

# TwinRadio HYC-Wi 2000

**Gigabit Full Duplex Radio Link 24 GHz**

**XPIC FDD Radio PTP Bridge IP Link**



Twin-Radio XPIC 2 Gigabit

Unlicensed bands 17 & 24 GHz, Specially suited for the Smart City, WISP & 5G.

Wi2.000-17/24 IP-native  
Dual Link Full-Outdoor

*Hypercable*

 [www.e-rake.fr](http://www.e-rake.fr)  
[www.hypercable.fr](http://www.hypercable.fr)

## User Manual

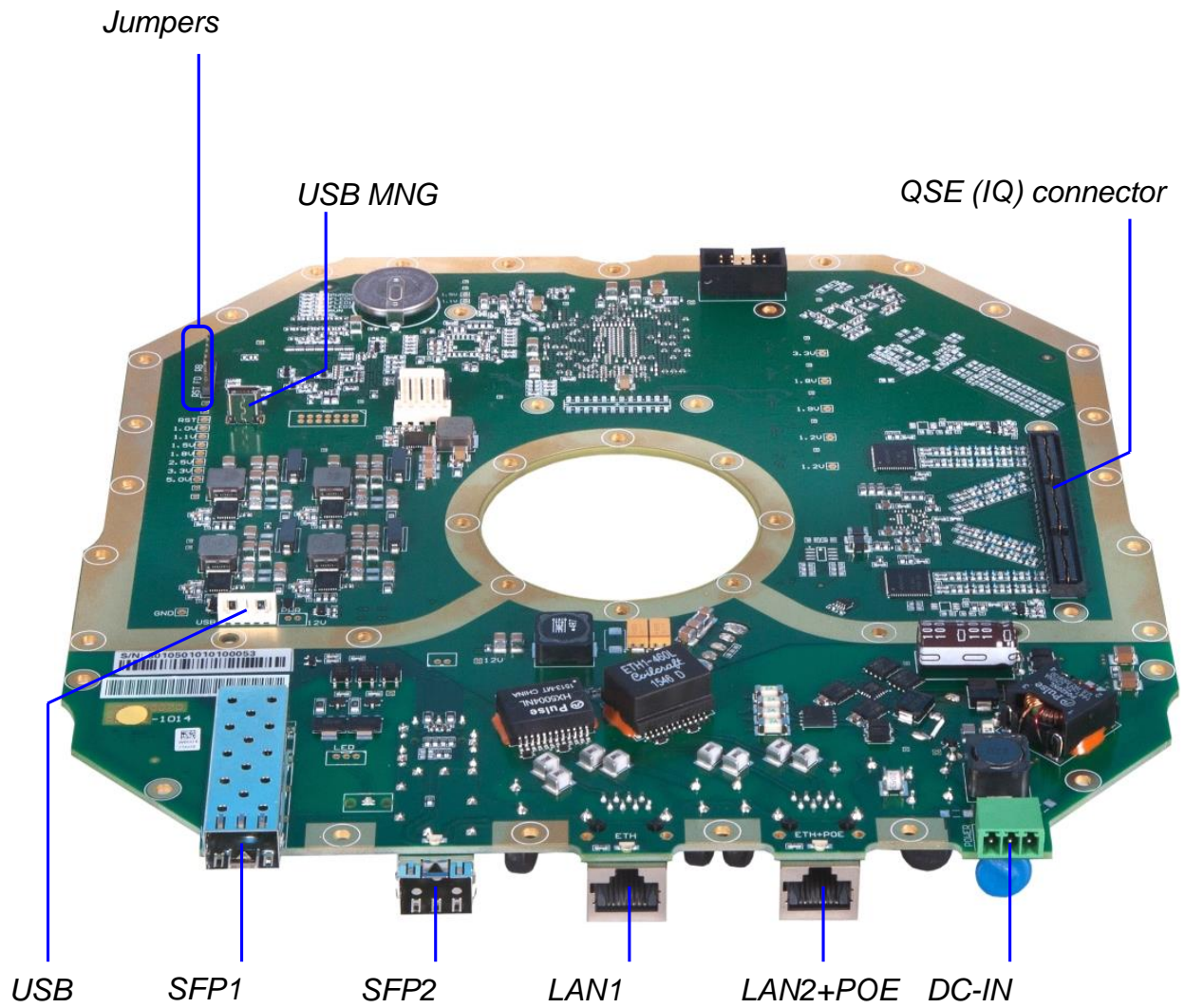
Includes install, configuration and trouble shooting information for the broadband wireless access outdoor radio.

1	SPU Description .....	4
1.1	Service connectors.....	4
1.2	Status LEDs .....	7
1.3	Interface LED .....	7
1.4	Power supply .....	10
2	Management Introduction .....	10
2.1	Management access .....	10
2.2	Local and remote setting.....	11
2.3	Storing the configuration and the configuration scope .....	11
3	First configuration steps .....	12
3.1	Connection and Login .....	12
3.2	General system configurations.....	13
3.3	IP configurations.....	14
3.4	Modem and Radio configurations .....	14
4	Graphical User Interface (WEB GUI).....	15
4.1	Web header & Side panel description.....	15
4.2	General .....	16
4.2.1	Status .....	16
4.2.2	Mode .....	16
4.3	Info.....	17
4.3.1	License .....	17
4.3.2	Date .....	17
4.3.3	Users .....	17
4.4	Alarms Page .....	17
4.4.1	Status .....	17
4.4.2	Alarm Conf.....	18
4.4.3	Logs.....	19
4.5	Radio Page .....	19
4.5.1	Parameters .....	19
4.5.2	Analyser .....	20
4.5.3	Diagram .....	21
4.5.4	ACM .....	21
4.5.5	Advanced .....	22
4.5.6	Details.....	22

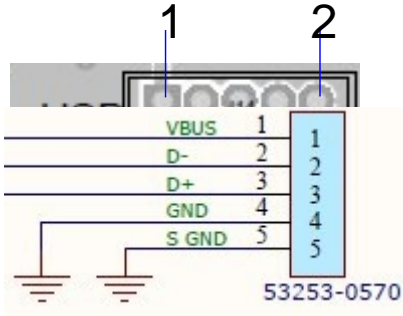
4.6	Ports Page.....	23
4.6.1	Parameters .....	23
4.6.2	ETH VLAN .....	24
4.6.3	ETH Advanced .....	26
4.7	IP Page .....	27
4.7.1	Address .....	27
4.7.2	Route/NAT .....	28
4.7.3	SNMP .....	29
4.7.4	Advanced .....	29
4.8	Count Page.....	30
4.8.1	Basic/BER .....	30
4.8.2	Ethernet .....	31
4.8.3	Management .....	31
4.8.4	Graphs.....	31
4.8.5	Online Graphs .....	32
4.9	Maintenance Page.....	32
4.9.1	Config.....	32
4.9.2	Terminal.....	32
4.9.3	Files.....	32
4.9.4	Advanced .....	33
5	Command Line Interface (CLI) .....	35
5.1	Basic command structure .....	35
5.2	Altering device configuration using CLI – enable mode .....	36
5.3	CLI command abbreviations .....	36
5.4	CLI online help .....	36
6	Simple Network Management Protocol (SNMP).....	37
6.1	Basic SNMP setting .....	37
6.2	MIB .....	38
6.3	Traps .....	38
6.4	Altering device configuration using SNMP .....	38

# 1 SPU Description.

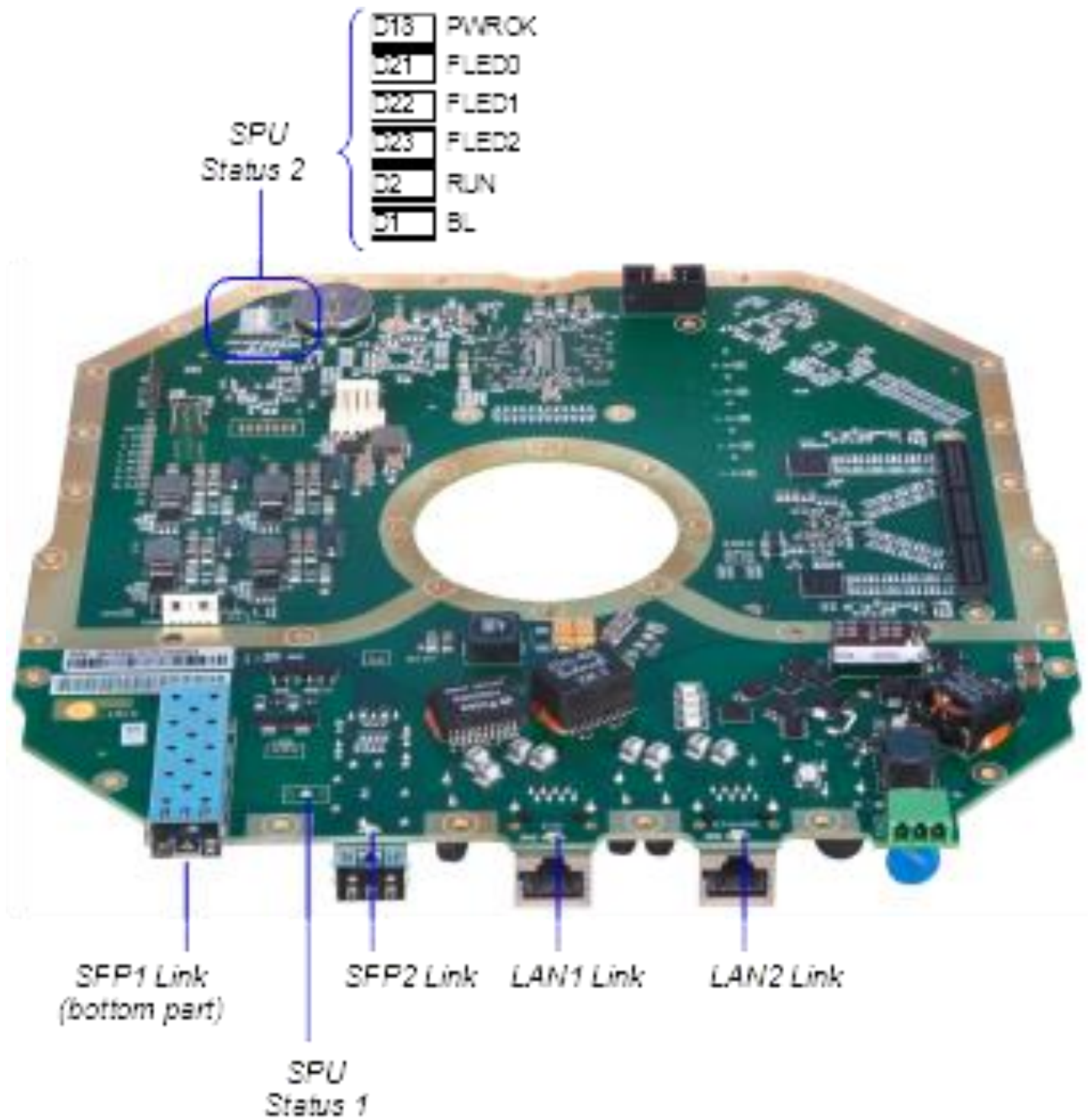
## 1.1 Service connectors



Connector	Description
SFP1	1x 1000BaseSX/Lx (SFP);primary SFP port for user traffic connection.
SFP2	1x 1000BaseSX/Lx (SFP);secondary SFP port for user traffic connection.
LAN1	1x 100/1000BaseT (RJ45); primary LAN port for user traffic connection. The priority based on ETH channel can be set in GUI or from the command line.
LAN2+POE	<p>1x 100/1000BaseT (RJ45);</p> <p>secondary LAN port for user traffic connection. This port is also dedicated for MNG through internal switch for separate IP access to AOU unit.</p> <p>A T the same time this port could be used for powering up of AOU unit over POE according to the standard LTPoE++ 90W.</p> <p>All of 8 pins on the connector must be used.</p> <p>(pins 1,2,7,8 – one polarity; pins 3,6,4,5 – the opposite polarity) Pin polarity can NOT be mixed.</p> <p>The priority based on ETH channel can be set in GUI or from the command line.</p>
DC-IN	-48VDC; separate power supply connector.
QSE (IQ) connector	QSE connector for connecting SPU to RF part. For the QSE connector pinout see the specification in section SPU-RFU interconnection.
USB MNG (DEVICE)	<p>MINI USB interface for an alternative IP access.</p> <p>Pin configuration according to the standard MINI USB.</p>

<p>USB Storage (HOST)</p>	<p>USB interface for connecting USB memory. It is meant for licenses backup and upload. Further it could be used for logs saving etc.</p> <p>The connection to USB port is via reduction cable. For pin configuration see a diagram below.</p> 
<p>FD Jumpers</p>	<p>Factory default jumper – by means of these two pins it is possible to reset the device to factory-default settings.</p> <p>Follow these steps - turn off the device and put a jumper to position FD. Then turn on the device for about 15 seconds. Turn off the device again and remove the jumper and then turn the device back on. The device will reboot with the factory-default settings.</p> <p>Attention! If this process is performed with jumper a T position RST, the complete device firmware is erased and the device is necessary to send back to producer.</p>
<p>RST Jumpers</p>	<p>Configuration jumper reserved for producer only!!</p>
<p>RB Jumpers</p>	<p>Configuration jumper reserved for producer only!!</p>

### 1.2 Status LEDs



### 1.3 Interface LED

<b>LED</b>	<b>State</b>	<b>Status</b>
SFP1 Link	Off	No Ethernet Link
	On	Ethernet Link established
	Random Flashing	Ethernet activity

SFP2 Link	Off	No Ethernet Link
	On	Ethernet Link established
	Random Flashing	Ethernet activity
LAN1 Link	Off	No Ethernet Link
	On	Ethernet Link established
	Random Flashing	Ethernet activity
LAN2 Link	Off	No Ethernet Link
	On	Ethernet Link established
	Random Flashing	Ethernet activity

## SPU Status 1 - LED indicators

<b>LED</b>	<b>State</b>	<b>Status</b>
SPU status	Orange/Green On or Flashing	LED indicators about the status of the device and its parts during the turn on process and while in operation.
SPU status - during the device turn on process	1) Orange On	Power supply OK
	2) Green/Orange Flashing	FPGA boot from CPU
SPU status - while in operation	Green On	Device in OK status (no alarms-warnings)
	Orange Flashing 1x per 2 seconds.	Status warning – a T least 1 warning is indicated
	Orange Flashing 2x (double-flash) per 2 seconds.	Status error – a T least 1 error is indicated



## SPU Status 2 – LED indicators

<b>LED</b>	<b>State</b>	<b>Status</b>
PWROK	On	Indication, that power supply (DC-IN or POE) runs fine and in the right order.
FLED0	Off	FPGA debugging LED, there is no allocated function yet.
FLED1	Off	FPGA debugging LED, there is no allocated function yet.
FLED2	Off	FPGA debugging LED, there is no allocated function yet.
RUN	Flashing	Indication of correct CPU run. Update loop.
BL	Off	CPU indication, there is no allocated function yet.

## 1.4 Power supply

The device could be powered up in two different ways. This could be either over POE (port LAN2-POE), or through isolated power supply over separate power supply connector DC-IN.

## 2 Management Introduction

### 2.1 Management access

By default is the local SPU unit's management access bounded to the LAN2 *ETH+POE* port further referenced by the unit's SW perspective as *LAN2*. In order to connect to the unit for the first time you have to setup your PC's network interface (NIC) IP address into the subnet corresponding to the unit's default IP address range and interconnect both PC and the unit by an appropriate Ethernet cable.

#### Example

Assuming that the unit has the default secondary IP address of 10.10.10.10/24 you will have to setup the managing computer's IP address in the network 10.10.10.0 with net-mask 255.255.255.0 (/24 in UNIX notation). Note that the computer's IP address must not be the same as the device's IP address. In this case valid IP addresses are within range from 10.10.10.1 to 10.10.10.254, except for 10.10.10.10.

#### Available access methods

Method	Port number	Example
WEB GUI interface	80 (http), 443 (https)	In your WEB browser enter address "https://10.10.10.10/" where the IP part corresponds to the unit's IP address
Secure Shell (ssh)	22	In your ssh/Telnet/SNMP client application enter the unit's IP address, credentials and confirm possible security notifications.  Note that the SNMP access is not enabled by default so this option is not suitable for the initial connection.
Telnet	23	
SNMP	161	

Please note that connecting to the http protocol (port 80) will result in automatic browser redirection to the secured https protocol (port 443).

#### The whole process of initial connection



1. Setup your computer's network adapter IP address according to the unit's default IP
2. Interconnect the unit's management port and PC by an Ethernet cable
3. Power up the unit if not already
4. Connect to the unit from your computer by one of the available methods

For the default IP addresses and credentials please refer to the section Connection and Login.

## 2.2 Local and remote setting

The unit allows to alter configurable parameters using any of the available access methods with administrative credentials. For purpose of this document we will be describing the WEB GUI interface but most of the settings have also the appropriate CLI command alternative as well as SNMP OID. For terminal and SNMP setting basics please refer to the Command Line Interface (CLI) and Simple Network Management Protocol (SNMP) sections of this document respectively.

### Altering local and remote settings


Each GUI section such as *Radio*, *IP*, *Ports*, etc., contains multiple user-changeable form elements such as *Tx Frequency* or *IP Address* text fields. Values provided within such fields will take effect immediately after confirmation by means of pressing of the button. The Apply  button colour indicates if pressing of such button alters the current configuration – blue button will alter the running configuration while greyed out button will have no effect. Alongside of the Apply button the GUI offers the button which will revert  any changes in the appropriate section to it's originals. Only such setting which has not been yet confirmed will be reverted.

Some setting sections allows simultaneous configuration of both local and remote parameters. Example of such section would be the *Radio/Parameters* section which will allow local and remote setting of each RF channel. Settings which belongs to the remote unit are indicated in an appropriate section header. The remote settings will be automatically transferred over internal management PPP connection to the remote unit. This feature requires active management channel communication over radio with the remote side as well as correct IP settings of both sides. You can easily confirm if the management channel is active by looking a T the WEB GUI header – if the remote side status indicator is not greyed out the remote management channel works.

## 2.3 Storing the configuration and the configuration scope

The unit stores its configuration in a restart persistent memory banks referenced as 'w0', 'w1', 'w2', 'w3' and 'fd':

- **w0** - the local unit start up configuration which is loaded during boot process
- **w1, w2, w3** – spare configuration slots for optional alternative configurations
- **fd** – a special non-changeable slot containing the factory default configurations

Although most of configurations take effect immediately upon setting, the start up memory (w0) will not be automatically updated. In order to make the setting restart-persistent such settings have to be committed into the w0 memory by means of pressing the button. Note that  the button will indicate pending unsaved changes by changing its colour to red.

Important notice: After pressing the Write button only the local unit settings are stored in the startup memory!!! The remote unit settings configured within the local unit have to be manually committed in the remote unit management.

For description of all possible settings please refer to Graphical User Interface (WEB GUI) section of this document.

### 3 First configuration steps

This chapter describes the necessary steps to make the device and RF link up and running. It is recommended to do the basic configurations off-site.

#### 3.1 Connection and Login

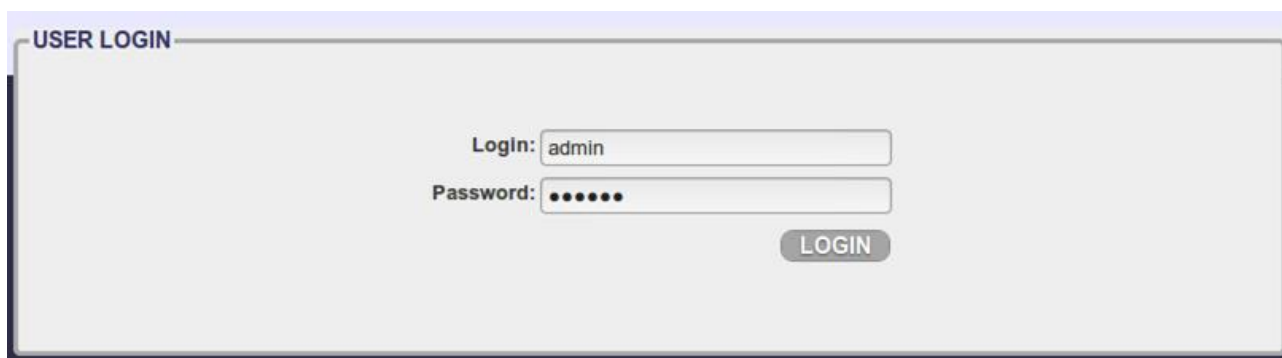
In order to be able to successfully login into the device you need to know either its primary or secondary IP address and appropriate credentials. The factory pre-set values are:

Role	Default account name	Default account password	Privileges
ADMIN	admin	secret	View and change settings, monitoring, licence and firmware updates, reboot, user administration
USER	user	test	View and change settings, monitoring, reboot
GUEST	guest	(no password)	View link related settings, monitoring

Interface	Default primary/secondary IP
ETH+POE (LAN2)	may vary / 10.10.10.10
USB MNG port	may vary / 10.10.11.10

Note that the USB MNG port is intended for manufacturing purposes only. The IP settings of this port is not visible in the WEB GUI but it is possible to alter its settings via the command line interface (CLI).

Once you have all required information as well as active management connection (as described in the section Management access) you can enter either the primary or the secondary IP address into your WEB browser address bar and the login window will appear:



USER LOGIN

Login:

Password:

After pressing **LOGIN** the button there are multiple possible results depending on active user connections:

No other active management connections or another 'admin', 'user' or 'guest' user logged in <ul style="list-style-type: none"> <li>• the CLI/SNMP with inactive 'enable' mode</li> </ul>	The main page will be displayed
Another 'guest' user logged in <ul style="list-style-type: none"> <li>• the WEB GUI</li> </ul>	
Another 'admin' or 'user' user logged in: <ul style="list-style-type: none"> <li>• the WEB GUI</li> <li>• the CLI/SNMP with active 'enable' mode</li> </ul>	A warning will be displayed with option to take over the management connection. The other connected user will be disconnected.

After successful connection the main GUI page will appear.

## 3.2 General system configurations

### User settings

The user account settings can be done in the *General/User* GUI section. There are three possible roles: *admin*, *user* and *test* each with their own set of privileges.

It is possible to alter the default *Login Names* and *Passwords*. The device does not support adding another user defined user accounts.

### Device name and description

It is recommended to conclusively define the device and link descriptions. The device identifiers can be defined in the *General/Info* GUI section.

See the possible identifier configurations in the Info section of this document.

### Device date and time settings

The date and time settings is located in the WEB GUI section *General/Date*. It is possible to set the *Date*, *Time* and *Time Zone* manually or to define a remote time synchronization server. It is possible to use three remote time synchronisation protocols:

- ntp
- ntpds
- rdate

If a remote time synchronisation server is defined and alive the device will automatically adjust its time parameters during boot and once per 24 hours.

### 3.3 IP configurations

During the initial configuration it is necessary to setup basic IP parameters. This step is necessary for proper communication between local and remote side and optionally for ensuring remote access to device from customer's network. The relevant IP settings is located in the *IP* GUI section:

- Primary IP / Mask - IP address assigned to port ETH0 (local device address) with appropriate net-mask specification. Net-mask value is inserted in form of decimal number which corresponds to numbers in binary subnet mask presentation. Such net-mask for subnet mask 255.255.255.0 is presented as decimal number 24. This IP address is used for general management access to the device as well as for internal management channel which handles the communication between local and remote devices.
- Gateway IP – the default gateway of the customer's management network
- Remote A IP (over rfi1) – the Primary IP address of the remote device

For purpose of the initial configuration leave the other parameters in their defaults.

See all possible IP settings in the IP Page section of this document.

### 3.4 Modem and Radio configurations

As the next step it is necessary to set the basic radio parameters according to the Telecommunication Authority requirements in manner which will be used for the final completion of the link installation.

All radio related settings can be found in the GUI section *Radio*. For initial link operation is necessary to set a T least these parameters:

- TX Frequency – The transmitting frequency as assigned by the Telecommunication Authority.
- RX Frequency - The transmitting frequency of the opposite radio. This value may be automatically set by the device in case when the radio part has a fixed spacing between Tx and Rx frequency.
- TX Power Limit – The maximal radio output power
- Bandwidth – The maximal modulation bandwidth

For purpose of the initial configuration and installation leave other values in their default configuration.

It is also strongly recommend to leave the *XPIC*, *ATPC* and *ACM* functions disabled during the initial link installation as they can distort the receiving levels through dynamic Tx Power and Tx Modulation adjustments making the initial RF link setup harder to fine tune and monitor.

During multi channel link installation is recommend to setup and adjust only one channel at a time having the other channel's *TX Mute Config* set to 'muted' state. This way ensures that the link quality indicators (MSE, RxL) will not be affected by a possible interference from the other channel. When both channels work satisfyingly separately you can 'unmute' both of them for final adjustments.

Important notice: Never operate the radio link indoor without proper waveguide equipment! Doing so may result in serious damage of the device and exposing operators to harmful levels of radio emissions.

## 4 Graphical User Interface (WEB GUI)

### 4.1 Web header & Side panel description

The screenshot displays the ATH System Web GUI interface. At the top, there are three header sections: 'LOGIN INFO / LOGOUT' with the ATH logo and 'Logged as role ADMIN'; 'HEADER / Local Info' with a table of metrics; 'HEADER / Link Info' showing 'TW24' link details; and 'HEADER / Remote Info' with another table of metrics. A 'WRITE BUTTON' is visible on the right. On the left is a 'MAIN MENU' with categories like General, Alarms, Radio, Ports, IP, Count, and Maintenance. Below the menu is 'BUILT-IN HELP' and 'DEVICE INFO SECTION' showing system details like Date, Time, Uptime, and Modem S/N. The main content area is divided into 'RADIO STATUS' and 'MODEM STATUS' tables. 'RADIO STATUS' shows parameters for Channel 1 and Channel 2 (LOCAL and REMOTE) such as TX Frequency, TX Power, and RX Level. 'MODEM STATUS' shows parameters like Modem Mode, Modem Sync, MSE, Bandwidth, and XPIC. At the bottom is the 'SYSTEM INFO' table, which lists details for the Modem, Radio 1, and Radio 2, including Serial Number, Product Number, and Firmware. A 'CONTENT FRAMES' label is also present in the bottom right of the main content area.

After successful login the main GUI window will appear:

The GUI is divided in 5 general sections:

#### Header section

Basic link parameters are displayed in this top bar section. A content in this section is common to all GUI pages but can differ across different *Modes*.

#### Main Menu

Main navigation menu which is accessible from each GUI page.

#### Device info section

This section gives the user overview of basic device informations such as device *Date*, *Time*, *Uptime*, *Login* session expiration (click for expiration reset), *Serial Number*, *Firmware* version, *License* status, active *Design* and active *Mode*.

## Status bar

This section informs the user about status of ongoing actions.

## Content frame

This area changes depending on the selected page. It contains various informational and functional elements. Moreover most segments of the web GUI have little index mark next to them which show built-in help informations related to such segment upon clicking.

## 4.2 General

### 4.2.1 Status

This is the front page of the GUI interface seen immediately after successful login. It is divided into two sections:

- RADIO STATUS
- SYSTEM INFO

These section gives the user the most important summary of link parameters and condition.

### 4.2.2 Mode

The *Mode* is definition of device role in the link. This page is divided into two sections:

#### MODEM MODE

Selection of the desired mode. Content of this menu depends on available system modes defined in the device license. Please note that it is recommended to save configuration and reboot the device after *Mode* change. The available modes are:

- end unit dual: both channels will be used
- end unit 1/2 : only the selected channel will be used
- aggregation: port aggregation mode

#### AGGREGATION CONFIG

When the aggregation mode is active a second section of the *Mode* page will appear. This section serves as configuration of the selected *Mode*. This section also provides a basic overview of the selected *Mode* condition. Only settings related to the selected *Mode* will be listed. The *AGGREGATION Mode* consists of the following options:

- AUTO – Data to both: The standard aggregation configuration. With this option selected the device automatically checks if both A and B channels are operable and will use only operable channels for the transmission.
- TX1/2 – Data to modem 1/2: By this option you can force the IDU to send all data through particular channel. This can be useful when you are diagnosing problems in the link such as accidental data drops, during maintenance and so on.



- **FORCE** – both, noauto: This option disables the availability checking described in the AUTO mode. Both channels will be used no matter what their condition is. Useful for debugging purposes.

### 4.3 Info

The info section serves number of optional user-defined description fields:

- **Device Name** – the device name shown in the header
- **Page Header** – the web browser page title
- **Link Name** - name of the whole link shown in the header
- **Custom Text** – free field for user input

#### 4.3.1 License

This section displays the content and status of the currently used license with available modulation schemes and options as well as remaining license time when a time limited license is in use.

#### 4.3.2 Date

The section with date, time and time zone settings. It also allows to define a remote time synchronisation method. Please note that the date and time settings may not be available if a time limited license is in use.

#### 4.3.3 Users

In this section you can define default credentials – login name and password. This page offers an option to accept only 'secure' passwords.

For description of available login *Roles* please see the Connection and Login section.

## 4.4 Alarms Page




### 4.4.1 Status

This section contains information about current and historical alarm events. The displayed content can be selected by means of these selectors:

- **Actual** – The list of alarms which are active in the particular moment. Under standard circumstances should be empty.
- **History** – The same as above for alarms which occurred in the past but which are no longer active. Moreover an extra button *ALARM HISTORY VALIDATION* will be shown. By pressing this button you are letting the unit to know that you have reviewed such historical alarm so the status of the device will be evaluated only from alarms which occurred after the manual validation.
- **All** – The conjunction of both *Actual* and *Historical* alarms. Moreover an extra button *CLEAR ALL ALARMS* will be shown. By pressing this button you can erase all active and historical alarms.

#### 4.4.2 Alarm Conf

On this page you can enable which alarms will be reported back to the user as device status and SNMP traps (if configured). Only such alarms which are enabled in this section will be recorded in the unit's *Status* section. The configurable parameters have an appropriate editable field. Alarms can be configured only for the local side but the actual status of both local and remote device is shown if available:

-  OK status
-  WARNING status
-  ALARM status

The section is divided into two parts:

##### ALARMS CONFIG

In this section are listed possible events with direct immediate impact on the link operability:

- Modem License – This alarm will be raised when the license file is about to expire or is expired already or contains an invalid data
- Modem HW – A hardware problem with the device such as non working ventilator
- Modem SW – A software problem such as incompatible mode selection on local and remote side
- Modem Sync - This alarm indicates actual status of modem synchronization
- Modem Mux Sync - This alarm indicates actual status of packet processor (PBPS) synchronization.
- Radio Telemetry – The status of communication with the radio part
- Radio HW – The status as reported by the radio part

##### WARNINGS CONFIG

In this section are listed possible events with partial immediate impact on the link:

- Modem Temperature – The temperature of the modem part
- Modem LAN1/2 Link – status of the LAN port Link
- Modem SFP1/2 Link - status of the SFP port Link
- Modem Aggr/Prot – Status of the Aggregation/Protection
- Modem MSE Level – Link quality indicator threshold settings and status
- Modem FER – The threshold for error frames per minute
- Radio Temperature - The temperature of the radio part
- Radio RX Level - The receiving level threshold
- Radio TX Mute – Transmitting Mute status

### 4.4.3 Logs

This section provides historical data of the device condition. Sections enlisted under this page are independent on the current alarm settings so all events will be recorded. The historic span of these informations depends on the link condition – a lot of events will cause quicker filling of these logs and sooner overwriting of the oldest records.

- Cnt&Sys&Alarm – Combination of Counter, System and Alarms log as described bellow
- Counter Log – System counter events. When an error is detected or resolved this file is appended by the actual link parameters in such moment
- System Log – System events such as license action, radio configuration changes, etc.
- Alarms Log – The alarm log
- Commands Log – History of performed commands
- Auth Log – Authentication history
- SNMPd Log – Reports of the internal SNMP daemon

## 4.5 Radio Page

### 4.5.1 Parameters

This section contains the most important radio and modem setting. It allows configuration of both local and remote side parameters. Note that the remote settings feature requires an active radio connection to the remote side in order to provision and apply the remote settings. Also note that you have to store any changed setting separately in both local and remote side.

#### RADIO

- TX Frequency – Transmission frequency can be set within the displayed frequency range in accordance with radio sub-band specification (read from the radio part). Such displayed range is the edge to edge flat diplexer frequency scope and therefore respective Tx Frequency value within that scope must be increased / decreased by one half of used modulation bandwidth if that is near these edges.
- RX Frequency - Receive frequency is usually set automatically as the radio part operate with the fixed T/R spacing.
- T/R Spacing – TX / RX frequency distance is a real calculated value of this parameter.
- TX Power Limit – Maximum transmission power parameter defines the maximum power level which is required for optimal transmission conditions. The operating TxPower then depends on:
  - Configured ATPC values
  - radio part power limit which depends on the used RF band and selected modulation.
- TX Power – The output RF power level that is actually transmitted of the radio part
- TX Mute Config – Transmitter mute configuration. Two modes of this parameter can be selected. Mute mode is selected for fixed radio mute configuration. Auto mute mode is a standard selection for this

parameter. In that case is the radio part automatically muted when abnormal transmission conditions are detected by the device.

- ATPC Function – Automatic Transmit Power Control enables or disables the ATPC feature. The transmitted power is automatically adjusted to ensure that the optimum RxLevel (ATPC RxL) is received at the remote side (hitless regulation).
- ATPC RX Level - Required level for Automatic Transmit Power Control. Field specifies the optimal receive level used for the ATPC function.

#### MODEM

- Modem Sync – Demodulator synchronization status is the basic indicator of proper function of the device's receiver
  - ok – It indicates that demodulator is synchronised with received air-frame
  - loss – It indicates that demodulator is not synchronised with received air-frame
  - n/a – Not available due to lack of RF/management connection to the remote side
- XPIC Function - XPIC allows the assignment of the same frequency to both vertical & horizontal polarization or in other words to operate both radio channels within the same frequency.
- Bandwidth – the bandwidth of the transmitting modulation. The number after the underscore indicates the variant of the modulation.
- Max RxACM Profile – The highest possible modulation at a given bandwidth. While the ACM function is enabled this value will be the highest possible modulation, otherwise this will be the actual modulation. Each modulation can have multiple Forward Error Correction variants:
  - medium – optimal FEC, medium throughput speed
  - strong – strong FEC, lowest throughput speed
- MUX sync – This box displays the actual Packet MUX synchronization status.
- ACM Setting – Gear icon indicates that the ACM settings do not match the factory defaults and leads the user to the ACM settings. If the ACM is set to defaults such information will be displayed instead.
- Advanced Setting - Link to the advanced radio settings.

#### 4.5.2 Analyser

Integrated spectral analyser for free channel lookup, or alternatively for detection of interference within the particular band.

This GUI section consists of two frames:

##### SPECTRUM ANALYSER

The spectrum analyser configuration frame.

- Local TX Mute Duration – TX Mute Duration in seconds for the Frequency analyser
- Delay Before Start - Delay before start of frequency analysis in seconds

- Auto Mute Remote Radio - Allows auto mute of remote radio if possible (this function requires synchronization with remote side)
- Delay status – A remaining delay time countdown

#### SPECTRUM ANALYSER OUTPUT

The spectrum analyser output frame. It displays the analyser results collected since last device reboot.

#### 4.5.3 Diagram

This section provides actual spectrum and constellation diagrams of all channels.

SPECTRUM: A simplified Rx spectrum plot.

CONSTELLATION DIAGRAM: A representation of a signal modulated by the digital modulation schemes. Two-dimensional scatter diagram in the complex plane a T symbol sampling instants. Measured constellation diagram can be used to recognize the type of interference and distortion in a signal.

- gaussian noise is displayed as fuzzy constellation points
- non-coherent single frequency interference is displayed as circular constellation points
- phase noise is displayed as rotationally spreading constellation points
- amplitude compression causes points located in the corner to move towards the centre

#### 4.5.4 ACM

The Hitless Adaptive modulation (ACM) settings. This page is divided in two separate sections:

##### ACM SETTINGS

- ACM function
  - auto pX – ACM enabled. The Rx modulation will be automatically adjusted according to the given ACM profile settings
  - man pX – ACM disabled. The Rx modulation will be fixed to the modulation specified by the *Max RxACM Profile* settings on the *Radio/Parameters* page
- ACM Offset – The MSE offset off the pre-set *thrLo* and *thrHi* constants (see below)

##### ACM PROFILE SETTINGS

The list of possible Rx modulations with their switching thresholds which will be used by the ACM in accordance with the selected profile.

- ACM\_nr – designation of the modulation
- en – enables a modulation for ACM switching
- mod/fec – bandwidth/forward error correction level
- spd – maximal throughput
- thrLo – MSE threshold for switching to lower Rx modulation

- thrHi - MSE threshold for switching to higher Rx modulation

Please note that the ACM settings of local and remote devices should match.

#### 4.5.5 Advanced

This section provides various options for advanced radio and modem part settings:

##### RADIO ADVANCED SETTINGS

- Radio Filter
  - auto – Filter is selected automatically according to the modulation BW (default)
  - narrow – Manual selection of narrow radio filter
  - wide – Manual selection of wide radio filter
- Radio Power Supply – by this option you can turn off the powering into the radio part

##### MODEM ADVANCED SETTINGS

- Modem Signal Type – Specification of modulation output. It is possible to replace standard modulated signal with carrier signal (CW) in this drop-down menu. The possible modes follows:
  - qam – TxIF modulated signal is presented a T IF output from the device (default)
  - cw – Carrier signal with given frequency is presented a T IF output
- CW Frequency – carrier signal frequency settings

#### 4.5.6 Details

This section provides summary of basic and advanced modem and radio parameters. These values are collected directly from respective parts and reflects the actual state of such parts. Description of listed parameters is out of scope of this document.

## 4.6 Ports Page

### 4.6.1 Parameters

In respect of management access type, traffic modification (number of independent channels over air) and the protection / aggregation function preference the user has to select the relevant *Mode* type (see the Mode settings) before starting any port settings. Each *Mode* uses similar but not identical port configuration scheme. By default the internal ETH switch is divided into four groups. Such setting prevents potential

DATAFLOW CONFIGURATION							
PORT		SFP1	SFP2	LAN1		LAN2	
PORT CONFIG	Status	SFP module not present	SFP module not present	LAN No LINK	LAN Gbit FULL		
	Hot Standby	off		off			
	Mode	auto1G	auto1G	auto	auto		
	MDIX	-	-	auto	auto		
	Flow Control	force	force	off	off		
1588	off	off	off	off			
ETH SWITCH							
	<p>Channel Select: none, none, none, none, ETH1a, none, RF11, RF12</p> <p>Connected Port: none, none, wana, none</p>						
PBPM	Traffic Channel	PTP1	EMM1	ETH1a	ETH1b		
	Speed Limit	auto	auto	1000	0		
Available Speed		438 Mbps			438 Mbps		

Figure 19: Port parameters, Aggregation Mode

loops a T connected LAN ports for all *Modes*.

The port settings consists of several configuration layers labelled leftmost of the configuration window:

- PORT CONFIG
  - Status – status of a port as detected by the device (speed, duplex mode, link, administrative down status).
  - Hot Standby – automatic switch over between ports according to actual link status. (Hot standby function (not yet implemented))
  - Mode – This drop-down menu displays and defines the actual port mode (speed/duplex, administrative down)
  - MDIX – It is possible to set particular ETH cable crossing like auto/mdo/mdx by means of this configuration

- Flow Control - Informative field displays the actual duplex flow control mechanism settings. Flow control setting is available from page Ports / ETH Advanced
- 1588 – Precision time protocol source. (Not yet implement)
- ETH SWITCH – This block illustrate the ETH switch fragmentation into groups and also their inter-connection with physical LAN ports and internal WAN ports. The group configuration is performed on ETH VLAN page
- SWAP
  - Channel Select - Settings of data multiplexor. By this settings you can cross connect a particular *Switch* port with a *Mux Channel*.
  - Connected Port – Current settings of the SWAP block
- PBPM - Priority Based Packet Multiplexer settings
  - Traffic Channel - shows boundary between the selected channel and port
  - Speed Limit - speed value for transmitting data with priority falling from left to right
- Available Speed – it indicates the available capacity of appropriate channel. This value depends on selection of the actual modulation scheme and license speed limits. This selection has similar functionality as egress limiting.

**Speed Limit example:**

Suppose the *Available Speed* is 110Mbps with *ETH1a Speed Limit* set to 50Mbps and *ETH1b Speed Limit* set to 110Mbps.

That means:

- ETH1a payload traffic will be 50Mbps, independently on ETH1b traffic because the port priority is taken from left to right
- ETH1b payload traffic will be the remainder of the available speed, in this case  $110 - 50 = 60$ Mbps

#### 4.6.2 ETH VLAN

VLAN configuration is basically used for the separation of management traffic from other customer data traffics. It can be useful to configure ETH VLANs also for customer traffic and filter ingress data traffic by means of this settings in some specific applications. The description of particular setting and display boxes:

##### VLAN MODE SETTINGS

- Port mode – it is possible to set-up the required VLAN mode separately for each ETH switch port. It is recommended to leave all ports in basic mode and edit VTU records first. The user has to be sure with correct VLAN configuration and has to set also his network into the similar VLAN support. VLAN Port modes are described bellow:
  - basic – Transparent mode where VLAN settings in VTU table are ignored. Frames are transmitted unchanged but they exit only those ports which are inside the same group.



- access – Port is a member of just one untagged VLAN defined with Default VLAN for the port. Only such ingress untagged packets are accepted, whose VLAN number (VID), which is assigned from port's Default VLAN, exist in VTU table. Frames are transmitted untagged and they are allowed to exit only those ports that are members of the frame's VLAN and are inside the same group.
- trunk – Port can be a member of more tagged VLANs (VID extracted from VLAN tag) and one untagged VLAN defined with Default VLAN for such port. Only such frames are accepted, whose VLAN number (assigned from VLAN tag or port's Default VLAN) exists in VTU table and Ingress port is member of VLAN. Frames are transmitted untagged or tagged according to the specification in VTU record for each port/VLAN and they are allowed to exit only those ports that are members of the frame's VLAN and are inside the same group.
- hybrid – When frame's VLAN number exists in VTU table the rules for trunk port are used, when the number does not exist then the basic rules are applied.
- Port Group – This parameter defines a separate MAC address table domains inside the internal switch and defines also the group of ports which can communicate to each other. Only the ports from the same group can communicate with one another. The other ports are completely isolated. It is possible that isolated networks (different groups) can use the same MAC addresses without any collision in the internal ETH switch ATU table.
- Default VLAN – This parameter is configured automatically depending on records in the VTU table. Default VLAN is updated for the port which is marked as untagged in the VTU record. VLAN No.1 can not be added into VTU table and it is just fictive VLAN for internal purposes. The port cannot be configured into access mode when Default VLAN of this port is 1. When Default VLAN value for the trunk port is 1, then the port accepts tagged frames only.

#### VTU SETTINGS

- ACTION – It adds or removes VTU records. A VTU record can not be removed when contains untagged port which is configured into access mode. Just simple VLAN NO. specification is required for VTU record erase.
- VLAN N. – The VLAN number of edited VLAN (added or deleted). Every VLAN can be defined for only one Port Group, multiple records of the same VLAN for more groups is not allowed.
- GROUP – It defines the port Group for which is VLAN edited.
- QOS PRI – When VTU override mode is selected then the QOS priority value of original frame is overridden. This configuration has influence only on the internal frame processing by means of queue controller (QPRI defined by OQPRI instead of IQPRI bits), but frames are still egressed with the initial priority assignment (FPRI is without any change).
- LAN 1-WAN P – It defines VLAN mode for each port in configured VLAN.
  - Deny – Port is not a member of edited VLAN. Ports which are defined in different Groups should be set into this mode.
  - Untag – Port is a member of edited VLAN as untagged.

- Tag – Port is a member of edited VLAN as tagged.

#### LISTING OF ACTUAL VTU VALUES

List of VTU records (defined VLANs) in the ETH switch. The abbreviations in this list correspond to the first letter of the port mode definition in VTU records.

### 4.6.3 ETH Advanced

#### QOS ETHERNET SETTINGS

This section makes it possible to configure extended QOS modes which are important for a specific traffic prioritization. The system uses four priority queues for each port where frames, with an assigned initial frame priority, an initial queue priority and an override queue priority, are mapped onto four output queues according to QPRI settings. A final frame queue priority is derived from the assigned initial queue or the override queue priority and it is used for deciding what queue will be used for frame buffering. The queue with a higher number is egressed with higher priority than the queues with lower numbers. The assigned initial frame priority is then used for replacing of frame's PRI bits in 802.3ac VLAN tag section, when the frame is egress tagged.

- QOS Modes
  - weighted – In the weighted scheme an 8, 4, 2, 1 round robin weighting is applied to the four priorities (8 frames from Q3, 4 frames from Q2, 2 frames from Q1 and 1 frame from Q0). This approach prevents the lower priority frames from being starved out with only a slight delay to the higher priority frames.
  - strict 3xxx – Strict priority for queue 3 and weighted round robin for queues 2,1 and 0. Queues 2,1,0 are served only when Q3 is empty.
  - strict 32xx – Strict priority for queues 3,2 and weighted round robin for queues 1 and 0. Queues 1,0 are served only when Q3 and Q2 are empty.
  - strict 3210 – Strict priority for all queues. Lower priority queues are served only when higher priority queues are empty.
- Priority policy – This drop-down menu defines the initial ingress queue policy. It defines the initial rules for what output queue will be assigned to every ingress frame.
- Port Priority – The configuration of default port priority. Value 0 up to 7 can be entered (0 is default value)
- Priority Override – It offers the possibility to replace an initial queue priority with a new priority. The new priority is assigned to each frame whose VLAN ID is defined in the VTU table with properly configured QOS PRI value.
  - off – QOS override is disabled
  - vtu – Queue priority override information (OQPRI). When this parameter is set to off state, override process is not active for appropriate VTU record, even though Priority override is enabled on the port.

#### FLOW CONTROL SETTINGS

This setting affect the Flow Control settings of particular ports. The settings is allowed for only such ports and *Modes* where is such settings possible. The possible values are:

- off – Flow control is disabled
- auto – Flow control is enabled during auto-negotiation process
- force-on – Flow control is active, even if connected device does not support it

## 4.7 IP Page

### 4.7.1 Address

Every device in the local network has its own and unique primary IP address. Thanks to this IP address it is possible to access each equipment in your network. While setting-up the IP address, pay attention to the configuration which needs to follow general IP addressing rules (IP address, IP net-mask, IP gateway). Customer has to ensures that correct IP addresses are assigned and configured for all units in the microwave network.

The description of particular setting and display boxes:

#### IP SETTINGS

- Primary IP / Mask – IP address assigned to port ETH0 (local address) with appropriate net-mask specification. Net-mask value is entered in form of decimal number which corresponds to number of ones in binary subnet mask presentation. Such net-mask for subnet mask 255.255.255.0 is presented as decimal number 24. Local network has its own and unique primary IP address.
- Gateway IP – Default Gateway IP address is used by MNG CPU when connection outside of IP range defined in system routing table is required. Such IP address must be a part of above mentioned routing table. Routing table can be checked on page „IP / Route/NAT”.
- Unnumbered IP mode – by enabling this option you will get option to manually configure the *RF port A/B IP (RF1/2)* settings (see bellow)
- RF port A/B IP (RF1/2) – it specifies internal IP address for RF1/2 port (connected with west/east remote unit). Default RF1/2 IP address uses the same value as ETH0 port (unnumbered mode). It can be helpful to set numbered ppp mode for a specific network configuration.
- Single remote IP mode – By default enabled. If unselected the user can define 2 separate remote IP addresses for cases when 2 separated remote devices are in use.
- Remote A/B IP (over rfi1/2) – such address specifies a remote unit IP connected over RF link. Such address is necessary for automatic MNG message exchange between these devices and also for correct out-of-band management functioning. Subnet mask is not required for this IP specification, because ppp protocol is used. The *Remote B* field will become configurable when the *Single remote IP mode* option is disabled.

#### MANAGEMENT ACCESS

- HTTPS, SSH – cannot be turned off. For https (secure web) access you can upload your own server certificate (SC). For client (browser) access, it is necessary to prevent an exception for this SC, the certificate of CA (signing SC) should be stored in your browser.

- HTTPS with Client Certificate – https access is possible only if the client (browser) has installed client certificate (CC) signed by certification authority (CA). This option is available only if the device has the CA certificate uploaded. Reset of the CA certificate is possible only if this option is not selected.
- HTTP, TELNET, SNMP – to increase security of device you can disable unencrypted access (http, Telnet, SNMP v2) and turn on only SSL, HTTPS, SNMP v3 (SNMP can be set on *IP/SNMP* page).
- SSH with KEY – You can define secure login to the device without username/password login prompt. It is required to have a public part of your SSH key loaded in the device. Multiple keys can be used. By default is this option switched on.
- SSH user/password login enabled – You can switch off SSH username/password login. You must be sure login without password is working! Reset of the SSH keys is possible only if this option is checked.

#### 4.7.2 Route/NAT

For a specific configuration of management access, it is sometimes necessary to add/change/delete static routes or NAT records. This is especially required for Out of band type of management access.

##### STATIC ROUTES

- Routed IP / MASK – the IP address from routed network and the appropriate network mask must be inserted. Routed network range is calculated from inserted values.
- Gateway IP – the correct IP address gateway for above mentioned network must be inserted.

##### NAT

- LocalPort DestIP:Port – the NAT record must be inserted in the following format: *local\_port destination\_ip:port* (example: '10443 192.168.1.2:443' => local port 10443 redirects to the port 443 (secure web - https) of the unit with IP 192.168.1.2)

##### RADIUS

- IP:destport SecString timeout – the definition of remote Radius server
  - IP – IP address of the Radius server
  - destport – Destination port. This is an optional parameter
  - secString – password of Radius Server login. The recommended length of the password is from 4 to 50 characters
  - timeout – connection time-out between the device and Radius Server. Recommended value is 1 – 5 second

##### SETTINGS

This frame informs the user about the *CONFIGURED* and *ACTUAL IP* settings. In order to activate the new setting please use the *APPLY & WRITE* button (you will be logged out) or *WRITE* the settings and reboot the device.

### 4.7.3 SNMP

This window provides the configuration options of the inbuilt SNMP server:

#### SNMP CONFIGURATION

- **SNMP Enable** – this check box enables the SNMP daemon in the device
- **SNMP Version** – SNMP v2c or SNMP v3 can be used for SNMP access to device
- **SNMP Port** – the parameter specifies which port will be used for SNMP communication. The same configuration must be set also in SNMP agent station
- **Trap Port** – the parameter specifies the destination port on which SNMP traps will be sent to. The same configuration must be set also in SNMP agent station
- **Trap Address 1-3** – up to three IP addresses can be configured as destination for SNMP trap distribution. Trap message events are configured in the same way as the alarm setting

#### COMMUNITY SETTINGS

These settings are required only for the SNMPv2 protocol. For SNMPv3 has no effect.

- **Community string** – the parameter specifies community string for secure SNMP management access (different setting for read only and read/write access can be entered, valid for SNMP v2). The number of characters in the input field have to be in range from 1 to 15. Valid characters are [a-z, A-Z, 0-9, \_]
- **IP Address/Mask** – up to three IP addresses or subnets can be configured as permitted IP source for SNMP management access. Please note that the *Mask* parameter is not optional.

#### SNMPv3

These settings are required only for the SNMPv3 protocol. For SNMPv2 has no effect.

- **User Name** – user name configuration for secure SNMP access with SNMP v3 protocol (different setting for read only and read/write access can be entered). The number of characters in the input field have to be in range from 4 to 15. Valid characters are [a-z, A-Z, 0-9, \_]
- **Auth and Privacy Password** – password configuration for secure SNMP access with SNMP v3 protocol, the identical password must be entered into Confirm Password box (different setting for read only and read/write access can be entered). The number of characters in the input field have to be in range from 8 to 15. Valid characters are [a-z, A-Z, 0-9, \_]
- **Encryption** – the encryption protocol for the SNMPv3
  - CFB-AES-128
  - CBC-DES

### 4.7.4 Advanced

This section allows configuration of secondary IP address as well as optional FILE TRANSFER settings:

- **Secondary IP/Mask** - it specifies secondary IP address for ETH0 management port. When default secondary IP address is in collision with other network configuration it can be changed with this parameter

- FTP/USB Server – when „usb” is written into this box, the USB port is used as destination/source interface for backup and/or restoration of device’s configuration. When “ftp://IP/directory\_structure/” is inserted into the box, an external FTP server is used as destination/source address for backup and/or restoration of device’s configuration and license/firmware upgrades. For secured FTP you can use syntax “ftp://user:password@IP/directory\_structure/”

## 4.8 Count Page

Sections of the Count Page provides detailed overview of the system conditions.

### 4.8.1 Basic/BER

#### MODEM COUNTERS

- FEC RX Blocks – the overall number of received air frames
- FEC Corrected Blocks – the number of air-frames which were repaired by FEC (Forward Error Correction). This number represents a fragment of the *FEC RX Blocks*
- FEC Uncorrected Errors – the number of air-frames which could not be repaired by FEC. This number represents a fragment of the *FEC RX Blocks*
- Uncorrected – Last Second – the number of air-frames which could not be repaired during the last second
- FEC Global Rate – the ratio of *FEC Uncorrected Errors / FEC RX Blocks*
- FEC Actual Rate – same as above but for latest second only
- Uncorrected TLE – time since last error; number of seconds from the last error occurrence. It should correspond to the time since pressing the CLEAR button
- Uncorrected TBE – time between last two error events
- Uncorrected EFS – error free seconds; it should correspond to time since pressing the CLEAR button
- Uncorrected ERS – error seconds; number of seconds during which errors occurred

#### STATISTICS - BIT ERROR RATE (BER)

This frame provides the built-in BER tester results. Please note that only unassigned capacity will be used for BER tester.

- Status – BER tester synchronisation status (sync|nosync) or n/a when there is no active link to the remote side or free capacity left for the BER tester
- Actual Tx Speed – shows reserved transmission speed for BER tester. This value roughly equals to half of the unassigned capacity which is used for the BER tester
- TX Pattern – shows transmission pattern for BER tester frames
- RX Pattern – shows receiving pattern of BER tester frames
- Rx Bit Count – shows number of received bits (BER)
- RX Err Count - shows number of received error bits (BER)

- Rx Sync Count – number of synchronisations of the BER tester
- BER – ratio of Rx Bit Count and Rx Err Count
- TLE – time since last BER error; number of seconds from the last error occurrence. It should correspond to time since pressing the CLEAR button
- TBE – time between the last two BER error events
- EFS – error free seconds of the BER tester; it should correspond to time since pressing the CLEAR button
- ERS – error seconds; number of seconds during which a BER error occurred

By pressing the CLEAR button, the values of counters for both device modems will be erased.

By pressing the Insert Error button, one error will be inserted into data streams of both modems.

#### 4.8.2 Ethernet

This page provides detailed overview of data frames flow. The section consists of the *LAN COUNTERS* which are captured by the device's switch and the *FPGA COUNTERS* which are captured by the modem.

#### 4.8.3 Management

This section provides IP statistics of device's interfaces:

- eth0 - Ethernet port of MNG CPU with its own MAC address and all the standard features of Ethernet interface. Primary / Secondary addresses and appropriate subnet masks are assigned to this interface.
- Rfi1/2 - ppp (point-to-point protocol) type of interface which interconnects local MNG CPU with the remote side MNG CPU accessible through the separate channel inside air-frame
- usb0 – an on-board service USB port which is dedicated for local service IP access

#### 4.8.4 Graphs

Graph describes the selected values in dependence on time. In case that the setting for connection with remote unit is correct, then the values from remote unit are also displayed.

For depiction it is possible to choose between the following options:

- TxPower – depicts the transmitted level of signal output
- RxL/MSE – received level of the signal output / quality of received signal
- Temperature – displays the temperature of modem and radio
- ETH\_Count – displays the transmission capacity for transmission and admission on the selected ports of the device
- Sync/Modul – value MLOCK = 1 displays modem synchronization, value MLOCK = 0 shows that there was no synchronization. If ACM is active, the most appropriate modulation for signal transmission or admission, is found. Individual modulations are indicated according their amount of states

You can zoom the graph by means of mouse selection of the range of interest and reset the zoom by pressing the *ZOOM OUT* button.

Please note that resolution of the displayed data will be lower for older records and higher for the newest. This time segmentation is 10 minutes, 1 minute and 1 second.

#### 4.8.5 Online Graphs

The functionality is inherited from the Graphs page described above with automatic refresh every 10 seconds with option to decrease the pooling period to 1 second. Please note that it can take up to 10 seconds before the 1 second refresh is activated. Also note that every such refresh will cause zoom reset.

### 4.9 Maintenance Page

#### 4.9.1 Config

In order to preserve the configured and modified link parameters through power cycle (or device restart), the new configuration must be saved first. The appropriate button for start-up configuration commit (W0) WRITE is available on each GUI page. Red background of the WRITE button indicates that the running configuration is not stored in the start-up memory yet. When the configuration is properly saved, it is possible to copy the actual configuration also into optional memories (W1-W3). This operation saves actual settings as alternative configuration for subsequent quick restoration of such configuration schemes with relevant RUN W0 – RUN W3 button click.

#### 4.9.2 Terminal

Inbuilt terminal window for interacting with device's CLI (Command Line Interface) directly from GUI.

For CLI usage description please see the Command Line Interface (CLI) section of this document.

#### 4.9.3 Files

This section associates device's file management:

##### FILES

This frame allows to collect various device reports as a downloadable archives in order to provide such files for off-site problem diagnostics and backup. The selected files can be collected by means of pressing the GENERATE button which will result in appropriate number of downloadable files listed in the sub-section AVAILABLE FILES. Please note that such files are erased during restart of the device.

- Save Log – archive of various log files for debugging purposes with link configuration and condition as plain text files
- License Request – a binary file with current license status. This file is meant for extending license expiration date
- Save Config – a binary file with complete configuration of the device. This file can be used for backing up the configuration or for transfer of such configuration into an another device. Please note that the configuration transfer should be done only between devices with matching firmware versions. Also please note that this file can not be read by the user.

##### CERTIFICATES AND KEYS

The other sections on this page are intended for management of SSH certificates and keys.



#### 4.9.4 Advanced

This section contains various administrative tools:

##### MODEM UPGRADE

In order to upgrade device's firmware, configuration or license the user should select the appropriate file and press the UPGRADE button. The common format of files is:

- Firmware (load files in this order)
  - hwbase.afw - software for internal HW parts
  - oskernel.afw - operating system
  - fwbase.afw - application software (WEB, SNMP, commands , etc.)
- Configuration
  - fwconf\_OriginatingSN\_Timestamp.afw (as fwconf\_3010501010100008\_1702141508.afw)
- License
  - licSN.afw (as lic3010501010100008.afw)

The name of files does not matter but the extension does. Please note that the device file validation is case sensitive so \*.afw does not equal to \*.AFW.

##### **Firmware upgrade procedure**

In order to upgrade the device:

1. save the current configuration by means of pressing the WRITE button
2. gradually select all files in order as described above. Please note that after uploading of the fwbase.afw file the device performs automatic reboot
3. after successful boot login back in the GUI and update the current start-up memory (W0) by means of these steps:
  - Navigate to *Maintenance/Config* page and press the WRITE W0 button to update the start-up configuration with newest values
  - Navigate to *Maintenance/Config* page and press the RUN W0 button to make the new start-up configuration active

Please note that firmware downgrade is not officially supported and such action can cause malfunction of the device.

The full upgrade procedure is described in *Firmware\_Release\_Notes* document which is distributed together with new firmware versions. Also please note that the firmware upgrade will not alter any customising options except for explicitly stated cases described in the *Firmware\_Release\_Notes* document. All devices in a link should operate the same firmware version.

##### DESIGN TYPE

According to the license file content a user can select specific Design Type which completely changes the system function. At the moment there is only one design available – Design 601.

#### AUTO CONFIGURATION

The start-up configuration (W0) is loaded after 10 minutes of continuous error state when the check box is selected. It is recommended to disable this function during link configuration and installation.

#### FACTORY DEFAULT

Restores the configuration of the device to its factory pre-set values. Please note that all settings including radio and IP settings will be reverted.

#### REBOOT DEVICE

After pressing the RESET button the device will perform soft-reboot. Please note that this operation will cause data drop.

## 5 Command Line Interface (CLI)

### 5.1 Basic command structure

The built-in CLI, accessible via SSH, Telnet and embedded GUI Terminal window, provides full set of commands for device settings and monitoring. The basic command structure and output looks like this:

```
device_name_NE|>show info
hw base : 12AT20601_000B0_195
fw base : 0101_01T15
www base : CLI1701251330T
os kernel: 0201_T
os dev : 0101
S/N : 3010501010100008
L/N : 3010501010100008
P/C : n/a
P/N : "AOU-2-101"
P/I1: "AOU-2"
P/I2: "Full Outdoor Unit"
P/I3: "Wideband, Dual IF FOU"
ok
```

`device_name` – the device name (set by command ‘set descr name new\_name’)  
`_NE|>` - the informative prompt. The convention is:

- `xxx_XXY>` > prompt in reading mode
- `xxx_XXY#` # prompt in enable mode
- `xxx_XX|Z` | prompt indicating unsaved changes (write w0 needed)
- `xxx_XX\Z` \ prompt indicating no unsaved changes (no write w0 needed)
- `xxx_NXYZ` N device is in ok state - see "sh alarm all"
- `xxx_EXYZ` E device is in alarm state - see "sh alarm all"
- `xxx_XNYZ` N device was not in alarm state since last alarm validation
- `xxx_XEYZ` E device was in alarm state since last alarm validation - see "sh history alarm"

**show info** – executed command ‘show’ with parameter ‘info’

**output** – output of the command

**ok** – the exit status of the command. Possible return values are:

- ok – the command was executed successfully

- not valid a T pos:1 – the numeric value represents position of unrecognised argument of the latest command. Such command was not executed
- no access – configuration changing action without ‘enable’ mode (see bellow)
- locked – an another active administrative session already in ‘enable’ mode (see bellow)

## 5.2 Altering device configuration using CLI – enable mode

In order to change any settings you have to acquire so called ‘enable’ mode. This mechanism ensures that only one login session (either CLI, SNMP or WEB) is allowed to alter the settings. Please note that this step is not necessary in the built-in WEB GUI Terminal as the administrative login in the WEB GUI acquires this ‘enable’ mode automatically.

The enable mode can be activated by means of command ‘enable’ and deactivated by command ‘exit’. It is also possible to forcefully takeover the enable mode by means of command ‘kill enable’.

Example:

```
device_name_NN>set descr name my_device // try to change device's name
no access // not in enable mode; command was not executed
device_name_NN>enable // try to acquire the enable mode
locked // an another session already in the enable mode
device_name_NN>kill enable // takeover the enable mode
ok // success
device_name_NN#set descr name my_device // try to change the device's name
ok // success; note the changed name
my_device_NE|#write w0 // commit the current settings
stage 0 ok
ok // success
my_device_NE#exit // exit the enable mode
ok // success
my_device_NE> // non administrative prompt
```

## 5.3 CLI command abbreviations

Most of the commands can be entered in their shortened form. For example:

enable = en

show = sh

write = wr

show history alarm all = sh his ala all

## 5.4 CLI online help

The CLI offers inbuilt online help accessible by means of ‘?’ question mark. Example:

```
my_device_NE|>?
- ? : print help...
- clear : clear counters (?)
```

```

- delayed : [x] [ cmd] run cmd after x seconds, result in 'sh hist del'
- enable : enable setting
- ping : [xx.xx.xx.xx] ping to ip
- quit : quit & logout
- show : system status & config & counters (?)
- ssh : [user] [xx.xx.xx.xx] ssh to ip
- telnet : [xx.xx.xx.xx] telnet to ip
ok

```

The syntax used in the online help:

[] required parameter

{ } optional parameter

(?) the parameter contains a nested parameters. Type '?' a T end of the command to see possible values and syntax

Some commands allows using the online help also for their parameters:

```

my_device_NN|#set rad1 ?
- analyzer : [my] start spectrum analyzer (option my means fine analysis around CF)
- atpc : radio atpc parameters (?)
- down : power-off radio part
...
ok
my_device_NE|#set rad1 atpc ?
- off : atpc off
- on : atpc on
- rxlevel : min rx level [-74 - 0]
ok

```

## 6 Simple Network Mangament Protocol (SNMP)

### 6.1 Basic SNMP setting

In order to monitor and manage the device with SNMP protocol you have to setup the SNMP daemon in the device:

1. Login in the WEB GUI
2. Navigate to *IP/SNMP* GUI page
3. Do the appropriate settings. Remember to choose the correct *SNMP Version* and to fill in the *COMMUNITY SETTINGS (SNMPv2)* or *SNMPv3* credentials
4. If you require the *Traps* functionality remember to enter the destination IP into the *Trap IP Address* fields

5. Check the *SNMP Enable* checkbox and hit the *APPLY & WRITE* button. Note that you will be logged-out in order to reset the IP settings. This can take few seconds but the user data flow will not be interrupted
6. Test the SNMP functionality

## 6.2 MIB

The SNMP MIB is a text file with human readable description of device's SNMP OID's. Without this file imported in your SNMP MIB agent of choice you will see the device's SNMP parameters in their numeric form (OID). With MIB file imported you will see the appropriate translation. For example:

SNMP OID	MIB Translation	Value
.1.3.6.1.4.1.12654.1.5.1.1.1.1	sysFceBasDevName	my_device
.1.3.6.1.4.1.12654.1.5.2.1.1.1	cnfFceMngIpEthAddr	192.168.3.78
.1.3.6.1.4.1.12654.1.5.3.2.2.1.3	infoFceRadMod1ActMod	1024_56000_02 medium

The process of MIB import is solely dependant on your MIB reader software. The MIB file can slightly differ across different firmware versions. The correct MIB is always included with firmware release.

## 6.3 Traps

When an alarm event occurs in the device a SNMP trap with basic summary of such event is sent to all addresses specified in the *Trap IP Address* fields. Then such trap can be accordingly processed by your NMS solution. This functionality requires that the SNMP is enabled in the device, a correct destination IP for traps is entered and such alarm is configured for logging and reporting by means of setting on the Alarm Conf page.

Example of trap content sent from the device:

Name: .1.3.6.1.4.1.1.4.5.1.0  
 Value: [OctetString] S;01.0.09;192.168.3.78 ;mod1\_sync

## 6.4 Altering device configuration using SNMP

The device can be configured by means of SNMP 'set' commands as long as the managing SNMP agent has 'write' rights correctly configured. Moreover, in order to modify the device's settings, it is necessary to acquire the exclusive *enable* mode. For more informations about the *enable* mode please see the Altering device configuration using CLI – enable mode section of this document.

In order to acquire the *enable* mode using SNMP you have to use this OID:

Name: .1.3.6.1.4.1.12654.1.5.1.1.2.2 (sysFceBasCmdEn)  
 Value: 1 (writeAccessSNMP)

Moreover remember to commit the changed configuration into the start-up memory:

Name: .1.3.6.1.4.1.12654.1.5.1.1.2.3

(sysFceBasCmdWr)

Value: 4 (startup)

RSL	RSSI BNC
-15	2,49
-20	2,34
-25	2,18
-30	2,02
-35	1,87
-40	1,71
-45	1,56
-50	1,40
-55	1,25
-60	1,09
-65	0,93
-70	0,78
-75	0,62
-80	0,47
-85	0,31
-90	0,16
-95	0,00

