7) ***AES key status*** – This information line shows the status of the actual AES key, as well as CRC of entered valid key. Note that such CRC value MUST match on both local and remote respective channels.
8) ***AES function*** – This box enables or disables AES encryption function. When enabled, the whole traffic stream from packet processor is encrypted by provided AES key. Out of band management channel is not encrypted in this mode, therefore remote access to remote IDU is possible in any way. It is required to define valid AES key(s) in order to enable the AES function.

When choosing Design type ***Design 511*** following additional configuration options will appear in this same section:

Figure 3.25 *"Config → System → Mode" page, Design 511 configuration*

9) ***Functional Mode*** – above mentioned Radio modes in ***Design 511*** can be combined with following Functional modes:
   a) ***Split 1+1 –*** full protection mode which uses one physical channel on each IDU. Two IDUs must be used on each side of the link.
   b) ***Split 2+2 –*** combination of both protection and aggregation modes. This setting requires two IDUs on each side of the link, each IDU with two radios attached.

Split 2+2 mode requires the PRT3 option in the license.

10) ***Link Protection Diversity*** modes – those modes are available when choosing above mentioned **Split 1+1** or **Split 2+2** Functional modes:
   a) ***FD*** – frequency diversity configuration with frequency separation in both physical channels of the IDU
   b) ***SD*** – space diversity configuration with single Tx channel, two Rx channels and two antennas in both directions. This mode does not support Tx switch-over
   c) ***HSB/SD*** – hot standby configuration with single Tx channel at a time and two Rx channels in both directions. This mode will switchover the Tx in case of Primary Tx failure.
11) ***Hot-Swap Startup Device Role*** – Hot-Swap configuration settings are following:
   a) ***Auto (primary)*** – auto Hot-Swap enabled, the device will be configured as 'primary' during start-up. The device will swap it's role if a protection Alarm occurs. The 'Auto (secondary)' setting MUST be set on the peer (FO) IDU. Change in this setting will not change the running device role.
   b) ***Auto (secondary)*** – auto Hot-Swap enabled, the device will be configured as 'secondary' during start-up. The device will swap it's role if a protection Alarm occurs. The 'Auto (primary)' setting MUST be set on the peer (FO) device! Change in this setting will not change the running device role.

c) ***Fixed primary*** – Hot-Swap disabled. The device role will be always 'primary'. The 'Fixed secondary' role should be set on the peer device (FO). Changing this setting will result in an immediate automatic role switch on both local devices (if interconnected).

d) ***Fixed secondary*** – Hot-Swap disabled. The device role will be always 'secondary'. The 'Fixed primary' role should be set on the peer device (FO). Changing this setting will result in an immediate automatic role switch on both local devices (if interconnected).

12) ***Running Role Swapping*** – this option is available only when the **Hot-Swap Startup Device Role** is configured in the 'Auto' mode. By pressing this button, it is possible to swap running roles of local devices

When choosing Functional mode ***Split 2+2*** the additional header information and Duplex Mode settings for both Channels will apper. Following additional configuration options will appear in this same section:

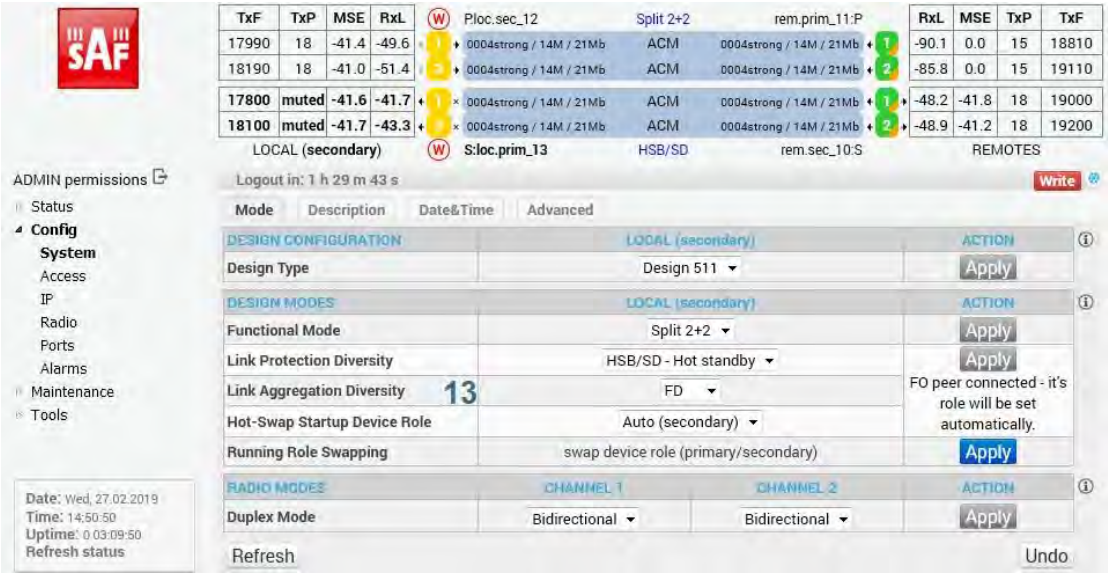


Figure 3.26 *"Config → System → Mode" page, 2+2 mode configuration*

13) ***Link Aggregation Diversity*** modes – those modes are available when choosing **Split 2+2** Functional mode:

a) ***FD*** – frequency diversity configuration with frequency separation in both physical channels of the device

b) ***XPIC*** – cross-polarization diversity with automatic attenuation of interfering signal from the X-polarized channel

Config → System → Description

It is possible to specify device information in this section.

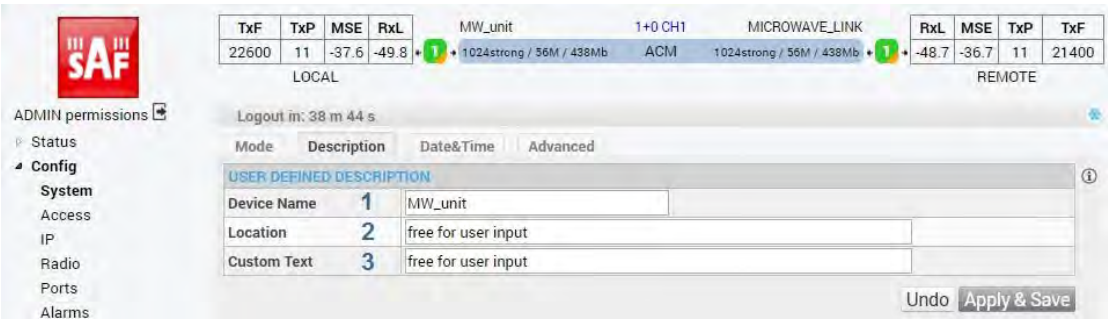


Figure 3.27 *"Config → System → Description" page*

1) ***Device Name*** – the IDU name shown in the header/web page title
2) ***Location*** – location of the IDU
3) ***Custom Text*** – free field for user input

Valid characters are [a-zA-Z0-9 _!@#%*()-+=:;',.?/] (including [] and without space character in device name)

Config → System → Time&Date

The section with date, time, time zone and the network time protocol settings.

The date and time settings may not be available if a time limited license is in use.

When ntpds value is selected, the device will be used as local NTP server. The NTP synchronization is directed by the protocol itself while the rdate synchronization is initialized once per 24 hours and during the start-up of the device.

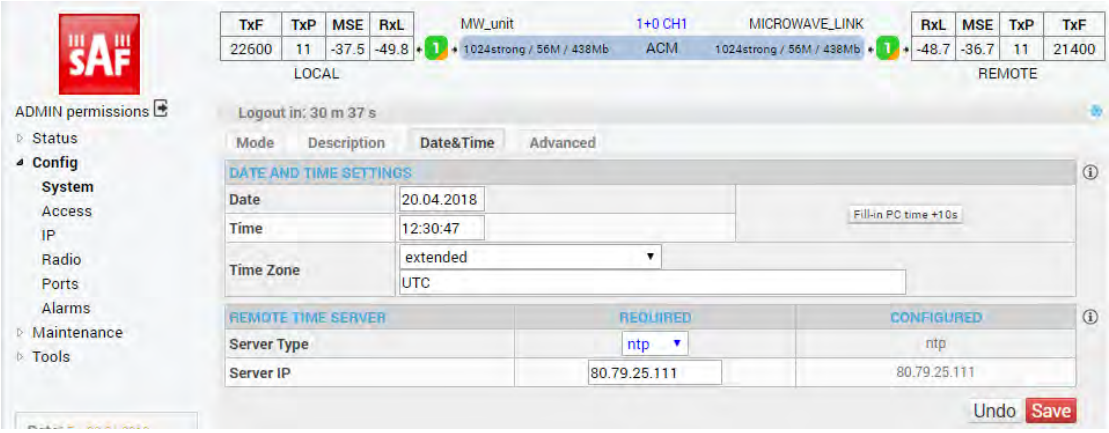


***Figure 3.28** "Config → System → Time&Date" page*

Config → System → Advanced

This section contains following advanced settings:

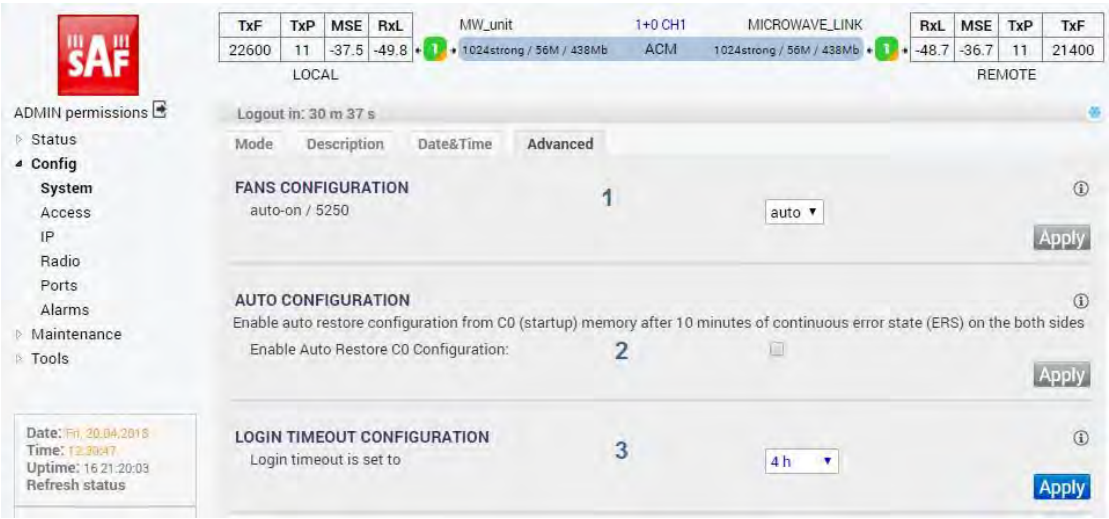


***Figure 3.29** "Config → System → Advanced" page*

1) ***Fand Configuration*** – the configuration of the inbuilt fans; options are following:
   a) ***on*** – the fan always is on
   b) ***off*** – the fan always is off
   c) ***auto*** – the fan is auto-regulated by the device (default setting)

> The thresholds for auto mode are following: >= 40°C to turn the fan on, <= 30°C to turn the fan off.

2) ***Auto Configuration*** – when the checkbox is selected, the start-up configuration (C0) will be loaded after 10 minutes of the continuous error state. It is recommended to disable this function during initial link configuration and installation. By default it is off.
3) ***LoginTimeout Configuration***– timeout settings of the GUI auto-logout. There is continuous communication between GUI and the device while logged on.

Config → Access → Users

Usernames and passwords settings

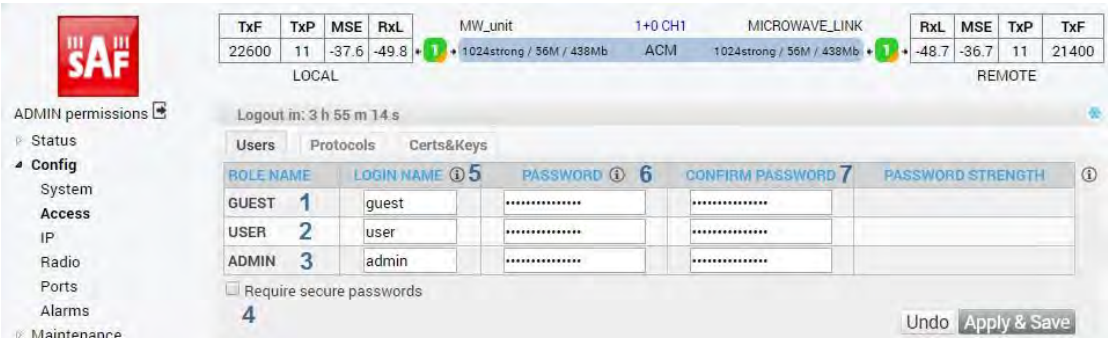


Figure 3.30 *"Config → Access → Users" page*

1) ***GUEST*** – user role with read-only access
2) ***USER*** – user role with standard management access
3) ***ADMIN*** – ser role with enhanced management access - enhanced settings, passwords, FW upgrade, etc.
4) ***Require secure passwords*** – if checked, only secure passwords will be accepted.

> **Secure password** is 8 or more characters long, contains lowercase, uppercase and numbers. More secure password consists of at least 13 characters and contains combination of lower/uppercase characters, numbers and symbols (! @ # % * ( ) _ - + = [ ] : ; ' , . ? /). Do not use other characters (^ & $ { } \ |)

5) ***LOGIN NAME*** – user name for selected level of the access The number of characters in the input field have to be in range from 4 to 12. Valid characters are [a-z, A-Z, 0-9, _]. it is not allowed to use user names which are already present in the system (for example – root, daemon, username present in other access level).
6) ***PASSWORD*** – password for selected level of the access. The number of characters in the input field have to be in range from 0 to 19. Password for ADMIN have to be in range from 1 to 19.
7) ***CONFIRM PASSWORD*** – has to be the same as *PASSWORD*.

Config → Access → Protocols

Management protocols and security configuration section.

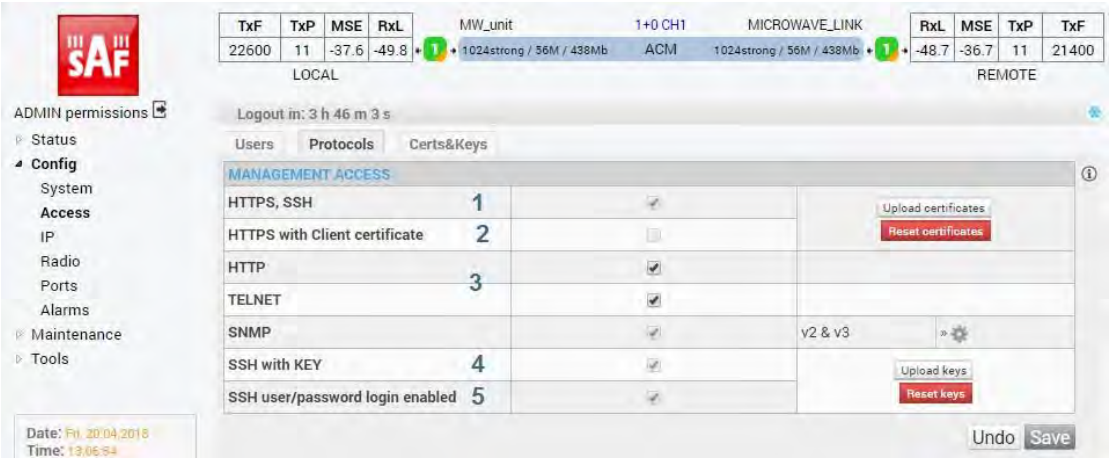


***Figure 3.31** "Config → Access → Protocols" page*

1) ***HTTPS, SSH*** – it is always enabled, cannot be turned off. By default, self-signed server certificate (SC) is used. This causes a browser security warning. To avoid this warning you can upload your own server certificate (SC) and upload the appropriate client certificate (CC) to the user browser.
2) ***HTTPS with Client Certificate*** – https access is possible only if the client (browser) has installed client certificate (CC). The option is available only if the device has uploaded the certification authority (CA) certificate signing CC. Reset of the CA certificate is possible only if this option is not checked.
3) ***HTTP, TELNET, SNMP*** – to increase the security of the device you can disable unencrypted access (http, telnet, SNMP v2) and turn on only encrypted SSH, HTTPS and SNMP v3 (SNMP can be set only on the Config/IP/SNMP page).
4) ***SSH with KEY*** – You can provide SSH keys in order to log in via SSH terminal without using a password.
5) ***SSH user/password login enabled*** – You can switch off SSH login using username/password. You have to be sure that login without password works. Reset of the SSH key is possible only if this option is enabled.

Config → Access → Certs&Keys

In this section is possible to import necessary certificates

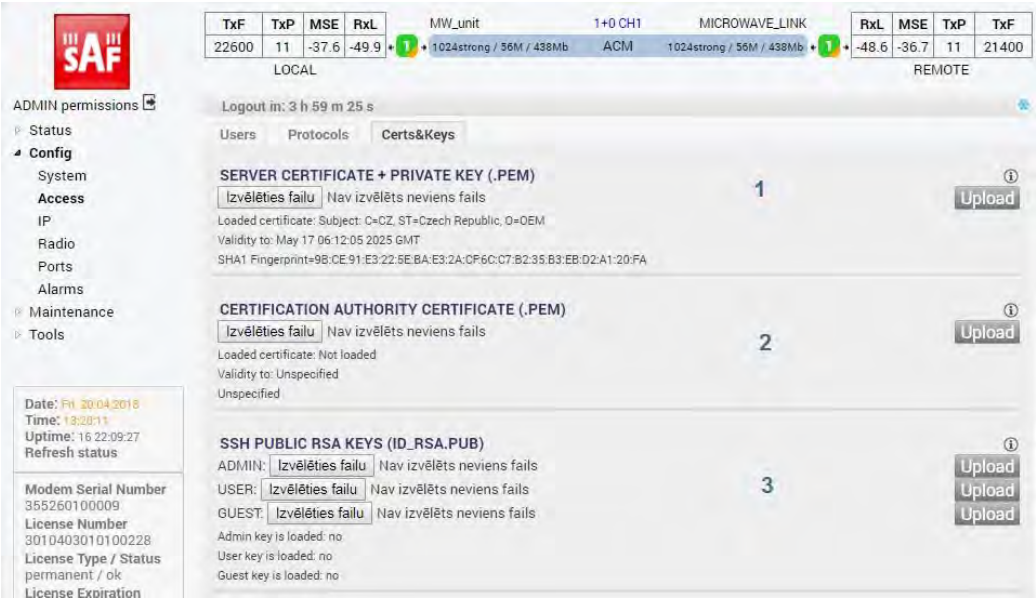


***Figure 3.32** "Config → Access → Certs&Keys" page*

1) ***Server Certificate + Private Key (.PEM)*** – a tool for HTTPS server certificate import. There is also shown basic information of actual HTTPS certificate. By default a self-signed certificate is loaded. It causes a browser security alert.
2) ***Certification Authority Certificate (.PEM)*** – it is possible to secure the access by means of a personal certificate loaded in the browser. In this sub-section it is possible to import a certificate of Certification Authority who signed personal certificate. There is also shown basic information about actual authority certificate.
3) ***SSH Public RSA Keys (ID_RSA.PUB)*** – it is possible to secure the SSH connection by means of importing customer's public SSH key. It is usually stored in home directory as "./ssh/id_rsa.pub". It is possible to load the key for each user role. Statuses are shown in this sub-section.

Important! The other file "id_rsa" (without extension) stored in the same directory is your PRIVATE key! It must not leave your home directory and/or computer!

Config → IP → Addresses

In this section IP addresses of the IDU can be configured.

***Figure 3.33** "Config → IP → Addresses" page*

1) ***Device IP / Mask*** – IP address assigned to port ETH0 (device local address) with the appropriate netmask specification. Netmask value is inserted in form of a decimal

number which corresponds to numbers in binary subnet mask presentation. For example, the 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.

2) ***Default Gateway IP*** – default Gateway IP address is used by CPU when connection outside of IP range defined in system routing table is required. Such IP address must be a member of the above defined Device IP subnet.

This sib-section also shows the REQUIRED and CONFIGURED IP settings. REQUIRED settings will be stored by the Save button. In order to activate the new settings use the IP Init button (you will be logged out, but user traffic will not be dropped) or Write the settings and reboot the device.

3) ***USB IP/Mask*** – it specifies IP address for USB0 management port. When default USB IP address is in collision with other network configuration it can be changed with this parameter. Factory default value is 10.10.11.10/24

4) ***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. Factory default value is 10.10.10.10/24

Note that configured Main IP and Gateway IP addresses are not in conflict with another internal IP addresses, especially with:

- used fallback IP address, either with default **10.10.10.10/24** or with optional **192.168.10.10/24**
- used USB IP address, either with default **10.10.11.10/24** or with optional **192.168.11.10/24**
- temporary remote1 IP address, either with default **192.168.253.243** or with optional **10.10.253.243**
- temporary remote2 IP address, either with default **192.168.253.244** or with optional **10.10.253.244**

Config → IP → SNMP

In this section SNMP settings can be configured

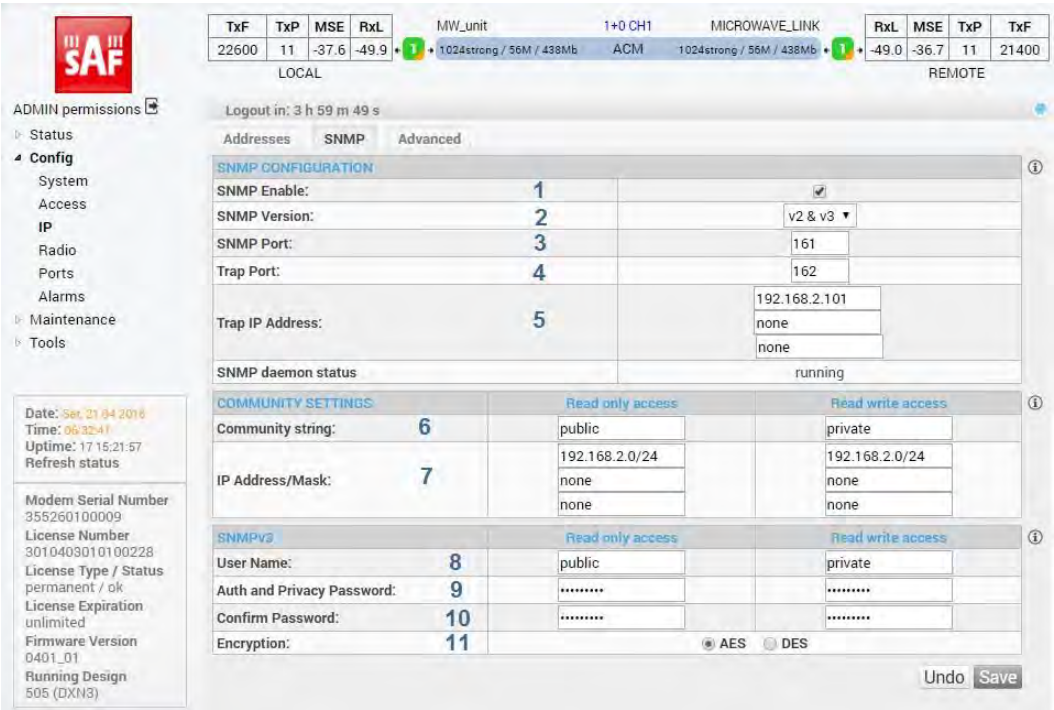


Figure 3.34 *"Config → IP → SNMP" page*

1) ***SNMP Enable*** – enables/disables the SNMP daemon in the device
2) ***SNMP Version*** – SNMP v2c & SNMP v3 or just SNMP v3 can be chosen for SNMP access to the device
3) ***SNMP Port*** – the parameter specifies which port will be used for SNMP communication. The same configuration must be set also in SNMP agent station
4) ***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
5) ***Trap IP Address*** – up to three IP addresses can be configured as the destination for SNMP trap distribution. Trap message events are configured in the same way as the alarm setting
6) ***Community string*** – the parameter specifies community string for secure SNMP v2c management access (a different setting for read-only and read/write access can be entered, valid for SNMP v2 only). The number of characters in the input field has to be in the range from 1 to 15. Valid characters are [a-z, A-Z, 0-9, _]
7) ***IP Address/Mask*** – up to three IP subnets can be configured as permitted IP source for SNMP v2c management access. Please note that the Mask parameter is mandatory.
8) ***User Name*** – username configuration for secure SNMP access with SNMP v3 protocol only (a different setting for read-only and read/write access can be entered). The number of characters in the input field has to be in the range from 4 to 15. Valid characters are [a-z, A-Z, 0-9, _]
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 (a different setting for read only and read/write access can be entered). The number of characters in the input field has to be in the range from 8 to 15. Valid characters are [a-z, A-Z, 0-9, _]
10) ***Confirm Password*** – Auth and Privacy password confirmation
11) ***Encryption*** – the encryption protocol for the SNMPv3: CFB-AES-128; CBC-DES

Config → IP → Advanced

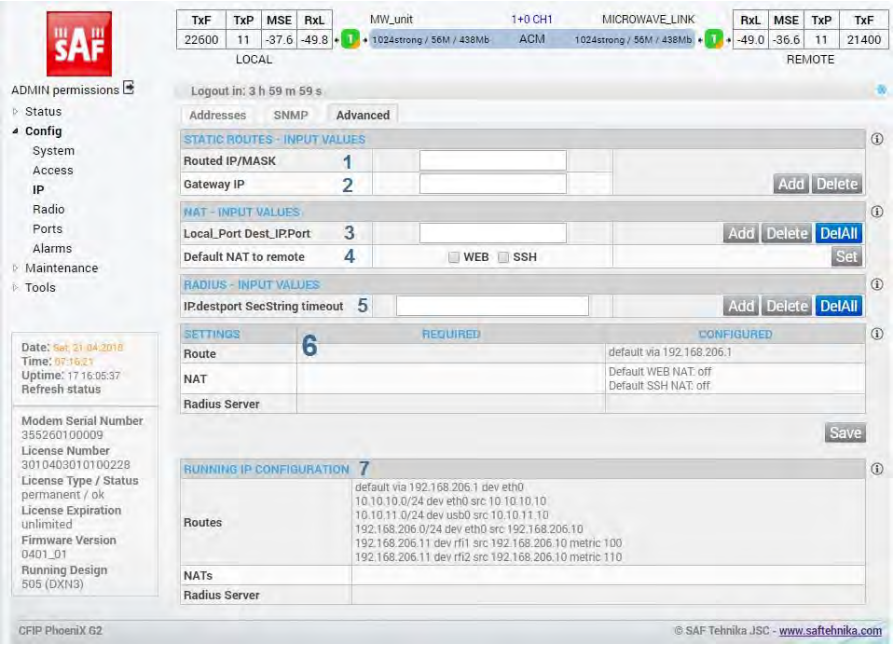


Figure 3.35 *"Config → IP → Advanced" page*

For a specific configuration of management access it might be necessary to add or delete static routes. It is possible to Delete an already specified route by specifying it in the ***Routed IP/MASK***. It is not necessary to specify the Gateway IP for route deletion.

When adding routes, the new configuration must be stored with Save button and re-initialised with the IP Init button.

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

For a specific configuration of management access, it might be necessary to add or delete NAT records. This is especially required for out-band type management access.

3) ***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)
4) ***Default NAT to remote*** –enable or disable the automatically generated NAT records for WEB and SSH management access. These records will work only when there is active connection between this device and the targetted device.
   a) ***WEB*** **-** This will add automatic NAT record for accessing the remote device's WEB GUI. The default values are as follows (the IP portion is only example and depends on actual running IP configuration):
      - 1443 192.168.3.91:443 - Remote device's GUI accessible on local port 1443 (e.g. https://localIP:1443)
      - 2443 192.168.3.92:443 - Second Remote (in Star mode) or direct Fiber Optics (FO) neighbour (in Full/Split Protection mode) device's GUI accessible on local port 2443
      - 3443 192.168.3.93:443 - Indirect Remote FO neighbour (ergo 'cross-corner' in Split Protection mode) device's GUI accessible on local port 3443
   b) **SSH -** This will add automatic NAT record for accessing the remote device's SSH . The default values follows (the IP portion is only example and depends on actual running IP configuration):
      - 1022 192.168.3.91:22 - Remote device's GUI accessible on local port 1022
      - 2022 192.168.3.92:22 - Second Remote (in Star mode) or direct FO neighbour (in Split Protection mode) device's GUI accessible on local port 2022
      - 3022 192.168.3.93:22 - Indirect Remote FO neighbour (ergo 'cross-corner' in Split Protection mode) device's GUI accessible on local port 3022

Radius access configuration:

5) ***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
6) This sub-section displays the REQUIRED and CONFIGURED Route/NAT/Radius settings. REQUIRED settings will be stored by means of the Save button. In order to

activate the new setting use the Save and IP Init button (user will be logged out, but data will not be dropped) or Save the IP settings and reboot the device.

7) This sub-section diaplays the IDU's active IP Route table, NAT records and Radius Server configuration. In order to populate this table with a new configuration, the IP configuration should be re-initialised by means of IP Init button.

Config → Radio→ Parameters

This section contains the most important modem and radio settings. 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 any changed settings have to be stored separately in both local and remote side.

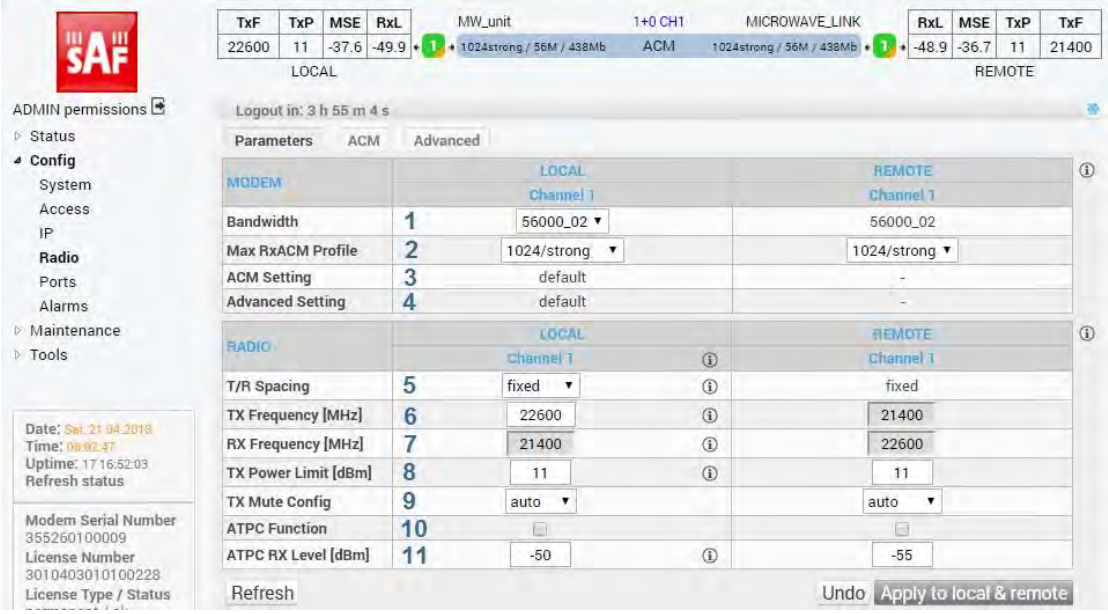


***Figure 3.36** "Config → Radio → Parameters" page*

1) ***Bandwidth*** – the bandwidth of the transmitting modulation. The number after the underscore indicates the modulation variant.
2) ***Max RxACM Profile*** – This is the highest modulation available for the ACM switching or a fixed modulation when the ACM is not enabled. Each modulation can have multiple Forward Error Correction variants:
   - medium – optimal FEC, medium throughput speed
   - strong – strong FEC, lowest throughput speed
3) ***ACM Setting*** – Gear icon indicates that the ACM settings does not match the factory defaults and leads the user to the ACM settings page. If the ACM is set to defaults such information will be displayed instead.
4) ***Advanced Setting*** – Gear icon indicates that the Advanced radio settings does not match the factory defaults and leads the user to the Advanced radio settings page. If the Advanced radio settings is set to defaults such information will be displayed instead.
5) ***T/R Spacing*** – TX / RX frequency distance mode. Note that available options depends on the attached radio type and it's capabilities.
6) ***TX Frequency*** – Transmission frequency can be set within the frequency range noted under the respective info icon in accordance with radio sub-band specification (read

from the radio part). Such displayed range is the edge to edge flat diplexer frequency scope increased/decreased by one half of the used modulation bandwidth.

7) ***RX Frequency*** – If *fixed* T/R spacing is selected the Receive frequency will be calculated automatically. If *manual* T/R spacing is selected the Receive frequency has to be calculated and specified manually.

8) ***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 (if ATPC is enabled)
   - radio part power limit (depends on the used RF band and selected modulation)

9) ***TX Mute Config*** – Transmitter mute configuration. Three modes of this parameter can be selected:
   - ***auto*** mute mode is the standard selection for this parameter. In this mode the radio part automatically is muted when required by design or when abnormal transmission conditions are detected by the device.
   - ***mute*** mode for fixed radio mute configuration
   - ***unmute*** option is available only on remote channels when there is not Rx connection from such remote channel. When selected the unmute command is send to the remote side which, if listening, will attempt to unmute it's respective Tx part.

10) ***ATPC Function*** – Automatic Transmit Power Control enables or disables the ATPC feature. The transmitted power is automatically adjusted to ensure that the remote side will receive signal of strength defined in its respective *ATPC RxL Level* settings with hysteresis of +/- 2dBm (hitless regulation).

11) ***ATPC RX Level*** – Required level for Automatic Transmit Power Control. This field specifies the optimal receive level used for the ATPC function. The remote unit will adjust it's Tx power in manner to match this required level as close as possible.

Config → Radio → ACM

Adaptive Coding anad modulation (ACM) settings

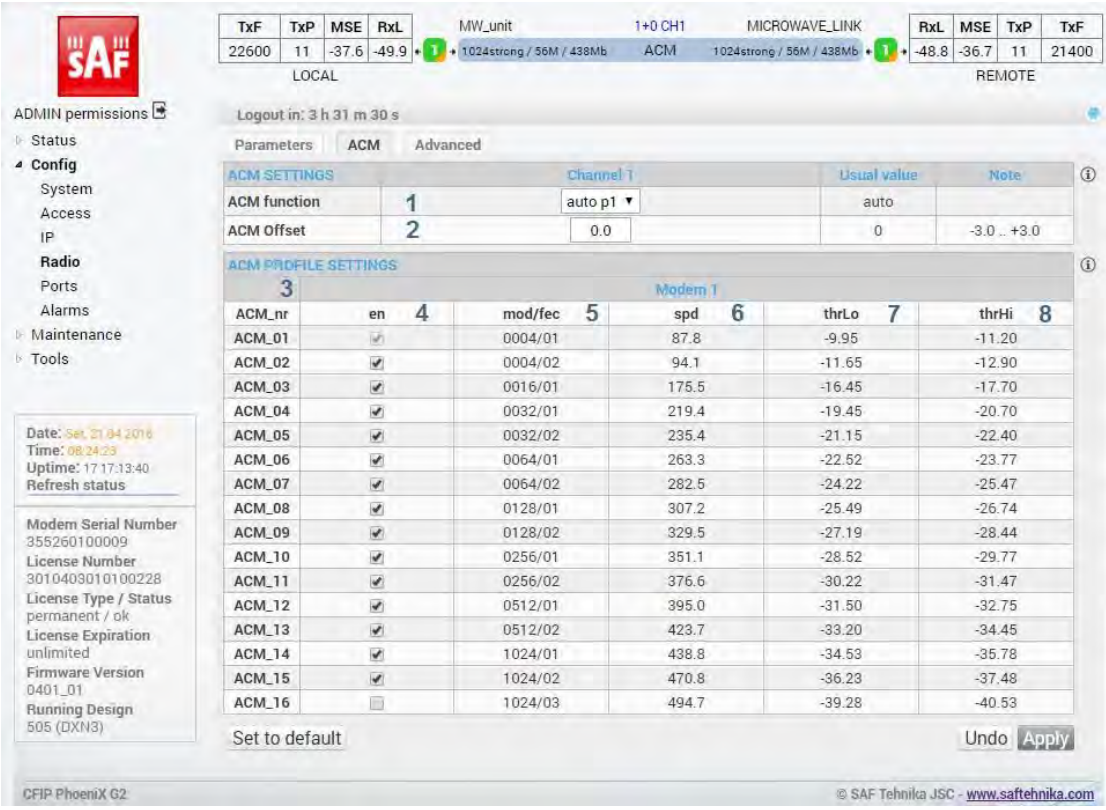


***Figure 3.37** "Config → Radio → ACM" page*

1) ***ACM Function*** – Adaptive Coding and Modulation. The possible modes are following:
   - **auto pX** – automatic modulation switching using ACM profile number X
   - **man pX** – disables the ACM function. The modulation defined in the *Max RxACM Profile* field on the *Parameters* tab will be used for transmission.
2) ***ACM Offset*** – The MSE offset off the pre-set thrLo and thrHi constants (see ACM profiles)
3) ***ACM_nr*** – designation of the modulation
4) ***en*** – enables a modulation for ACM switching
   - "l" means unlicenced modulation
   - "e" means error setting
5) ***mod/fec*** – bandwidth/forward error correction level
6) ***spd*** – maximal throughput
7) ***thrLo*** – the MSE threshold value for switching from this respective modulation to a lower Rx modulation
8) ***thrHi*** – the MSE threshold value for switching to this respective modulation

The ACM settings of local and remote devices should match.

It is recommended not to use ACM when 1+1 SD or 1+1 HSB/SD modes are used with separated antennas in each side of the link. In some circumstances the ACM in combination with 1+1 SD mode might not work properly. For more details please refer to SAF technical support at techsupport@saftehnika.com

Config → Radio → Advanced

This section provides several options for advanced radio part and modem settings

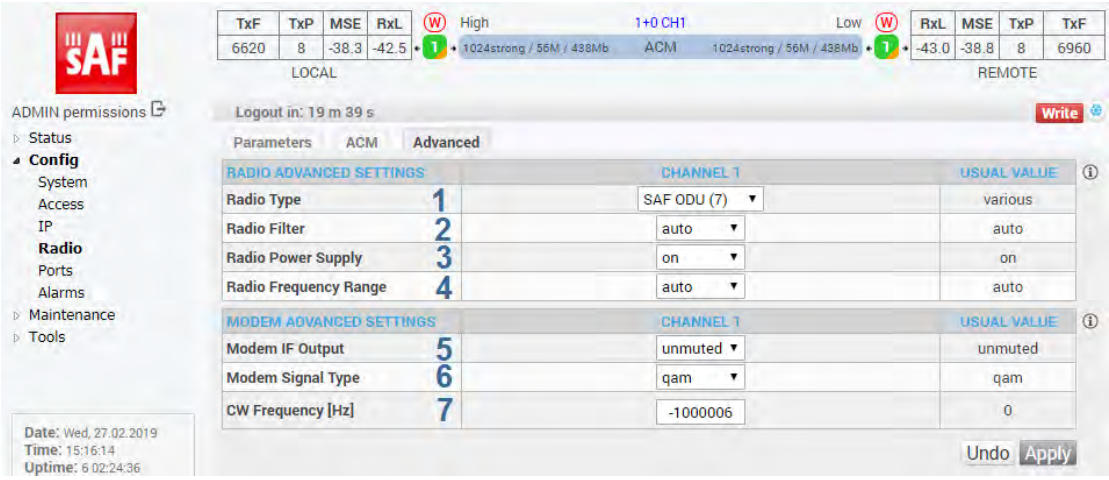


***Figure 3.38** "Config → Radio → Advanced" page*

1) ***Radio Type*** – selection of the connected radio type. This setting is available only on supported systems
2) ***Radio Filter*** options are following:
   - **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
3) ***Radio Power Supply*** options are following:
   - **on** – enables power output to the respective radio part
   - **off** – disables power output to the respective radio part
4) ***Radio Frequency Range*** options are following:
   - **auto** – the unit automatically calculates the usable frequency range by subtracting/adding half of the current bandwidth from the radio frequency edges
   - **hw**– the radio frequency limits are used. This is suitable only for special use cases
5) ***Modem IF Output*** options are following:
   - **unmuted** – modem IF Tx is transmitting
   - **muted** – modem IF Tx is muted
6) ***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 are following:
   - **qam** – TxIF modulated signal is presented at IF output from the device (default)
   - **cw** – Carrier signal with given frequency is presented at IF output
7) ***CW Frequency*** – carrier signal frequency settings

Config → Ports → MUX

In respect of management access type, traffic modification (number of independent channels over air) and the aggregation function preference the user has to select the relevant Mode type (Refer to Config → System → 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 Ethernet loops at connected LAN ports for all Modes. The port settings consist of several configuration layers labelled leftmost of the configuration window

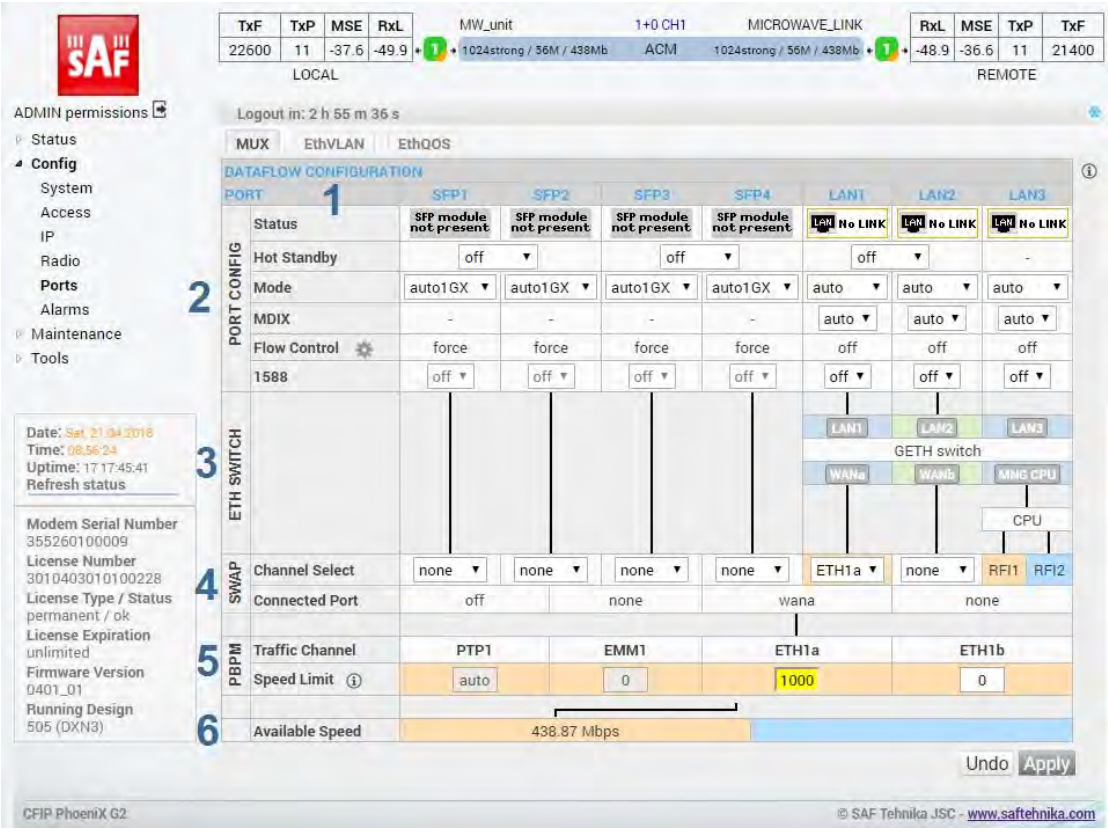


***Figure 3.39** "Config → Ports → MUX" page*

1) ***PORT*** sub-section contains information about available ports:
   a) ***SFP1-4*** – 1G optical interface for user data or EMM card chain
   b) ***LAN1-2*** – Ethernet 1G (data) interface
   c) ***LAN3*** – Ethernet 1G (management) interface
2) ***PORT CONFIG:***
   a) ***Status*** – status of the port as detected by the device (speed, duplex mode, link, administrative down status).
   b) ***Hot standby*** – automatic switch over between ports according to actual link status
   c) ***Mode*** – displays and defines the actual port mode (speed/duplex, administrative down)
   d) ***MDIX*** – set particular ETH cable crossing option like auto/mdi/mdx
   e) ***Flow Control*** – displays the actual duplex flow control mechanism settings. Flow control configuration is possible in page Config → Ports → EthQOS
   f) ***1588*** – Precision time protocol source
3) ***ETH SWITCH*** illustrates the ETH switch fragmentation into groups and also their interconnection with physical LAN ports and internal WAN ports. The group configuration is available on page Config → Ports → EthVLAN
4) ***SWAP:***
   a) ***Channel Select*** – settings of data multiplexer. By this settings it is possible to cross connect a particular Switch port with a Mux Channel.
   b) ***Connected Port*** – current settings of the SWAP block
5) ***PBPM*** (Priority Based Packet Multiplexer)***:***
   a) ***Traffic Channel*** – shows bonding between the selected channel and port
      - **PTPx** – Precision time protocol channel
      - **EMMx** – EMM channel. Speed will be computed automatically

- **ETHxa** – high priority data channel. Speed can be limited - see field color and bubble help

> Firmware version 0401_01 does not allow to assign ETHxa data channel to any of SFP ports if PTP1588 feature is not licensed. It will not pass Ethernet traffic over SFP ports in this case.

- **ETHxb** – low priority data channel. Speed can be limited - see field color and bubble help

b) ***Speed Limit*** – speed value for transmitting data with priority falling from left to right

c) ***Act Aggr Speed*** – it indicates the actual aggregated capacity in 2+0 mode. It depends on channels statuses and asymmetry. Actual aggregated capacity may be less than sum of available channels capacities.

6) ***Available Speed*** indicates the available capacity of appropriate channel. This value depends on the actual modulation scheme and license speed limits.

Config → Ports → EthVLAN

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 these settings in some specific applications.

Figure 3.40 *"Config → Ports → EthVLAN" page*

1) ***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 (802.1Q disabled at the port) and edit VTU (VLAN rules table: **V**LAN **T**ugged/**U**ntagged) 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:

a) **basic** – 802.1Q VLAN mode is disabled. Only port group rules are applied. It is a transparent mode where VLAN settings in VTU table are ignored.
Ingress policy – both untagged or tagged frames are accepted at port entry and exit only those ports of ETH switch which are members of the same group as the input port. The port default VLAN number is assigned as frame VID (VLAN ID) for next internal switch processing

Egress policy – frames are transmitted unchanged

b) **access** – 802.1Q VLAN mode is enabled. VTU rules in conjunction with port group rules are applied. Such port is a member of just one VLAN ID defined in VTU table whose VID is identical with the port Default VLAN number. This port is configured in VLAN VTU record as untagged.
Ingress policy – only untagged frames are accepted at entry port. Internal frame VID of such untagged frame is automatically assigned from port's Default VLAN. Frames are allowed to exit only those ports that belong to the frame's VLAN and are inside the same group as the input port.
Egress policy – frames are transmitted untagged from this port. The egressing frame's VID is checked against VTU table and if VID doesn't exist in VTU table such frame is filtered (discarded).

c) **trunk** – 802.1Q VLAN mode is enabled. VTU rules in conjunction with port group rules are applied. Port can be a member of more tagged VLANs according to VID extracted from VLAN tag and one untagged VLAN defined by port Default VLAN.
Ingress policy – only such frames are accepted, whose VID assigned from VLAN tag (tagged frames) or port's Default VLAN (untagged frames) exist in VTU table, and the entry port is a member of such VLAN. Frames are allowed to exit only those ports that belong to the frame's VLAN and are inside the same group as the input port.
Egress policy – frames are transmitted untagged or tagged according to the specification in VTU record table. The egressing frame's VID is checked against VTU table and if VID doesn't exist in VTU table such frame is filtered (discarded).

d) **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.

2) ***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 each other. The other group 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.

3) ***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.

When a new VLAN configuration is applied, it is required to press the Write button to confirm the new configuration. Otherwise, previous VLAN configuration will be restored after 120 seconds.

4) ***ACTION*** – it adds or removes VTU records. A VTU record can not be removed if it contains an untagged port which is configured into access mode. Just simple VLAN Nr. specification is required for VTU record eraseing.

5) ***VLAN N.*** – The VLAN number of edited VLAN (added or removed). Please note the VLAN No. 0 & 1 are reserved by the system and can not be set; thus the valid VLAN No. are from 2 to 4095

6) ***FID*** – defines the MAC address database table for each VTU VLAN record. When more than one VLAN is added into the same FID table then such VLANs will share the same MAC address database; thus they will not be completely isolated. Usually, it is desired that each VLAN has its unique FID. Note that the port Groups 1-4 are assigned to the MAC address databases FIDs 1-4, and thus these FIDs should not be used for VTU VLAN separation (especially for VTU VLANs 2-4) unless the MAC table sharing between such defined VLAN and a particular port Group is the desired state.

7) ***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).
8) ***LAN 1-WAN B*** – it defines VLAN mode for each port in configured VLAN.
   a) **Deny** – port is not a member of edited VLAN. Ports which are defined in different groups should be set into this mode.
   b) **Untag** – port is a member of edited VLAN as untagged.
   c) **Tag** – port is a member of edited VLAN as tagged.

> "Tag" option is not supported for LAN3 port as this port is reserved for local management access. LAN3 port can be set in "Deny" or "Untag" modes depending on customer's VLAN configuration scenario

9) ***Listing of actual VTU values*** – the 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.

Config → Ports → EthQOS

This section allows configuring Flow Control and 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.

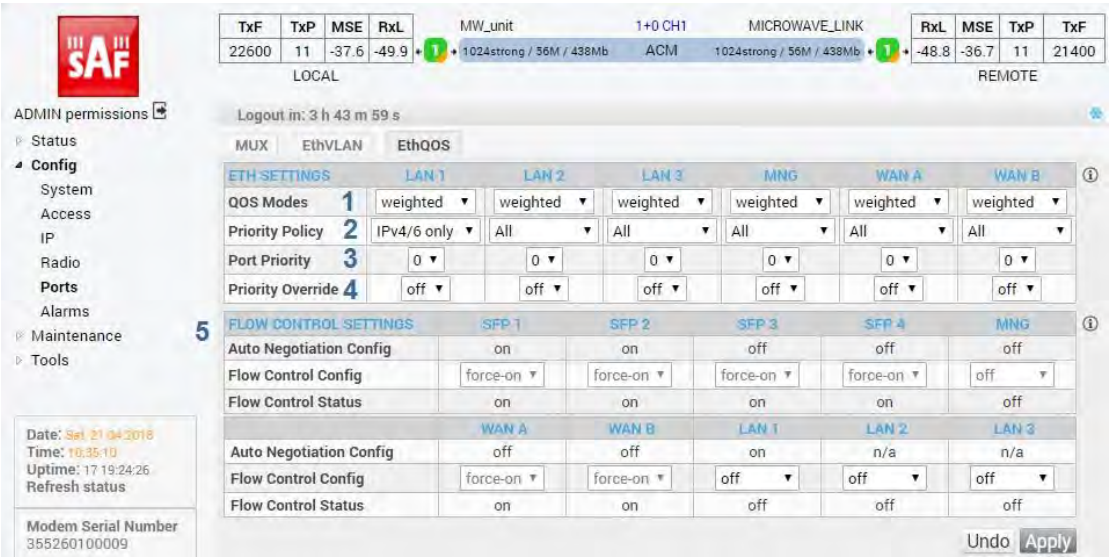


Figure 3.41 *"Config → Ports → EthQOS" page*

1) ***QOS Modes:***
   a) **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 served out with only a slight delay to the higher priority frames.

b) **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.

c) **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.

d) **strict 3210** – strict priority for all queues. Lower priority queues are served only when higher priority queues are empty.

2) ***Priority policy*** – defines the initial ingress queue policy. It defines the initial rules for what output queue will be assigned to every ingress frame.

3) ***Port Priority*** – the configuration of default port priority. Value 0 up to 7 can be entered (0 is default value)

4) ***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.

a) **off** – QOS override is disabled

b) **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.

5) ***Flow Controll settings*** allows to configure Flow control for each port:

a) ***off*** – Flow control is disabled

b) ***auto*** – Flow control is enabled during auto-negotiation process

c) ***force-on*** – Flow control is active, even if connected device does not support it

Config → Ports → EMM

This section will appear only if the EMM module is successfully connected to any of SFP ports of the Phoenix G2 IDU and in Config → Ports → MUX section **EMM1** or **EMM2** option is chosen in ***Channel Select*** cell for particular SFP port where the EMM module is connected:

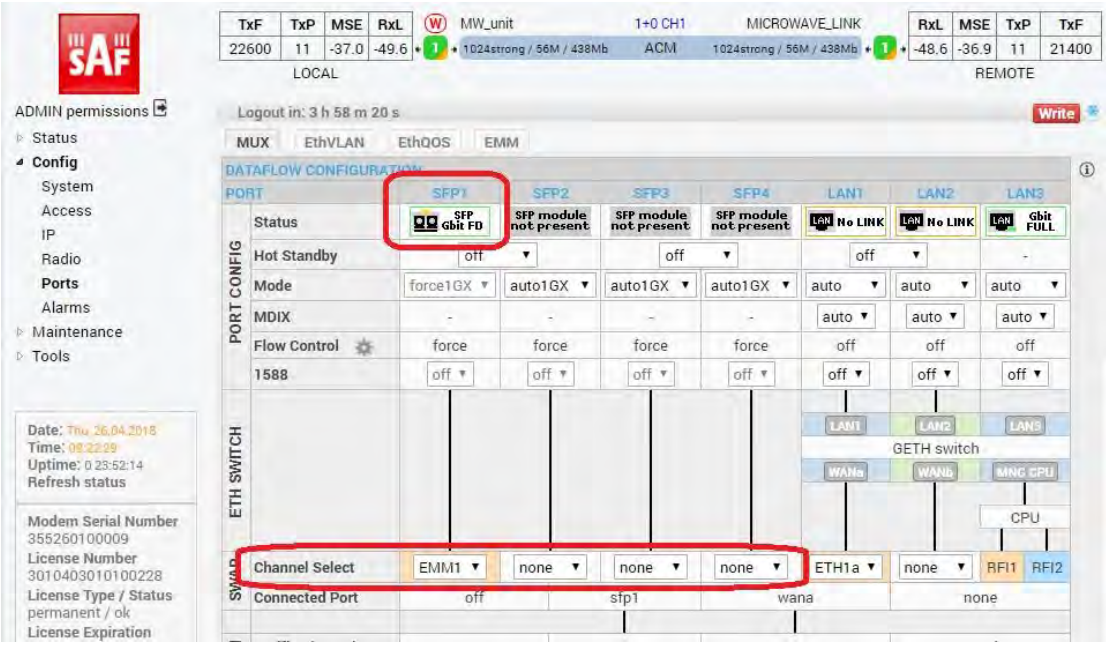


Figure 3.42 *Enabling of EMM module*

'Config → Ports → EMM' section provides monitoring and configuration of EMM modules basic functions. Following information will be displayed for ASI EMM module:

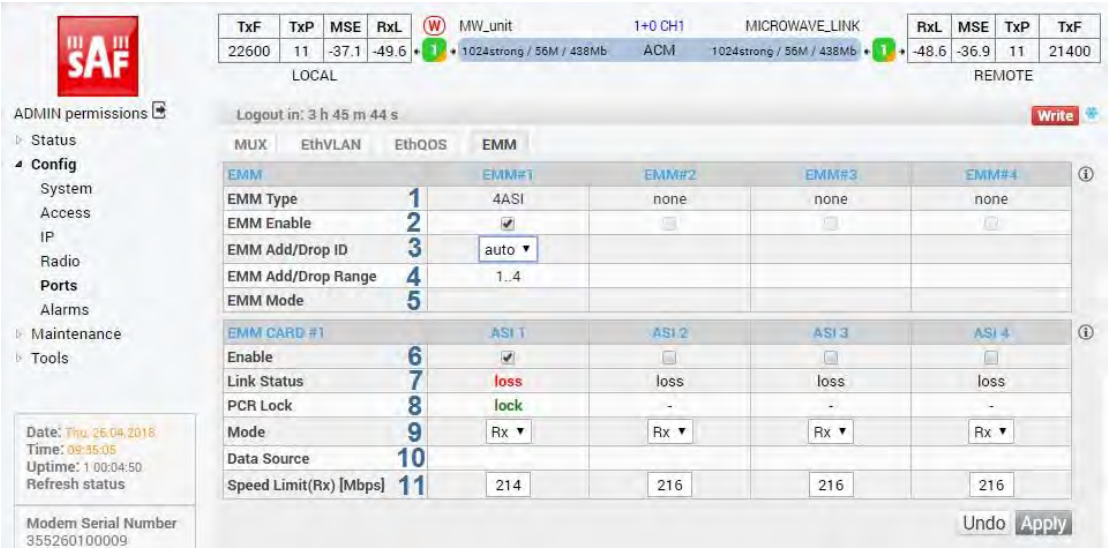


Figure 3.43 *"Config → Ports → EMM" ASI EMM configuration page*

1) ***EMM Type*** – displays the type of connected EMM card. The 'none' type indicates that particular position is empty, the 'RELAY-SYS' indicates that the relay IDU is connected directly to the device's SFP port (relay application) or to EMM secondary SFP port (add/drop configuration).
2) ***EMM Enable*** – enables generation/reception of data frames to/from Fiber Optic stream. When EMM is enabled then EMM occupies an appropriate range of traffic port channels (described below).
3) ***EMM Add/Drop ID*** – in 'auto' mode EMM card occupies port-channel range according to its position in EMM chain. For Add/Drop application it is sometimes necessary to set different (manual) Add/Drop ID, especially when EMM card should drop port channels from specific Add/Drop range.
4) ***EMM Add/Drop Range*** – displays appropriate port-channel range according to the EMM card position and EMM Add/Drop ID setting.
5) ***EMM Mode*** – it selects the mode of connected EMM 16E1/T1 card
6) ***Enable*** – this checkbox selects which ASI ports are configured for DVB ASI connection. The necessary link capacity is automatically allocated according to the amount of all ASI Rx streams.
7) ***Link Status*** – it displays the actual status of ASI port. Status depends on chosen Rx or Tx mode:
    a) In **Rx mode:**
        - **ok** - a valid ASI signal is presented at the appropriate input port
        - **ok** - a valid ASI signal is presented at the appropriate input port, but the port is not enabled for traffic application.
        - **Idle** - ASI signal detected and successfully synchronized, but the signal does not contain user data (MPEG stream is missing).
        - **Idle** - ASI signal detected and successfully synchronized but the signal does not contain user data (MPEG stream is missing) and the particular port is not enabled for traffic application.
        - **nosync** - indicates that synchronization is not established for current receiving ASI signal.
        - **nosync** - indicates that synchronization is not established for current receiving ASI signal and the port is not enabled for traffic application.
        - **loss** - no signal detected at ASI input port.
        - **loss** - no signal detected at ASI input port and the port is not enabled for traffic application.

b) In **Tx mode:**
- **ok** - a valid inbound signal is presented and transmitted via appropriate ASI port.
- **ok** - a valid inbound signal is presented, but the port is not enabled for transmission.
- **Idle** - the low-level code is detected, but the MPEG code was lost in the service.
- **Idle** - the low-level code is detected, but the MPEG code was lost in the service, and the particular port is not enabled for traffic application.
- **noSync** - high-level MPEG code was not detected.
- **noSync** - high-level MPEG code was not detected, and the particular port is not enabled for traffic application.

8) ***PCR Lock*** – in **Rx mode** it is always 'lock', but in Tx mode following options are available:
- **lock** – PCR recovery loop is locked
- **noLock** – PCR interval is not guaranteed

9) ***Mode*** – specifies if the particular port operates in Rx (ingress from coaxial cable) or Tx (egress to coaxial cable) mode.

10) ***Data Source*** – specifies the source for Tx signal. Either remote ASI port (Remote CH1-4) or one of available local ASI Rx port (Local Ch1-4) can be chosen. This setting is available in **Tx mode** only.

11) ***Speed Limit*** – maximal data rate for inbound traffic to avoid overloading of overall link capacity. This setting is available in **Rx mode** only.

Following information will be displayed for E1/T1 EMM module:

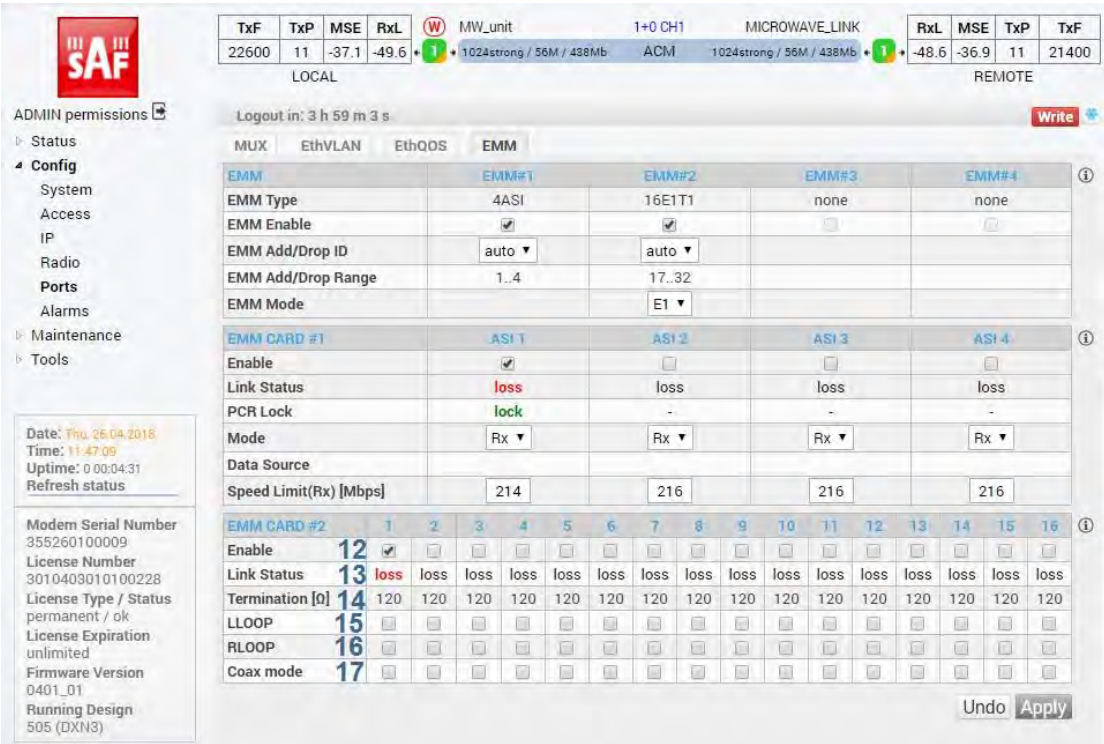


Figure 3.44 *"Config → Ports → EMM" E1/T1 EMM configuration page*

12) ***Enable*** – select which E1/T1 ports are configured for customer traffic connection. Those ports require appropriate capacity allocation from IDU, even though customer traffic is not carried (e.g. cable is disconnected).

13) ***Link Status*** – it displays the actual status of E1/T1 port or appropriate internal traffic channel.

14) ***Termination*** – displays the actual impedance matching of E1/T1 port according to Coax mode setting.
15) ***LLOOP*** – local loopback configuration, incoming data from the E1/T1 port to modem are sent to the modem and simultaneously looped back to the E1/t1 port. This is a debugging function.
16) ***RLOOP*** – remote loopback configuration, incoming data from the modem to E1/T1 port are sent to this port and simultaneously looped back to the modem. This is a debugging function.
17) ***Coax Mode*** –changes the E1/T1 mode from standard 120Ω balanced to 75Ω unbalanced.

In case of ***Design 511*** and **Split 1+1** or **Split 2+2** modes are used, additional EMM protection settings will appear in EMM configuration section:

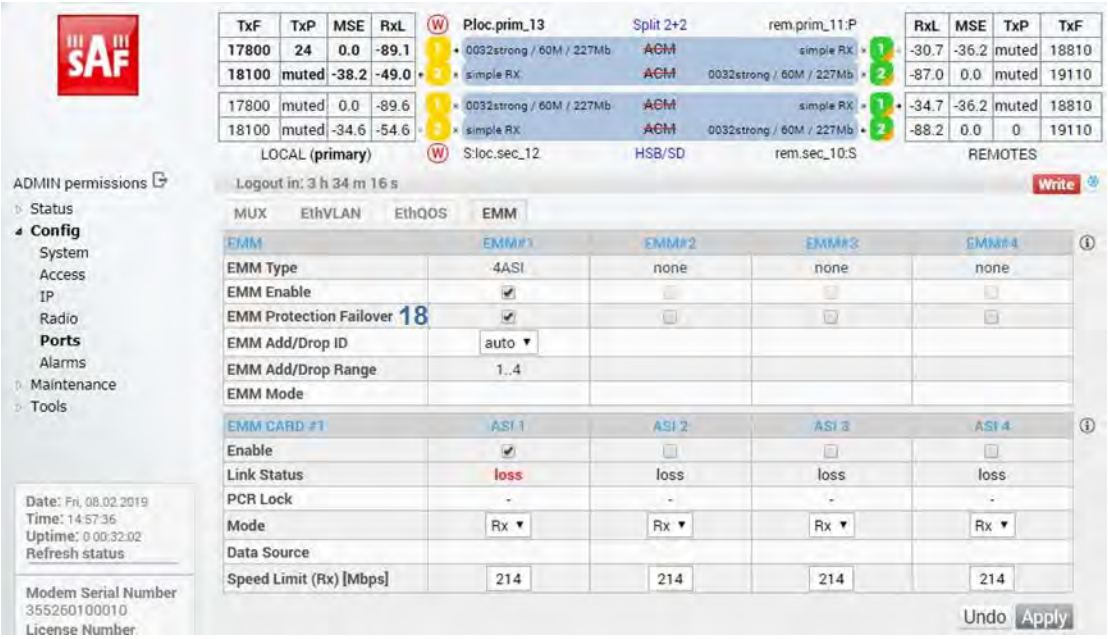


Figure 3.45 *"Config → Ports → EMM" ASI configuration in Split 1+1 and in Split 2+2 modes*

18) ***EMM Protection Failover*** – if this option is enabled, transmitters of secondary EMM modules are muted, and receivers are in Hi-Z(E1) or usual(ASI) impedance - simple passive external splitter is needed in this case for EMM traffic protection

Config → Alarms → Major

This section contains possible events/alarms with direct impact on the link operability.

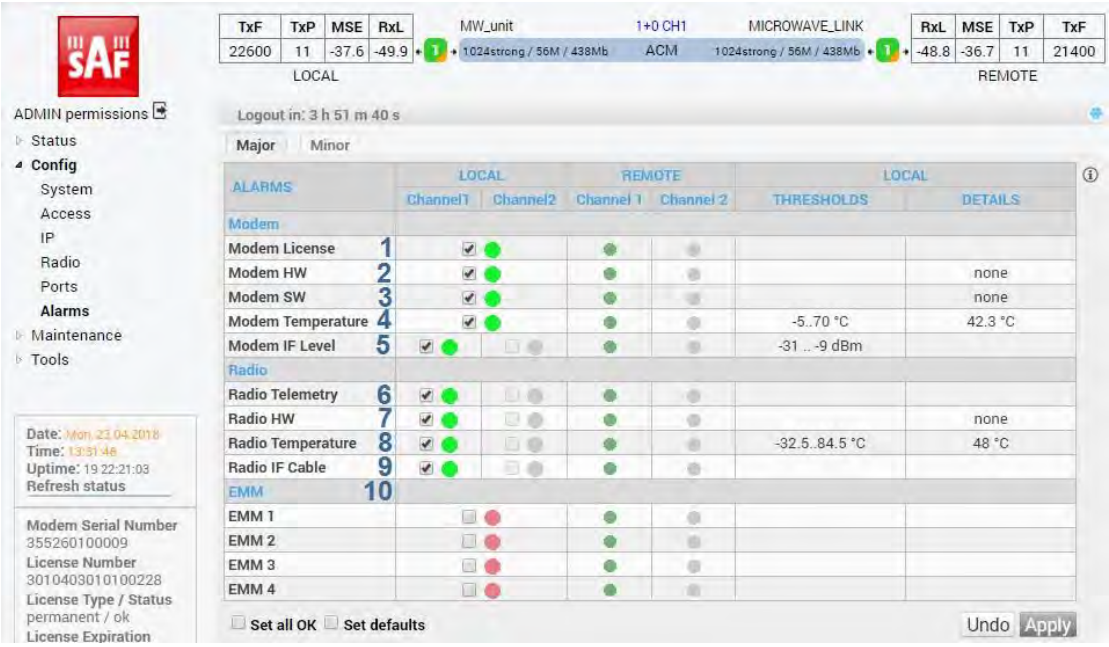


Figure 3.46 *"Config → Alarms → Major" page*

1) ***Modem License*** – this alarm will be raised when the license file is about to expire or is expired already, or contains an invalid data
2) ***Modem HW*** – a hardware problem
3) ***Modem SW*** – a software problem (for example incompatible mode selection on local and remote side)
4) ***Modem Temperature*** – the temperature of the modem part
5) ***Modem IF Level*** – this alarm indicates low or high level of modem input (140 MHz)
6) ***Radio Telemetry*** – the status of communication with the radio part
7) ***Radio HW*** – the status as reported by the radio part
8) ***Radio Temperature*** – the temperature of the radio part
9) ***Radio IF Cable*** – this alarm indicates bad radio IF input (350 MHz)
10) ***EMM 1-4*** – the status of bidirectional FO communication with respective EMM module

In case if ***Design 511*** **Split 1+1** or **Split 2+2** mode is enabled, the additional Pri/Sec switch co.lumn will appear:

Figure 3.47 *"Config → Alarms → Major" page using Split 1+1 and Split 2+2 modes*

11) ***Pri/Sec switch*** – For correct protection role switching in 1+1 mode the user have to appropriately configure the **Pri/Sec switch** alarms marked as "yes". Only the alarms which are enabled and listed as **Pri/Sec switch** will be used as criteria for protection switching. This same refers to Minor alarms in Config → Alarms → Minor section

Config → Alarms → Minor

This section contains possible events/alarms with partial immediate impact on the link operability.

For correct protection role switching in 1+1 mode the user have to appropriately configure all the **Pri/Sec switch** alarms. Only the alarms which are enabled and listed as **Pri/Sec switch** will be used as criteria for protection switching.

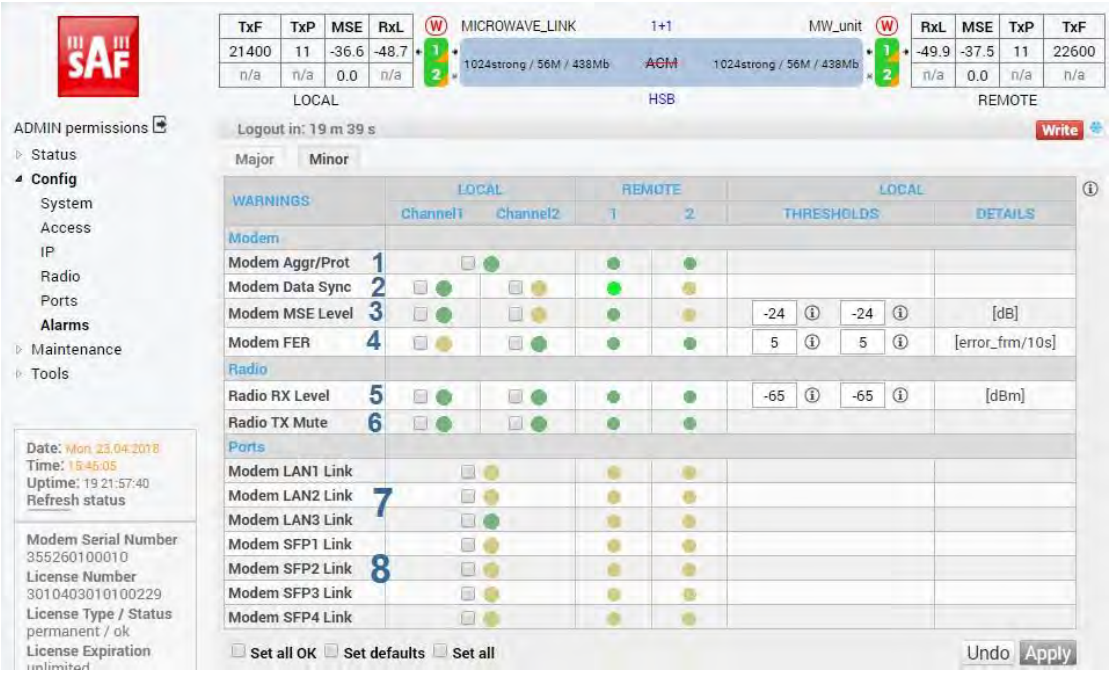


***Figure 3.48** "Config → Alarms → Minor" page*

1) ***Modem Aggr/Prot*** – status of the Aggregation/Protection (displayed only if 1+1 or 2+0 modes enabled)
2) ***Modem Data Sync*** – this alarm indicates actual status of the packet processor (PBPS) synchronization.
3) ***Modem MSE Level*** – the alarm indicated if MSE threshold is trespassed. Usual MSE values can be checked in the ACM profile table under menu Config → Radio → ACM.
4) ***Modem FER*** – the threshold for error frames per 10s
5) ***Radio RX Level*** – the receiving level threshold
6) ***Radio TX Mute*** – transmitting Mute status
7) ***Modem LAN1/2/3 Link*** – status of the LAN port Link
8) ***Modem SFP1/2/3/4 Link*** – status of the SFP port Link

Maintenance

Maintenance → Configuration → Save&Run

This section allows to store, display, export and execute the start-up configuration and IP settings.

***Figure 3.49** "Maintenance → Configuration → Save&Run" page*

Write - store the actual configuration.

Show c0 - displays the device's stored start-up configuration as list of commands. Note that the order of commands in this list is important. This configuration is not automatically updated unless this button is pressed again.

Run c0 - this will execute the current start-up memory content. Note that this action will cause data loss and the loss of all unsaved configuration changes.

Show IP - shows the device IP configuration as list of commands. Note that this configuration is not automatically updated unless this button is pressed again.

IP Init - it will execute the current start-up memory IP settings content as well as re-initialization of IP interfaces. Note that this action will not cause user data loss but it will disconnect all active management sessions.

Maintenance → Configuration → Backup&Restore

This section allows to BACKUP the start-up configuration into the internal restart persistent memory. Only stored configuration will be backed up. Only one backup is allowed.

This backup is not automatically updated after firmware upgrade and thus it should be re-generated by the user manually.

The RESTORE button will appear if there is a configuration file stored. This file can be downloaded from this section directly.

- After pressing the RESTORE button the start-up configuration will be immediately replaced by the restored configuration.
- The restored configuration is not automatically activated. The Run c0 button should be applied or soft reboot performed in order to activate it.
- The RESTORE should be performed on the same FW version as it was created

In this section it is possible to select and upload previously saved configuration file (*.afw) from external location.

- After pressing the Upload and execute button the start-up configuration will be immediately replaced by the restored configuration.
- The restored configuration is not automatically activated. The Run c0 button should be applied or soft reboot performed in order to activate it.
- The RESTORE should be performed on the same FW version as it was created

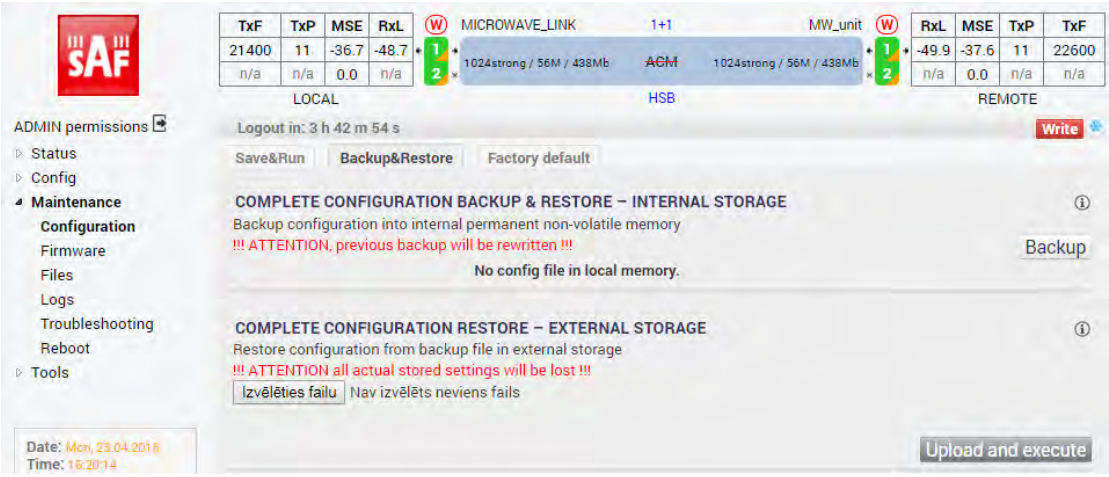


***Figure 3.50** "Maintenance → Configuration → Backup&Restore" page*

Maintenance → Configuration → Factory default

In this section it is possible to restore the configuration of the device to its factory pre-set values including login credentials, radio and IP settings.

The IDU will be rebooted automatically after loading factory configuration.

***Figure 3.51** "Maintenance → Configuration → Factory default" page*

In case of lost password or any other issues to access Phoenix G2 IDU web GUI via LAN MNG and /or USB MNG port, contact SAF technical support team at techsupport@saftehnika.com.

Maintenance → Firmware → Upgrade

To update the firmware, follow the upgrade wizard in this section. It will guide through the whole firmware upgrade process. If an EMM chain is used, update the EMM chain as well in the same web GUI page.

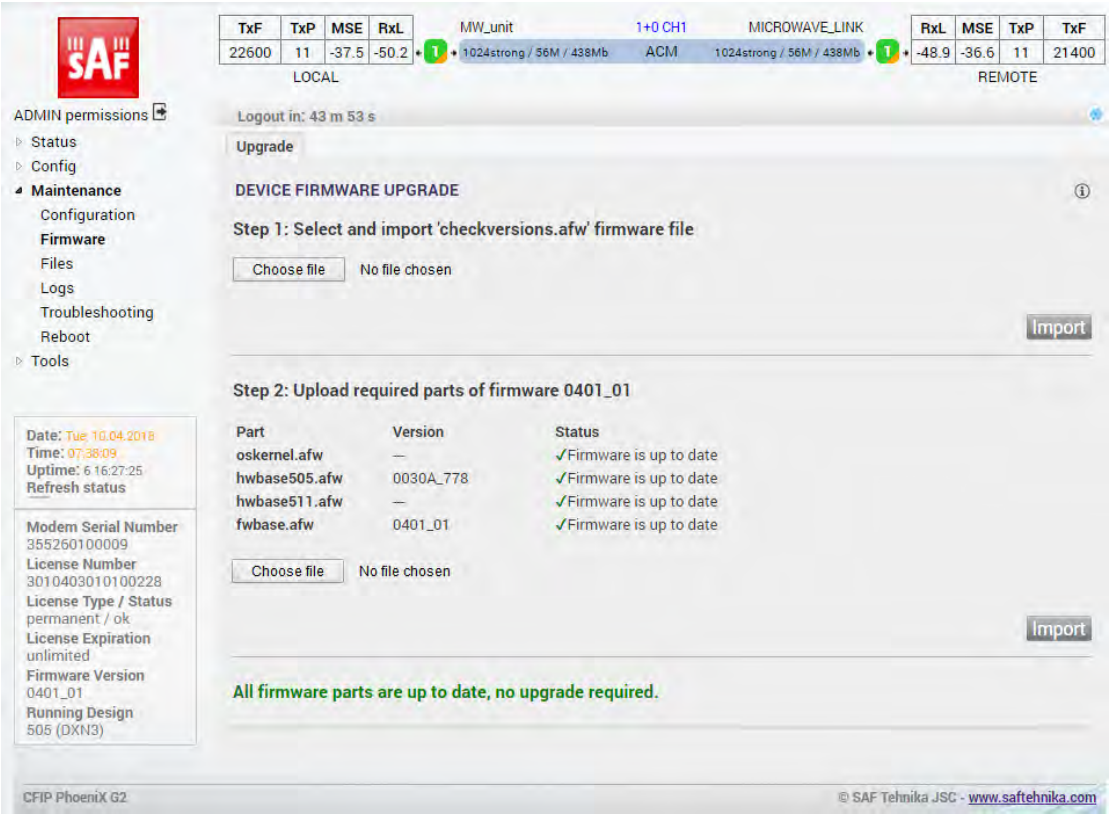


***Figure 3.52** "Maintenance → Firmware → Upgrade" page*

Basically the firmware upgrade can be done in 3 steps:

- **Step 1** - import the "checkversion.afw" file. This will display the frame with information about the firmware parts which are needed for the upgrade.
- **Step 2** - import all required firmware parts. Once completed the firmware upgrade frame will be displayed.
- **Step 3** – in firmware upgrade frame initiate the upgrade by pressing UPGRADE MODEM or UPGRADE MODEM & EMM button. Firmware upgrade initialized in this step will cause data drop - approximately one minute for the modem part plus about 30 seconds per each attached EMM card.

UPGRADE MODEM & EMM button will simultaneously update modem and all attached outdated EMM cards.

UPGRADE MODEM button will update modem only. This button will be displayed if no EMM cards are present or if such cards do not require an update.

Release Notes document is always released with a new firmware describing all changes in comparison to previous releases.

The firmware upgrade does not rewrite any customizing options. All customizing options such as customer logo are part of the license file.

Maintenance → Firmware → EMM

This tab will appear only if any EMM module is connected to the IDU and enabled.

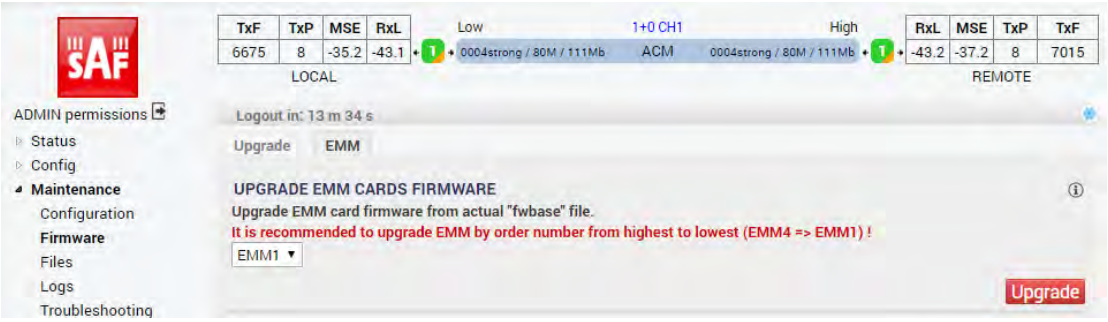


***Figure 3.53** "Maintenance → Firmware → EMM" page*

This section allows to upgrade firmware in attached EMM modules. It is recommended to update EMM modules in reverse order as follows:

EMM4->EMM3->EMM2->EMM1

During firmware upgrade there will be a data drop for about 15 seconds per one module.

Maintenance → Files → Exports

This section allows collect various device reports as downloadable archives for problem diagnostics/troubleshooting 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 EXPORT GENERATED FILES FROM VOLATILE MEMORY. Those files are erased during restart of the device or by means of the Remove button.

***Figure 3.54** "Maintenance → Files → Exports" page*

1) ***Generate ALL*** – selects all below listed items for file generation at once.
2) ***Generate Log File*** – archive of various log files for debugging purposes with link configuration and condition as plain text files.
3) ***Generate License Request*** – a binary file with current license status. This file is meant for extending license expiration date.
4) ***Generate Configuration File*** – 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. The configuration transfer should be done only between devices with matching firmware versions. This file can not be read by the user.

Maintenance → Files → Upload

In this section it is possible to upgrade firmware files manually, configuration file and the license file. In this case user should select the appropriate file and press the UPLOAD AND EXECUTE button.

Figure 3.55 *"Maintenance → Files → Upload" page*

Examples of files are as follows:

Firmware (load files in the following order):

- hwbase505.afw, hwbase511.afw – software for internal HW parts
- oskernel.afw – operating system
- fwbase.afw – application software (WEB, SNMP, commands , etc.)

Configuration:

- fwconf_OriginatingSN_Timestamp.afw (example: fwconf_3010501010100008_1702141508.afw)

License:

- licSN.afw (example: lic3010501010100008.afw)

The extension of the file is important. The device file validation is case sensitive so *.afw is not equal to *.AFW.

Maintenance → Logs

This section displays device's historical data. 3rd level sections enlisted under this section do not depend on the alarm settings, thus all events are recorded. The historic span of this information depends on the link condition – a lot of events will cause quicker filling of these logs and sooner overwriting of the oldest records.

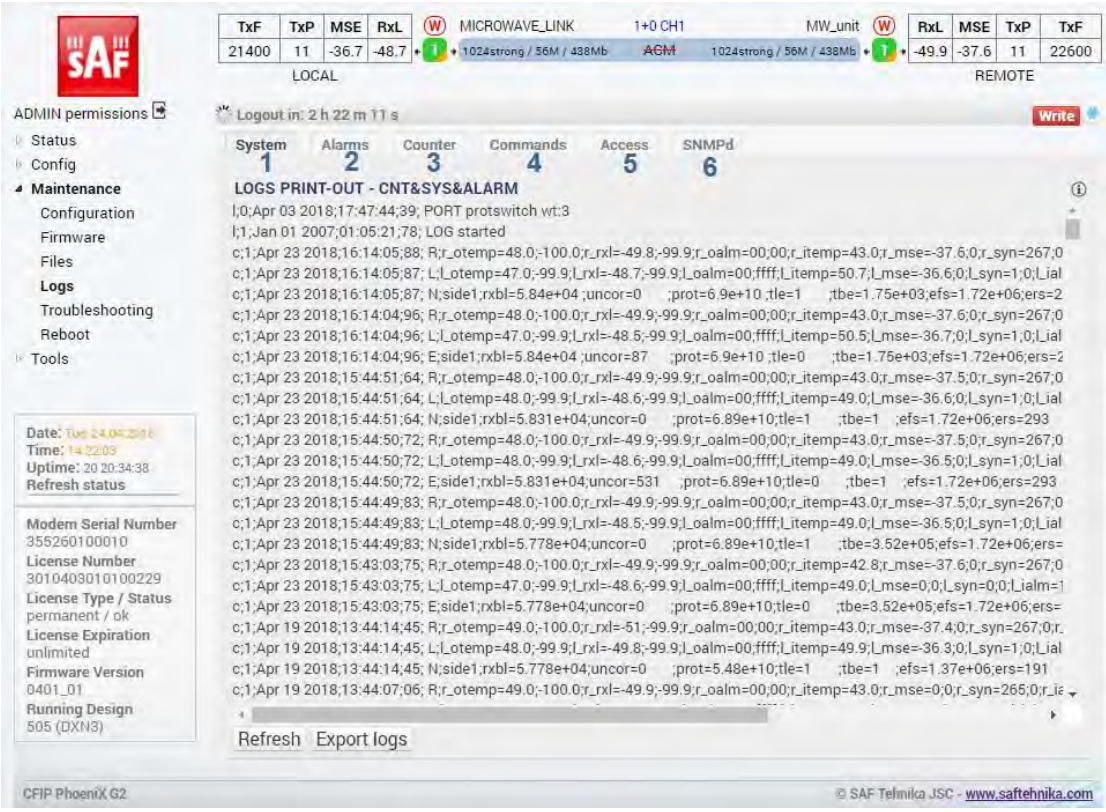


Figure 3.56 *"Maintenance → Logs" page*

1) ***System*** – system events (for example: license action, radio configuration changes, etc.)
2) ***Alarms*** – the alarm log
3) ***Counter*** – system counter events. When an error is detected or resolved this file is appended by the actual link parameters at this moment
4) ***Commands*** – history of performed commands
5) ***Access*** – authentication history
6) ***SNMPd*** – reports of the internal SNMP daemon

Maintenance → Troubleshooting → Assistant

Troubleshooting assistant displays status information about each configured channel. According to this information it is possible to point out possible issues with the equipment like misconfiguration, non-default settings and other device performance issues.

***Figure 3.57** "Maintenance → Troubleshooting → Assistant" page*

Maintenance → Troubleshooting → Detail-SYS

Device status summary is displayed in this section. Additional debug information will be shown in case of error state.

***Figure 3.58** "Maintenance → Troubleshooting → Detail-SYS" page*

1) ***Alarms stat*** – actual device alarm status. Only enabled alarms are considered.
2) ***Drivers stat*** – actual status of low level drivers. An eventual error suggests unsuccessful or ongoing communication between respective driver and the system driver. The system driver is responsible for interpretation of device status to front ends (CLI, GUI, SNMP).
3) ***Settings stat*** – actual configuration status. An eventual error suggests that a required settings could not be set.

Maintenance → Troubleshooting → Detail-IF

This section provides summary of basic and advanced status details of the IF part.

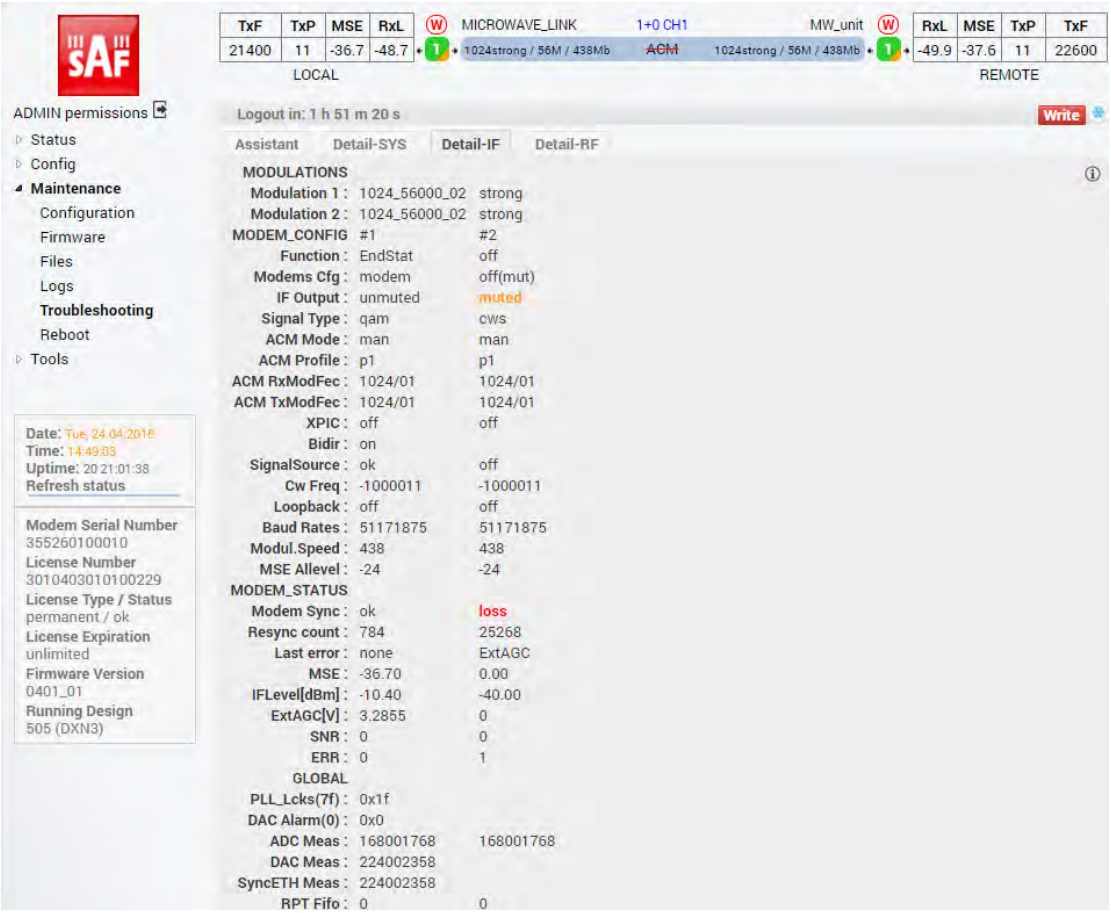


***Figure 3.59** "Maintenance → Troubleshooting → Detail-IF" page*

Maintenance → Troubleshooting → Detail-RF

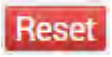
This section provides summary of basic and advanced radio parameters. These values are collected directly from the ODU and reflect its actual state.

***Figure 3.60** "Maintenance → Troubleshooting → Detail-RF" page*

Maintenance → Reboot

***Figure 3.61** "Maintenance → Reboot" page*

- IDU's reboot will be performed by pressing this button. This operation will cause data drop.



- this section will appear only if any of AMM modules is connected to the IDU and enabled. EMM cards will be initialized when this button will be pressed. This operation will cause data drop.

- re-initialization of IP interfaces, SSH, WEB, SNMP and NTP daemons will be performed by pressing this button.

Tools

Tools → Terminal

In this section built-in terminal window for accessing CLI (Command Line Interface) is available.

Execute command '?' in order to display all available commands. In order to check available sub-commands, question mark must be typed after the main command, for example command 'show ?' will print out all available 'show' sub-commands.

***Figure 3.62** "Tools → Terminal" page*

Tools → IP Ping

Possibility to send 'ICMP ECHO_REQUEST' to network hosts by entering IP address in ***Target IP address*** cell.

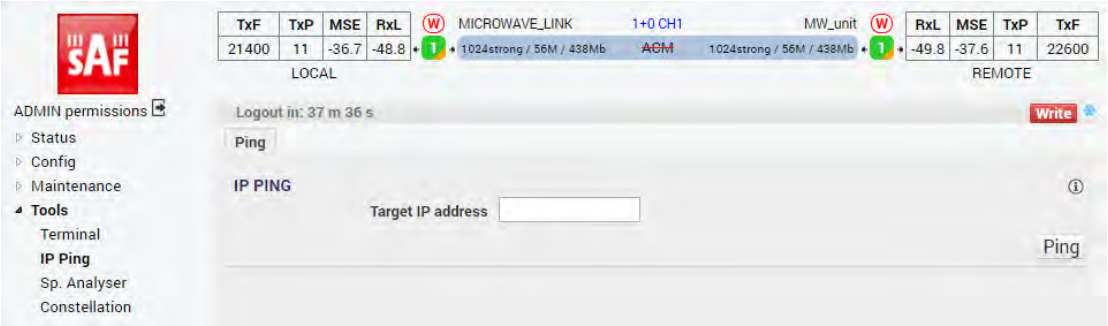


***Figure 3.63** "Tools → IP Ping" page*

Tools → Sp. Analyser

This section provides integrated spectrum analyser for free channel lookup, or alternatively for detection of interference within the particular band.

The frequency scanning consists of 3 automated steps:

a. local transmitter is muted;
b. local Rx frequency is sequentially tuned from lowest to highest frequency
c. the local Rx level is recorded for each frequency

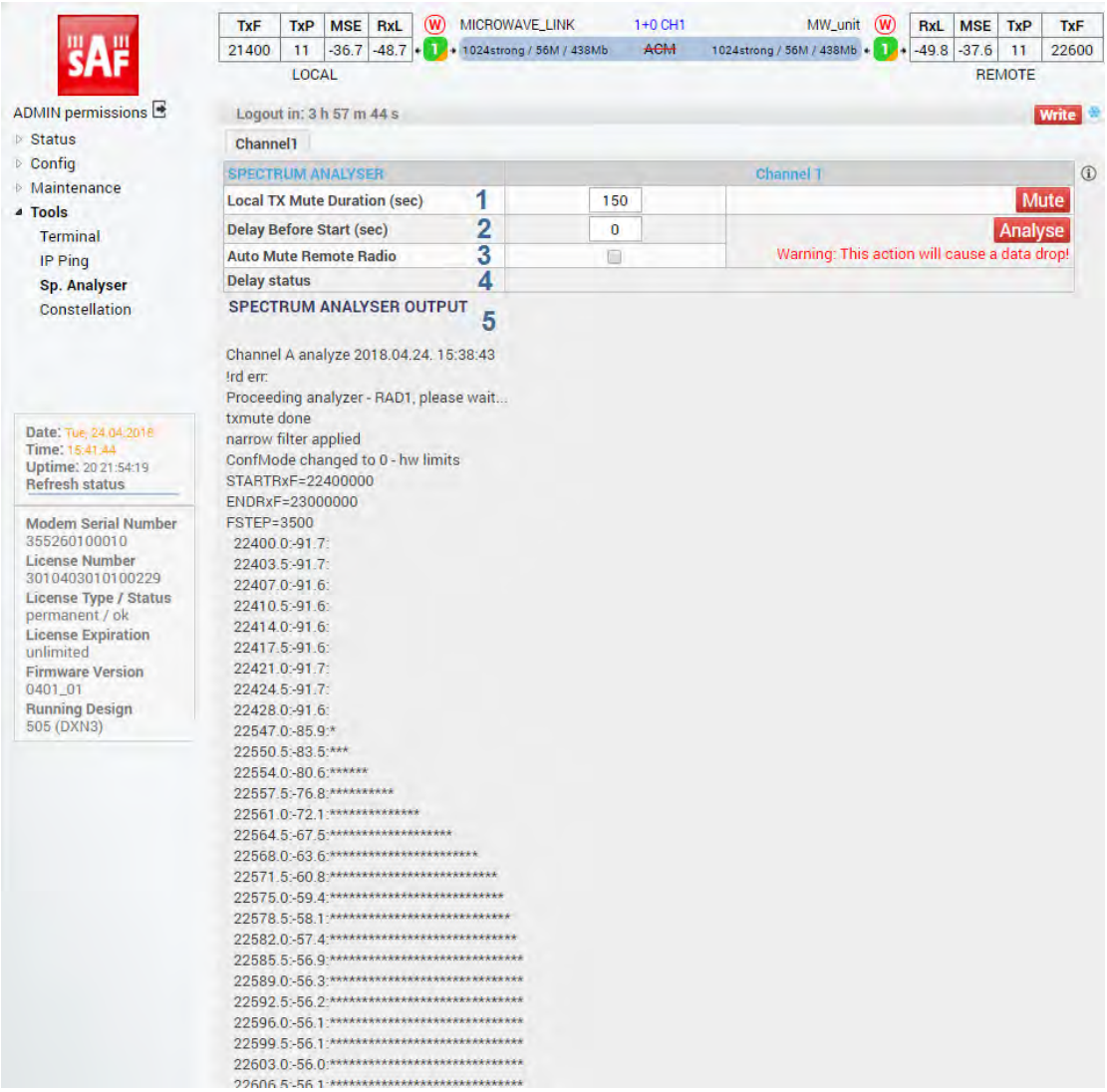
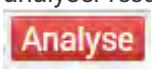


***Figure 3.64** "Tools → Sp. Analyser" page*

1) ***Local TX Mute Duration*** – manual Tx mute setting for the local radio for the specified duration. During this period the frequency scan should be performed on the remote device. This will not invoke the frequency scanning.
2) ***Delay Before Start*** – delay before frequency analysis starting (in seconds)
3) ***Auto Mute Remote Radio*** – allows auto mute of remote radio if possible (this function requires synchronization with remote side)
4) ***Delay status*** – a remaining delay time countdown
5) ***SPECTRUM ANALYSER OUTPUT*** – the spectrum analyser output frame. It displays the analyser results collected since last device reboot. It will be displayed only after pressing 

button.

The radio frequency scan can take between 30sec and 2min depending on used radio type and bandwidth. Data will be dropped during the frequency scanning.

Tools → Constellation

This section provides actual spectrum and constellation diagram outputs.

SPECTRUM shows simplified Rx spectrum plot.

CONSTELLATION DIAGRAM is a representation of a signal modulated by the digital

modulation schemes 1024QAM, 512QAM, 256QAM, 128QAM, 64QAM, 32QAM, 16QAM or 4QAM. It displays the signal as a two-dimensional scatter diagram in the complex plane at symbol sampling instants. Measured constellation diagram can be used to recognize the type of interference and distortion in a signal.

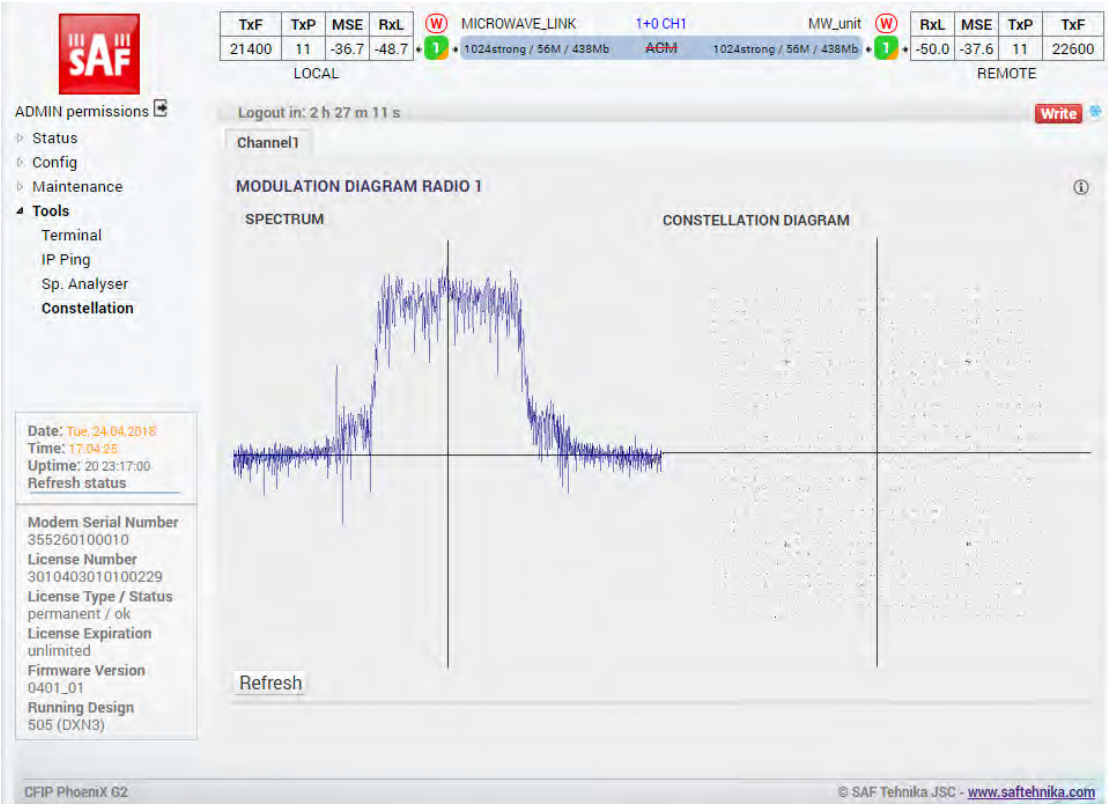
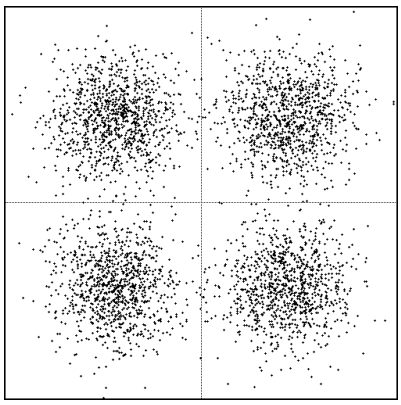


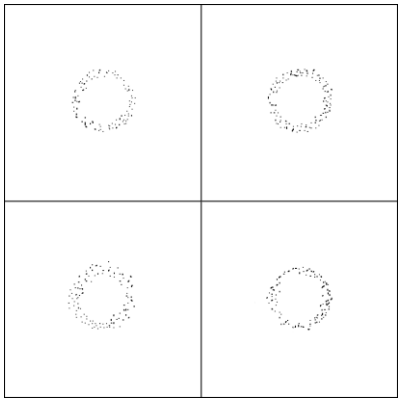
***Figure 3.65** "Tools → Constellation" page*

For the purpose of analysing the received signal quality, some types of corruption are evident in the constellation diagram. For example:

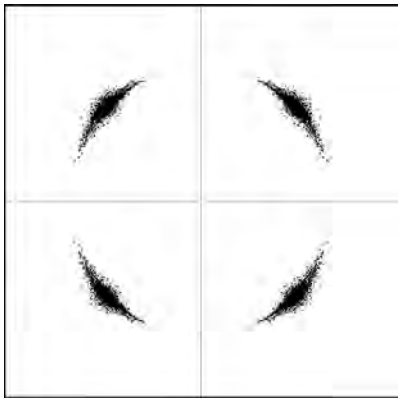
1) Gaussian noise is displayed as fuzzy constellation points:



2) Non-coherent single frequency interference is displayed as circular constellation points:



3) Phase noise is displayed as rotationally spreading constellation points:



Chapter 4: COMMAND LINE INTERFACE

Command line interface (CLI) is available via 3 individual interfaces:

- Secure Shell (SSH);
- Telnet;
- Web GUI (Tools→Terminal, partial functionality)

Telnet and SSH terminal is available via Ethernet management port. CLI is also available in web GUI in Tools → Terminal page.

Command line management interface offers the same configuration and monitoring functionality as it is in web GUI.

> Default username for SSH and Telnet connections is ***admin*** and password - ***secret***
> To end Telnet and/or SSH session enter command "quit". Opening the session again, the prompt will appear to enter username and password.

The basic command structure and output description is following:

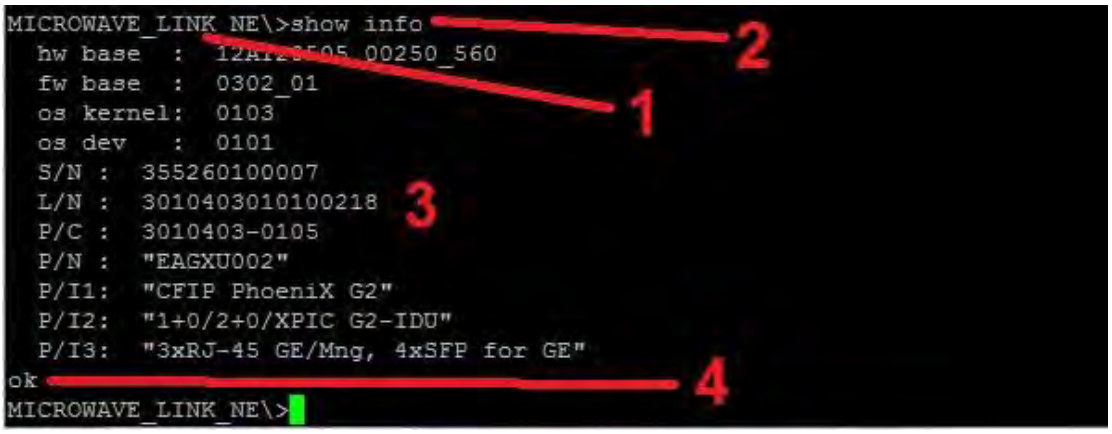


Figure 4.1 *CLI command structure*

1 Name and informative prompt of the device

a) "MICROWAVE_LINK" – the name of the device, can be changed by user (command **set descr name <new_name>**)

b) "_NE\>" – informative prompt, following meaning are provided:

- "xxx_XXY**>**" - **>** prompt in reading mode
- "xxx_XXY**#**" - **#** prompt in enable mode
- "xxx_XX|Z" - **|** prompt indicates unsaved changes (write w0 is needed)
- "xxx_XX****Z" - **** prompt indicates no unsaved changes (no write w0 needed)
- "xxx_**N**XYZ" – **N** indicates that device is in ok state (command to check alarms **sh alarm all**)
- "xxx_**E**XYZ" – **E** indicates that device is in alarm state (command to check alarms **sh alarm all**)
- "xxx_X**N**YZ" – **N** indicates that device was not in alarm state since last alarm validation
- "xxx_X**E**YZ" – **E** indicates that device as in alarm state since last alarm validation (command to check **sh history alarm**)

2 Executed command

Command executed by user

3 Output field of the command

Output of the executed command

4 The exit status of the command

Possible return values are following:

- **ok** – the command was executed successfully
- **not valid at 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
- **locked** – another active administrative session already in 'enable' mode

In order to change any settings in command line 'enable' mode must be acquired. This mechanism ensures that only one login session (CLI, SNMP or WEB) is allowed to change the settings. This step is not necessary in the built-in WEB GUI Terminal as the administrative login in the WEB GUI acquires '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**.

An example of using 'enable' mode is shown in the example below:

```
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
```

Figure 4.2 *'Enable' mode examples*

The CLI offers inbuilt online help accessible by means of '?' question mark.

```
SAF_NN\>?
 - ? : 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
SAF_NN\>
```

Figure 4.3 *CLI online help*

Syntax used in online help

- [ ] required parameters
- { } optional parameters
- (?) the parameter contains nested parameters. Type '?' at end of the command to see possible values and syntax

Some commands allow using the online help also for their sub-parameters. Refer to the example in ***Figure 4.4***

Most of commands can be entered in their shortened form. For example: enable = en, show = sh, write = wr, etc.

```
SAF_NE\#set rad1 ?
 - analyzer : [my] start spectrum analyzer (option my means fine analysis around
 CF)
 - atpc : radio atpc parameters (?)
 - down : power-off radio part
 - up : power-on radio part
 - filter : radio filter parameters (?)
 - mute : mute RF output from power amplifier
 - unmute : enable RF output from power amplifier
 - rxfreq : [number] set radio Rx frequency (MHz), valid only for some radio typ
es
 - tr : [low/high] Tx-Rx frequency distance, valid only for some radio types
 - txfreq : [number] set radio Tx frequency (MHz), ? for valid range (?)
 - txpower : [number] set radio Tx power (dBm), ? for valid range (?)
ok
SAF_NE\#set rad1 atpc ?
 - off : atpc off
 - on : atpc on
 - rxlevel : min rx level [-74 - 0]
ok
```

Figure 4.4 *CLI online help*

Connecting to SSH

SSH connection to Phoenix G2 IDU is carried out using Ethernet management connection. Please refer to Chapter Ethernet management connection configuration for Ethernet management port connection details.

You can use any SSH client. Below are connection steps with *PuTTY* - Windows freeware software.

1. Open *PuTTY*, choose "Connection Type": "SSH", enter IP address and make sure that correct port number is used ("22" by default):

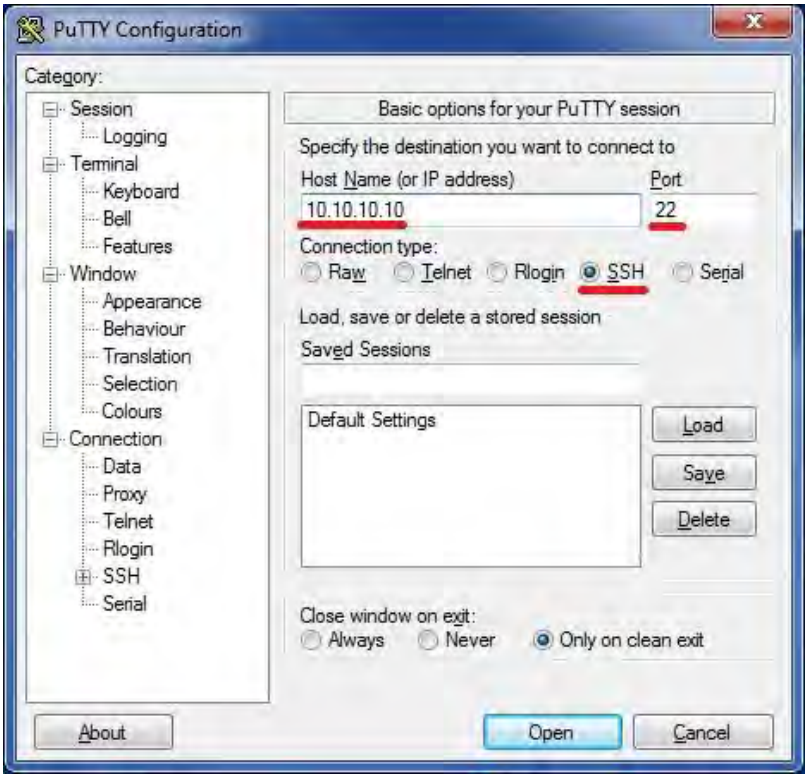


Figure 4.5 *PuTTY configuration*

2. Press "Open", enter login credentials (default user name is *admin* and password - *secret*). After successful login following prompt should appear:

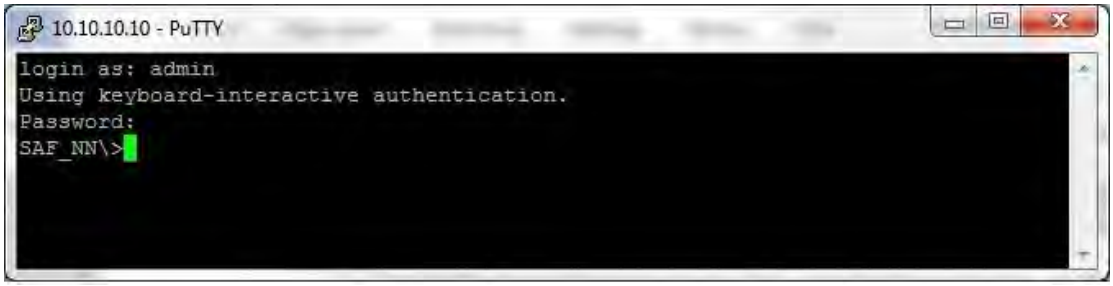


Figure 4.6 *PuTTY SSH prompt*

Connecting to Telnet

Telnet connection to Phoenix G2 IDU is carried out using Ethernet management connection. Please refer to Chapter Ethernet management connection configuration for Ethernet management port connection details.

You can use any Telnet client. Below are connection steps with *PuTTY* - Windows freeware software.

1. Open *PuTTY*, choose "Connection Type": "Telnet", enter IP address and make sure that correct port number is used ("23" by default):

Figure 4.7 *PuTTY confguration*

2. Press “Open”, enter login credentials (default user name is *admin* and password - *secret*). After successful login following prompt should appear:

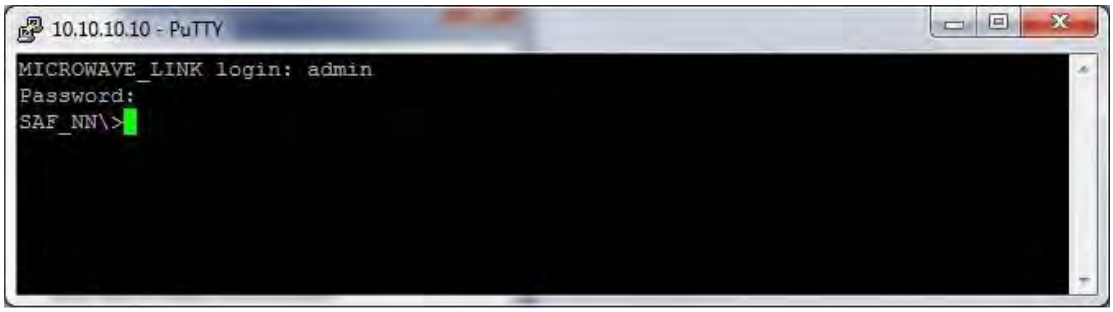


Figure 4.8 *PuTTY Telnet prompt*

Chapter 5: EXAMPLES

Example 1 – Configuration of SFP ports for GE traffic transmission

There are two ways of SFP port configuration to transmit Gigabit Ethernet traffic:

1) SFP port interconnected with built-in switch
2) SFP port directly interconnected with data channel, bypassing built-in switch

The option when **SFP port is interconnected with built-in switch** can be used in cases if:

- It is needed to access management of the IDU via SFP port
- It is needed to apply VLAN or QoS rules on the SFP stream

In this case the SFP port will be connected to one of WAN ports and it automatically consumes one of two WAN ports, and in case if for example two separated LAN traffics are needed, this option can not be used.

Configuration steps of this option are following:

1) In web GUI 'Config->Ports->EthVLAN' page configure port grouping so that WANA and WANB ports are in the same group.

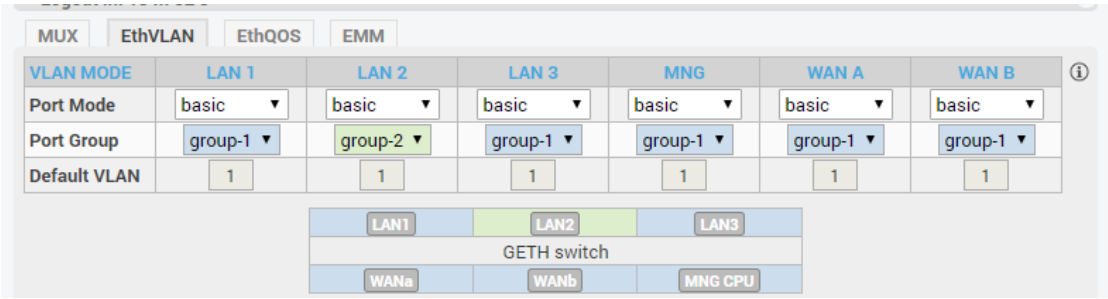


Figure 5.1 *Example of group configuration for WANA and WANB ports*

2) In web GUI page 'Config->Ports->MUX' for particlular SFP port select one of WAN ports in the 'Channel Select' row thus interconnecting this SFP port with the WAN port of the built-in switch.

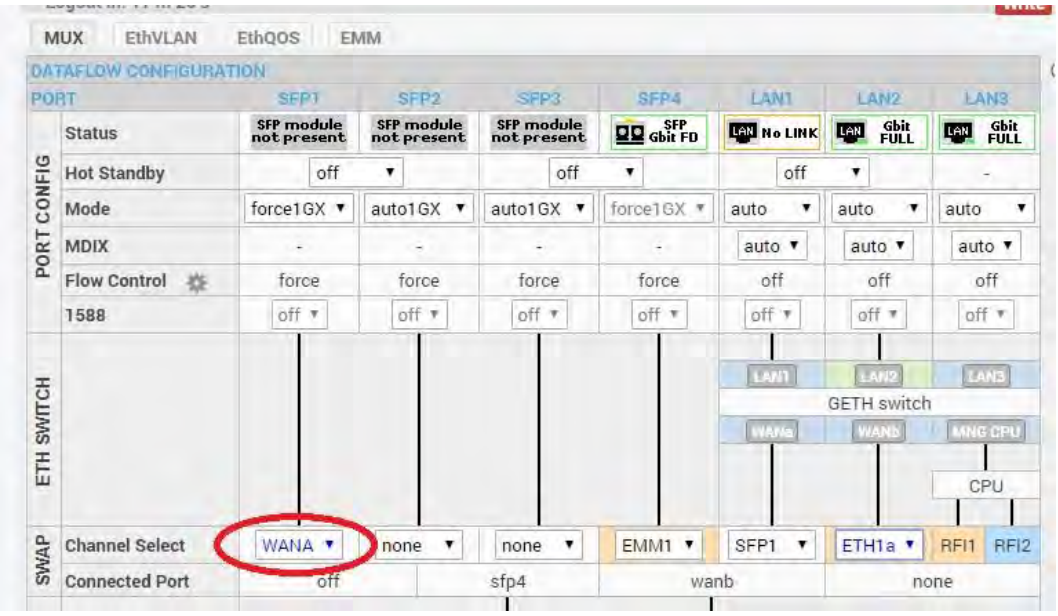


Figure 5.2 *Example of SFP port and WAN port interconnection*

3) In the same web GUI page for the second WAN port (the one which is not interconnected with SFP port) choose option ETH1a in 'Channel Select' drop-down thus interconnecting the second WAN port with data channel over the RF (refer to ***Figure 5.3***). In order to have remote MNG access the MNG port must be in the same group with both WAN ports (refer to ***Figure 5.1***).

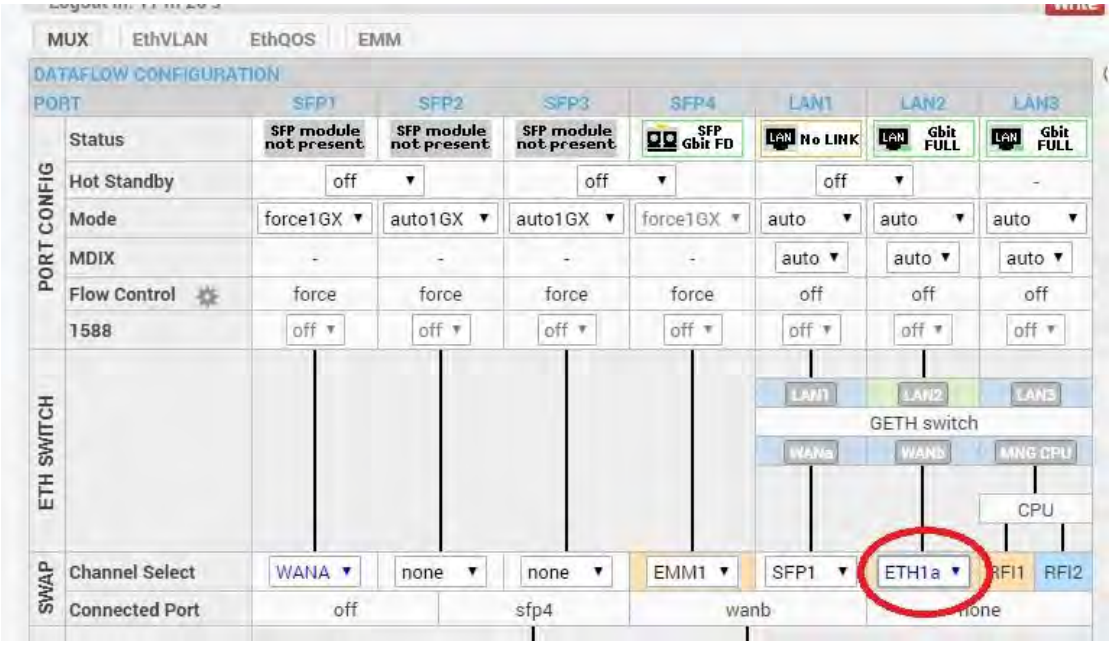


Figure 5.3 *Example of WAN port and data channel interconnection*

4) Configure the same settings also in the remote Phoenix G2 IDU. Save new settings by pressing 

button.

The option when **SFP port directly is interconnected with data channel, bypassing built-in switch** can be used in cases if:

- It is needed to simply pass SFP traffic transparently over the link
- It is needed to have jumbo packet support
- It is need to have SFP traffic separated from the other data
- There is no need for any of the built-in switch capabilities

Configuration steps of this option are following:

1) In page 'Config->Ports->MUX' for particlular SFP port select ETH1a option to interconnect it directly with data channel.

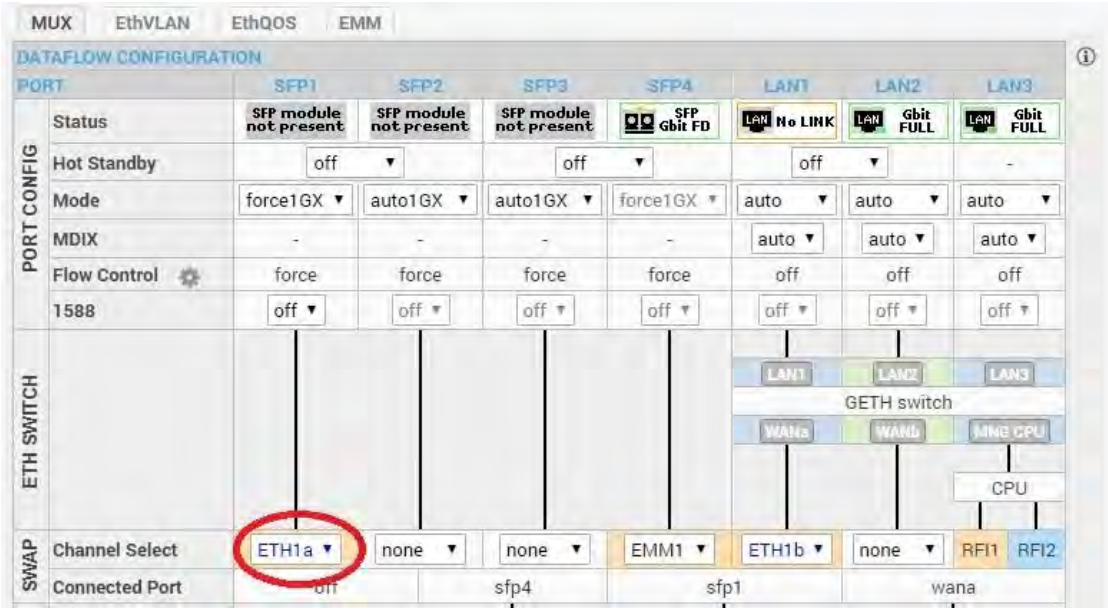


Figure 5.4 *Example of SFP port and data channel interconnection*

2) In the same page interconnect one of WAN ports with ETH1b data channel by choosing it in ‘ Channel Select’ drop-down thus enabling remote MNG access (refer to ***Figure 5.5***). Note that MNG port must be in the same group as chosen WAN port

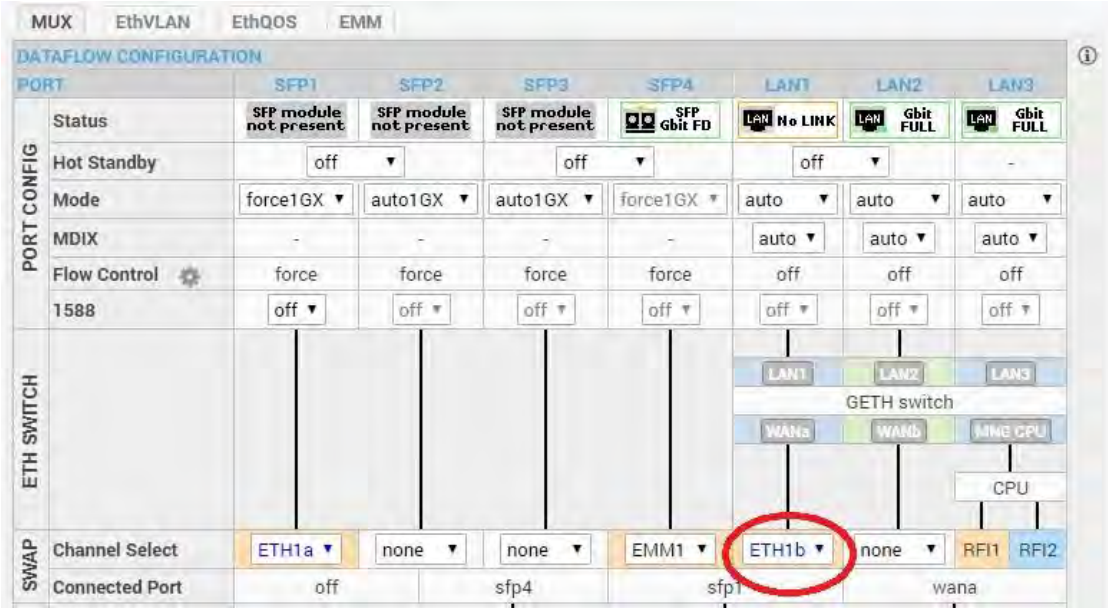


Figure 5.5 *Example of WAN port and data channel interconnection*

3) In the same page set speed limits for both ETH1a and ETH1b channels. Note that ETH1a channel is high priority channel and if the maximum allowable speed will be set for this port, the ETH1b (low priority data channel) speed will be left as 0 Mbps and MNG traffic will not be possible over the link

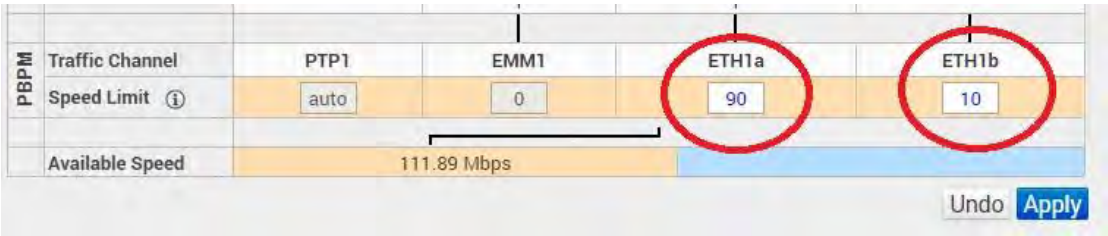


Figure 5.6 *Example of data channel speed limit configuration*

4) Configure the same settings also in the remote IDU. Save new settings by pressing  button.

Example 2 – Basic 1+1 HSB/SD protection scheme

The basic 1+1 HSB/SD (Hot Standby/Space Diversity) protection schemes ensure the correct data transmission over the microwave link in case of specific HW block (ODU, IDU-ODU cable, modem) failure or receive conditions degradation.(multipath fading, ..). **This scheme requires one Phoenix G2 IDU with connected two ODUs per site**.

1+1 HSB/SD protection scheme can be enabled by software in web GUI of the IDU in 'Config->System->Mode' page. Physically 1+1 HSB or 1+1 SD mode is determined by antenna usage in sites – for 1+1 HSB one antenna and coupler can be used per each site with two ODUs connected to the coupler, while 1+1 SD requires two antennas in each site with one ODU connected to each antenna.

In 1+1 HSB/SD mode one transmitter is active (second one is automatically muted), while two receivers receive the identical signal and the IDU decides what stream will be used for final data de-multiplexing. The equipment provides hitless switchover in case of ODU Rx failure, and short data drop in switchover in case of ODU Tx failure.

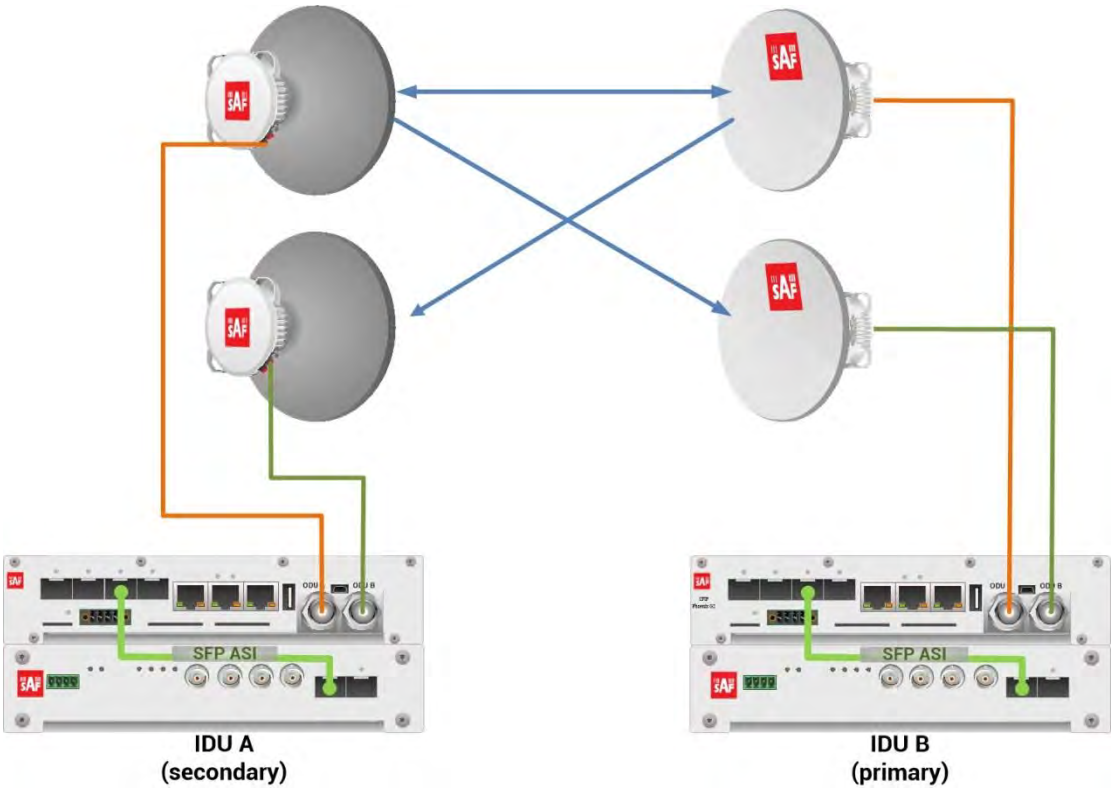


Figure 5.7 *Example of 1+1 SD mode*

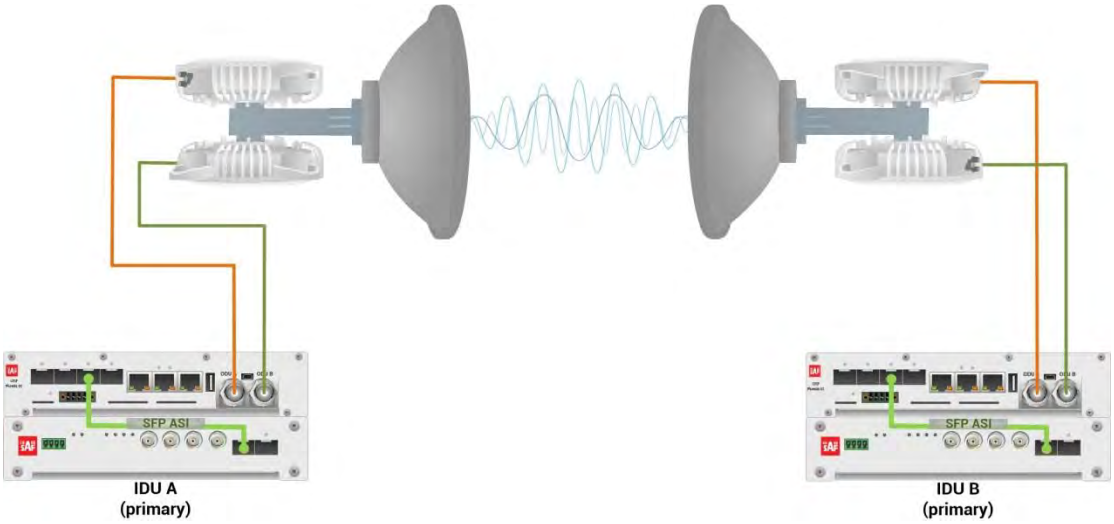


Figure 5.8 *Example of 1+1 HSB mode*

This concrete example describes an application where the Design Type 'Design 505', Functional mode '1+1' and Link diversity 'HSB/SD – hot standby' are selected on both link sides, modulation is 32QAM in BW 60 MHz and the appropriate maximal data speed is about 227 Mbps. The management access is In-Band management described in section '[Management channel configuration options]'.

Configuration steps for basic 1+1 HSB/SD protection scheme are following:

1) In web GUI '[Config->System->Mode]' choose design type 'Design 505', Functional mode '1+1' and Link Diverity 'HSB/SD – hot standby' in both Phoenix G2 IDUs:

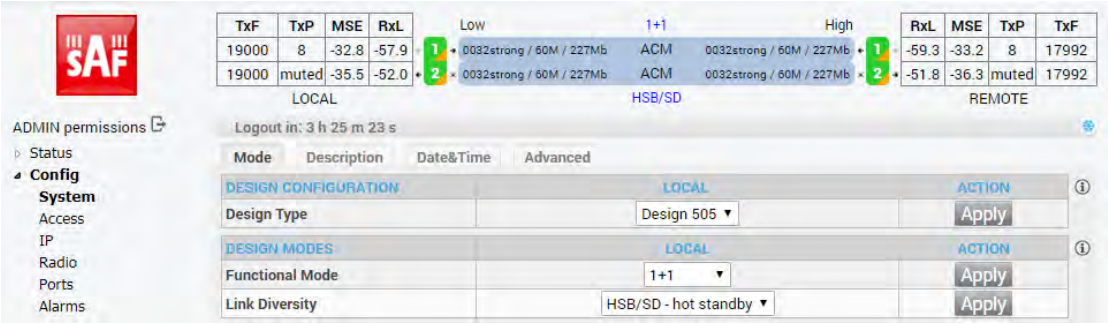


Figure 5.9 *Example of System configuration*

2) In web GUI '[Config->Radio->Parameters]' configure basic radio and modem parameters in both Phoenix G2 IDUs. Use the same frequency channel for both ODU pairs:

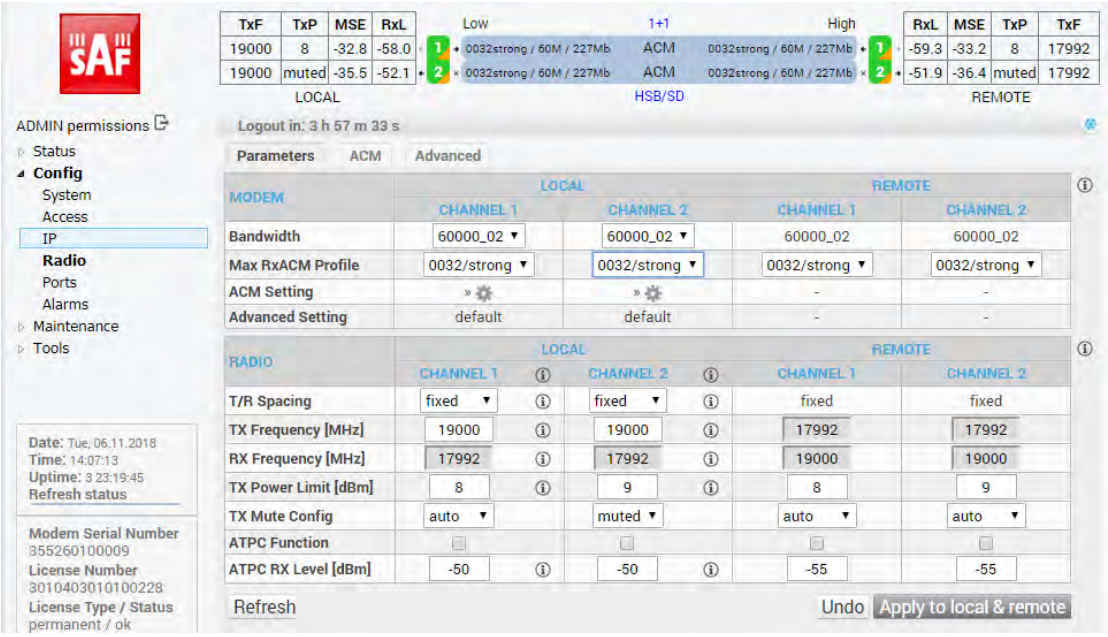


Figure 5.10 *Example of basic Radio parameters configuration*

3) Port group configuration must be done according to customer requirements. The requirement in this example is to have In-band management which means that the management is accessible via the same ports where user traffic is passed through. In this case management port must be allocated in the same group with traffic ports (LAN and WAN ports). In the example Management port (MNG) and traffic ports (LAN1, LAN3 and WANa) are grouped into Group 1. Other ports – LAN2 and WANb are grouped in the Group 2 and will not be used or can be intended for any other independent and separated user data traffic. Port grouping configuration is available in web GUI 'Config->Ports->EthVLAN' and must be done in both Phoenix G2 IDUs.

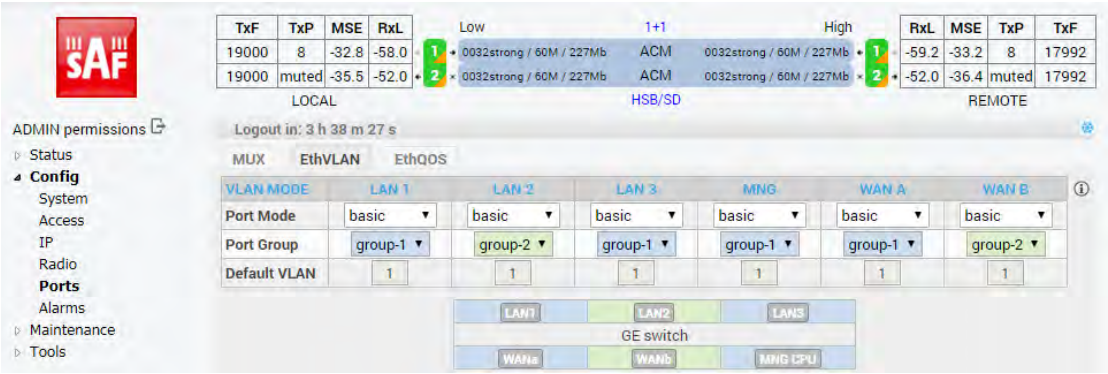


Figure 5.11 *Example of port grouping*

4) In web GUI 'Config->Ports->MUX' specify Data channel and port speed for WAN (radio direction) port in both Phoenix G2 IDUs. In the example WANa port is connected to high priority data channel 'ETH1a' and is set on full speed limit 1000 Mbps.

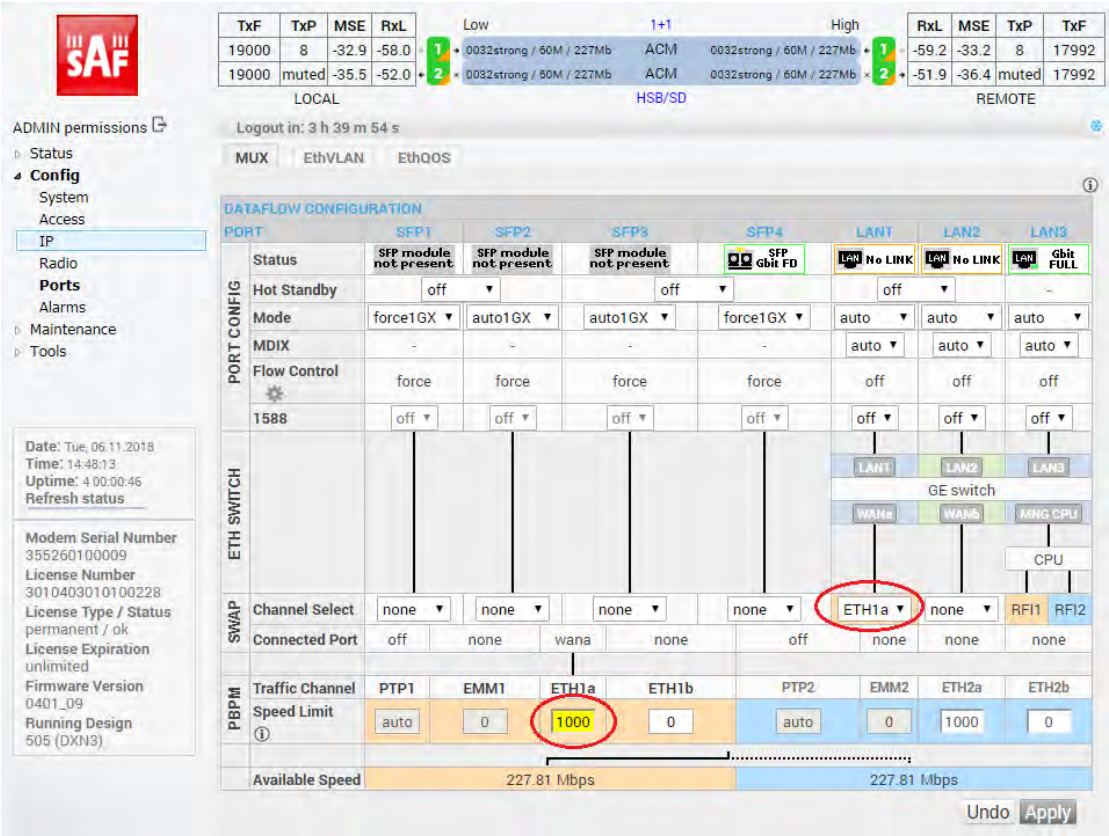


Figure 5.12 *Example of port configuration*

5) In case if EMM module is used, configure it according to EMM configuration description described in section '[Config->Ports->EMM](#)' in both Phoenix G2 IDUs.

6) Save new settings by pressing 

button.

The status of 1+1 configuration is displayed in the header of the web GUI:

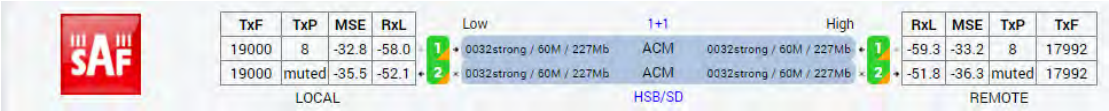


Figure 5.13 *Status of 1+1 HSB/SD mode*

Example 3 – Basic 1+1 FD protection scheme

The basic 1+1 FD (Frequency Diversity) protection scheme ensure the correct data transmission over the microwave link in case of specific HW block (ODU, IDU-ODU cable, modem) failure or receive conditions degradation, like multipath fading. Two frequency channels are used in this mode – one frequency channel for the Primary ODU pair and another frequency channel for the Secondary ODU pair. **This scheme requires one Phoenix G2 IDU with connected two ODUs per site**.

1+1 FD protection scheme can be enabled by software in web GUI of the IDU in '[Config->System->Mode](#)' page. 1+1 FD mode can be used with one antenna and coupler (or OMT adapter) per site, two ODUs are connected to the coupler. Also two separated antennas per site can be used.

In 1+1 FD mode two transmitters are active, and two receivers receive the identical signal and the IDU decides what stream will be used for final data de-multiplexing. The equipment provides hitless switchover.

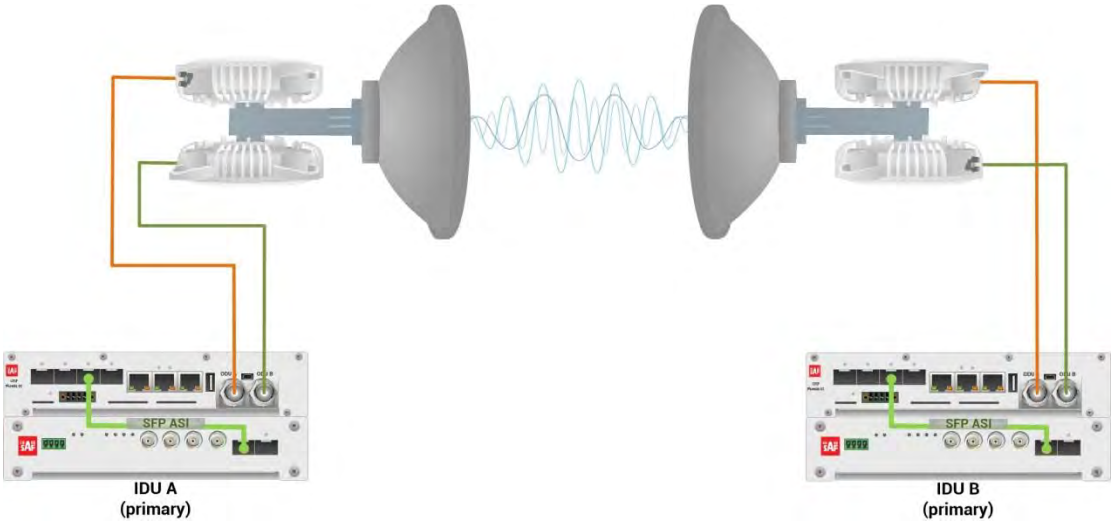


Figure 5.14 *Example of 1+1 FD mode*

This concrete example describes an application where the Design Type 'Design 505', Functional mode '1+1' and Link diversity 'FD – freq diversity' are selected on both link sides, modulation is 32QAM in BW 60 MHz and the appropriate maximal data speed is about 227 Mbps. The management access is Out-Band management described in section '[Management channel configuration options: Management in Separate Channel]'.

Configuration steps for basic 1+1 FD protection scheme are following:

1) In web GUI '[Config->System->Mode]' choose design type 'Design 505', Functional mode '1+1' and Link Diverity 'FD – freq diversity' in both Phoenix G2 IDUs:

Figure 5.15 *Example of System configuration*

2) In web GUI '[Config->Radio->Parameters]' configure basic radio and modem parameters in both Phoenix G2 IDUs. Use different frequency channels for each ODU pair:

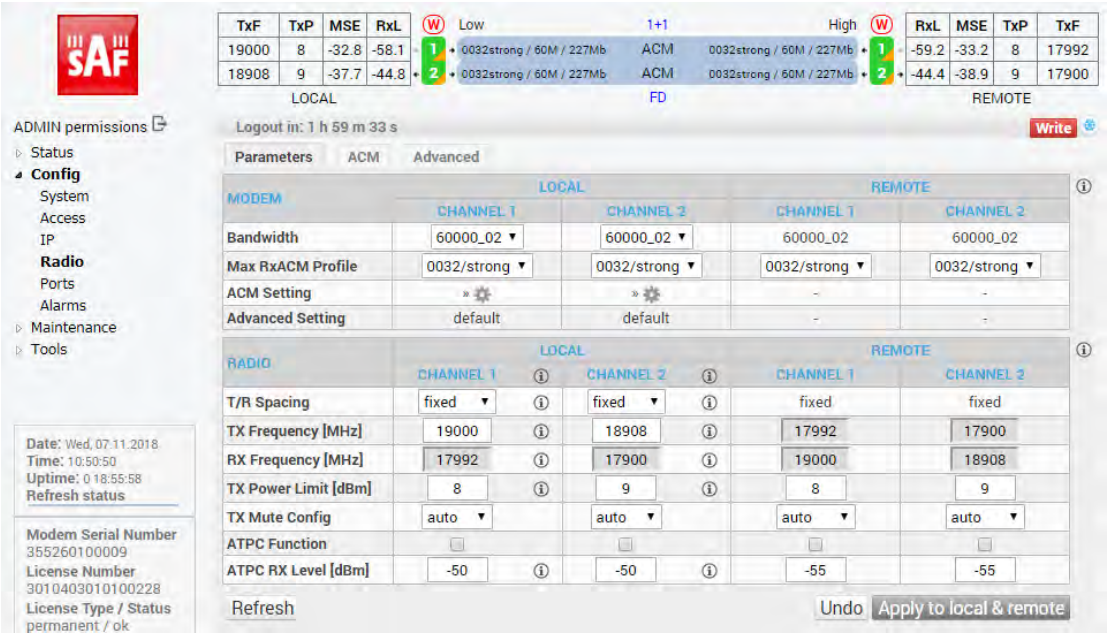


Figure 5.16 *Example of basic Radio parameters configuration*

3) Port group configuration must be done according to customer requirements. The requirement in this example is to have Out-band management which means that the management is accessible via separated LAN port from traffic ports. In this case management port and traffic ports must be in different groups. In the example Management port (MNG) will be available only via LAN3 port. In this case those both ports and one of WAN ports (WANa) will be grouped together in the same one group - in Group 1. Other ports which will be used for traffic – LAN1, LAN2 and the second WAN port (WANb) will be grouped in the separated group - Group 2. Port grouping configuration is available in web GUI 'Config->Ports->EthVLAN' and must be done in both Phoenix G2 IDUs.

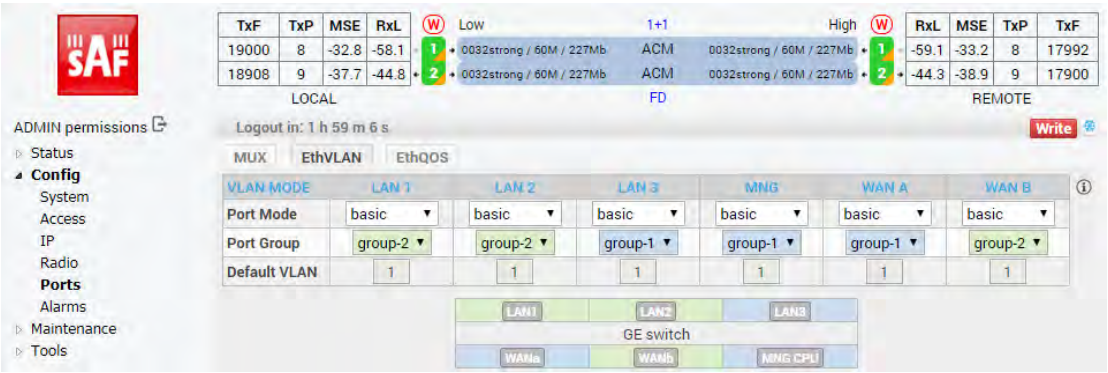


Figure 5.17 *Example of port grouping*

4) In web GUI 'Config->Ports->MUX' specify Data channel and port speeds for WAN (radio direction) ports in both Phoenix G2 IDUs. In the example WANa (management) port is connected to high priority data channel 'ETH1a' and is set on speed limit 2 Mbps; WANb (traffic) port is connected to low priority data channel 'ETH1b'and is set on speed limit 300 Mbps.

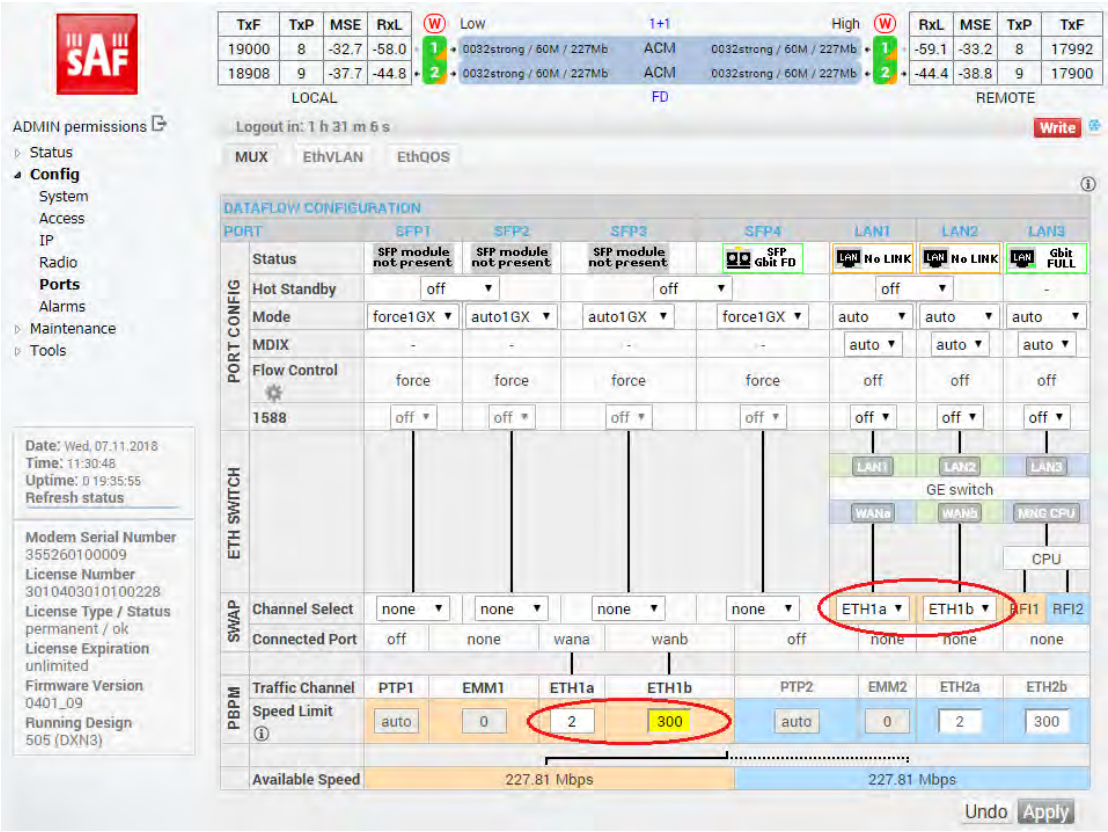
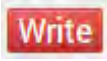


Figure 5.18 *Example of port configuration*

5) In case if EMM module is used, configure it according to EMM configuration description described in section 'Config->Ports->EMM' in both Phoenix G2 IDUs.

6) Save new settings by pressing  button.

The status of 1+1 configuration is displayed in the header of the web GUI:

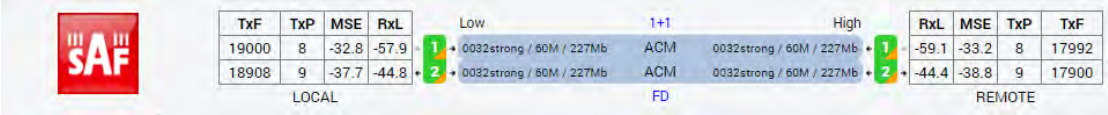


Figure 5.19 *Status of 1+1 FD mode*

Example 4 – Basic 2+0 FD traffic aggregation

The basic 2+0 FD (Frequency Diversity) aggregation mode allows to increase / double Ethernet traffic capacity over the microwave link using two ODU pairs. Each ODU pair uses its own frequency channel. Provided aggregation is Layer 1 capacity aggregation which internally combines the capacity of both physical channels, therefore aggregation doesn't depend on the MAC addresses of the aggregated frames. **This scheme requires one Phoenix G2 IDU with connected two ODUs per site**.

2+0 FD mode can be used with one antenna and OMT adapter per site, two ODUs are connected to the OMT adapter. Two separated antennas per site can be used as well.

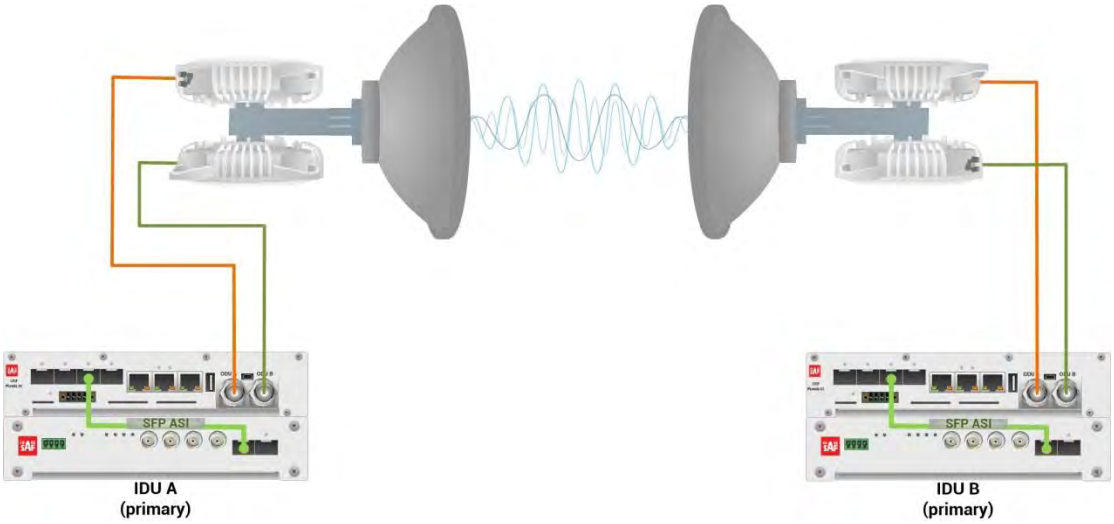


Figure 5.20 *Example of 2+0 FD mode*

This concrete example describes an application where the Design Type 'Design 505', Functional mode '2+0' and Link diversity 'FD – freq diversity' are selected on both link sides, modulation is 32QAM in BW 60 MHz. The appropriate maximal data speed per one ODU pair is about 227 Mbps. Total aggregated throughput is about 455 Mbps. The management access is In-Band management described in section '[Management channel configuration options]'.

Configuration steps for basic 2+0 FD protection scheme are following:

1) In web GUI '[Config->System->Mode]' choose design type 'Design 505', Functional mode '2+0' and Link Diverity 'FD – freq diversity' in both Phoenix G2 IDUs:

Figure 5.21 *Example of System configuration*

2) In web GUI '[Config->Radio->Parameters]' configure basic radio and modem parameters in both Phoenix G2 IDUs. Use different frequency channels for each ODU pair:

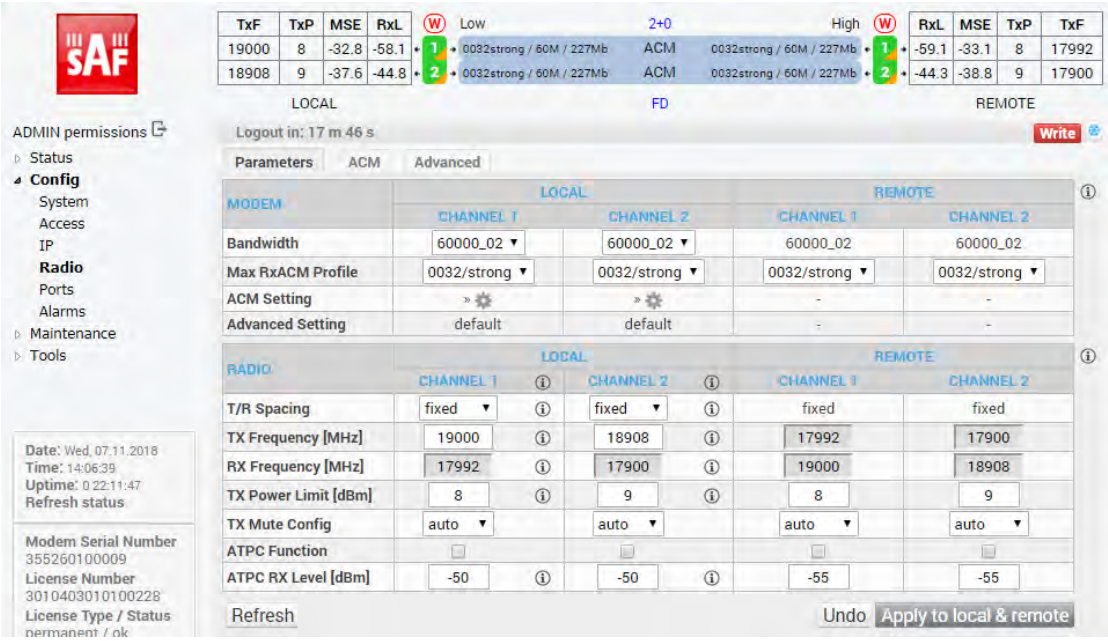


Figure 5.22 *Example of basic Radio parameters configuration*

3) Port group configuration must be done according to customer requirements. The requirement in this example is to have In-band management which means that the management is accessible via the same ports where user traffic is passed through. In this case management port must be allocated in the same group with traffic ports (LAN and WAN ports). In the example Management port (MNG) and traffic ports (LAN1, LAN2, LAN3 and WANa) are grouped into Group 1. WANb port is left disconnected and will not be used, so it is assigned to another group which is Group 2 in this case. Port grouping configuration is available in web GUI 'Config->Ports->EthVLAN' and must be done in both Phoenix G2 IDUs.

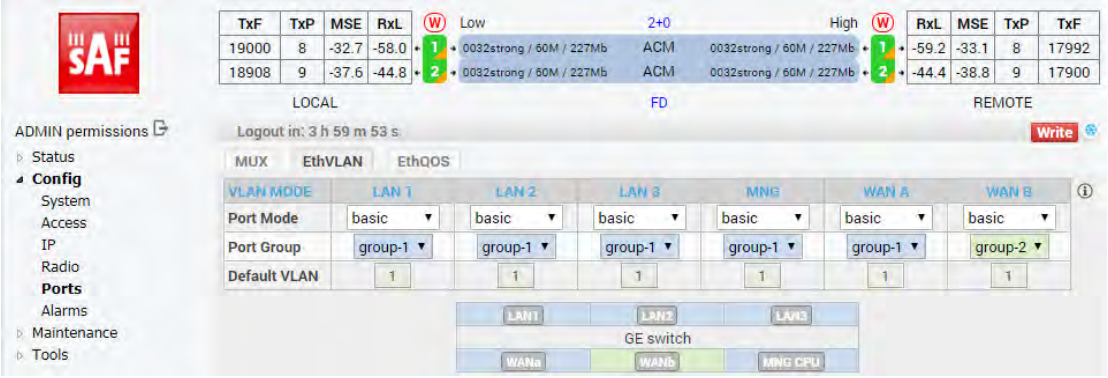


Figure 5.23 *Example of port grouping*

4) In web GUI 'Config->Ports->MUX' specify Data channel and port speed for WAN (radio direction) port in both Phoenix G2 IDUs. In the example WANa port is connected to high priority data channel 'ETH1a' and is set on full speed limit 1000 Mbps.

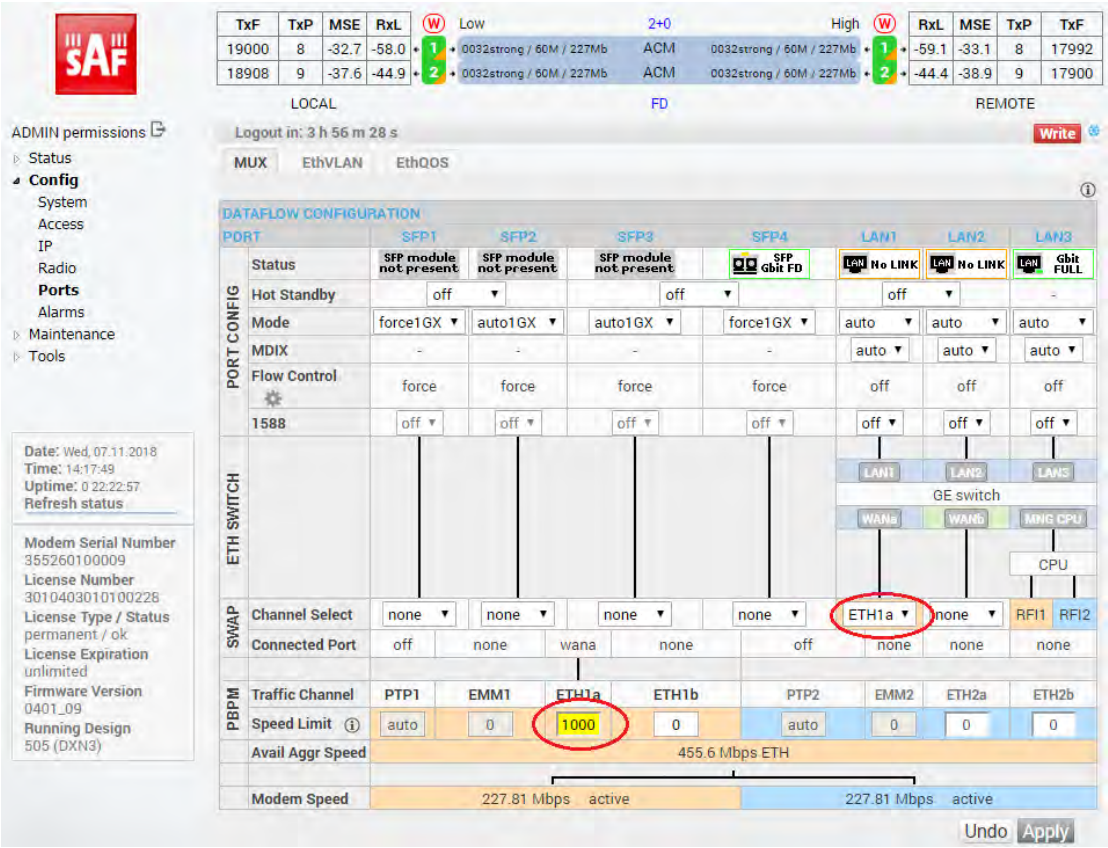
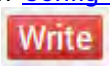


Figure 5.24 *Example of port configuration*

5) In case if EMM module is used, configure it according to EMM configuration description described in section '[Config->Ports->EMM](#)' in both Phoenix G2 IDUs.

6) Save new settings by pressing  button.

The status of 2+0 configuration is displayed in the header of the web GUI:

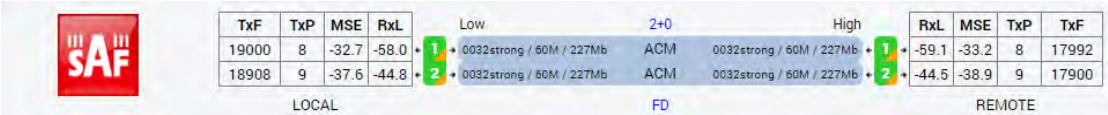


Figure 5.25 *Status of 2+0 FD mode*

Example 5 – Basic 2+0 XPIC traffic aggregation

The basic 2+0 XPIC (Cross-polar Interference Cancellation) aggregation mode allows to increase / double Ethernet traffic capacity over the microwave link using two ODU pairs. Both ODU pairs use the same frequency channel in different polarization– one ODU pair works in Horizontal polarization, the second ODU pair works in Vertical polarization. Provided aggregation is Layer 1 capacity aggregation which internally combines the capacity of both physical channels, therefore aggregation doesn't depend on the MAC addresses of the aggregated frames. **This scheme requires one Phoenix G2 IDU with connected two ODUs per site**.

2+0 XPIC mode can be used with one antenna and OMT adapter per site, two ODUs are connected to the OMT adapter.

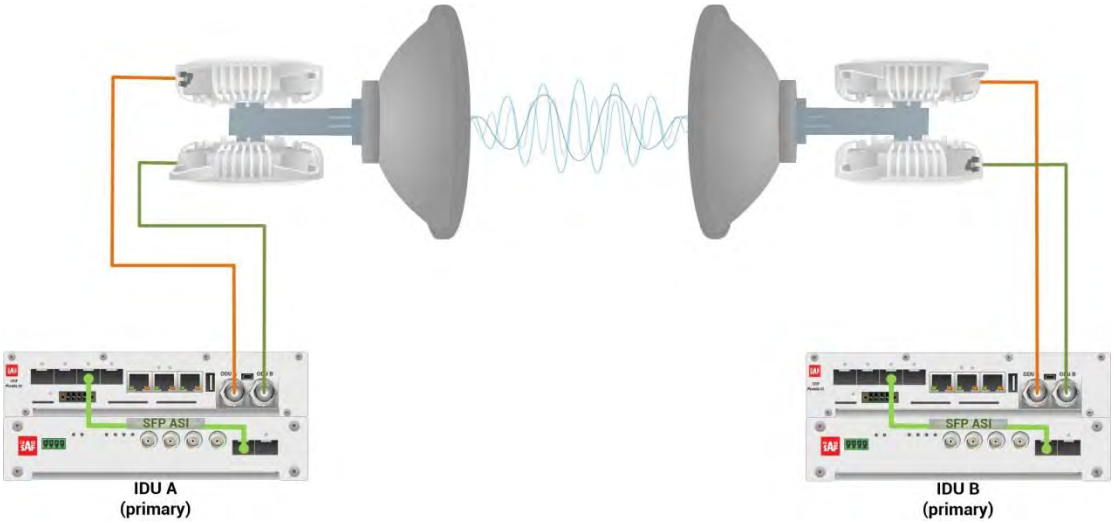


Figure 5.26 *Example of 2+0 XPIC mode*

This concrete example describes an application where the Design Type 'Design 505', Functional mode '2+0' and Link diversity 'XPIC' are selected on both link sides, modulation is 32QAM in BW 60 MHz. The appropriate maximal data speed per one ODU pair is about 227 Mbps. Total aggregated throughput is about 455 Mbps. The management access is In-Band management described in section '[Management channel configuration options]'.

Configuration steps for basic 2+0 XPIC protection scheme are following:

1) In web GUI '[Config->System->Mode]' choose design type 'Design 505', Functional mode '2+0' and Link Diverity 'XPIC' in both Phoenix G2 IDUs:

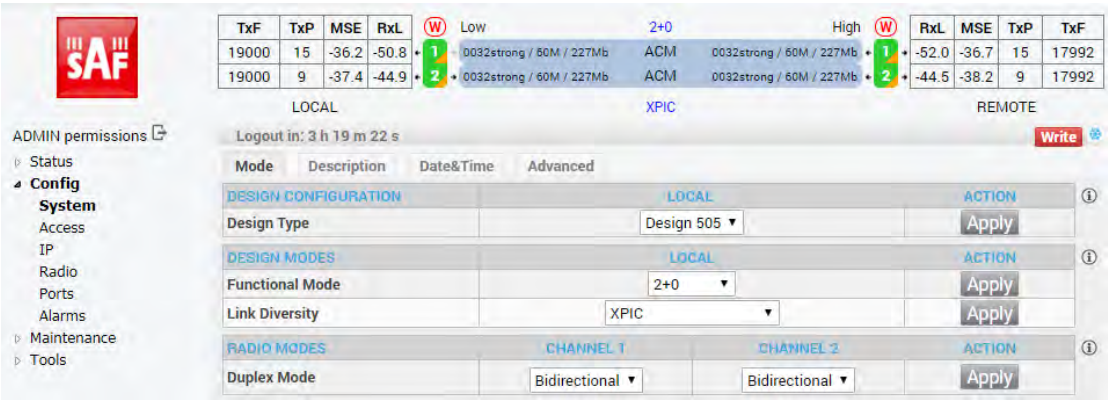


Figure 5.27 *Example of System configuration*

2) In web GUI '[Config->Radio->Parameters]' configure basic radio and modem parameters in both Phoenix G2 IDUs. Use the same frequency channel for both ODU pairs:

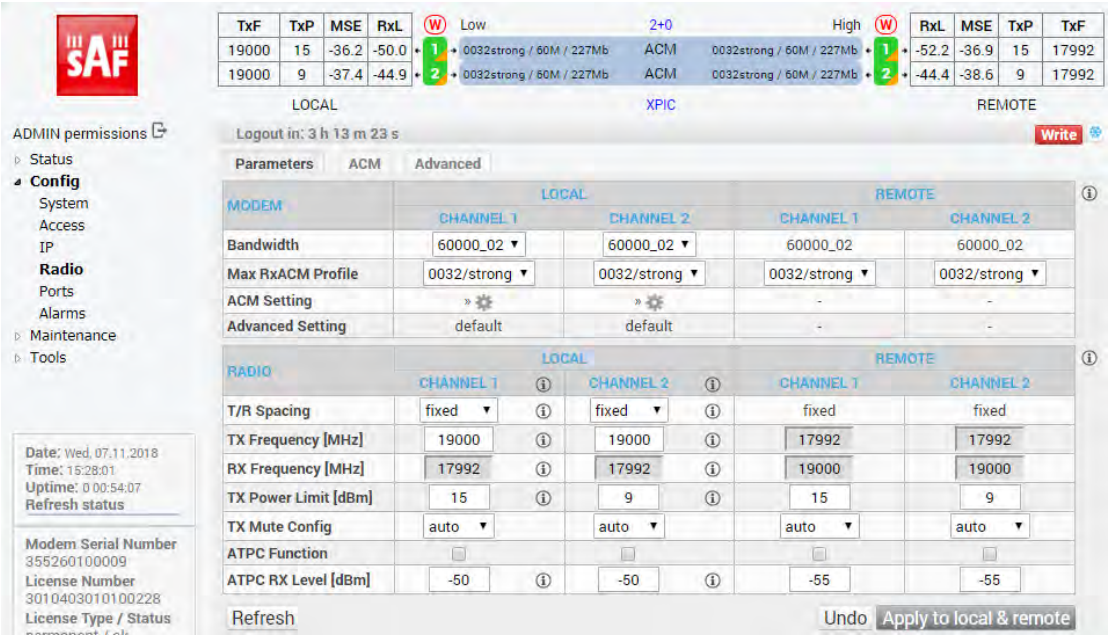


Figure 5.28 *Example of basic Radio parameters configuration*

3) Port group configuration must be done according to customer requirements. The requirement in this example is to have In-band management which means that the management is accessible via the same ports where user traffic is passed through. In this case management port must be allocated in the same group with traffic ports (LAN and WAN ports). In the example Management port (MNG) and all traffic ports (LAN1, LAN2, LAN3, WANa and WANb) are grouped into Group 1. Port grouping configuration is available in web GUI 'Config->Ports->EthVLAN' and must be done in both Phoenix G2 IDUs.

Figure 5.29 *Example of port grouping*

4) In web GUI 'Config->Ports->MUX' specify Data channel and port speed for WAN (radio direction) port in both Phoenix G2 IDUs. In the example WANa port is connected to high priority data channel 'ETH1a' and is set on full speed limit 1000 Mbps.

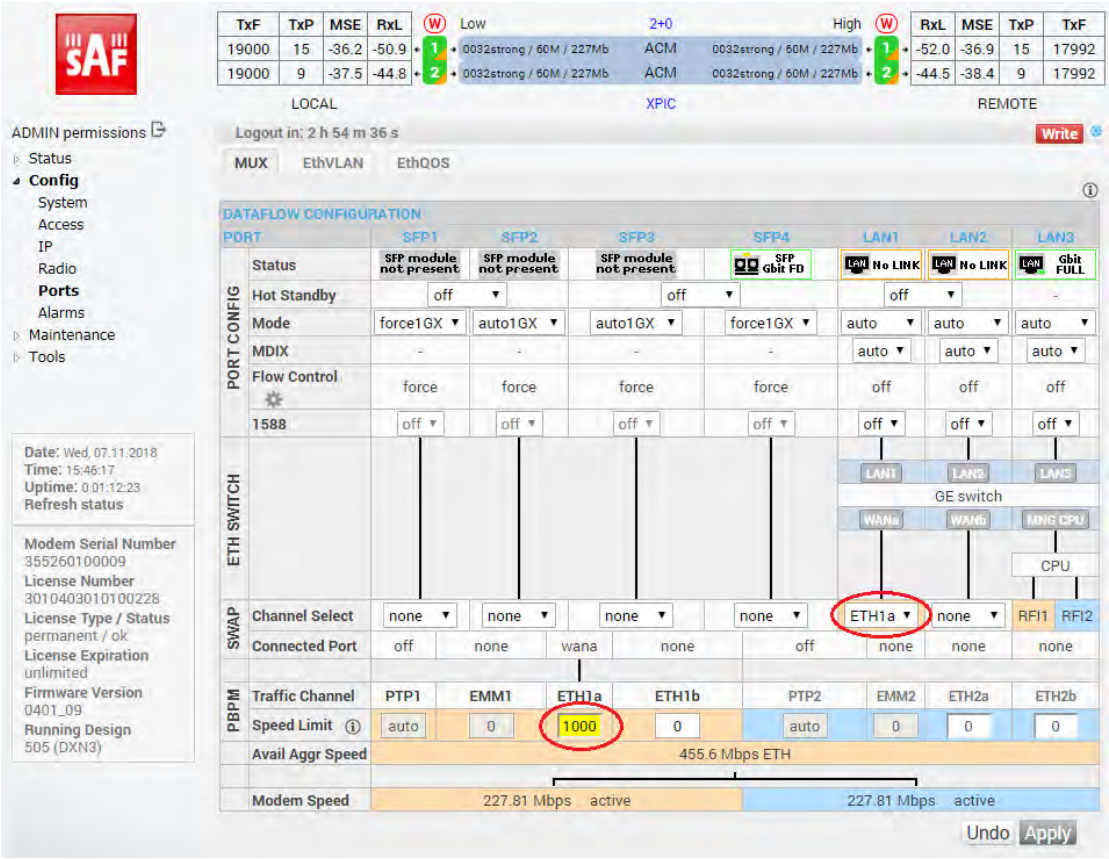


Figure 5.30 *Example of port configuration*

5) In case if EMM module is used, configure it according to EMM configuration description described in section '[Config->Ports->EMM](#)' in both Phoenix G2 IDUs.

6) Save new settings by pressing  button.

The status of 2+0 configuration is displayed in the header of the web GUI:

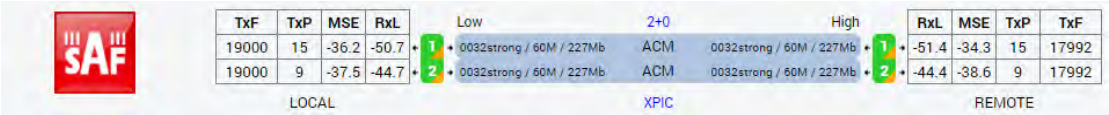


Figure 5.31 *Status of 2+0 XPIC mode*

Example 6 – 1+0 Dual FD connection scheme for link capacity increasing

The 1+0 Dual FD (Frequency Diversity) mode is advanced 1+0 mode which allows increasing Ethernet traffic capacity of the link by passing two independent Ethernet data streams over two separated independent physical data channels using two ODU pairs. Each ODU pair uses its own frequency channel. This configuration can be used for two independent network data passing through the link, internal aggregation is not provided in this configuration. If required, external aggregation can be performed in external network devices. **This scheme requires one Phoenix G2 IDU with connected two ODUs per site**.

In case of link capacity increasing the 1+0 Dual FD mode can be used with one antenna and OMT adapter per site, two ODUs are connected to the OMT adapter. Two separated antennas per site can be used as well.

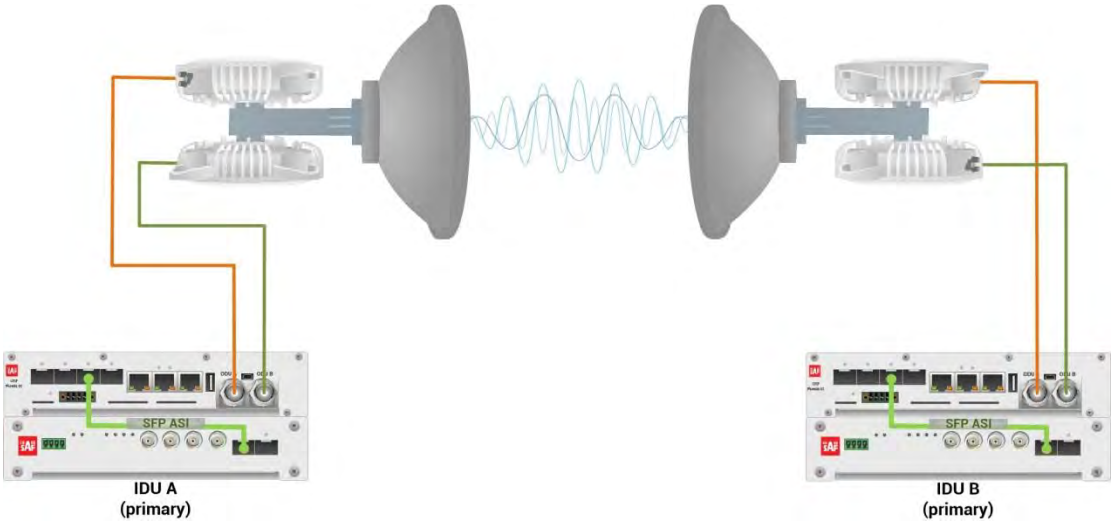


Figure 5.32 *Example of 1+0 Dual FD mode for link capacity increasing*

This concrete example describes an application where the Design Type 'Design 505', Functional mode '1+0 Dual' and Link diversity 'FD – freq diversity' are selected on both link sides, modulation is 32QAM in BW 60 MHz. The appropriate maximal data speed per each physical data channel (per one ODU pair) is about 227 Mbps. Total throughput over the link is about 227Mbps + 227Mbps = 454 Mbps. The management access is In-Band management described in section 'Management channel configuration options'.

Configuration steps for this 1+0 Dual FD mode are following:

1) In web GUI 'Config->System->Mode' choose design type 'Design 505', Functional mode '1+0 Dual' and Link Diversity 'FD – freq diversity' in both Phoenix G2 IDUs:

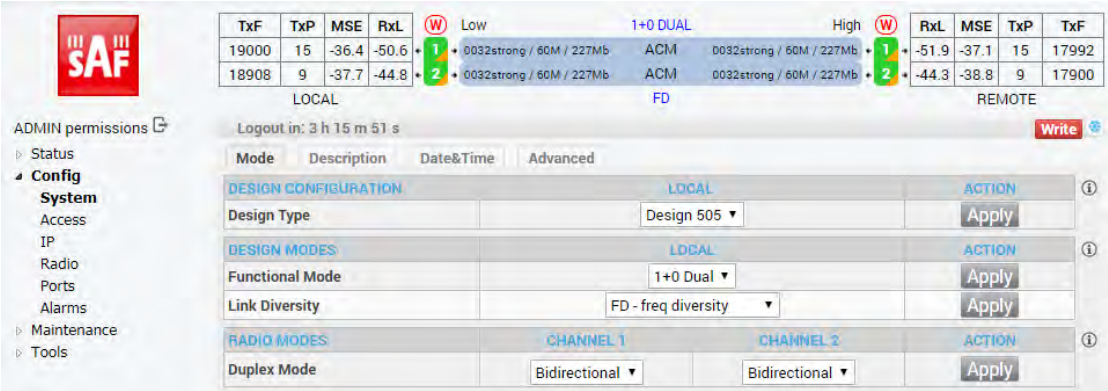


Figure 5.33 *Example of System configuration*

2) In web GUI 'Config->Radio->Parameters' configure basic radio and modem parameters in both Phoenix G2 IDUs. Use different frequency channels for each ODU pair:

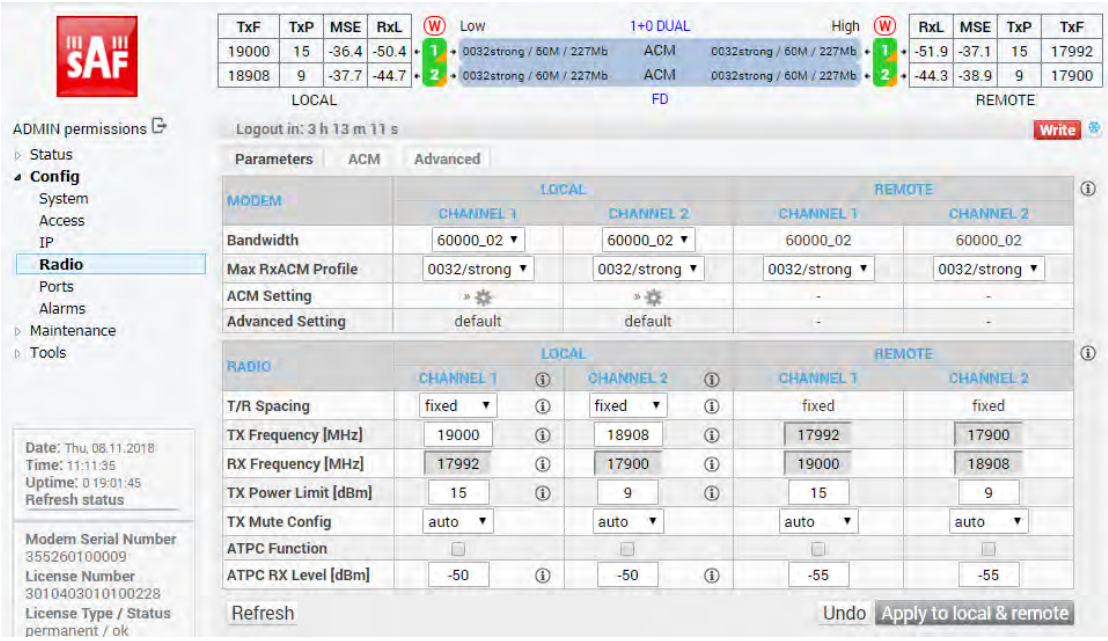


Figure 5.34 *Example of basic Radio parameters configuration*

3) Port group configuration must be done according to the customer requirements. The requirement in this example is to have In-band management which means that the management is accessible via the same port where user traffic is passed through. In this 1+0 Dual FD configuration two separated data streams are used which means that also LAN ports must be separated for user traffic by assigning them into different groups. In this case management port must be allocated in the group with one of both traffic ports (LAN and WAN ports). In the example the first Ethernet data stream will use LAN1 and WANa ports and will be grouped in Group 1, but the second Ethernet data stream will use LAN2 and WANb ports and will be grouped in Group 2. Management port (MNG) will be accessible via LAN3 port and will be added to Group 1 in order to have remote access.

Adding both Ethernet data stream ports (LAN and WAN) in the same one group will create Ethernet loop.

Out-band management is available only for local management access by assigning MNG port and management LAN port (LAN3) to the third group which differs from both traffic port groups. Both WAN ports are assigned to traffic port groups. That is why management in this case will not be available remotely.

Port grouping configuration is available in web GUI '[Config->Ports->EthVLAN](#)' and must be done in both Phoenix G2 IDUs.

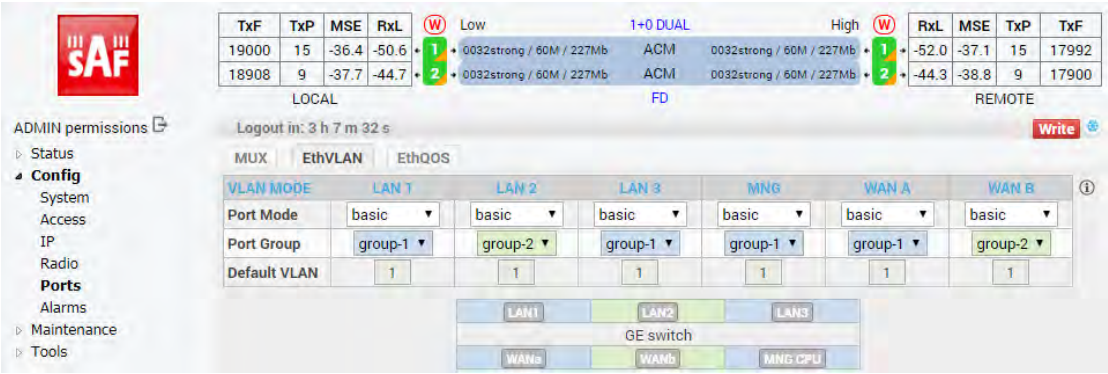


Figure 5.35 *Example of port grouping*

4) In web GUI ‘Config->Ports->MUX’ specify Data channel and port speed for WAN (radio direction) port in both Phoenix G2 IDUs. In the example WANa port is connected to high priority data channel ‘ETH1a’ of the first independent data channel and is set on full speed limit 1000 Mbps, but the WANb port is connected to high priority data channel ‘ETH2a’of the second independent data channel and is set on full speed limit 1000 Mbps.

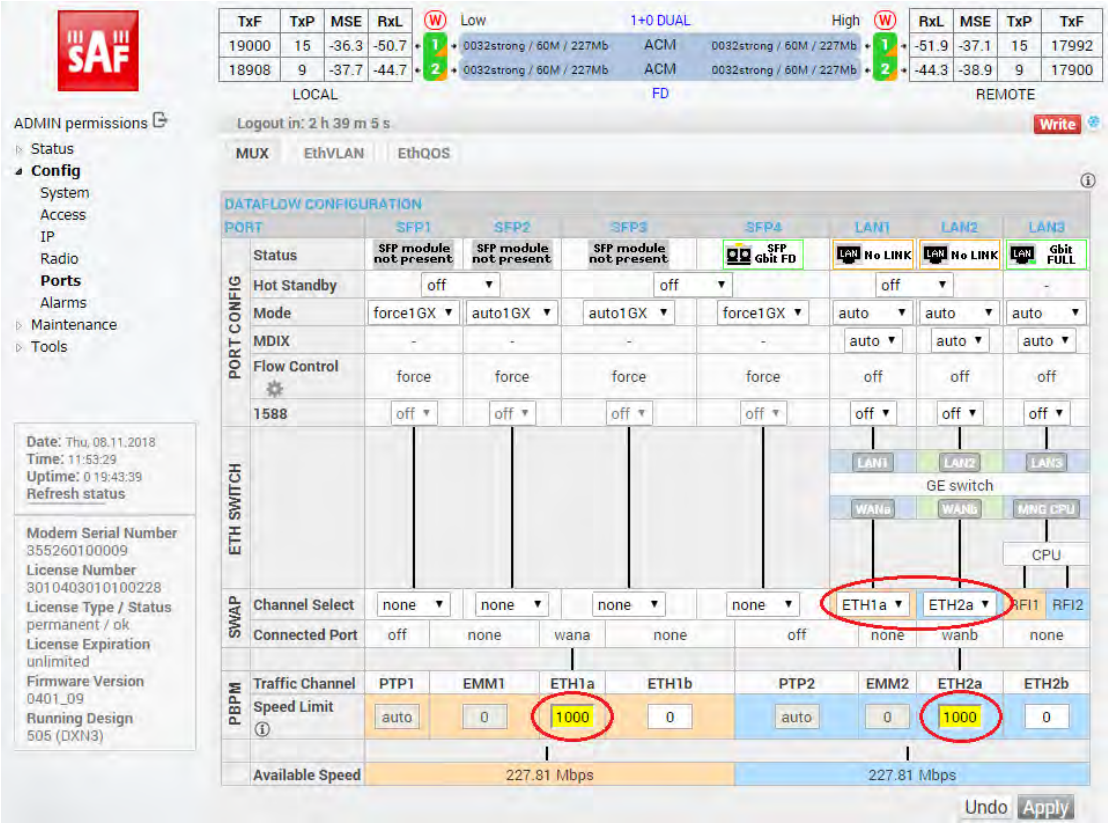


Figure 5.36 *Example of port configuration*

5) In case if EMM module is used, configure it according to EMM configuration description described in section ‘Config->Ports->EMM’ in both Phoenix G2 IDUs.

6) Save new settings by pressing 

button.

The status of 1+0 Dual FD configuration is displayed in the header of the web GUI:

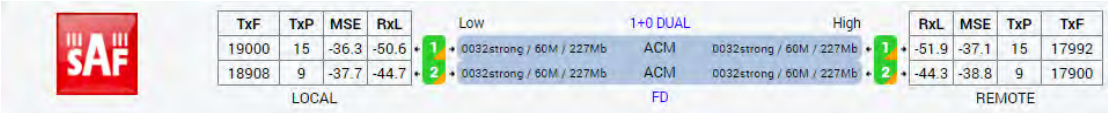


Figure 5.37 *Status of 1+0 Dual FD mode*

Example 7 – 1+0 Dual XPIC connection scheme for link capacity increasing

The 1+0 Dual XPIC (Cross-polar Interference Cancellation) mode is advanced 1+0 mode which allows increasing Ethernet traffic capacity of the link by passing two independent Ethernet data streams over two separated independent physical data channels using two ODU pairs. Both ODU pairs use the same frequency channel in different polarization– one ODU pair works in

Horizontal polarization, the second ODU pair works in Vertical polarization. This configuration can be used for two independent network data passing through the link, internal aggregation is not provided in this configuration. If required, external aggregation can be performed in external network devices. **This scheme requires one Phoenix G2 IDU with connected two ODUs per site**.

In case of link capacity increasing the 1+0 Dual XPIC mode can be used with one antenna and OMT adapter per site, two ODUs are connected to the OMT adapter. Two separated antennas per site can be used as well.

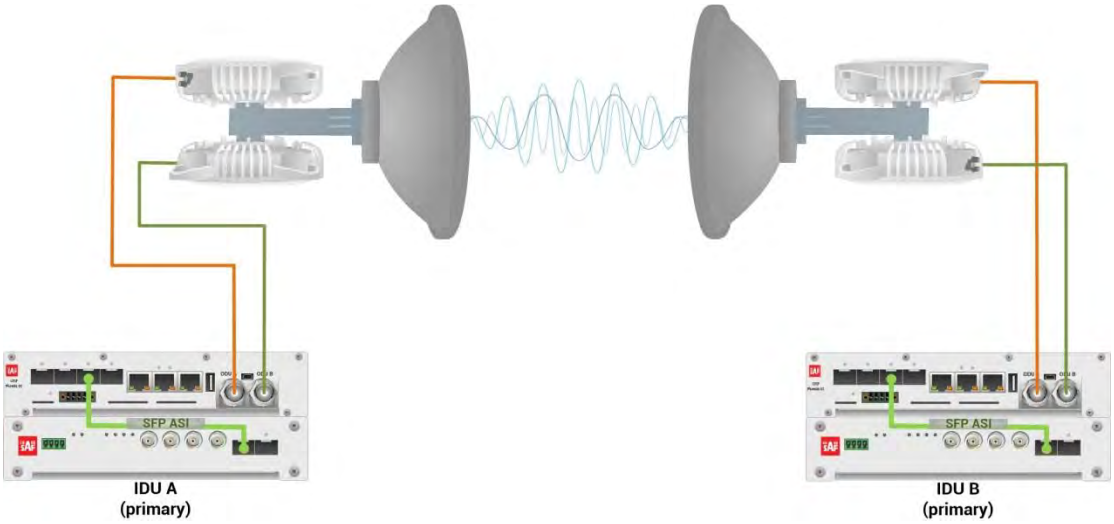


Figure 5.38 *Example of 1+0 Dual XPIC mode for link capacity increasing*

This concrete example describes an application where the Design Type 'Design 505', Functional mode '1+0 Dual' and Link diversity 'XPIC' are selected on both link sides, modulation is 32QAM in BW 60 MHz. The appropriate maximal data speed per each physical data channel (per one ODU pair) is about 227 Mbps. Total throughput over the link is about 227Mbps + 227Mbps = 454 Mbps. The management access is In-Band management described in section '[Management channel configuration options]'.

Configuration steps for this 1+0 Dual XPIC mode are following:

1) In web GUI '[Config->System->Mode]' choose design type 'Design 505', Functional mode '1+0 Dual' and Link Diversity 'XPIC' in both Phoenix G2 IDUs:

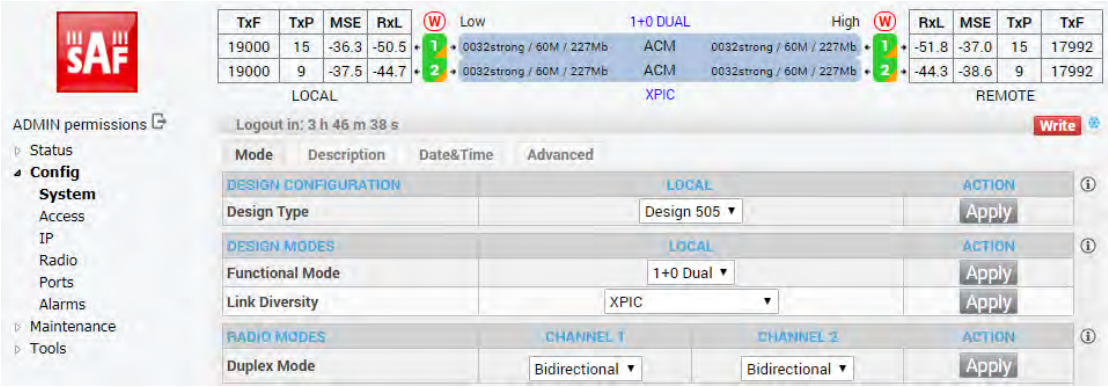


Figure 5.39 *Example of System configuration*

2) In web GUI '[Config->Radio->Parameters]' configure basic radio and modem parameters in both Phoenix G2 IDUs. Use the same frequency channel for both ODU pairs:

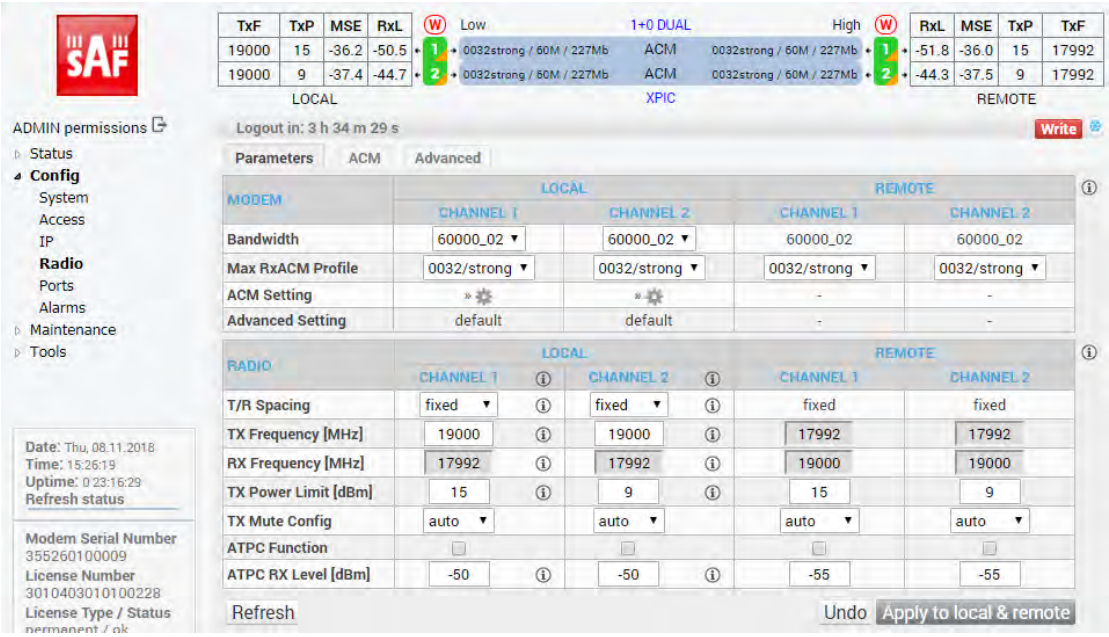


Figure 5.40 *Example of basic Radio parameters configuration*

3) Port group configuration must be done according to the customer requirements. The requirement in this example is to have In-band management which means that the management is accessible via the same port where user traffic is passed through. In this 1+0 Dual XPIC configuration two separated data streams are used which means that also LAN ports must be separated for user traffic by assigning them into different groups. In this case management port must be allocated in the group with one of both traffic ports (LAN and WAN ports). In the example the first Ethernet data stream will use LAN1 and WANa ports and will be grouped in Group 1, but the second Ethernet data stream will use LAN2 and WANb ports and will be grouped in Group 2. Management port (MNG) will be accessible via LAN3 port and will be added to Group 1 in order to have remote access.

Adding both Ethernet data stream ports (LAN and WAN) in the same one group will create Ethernet loop.

Out-band management is available only for local management access by assigning MNG port and management LAN port (LAN3) to the third group which differs from both traffic port groups. Both WAN ports are assigned to traffic port groups. That is why management in this case will not be available remotely.

Port grouping configuration is available in web GUI '[Config->Ports->EthVLAN](#)' and must be done in both Phoenix G2 IDUs.

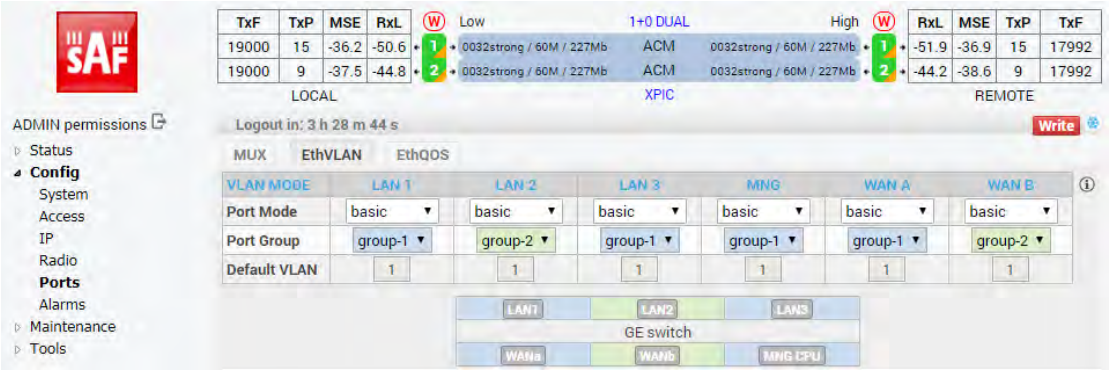


Figure 5.41 *Example of port grouping*

4) In web GUI ‘Config->Ports->MUX’ specify Data channel and port speed for WAN (radio direction) port in both Phoenix G2 IDUs. In the example WANa port is connected to high priority data channel ‘ETH1a’ of the first independent data channel and is set on full speed limit 1000 Mbps, but the WANb port is connected to high priority data channel ‘ETH2a’of the second independent data channel and is set on full speed limit 1000 Mbps.

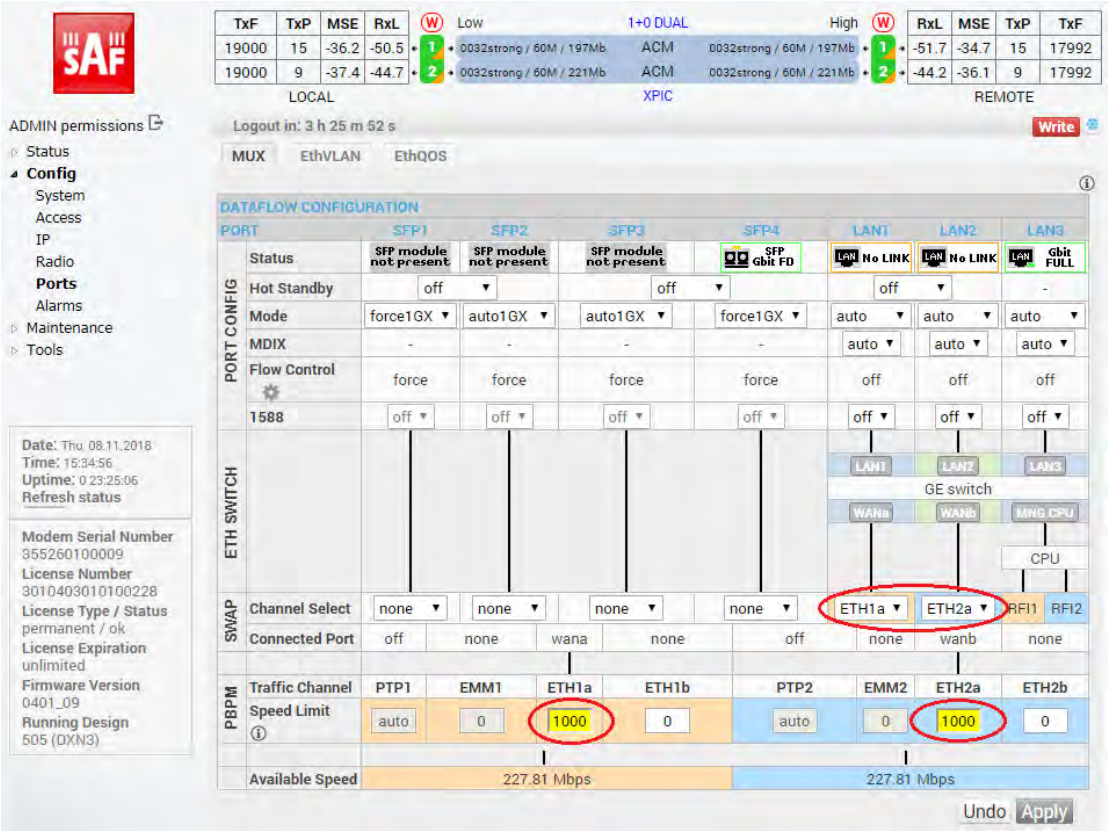
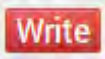


Figure 5.42 *Example of port configuration*

5) In case if EMM module is used, configure it according to EMM configuration description described in section ‘Config->Ports->EMM’ in both Phoenix G2 IDUs.

6) Save new settings by pressing 

button.

The status of 1+0 Dual XPIC configuration is displayed in the header of the web GUI:

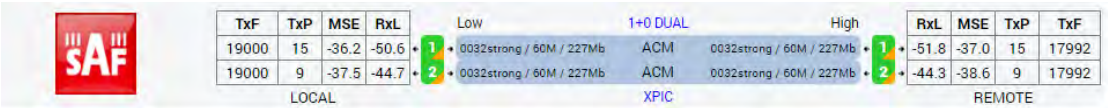


Figure 5.43 *Status of 1+0 Dual XPIC mode*

Example 8 – 1+0 Dual FD repeater connection scheme

The 1+0 Dual FD (Frequency Diversity) mode is advanced 1+0 mode which allows IDU to operate as active repeater. Two ODUs are connected to modems of the single IDU and operates to two different directions.

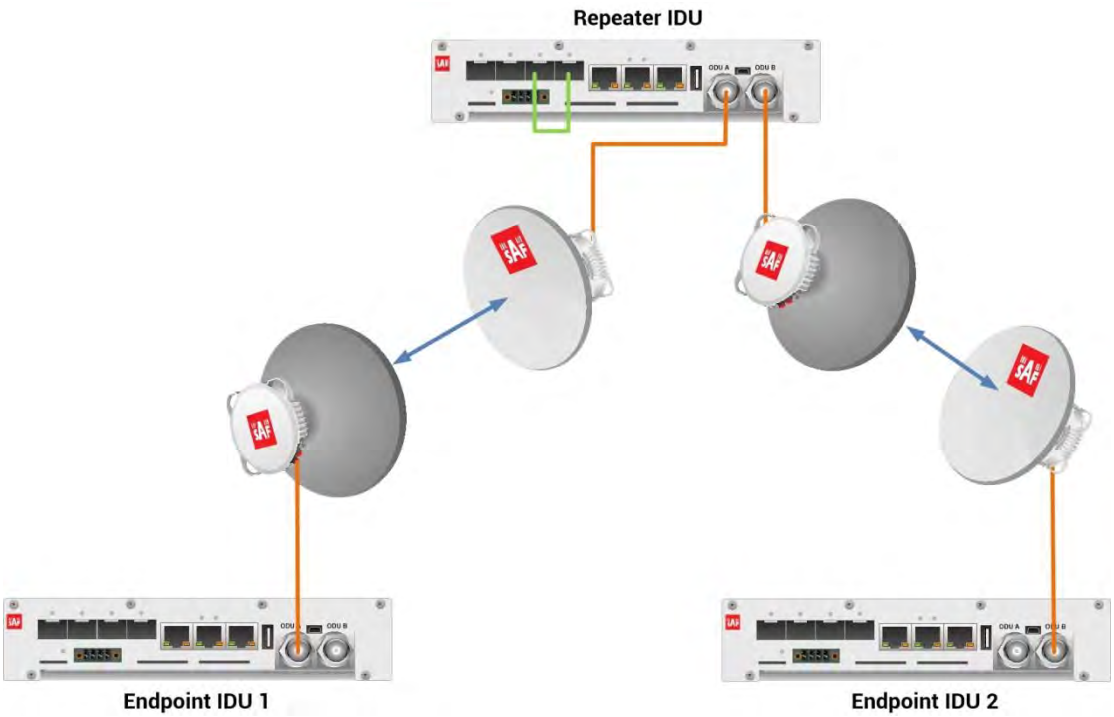


Figure 5.44 *Example of 1+0 Dual FD repeater configuration*

As the 1+0 Dual mode uses two independent physical data channels, the following physical data channel interconnection rule must be observed between Repeater IDU and both Endpoint IDUs: the modem output of the Repeater IDU must be linked only with the same modem output on the remote Endpoint IDUs. In the example the modem output ODU 1 of the Repeater IDU is interconnected with the modem output ODU 1 on the Endpoint IDU 1 (Channel 1), while modem output ODU 2 is interconnected with modem output ODU 2 on the Endpoint IDU 2 (Channel 2).

The 1+0 Dual repeater configuration does not support ASI/E1 EMM traffic.

This concrete example describes an application where the Design Type 'Design 505', Functional mode '1+0 Dual' and Link diversity 'FD – freq diversity' are selected on Repeater IDU; Functional mode '1+0 Ch1' is selected on Endpoint IDU 1; Functional mode '1+0 Ch2' is selected on Endpoint IDU 2. Modulation is 32QAM in BW 28 MHz on all three IDUs. Two independent Ethernet data streams in one physical data channel are passed through the link (between Endpoint IDU1 and Endpoint IDU2), each configured on 20 Mbps.

In the Repeater IDU both Ethernet data streams must be interconnected between physical data channels (Channel 1 between Endpoint IDU 1 and Repeater IDU, Channel 2 between Repeater IDU and Endpoint IDU 2) in order to get Ethernet streams passing from the Endpoint IDU 1 to the Endpoint IDU 2 and back. One Ethernet data stream will be interconnected via built-in switch using both WAN ports which are configured in the same port group, but the second Ethernet data stream will be interconnected via SFP ports which are physically interconnected with optical cable.

The management access is In-Band management described in section 'Management channel configuration options'.

Configuration steps for this 1+0 Dual FD mode are following:

1) In web GUI 'Config->System->Mode' choose design type 'Design 505', Functional mode '1+0 Dual' and Link Diversity 'FD – freq diversity' in Repeater IDU:

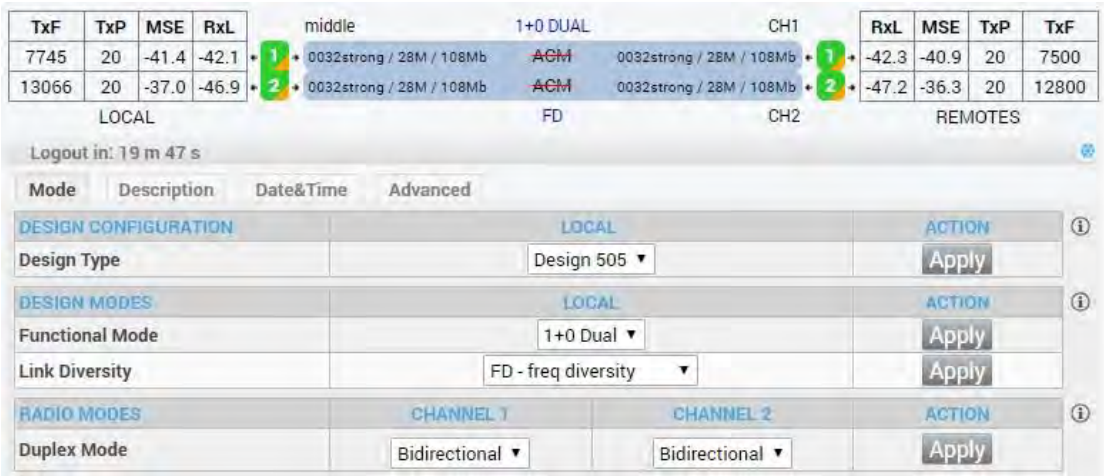


Figure 5.45 *Example of System configuration of Repeater IDU*

2) In web GUI 'Config->System->Mode' choose design type 'Design 505', Functional mode '1+0 Ch1' in Endpoint IDU 1:

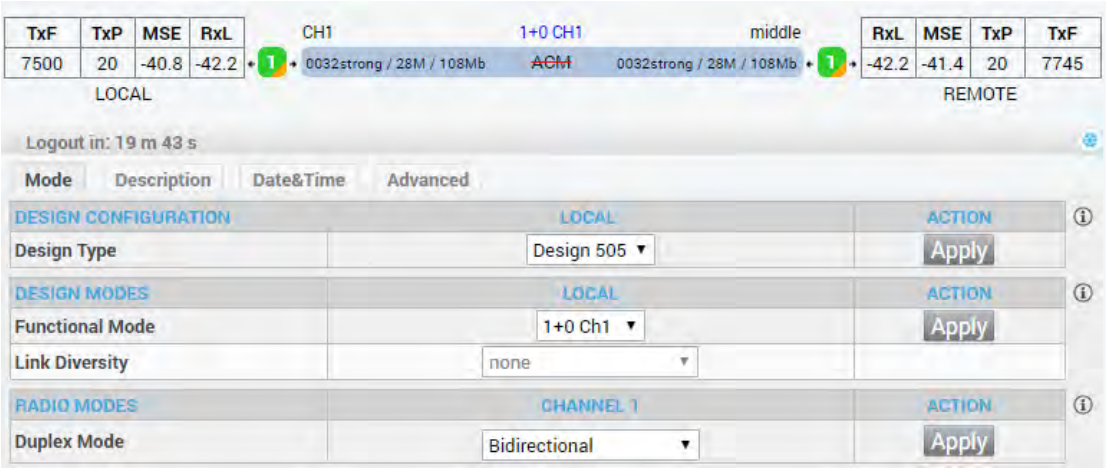


Figure 5.46 *Example of System configuration of Endpoint IDU 1*

3) In web GUI 'Config->System->Mode' choose design type 'Design 505', Functional mode '1+0 Ch2' in Endpoint IDU 2:

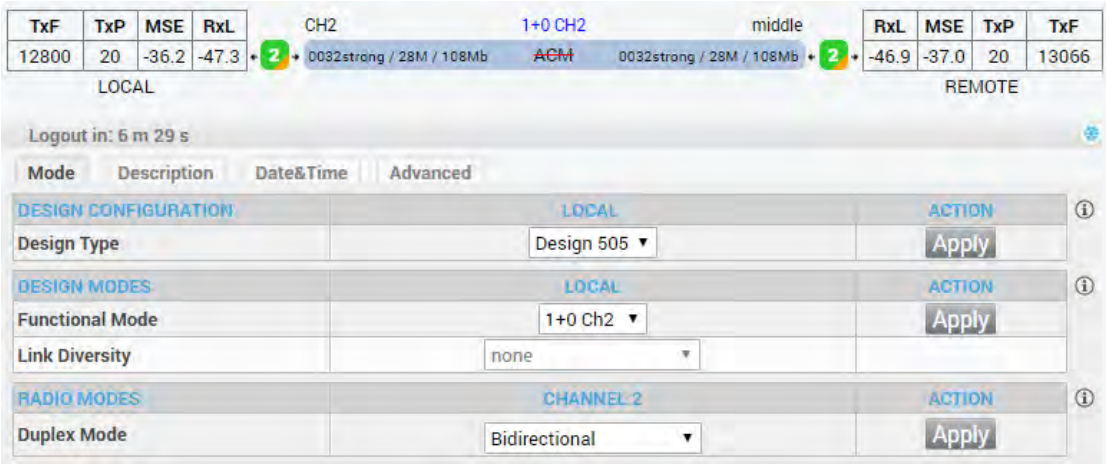


Figure 5.47 *Example of System configuration of Endpoint IDU 2*

4) In web GUI 'Config->Radio->Parameters' configure basic radio and modem parameters of the Repeater IDU:

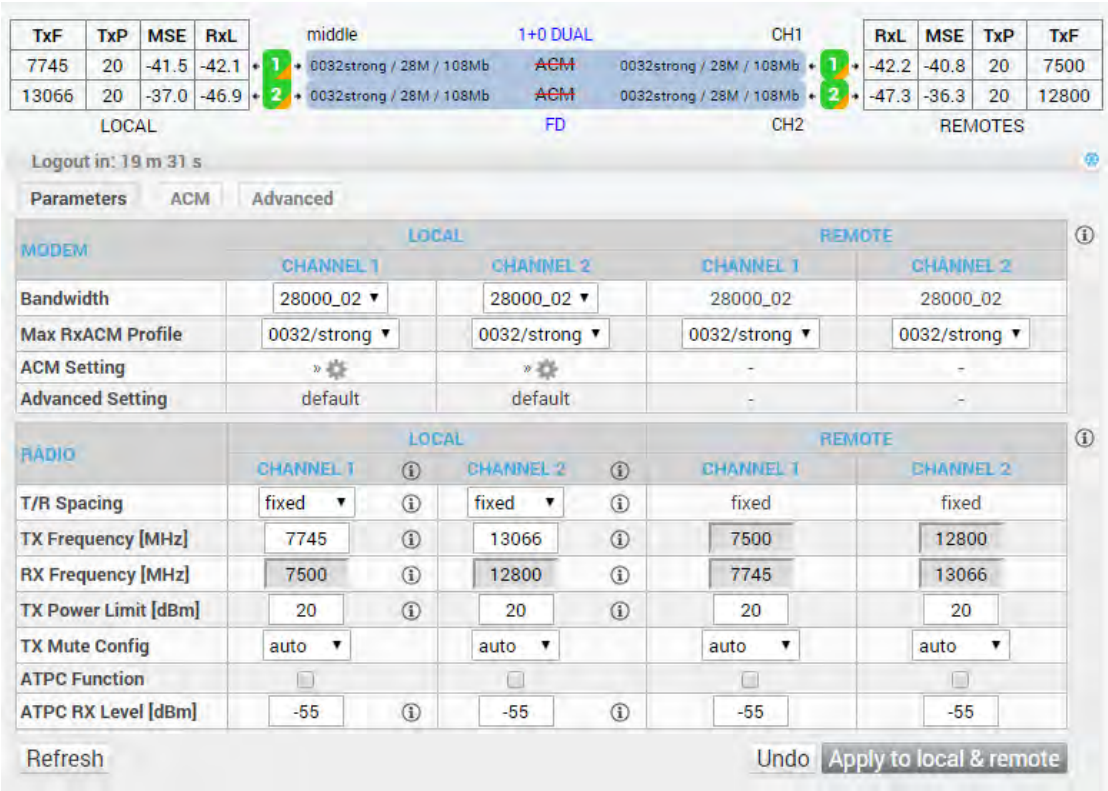


Figure 5.48 *Example of basic Radio parameters configuration of the Repeater IDU*

5) In web GUI 'Config->Radio->Parameters' configure basic radio and modem parameters of the Endpoint IDU 1:

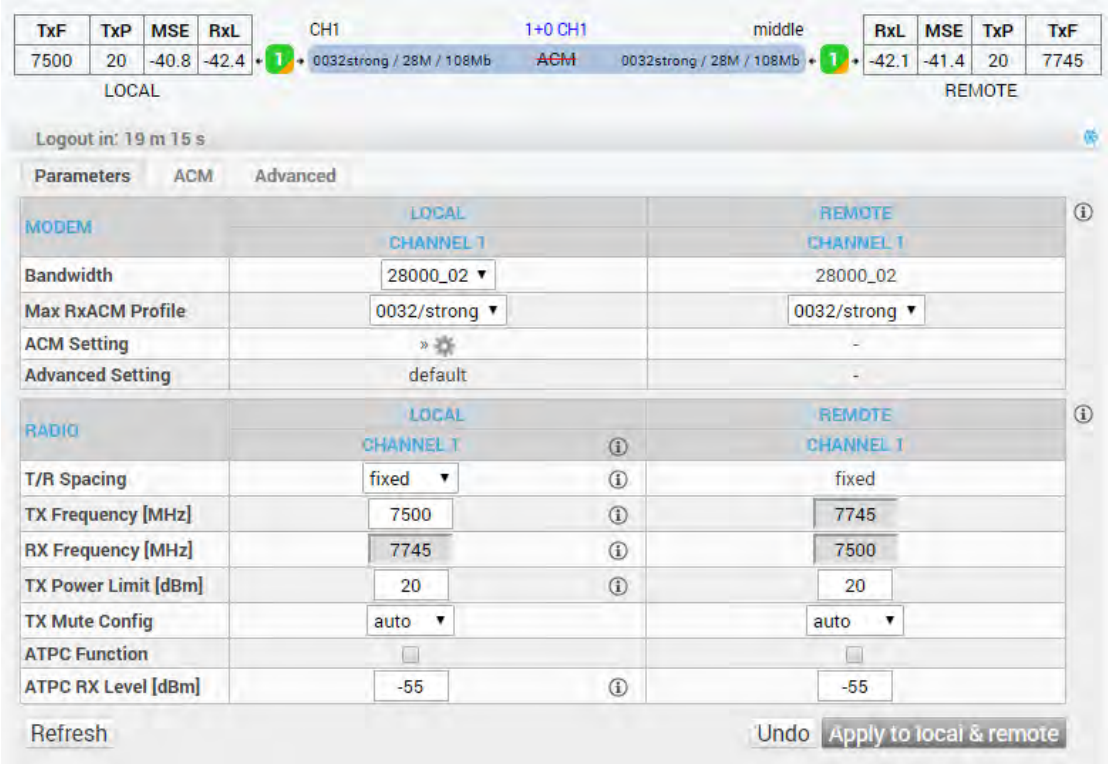


Figure 5.48 *Example of basic Radio parameters configuration of the Endpoint IDU 1*

6) In web GUI 'Config->Radio->Parameters' configure basic radio and modem parameters of the Endpoint IDU 2:

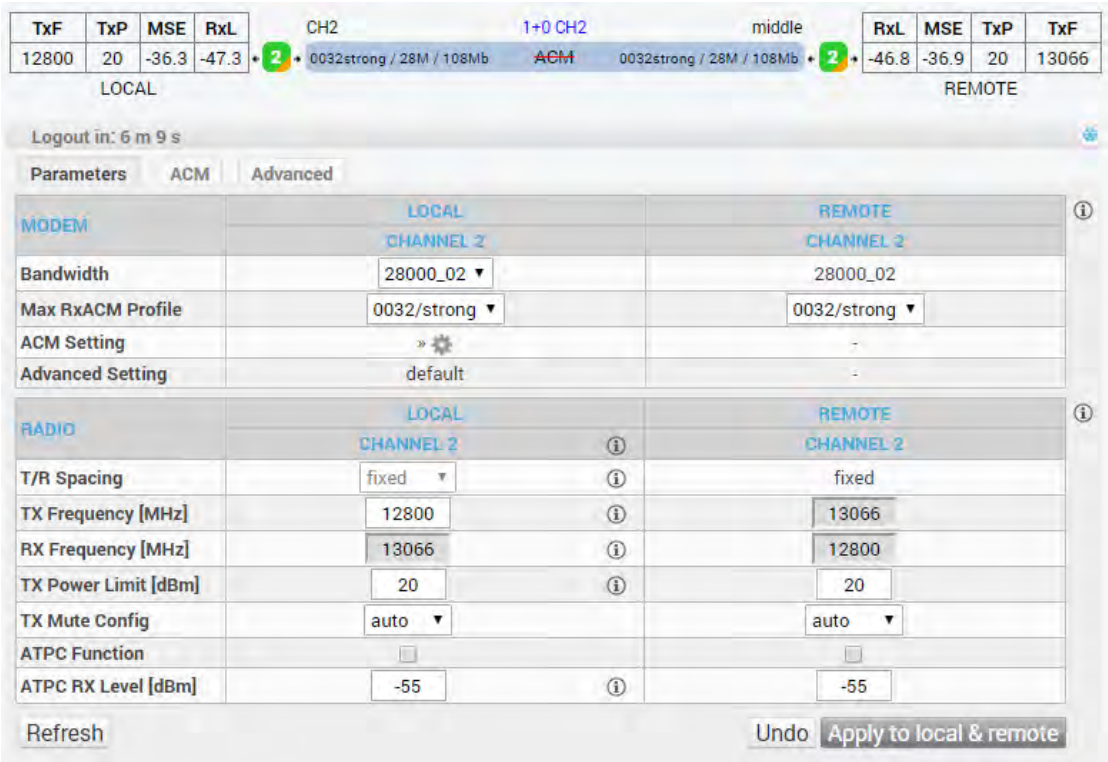


Figure 5.49 *Example of basic Radio parameters configuration of the Endpoint IDU 2*

7) In the repeater IDU, port grouping must be configured in order to fill customer requirement about in-band management and to interconnect one Ethernet data stream between physical channels (Channel 1 and Channel 2). In this case both WAN ports must be grouped in the same one group; also the management (MNG) port and at least one of LAN ports must be connected to the same group in order to have local and remote management access. Other LAN ports also may be added to the same group. In this example all above mentioned ports are added to the Group 1.
Port grouping configuration is available in web GUI 'Config->Ports->EthVLAN':

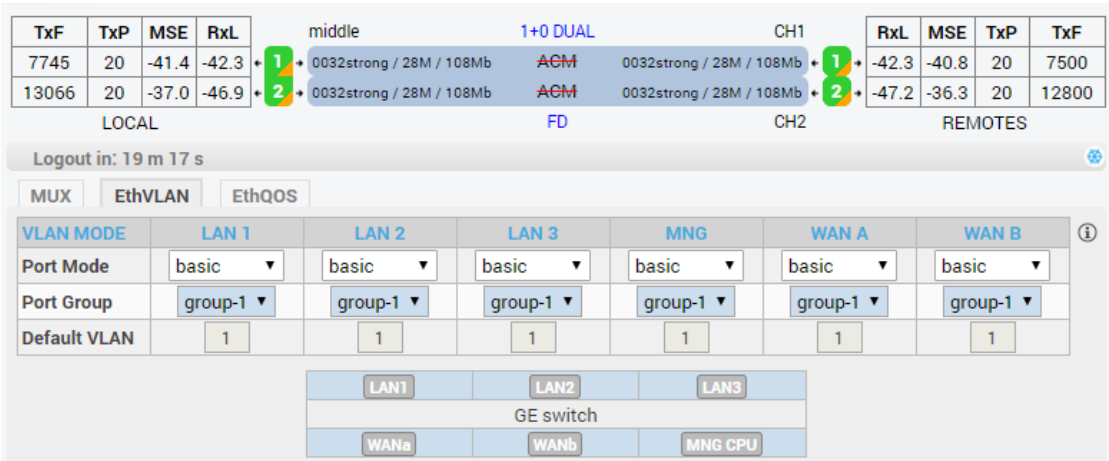


Figure 5.50 *Example of port grouping in the Repeater IDU*

Only one Ethernet data stream can be interconnected between physical data channels in the built-in switch using WAN port grouping. The second Ethernet data stream will be linked between physical data channels via SFP ports outside built-in switch.

8) In the Endpoint IDU 1, port grouping must be configured in order to have in-band management and two separated Ethernet data streams. In the example the first Ethernet data stream will use LAN1 and WANa ports and will be grouped in Group 1, but the second Ethernet data stream will use LAN2 and WANb ports and will be grouped in Group 2. Management port (MNG) will be accessible via LAN3 port and will be added to Group 1 in order to have remote access:

Figure 5.51 *Example of port grouping in the Endpoint IDU 1*

9) In the Endpoint IDU 2, port grouping must be also configured in order to have in-band management and two separated Ethernet data streams. In the example the first Ethernet data stream will use LAN1 and WANa ports and will be grouped in Group 1, but the second Ethernet data stream will use LAN2 and WANb ports and will be grouped in Group 2. Management port (MNG) will be accessible via LAN3 port and will be added to Group 1 in order to have remote access:

Figure 5.52 *Example of port grouping in the Endpoint IDU 2*

10) In the Repeater IDU, in web GUI '[Config->Ports->MUX](#)' configure both Ethernet data stream interconnections between physical data channels (Channel 1 and Channel 2) and port speeds:
   a) The first Ethernet data stream will be set as high priority Ethernet channel (ETH1a from Endpoint IDU1, and ETH2a from Endpoint IDU2). In the example in "Channel Select" drop-down the high priority data channel 'ETH1a' is connected to WANa port and is set on Speed limit 20 Mbps, and 'ETH2a' is connected to the WANb port and also is set on Speed limit 20 Mbps. As both WAN ports are already allocated in the same port group thus the first Ethernet data stream has been interconnected between Channel 1 and Channel 2.

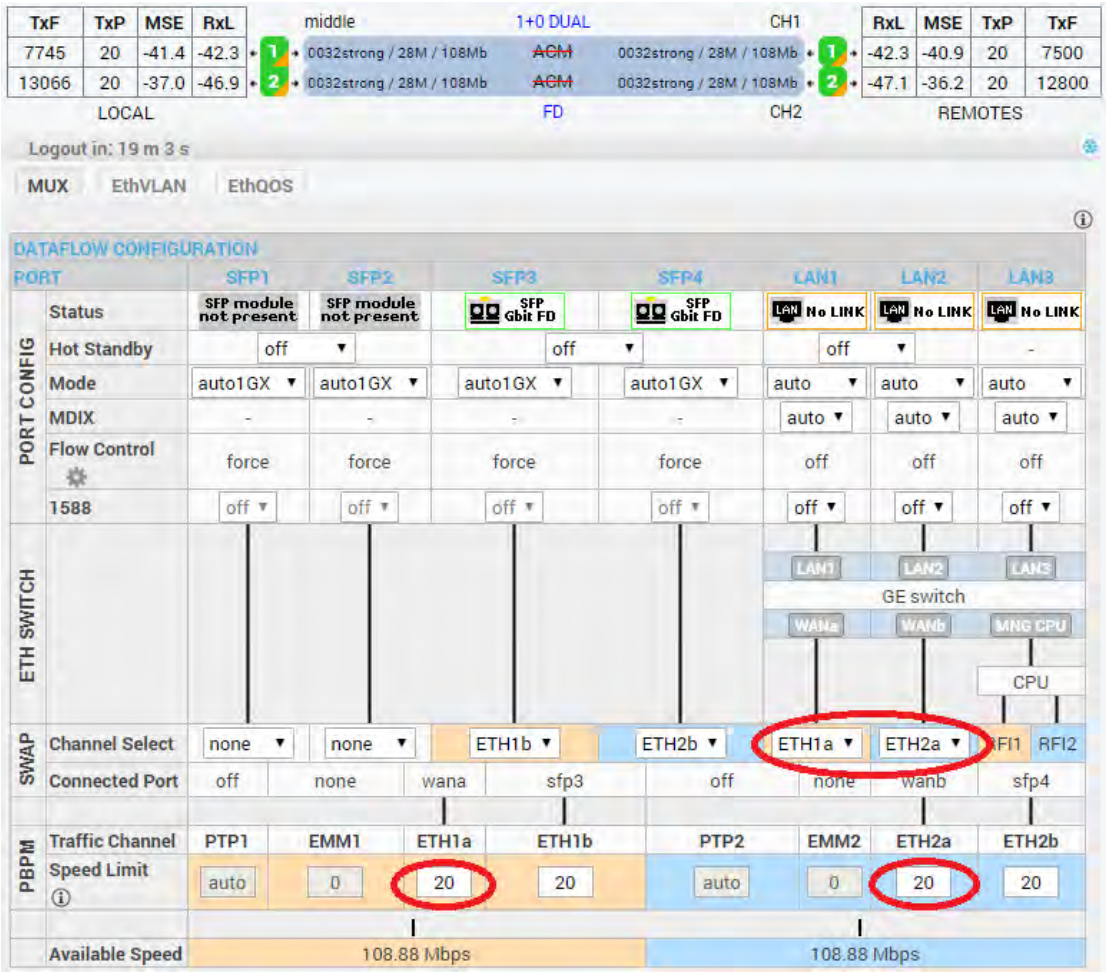


Figure 5.53 *Example of port configuration in Repeater IDU*

b) The second Ethernet data stream will be set as low priority Ethernet channel (ETH1b from Endpoint IDU1, and ETH2b from Endpoint IDU2). In the example in the "Channel Select" drop-down the low priority data channel 'ETH1b' is connected to SFP3 port and is set on Speed limit 20 Mbps, and 'ETH2b' is connected to the SFP4 port and also is set on Speed limit 20 Mbps. In this case in order to interconnect the second Ethernet data stream between Channel 1 and Channel 2 both SFP ports must be interconnected with optical cable externally

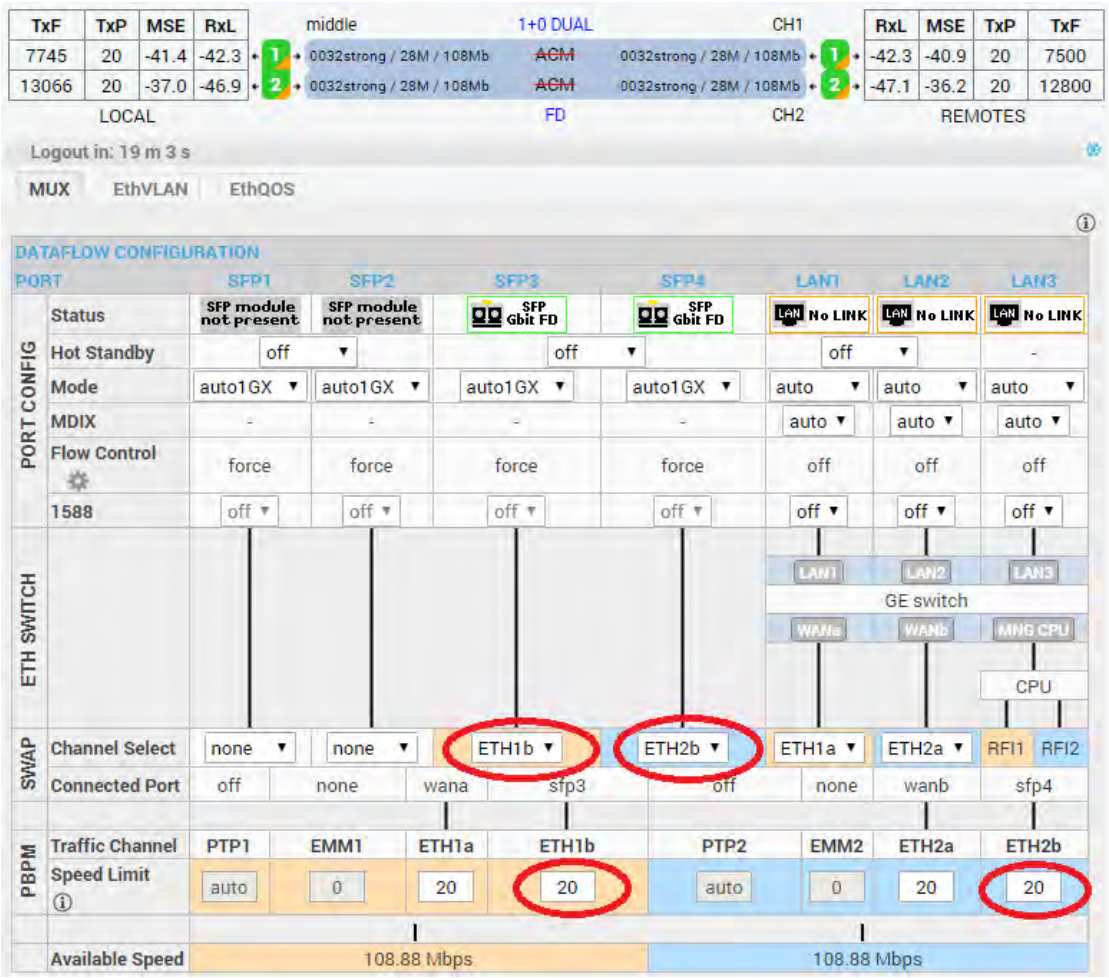


Figure 5.54 *Example of port configuration in Repeater IDU*

11) In the Endpoint IDU 1, in web GUI '[Config->Ports->MUX](#)' specify data channels and ports speeds. In the example the first Ethernet data stream ETH1a (high priority) is connected to WANa port and is set on speed limit 20 Mbps. The second Ethernet data stream ETH1b (low priority) is connected to WANb port and is set on speed limit 20 Mbps

Figure 5.55 *Example of port configuration in Endpoint IDU 1*

12) In the Endpoint IDU 2, in web GUI 'Config->Ports->MUX' specify data channels and ports speeds. In the example the first Ethernet data stream ETH2a (high priority) is connected to WANa port and is set on speed limit 20 Mbps. The second Ethernet data stream ETH2b (low priority) is connected to WANb port and is set on speed limit 20 Mbps