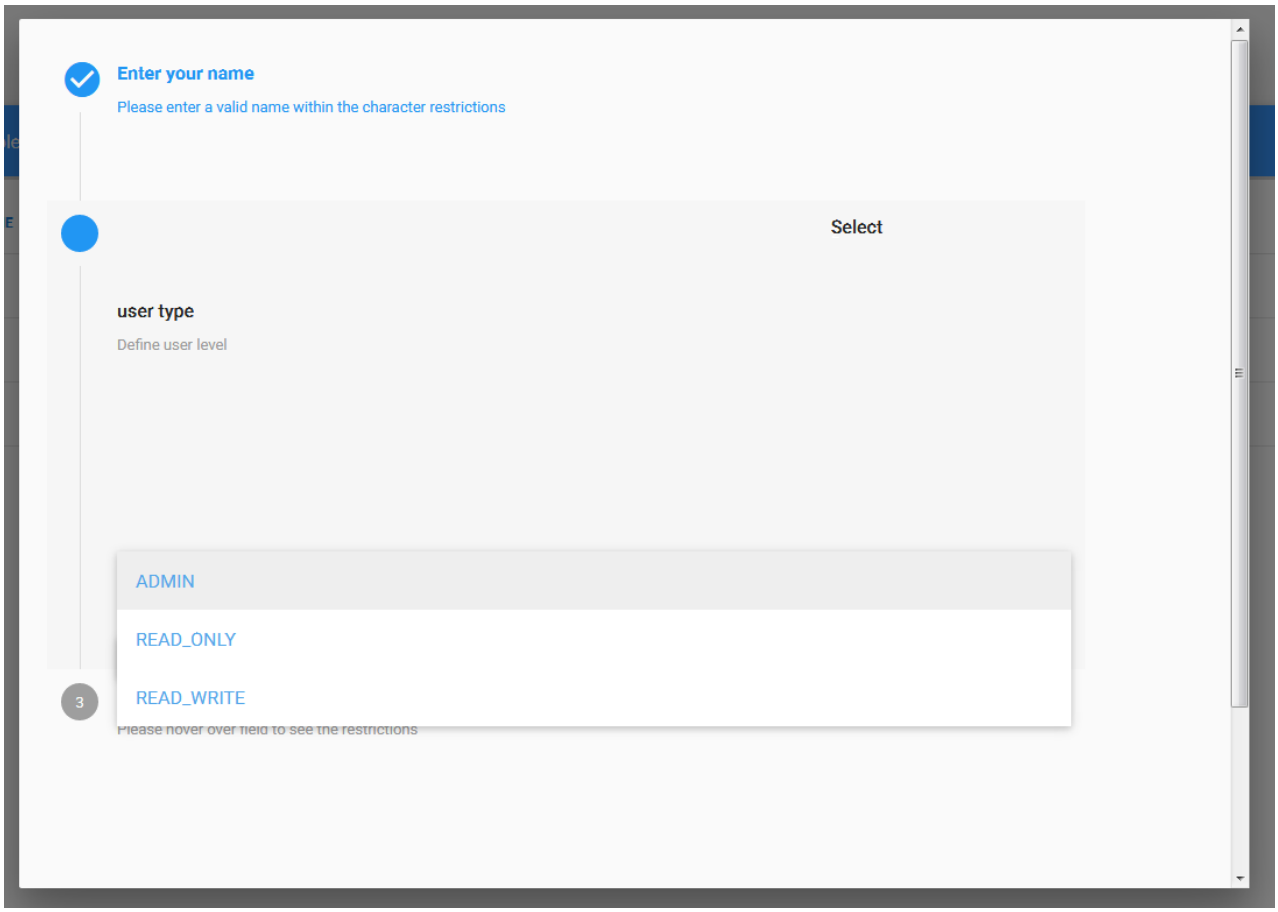
On **User Settings** page, operator can add new users, and remove or change password to existing users. Up to 10 users can be created, and no limitations are there in terms of users class these new users belong to. Thus, operator is free to create any number of Admin, Operator, Monitor users in the above table.

To add a new user, operator shall click on **Add User** icon; a stepper window will be started, where **Username**, **User Class** and **User Password** are required. At the end of the step process, the new user will be added to the User table. Date of creation will be also traced in the table.

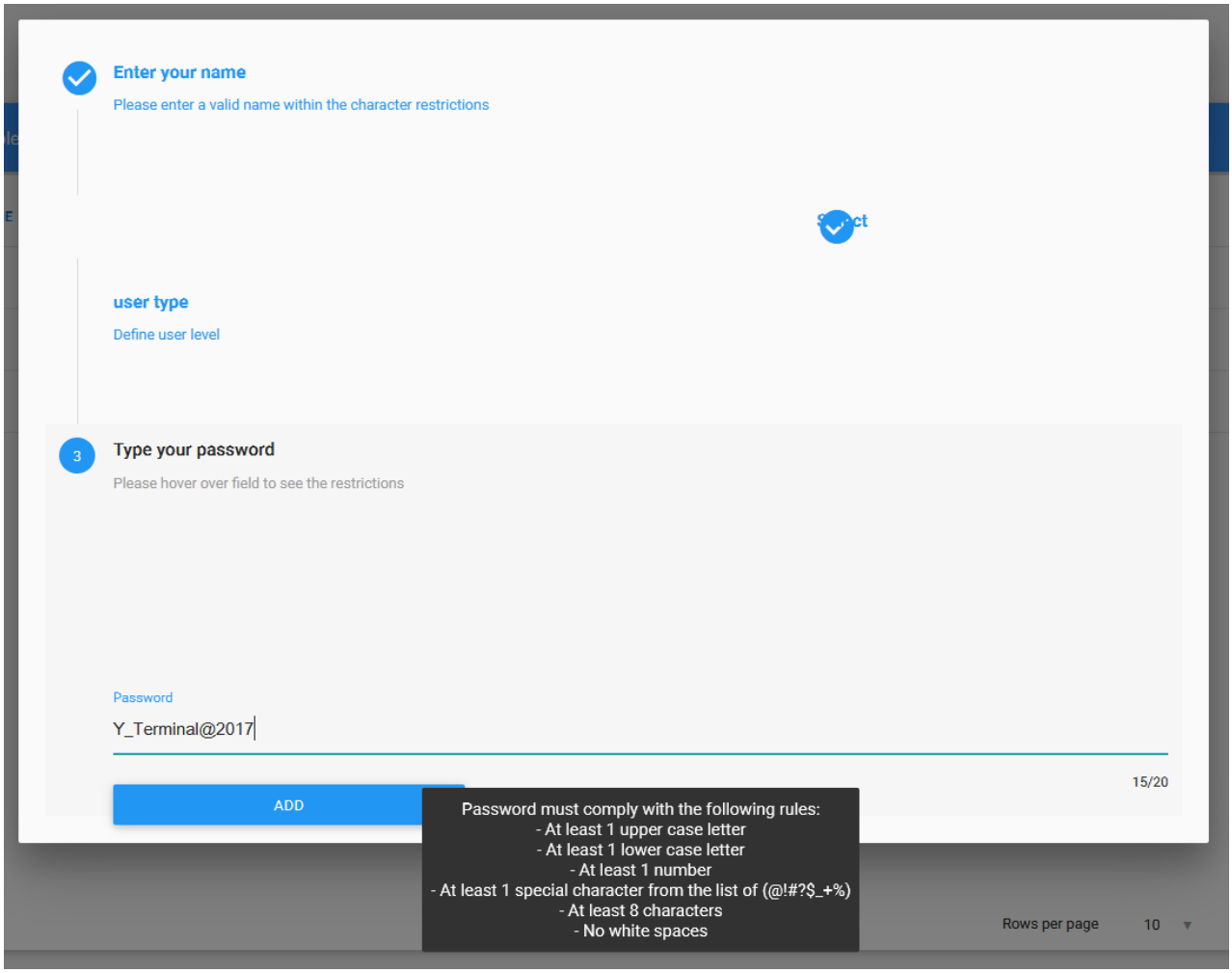
Please find below the three steps to create a new user:



Picture 7.2 – Step 1, insert Username



Picture 7.3 – Step 2, insert User Type



Picture 7.4 – Step 3, insert Password

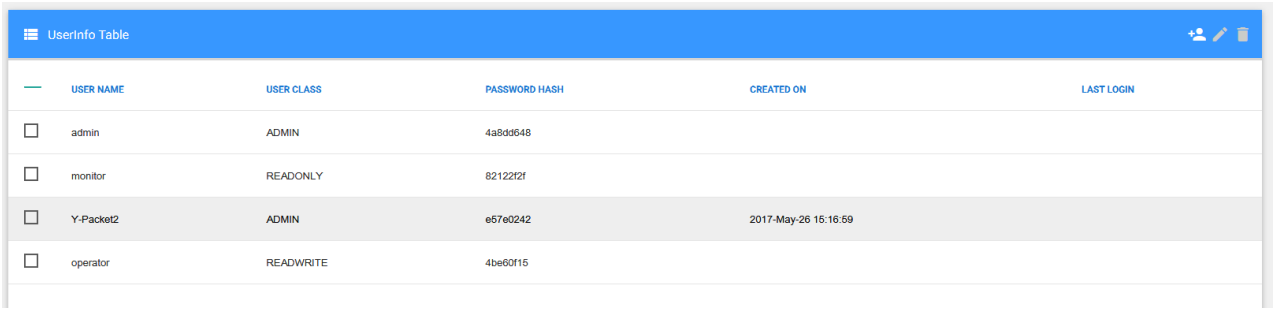
Please find below the properties for each user field:

! **Username**: it is an alphanumeric string, shall be at least 6 characters, shall not contain special characters

! **User Class**: it is the class identifying the rights associated to each user, it can be Admin, Read-Only or Read-Write, and it can be selected from a scrolldown menu.

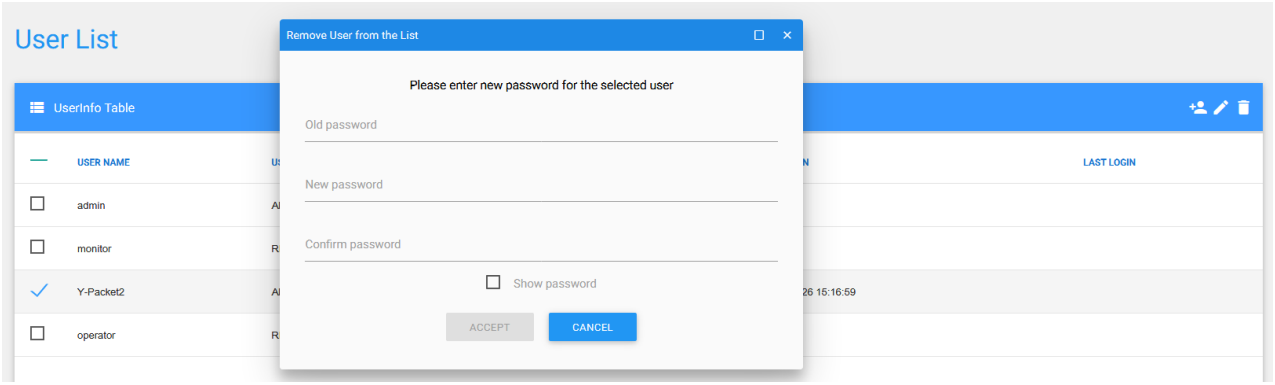
! **Password**: it is an alphanumeric string, shall be at least 8 characters, and shall contain at least: one upper case letter, one lower case, one numeric character, one special character from the list specified in the info window, no white spaces

The picture below shows an example of new user with Admin rights.



Picture 7.5 – New Admin class user

In order to change password to an existing user, the desired user shall be selected first; then, clicking on **Edit User** icon a window will be opened, where operator is asked to introduce **Old Password**, **New Password**, **Confirm New Password**.



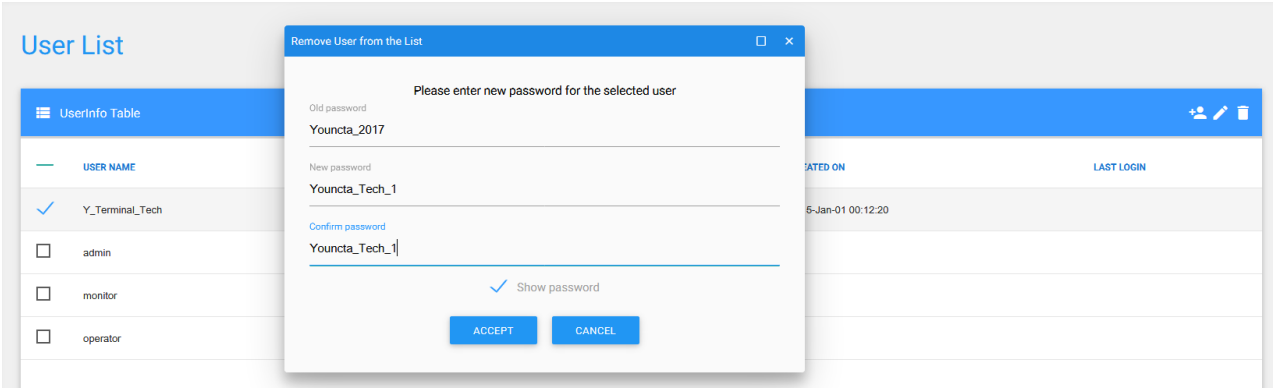
Picture 7.6 – Window for changing password to an existing user

! **Old Password**: it is the current user password we want to change; it is an alphanumeric string, shall be at least 8 characters, and shall contain at least: one upper case letter, one lower case, one numeric character, one special character from the list specified in the info window, no white spaces

! **New Password**: it is the new password; it is an alphanumeric string, shall be at least 8 characters, and shall contain at least: one upper case letter, one lower case, one numeric character, one special character from the list specified in the info window, no white spaces

! **Confirm Password**: it is the new password repeated, it is introduced to avoid mistyping when writing the password field

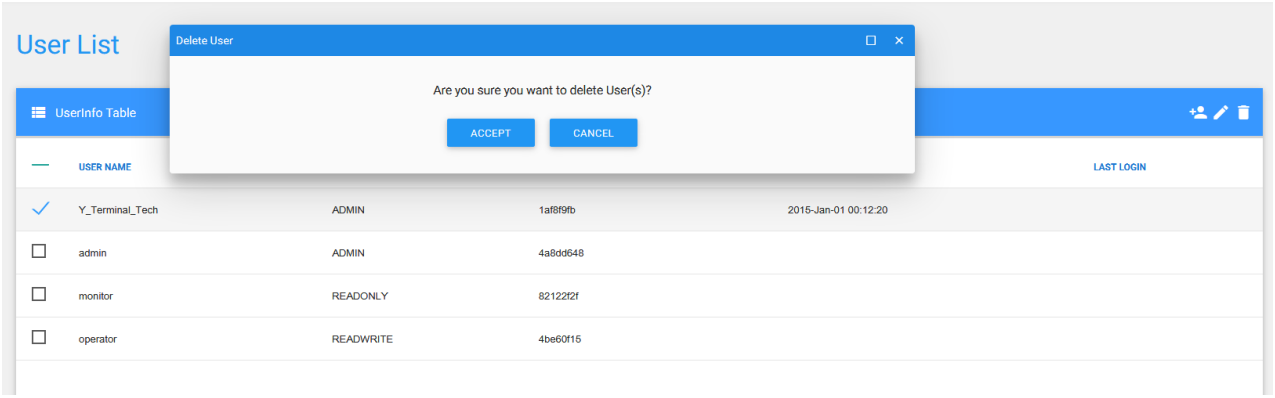
Please find below an example of changing password to an existing user.



Picture 7.7 – Changing password to an existing user

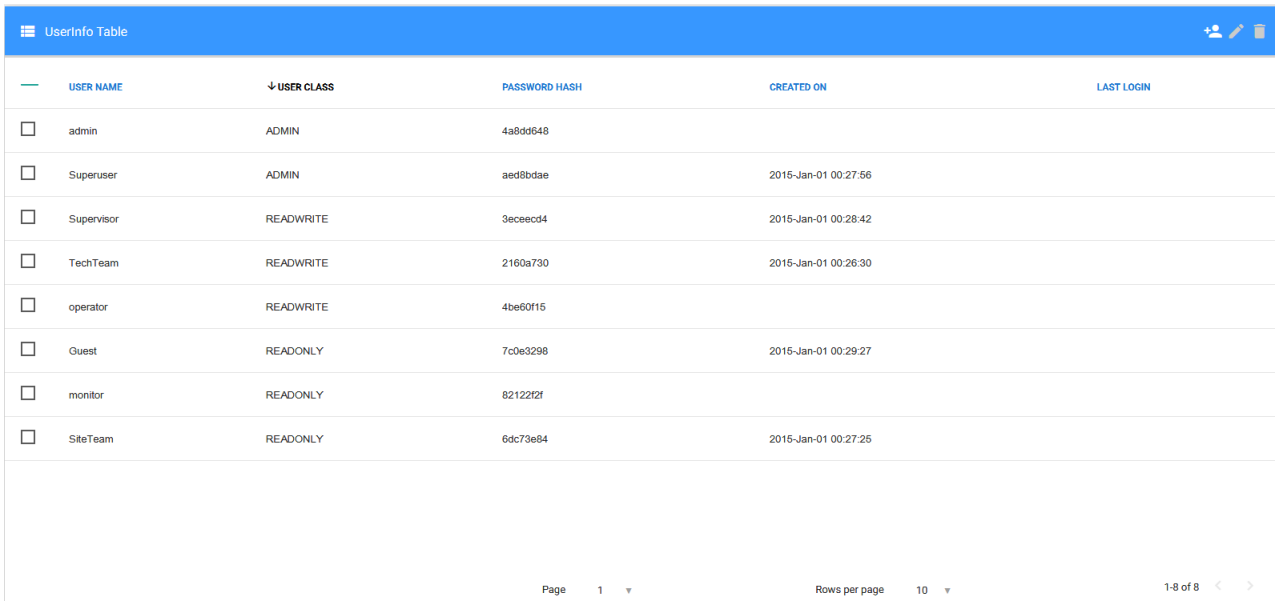
When changing password, operator can choose if showing the passwords or not, by means of the **Show Password** check-box.

In order to remove an existing user, the desired user shall be selected and highlighted first; then, by clicking on **Remove User** icon, user will be asked for confirmation he wants to delete that user; clicking on Accept, user will be deleted.



Picture 7.8 – Removing an existing user

Please find below an example of **Users** table, with eight users created; as it can be seen, there are no constraints in terms of how many users for each user class can be created in the table.



Picture 7.9 – Example of table of users, belonging to different user classes

7.1 Levels of Users

In this section we will provide detail of the rights associated to each of the three user classes, namely: Admin, Read-Write and Read-Only.

Generally, we can summarize saying that:

! Admin: this user belongs to Admin class; has full configuration and administration rights on the equipment; and has full rights to add, modify, delete all other users

! Operator: this user belongs to Read-Write class; has full configuration and administration rights on the equipment; has no rights at all on users, including not being able to change his own password (he is not even displayed the **User Settings** Y-Terminal page when logging in)

! Monitor: he belongs to Read-Only class; has no configuration and administration rights on the equipment; has no rights at all on users, including not being able to change his own password (he is not even displayed the **User Settings** Y-Terminal page when logging in)

Now we will explain the access policies among different types of users:

! User with **write** permissions: Admin and Read-Write users belong to this category. Once that one user, having write permissions on the equipment, is logged into the Y-Terminal, no more users with write permissions are allowed to login to the web management interface. This is done in order to avoid that concurrent, and possibly different configurations, be done at the same time from two different users

! User with **read** permissions: Read-Only users belong to this category. A user with read permissions is allowed to access to the Y-Terminal any the type of other user that might be already logged in

The maximum number of concurrent sessions is two, regardless that both can be Read-Only users or one Read-Only and one Admin or Read-Write.

8 Timing & Synchronization

When managing and monitoring a network of several devices, it is strongly recommended that administrators set date and time on all equipment, in order to have valid timestamps in the Event History logs and Performance/Statistics collections. In case date and time are not aligned in a link or network, it will be difficult to perform troubleshooting or fault management, as no correlation will be possible between alarm timestamps on the two sides of the link. This chapter will explain how to synchronize date and time on the Y-Packet 2.

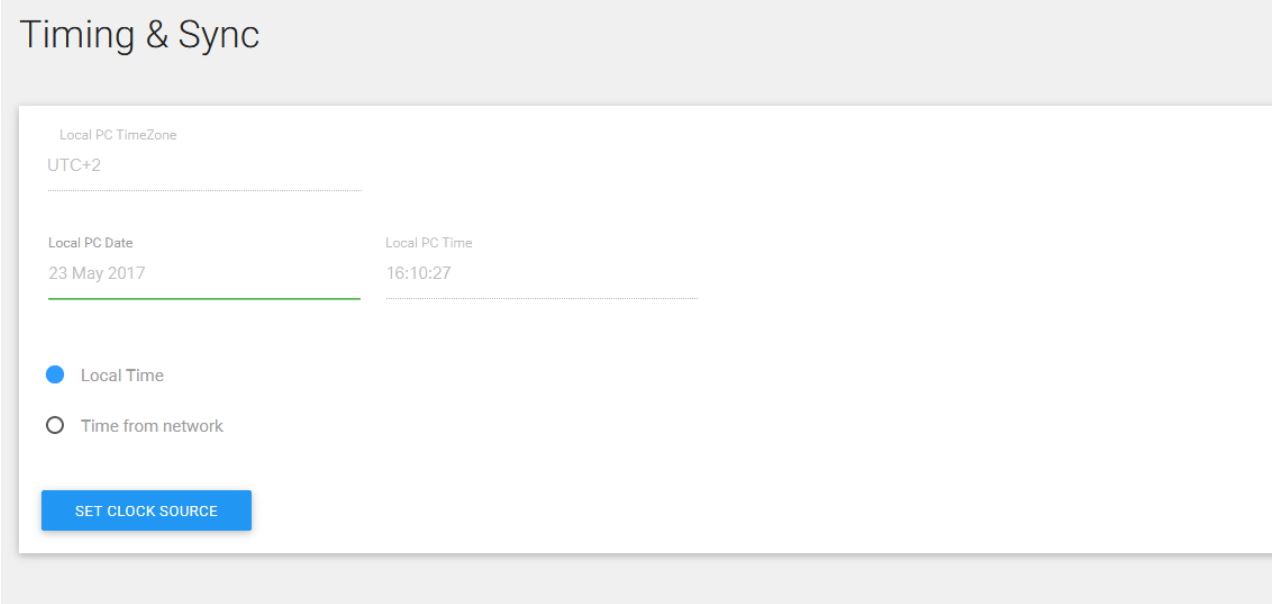
8.1 Local time

By default, when the Y-Packet 2 is started, it uses date 01 Jan 2010, so operator needs to update timing data, and lock it to some common source. One quick choice is to lock to the Local PC time: this can be done by opening Timing & Sync page in the Y-Terminal, then selecting the Local Time option and clicking on the Set Clock Source button.
Although this choice synchronizes date and time on the equipment, user shall be aware that:

! Date and time are lost every time the equipment is power cycled or rebooted. So, after each reboot, operator will need to manually re-synchronize Y-Packet 2 to Local PC.

! There can be cases where local PC belongs to a different time zone than the one where the equipment is installed, so care must be taken that equipment is locked to a valid local source.

Please find below how to update date and time to local PC time:



Picture 8.1 – Synchronizing date and time to local PC time on Y-Terminal

Date and time are locked to following parameters:

! Local PC TimeZone: it is retrieved from PC, and cannot be changed

! Local PC Date: it is retrieved from PC, so in case it is changed on the PC, also on the Y-Packet 2 it will be changed (it is required that user clicks on **Set Clock Source** button after changing date on the PC)

! Local PC Time: it is retrieved from PC, so in case it is changed on the PC, also on the Y-Packet 2 it will be changed (it is required that user clicks on **Set Clock Source** button after changing time on the PC)

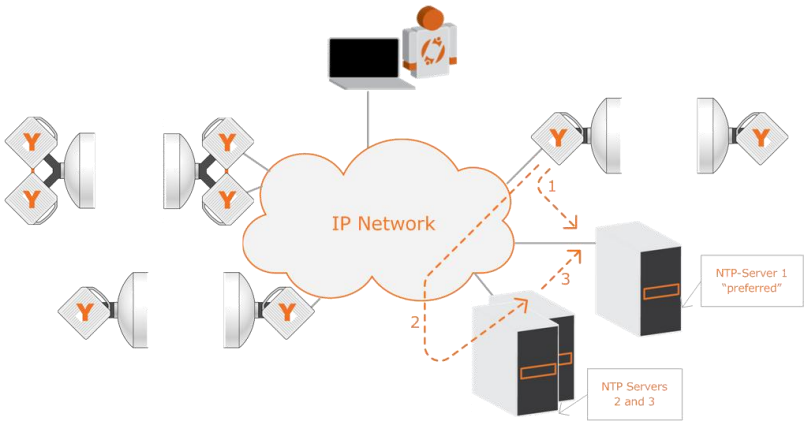
Once that the Y-Packet 2 date and time are aligned to local PC time, although the PC might be disconnected, the equipment will increment date and time following its internal clock.

8.2 Time from Network (NTP)

This section introduces the basic working of NTP protocol on Y-Packet 2. NTP stands for Network Time Protocol, and it is used to synchronize the clocks of computers and devices to one or more time references. The protocol is implemented on Y-Packet 2 in terms of a client-server model, where Y-Packet 2 acts as a client and up to three different NTP servers can be configured.

Once that the NTP process has been enabled, each of the configured and enabled NTP Servers will be polled by system. One of the NTP servers (NTP-Server 1), is marked as “preferred”: this means that, although synchronized with any of the remaining 2 servers, the system will check availability of preferred NTP-Server 1, and synch to it where service available.

With reference to the network below, this is how NTP client works on Y-Packet 2:



Picture 8.2 – NTP network reference scenario

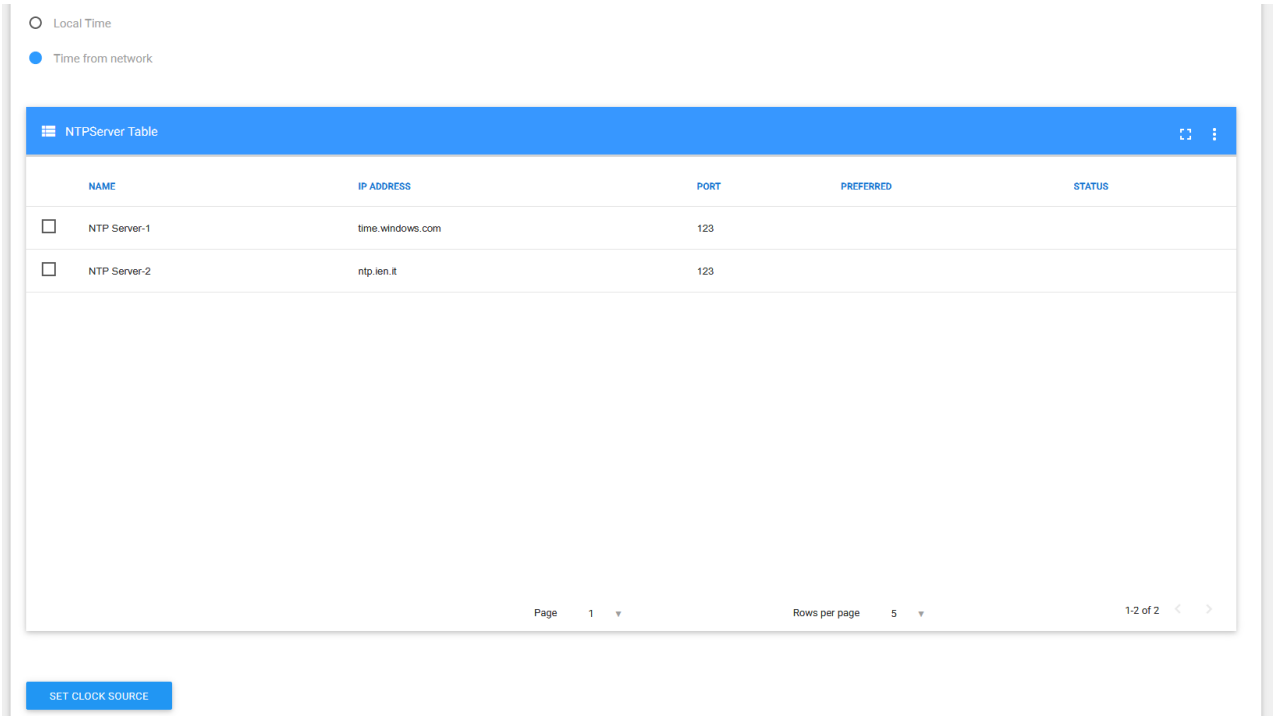
1 – Y-Packet 2 sends a NTP synchronization request to NTP-Server 1 "preferred". If NTP-Server 1 is not available, then 2

2 – Y-Packet 2 sends a NTP synchronization request to NTP-Servers from 2 to 3, synchronizing to the first available one. Although synchronized to NTP Server 2 or 3, after some time it goes to 3

3 – Although synchronized, Y-Packet 2 sends again a NTP synchronization request to NTP-Server 1 "preferred", trying to synchronize to it

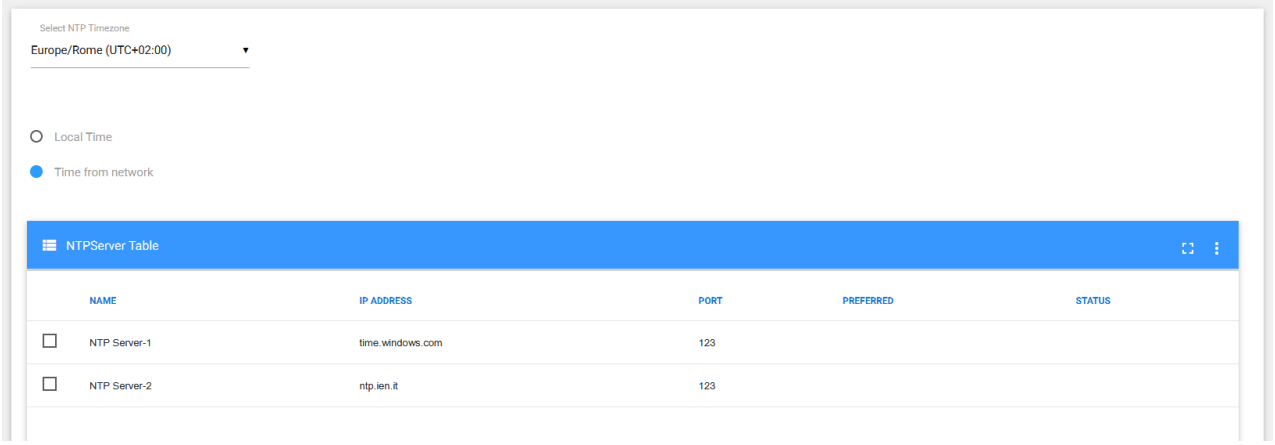
The NTP settings can be configured by opening **Timing & Sync** page in the Y-Terminal, then selecting the **Time from network** option and clicking on the **Set Clock Source** button.

Once that the NTP client has been enabled, each of the configured NTP Servers will be polled by system. Three default NTP Servers are provided, with domain name of NTP servers to synchronize to. Clicking on **Set Clock Source** button is then required to apply the desired configuration.



Picture 8.3 – Configuring NTP as synchronization source

NTP can synchronize to a time reference, but no information about local time zones or daylight saving time is transmitted. Thus, it is required that all settings about time zones and daylight savings be configured manually by user at Y-Terminal. For those regions where the time zone contains fractions of hours, a list of all possible fractional time zones is provided.



Picture 8.4 – Configuring Time zone

In case NTP is enabled, please note that:

! Date and time are lost every time the equipment is power cycled or rebooted. With NTP enabled, Y-Packet 2 will automatically attempt a re-synchronization with the configured NTP servers every 15 seconds, until synchronized status is reached.

9 SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol for exchanging management information between network devices. SNMP provides a method of managing network hosts from a centrally-located server running network management software. SNMP performs management services by using a distributed architecture of SNMP "managers" and "agents".

Because network management is critical for both auditing and resource management, SNMP can be used to:

! configure remote devices; configuration information can be sent to each host from the management system

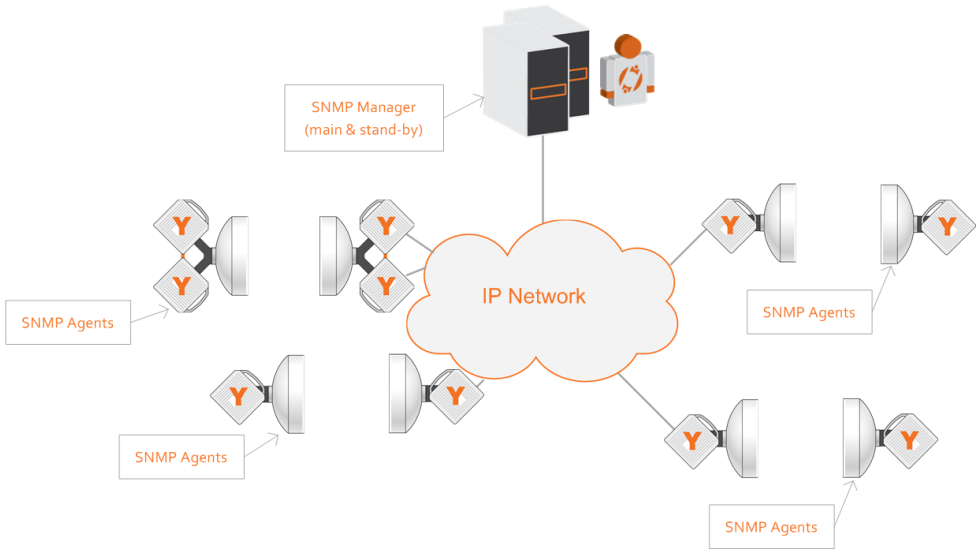
! monitor network performances; you can track the network throughput and collect information about data transmission

! detect network faults or inappropriate access; you can configure trigger alarms on network devices when certain events occur; when an alarm is triggered, the device forwards an event message to the management system.

SNMP basic components are **SNMP Managers** and managed devices where **SNMP agent** is running; both managers and agents process their operation based on equipment Management Information Base, otherwise called **MIB**. We will list for all components their basic functionalities.

SNMP Manager: a management system that is responsible to communicate with the SNMP agents implemented in each managed network device. This is typically a computer or server that is used to run one or more network management system. SNMP Manager's key functions are: send queries to agents, getting responses from agents, setting variables in agents MIBs, acknowledging asynchronous events from agents.

SNMP Agent: the program that is packaged within the managed network device. SNMP agent collects the info from the MIB device locally and makes it available to the SNMP manager, when it is queried for. SNMP agent's key functions are: collecting management information about its local environment, storing and retrieving management information as defined in the MIB, send notification of events to the manager.



Picture 9.1 – Example of SNMP management, with Managers and Agents

Every SNMP agent maintains an information database which describes the managed device parameters. The SNMP manager uses this database to request the agent for specific information. This commonly shared database between the Agent and the Manager is called **Management Information Base (MIB)**.

Typically, MIBs on an equipment contain standard set of statistical and control values, but also allow the extension to values specific to a particular agent, through the use of private MIBs. A MIB is a collection of information, made up of managed objects identified by name and Object Identifier (OID); each identifier is unique and denotes specific characteristics of a managed device.

Y-Packet 2 supports basic commands of SNMP, as listed below:

GET - the SNMP-get operation is a request sent by the manager to the agent; it is performed to retrieve one or more values from the managed device

GET NEXT - this operation is similar to the SNMP-get, with the significant difference is that retrieves the value of the next OID in the MIB tree

GET BULK - this operation is similar to the SNMP-get, with the significant difference is that retrieves a set of values of OIDs in the MIB tree

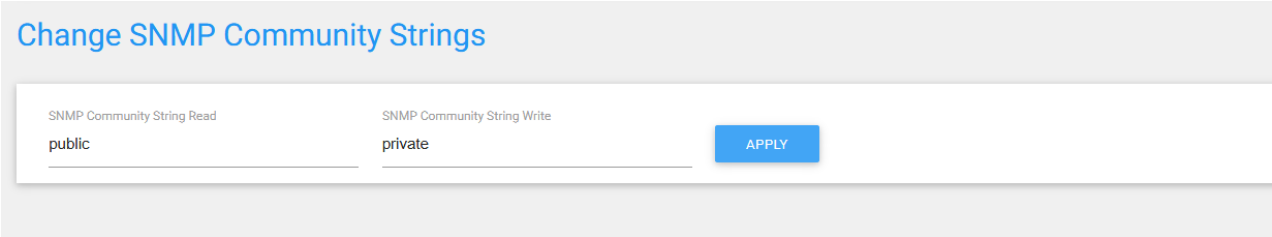
SET - this operation is used by managers to set or modify a value on a specific OID in the MIB of the managed device

GET/SET RESPONSE - it is the command used by agent to carry back the value of SNMP-get/set issued by the SNMP manager

TRAPS - unlike the above commands, which are initiated from the SNMP Manager, TRAPS are initiated by the agents; these are notifications to the SNMP manager by the agent on the occurrence of an event (typically an alarm)

On Y-Packet 2, at its factory default configuration, SNMP communication is enabled, and SNMP Community Strings are set to the default "public" for **Read** (SNMP-get operation) and "private" for **Write** (SNMP-set operation). Community Strings can be changed at any time: the new strings can be alphanumeric, and can contain special characters.

On Y-Terminal **SNMP** page user can set the desired configuration for access over SNMP protocol.



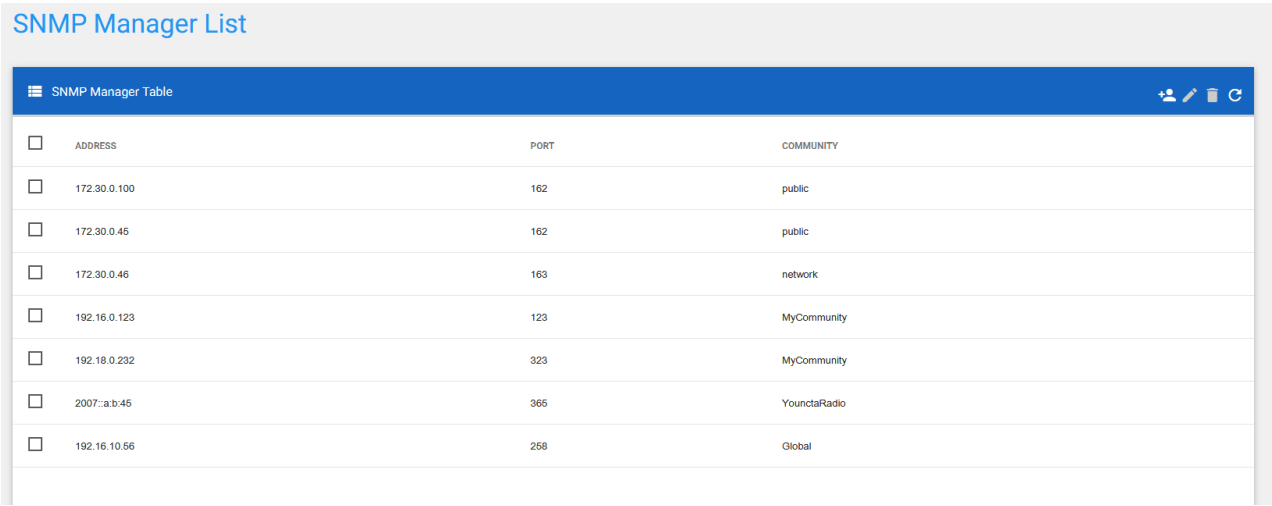
Picture 9.2 – SNMP default Community Strings

As per default values, Y-Packet uses UDP port 161 for SNMP-set/get; UDP default port for TRAPS is 162, but can be configured to a different value. The SNMP version implemented is the SNMPv2c (community-based security).

9.1 SNMP Manager List

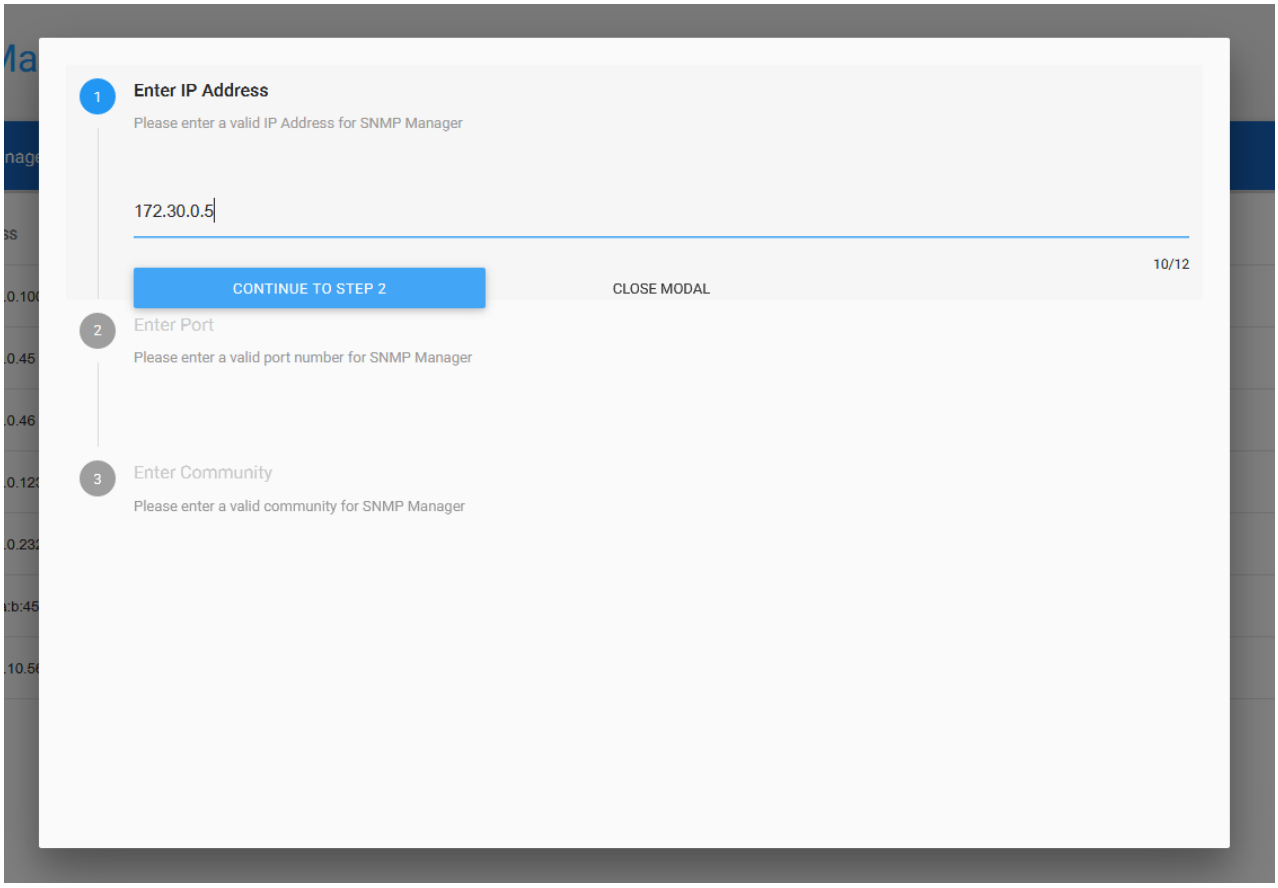
On Y-Terminal **SNMP** page, **SNMP Manager List** table, user can configure the desired list of hosts which will receive SNMP Traps spontaneously from equipment SNMP agent. SNMP-Traps are initiated by the agents; these are notifications to the SNMP manager of the occurrence of an event, which is typically an alarm.

On **SNMP Manager List** table, operator can configure the **IP address** of SNMP Manager, the destination **UDP Port** to sent SNMP-Traps to, and finally the **Community** for each SNMP Manager. Up to 10 SNMP Managers can be configured.



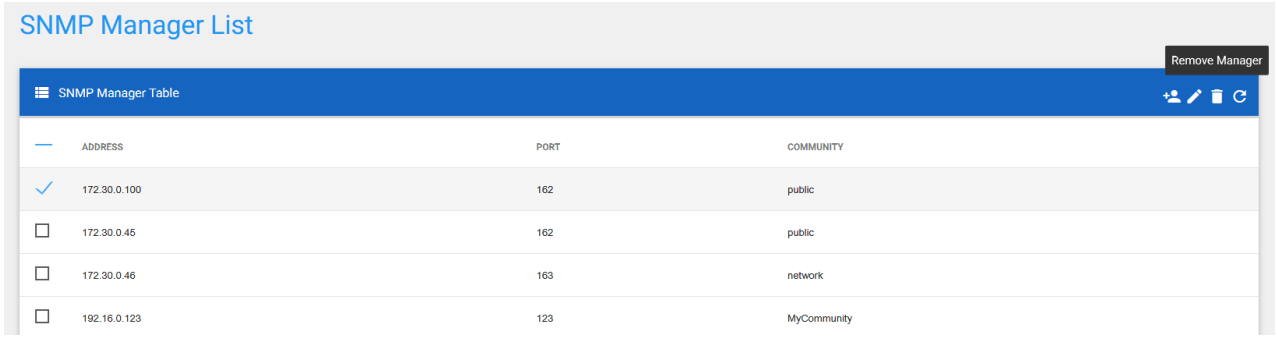
Picture 9.3 – Example of SNMP Manager List table

In case operator wants to add more SNMP Managers, an **Add Manager** icon is available, which opens a window where all parameters for the new SNMP Manager shall be inserted.



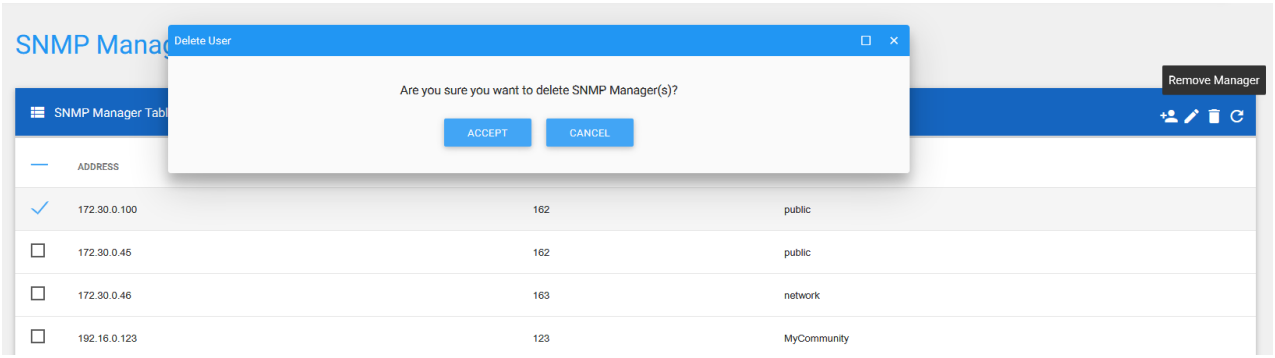
Picture 9.4 – Example of adding a new SNMP Manager

In the same way, in case operator wants to permanently remove a SNMP Manager, he shall select and highlight one from the list, then click on the **Remove Manager** icon.



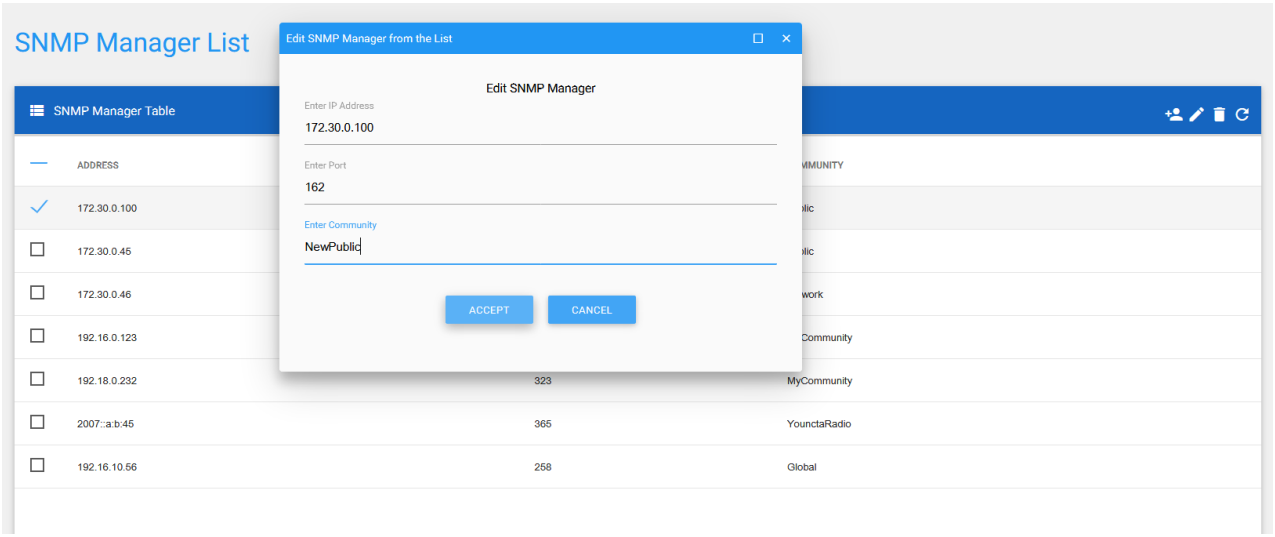
Picture 9.5 – Highlight one entry before removing a SNMP Manager

Before deleting, the system will display a message asking user confirmation about deleting the selected SNMP Manager. Clicking on Accept, the selected SNMP Manager will be removed.



Picture 9.6 – Confirmation message before removing an existing SNMP Manager

A **Edit Manager** icon is also provided, used to change IP address, UDP port or Community string of the SNMP Manager.



Picture 9.7 – Changing the values of an existing SNMP Manager with the Edit Manager icon

9.2 Alarms

This chapter is dedicated to Y-Packet 2 alarms, where we will explain, for each alarm, all the possible root causes, in order to give operators a full understanding of link and equipment status against possible failures. For corrective actions to perform in case of outstanding alarms, please refer to Y-Packet 2 Operator Manual.

After explaining about how Y-Packet can be managed over SNMP protocol, and basic SNMP message types, we can now focus on SNMP-Traps, those messages spontaneously sent by SNMP agents (Y-Packet in our case) to any configured SNMP manager.

SNMP Traps use UDP destination port 162 by default, but this default can be changed to any desired value when creating new SNMP Trap Receivers in the SNMP Trap receivers table.

Most of the SNMP Traps sent by Y-Packet are used to notify SNMP Managers of an alarm, or in some cases notify manual operation that may as well require attention.

Here following, you find a list of all possible alarms/notifications raised by Y-Packet 2. For any notification, we will provide Name, Type, Severity and description.

Name	Type	Severity	Description	Notes
PoE Link Down	Ethernet	Major	The PoE interface could not establish a valid connection with the Link Partner, resulting in a link down condition	
PoE Autonegotiation Failure	Ethernet	Major	The PoE interface could not accomplish a valid autonegotiation process with the Link Partner, resulting in autonegotiation not complete	
SFP Link Down	Ethernet	Major	The SFP interface could not establish a valid connection with the Link Partner, resulting in a link down condition	
SFP LOS	Ethernet	Major	The SFP interface is receiving degraded signal power	
SFP Tx Fault Alarm	Ethernet	Major	The SFP port is not transmitting any power	
SFP Missing	Ethernet	Major	The SFP optical module is missing, can be broken or out of its cage	

Name	Type	Severity	Description	Notes
Service Channel Error Alarm	Equipment	Major	ODU-to-ODU radio communication service channel out of service, no status information received from/to the Remote ODU	
Mate Channel Alarm	Equipment	Critical	ODU-to-ODU data channel out-of-service in 1+1 HSB System Type; can be cable unplugged or broken, or mate equipment broken	Applicable to 1+1 HSB System Type only
Remote Peer Unreachable Alarm	Equipment	Major	The Remote Peer is not reachable from local end, connection to remote Y-Terminal not possible	
XPIC Signal Loss Alarm	Equipment	Major	ODU-to-ODU data channel out-of-service in XPIC System Type; can be cable unplugged or broken, or mate equipment broken	Applicable to XPIC System Type only
RLA Signal Loss Alarm	Equipment	Major	ODU-to-ODU data channel out-of-service in Radio Link Aggregation System Type; can be cable unplugged or broken, or mate equipment broken	Applicable to RLA System Type only
SW Mismatch Alarm	Equipment	Warning	The local ODU is running a different SW version than the Remote ODU	

Name	Type	Severity	Description	Notes
NTP Server Unreachable Alarm	Common	Minor	NTP Synchronization with configured NTP Server failed	
Temperature Alarm	Common	Critical	ODU temperature out of range	
Digital Board Failure Alarm	Equipment	Critical	A HW failure has been detected on the digital board	

SyncE Unlocked Alarm	Common	Major	Recovered clock not locked to the incoming Rx Clock	

Name	Type	Severity	Description	Notes
Timed CW	Maintenance	---	Transmission of an unmodulated carrier set by the operator; can be set by the operator for link testing purposes	No associated severity, it is classified as Manual Operation
Timed Loop	Maintenance	---	A loop performed on the Radio interface; can be set by the operator for link testing purposes	No associated severity, it is classified as Manual Operation
Timed Squelch	Maintenance	---	Timed muting of Radio transmitter; can be set by the operator for link testing purposes	No associated severity, it is classified as Manual Operation
SFP Loop	Maintenance	---	A loop performed on the SFP interface; can be set by the operator for testing purposes	No associated severity, it is classified as Manual Operation
PoE Loop	Maintenance		A loop performed on the PoE interface; can be set by the operator for testing purposes	No associated severity, it is classified as Manual Operation

Name	Type	Severity	Description	Notes
LO (Local Oscillator) Alarm	Radio	Critical	Synthesizer alarm: reports problems on the VCO of OL on Tx and/or Rx side	
Tx Power Alarm	Radio	Major	Transmitted Power differs more than 6 dB versus the operator defined value, or above a threshold when transmitter is squelched	
Rx Power Alarm	Radio	Major	Received Power is below threshold; threshold is a function of configured Bandwidth and configured/operational modulation level	
Remote Rx Power Alarm	Radio	Major	Received Power is below threshold on the Remote ODU; threshold is a function of configured Bandwidth and configured/operational modulation level	
Demodulator Alarm	Radio	Major	Wrong state of the demodulator	
High BER	Radio	Major	Detected value of Bit Error Rate ≥ 10-3 (based on MSE evaluation)	
Low BER	Radio	Minor	Detected value of Bit Error Rate ≥ 10-6 (based on MSE evaluation)	
Delineation Alarm	Radio	Major	No Ethernet frames detected over the radio link	
No Present Alarm	Radio	Critical	The RF board is not responding	
Power Failure Alarm	Radio	Critical	Power failure detected on the equipment	

10 Alarms & Events

The **Alarms & Events** table provides operators with useful information for their Y-Packet 2 network deployment, tracing several types of events such as user activity, equipment configuration changes, equipment operational status changes, alarms.

The Alarms & Events table allow users to monitor and manage system, security, application events and errors on system. It is a repository for all events, from critical like HW failures, up to not so critical, such as an incorrect password entered when a generic user was attempting log in to Y-Terminal.

The Alarms & Events engine maintains a comprehensive, up-to-date run-time representation of the administrative and operational state of the Y-Packet 2 system.

Any configuration or state change is considered an event. Some events are part of the normal workflow, thus there is no need to record their occurrence, nevertheless events shall be brought to the attention in case they meet one of the following criteria:

! the event records a change of configuration on equipment

! the event records a change of operational status of equipment

! the event records an alarm condition detected on the equipment

! the event records a user action that is required to be auditable

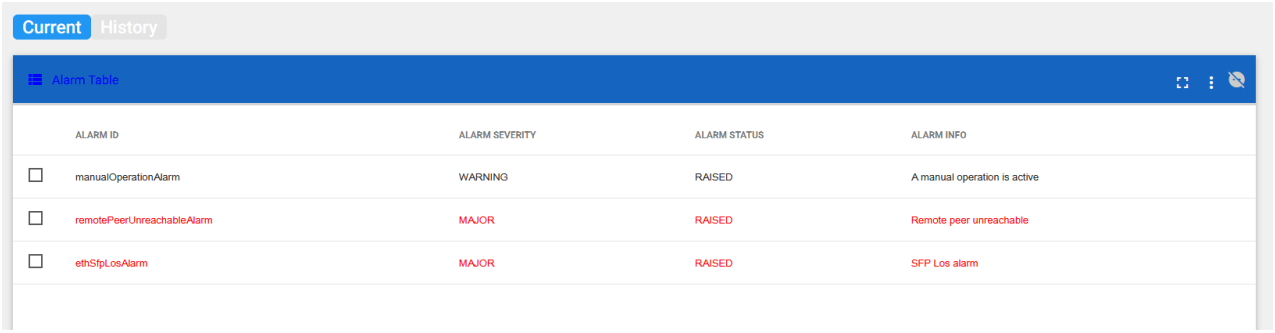
Alarms & Events section is arranged into two different tables:

! **Alarms & Events – Current**: it records outstanding alarms only, no configuration changes or user action are recorded here. The outstanding alarms are listed inside **Alarm Table**. A second table is provided, for **Acknowledged Alarm Table**: acknowledging an outstanding alarm is an action that user can perform for those alarms that are still outstanding, nevertheless is has been managed and so there is no need to be listed as active. User shall always take care before acknowledging alarms, as once in this table no more warning will be provided to that type of alarm even after a possible equipment reboot.

! **Alarms & Events – History**: it records alarms, configuration changes, operational status changes, user actions. An event remains in the **History** until it is purged, when the log reaches its maximum capacity and space is needed for new event records. The maximum number of logs that the system can retain is 500, the retention and purge behavior for each log is FIFO.

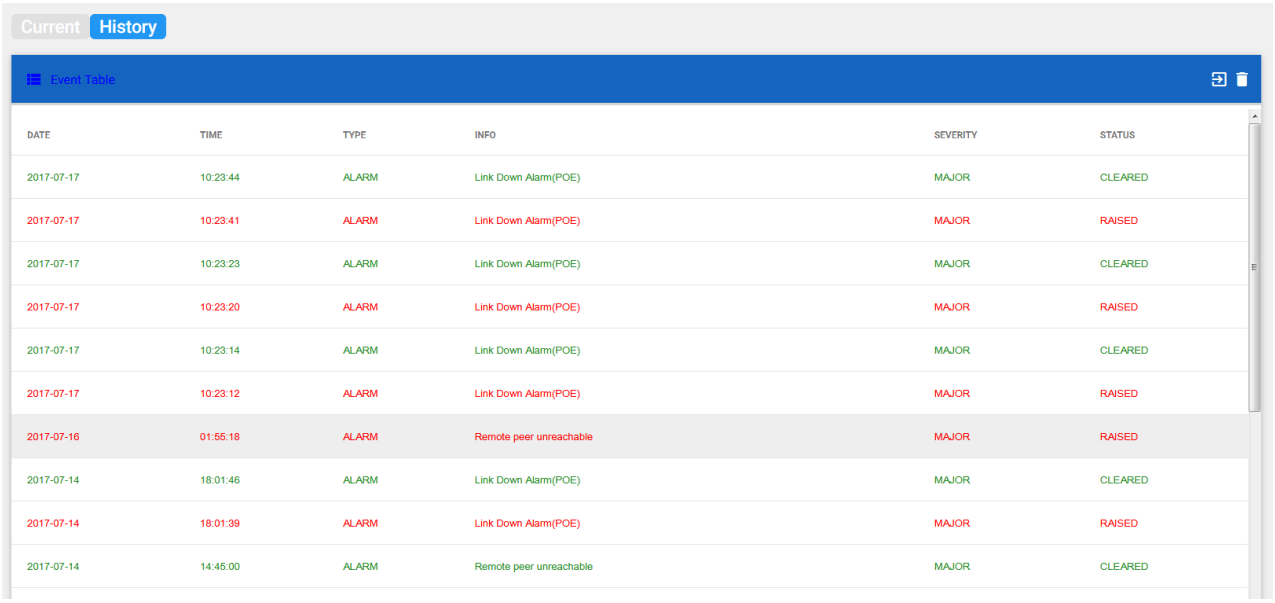
In case the equipment experiences a restart, the **Alarms & Events - Current** table is updated to the state after equipment reboot, while the **Alarms & Events - History** table is not lost, as its engine triggers an automatic saving of event list.

The picture below is an example of **Alarms & Events - Current** Y-Terminal page:



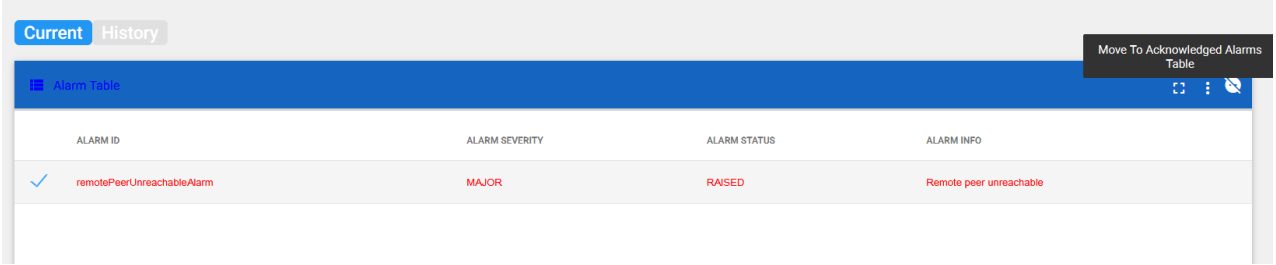
Picture 10.1 – Example of Alarms & Events Current, Alarm Table

This one below is an example of **Alarms & Events - History** Y-Terminal page



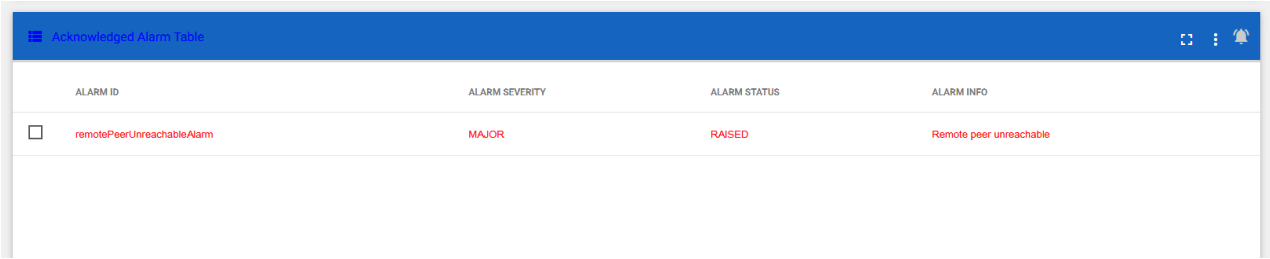
Picture 10.2 – Example of Alarms & Events History, Event Table

In the **Alarms & Events - Current** Y-Terminal page, as explained before, there is chance to acknowledge outstanding alarms. User shall select one or more outstanding alarms to be acknowledged, then click on the **Move to Acknowledged Alarms Table** icon. The alarms will be moved to the same page, but inside **Acknowledged Alarm Table**.



Picture 10.3 – How to acknowledge an outstanding alarm

After moving, the outstanding alarm will be removed from **Alarm Table**, and displayed inside **Acknowledged Alarm Table**.



Picture 10.4 – The outstanding alarm is now displayed inside Acknowledged Alarm Table

User shall take care when acknowledging alarms, as also in case the acknowledged alarm is cleared and then raised again, that same type of alarm won't be displayed in the **Alarm Table**, outstanding, anymore.

For each event, the system traces following data:

! **Date** : it is the date when event was recorded, in the format yyyy-mm-dd

! **Time** : it is the time of day when event was recorded, in the format hh:mm:ss

! **Type**: it is "Configuration" for events like configuration changes or user activities; it is "Info" for those action spontaneously done by system; it is "Critical/Major/Minor Alarm" for all alarm events, both raised and cleared

! **Info**: it is a short textual description of the event

! **Severity**: it is traced for alarms only, not for events, and represents the severity of the alarm

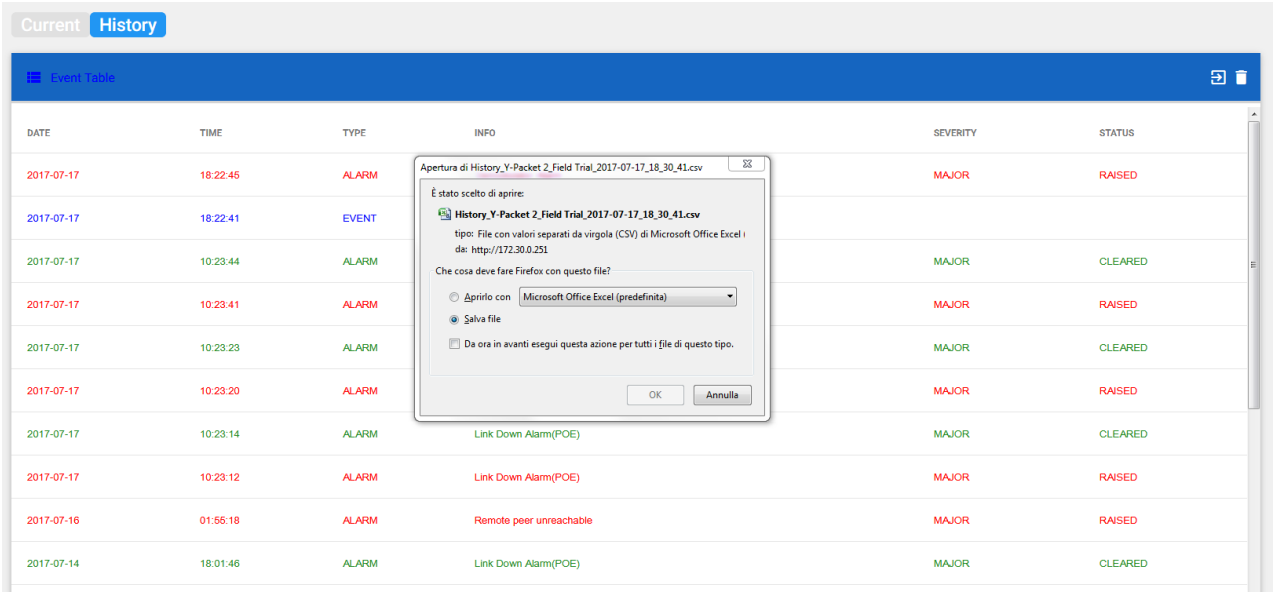
! **Status**: it is traced for alarms only, not for events, and represents the status of alarm, if raised or cleared

The list of alarms/events can be sorted ascending or descending, by any of the values represented in each column.

To manage the **Alarms & Events - History**, two icons are available:

! **Export Events**: by clicking this icon, a window is displayed, allowing the log to be saved as a file on the local PC. The file uses Comma Separated Values format, and can be opened by standard spreadsheet applications. The file name is: <History_SystemName_LocationName_yyyy-mm-dd_hh_mm_ss>.csv

! **Clear Events**: all history entries are cancelled



Picture 10.5 – Example of Export of Alarms & Events - History log

Alarms & Event - History is very useful when operator is performing troubleshooting on a link, as it provides a complete tracing, in configuration and operational status, with time. Rather than on a single equipment, the Alarms & Event - History tool is even more powerful when events on both equipment of the radio link are compared and correlated. In order to get the most accurate info about the link, it is fundamental the two equipment be aligned to a common source of timing, like for example a common NTP server.

11 MIB Backup & Restore

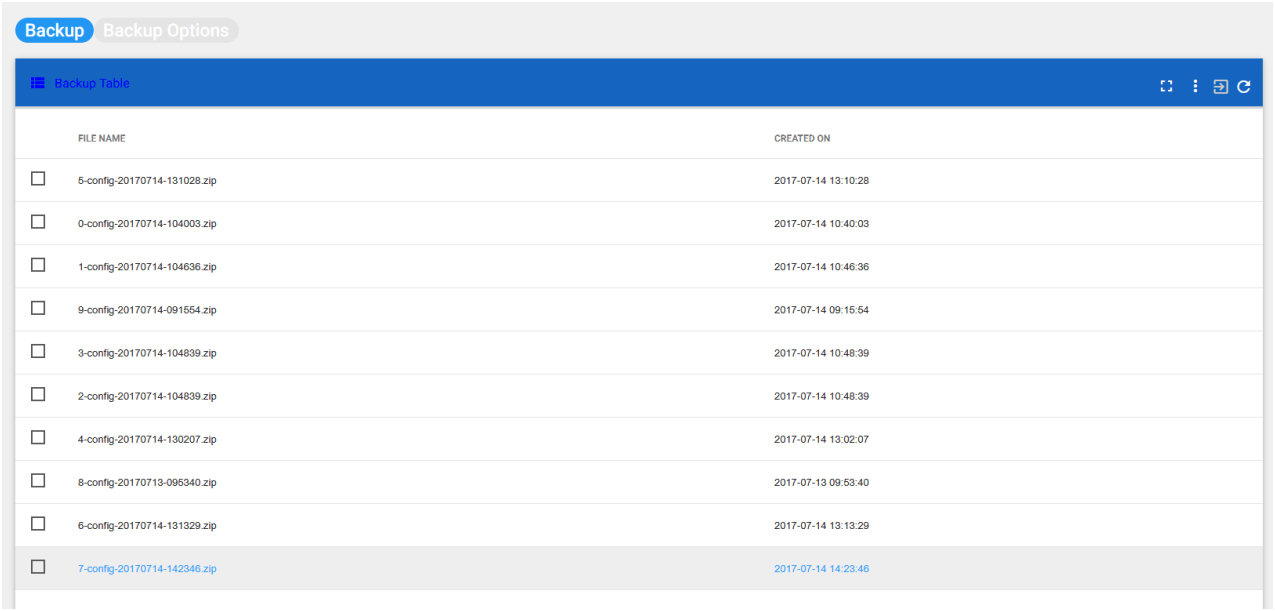
This section provides info about backup and restore of equipment configuration.

11.1 Backup

In case operator wants to perform a backup of the equipment configuration, he can open the **Backup & Restore** Y-Terminal page. The backup function enable operators to store, inside the equipment or locally on a PC, a configuration back-up file, which can be used at any time to retrieve all equipment configuration as it is written inside the equipment MIBs. With this function, operators can avoid extensive manual reconfiguration via Y-Terminal in case of equipment replacement or other circumstances.

At the **Backup & Restore** Y-Terminal page, two tabs are displayed. The first is the **Backup** tab, which always reports a list of 10 equipment configurations: every time that user changes, and applies, any configuration parameter, a new configuration **.zip** file is created, and stored inside the equipment memory. This is a form of automatic backup, it is always running and cannot be disabled.

All configuration files are displayed in black color, except one, highlighted in blue: the blue color indicates that it is the current configuration running on the equipment.



Picture 11.1 – List of configuration files: the current one is highlighted in blue

The 10 configuration files are named according to following rule:

<N°-config-yyyymmdd-hhmmss.zip>

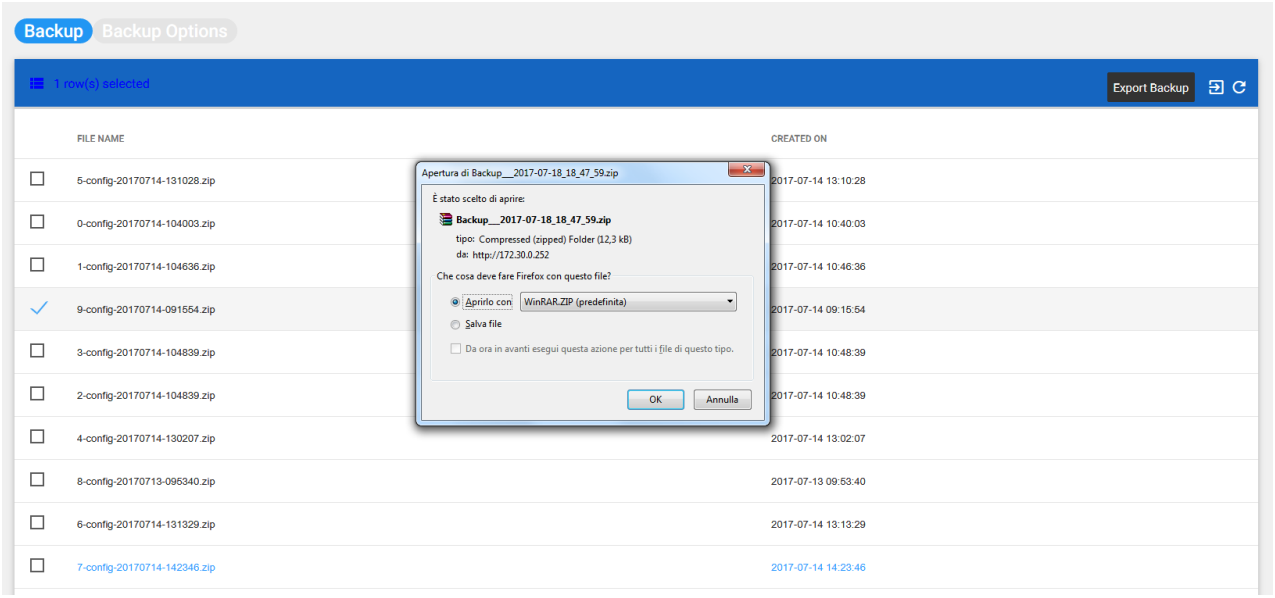
where:

! **N°-config** : N° is a progressive number, from 0 to 9; progressive number is overwritten after 10 automatic backups, restarting from the lower value

! **Date** : it is expressed in the format yyyymmdd

! **Time** : it is expressed in the format hhmmss

User can select one configuration file only, and once selected click on the Export Backup icon. Clicking on this icon, a window is opened, asking user to open or save on local PC.



Picture 11.2 – Performing a Export of a configuration file

The file with equipment configuration will be saved in compressed **.zip** format, and can be uncompressed and then opened by standard applications. The file name is:

Backup_SystemName_LocationName_yyyy-mm-dd_hh_mm_ss.zip

The second tab displayed at the **Backup & Restore** Y-Terminal page is the **Backup Options** tab. Here user is guided, through a simple wizard, to configure all the desired backup customized options.

Here following you find description for each step of backup mode setting:

! **Backup Type** : can be set to Automatic or Manual

! **Backup Scheduling and Retention** : can be set to Equipment or Locally on PC

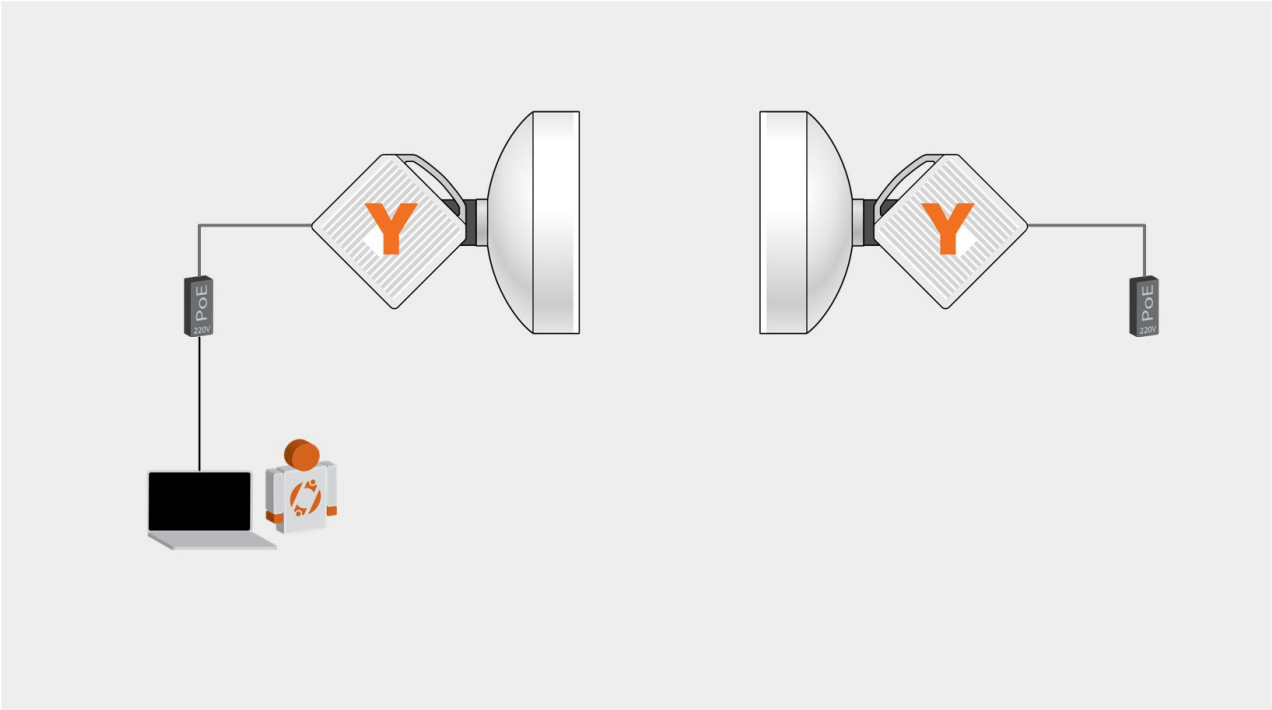
! **Backup File Name** : it is the file name the user wants to use to save the backup

12 SW & Maintenance

This section provides info about how to perform SW upgrade on Y-Packet 2. Then it describes the basic operations of restoring to factory default and SW reboot of equipment.

12.1 Software Upgrade

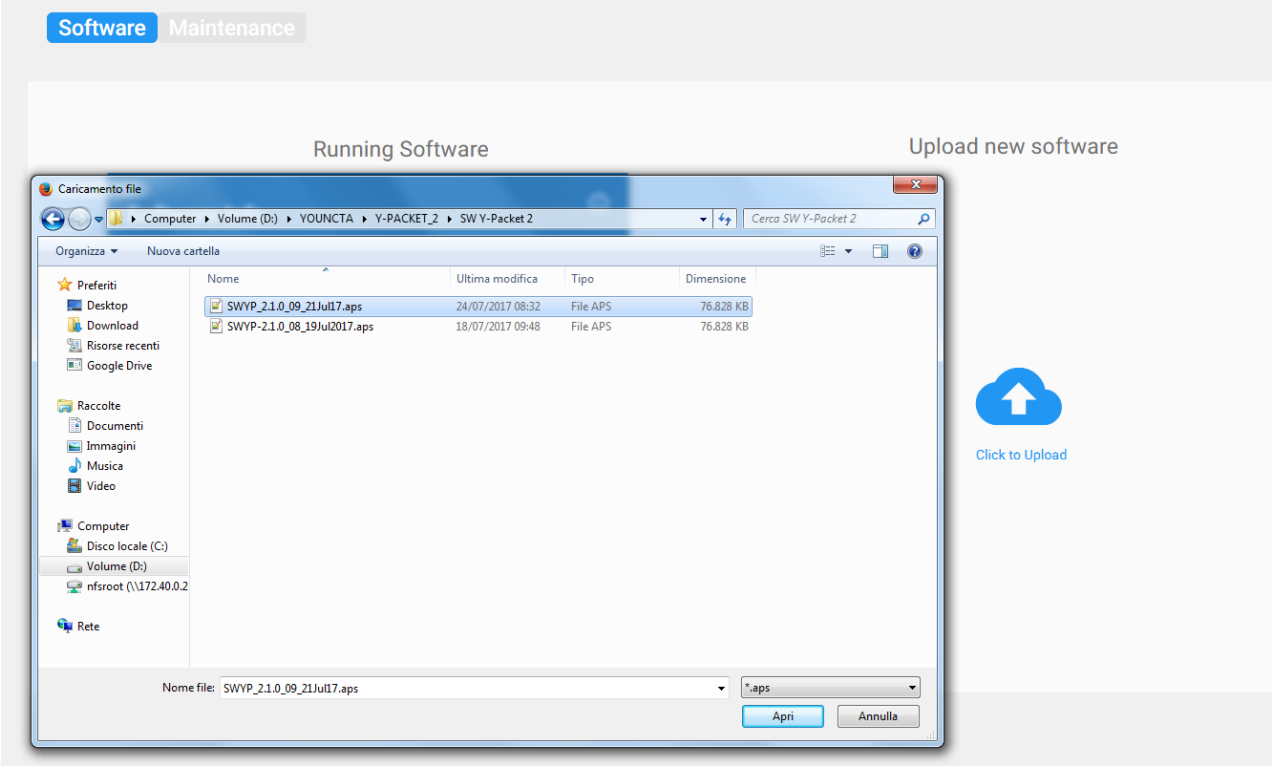
SW upgrade on Y-Packet 2 can be done on a link basis, which means that operator can normally proceed to upgrade both Remote ODU and Local ODU from one single PC connected to local ODU. Please refer to network layout below:



Picture 12.1 – Reference scenario for SW upgrade

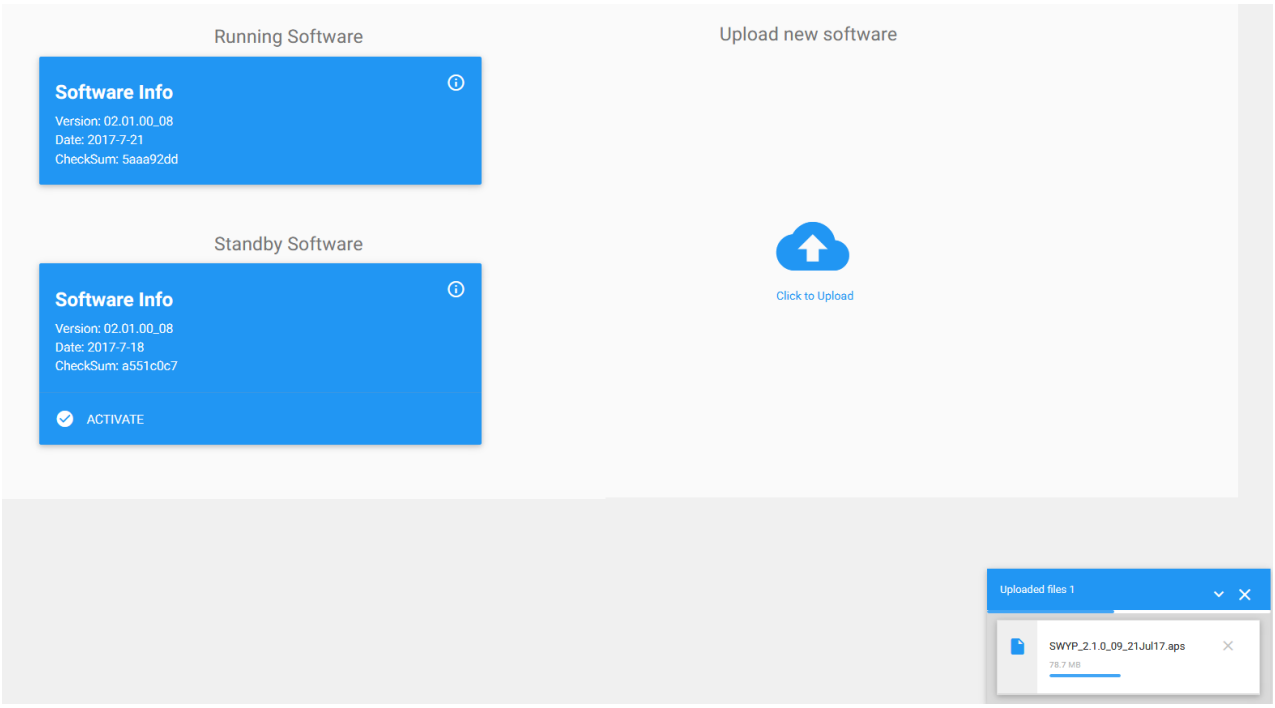
To perform SW upgrade, operator shall follow the steps below:

! Connect to Y-Terminal of both Local ODU and Remote ODU, on both devices open **Software & Maintenance** page, **Software** tab. Then, click on **Upload New Software** icon, and from selection window browse to new SW package to upload



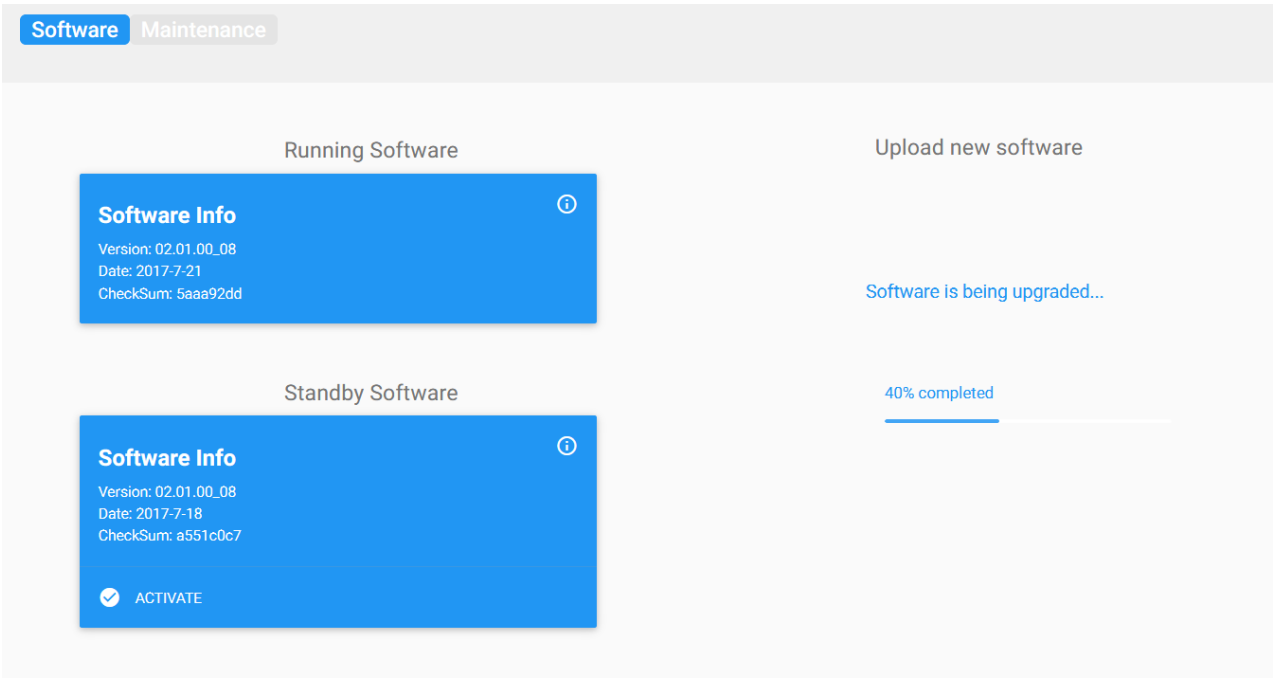
Picture 12.2 – Selection window to upload new SW package on Stand-by bank

! As soon as the SW package is selected, the equipment prepares for upload, as shown in the box at right-bottom of page (this takes few seconds only)



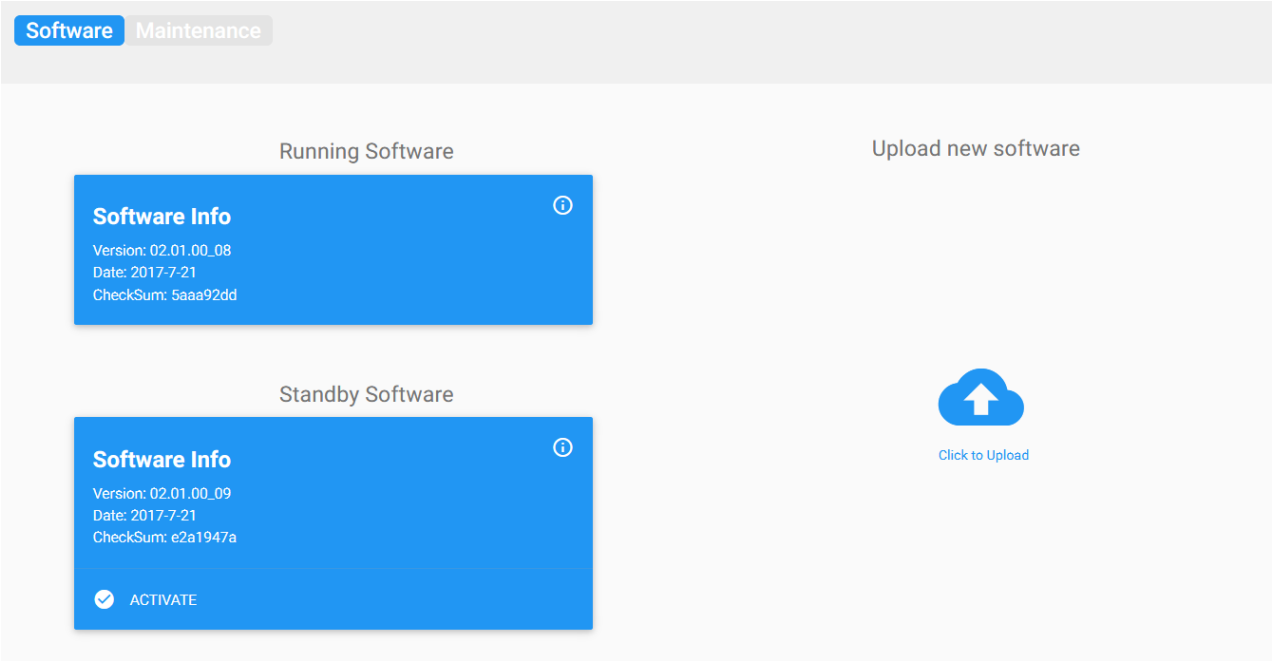
Picture 12.3 – Equipment is preparing for SW upload

! Eventually the SW upload starts, and a progression bar is displayed



Picture 12.4 – Uploading software and progression bar

! At the end of upload, the new SW package will be stored on Stand-by bank



Picture 12.5 – The new SW package is stored on Stand-by bank

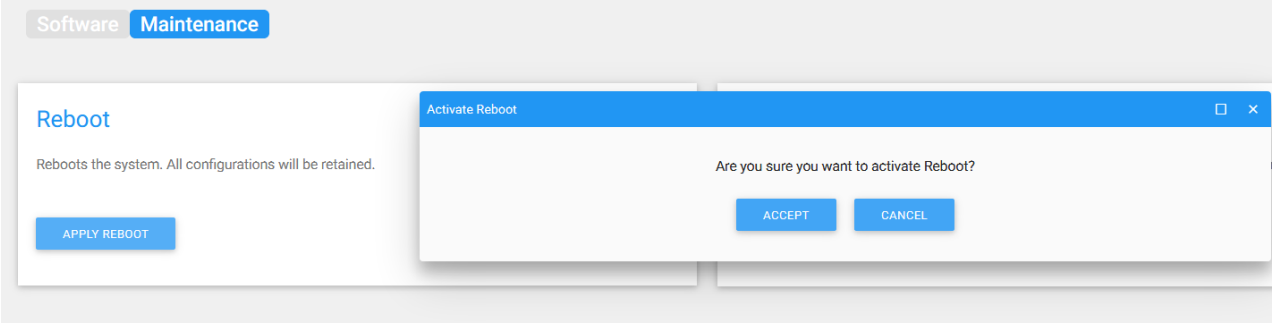
! Now, on Y-Terminal of each equipment, click on **Activate** icon: a window opens, asking user confirmation that he wants to proceed with SW upgrade. Click on **Accept.** After clicking on Accept, the Y-Terminal will be redirected to login page, and after a while it will be ready for a new user session login.

! It is suggested to activate on Remote ODU first, wait for the switch banks to be completed, then proceed on Local ODU.

12.2 Reboot & Restore to Factory Default

In case operator wants to reboot equipment, or restore equipment configuration to its factory default, he can open the Y-Terminal **Software & Maintenance** page, **Maintenance** tab.

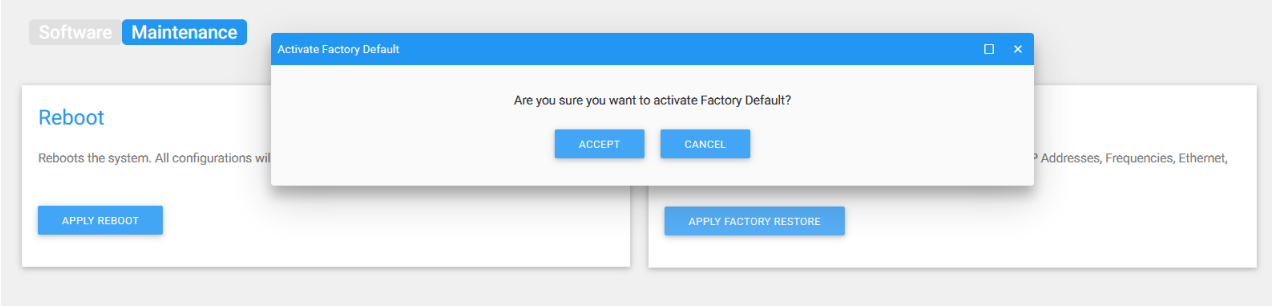
In order to perform a SW reboot on the equipment, user can click the **Apply Reboot** button. A confirmation message will be displayed to user, and when confirmed it will start a warm reset on equipment.



Picture 12.6 – Confirmation message before rebooting equipment

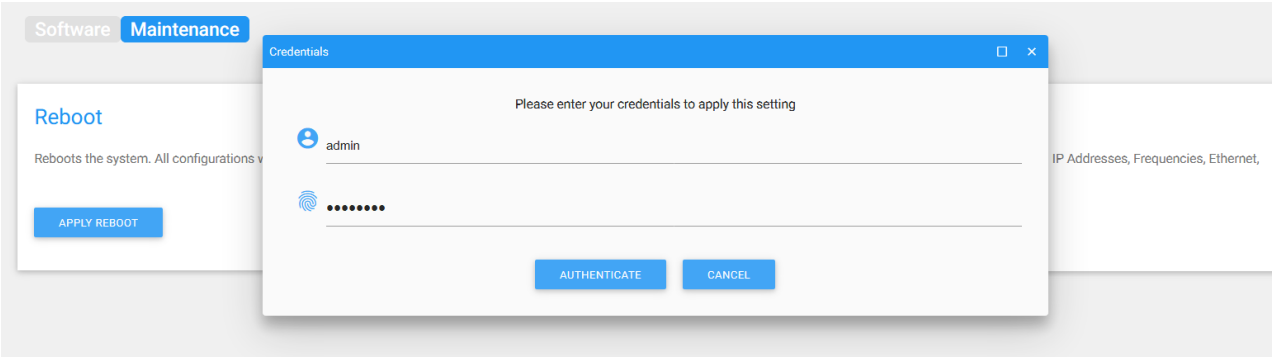
! It is important to remark that only users with administration rights on equipment (Admin, Read-Write) can perform such operation.

To restore Y-Packet 2 configuration to its factory defaults, a **Apply Factory Restore** button is provided. Clicking on it, a confirmation message will be displayed to user; who is asked to confirm with the **Accept** button.



Picture 12.7 – Confirmation message before restoring equipment to factory defaults

Once accepted, a new window is opened, asking for insertion of credentials. As far as operator provides valid credentials and clicks on **Authenticate** button, the factory restore process is started.



Picture 12.8 – Authentication is required before proceeding to restore factory default values

! It is important to remark that only users with administration rights on equipment (Admin, Read-Write) can perform such operation.