

User manual

Phoenix G2 IDU

VER 1.30

FW 0805_01

Proprietary notice

The information presented in this guide is the property of SAF Tehnika, JSC. No part of this document may be reproduced or transmitted without proper permission from SAF Tehnika, JSC.

The specifications or information contained in this document are subject to change without notice due to continuing introduction of design improvements. If there is any conflict between this document and compliance statements, the latter will supersede this document.

SAF Tehnika, JSC has no liability for typing errors in this document or damages of any kind that result from the use of this document.

To get up to date information about accessories and their availability, please contact sales representative.



IDU does not contain serviceable parts. Warranty will not be applicable in the event IDU has been hermetically unsealed.



SAF Tehnika, JSC is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

Copyright Notice
Copyright © 2024 SAF Tehnika, JSC. All rights reserved.

Contents

Safety Measures 6
Microwave Radiation 6
Chapter 1: OVERVIEW 7
PhoeniX G2 IDU features summary 7
Labelling 9
IDU front panel interfaces and LEDs 11
Basic Application Examples 12
EMM extension modules description 15
ASI EMM extension module 15
E1/T1 EMM extension module 22
Phoenix G2 ODU and IRFU interfaces and ports 28
SP/HP ODU with SAF radio interface 28
SP/HP ODU with SAF2/SAF2R radio interface 30
VHP ODU 31
IRFU with built-in diplexer 32
IRFU without built-in diplexer 34
IBU without active switch 35
IBU with active switch 38
Chapter 2: INSTALLATION 41
Getting started 41
Attaching Phoenix G2 ODU to antenna 42
SP/HP ODU with SAF radio interface 42
VHP and SP/HP ODU with SAF2/SAF2R radio interface 44
IBU installation 49
IBU installation into the rack 49
IBU interconnection with IRFU 49
IBU interconnection with waveguide/antenna 51
Cable requirements 52
Powering Phoenix G2 IDU/ODU 55
Powering External Multiplexer Modules (EMM) 56
Powering Phoenix G2 IRFU 56
Powering active IBU 56
Chapter 3: WEB GUI 57
Initial configuration 57
System requirements 57
Ethernet management connection configuration 57
USB Management connection configuration 58
Accessing PhoeniX G2 IDU Web GUI 58
Web GUI description 59
Button conversion and configuration box description 62
Configuration of basic system parameters 63
Management channel configuration options 65
Status 67
Status → General → Overview 67
Status → General → Ports 68
Status → General → System 69

Status → General → License 70
Status → Events → Actual 71
Status → Events → Historical 71
Status → Events → All 72
Status → Counters → Modem 73
Status → Counters → Traffic 74
Status → Counters → Management 75
Status → Counters → EMM 76
Status → Trends → Actual 77
Status → Trends → Historical 77
Status → Inventory 78
Config 79
Config → System → Mode 79
Config → System → Description 83
Config → System → Time&Date 84
Config → System → Advanced 84
Config → Access → Users 85
Config → Access → Protocols 85
Config → Access → Certs&Keys 86
Config → IP → Addresses 87
Config → IP → SNMP 88
Config → IP → Advanced 90
Config → Radio→ Parameters 91
Config → Radio → ACM 93
Config → Radio → Advanced 94
Config → Ports → MUX 95
Config → Ports → EthVLAN 99
Config → Ports → EMM 102
Config → Alarms → General 105
Config → Alarms → EMM 107
Maintenance 109
Maintenance → Configuration → Save&Run 109
Maintenance → Configuration → Backup&Restore 109
Maintenance → Configuration → Factory default 110
Maintenance → Firmware → Upgrade 111
Maintenance → Files → Exports 112
Maintenance → Files → Upload 113
Maintenance → Logs 113
Maintenance → Troubleshooting → Assistant 114
Maintenance → Troubleshooting → Detail-SYS 115
Maintenance → Troubleshooting → Detail-IF 115
Maintenance → Troubleshooting → Detail-RF 116
Maintenance → Reboot 117
Tools 117
Tools → Terminal 117
Tools → IP Ping 117
Tools → Sp. Analyser 118
Tools → Constellation 119

Chapter 4: COMMAND LINE INTERFACE 121
Connecting to SSH 123
Connecting to Telnet 124
Chapter 5: EXAMPLES 126
Example 1 – Configuration of SFP ports for GE traffic transmission 126
Example 2 – 1+1 HSB/SD mode (Design 505) 128
Example 3 – 1+1 FD mode (Design 505) 131
Example 4 – 2+0 FD mode (Design 505) 134
Example 5 – 2+0 XPIC mode (Design 505) 137
Example 6 – 1+0 Dual FD mode (Design 505) 140
Example 7 – 1+0 Dual XPIC mode (Design 505) 143
Example 8 – 1+0 Star mode (Design 505) 146
Example 9 – 1+1 HSB/SD Dual-band configuration (Design 511) 154
Example 10 – 2+2 FD aggregation HSB/SD protection mode (Design 511) 175
Example 11 – 2+2 FD aggregation FD protection mode (Design 511) 181
Example 12 – 2+2 XPIC aggregation HSB/SD protection mode (Design 511) 188
Example 13 – 2+2 XPIC aggregation FD protection mode (Design 511) 194
Example 14 – 1+1 HSB/SD Full protection mode (Design 511/513) 201
Example 15 – 1+1 FD Full protection mode (Design 511/513) 207
Example 16 – Full protection 1+1 Repeater mode (Design 513) 213
Scenario 1 213
Scenario 2 219
Scenario 3 226
Scenario 4 231
Example 17 – VLAN configuration 238
Example 18 – PTP channel configuration 241
Example 19 – Pri-Sec interconnection (Summed mode) configuration 242
In-band management access: IP traffic 1 + MNG option 243
In-band management access: IP traffic 2 + MNG option 246
Out-band management access 250
Example 20 – ASI traffic retranslation over repeater 254
Appendix A: TECHNICAL SPECIFICATION 257
Appendix B: ASI EMM TECHNICAL SPECIFICATION 261
Appendix C: E1/T1 EMM TECHNICAL SPECIFICATION 262
Appendix D: IRFU TECHNICAL SPECIFICATION 263
ABBREVIATIONS 264

Safety Measures

Following safety measures must be considered when working/using the Phoenix G2 equipment:

- This product is not suitable for use in locations where children are likely to be present
- A suitable and easily accessible disconnecting device or switch must be used to interconnect Power Supply Circuits

Microwave Radiation

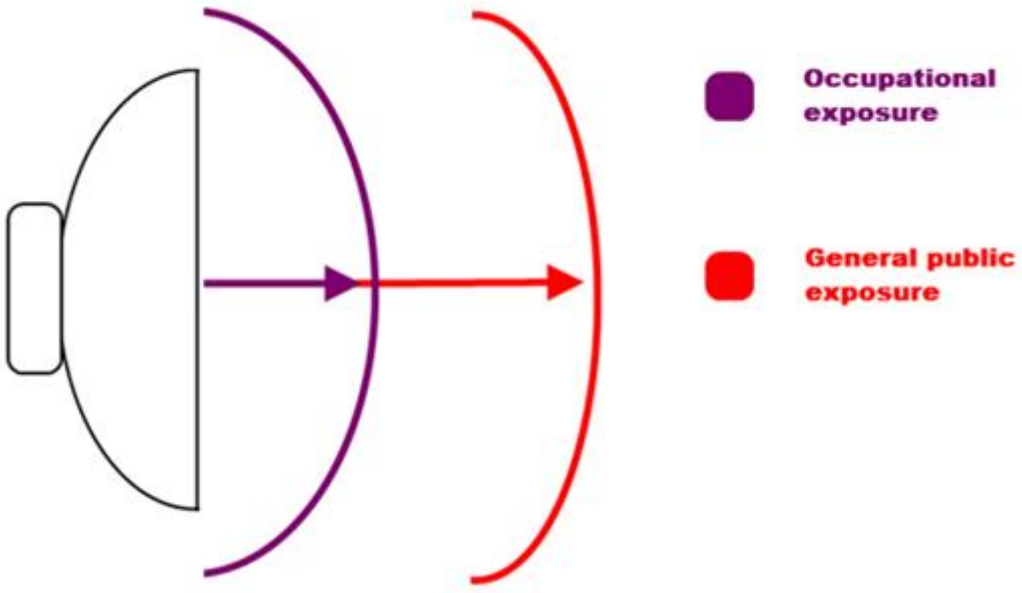


Figure 1 *Microwave radiation exposure diagram*

Phoenix G2 radios conform to both occupational and general public exposure limit guidelines and restrictions to time-varying electric, magnetic and electromagnetic fields which are specified or referred in the documents below:

- 1999/519/EC: Council Recommendation of July 12, 1999, on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz);
- WHO: Environmental Health Criteria 137: ´Electromagnetic Fields (300 Hz to 300 GHz);
- ANSI/IEEE C95.1, 1999: ´IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz;
- BRD, Bundesimmissionsschutzgesetz, 26. BImSchV Verordnung über elektromagnetische Felder;
- Bundesamt für Umwelt, Wald und Landwirtschaft (BUWAL), Bern/Schweiz Schriftenreihe Umwelt Nr. 164, Luft, Mai 1992 ´Messung nichtionisierender elektromagnetischer Strahlung, 1. Teil: Frequenzbereich 100 kHz bis 300 GHz;
- DIN VDE 0848-2, Entwurf, Oktober 1991: ´Sicherheit in elektrischen, magnetischen und elektromagnetischen Feldern, ´Teil 2: Schutz von Personen im Frequenzbereich von 30 kHz bis 300 GHz;
- ENV 50166-2, January 1995 (withdrew in December 1999 by CENELEC) ´Human Exposure to Electromagnetic Fields (10 kHz – 300 GHz)

Chapter 1: OVERVIEW

This document briefly describes the PhoeniX G2 series TDM/ASI/IP split mount system (IDU+ODU) covering the built-in management system, configuration functionality, hardware features, etc.
The Phoenix G2 is a robust and versatile dual-channel Indoor Unit designed for High Capacity point-to-point microwave networks. Two integrated modems in one Indoor Unit provide excellent ability to connect two active ODUs and aggregate or switch the traffic between two links. The device operates with SAF ODUs and allows to build wireless links in protected (hitless 1+1 HSB, SD, FD), aggregate (2+0) and “Dual End Station” configurations. Due to its design and license keys the device is fully scalable and allows a seamless upgrade of transmission capacity, unlock the additional functionality and expand with more interface ports (e.g., E1/T1 for TDM application or DVB-ASI for video broadcasting). The open device architecture is prepared for growing along with customer needs in the future.
The primary traffic interface for PhoeniX G2 split mount system is Gigabit Ethernet. As PhoeniX G2 system is capable of providing bit rate of up to 452Mbps, it is a great addition to SAF portfolio. PhoeniX G2 radio and modem performance allows achieving high system capacity by employing 1024-decision states modulation scheme by user’s choice. Apart from the full system capacity of 452Mbps, it is possible to configure the radio to any of 10, 14, 20, 25, 28, 30, 40, 50, 56 and 60 MHz channels as well as to any of QPSK, 16QAM, 32QAM, 64QAM, 128QAM, 256QAM, 512QAM and 1024QAM modulations, thus providing various capacities to suit particular needs.
SAF Tehnika has employed most modern design solutions and components to create high performance split mount system with low power consumption – 43-85W per system.
PhoeniX G2 system is a perfect building block for any modern future proof wireless network, including mobile service providers, fixed data service operators, enterprise customers, municipal and governmental networks among others.

PhoeniX G2 IDU features summary

Main features:

- Split mount system solution
- 1+0, 1+1 (HSB, FD, SD) and 2+0 configuration schemes
- 1+1 Full protection split mode utilizing two IDU units
- Repeater (East/West) configuration
- Integrated XPIC mechanism
- Capacity: up to 452 Mbps over single channel, 904 Mbps aggregated capacity
- Channel Bandwidth ETSI and ANSI: 7/10/14/20/25/28/30/40/50/56/60 MHz
- Modulations: QPSK/16QAM/32QAM/64QAM/128QAM/256QAM/512QAM/1024QAM
- Interfaces: 10 / 100 / 1000 Eth
- Traffic: Ethernet (4xSFP, 3xLAN), E1 (up to 64E1), ASI (up to 16 ASI streams)
- TDM and ASI port extension by means of “External MUX Module (EMM)”
- Frequency bands: 2.3 / 4 / 6 / 7 / 8 / 10 / 11 / 13 / 15 / 18 / 23 / 26 / 38 GHz



The 2.3 GHz radio unit complies with FCC part 27

- Hitless ACM and ATPC functions
- 802.1Q VLAN support
- AES256 and AES128 encryption



AES-256 encryption is FIPS-197 certified

- PTP 1588v2 synchronization
- Standard management access: HTTPS, SNMP v2&3, Telnet, SSH
- Two integrated wide-band modems in one indoor unit for different Point-to-Point applications
- Single USB port for local management access



For 2.3GHz radio, end-user is responsible for limiting systems E.I.R.P within allowed operational license to be in line with Tx Power plus antenna gain and minus attenuation in cabling between radio and antenna. For example, to assuming the operational license allows 2000W E.I.R.P and radio Tx power is set at 36 dBm and there is 0 dB cable loss between radio and antenna, then antenna max allowed gain is 26.9 dBi.

For compliance with Canada General Population Limit the minimum safe operational distance is 5.5 meters.

IDU mechanical features

- 1U high
- Power consumption <30W
- Dimensions 45x210x240 mm, weight 2.22 kg



Figure 1.1 *Phoenix G2 IDU*

ODUs mechanical features

- Compact unit, 288x288x80mm, 3.5kg (SP/HP ODUs); 280x437x110mm, 7.5kg (VHP ODU)
- 3 handles (SP/HP ODU) and 1handle (VHP ODU) for user convenience
- Safe and easy to use 4 side locking/tightening arrangement
- All connectors on the side of the unit, always at 45° regarding vertical axis for both V and H polarization on the SP/HP ODUs
- All the connectors downwards on the VHP ODU
- Power consumption: 13-39W (SP/HP ODUs) and 39-55W (VHP ODU)



Figure 1.2 *Phoenix G2 ODUs*

IRFU mechanical features

- Indoor radio unit (IDU+IRFU)
- 2U high
- Power consumption: 13-39W

- Dimensions 90x430x260 mm, weight 5.8 kg.



Figure 1.3 *Phoenix G2 IRFU*

Labelling

The label contains the following information (see samples in the picture below):

Product model name (PhoeniX G2 IDU for PhoeniX G2 Indoor Unit, CFIP-18-PhoeniX for 18GHz Outdoor Unit, etc).
Product Number / Model Number (P/N or M/N) (EAGXU002, S18RFU05LA): product/model number contains information about the unit.
Serial Number (355260100007): the serial number uniquely identifies the unit.



Figure 1.4 *Label of the PhoeniX G2 Indoor Unit*

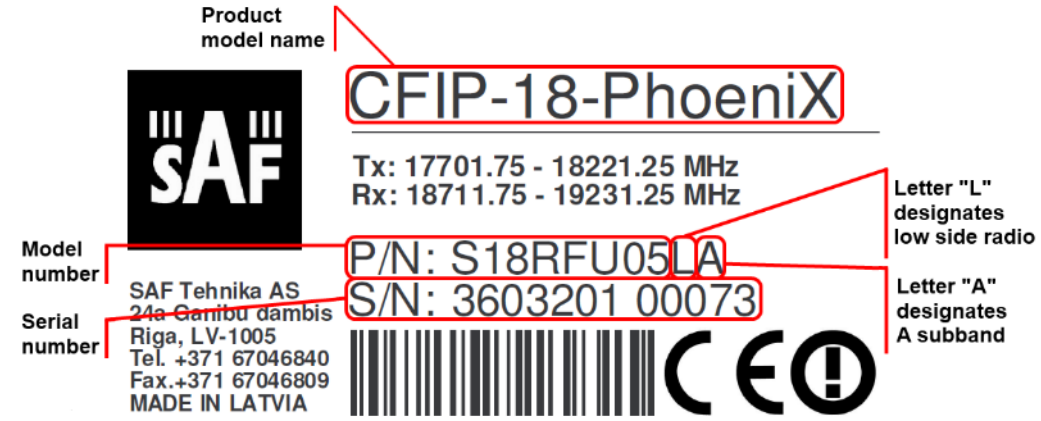


Figure 1.5 *Label of the PhoeniX G2 ODU*

P/N Translation for CFIP PhoeniX G2 ODU:

- “S” designates CFIP split mount series product;
- “18” designates Frequency range (18 GHz) of the Unit;
- “RF” designates standard power radio;
- “U” designates unified band ODU operating 7 - 60MHz;
- “05” designates the version number of the Unit;
- “L” designates the band side in which ODU operates (H, L);
- “A” designates the subband in which ODU operates (A, B, C).

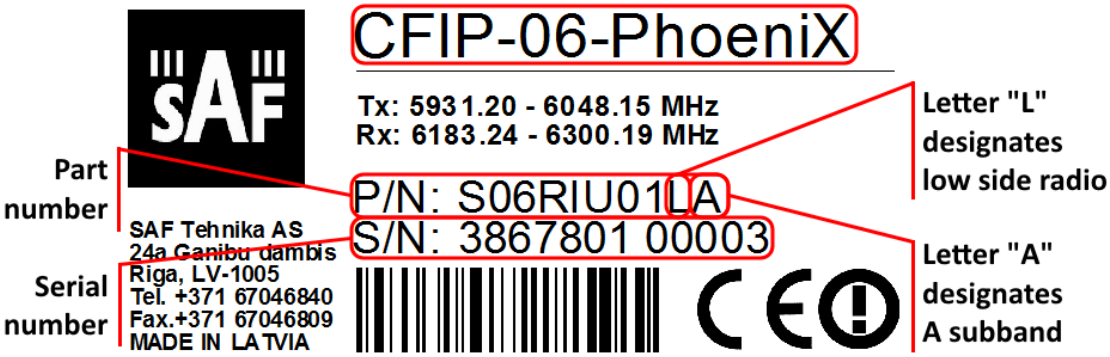


Figure 1.6 *Label of the PhoeniX G2 IRFU*

P/N Translation for CFIP PhoeniX G2 IRFU:

- “S” designates CFIP split mount series product;
- “06” designates Frequency range (6 GHz) of the Unit;
- “RI” designates IRFU radio;
- “U” designates unified band radio operating 7 - 60MHz;
- “01” designates the version number of the Unit;
- “L” designates the band side in which ODU operates (H, L);
- “A” designates the subband in which ODU operates (A, B, C).

IDU front panel interfaces and LEDs

Phoenix G2 IDU has following interfaces:

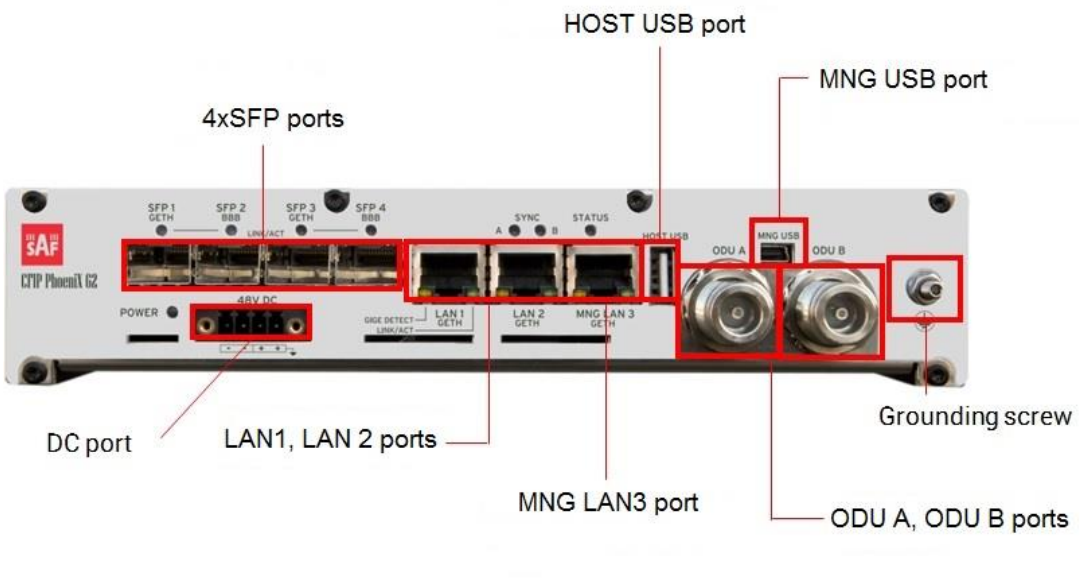


Figure 1.7 *PhoeniX G2 IDU interfaces*

DC port

48V power supply connection. Input DC voltage operating range is -40.5V to -57V (max current up to 3A). 4-wire DC power connector with screw terminals included. Polarity layout indicated on the front panel. Any 2 wire power cable of good quality which fits well in SAF Tehnika's supplied 4 pole "screw on" power connector could be used.

4xSFP ports

SFP slots 1 to 4 for Gigabit Ethernet traffic. Any type of SFP modules can be used (Single-mode or Multi-mode optical fibre). SFP ports are used also for interconnecting IDUs in case of 1+1 full protection configuration, and for IDU interconnection with EMM modules. 2.5 Gbps optical fibre cable and SFP modules must be used to interconnect Phoenix G2 IDUs in 1+1 full protection mode. 1 Gbps optical fibre cable and SFP modules can be used to interconnect Phoenix G2 IDU with EMM modules. the length of optical fibre cable is limited by sensitivity of SFP module. The SFP ports which are not connected must be disabled.

LAN1, LAN2 ports

10/100/1000Base-Tx Ethernet traffic ports (RJ-45). Recommended cable as minimum is unshielded twisted pair Ethernet cable Cat5. The maximum cable length is 100 meters.

MNG LAN3 port

10/100/1000Base-Tx port, which is out-of-band management by default and provides access to the management via web GUI, Telnet or SSH communication facilities. It can be re-configured for traffic purposes as well

HOST USB port

USB port reserved for flash memory

MNG USB port

USB mini port dedicated for local management access via its own IP address.

ODU A, ODU B ports

N-type female 50Ω coaxial ports for connecting ODUs. Any type of 50 Ω coaxial cable of good quality can be used to interconnect the Phoenix G2 IDU and ODUs. The cable should be equipped with N–type male connectors on each end.

Grounding screw

Grounding screw for equipment grounding. The equipment grounding can be done by connecting it to the grounding point of the rack, or directly to the grounding point in the equipment room. The recommended minimum grounding cable wire cross-section must be 2.5 mm2 and the recommended maximum length of the grounding cable is 1 m.

Phoenix G2 IDU front panel alarm LED indications:

LED name	Description
SYNC (A,B)	**Orange –** OK, synchronization of link (A and/or B) established **Orange blinks –** loss of synchronization
STATUS	**Orange –** OK, no alarms present **Orange blinks –** one or several alarms are active
SFP (1-4)	**Orange –** SFP port connected **Off –** SFP port not connected
Power	**Green** – power supply is OK

Ethernet RJ-45 connector LED indications:

LED color	Description
Yellow	**ON** – link speed is 1000Mbps/s **OFF** – link speed is 100Mbps/s
Green	**ON –** Ethernet link is up **Blinking –** activity on port's egress/ingress directions

Basic Application Examples

PhoeniX G2 1+0 configuration:

- Basic split-mount 1+0 system with up to 452 Mbps Ethernet

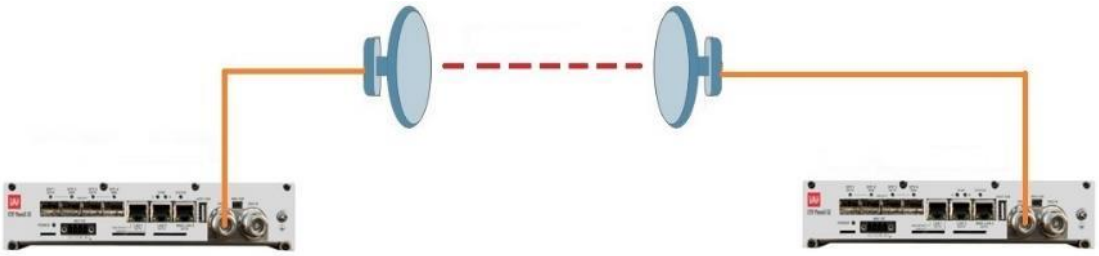


Figure 1.8 *PhoeniX G2 1+0 configuration*

PhoeniX G2 1+0 Star (Repeater) configuration:

- Dual-core modem allows to use one IDU as repeater node
- Both ODUs are working to different directions (East/West)



Figure 1.9 *PhoeniX G2 1+0 Repeater configuration*

PhoeniX G2 1+1 Frequency Diversity (FD):

- FD protected (1+1) configuration is used with single antenna and OMT (orthomode transducer) or a coupler at each side of the link
- Each pair of ODUs utilizes its own frequency channel (f_{low}, f_{high}, f'_{low}, f'_{high})
- The outgoing (Tx) traffic at each site is passed to both ODUs, and both are always transmitting
- The incoming (Rx) traffic is picked from one of the ODUs
- 1+1 configuration provides hardware redundancy and mitigates multipath fading
- Both Tx and Rx switching is hitless

PhoeniX G2 1+1 Hot Standby (HSB):

- HSB protected (1+1) configuration is used with single antenna and a coupler at each side of the link
- Both the incoming (Rx) and outgoing (Tx) traffic is switched to either one link or other, only single ODU at each side is transmitting
- Protects modem and radio from failure

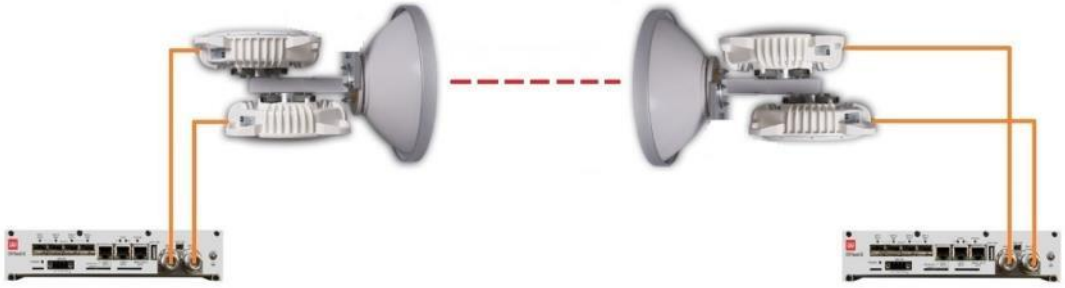


Figure 1.10 *PhoeniX G2 1+1 FD and HSB configuration with coupler*

PhoeniX G2 1+1 Space Diversity (SD):

- SD protected (1+1) configuration is used with two antennas at each side of the link
- Both the incoming (Rx) and outgoing (Tx) traffic is switched to either one link or other, only single ODU at each side is transmitting
- In Space Diversity mode antennas are located 10-12 meters apart hence allows avoiding frequency selective fading - multipath (e.g. reflection over water, air refraction, etc.)
- Rx switching is hitless , Tx switching <50ms

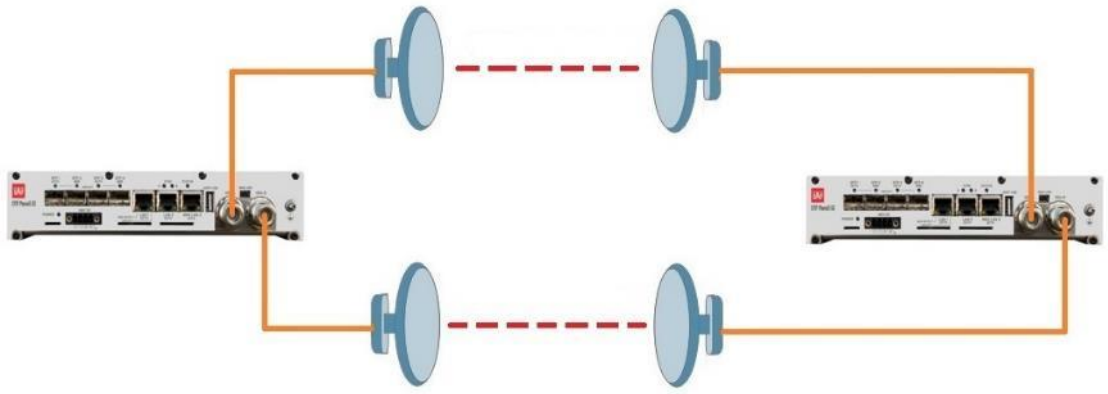


Figure 1.11 *PhoeniX G2 1+1 SD configuration*

PhoeniX G2 1+1 Full protection configuration:

- 1+1 HSB, FD and SD full protection is provided. SD supports only fixed hot-swap role – primary or secondary
- This protection type protects the link also against IDU, power supply and interface failures
- In case of protection, when the Primary link fails, the secondary re-configures itself to the Primary role

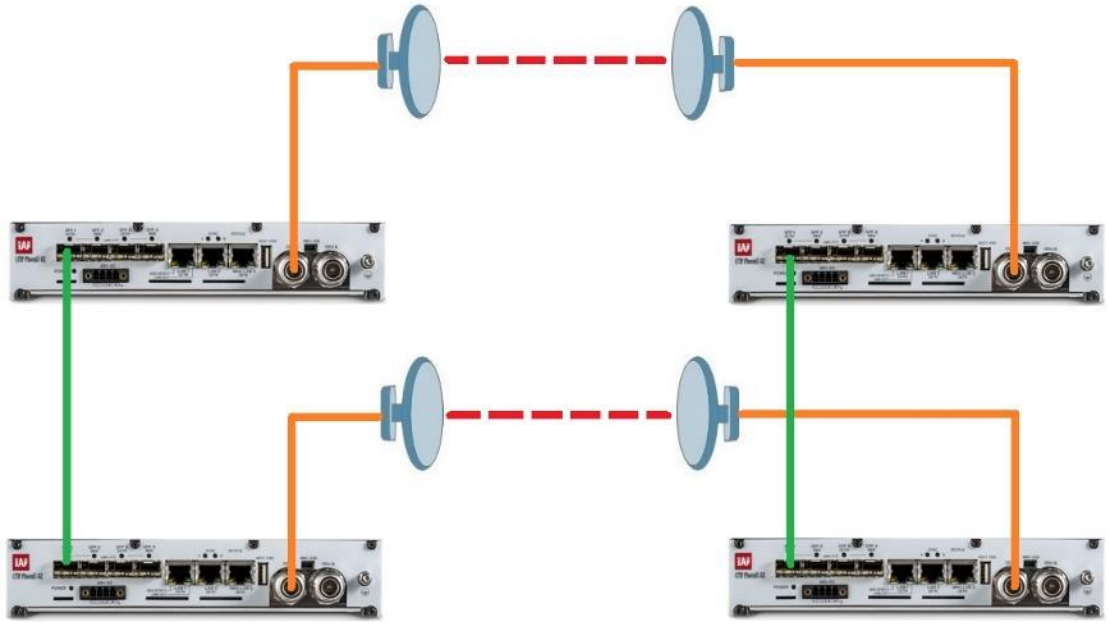


Figure 1.12 *PhoeniX G2 1+1 full protection configuration*

2.5 Gbps SFP modules must be used for both IDU FO interconnection (P/N I0ASMK02 optical cable kit can be used for that purpose). In Design Type 511 both SFP ports work in "Forced 2G5" mode.

PhoeniX G2 2+0/2+0 XPIC configurations:

- 2+0 configuration is used to aggregate payload traffic (capacity doubling). In this case 2 frequency channels are required
- 2+0 XPIC configuration is used to aggregate payload traffic using 1 frequency channel in both polarizations Vertical and Horizontal simultaneously

- Layer 1Link bonding is supported as aggregation technique

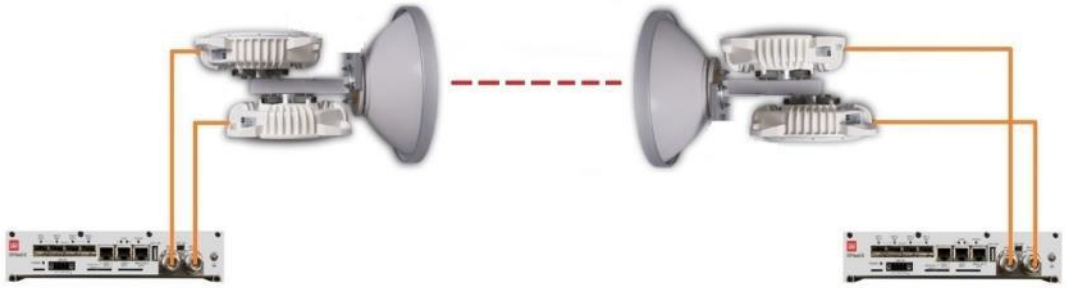


Figure 1.13 *PhoeniX G2 2+0/2+0 XPIC configurations*

PhoeniX G2 2+2 FD/2+2 XPIC configurations:

- 2+2 FD configuration is used to aggregate payload traffic (capacity doubling) using 2 frequency pairs. HSB/SD and FD protection is provided for the aggregated links.
- 2+2 XPIC configuration is used to aggregate payload traffic using 1 frequency channel in both polarizations Vertical and Horizontal simultaneously. HSB/SD and FD protection is provided for the aggregated links.
- Layer 1Link bonding is supported as aggregation technique

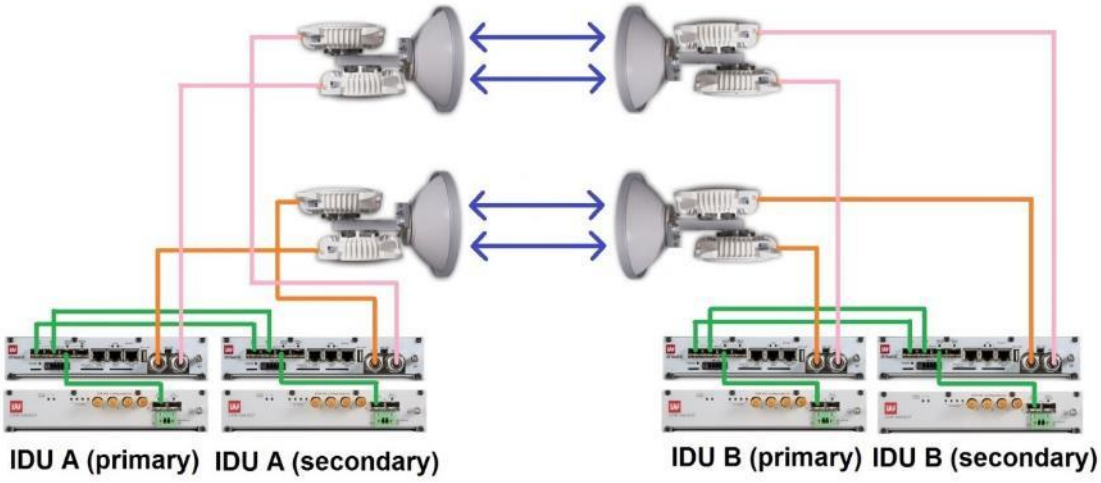


Figure 1.14 *PhoeniX G2 2+2 FD/2+2 XPIC configurations*

Both IDUs in each side of the link are interconnected with 2 optical cables on ports SFP1 and SFP2. 2.5 GB SFP modules must be used for this interconnection. P/N I0ASMK02 optical cable kit can be used for that purpose. SFP3 or SFP4 ports can be used for the IDU interconnection with EMM modules.

EMM extension modules description

ASI EMM extension module

The ASI EMM extension module provides ASI interface extension for Phoenix G2 IDUs. The ASI EMM module multiplexes up to 4 ASI channels into the compact stream which is directed

over the fibre optic (FO) connection to/from the Phoenix G2 IDU. The ASI EMM module features 4 x ASI built-in ports (one BNC per ASI channel) and 2 x SFP 1000Base-SX ports.

The compact, simple to configure, and easily scalable design enables cascading with other EMM extension devices (e.g. ASI EMM and/or E1/T1 EMM). The configuration is performed in the web GUI of the IDU, in section *Config → Ports → EMM*.

Maximum speed for single ASI channel is 216 Mbps. The actual ASI channel speed is auto-detected by the system and is displayed in *Config → Ports → MUX* section.

Each ASI channel can be independently configured into Tx or Rx mode. Following port combinations are possible:

- 4x ASI Tx (unidirectional)
- 3x ASI Tx and 1x ASI Rx (bidirectional)
- 2x ASI Tx and 2x ASI Rx (bidirectional)
- 1x ASI Tx and 3x ASI Rx (bidirectional)
- 4x ASI Rx (unidirectional)

Up to 4 EMM modules can be connected into the cascade and thus get the maximum quantity of external ports (ASI EMM and E1/T1 EMM modules combination is possible). Maximum 4 EMM modules can be cascaded and in case of ASI EMM modules the maximum count of ASI channels is 16. SFP 1000Base-SX on the left side **SFP 2 UPLINK 2** is dedicated for the modules interconnection into cascade. The configuration of all EMM modules is performed from the web GUI of the IDU.

ASI EMM extension module has following interfaces/connectors:



Figure 1.15 *ASI EMM extension module interfaces*

4xDVB ASI ports

Four configurable Input / Output DVB-ASI ports (75 Ohm). The 75 Ohm double shielded coaxial cable with BNC connectors is recommended to use for connection to ASI ports. Allowable maximum attenuation in the cable is 20 dB. The ASI ports which are left disconnected must be set in Rx mode.

SFP 1 UPLINK 1

Primary SFP port reserved for connection to the IDU or to primary EMM extension module in EMM extension module chain.

SFP 2 UPLINK 2

Secondary SFP port reserved for connection to secondary / next EMM extension module in EMM module chain or for connection to relay IDU in add/drop configuration.

DC port

48V power supply connection. Input DC voltage operating range is -20V to -72V (max current up to 3A). 2-wire DC power connector with screw terminals included. Polarity layout indicated on the front panel. Any 2 wire power cable of good quality which fits well in SAF Tehnika's supplied 2 pole "screw on" power connector could be used.

Grounding screw

Grounding screw for equipment grounding. The equipment grounding can be done by connecting it to the grounding point of the rack, or directly to the grounding point in the equipment room. The recommended minimum grounding cable wire cross-section must be 2.5 mm2 and the recommended maximum length of the grounding cable is 1 m.

ASI EMM module front panel alarm LED indications:

LED name	Description
STATUS	**Orange –** OK, module enabled, proper communication with the IDU **Orange blinks –** WARNING, module is not enabled in the system or no communication with IDU, or configuration is not finished yet **Off** – ERROR, firmware is not loaded into EMM module HW
POWER	**Green –** power supply is OK **Off** – no power supply
SFP 1/2 LINK	**Orange blinks –** signal detected and synchronized, valid communication with the IDU **Off –** no correct signal detected
ASI STATUS	***ASI port in Tx mode:*** **Orange blinks –** ASI signal is presented, sending the data **Off** – no data (IDLE status) ***ASI port in Rx mode:*** **Orange** – signal detected, but its status is IDLE or Nosync mode **Orange blinks –** incoming ASI signal **Off** – no ingress signal detected

Interconnection of Phoenix G2 IDU and ASI EMM module must be done using optical cable and SFP modules (P/N I0ASMK02 optical cable kit can be used for that purpose). For 1+0 and 2+0 configurations any of all 4 SFP ports on the IDU can be used for connection to EMM module. In 1+1 full redundancy configuration SFP ports 3 and 4 can be used to connect to EMM module. On EMM module SFP port 1 can be used to connect to Phoenix G2 IDU and SFP port 2 must be used to connect to the next cascaded EMM module.

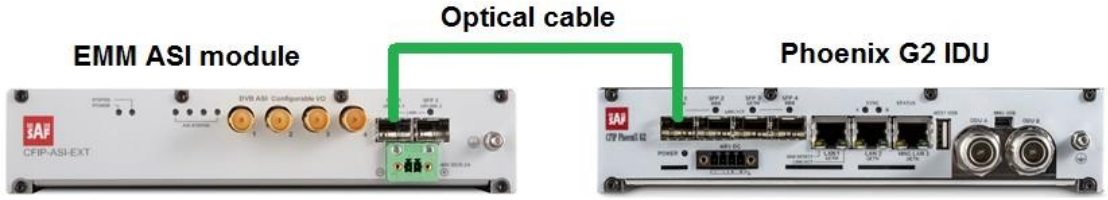


Figure 1.16 *Phoenix G2 IDU and ASI EMM module interconnection*

Application of 1+0 link connection with ASI EMM modules:

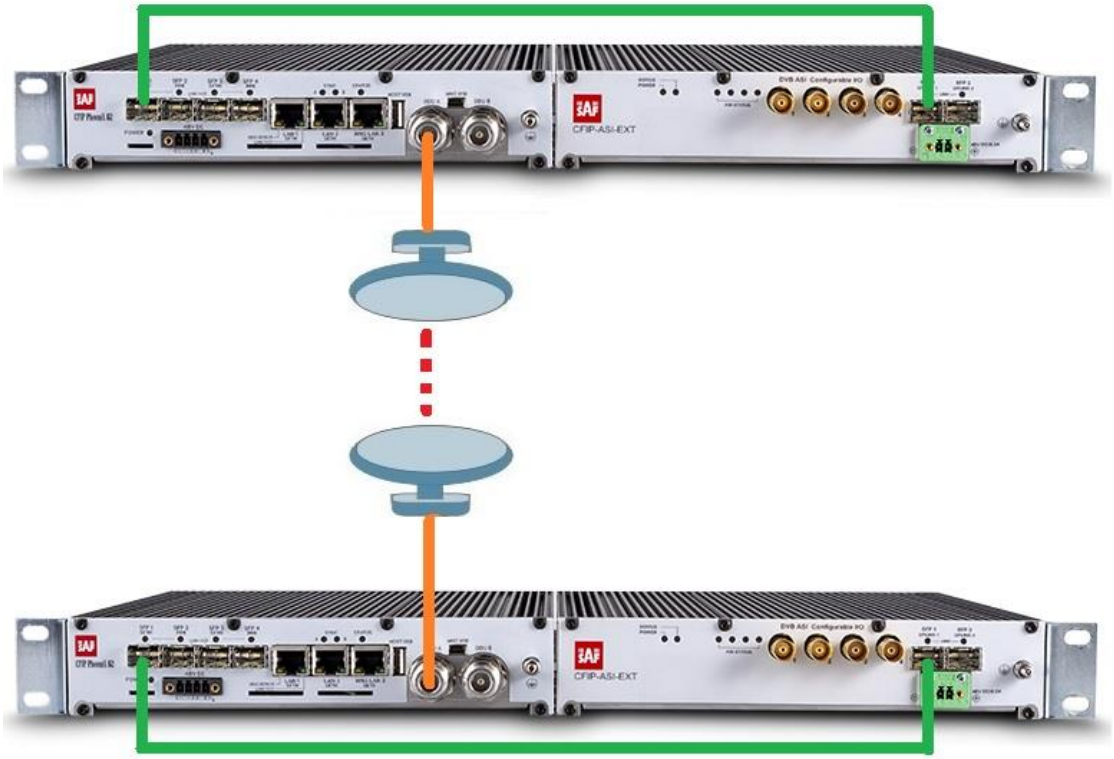


Figure 1.17 *1+0 link with ASI EMM modules*

Application of 1+1 link connection with ASI EMM modules:

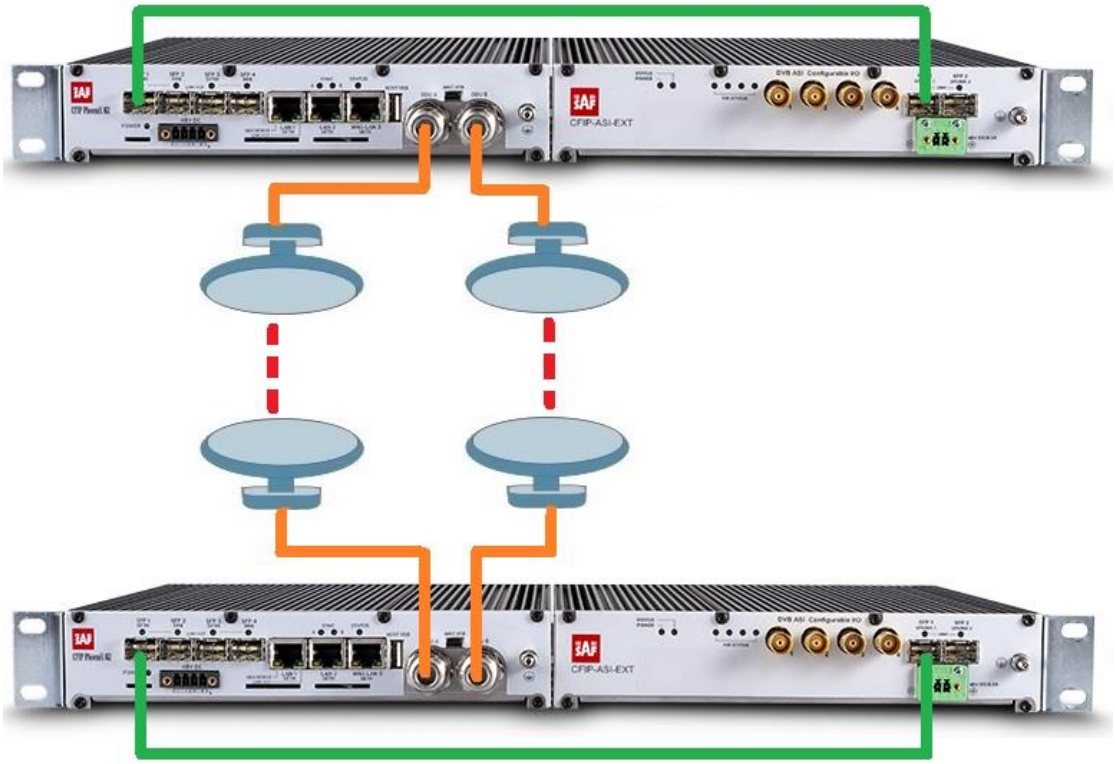


Figure 1.18 *1+1 link with ASI EMM modules*

Application of 1+1 full protection link connection with ASI EMM modules:

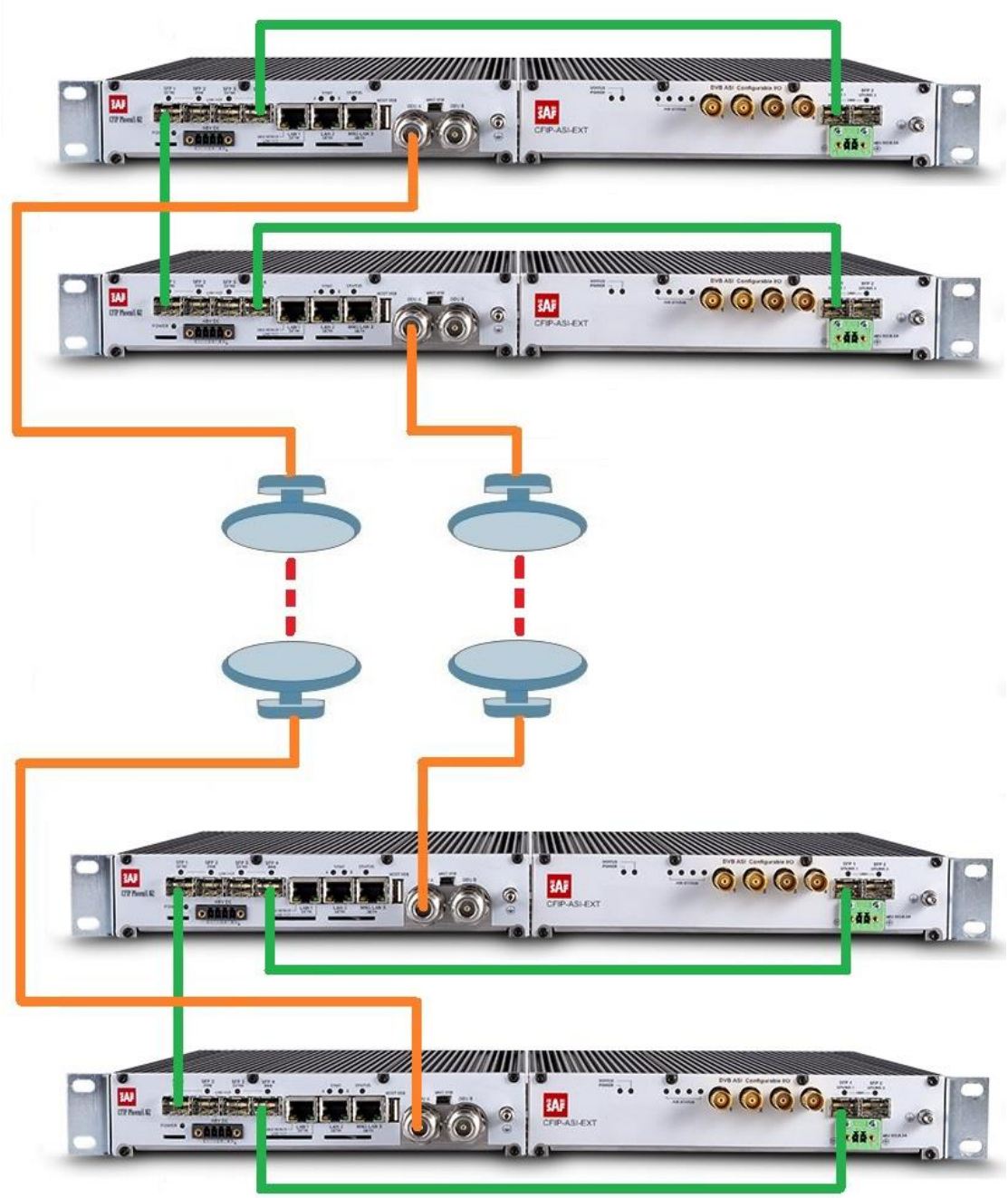


Figure 1.19 *1+1 full protection link with ASI EMM modules*

In 1+1 Full protection mode EMM modules can be connected only to SFP3 and SFP4 ports of the Phoenix G2 IDU. SFP1 port is for both Phoenix G2 IDU interconnection and SFP2 port is reserved for 2+2 modes

1+0 retranslation application with ASI EMM modules:

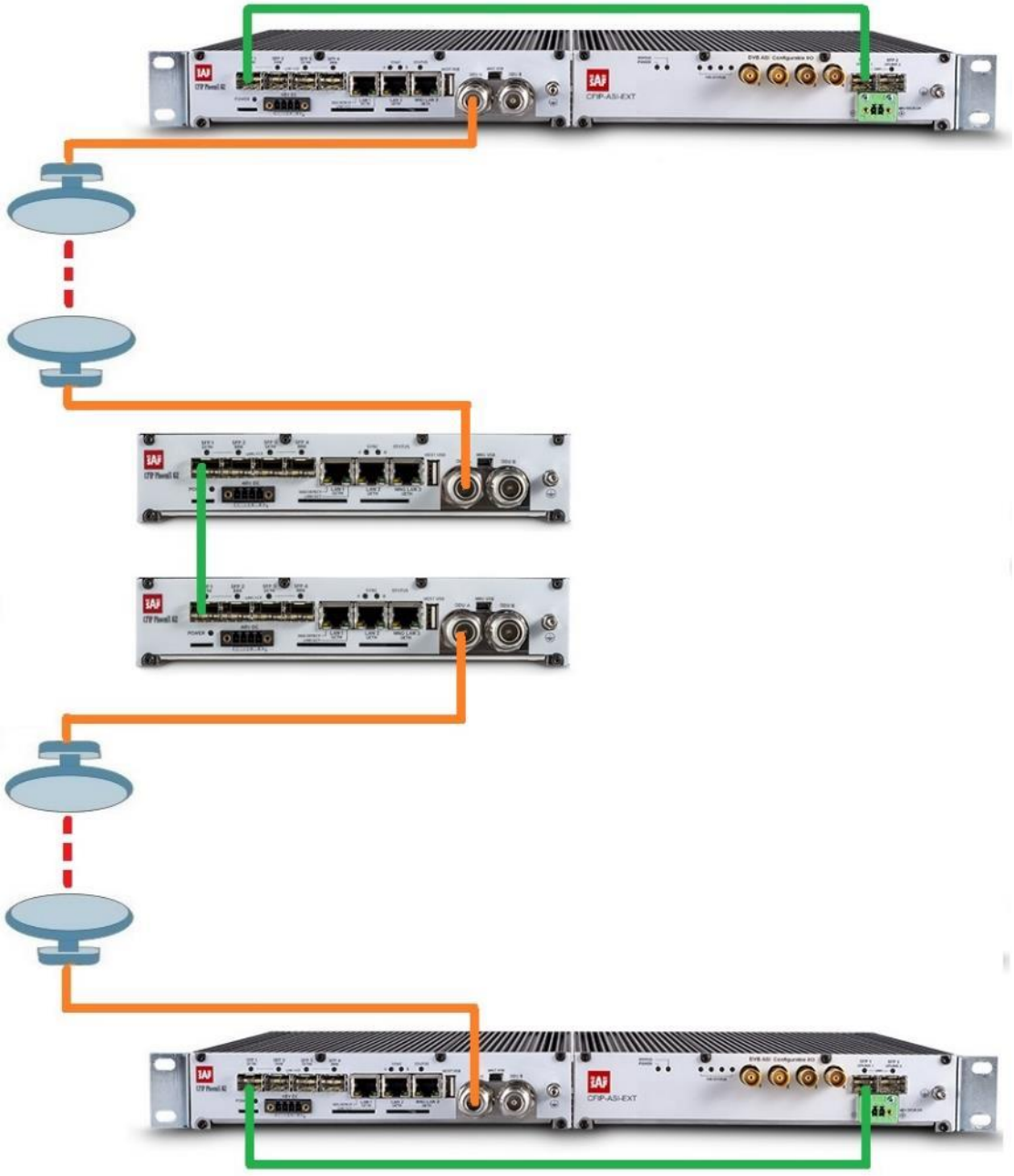


Figure 1.20 *1+0 retranslation link with ASI EMM modules*

1+0 retranslation application with 2xASI streams '*Drop*' in the retranslation site. Other 2xASI streams are forwarded to the end-point:

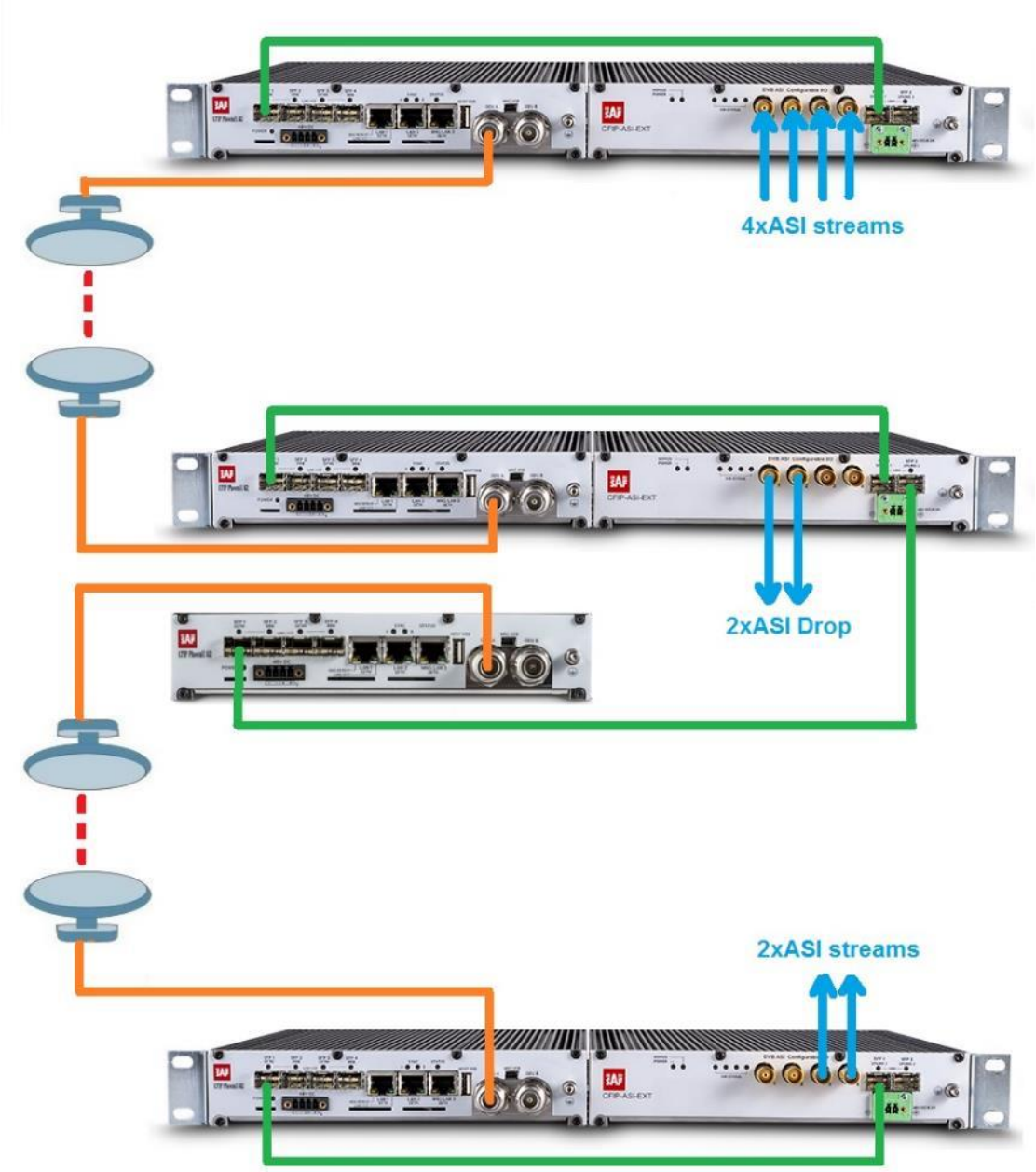


Figure 1.21 *1+0 retranslation link with ASI stream Drop*

1+0 retranslation application example with 2xASI streams '*Drop*' and 2xASI streams '*Add*' in the retranslation site:

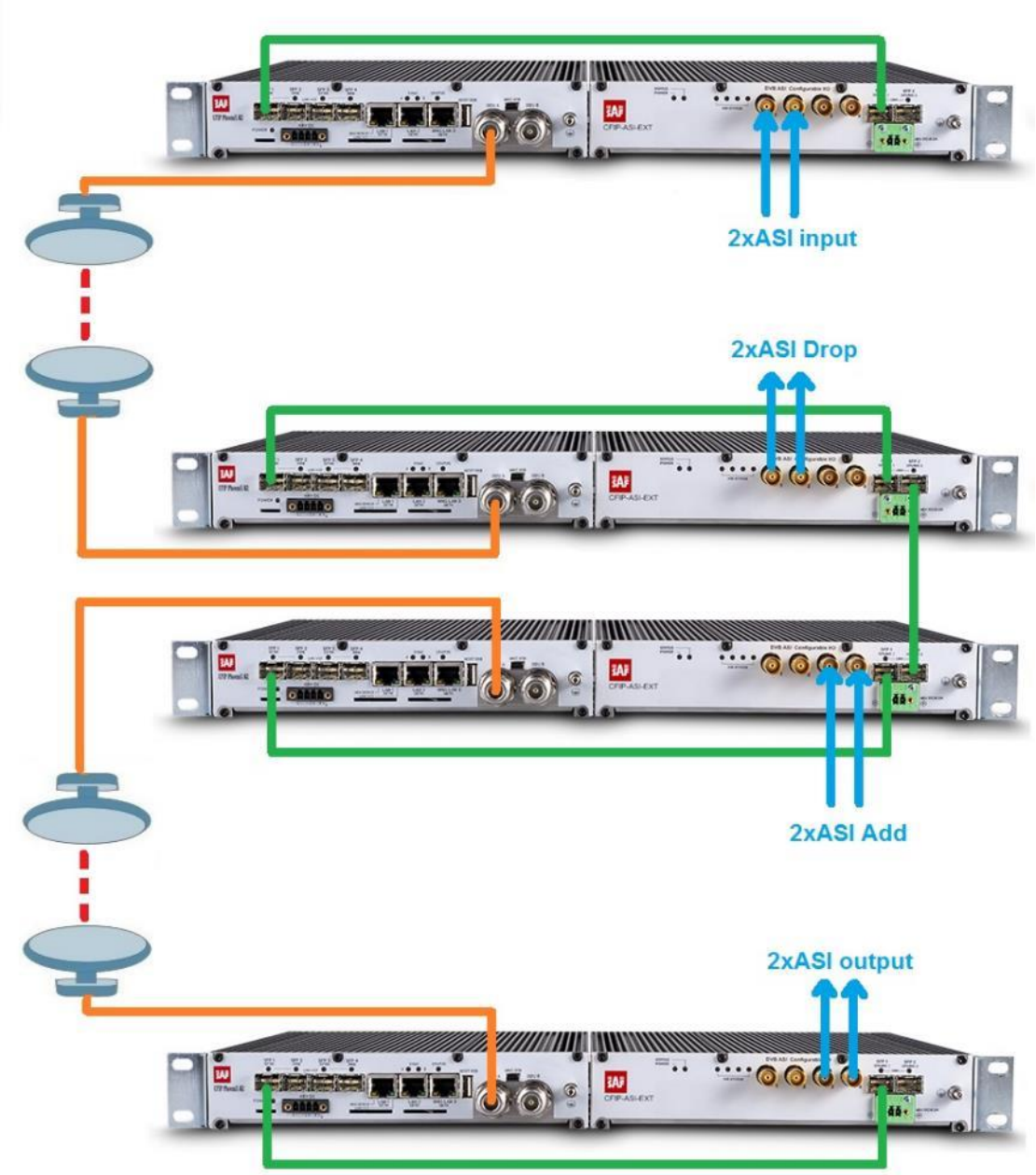


Figure 1.22 *1+0 retranslation link with ASI stream Add/Drop*

E1/T1 EMM extension module

The E1/T1 EMM extension module provides E1/T1 interface extension for Phoenix G2 IDUs. The E1/T1 EMM module multiplexes up to 16 E1/T1 channels into the compact stream which is directed over the fibre optic (FO) connection to/from the Phoenix G2 IDU. The E1/T1 EMM module features 16 x E1/T1 built-in ports (one RJ-45 per e1/t1 channel) and 2 x SFP 1000Base-SX ports.

The compact, simple to configure, and easily scalable design enables cascading with other EMM extension devices (e.g. E1/t1 EMM and/or ASI EMM). The configuration is performed in the web GUI of the IDU, in section *Config → Ports → EMM*.

Maximum speed for single E1 channel is 2.048 Mbps and for single T1 channel is 1.544 Mbps. The actual/total E1/T1 channels speed is auto-detected by the system and is displayed in *Config → Ports → MUX* section.

Up to 4 EMM modules can be connected into the cascade and thus get the maximum quantity of external ports (E1/T1 EMM and ASI EMM modules combination is possible). Maximum 4 EMM modules can be cascaded and in case of E1/t1 EMM modules the maximum count of E1/t1 channels is 64. SFP 1000Base-SX on the left side **SFP 2 UPLINK 2** is dedicated for the modules interconnection into cascade. The configuration of all EMM modules is performed from the web GUI of the IDU.

E1/T1 EMM extension module has following interfaces/connectors:

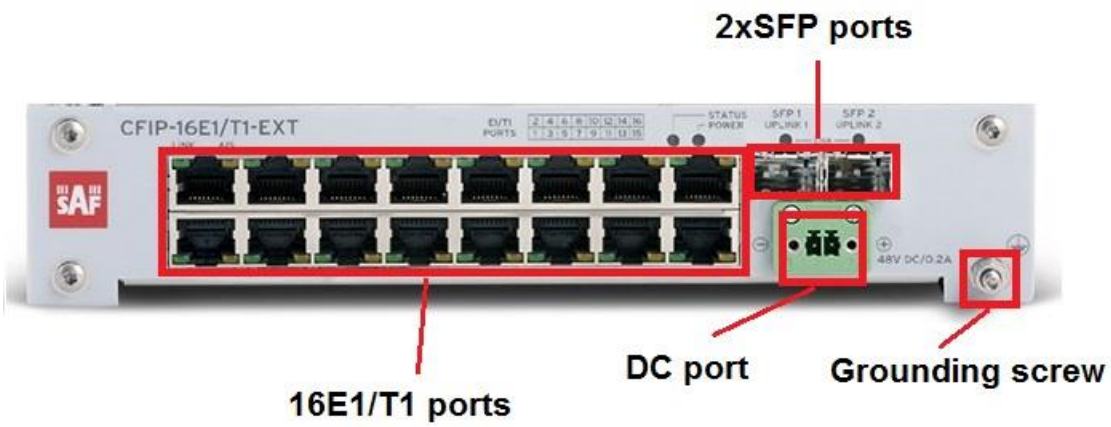


Figure 1.23 *E1/T1 EMM extension module interfaces*

16xE1/T1 ports

16 configurable Input / Output E1/T1 ports (120 Ohm). The 120 Ohm shielded twisted pair Ethernet cable Cat5e is recommended to use for connection to E1 ports. Allowable maximum attenuation in the cable is 10 dB. The E1 ports which are left disconnected must be disabled.

SFP 1 UPLINK 1

Primary SFP port reserved for connection to the IDU or to primary EMM extension module in EMM extension module chain.

SFP 2 UPLINK 2

Secondary SFP port reserved for connection to secondary / next EMM extension module in EMM module chain or for connection to relay IDU in add/drop configuration.

DC port

48V power supply connection. Input DC voltage operating range is -20V to -72V (max current up to 3A). 2-wire DC power connector with screw terminals included. Polarity layout indicated on the front panel. Any 2 wire power cable of good quality which fits well in SAF Tehnika's supplied 2 pole "screw on" power connector could be used.

Grounding screw

Grounding screw for equipment grounding. The equipment grounding can be done by connecting it to the grounding point of the rack, or directly to the grounding point in the equipment room. The recommended minimum grounding cable wire cross-section must be 2.5 mm2 and the recommended maximum length of the grounding cable is 1 m.

E1/T1 EMM module front panel alarm LED indications:

LED name	Description
STATUS	**Orange –** OK, module enabled, proper communication with the IDU **Orange blinks –** WARNING, module is not enabled in the system or no communication with IDU, or configuration is not finished yet **Off** – ERROR, firmware is not loaded into EMM module HW
POWER	**Green –** power supply is OK **Off** – no power supply
SFP 1/2 LINK	**Orange blinks –** signal detected and synchronized, valid communication with the IDU **Off –** no correct signal detected
E1/T1 STATUS	***LINK:*** **Green –** E1/T1 signal detected at the port **Off** – no link at the port ***AIS (Alarm Indication Signal):*** **Orange** – AIS signal detected **Off** – no AIS on the port

The position and indexing of 16 E1 user ports indicates the legend below:

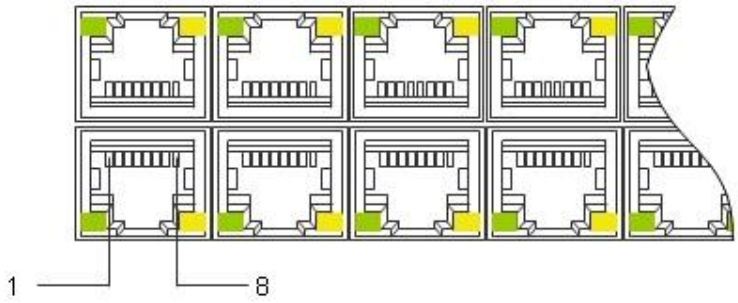


Figure 1.24 *Indexing of E1/T1 ports*

The legend of e1/t1 port pins is following:
Pin1 – Rx-
Pin2 – Rx+
Pin4 – Tx-
Pin5 – Tx+
All the E1/T1 ports are protected against ESD (electrostatic discharge), CDE (Cable Discharge Events), and lightning.
In the case of connecting 16E1 balanced RJ-45 interface to customer's unbalanced BNC E1 interface ports the following cable must be used:

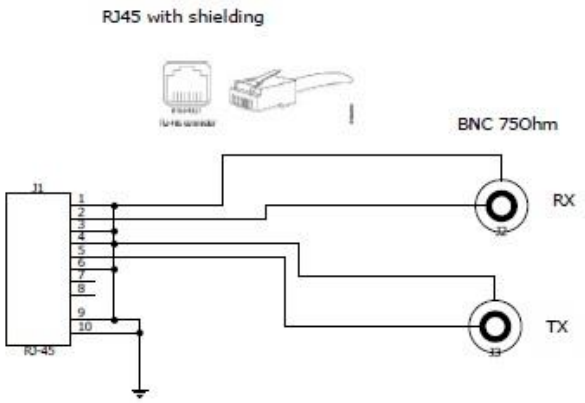


Figure 1.25 *Cable for interconnecting to unbalanced E1/T1 CPE*

Pinout for such cable is following:

Pin	Signal
1	Rx ring
2	Rx tip
3	GND (over resistor 08050R)
4	Tx ring
5	Tx tip
6	GND (over resistor 08050R)
7	NC
8	NC

Interconnection of Phoenix G2 IDU and E1/T1 EMM module must be done using optical cable and SFP modules (P/N I0ASMK02 optical cable kit can be used for that purpose). For 1+0 and 2+0 configurations any of all 4 SFP ports on the IDU can be used for connection to EMM module. In 1+1 full redundancy configuration SFP ports 3 and 4 can be used to connect to EMM module. On EMM module SFP port 1 can be used to connect to Phoenix G2 IDU and SFP port 2 must be used to connect to the next cascaded EMM module.



Figure 1.26 *Phoenix G2 IDU and E1/T1 EMM module interconnection*

Application of 1+0 link connection with E1/T1EMM modules:

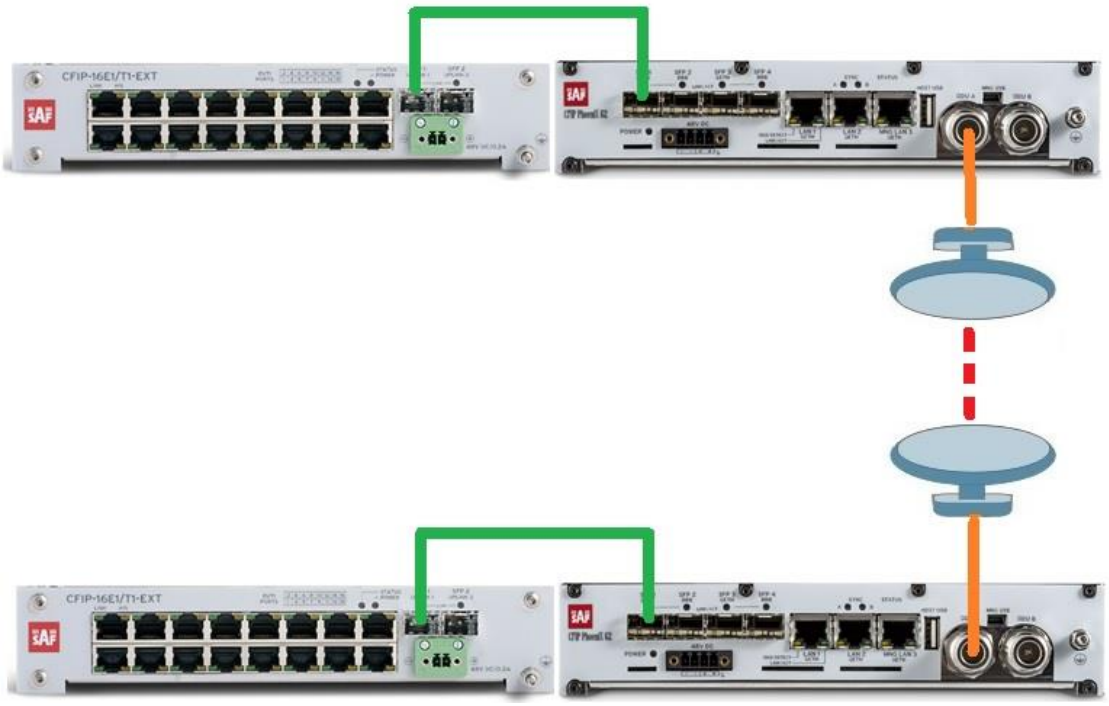


Figure 1.27 *1+0 link with E1/T1 EMM modules*

Application of 1+1 link connection with E1 EMM modules:

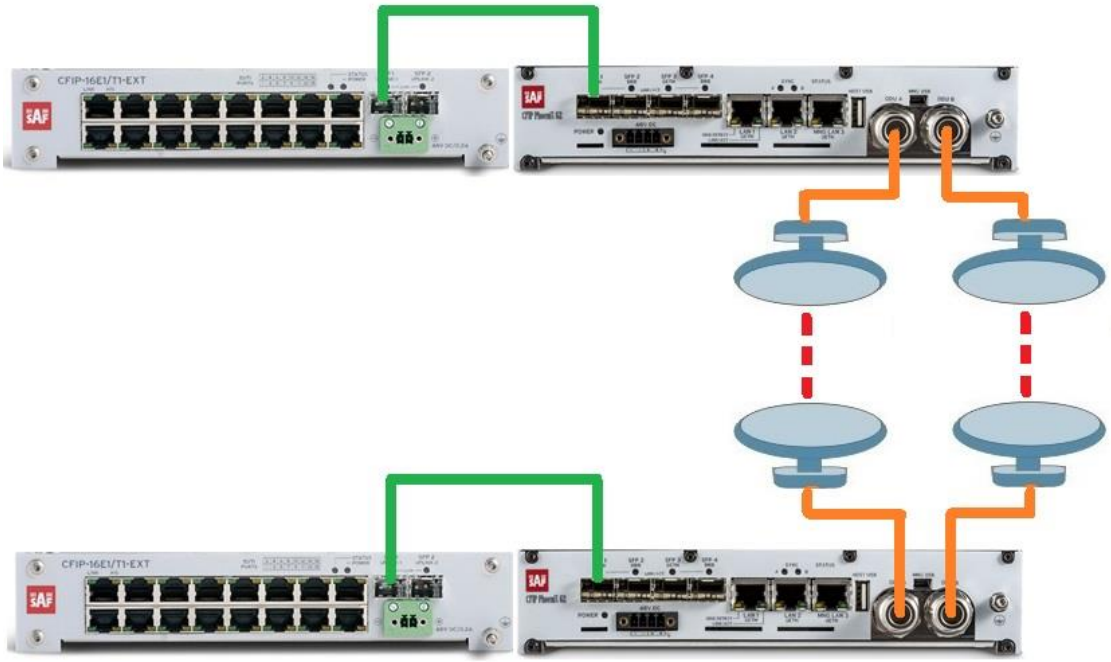


Figure 1.28 *1+1 link with E1/T1 EMM modules*

Application of 1+1 full protection link connection with E1/T1 EMM modules:

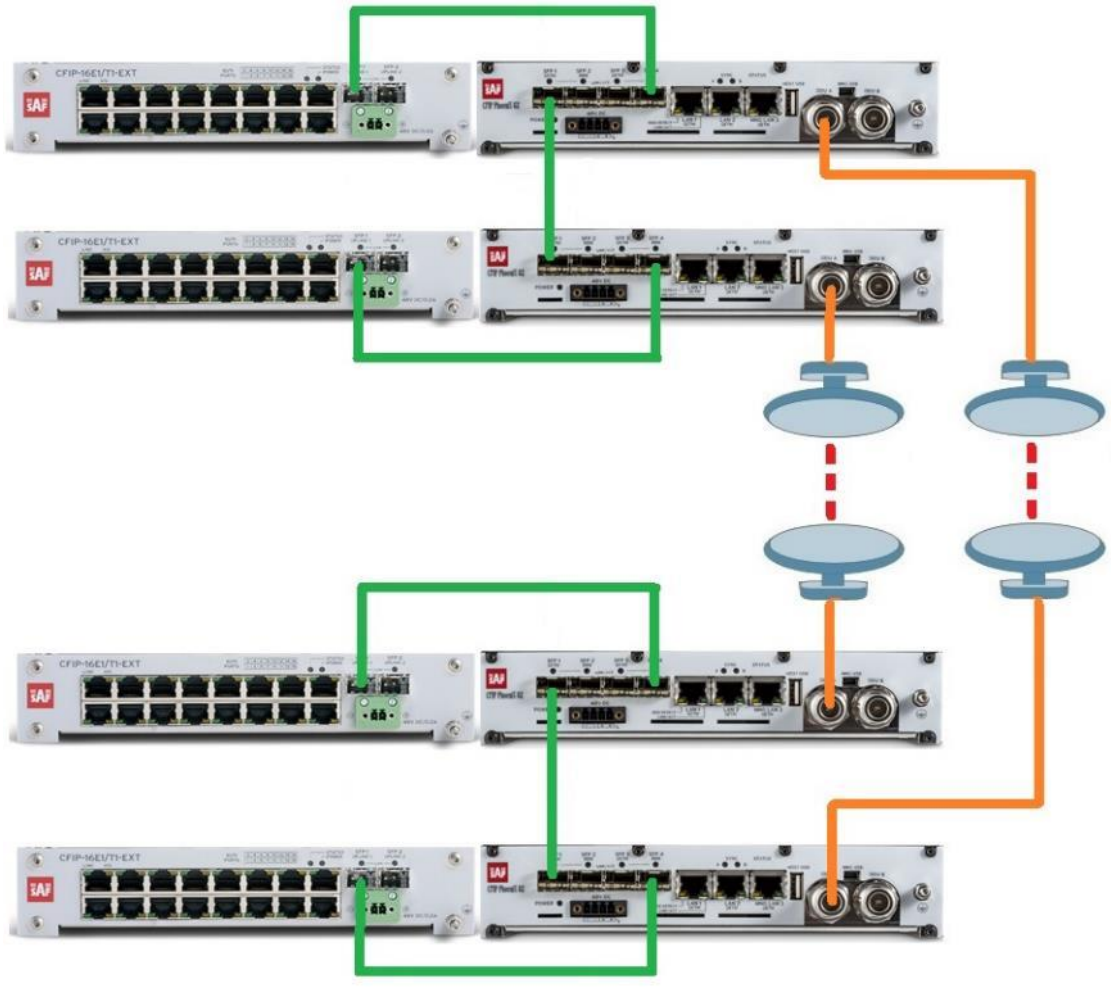


Figure 1.29 *1+1 full protection link with E1/T1 EMM modules*

In 1+1 Full protection mode EMM modules can be connected only to SFP3 and SFP4 ports of the Phoenix G2 IDU. SFP1 port is for both Phoenix G2 IDU interconnection and SFP2 port is reserved for 2+2 modes

1+0 retranslation application with E1/T1 EMM modules:

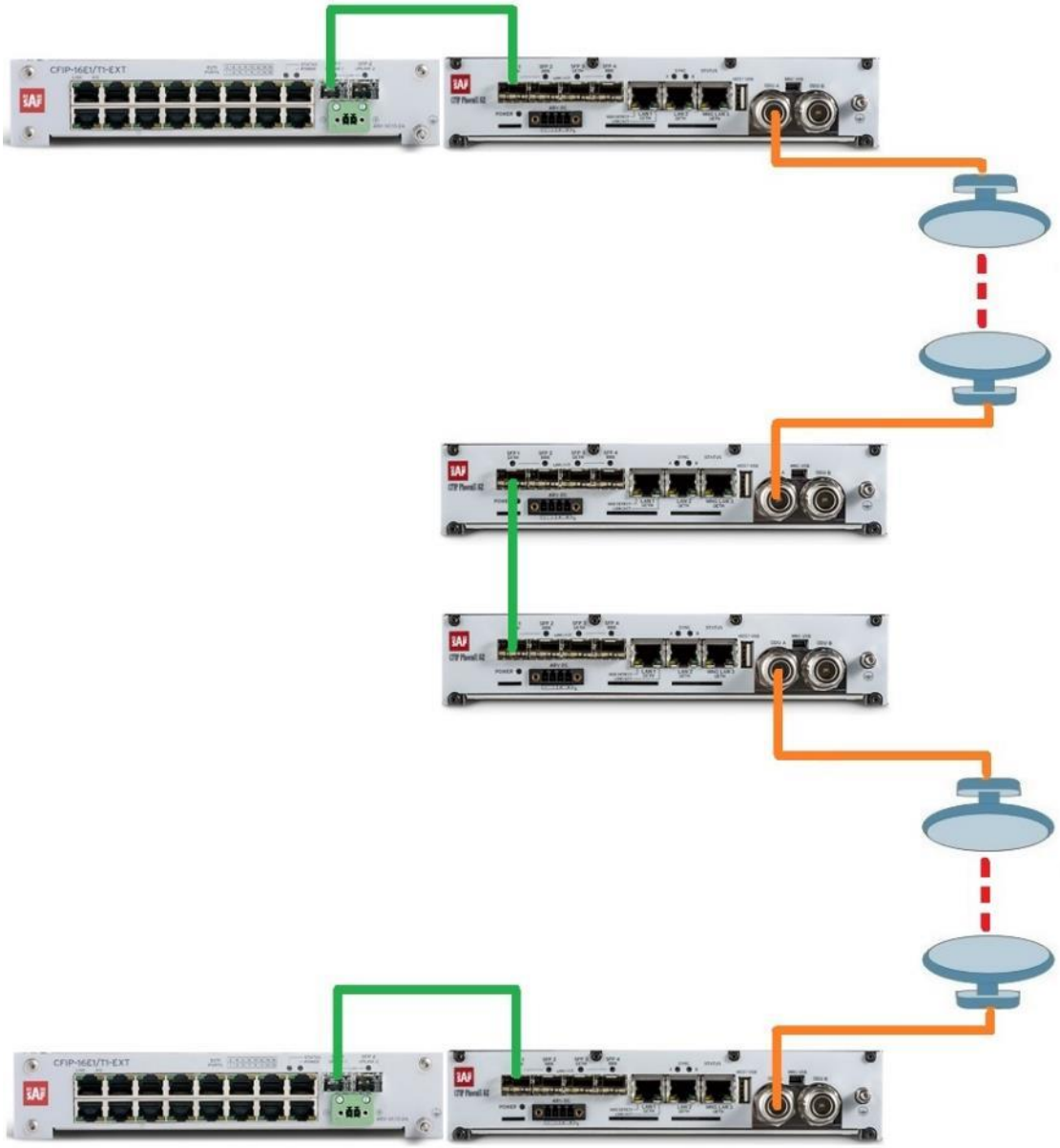


Figure 1.30 *1+0 retranslation link with E1/T1 EMM modules*

1+0 retranslation application with E1/T1 Add/Drop in the retranslation site:

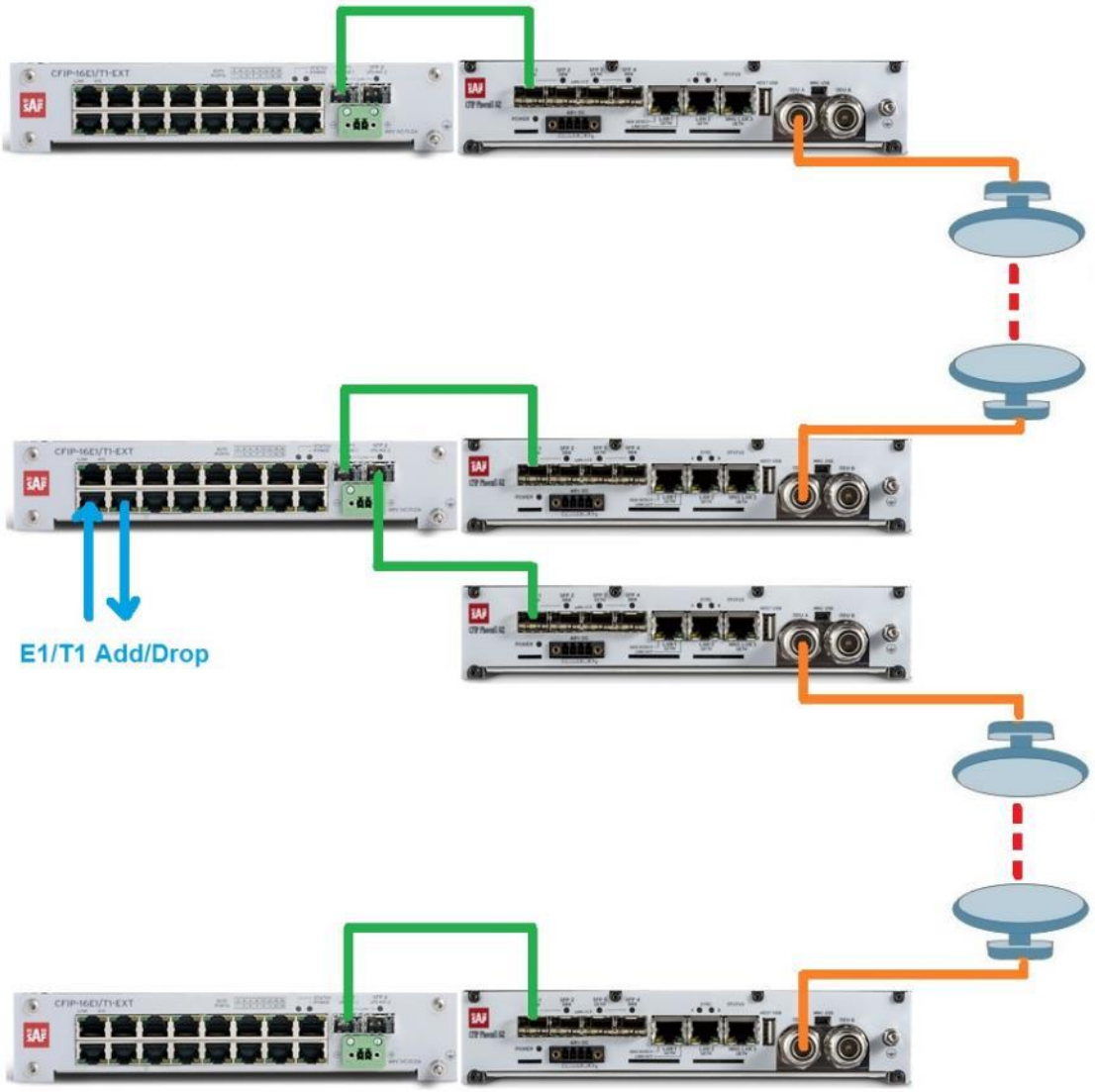


Figure 1.31 *1+0 retranslation link with E1/T1 Add/Drop*

Phoenix G2 ODU and IRFU interfaces and ports

SP/HP ODU with SAF radio interface

Phoenix G2 Standard Power (SP)/High Power (HP) ODU has following interfaces:

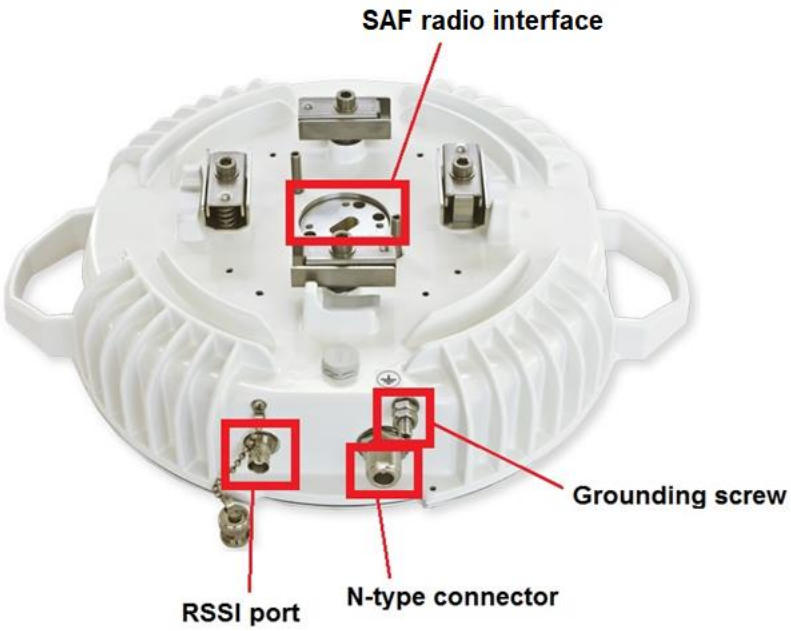


Figure 1.32 *SP/HP ODU with SAF radio interface*

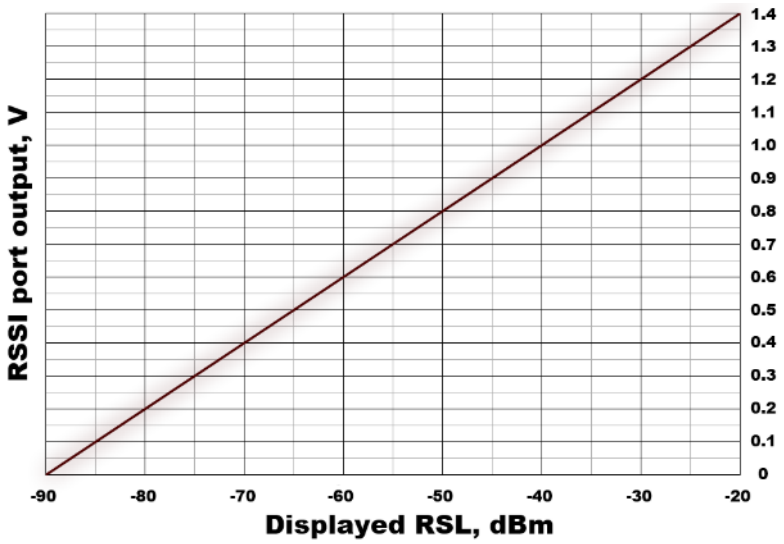
SAF radio interface

SAF radio interface (7-38GHz) conforms to UBR standard flange pattern. Flange size depends on the frequency used.

RSSI port

RSSI (Received Signal Strength Indicator) port is used to adjust the alignment of antenna for best performance (for both rough and fine adjustment); this can be done using digital multimeter which is connected to the RSSI port. The output of the RSSI port is DC voltage and varies depending on received signal level.

The following chart and table shows typical relationship of the received signal level (Rx level) displayed by Phoenix G2 vs. RSSI port output voltage. The evaluated Rx level has the error +/- 2 dB.



Displayed RSL, dBm	RSSI, V
-90	0
-85	0,1
-80	0,2
-75	0,3
-70	0,4
-65	0,5
-60	0,6
-55	0,7
-50	0,8
-45	0,9
-40	1
-35	1,1
-30	1,2
-25	1,3
-20	1,4

Figure 1.33 *Typical RSSI=f(RSL) chart*

N-type connector

N-type Female connector for ODU interconnection to IDU with coaxial cable

Grounding screw

Grounding screws should be interconnected with grounding cable and connected to ground circuit

SP/HP ODU with SAF2/SAF2R radio interface

Phoenix G2 Standard Power (SP)/High Power (HP) ODU with circular SAF2 (15-38 GHz) and rectangular SAF2R (7-13 GHz) adaptation has following interfaces:

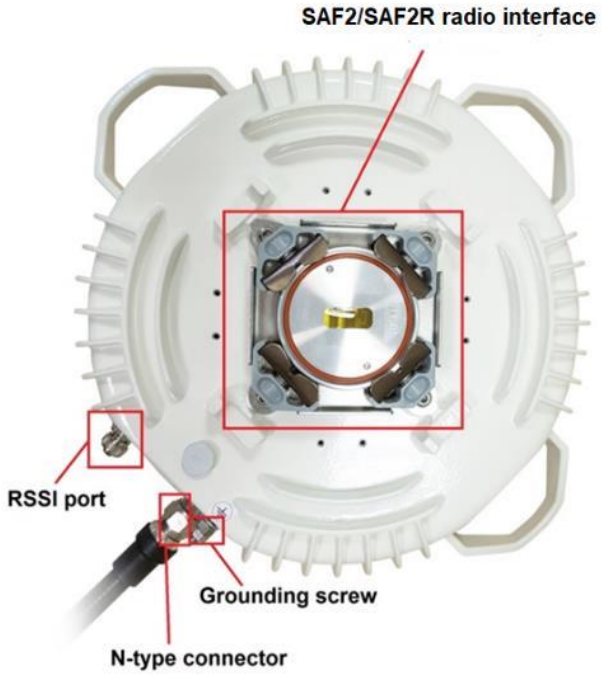


Figure 1.34 *SP/HP ODU with SAF2/SAF2R radio interface*

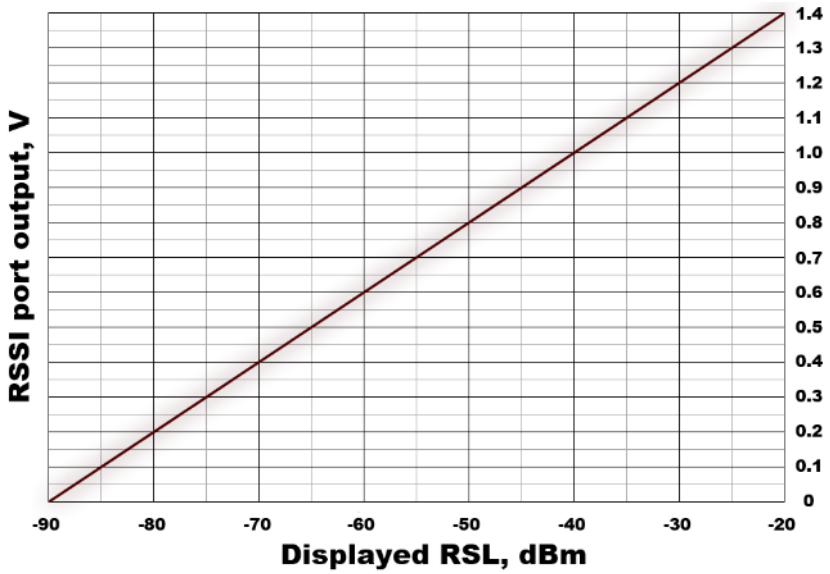
SAF2 or SAF2R radio interface

Circular or Rectangular flange for ODU interconnection with antenna equipped with SAF2 or SAF2R interface. Flange size depends on the frequency used.

RSSI port

RSSI (Received Signal Strength Indicator) port is used to adjust the alignment of antenna for best performance (for both rough and fine adjustment); this can be done using digital multimeter which is connected to the RSSI port. The output of the RSSI port is DC voltage and varies depending on received signal level.

The following chart and table shows typical relationship of the received signal level (Rx level) displayed by Phoenix G2 vs. RSSI port output voltage. The evaluated Rx level has the error +/- 2 dB.



Displayed RSL, dBm	RSSI, V
-90	0
-85	0,1
-80	0,2
-75	0,3
-70	0,4
-65	0,5
-60	0,6
-55	0,7
-50	0,8
-45	0,9
-40	1
-35	1,1
-30	1,2
-25	1,3
-20	1,4

Figure 1.35 *Typical RSSI=f(RSL) chart*

N-type connector

N-type Female connector for ODU interconnection to IDU with coaxial cable

Grounding screw

Grounding screws should be interconnected with grounding cable and connected to ground circuit

VHP ODU

Phoenix G2 Very High Power (VHP) ODU (6-13 GHz) has following interfaces:

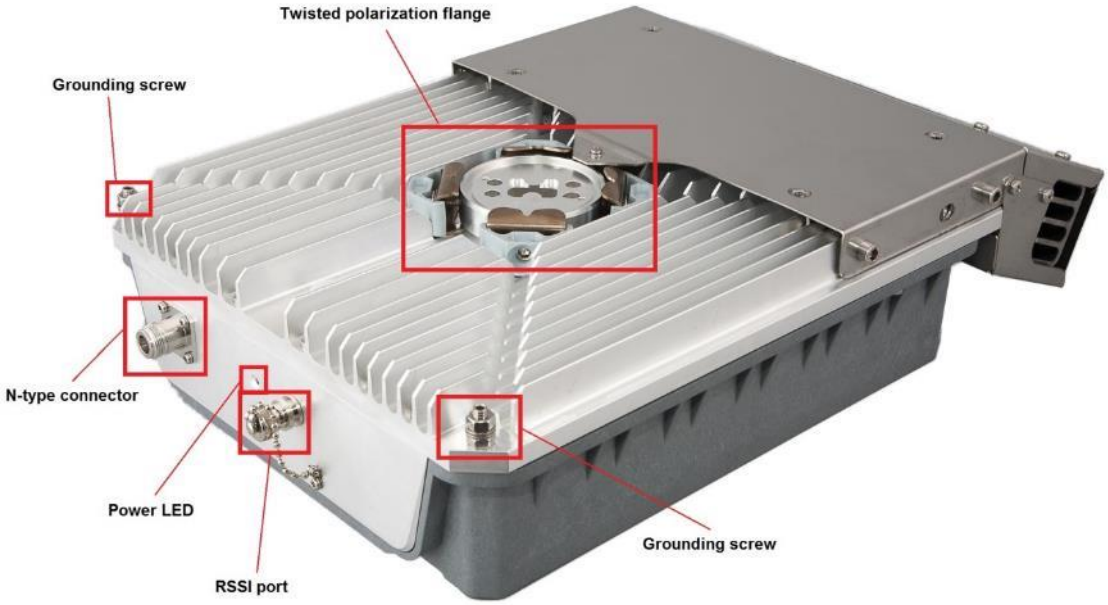


Figure 1.36 *VHP ODU interfaces*

Twisted polarization flange

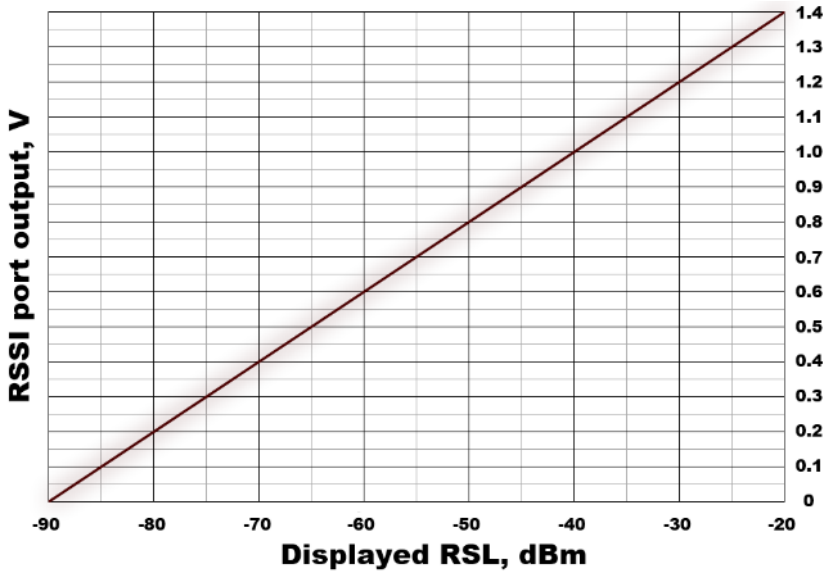
Phoenix G2 VHP ODU 6-13GHz features twisted polarization flange and resulting signal polarization is determined by SAF2R interface on antenna radio adapter/OMT. To change signal polarization, only the antenna interface should be rotated, as radio always remains in vertical position.

VHP ODU 18-23 GHz features square flange compatible with antenna SAF2 adaptation interface. The signal polarization can be changed by rotating the square flange on the ODU

RSSI port

RSSI (Received Signal Strength Indicator) port is used to adjust the alignment of antenna for best performance (for both rough and fine adjustment); this can be done using digital multimeter which is connected to the RSSI port. The output of the RSSI port is DC voltage and varies depending on received signal level.

The following chart and table shows typical relationship of the received signal level (Rx level) displayed by Phoenix G2 vs. RSSI port output voltage. The evaluated Rx level has the error +/- 2 dB.



Displayed RSL, dBm	RSSI, V
-90	0
-85	0,1
-80	0,2
-75	0,3
-70	0,4
-65	0,5
-60	0,6
-55	0,7
-50	0,8
-45	0,9
-40	1
-35	1,1
-30	1,2
-25	1,3
-20	1,4

Figure 1.37 *Typical RSSI=f(RSL) chart*

N-type connector

N-type Female connector for ODU interconnection to IDU with coaxial cable

Power LED

Indicates if the ODU is powered ON

Grounding screw

Grounding screws should be interconnected with grounding cable and connected to ground circuit

IRFU with built-in diplexer

Phoenix G2 IRFU with built-in diplexer has following interfaces:

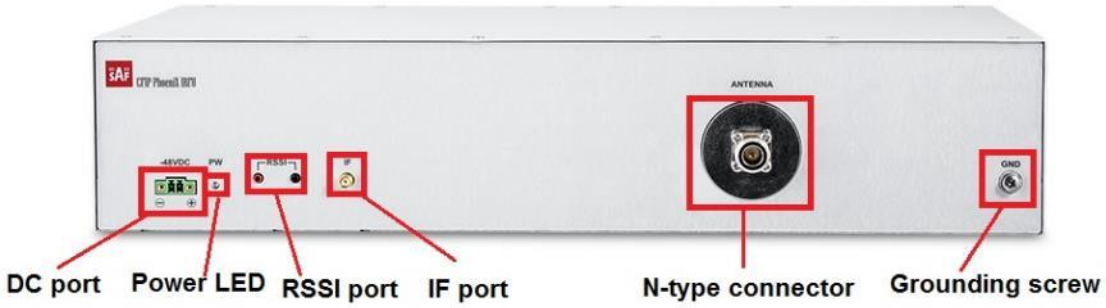


Figure 1.38 *IRFU interfaces*

DC port

48V power supply connection. Input DC voltage operating range is -40.5V to -57V (max current up to 3A). 2-wire DC power connector with screw terminals included. Polarity layout indicated on the front panel. Any 2 wire power cable of good quality which fits well in SAF Tehnika's supplied 2 pole "screw on" power connector could be used.

As the main power supply source for the IRFU is from the IDU via IF port, the DC port can be used for extra power supply connection in specific cases. It is not recommended to power the IRFU via DC port in 1+1 Full protection and 2+2 Full protection applications

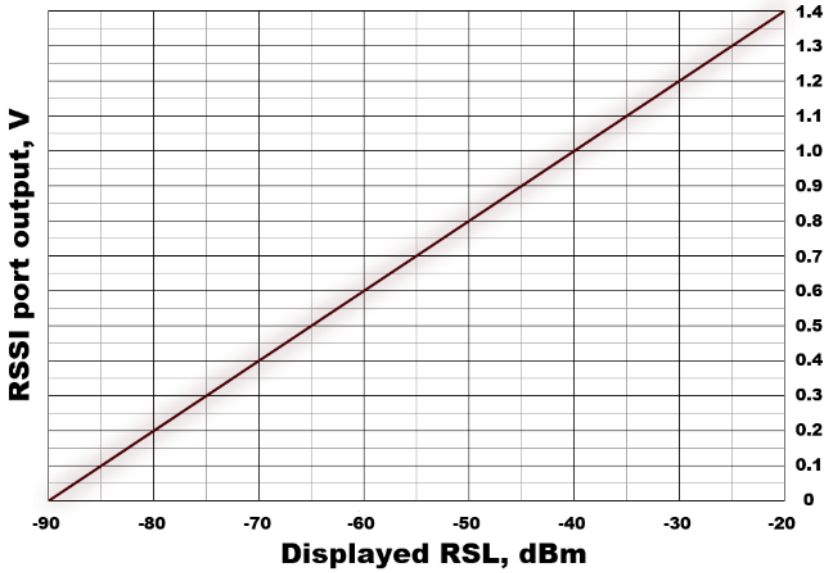
Power LED

Indicates if the IRFU is powered ON

RSSI port

RSSI (Received Signal Strength Indicator) port is used to adjust the alignment of antenna for best performance (for both rough and fine adjustment); this can be done using digital multimeter which is connected to the RSSI port. The output of the RSSI port is DC voltage and varies depending on received signal level.

The following chart and table shows typical relationship of the received signal level (Rx level) displayed by Phoenix G2 vs. RSSI port output voltage. The evaluated Rx level has the error +/- 2 dB.



Displayed RSL, dBm	RSSI, V
-90	0
-85	0,1
-80	0,2
-75	0,3
-70	0,4
-65	0,5
-60	0,6
-55	0,7
-50	0,8
-45	0,9
-40	1
-35	1,1
-30	1,2
-25	1,3
-20	1,4

Figure 1.39 *Typical RSSI=f(RSL) chart*

IF port

SMA IF connector for connection to IDU

N-type connector

N-type Female connector for IRFU interconnection to antenna with coaxial cable

Grounding screw

Grounding screws should be interconnected with grounding cable and connected to ground circuit. The equipment grounding can be done by connecting it to the grounding point of the rack, or directly to the grounding point in the equipment room. The recommended minimum grounding cable wire cross-section must be 2.5 mm2 and the recommended maximum length of the grounding cable is 1 m.

IRFU without built-in diplexer

Phoenix G2 IRFU without built-in diplexer has following interfaces:

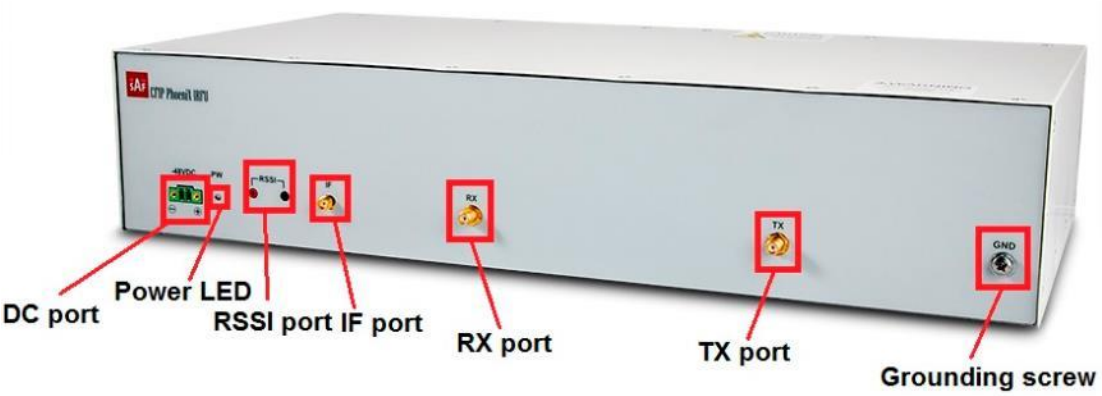


Figure 1.40 *IRFU interfaces*

DC port

48V power supply connection. Input DC voltage operating range is -40.5V to -57V (max current up to 3A). 2-wire DC power connector with screw terminals included. Polarity layout indicated on the front panel. Any 2 wire power cable of good quality which fits well in SAF Tehnika's supplied 2 pole "screw on" power connector could be used.

As the main power supply source for the IRFU is from the IDU via IF port, the DC port can be used for extra power supply connection in specific cases. It is not recommended to power the IRFU via DC port in 1+1 Full protection and 2+2 Full protection applications

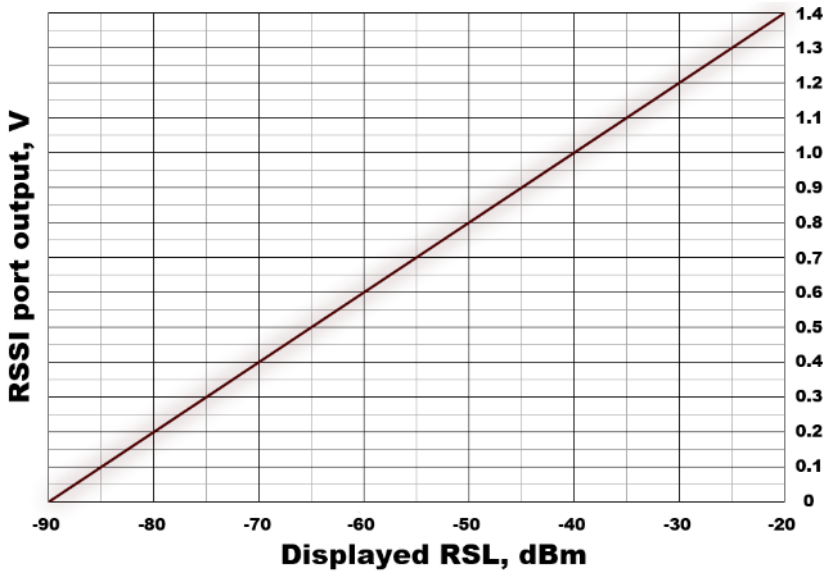
Power LED

Indicates if the IRFU is powered ON

RSSI port

RSSI (Received Signal Strength Indicator) port is used to adjust the alignment of antenna for best performance (for both rough and fine adjustment); this can be done using digital multimeter which is connected to the RSSI port. The output of the RSSI port is DC voltage and varies depending on received signal level.

The following chart and table shows typical relationship of the received signal level (Rx level) displayed by Phoenix G2 vs. RSSI port output voltage. The evaluated Rx level has the error +/- 2 dB.



Displayed RSL, dBm	RSSI, V
-90	0
-85	0,1
-80	0,2
-75	0,3
-70	0,4
-65	0,5
-60	0,6
-55	0,7
-50	0,8
-45	0,9
-40	1
-35	1,1
-30	1,2
-25	1,3
-20	1,4

Figure 1.41 *Typical RSSI=f(RSL) chart*

IF port

SMA IF connector for connection to IDU

RX port

SMA connector for IRFU Rx interconnection with external branching unit

TX port

SMA connector for IRFU Tx interconnection with external branching unit

Grounding screw

Grounding screws should be interconnected with grounding cable and connected to ground circuit. The equipment grounding can be done by connecting it to the grounding point of the rack, or directly to the grounding point in the equipment room. The recommended minimum grounding cable wire cross-section must be 2.5 mm2 and the recommended maximum length of the grounding cable is 1 m.

On some IRFU devices optional RJ-45 control port can be available for interconnection with IBU device which is equipped with active switch. In case if the IRFU is equipped with the Control port, additional LED indications are available on:

LED name	Description
POWER	**Green –** power supply is OK **Off** – no power supply
Control (optional)	**Green –** works correctly **Off –** not connected, cable fault

IBU without active switch

Phoenix G2 IBU (Indoor Branching Unit) without built-in active switch has following interfaces on the front panel:



Figure 1.42 *IBU front panel interfaces*

RX1 and RX2 ports

SMA connector for IBU interconnection with corresponding IRFU Rx port

TX1 and TX2 ports

SMA connector for IBU interconnection with corresponding IRFU Tx port

Backpanel of the IBU:

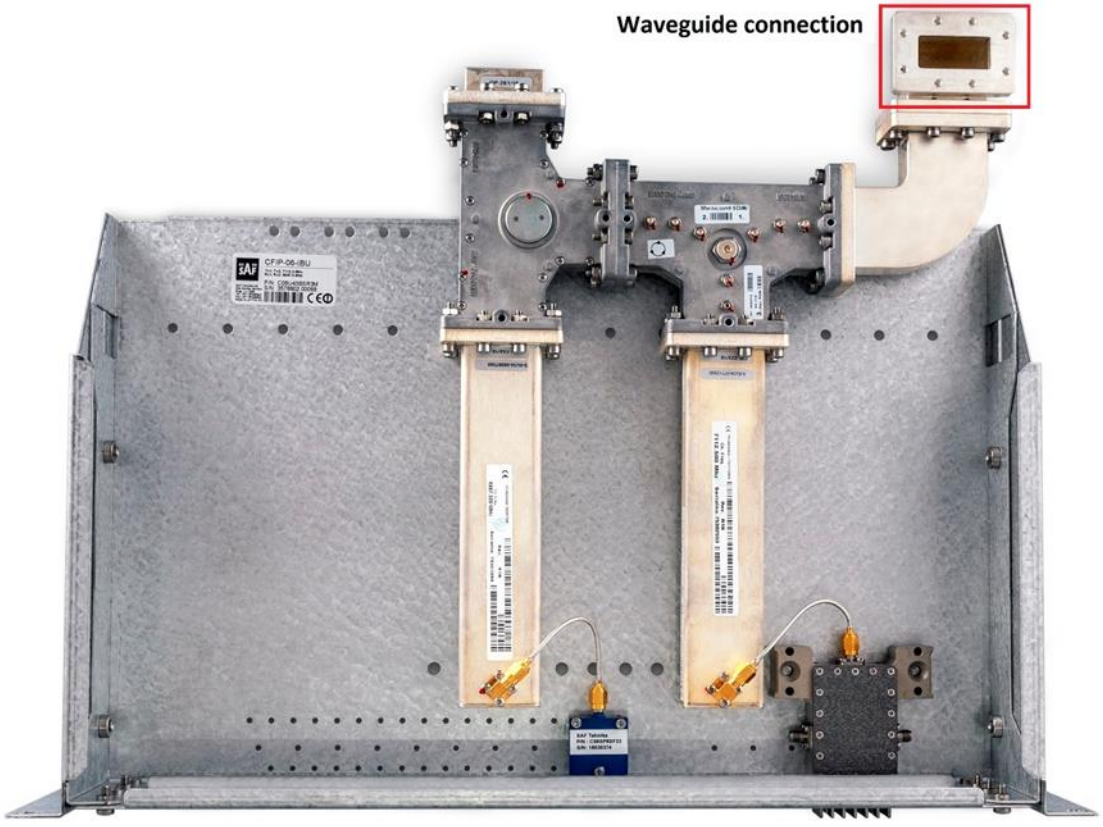


Figure 1.43 *IBU top-back panel interfaces*

Waveguide connection

Interconnection with waveguide.

The ***Figure 1.43*** shows the IBU P/N C06U43BSR3M with outgoing CMR137 (UER70) waveguide flange. For other options refer to the IBU product datasheet or SAF representative.

Example of IRFU and IBU interconnection using the 1+1 or 2+0 application with single IDU:

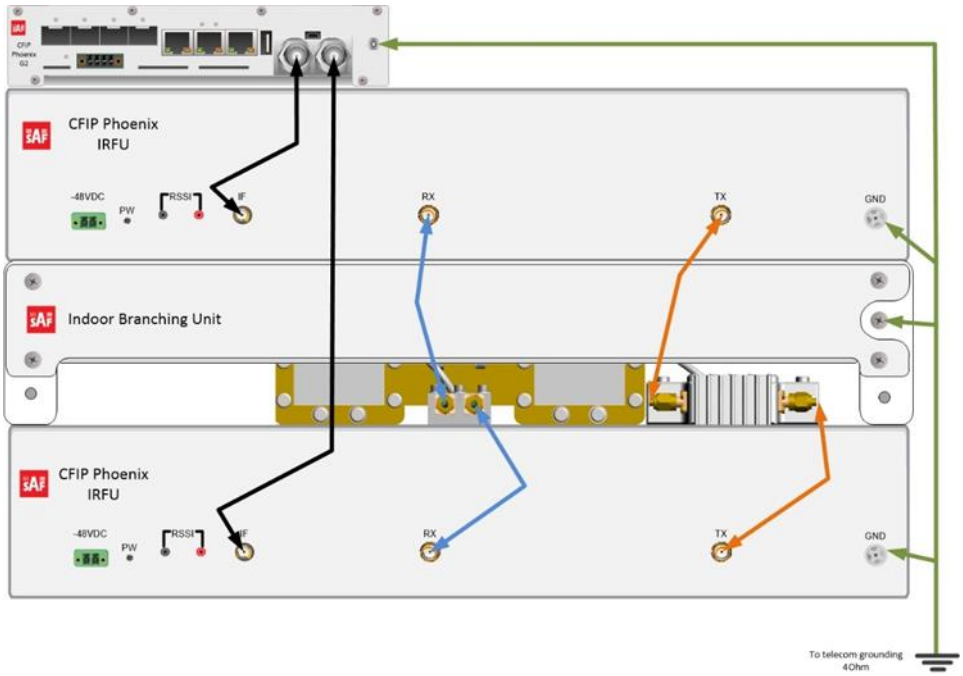


Figure 1.44 *IRFU and IBU interconnection using single IDU*

Example of IRFU and IBU interconnection using the 1+1 full redundancy application with two IDUs:

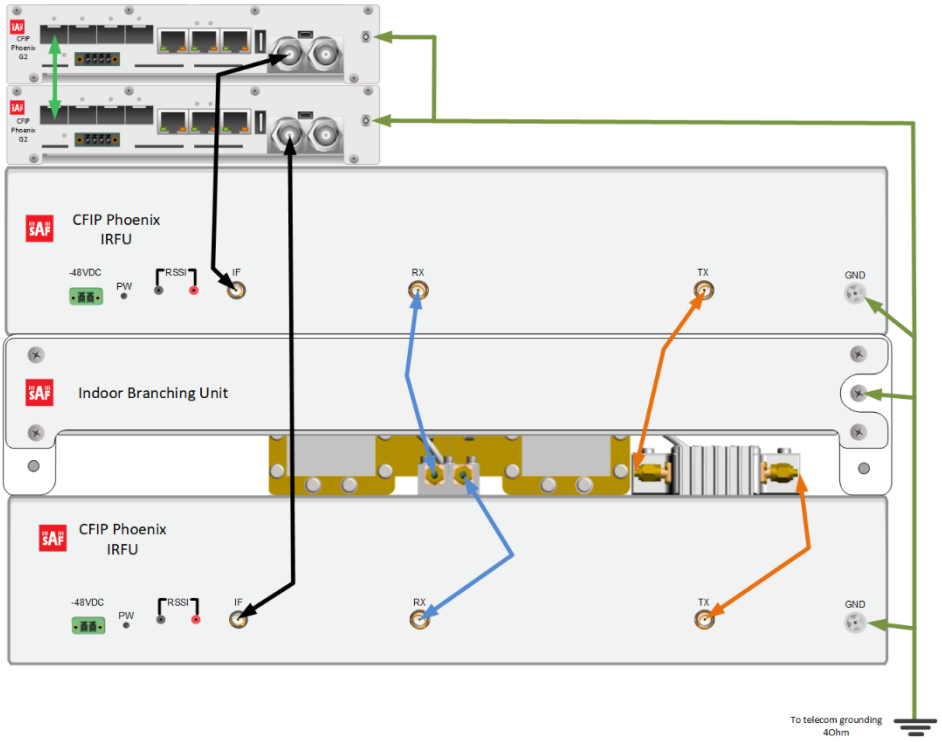


Figure 1.45 *IRFU and IBU interconnection using two IDUs*

IBU with active switch

Phoenix G2 IBU with built-in active switch has following interfaces on the front panel:

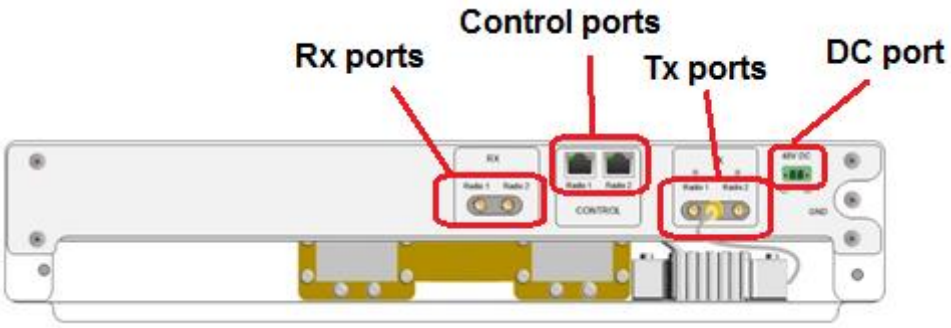


Figure 1.46 *IBU with active switch front panel interfaces*

RX1 and RX2 ports

SMA connector for IBU interconnection with corresponding IRFU Rx port

TX1 and TX2 ports

SMA connector for IBU interconnection with corresponding IRFU Tx port

Radio 1 and Radio 2 Control ports

RJ-45 connector for IBU interconnection with corresponding IRFU Control port

DC port

48V power supply connection. Input DC voltage operating range is -40.5V to -57V (max current up to 3A). 2-wire DC power connector with screw terminals included. Polarity layout indicated on the front panel. Any 2 wire power cable of good quality which fits well in SAF Tehnika's supplied 2 pole "screw on" power connector could be used.

Phoenix G2 IBU front panel alarm LED indications:

LED name	Description
Control (Radio 1/2)	**Green –** normal operation – control cable connected, IRFU is powered on **Off** – control cable unplugged or damaged, or IRFU is not powered on
TX (Radio 1/2)	**Green –** Normal operation – Tx part is active or in active search during the switchover **Off –** Tx part is in standby state, normal operation **Red** – alarm condition – both Tx are working simultaneously, faulty control cable or IRFU is not powered on *

** In case of 1+1 configuration the IRFU must not be powered on via DC port, that is why in this case the Red LED is acceptable*

Example of IRFU and IBU interconnection using the 1+1 or 2+0 application with single IDU:

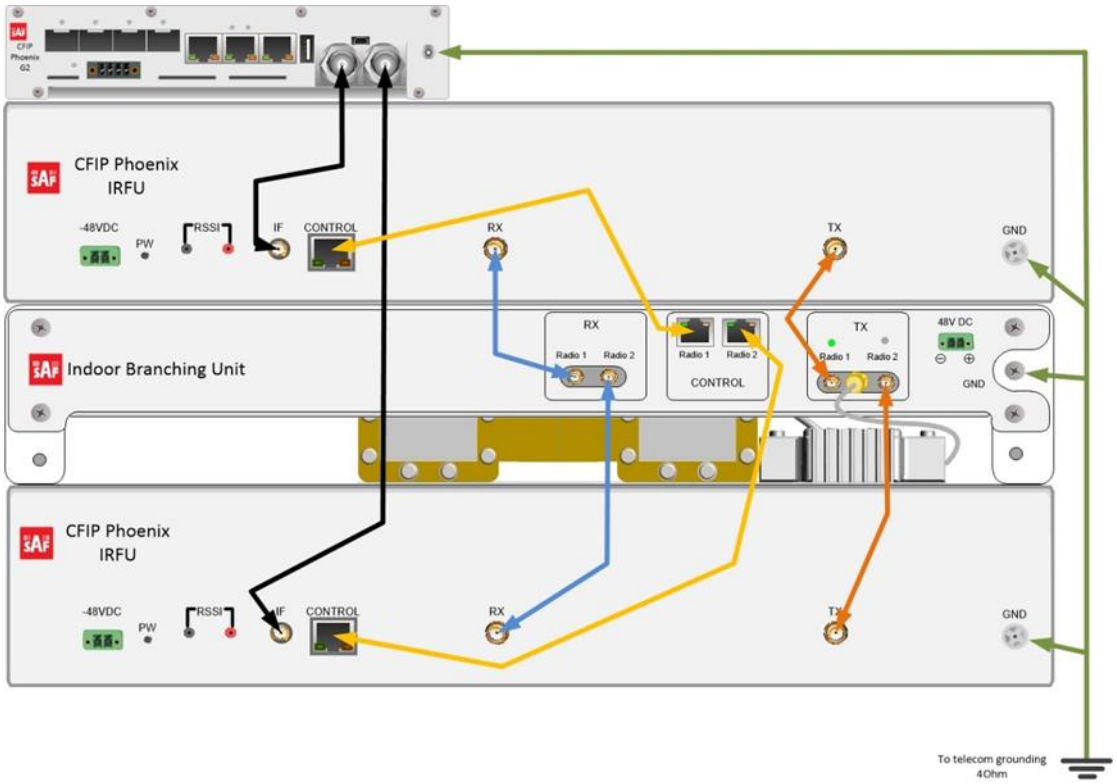


Figure 1.47 *IRFU and IBU interconnection using single IDU*



It is not recommended to use external PSU for powering the IRFU via DC port in 1+1 configuration, as the redundancy functionality may be lost

Example of IRFU and IBU interconnection using the 1+1 full redundancy application with two IDUs:

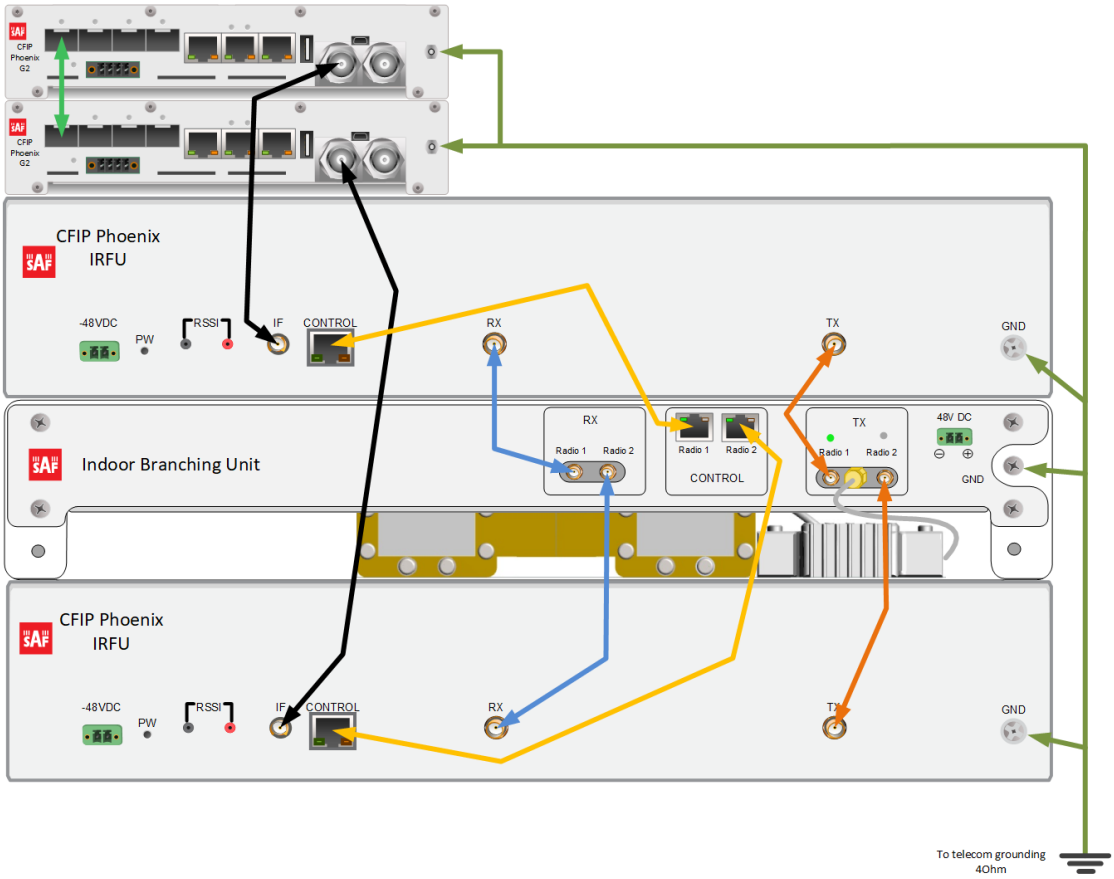


Figure 1.48 *IRFU and IBU interconnection using two IDUs*

More detailed information about recommended IRFU and IBU combinations, as well as IBU assembly and installation refer to *Phoenix G2 IBU filter assembly manual*

Chapter 2: INSTALLATION

Getting started

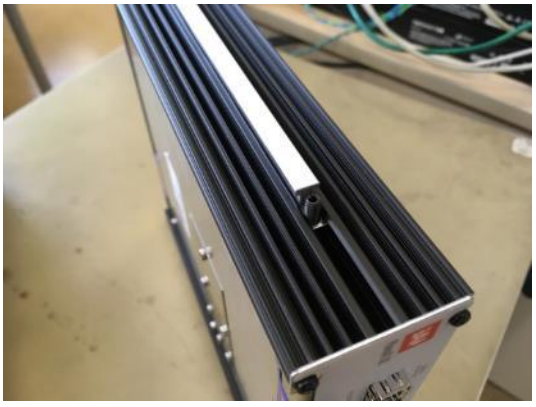
The installation of Phoenix G2 IDU and ODU link involves the following steps:

- Install the Phoenix G2 IDU in 19" rack: as the IDU is ½ width of the 19" inch rack position, there are two options how to install it in the rack:
  Option one: Single device installation: attach blank panel and bracket to the IDU (all included in the package). Install the IDU in the rack using attached blank panel and rack mount bracket.

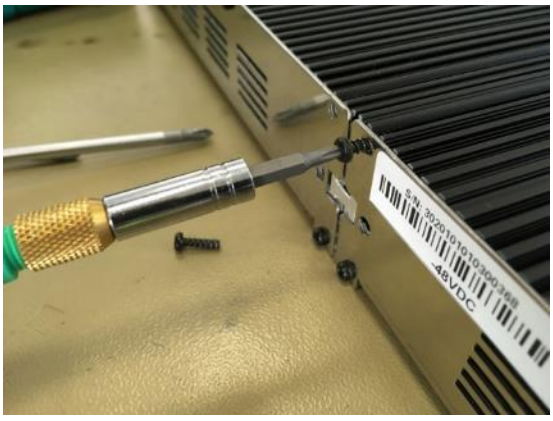


Figure 2.1 *Single device installation*

Option two: Dual device installation: interconnect two devices (IDU and EMM, or IDU with IDU) using dual device mount kit, attach brackets to each device. Brackets are included in the package of IDUs; dual device mount kit is included in EMM module package, and can be ordered as an optional accessory if two IDUs must be interconnected.
Dual device mounting kit includes aluminium mounting profile (P/N EASMEX03) which must be inserted in side panel grooves of IDUs thus fastening both devices together. In order to fix it and avoiding of both IDU movements use mounting plate (P/N WAKMEXS1.001) for fixation. The mounting plate must be attached to IDUs on back-panel using already existing screws from the IDUs. Those screws must be removed and used for attaching the mounting plate to IDUs.



1 Insert the aluminium mounting profile in side panel grooves of IDUs, fix it using setscrew with square nut



2 Remove 2 existing screws from both IDUs back panel



3 Attach the mounting plate to IDUs and fix it to IDUs using the same existing screws



4 Final view of back panel of interconnected IDUs

Install both devices in the rack using attached rack mount brackets.



Figure 2.2 *Dual device installation*

- Ground Phoenix G2 IDU by interconnecting it's grounding screw with the grounding point of the rack. For grounding cable requirements refer to *IDU front panel interfaces and LEDs* and *EMM extension modules description*
- In case if the Phoenix G2 IDU will be used in **1+0 Ch1** mode, connect ODU to the IDU's IF port **ODU A** with coaxial cable before turning on the power
- In case if the Phoenix G2 IDU will be used in **1+0 Ch2** mode, connect ODU to the IDU's IF port **ODU B** with coaxial cable before turning on the power
- In case if the Phoenix G2 IDU will be used in modes **1+1 Dual**, **2+0** or **1+1**, connect ODUs to the IDU's IF ports **ODU A** and **ODU B** with coaxial cables before turning on the power

In case of IDU tests in the lab without ODU, the IDU can be powered on without ODU connected, it will not damage the unit

Attaching Phoenix G2 ODU to antenna

SP/HP ODU with SAF radio interface

Tools required: SAF tightening tool

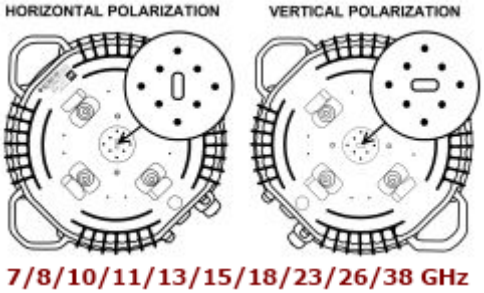


In order to attach SP/HP ODU to SAF adapted antenna use two guidance pins for fixing polarization and 4 side lockings for attachment. Lockings should be tightened in diagonal sequence.



Figure 2.3 *Locking of ODU with tightening tool*

Pair radios in licensed frequency bands 6 - 38 GHz use same polarization for Tx/Rx channels on both ends of the link – either horizontal, or vertical.

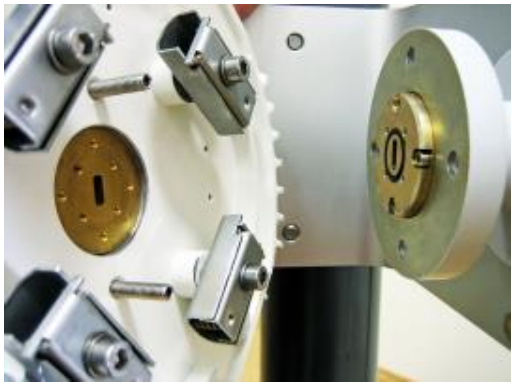


In case of 6GHz (N-Type connectors) polarization is determined by antenna and should be same on both ends of the link.

Examples:



7GHz (vertical polarization)



23GHz (horizontal polarization)

For extra protection from sun radiation it is recommended to install sun shield to cover the radio.

In order to attach the SP/HP ODU to SAF non-adapted antenna separated ODU mounting bracket (P/N S0SPKS03) and flexible waveguide/coaxial cable is required

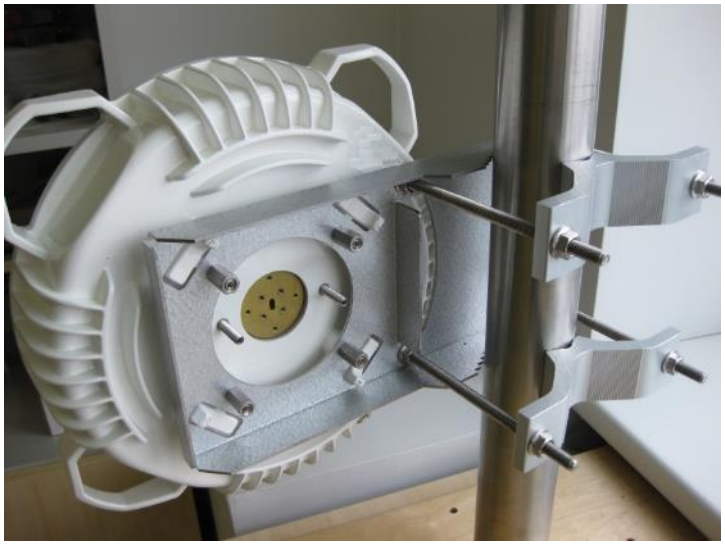


Figure 2.4 *SP/HP ODU with mounting bracket*

For instructions how to connect SP/HP ODU to mounting bracket refer to “SAF mounting bracket installation V1.0” document

VHP and SP/HP ODU with SAF2/SAF2R radio interface

Tools required: Size 5 Allen wrench, 240mm

Level for VHP ODU (not supplied)



Phoenix G2 VHP ODU 6-13GHz features twisted polarization flange and resulting signal polarization is determined by SAF2R interface on antenna radio adapter/OMT. Polarization is determined by the physical orientation of the radio adapter on the antenna. Radio position remains the same in case of both polarizations. The handle should be always positioned up, while traffic/service ports - down.

Phoenix G2 VHP ODU 18-23 GHz features square flange compatible with antenna SAF2 adaptation interface. The signal polarization can be changed by rotating the square flange on the ODU.

Phoenix G2 SP/HP ODU 15-38 GHz with SAF2 radio interface supports circular flange compatible with antenna equipped with SAF2 radio interface. Polarization is determined by the physical position of the radio relative to the ground. In some cases, the radio enclosure may have a sticker indicating the actual polarization depending on the radio position. Otherwise, all connectors on the side of the radio unit always have to stay at 45 degrees relative to its vertical axis in case of both polarizations.

Phoenix G2 SP/HP ODU 7-13 GHz with SAF2R radio interface supports rectangular flange which must match with the SAF2R interface flange position on antenna. Polarization is determined by the physical orientation of the radio adapter on the antenna. The orientation of the radio flange and the adapter flange should match. Both sides of the link should be set to the same polarization.

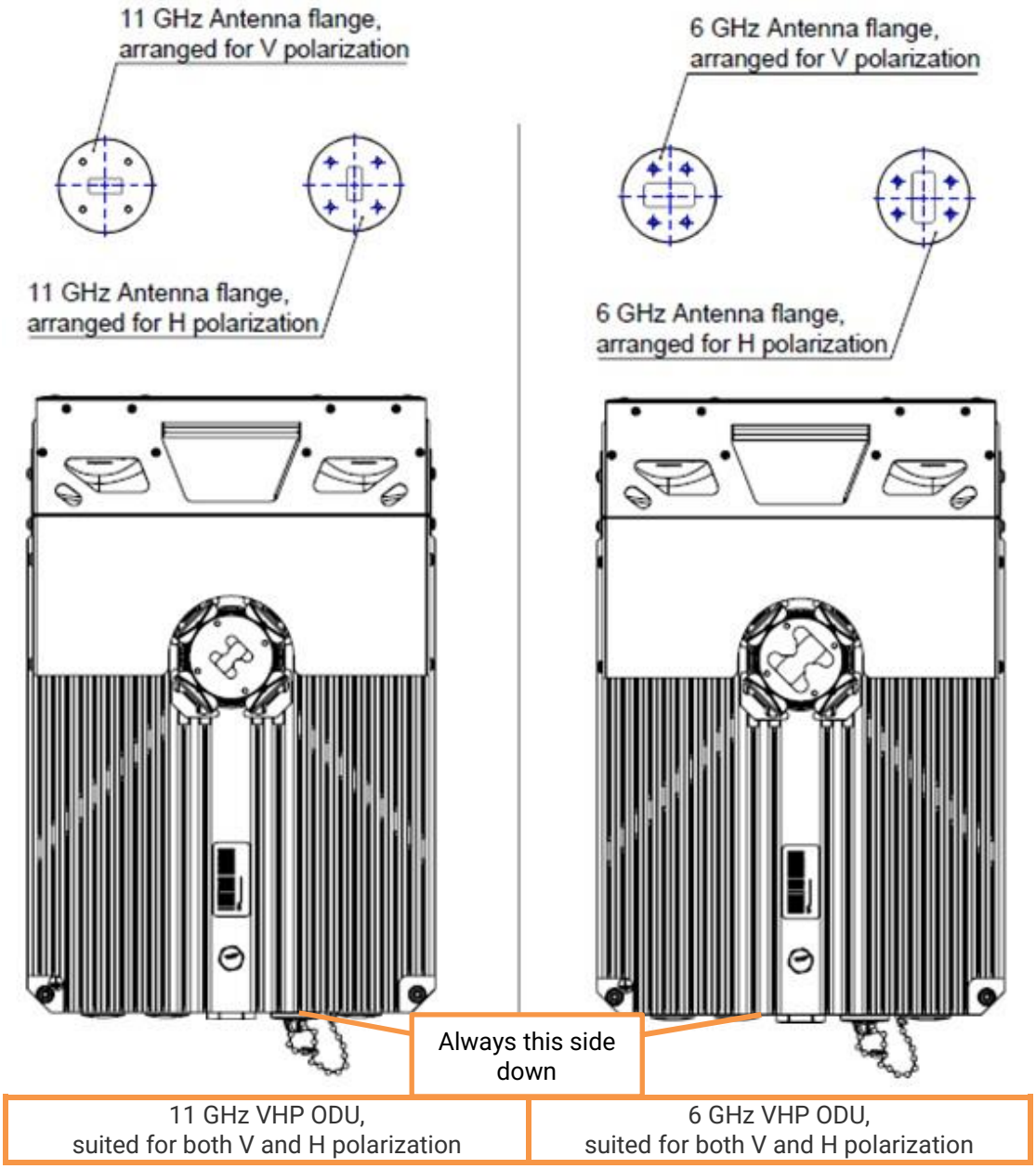
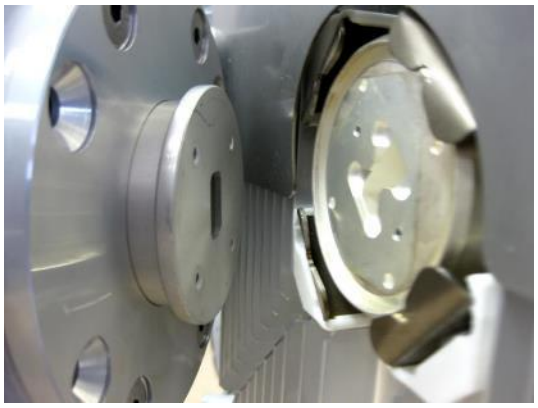


Figure 2.5 *VHP ODU 6-13 GHz flange*

Examples of VHP ODU 6-13 GHz polarizations:



Example of vertical polarization interconnection



Example of horizontal polarization interconnection

Examples of SP/HP ODU 7-13 GHz with SAF2R adaptation interface polarizations:

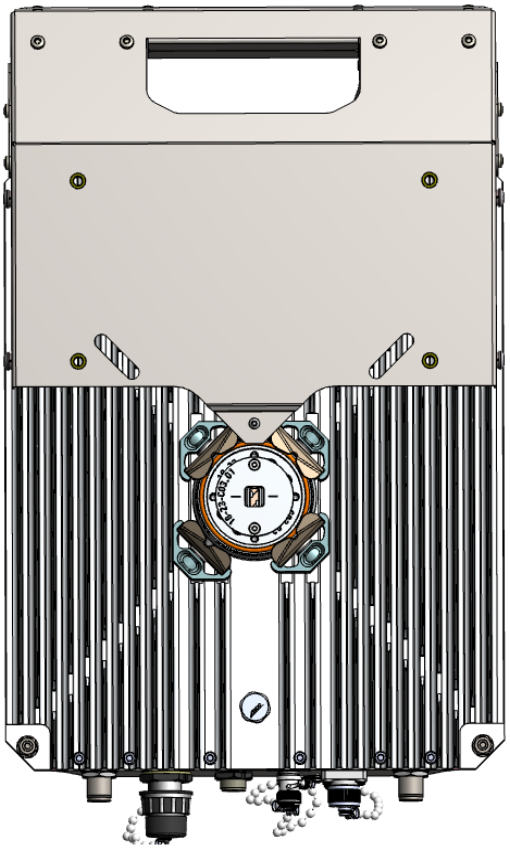


Example of vertical polarization

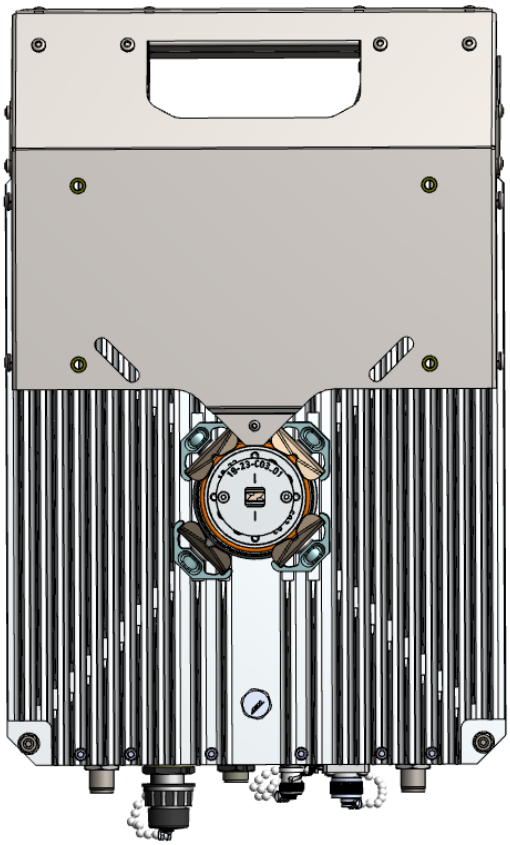


Example of horizontal polarization

Examples of VHP ODU 18-23 GHz polarizations. Polarization determination lines are engraved on the flange:



Example of horizontal polarization

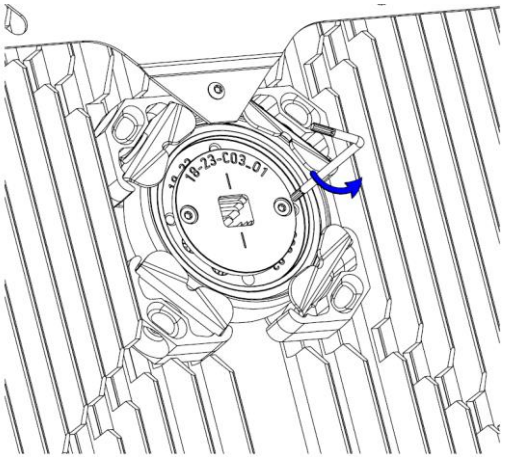


Example of vertical polarization

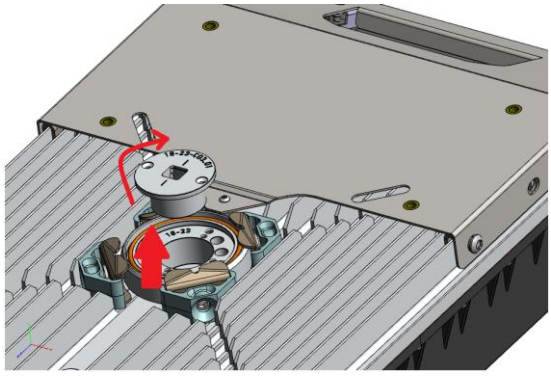
Polarization change on VHP 18-23GHz ODU can be done as per following instructions (if required):

Tools required: Torx T10 key

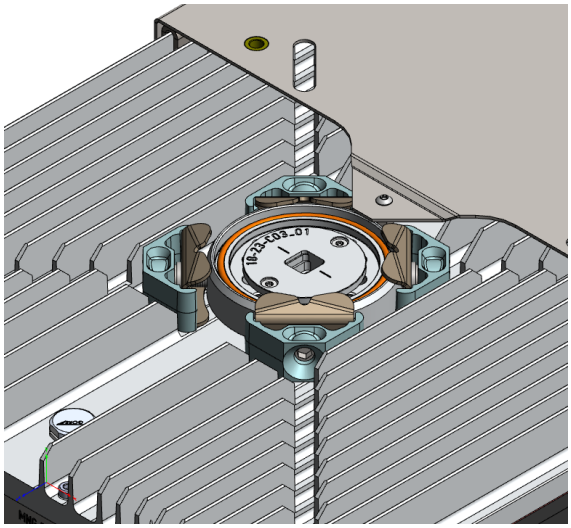




1 Unscrew both screws on the flange using Torx T10 key



2 When both screws are removed, lift the flange up, rotate by 90 degrees and plug it back into the radio.



3 Tighten the flange with the same two screws using Torx T10 key.

Steps of VHP ODU and SP/HP ODU with SAF2/SAF2R interface interconnection with antenna are given below:

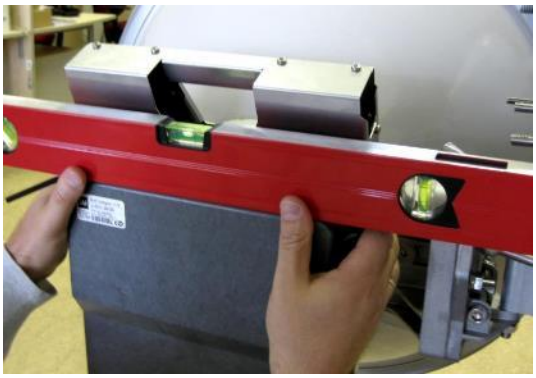


1 Put ODU on antenna adapter flange by hooking half-turn loosened clamp at the top and leaving the completely loosened clamp at the bottom. Make sure O-ring is in place and the adapter flange fits into the ODU transition flange socket.

Note! The protective sticker should be removed before attaching the ODU to the antenna.



2 Tighten bottom fixation clamps.



3 Use air level to verify that VHP ODU is properly levelled. Tighten all four fixation clamps properly.



4 Final view of assembled VHP ODU 1+0 setup.



5 Final view of assembled SP/HP ODU with SAF2/SAF2R adapter in Horizontal polarization



6 Final view of assembled SP/HP ODU with SAF2/SAF2R adapter in Vertical polarization

Acceptable angle of polarization tolerance of SP/HP ODU is up to 30º

In case of mounting the Phoenix G2 SP/HP ODU and VHP ODU directly on CommScope 1.8m VHLP series antennas, following specific requirements must be considered. The antenna mount orientation depends on the ODU type (SP/HP or VHP) is being used:

1) Proceed with standard CommScope 1.8m VHLP series antenna mounting as per antenna installation instructions (included in antenna package) when interconnecting it directly with SP/HP ODU
2) In case of VHP ODU direct interconnection with CommScope 1.8m VHLP series antenna following requirements must be noticed:
   a) The antenna mount/reflector must be installed with 180 degrees offset comparing with standard antenna mount/reflector mounting position
   b) 90° angle N-Type connector (P/N CLAANC01) must be used for IDU-ODU coaxial cable interconnection
   c) Dielectric silicone grease must be used to protect the 90° angle N-Type connector

In order to attach the VHP ODU to SAF non-adapted antenna separated ODU mounting bracket (P/N S0SPKS06 – for single radio; P/N S0SPKS09 – for two radios) and flexible waveguide/coaxial cable is required

If any further assistance is required, please contact techsupport@saftehnika.com

IBU installation

IBU installation into the rack

The IBU can be installed in 19” rack, it is equipped with adjustable brackets. The brackets allow to move the IBU in depth for 74 mm (2.9”). This can be done by loosening bracket fixation screws with size 5 Allen wrench.

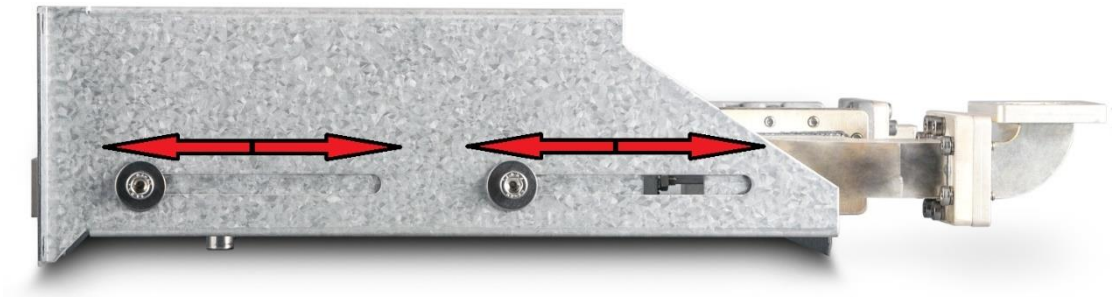


Figure 2.5 *Adjusting the IBU for installation into the rack*

IBU interconnection with IRFU

IBU and IRFU must be interconnected using short coaxial cables included in the IBU package. The Tx ports on the IBU must be interconnected with Tx port on IRFUs, and, accordingly, the

Rx ports of the IBU must be interconnected with the Rx port on IRFUs:

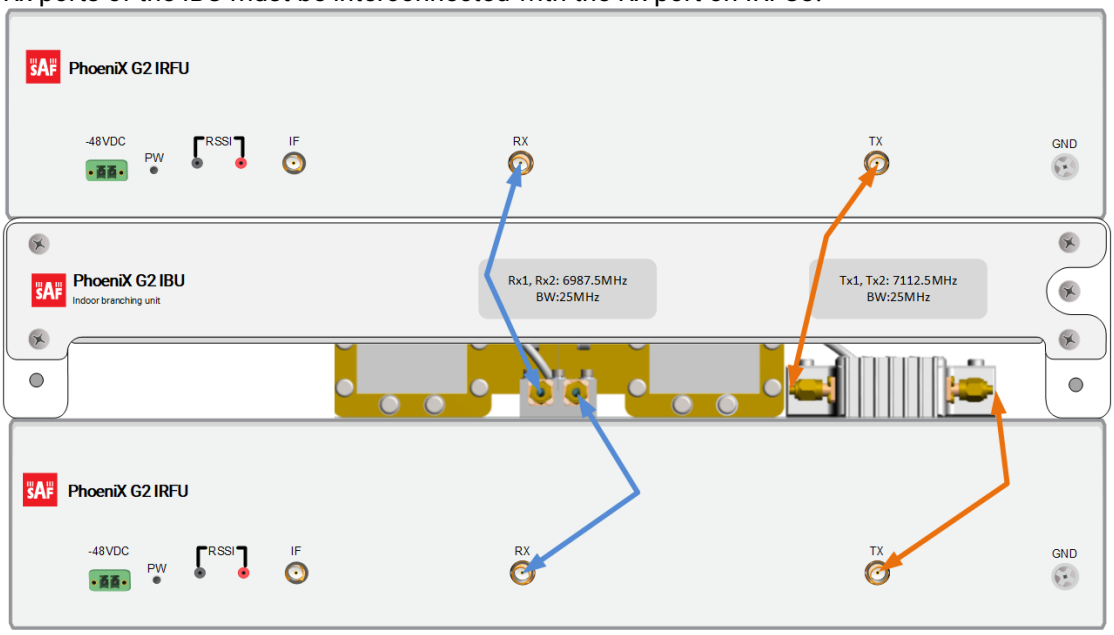


Figure 2.6 *IBU and IRFU interconnection*

In case of using active IBU, additionally the control ports (RJ-45) of IBU and both IRFUs must be interconnected with short Ethernet patch cables (included in the IBU package):

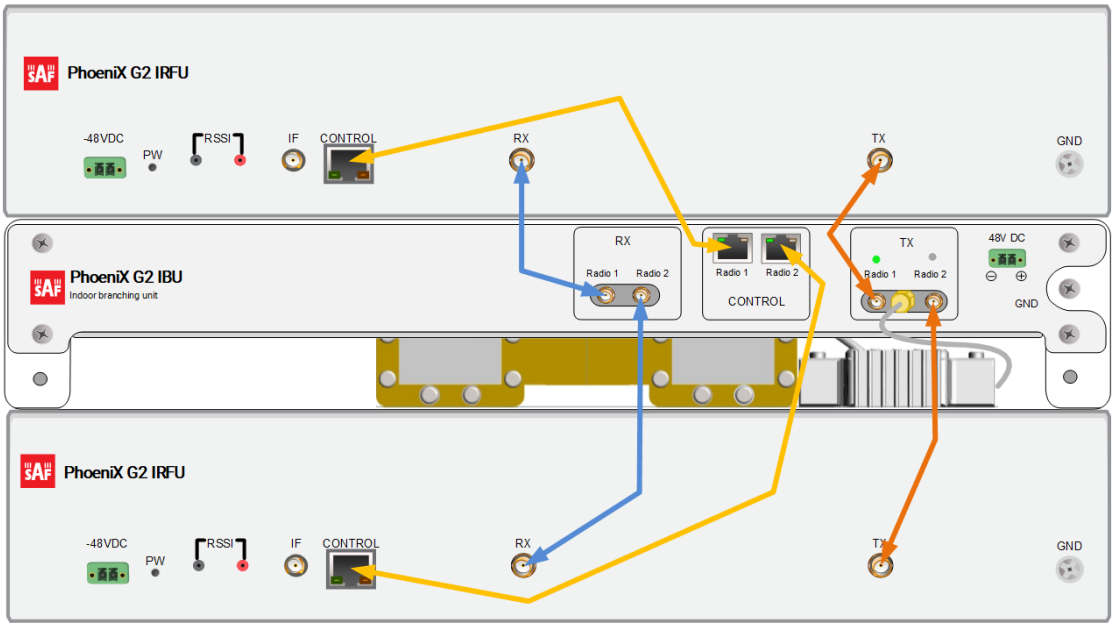


Figure 2.7 *Active IBU and IRFU interconnection*

Active IBU has DC port which must be connected to 48 V DC power source

As the active IBU contains active RF Tx switch, make sure the cable between the switch central port and the RF filtering system is connected. During transportation the cable might be disconnected from the central port of the Tx switch. Connect it if it was disconnected:



Figure 2.8 *Cable between RF Tx switch and RF filtering system on the active IBU*

IBU interconnection with waveguide/antenna

The antenna output/input port (one or two) is located on the back panel of the IBU. 90deg angle waveguide flange is connected to the antenna input/output port for easier interconnection with external waveguide. Therefore, the waveguide flange has standard UER flange size for each supported frequency band; and it can be removed if necessary. Top view of the IBU with 90-deg angle waveguide flange marked is shown in following figure:

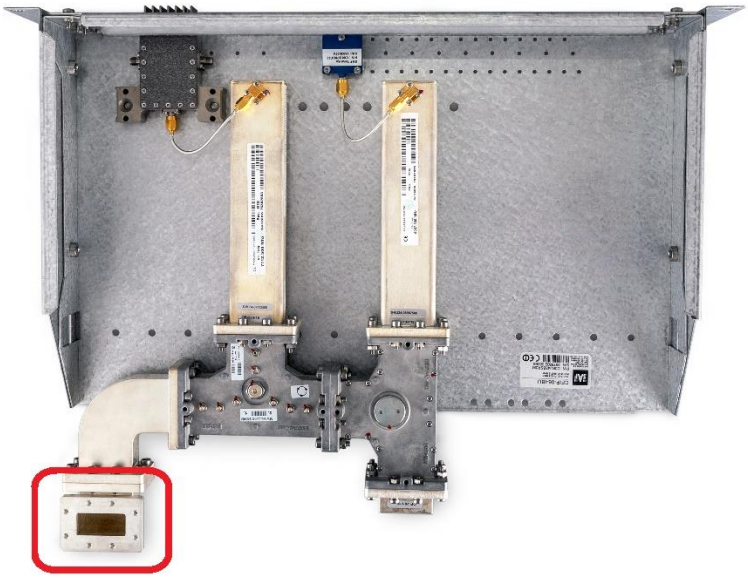
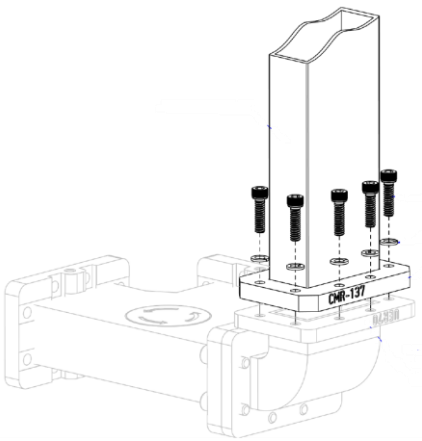
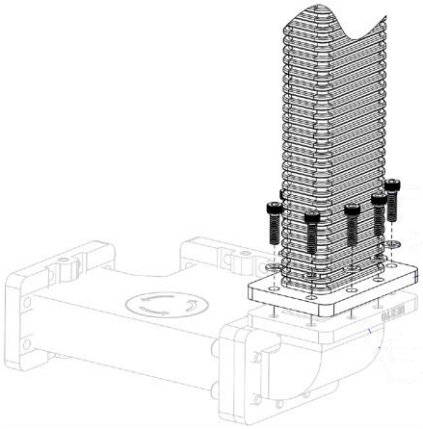


Figure 2.9 *Top view of the IBU, with 90-deg angle waveguide flange marked*

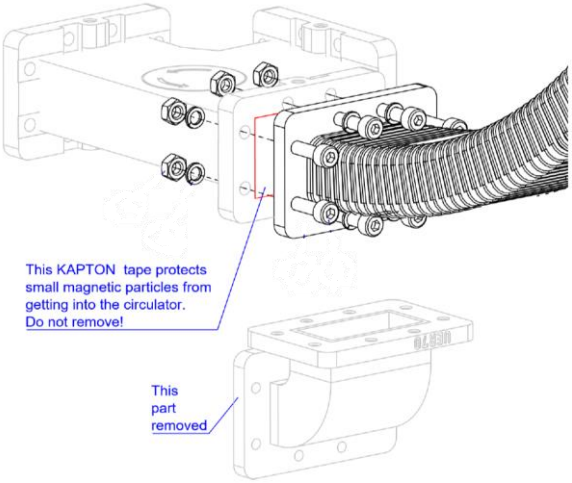
300mm seamless flexible waveguide is included in the IBU package for extension or extra flexibility, or for cascading of two IBUs. Some examples of IBU-waveguide interconnection:



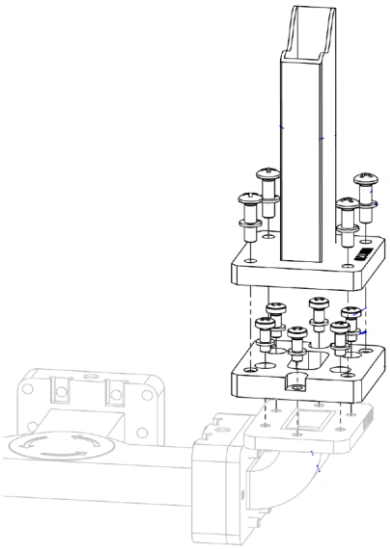
1 IBU waveguide flange direct interconnection with external waveguide



2 IBU waveguide flange interconnection with seamless flexible waveguide for extension, extra flexibility or for cascading the IBUs



3 IBU input/output port interconnection with seamless flexible waveguide with 90-deg angle waveguide flange removed. For extension, extra flexibility or for cascading the IBUs



4 Adapter plate can be used between the IBU waveguide flange and external waveguide if there are different flange types on each part. The same applies for external waveguide connection with seamless flexible waveguide

Cable requirements

IDU-ODU cable:

IDU–ODU cable is a 50 Ω coaxial cable intended to interconnect the Indoor Unit with the Outdoor Unit. Any type of 50 Ω cable of good quality can be used; the cable should be equipped with N–type male connectors on each end. There are two N–type male connectors included in each radio unit delivery that fit LMR400 cables or other cables with a surface diameter of 10 mm. As the attenuation of the cable is essential particularly at 350 MHz frequency, its usage is restricted, - the attenuation of the signal should not exceed 15 dB at 350 MHz. Along with the power supply to ODU, following frequencies are used for IF and telemetry in the cable between Phoenix G2 IDU and ODU:

- 350MHz: Intermediate Frequency from IDU to ODU
- 140MHz: Intermediate Frequency from ODU to IDU
- 4.5MHz: Telemetry Frequency from IDU to ODU
- 10MHz: Telemetry Frequency from ODU to IDU



Figure 2.10 *PhoeniX G2 IDU-ODU cable*

IDU-IRFU cable:

IDU–IRFU cable is a 50 Ω coaxial cable intended to interconnect the Indoor Unit with the Indoor Radio Unit. SAF Tehnika can provide LMR-240 type cable which is equipped with 90° N-type male connector for IDU connection and 90° SMA male connector for IRFU connection. The length of the cable can vary, depending on the purchased cable P/N code. For example, P/N CLAC2NS006 is 0.6m (2ft) long IDU-IRFU cable. Along with the power supply to IRFU, following frequencies are used for IF and telemetry in the cable between Phoenix G2 IDU and IRFU:

- 350MHz: Intermediate Frequency from IDU to IRFU
- 140MHz: Intermediate Frequency from IRFU to IDU
- 4.5MHz: Telemetry Frequency from IDU to IRFU
- 10MHz: Telemetry Frequency from IRFU to IDU



Figure 2.11 *PhoeniX G2 IDU-IRFU cable*

DC power cable:

Any good quality 2 wire power cable with the minimum wire cross-section of 2x 1 mm2 which fits well in SAF Tehnika's supplied single block 4 pole "screw on" power connector can be used. Recommended maximum length of the DC power cable is up to 2 m. The power connector is 2 pole, type 2ESDV-04P.

USB B Serial Connection:

USB B management port must be used for management access with alternative IP address. This requires USB cable (USB A connector – computer side / USB mini B connector – IDU side).



Figure 2.12 *PhoeniX G2 USB management cable*

RSSI BNC cable:

To connect the digital multimeter to the PhoeniX G2 ODU RSSI port in order to adjust the antenna alignment, a coaxial cable with BNC connector on one end and appropriate termination on other end can be used (P/N CLGCRS01).



Figure 2.13 *Cable for connecting the multimeter to the PhoeniX G2 ODU RSSI port*

Optical cable:

Optical cable supporting 1 Gbps must be used to interconnect PhoeniX G2 IDU and EMM (ASI or E1) modules. Either Single-mode or Multi-mode optical fiber can be used. The same type SFP modules have to be installed in both devices PhoeniX G2 IDU and EMM. In order to interconnect two Phoenix G2 IDUs for 1+1 Full redundancy configuration 2.5 Gbps optical cable and SFP modules must be used (recommended cable kit P/N I0ASMK02). Maximum length of optical cable is limited by sensitivity of SFP modules.



Figure 2.14 *Optical cable and SFP modules for Phoenix G2 IDU and EMM module interconnection*

Powering Phoenix G2 IDU/ODU

Next step is to interconnect LLM IDU DC power connector with power source using power cable. In case AC/DC Power supply, 48VDC, 80W (EU - P/N I0AB4810, US – P/N I0AB4811, AUS – P/N I0AB4818) provided by SAF Tehnika JSC is used to power up PhoeniX G2 IDU, interconnect IDU and power source through appropriate connectors. Otherwise perform the following steps to ensure that PhoeniX G2 IDU is powered up correctly:

1. It is necessary to interconnect PhoeniX G2 IDU DC power connector (located on left side of front panel) with power source. For this purpose power cable is required. Any 2 wire power cable of good quality which fits well in SAF Tehnika's supplied 4 pole "screw on" power connector could be used. The power cable connector is 4 pole, type 2ESDV-04. This connector has screw clamp terminals that accommodate 24 AWG to 12 AWG wire. The recommended wire size for construction of power cables under 3 meters in length, supplying -48 V DC, is 18 AWG. The opposite end of the power cable should have a termination appropriate for the power supply being used. The power cable should be of sufficient length to avoid tension in the cable and provide a service loop for connection, but not be of excessive length. Using the power cable connector of type 2ESDV-04, pins 1/2 (labelled '-') should be connected to the power supply terminal supplying -48 V DC, while pins 3/4 (labelled '+') should be grounded. Refer to ***Figure 2.15***.



Note that pins 3/4 ('+') of the PhoeniX G2 IDU DC Power connector (***Figure 2.15***) is connected to the IDU chassis ground internal to the IDU. Use of a power supply with an inappropriate ground reference may cause damage to PhoeniX G2 IDU and/or the power supply.

2. Connect the power cable to the -48 V DC power supply, and place the voltmeter probes at the unconnected ends of the power cable, with the positive voltmeter probe on pin 1/2 ('-') of the cable connector and the negative probe on pin 3/4 ('+'). The connector screw terminal screw heads may be used as convenient monitor points. Refer to ***Figure 2.15***.
3. Turn on the –48 V DC supply. Verify that the digital voltmeter reads between -36 V DC and -57 V DC when monitoring the cable points specified above. Adjust the power supply output voltage and/or change the connections of the power supply to achieve this reading.
4. With the negative voltmeter probe still on pins 3/4 ('+') of the power cable connector (and the power supply still on), put the positive voltmeter probe to the PhoeniX G2 IDU chassis and verify a potential of zero volts between the IDU chassis and cable pins 3/4 ('+'). If the measured potential is not zero, the power supply may be grounded incorrectly and should not be used for PhoeniX G2 IDU powering. Note that this measurement assumes that PhoeniX G2 IDU is installed and properly grounded. If that is not the case, the same measurement can be made between cable pins 3/4 ('+') and a convenient ground (such as an AC outlet third-wire ground).
5. Turn the -48 V DC supply off.
6. Plug the power cable into PhoeniX G2 IDU front panel DC Power connector (**DC port**). Place the voltmeter probes on the cable connector screw terminal screw heads as described in step 2 above. Refer to ***Figure 2.15***. Note that PhoeniX G2 IDU does not have a power on/off switch. When DC power is connected, the digital radio powers itself up and is operational. There can be up to 500 mW of RF power present at the antenna port. The antenna should be directed safely when power is applied.
7. Turn on the -48 V DC power supply, and verify that the reading on the digital voltmeter is as specified in step 3 above.

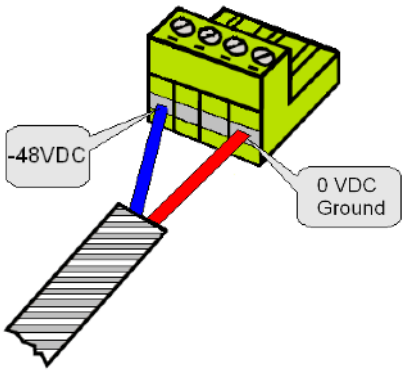


Figure 2.15 *Phoenix G2 IDU DC Power Cable Connector of type 2ESDV-04*

Depending on the ODU type and supported frequency the power consumption of one Phoenix G2 IDU and 2xODUs can be up to 180 W. So this should be taken in account when choosing power adaptor.

Use 5-10 A rated type B circuit breaker in the chain between the 48 V power supply and the IDU.

Powering External Multiplexer Modules (EMM)

The External Multiplexer Module (ASI, E1/T1) unit (if used) must be connected to the power supply separately, with a nominal voltage of -48 VDC and GND must be connected to the positive pole. Connector type 2-pin MC 1,5/ 2-STF-3,81 is supported. Its power consumption is <9 W.

Powering Phoenix G2 IRFU

PhoeniX G2 IRFU (if used) can be powered via coaxial IF cable or using separate power supply, providing at least 60W load power.

It is not recommended to power the IRFU via DC port in 1+1 Full protection and in 2+2 Full protection configurations, as the 1+1 switching algorithm is based on the standard powering of the radio via IF port from the IDU

Note that pin 2 ('+') of the PhoeniX G2 IRFU DC Power connector is connected to the IDU's internal chassis ground. Use of a power supply with an inappropriate ground reference may cause damage to PhoeniX G2 IRFU and/or the power supply.

Powering active IBU

The active IBU unit (if used) must be connected to the power supply separately, with a nominal voltage of -48 VDC. "+" and "-" polarities are indicated on the label at the DC port. 2-pin power supply connector is included in the package.

Chapter 3: WEB GUI

Initial configuration

System requirements

To access PhoeniX G2 IDU Web GUI you will need a PC with the following system requirements:

Operating system

- Microsoft Windows XP / Vista / 7 / 8/10;
- Linux

Web browser

- Google Chrome;
- Mozilla Firefox;
- Internet Explorer 8 (or above)



Ethernet management connection configuration

Before proceeding with initial link setup in Web GUI, you must adjust IPv4 settings of your LAN adapter to 10.10.10.0 subnet. IP address should be other than default IP address (10.10.10.10).

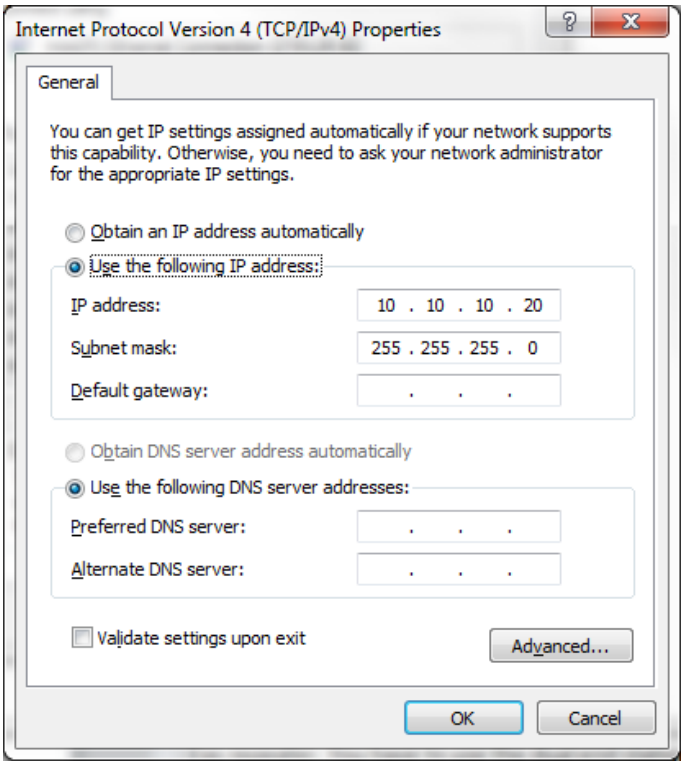


Figure 3.1 *TCP/IPv4 Properties*

After applying these settings you are ready to connect to Web GUI or establish SSH/Telnet connection.

USB Management connection configuration

In case MNG USB B serial port is used for Web GUI access, following steps can be taken:

- Interconnect PC with USB B port of the IDU using USB/USB mini B cable (USB A connector – computer side / USB mini B connector – IDU side). USB cable is shown in ***Figure 2.6***
- If the connection is done for the first time, wait while device driver software will be installed automatically. If it does not happen automatically, contact SAF Technical support.
- If driver is successfully installed, in PC's Network Connection panel new network adapter will appear:

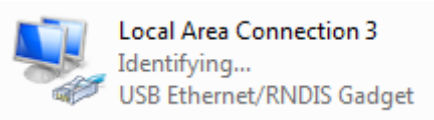


Figure 3.2 *PC IP USB setup – USB network adapter*

- Adjust IPv4 settings of USB Ethernet network adapter to 10.10.11.0 subnet. IP address should be other than default IP address (10.10.11.10).

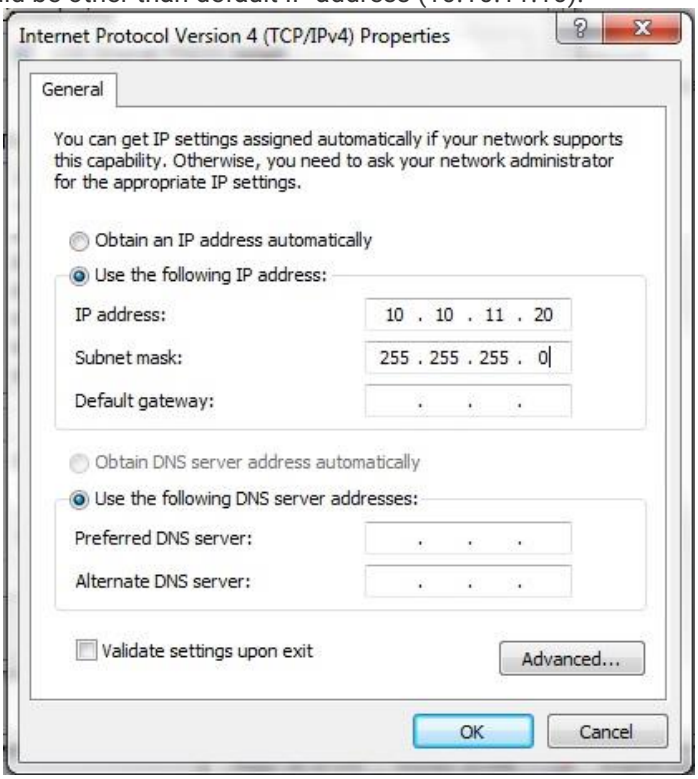


Figure 3.3 *TCP/IPv4 Properties*

After applying these settings you are ready to connect to Web GUI.

Accessing PhoeniX G2 IDU Web GUI

1. Connect your PC to MNG LAN 3 port on PhoeniX G2 IDU with Ethernet patch cable.
2. Launch your Web browser and in address field enter PhoeniX G2 IDU IP address. Default IP address is 10.10.10.10.

Another management access options are following:

- LAN 3 port - IP Address 10.10.10.10, Netmask 255.255.255.0 - factory default
- LAN 3 port - IP Address 192.168.2.95, Netmask 255.255.255.0 - configurable alternative

- MNG USB port - IP Address 10.10.11.10, Netmask 255.255.255.0 - factory default
- MNG USB port - IP Address 192.168.11.10, Netmask 255.255.255.0 - configurable alternative

Depending on your WEB Browser you may be warned that the device has a self-signed certificate and thus it is not secure to connect to it. To avoid this message you have to either setup device certificates or allow an exception for the target IP. This exception needs to be set up once per each IP address and WEB browser.

3. Press “Enter” key.
4. Login screen will appear.
5. Enter username and password. Default credentials are as follows:
   - Username: **admin**
   - Password: **secret**

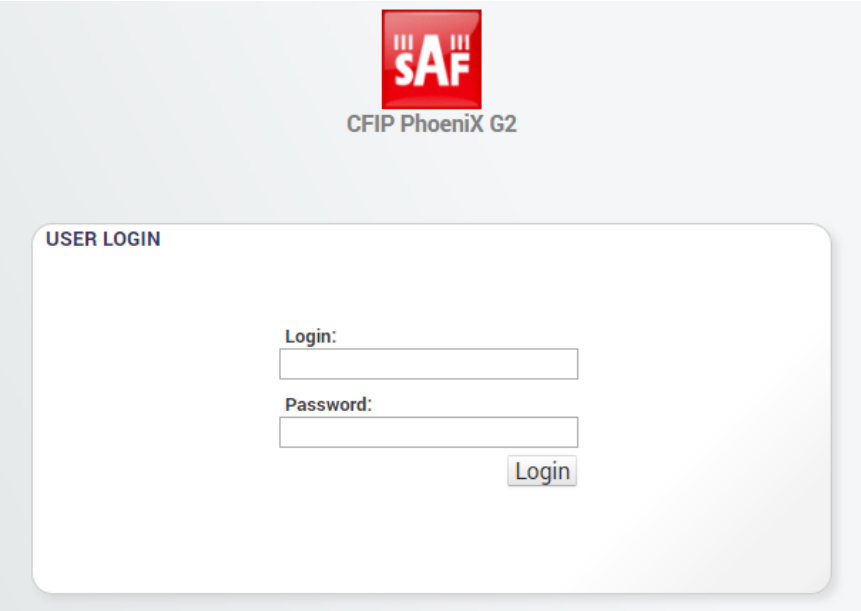


Figure 3.4 *Login screen*

6. Press Login button.

The WEB GUI interface requires enabled JavaScript in your browser.

There are three access levels available. Default access details for each level are following:

ACCESS level	LOGIN name	Password
Administrator	admin	secret
User	user	test
Guest	guest	*no password*

Web GUI description

The WEB GUI is designed as a standalone web application which receives status updates from the device. This communication is done asynchronously; thus it may take a while until the change is reflected in the GUI. WEB interface consists of five parts, those parts are following:

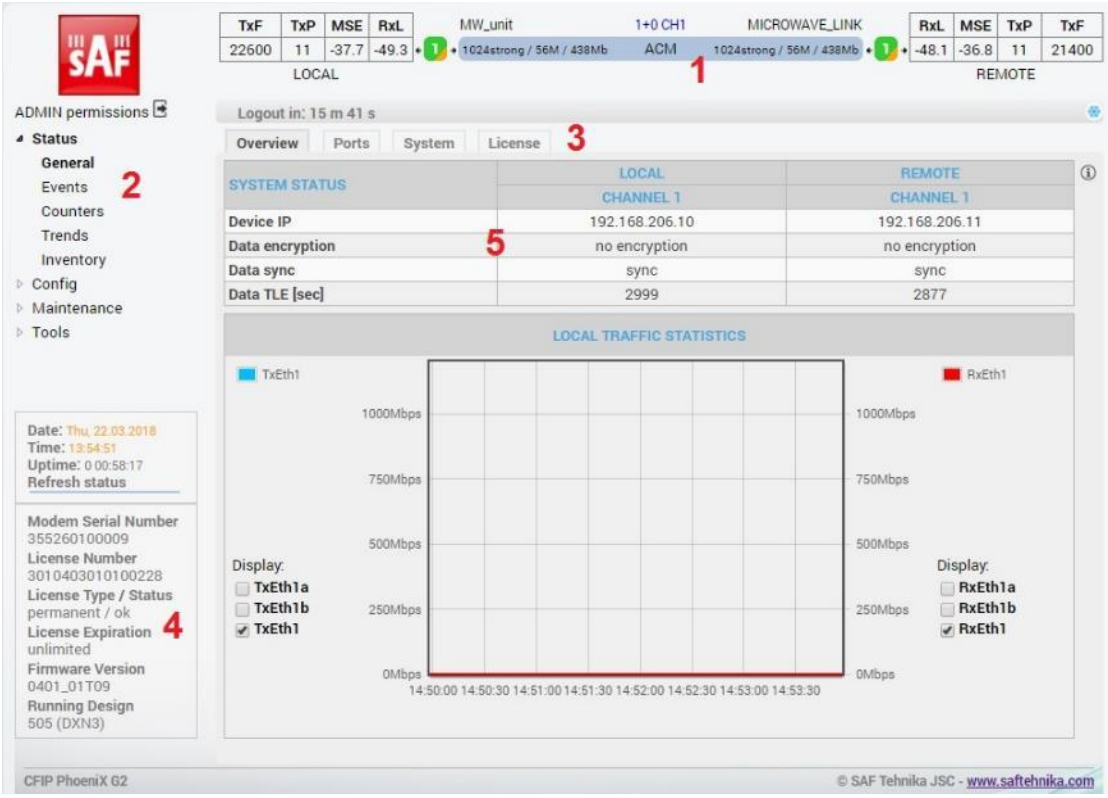


Figure 3.5 *PhoeniX G2 web GUI*

Web GUI is divided into 5 sections:

1 Header and status bar

The header displays the actual link condition. The RF path diagram varies depending on the used Design and Mode setting. In the Split 511 design, the actual Local Primary unit is displayed in the first header row, the Local Secondary on the second row. Bold font highlights the actually managed unit. The physically linked RF units are always in the same row. The displayed speed is average maximal throughput per last second. Meaning of the used graphics is described in the following picture:

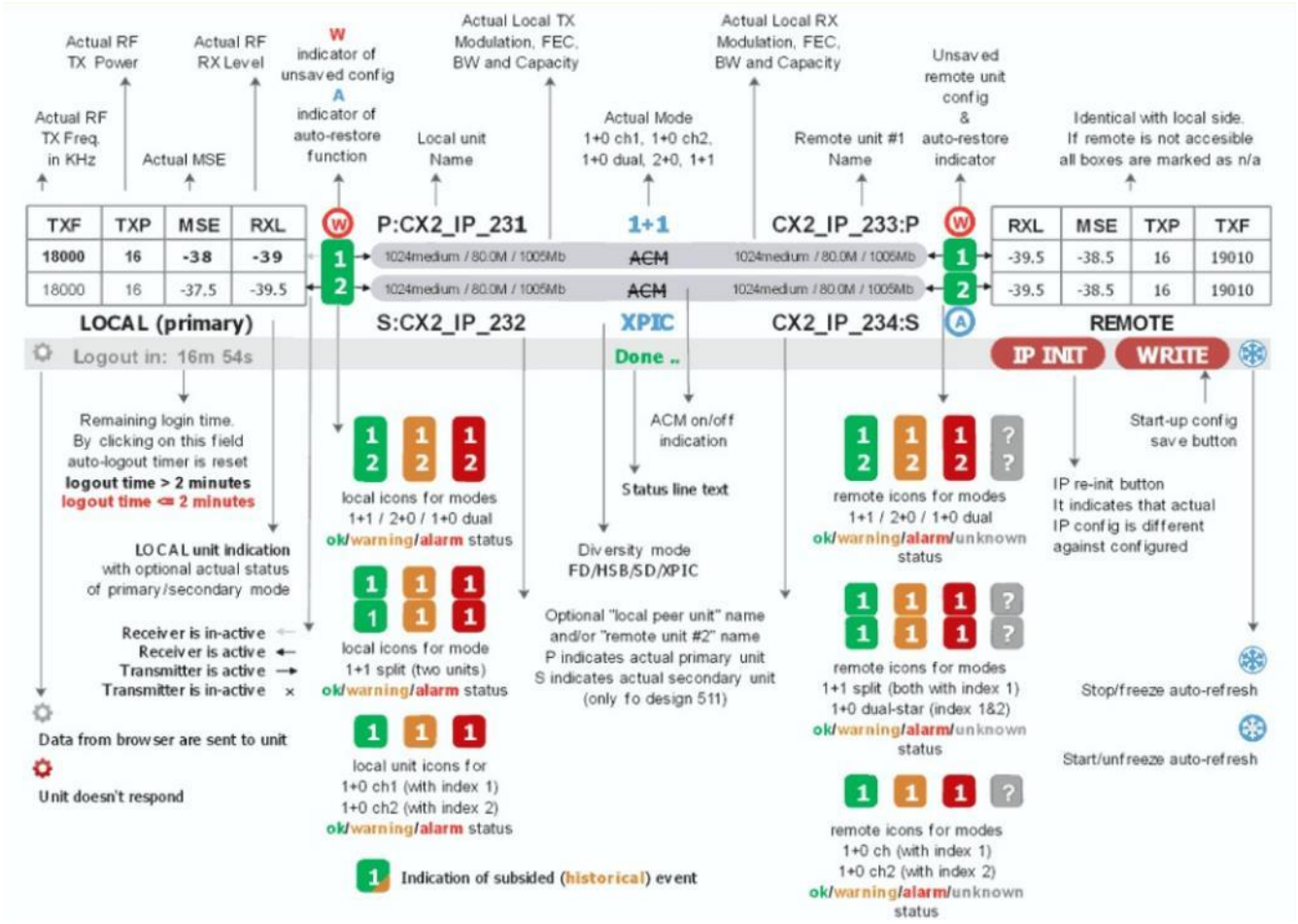


Figure 3.6 *PhoeniX G2 web GUI header and status bar*

2 Two level menu and Login/Logout box

Allows navigating between main pages and sub-pages. The user can expand the menu tree structure either by using the arrows on the left or using double-click on the desired section. The menu tree structure is sorted in the following manner to allow successive configuration and monitoring: :

- **Status** - informational section designed for link performance monitoring
- **Config** - configuration section. The user can perform configuration of all necessary parameters from top to bottom as some options may override consecutive settings, for example, the Design and Mode change invokes a preset load and changes page layout of the Ports section. It is highly recommended to save and reboot the device once the first complete configuration is done.
- **Maintenance** - a device management section which houses tools for device configuration backups, FW/License upgrade, log files and troubleshooting sections, and reboot.
- **Tools** - set of various tools for advanced debugging tasks such as Ping, Terminal, Constellation and Spectrum analysis.

3 Third level menu

Allows navigating between 3rd level pages of each subpage

4 Side bar frames

The Side Bar located on the left side of the GUI shows the summary of important device information:

- **Date** – system date

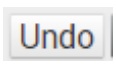
- **Time** – system time
- **Uptime** – time since startup
- **Refresh status** – indicates the amount of time until the next GUI refresh. The bar changes its colour to red if the GUI auto-refresh is frozen through the  button. The refresh interval of information shown in the GUI is automatically calculated by the device depending on actual transmission speed between the WEB browser and the device. The minimum refresh interval is 2 seconds, the maximal then 30 seconds.
- **Modem Serial Number** – device Serial Number. It is shown only when it differs from the License Number
- **License Number** – the license number
- **License Type / Status** – shows if the license is permanent or time-limited and its status
- **License Expiration** – shows the remaining time until the license expires.
- **Firmware Version** – version of the device firmware.
- **Running Design** – active design type.

5 Information field

Shows monitoring and configuration pages chosen in menu.

Button conversion and configuration box description

There are multiple buttons available across the GUI interface. Buttons have distinctive colors depending on the effect on the system: pressing the red button may cause immediate data drop or direct overwriting of start-up parameters in flash memory; pressing the grey button has not effect; pressing the blue button alters the running configuration but such configuration needs to be stored by means of the WRITE button else it will not persist through the device reboot; and the white button has only data refreshing option, but such action does not alter the running or stored configuration. Most common button types used in the WEB GUI are following:

Button	Function
	Opens Help/information page
	Shown in the status bar when there are unsaved changes on a connected device in the link. Using this button, you update the startup configuration by actually running configuration on all linked units.
	Shown when a value is modified directly in flash memory but command activation requires either parameter initialization or system reboot, for example, IP settings.
	Shown when there are pending changes in the IP settings. By pressing this button, the device performs a network interfaces reset. Note, this action does not cause the user data outage, but it disconnects all active management sessions (GUI, CLI, SNMP).
	Apply all the changes at current GUI page or in a respective frame.
	Revert all unconfirmed changes in a respective frame.

Refresh	Shown only on pages which contain values which are not automatically refreshed. It pulls information from the device and renders it on the screen.

The colour of configuration value entered in a setting box indicates the status of the following value:

- **black** – unmodified value
- **blue** – modified but non-applied value
- **red** – entered value does not match the allowed range
- **purple** – the actual configuration does not match the required modem settings.

Setting input boxes may change its border colour to red if the entered value is not applicable, for example, invalid IP address or a character in an integer-type field. In such event, the Apply button is hidden until the problem is fixed.

Configuration of basic system parameters

In order to establish the link, following main configuration steps should be performed:

1) **Step 1** – in web GUI navigate to "*Config → System → Mode*" and specify ***Design Type***, ***Duplex mode*** and ***Functional Mode***. With those settings user defines the basic configuration of the equipment:
   a) 1+0 single channel configuration,
   b) 1+0 dual channel configuration,
   c) 1+0 star configuration
   d) 1+1 (HSB, FD, SD, XPIC) standard redundancy configuration,
   e) 1+1 (HSB, FD, SD) full redundancy configuration,
   f) 2+0 FD aggregation configuration,
   g) 2+0 XPIC aggregation configuration
   h) Bidirectional transmission
   i) Unidirectional transmission

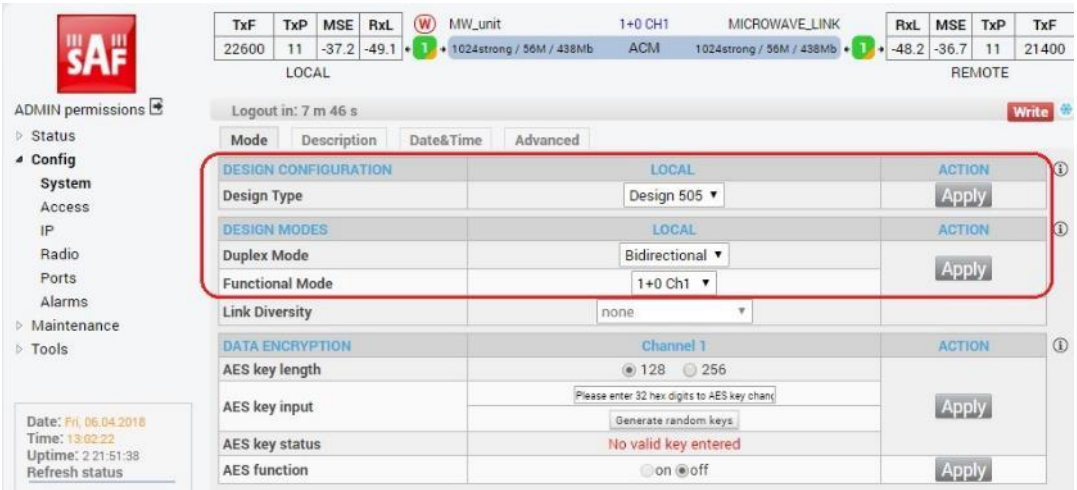


Figure 3.7 *Design and modes configuration*

2) **Step 2** – in web GUI "*Config → IP → Addresses*" configure ***IP address/subnet mask*** and ***Gateway IP*** address of the IDU.



Figure 3.8 *IP address configuration*

3) **Step 3** – in web GUI "*Config → Radio → Parameters*" set ***Bandwidth*** and Max ***RxACM Profile*** settings for modem, and ***Tx Frequency***, ***Tx Power Limit*** and ***Tx Mute Config*** settings for radio

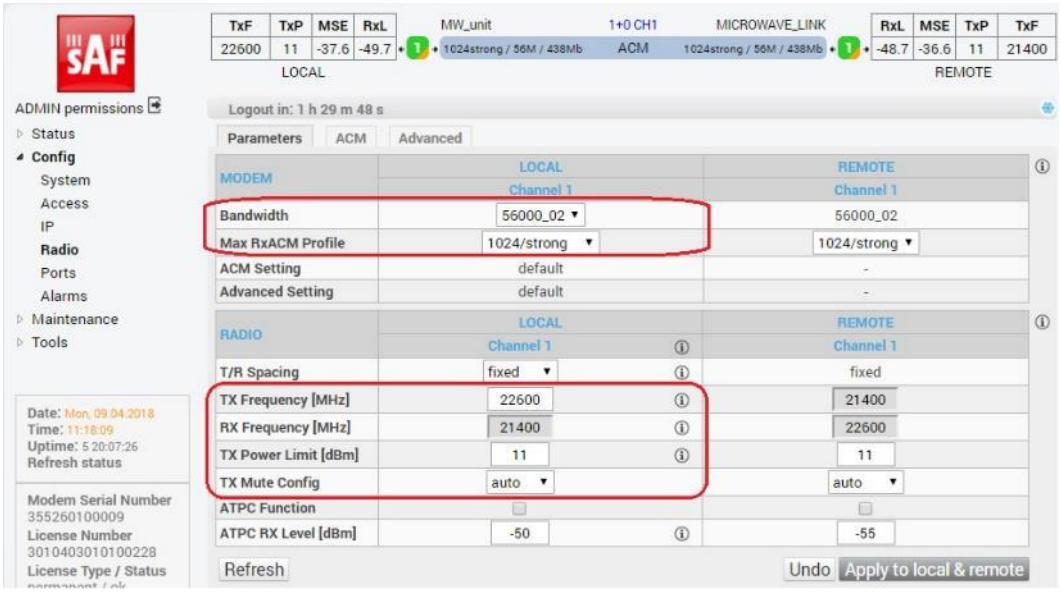


Figure 3.9 *Modem and Radio parameters configuration*

4) **Step 4** – in web GUI "*Config → Ports → EthVLAN*" specify **port grouping** to enable required type of management access and port groups.

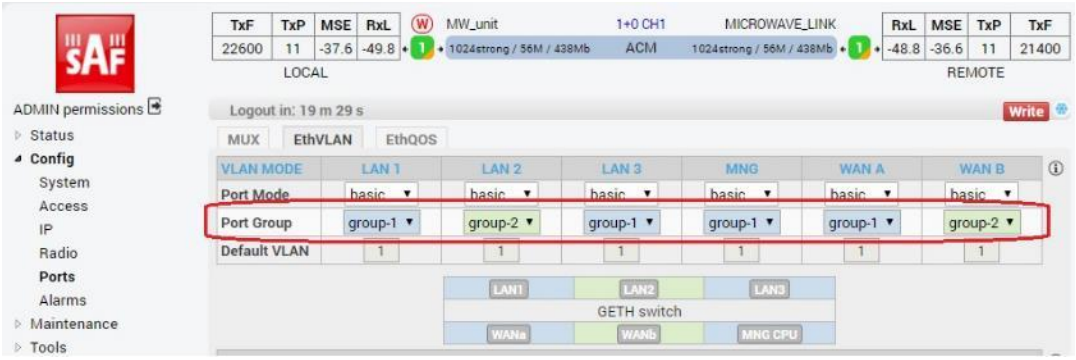


Figure 3.10 *Port group configuration*

5) **Step 5** – save configuration by pressing Write button.

Management channel configuration options

There are several options for accessing the remote side management from or via local device:

- In-Band management
  - User data and management data share the common link capacity and are separated by a VLAN
- Out-of-Band management
  - Using internal management channel (NAT) through separate management channel
  - Management alone in a separate traffic channel

In-Band Management

In-Band management configuration with management traffic separation by means of VLAN is a preferred scheme when just one ETH connection (management & data traffic) into microwave link is accomplished. Communication with the remote side is ensured by sharing the capacity for data and management traffics through internal ETH switch. The management data together with the user data are brought via the common Gigabit cable from the external Ethernet switch to the device, and the same VLAN is then used in the whole management network for management traffic separation. For Port group and VLAN configuration refer to *Config → Ports → MUX* and *Config → Ports → EthVLAN*

The advantages of such option are following:

- Fast management access to local and remote device
- Just one Ethernet cable is required for data and management traffic connection

The disadvantages of such option are following:

- Management traffic shares capacity with the data traffic
- It is required to know what is the type of customer traffic, especially VLAN configuration at provider and customer side

Out-Band Management

1) **Using Internal Management Channel (NAT)**:
   Out-Band management configuration with NAT is a preferred scheme when just one link is supervised and management access is originated from provider side of the link. Management and data traffic must be separated at provider side in this mode. Communication with the remote side is ensured through fixed internal management channel. Management traffic is routed through management CPU inside the device. The device has an option to auto-configure the NAT setting under section *Config → IP → Advanced*.
   For the NAT auto-configuration it is possible to enable one or both of these options:

a) **WEB** – this option will add automatic NAT records for accessing the remote device's WEB GUI. The default values are as follows (the IP portion is only an example and depends on actual running IP configuration):

1443 192.168.3.91:443	Remote IDU's GUI accessible on local port 1443
2443 192.168.3.92:443	Second remote (in 505 1+0 dual mode with two separate remotes) or direct FO neighbor (in Split Protection mode) IDU's GUI accessible on local port 2443
3443 192.168.3.93:443	Indirect remote FO neighbor (ergo 'cross-corner' in split protection mode) IDU's GUI accessible on local port 3443

b) **SSH** – this option will add automatic NAT record for accessing the remote IDU's SSH. The default values are as follows (the IP portion is only an example and depends on actual running IP configuration):

1022 192.168.3.91:22	Remote IDU's GUI accessible on local port 1022
2022 192.168.3.92:22	Second remote (in 505 1+0 dual mode with two separate remotes) or direct FO neighbor (in Split Protection mode) IDU's GUI accessible on local port 2022
3022 192.168.3.93:22	Indirect Remote FO neighbor (ergo 'cross-corner' in split protection mode) device's GUI accessible on local port 3022

Example:

The local device has IP address of 192.168.3.90 and remote 192.168.3.91, the NAT records of local device for accessing the remote will be these:

- 1443 192.168.3.91:443
- 1022 192.168.3.91:22

To access the remote device's GUI, it is required to open a new page in WEB browser and navigate to address 192.168.3.90:1443. Note this is the address of the local device plus port which is then redirected according to the appropriate NAT record to the remote side. The SSH access is realized in the same manner.

The advantage of such option is following:

- Separate management channel for local and remote device access. The whole system capacity is available for data traffic

The disadvantage of such option is following:

- The management traffic uses dedicated slower channel; therefore, management responses are little longer in comparison to the In-Band management scheme

2) **Management in a Separate Channel:**
Out-Band management configuration in a separate channel is a preferred scheme when more links in series are managed, and the management access is originated from any device in such link or from provider's management node. The communication with the remote side is ensured by means of a configurable separated traffic channel. Management and data traffic are separated at provider side, and they are then kept separated by a reserved standalone channel through radio links. Management access is available also from opposite side (customer side) by a similar configuration of the channel separation.
This configuration can be achieved on the section *Config → Ports → EthVLAN* where user have to put the MNG, the dedicated management LAN3 port and one WAN channel into the same group. Simultaneously user needs to put the remaining WAN port, and user data LAN port into a different group than the management ports are in. Finally, on the section *Config → Ports → MUX*, user has to configure the speed limit for both management and data. It is recommended to assign 2Mbits for the

management channel. The management channel should have the highest priority. Note that the port priority is falling from left to right.

The advantages of such option are following:

- Easy configuration
- Allows ICMP packet transfer (ping)

The disadvantages of such option are following:

- One whole traffic channel has to be dedicated to such management
- The management and data have to be separated in the switch before the device
- A network loop risk when link operates within a single network

Status

Status → General → Overview

It indicates overall system status. Indicated system parameters will depend on configured functional mode. EMM status information will appear only if EMM will be enabled.

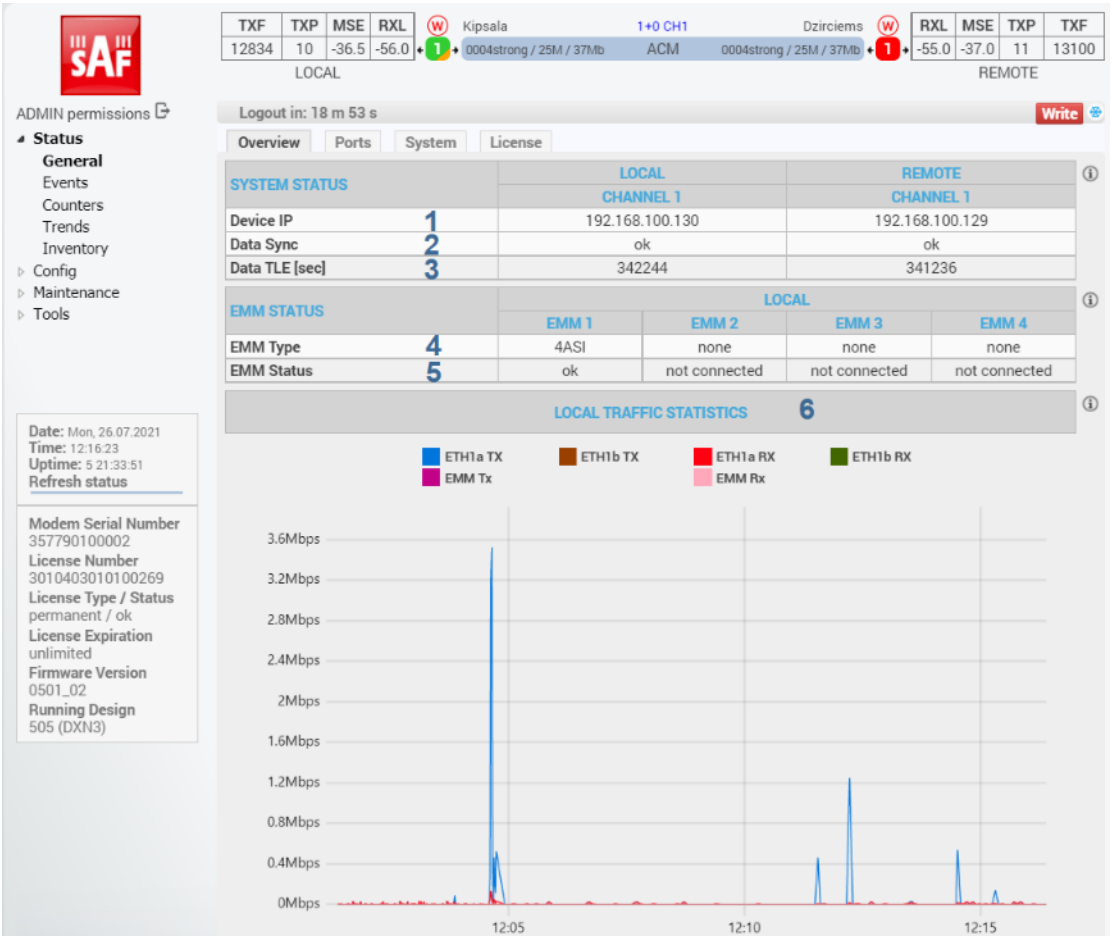


Figure 3.11a *Status → General → Overview screen for 1+0 configuration*

1) ***Device IP*** – IP addresses of devices in the link;
2) ***Data sync*** – modem synchronization status;
3) ***Data TLE [sec]*** – time since last error occurrence;
4) ***EMM Type*** – type of connected EMM card
5) ***EMM Status*** – current EMM status. Possible values are:

a) **ok** – EMM card is operational
b) **warning** – EMM card has an active alarm
c) **not connected** – no EMM detected in this position
d) **offline** – EMM card is configured, but not connected
e) **bad type** – EMM card configured as another type than actually connected
f) **bad fw** – incompatible FW loaded in this card. Use the inbuilt FW wizard for FW upgrade

6) ***Local Traffic Statistics*** – an interactive graph depicting the link throughput since login.

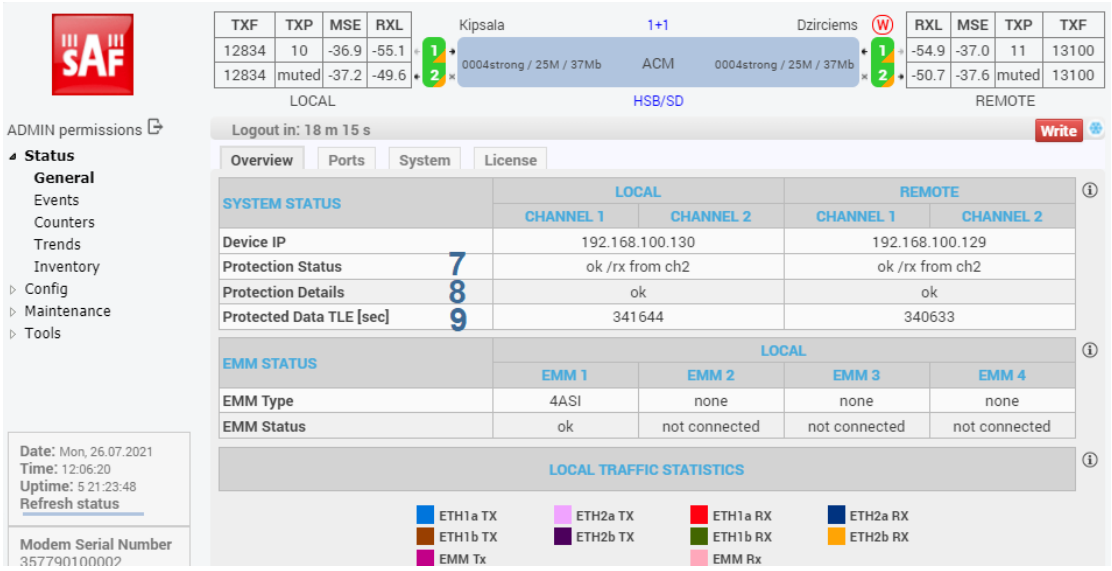


Figure 3.11b *Status → General → Overview screen for 1+1 configuration*

7) ***Protection Status*** – status of the protection. Possible values are:
a) **ok / rx source** – no protection alarms active/actual rx source
b) **backup / rx source** – protection alarms active, running from the backup line / actual rx source
c) **data loss** – no data passing through
8) ***Protection Details*** – possible values are:
a) **ok** – correct status
b) **noMSE** – missing modulation signal
c) **hiFEC** – high Forward Error correcting level
d) **noFO** – missing interconnection with the peer IDU
9) ***Protected Data TLE*** – time since last unprotected error occurred

Status → General → Ports

This section provides a summary status of all physical IO ports of the device.



Figure 3.12a *Status → General → Ports screen*

1) ***Link Status (actual)*** – actual status of a port as detected by the device (speed, duplex mode, link, administrative down status);
2) ***Mode*** – actual port settings (speed/duplex, administrative down);
3) ***Flow Control*** – actual duplex flow control mechanism settings;
4) ***VLAN group*** – actual port separation.

It is possible to change those settings in *Config → Ports page*.

If any of EMM modules are connected to the IDU and enabled, additional EMM information will appear in this section:

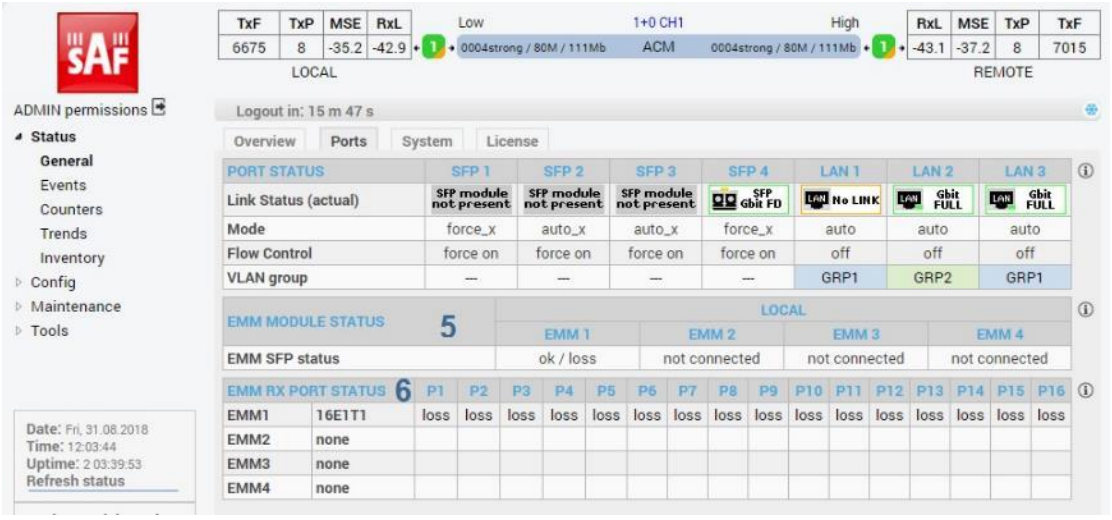


Figure 3.12b *Status → General → Ports screen*

5) ***EMM module status*** – shows summary status of all attached EMM cards;
6) ***EMM RX port status*** – shows detailed status of all ports of each attached EMM. For detailed description of all possible values, please refer to page *Config → Ports → EMM*

Status → General → System

This section displays modem unit status, RF/IF unit status, telemetry status and running IP configuration.

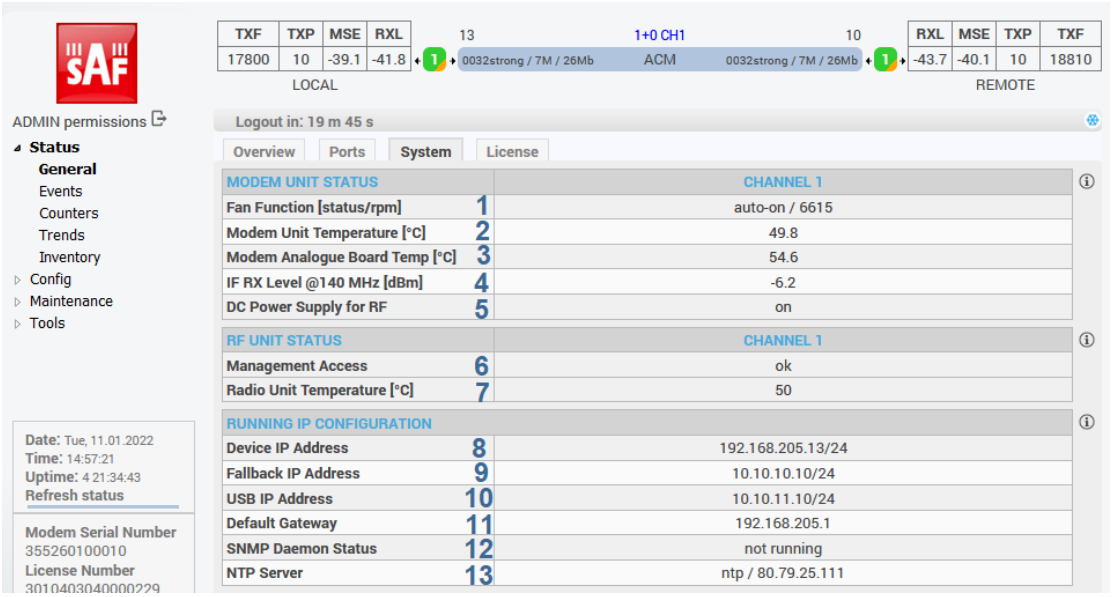


Figure 3.13 *Status → General → System screen*

1) ***Fan Function*** – shows the actual fan configuration status and actual spinning speed;
2) ***Modem Unit Temperature*** – temperature of the modem part;
3) ***Modem Analog Board Temp*** – temperature of the analogue board
4) ***IF Rx Level @140 Mhz*** – the IF signal strength detected on the cable input of the modem part;
5) ***DC Power Supply For RF*** – the actual status of power supply for the radio part;
6) ***Management Access*** – status of telemetry communication between the device and radio part;
7) ***Radio Unit Temperature –*** temperature read from the radio part;
8) ***Device IP Address*** – the IP address of this IDU;
9) ***Fallback IP Address*** – the fallback IP address of this IDU;
10) ***USB IP Address*** – the fallback USB IP address of this IDU;
11) ***Default Gateway*** – the default gateway IP address of this IDU;
12) ***SNMP Daemon status*** – the status of the inbuilt SNMP daemon;
13) ***NTP server*** – the time synchronization server configuration.

Status → General → License

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

By pressing the Generate license request button, a License Request (licreq_SN_timestamp.afw) file will be generated and downloaded. It will be required for extending of time-limited License. It can be downloaded from *Maintenance → Files → Exports page*.

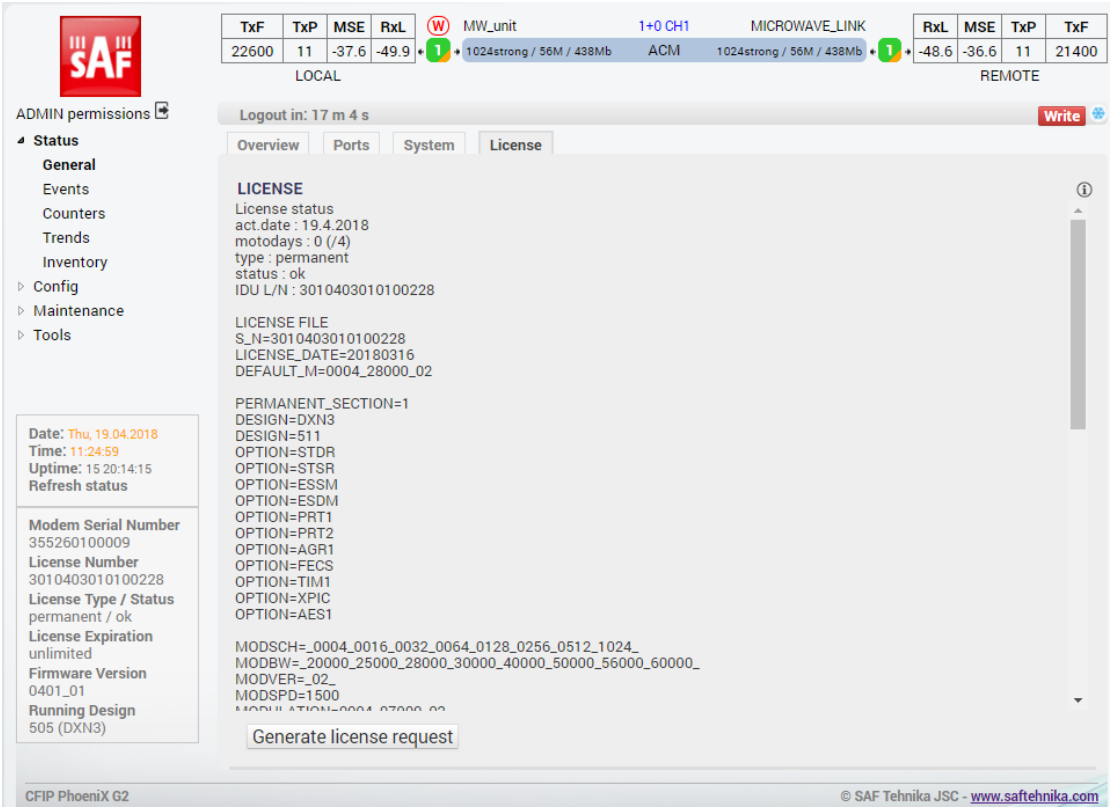


Figure 3.14 *Status → General → License screen*

Status → Events → Actual

This section contains the list of alarms which are active at the current moment. It should be empty when the equipment works properly and without alarms.

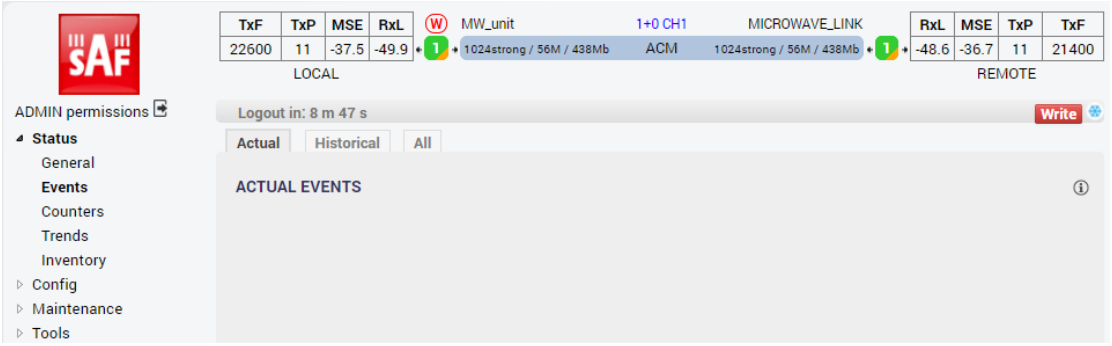


Figure 3.15 *"Status → Events → Actual" page*

Status → Events → Historical

This section contains the list of alarms which occurred in the past, but which are no longer active. By pressing Alarm History Validation button the alarms are manually acknowledged and the status of the device will be evaluated only from alarms which occurred after the manual validation.

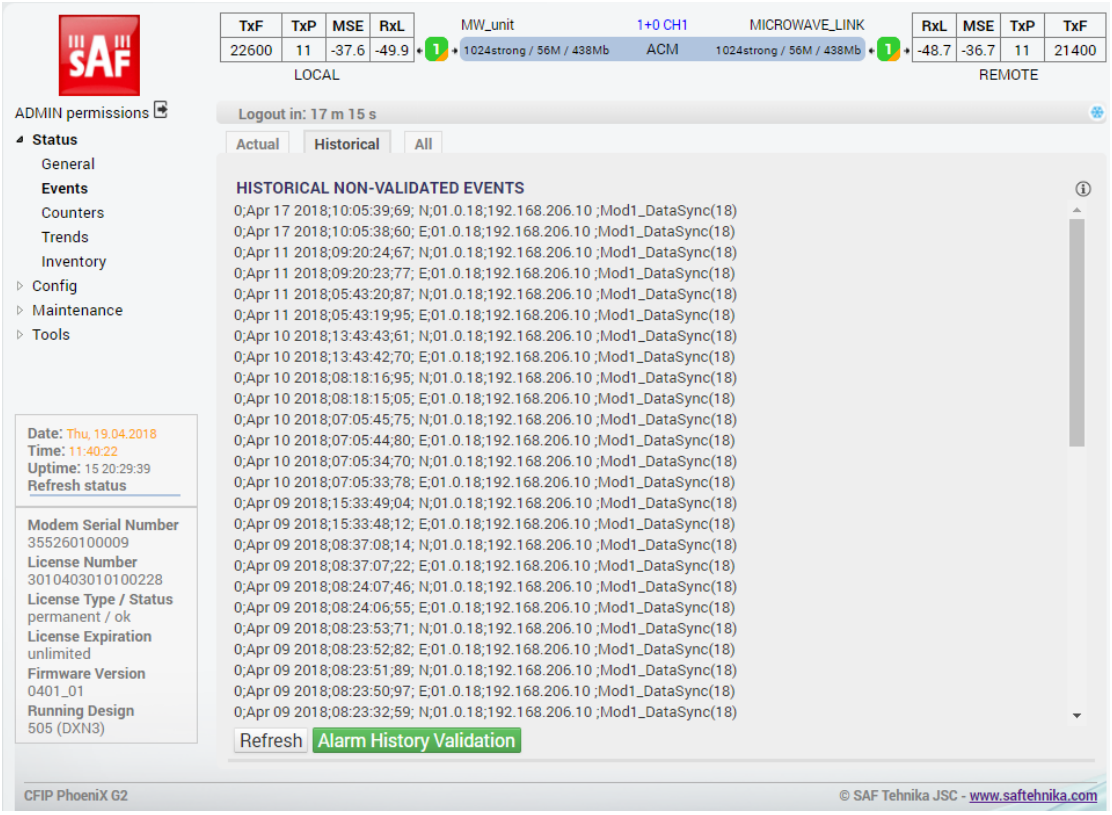


***Figure 3.16** "Status → Events → Historical" page*

Status → Events → All

This section contains the conjunction of both Actual and Historical alarms.

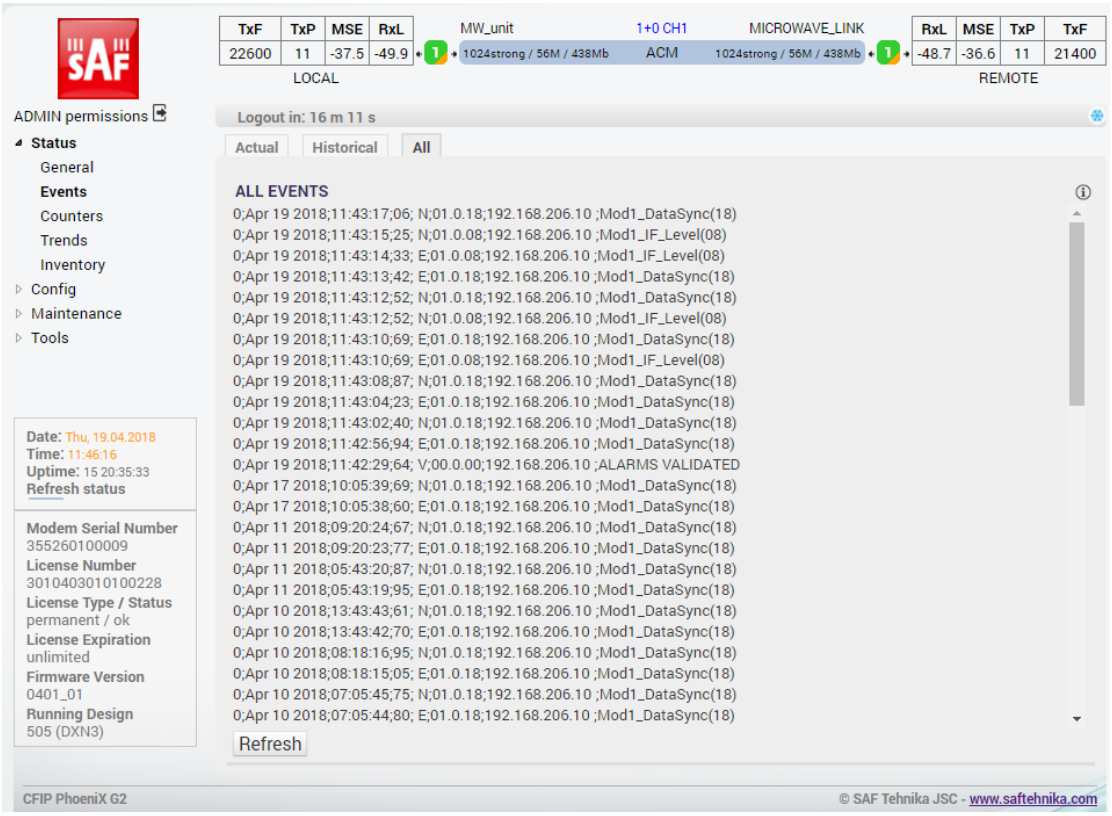


***Figure 3.17** "Status → Events → All" page*

Status → Counters → Modem

This section displays basic modem performance counters and built-in Bit Error Rate (BER) counters. For BER counter only unassigned capacity will be used (Refer to *Config → Ports → MUX section*)



***Figure 3.18** "Status → Counters → Modem" page*

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

11) ***Consecutive ERS*** – consecutive error seconds; number of successive seconds during which errors occurred. When the AUTO-RESTORE CONFIGURATION is enabled, it will automatically reload the startup configuration when this counter reaches 600 seconds. Every error-free second resets this counter. In order to prevent outage on working channels, all operating channels need to reach this threshold before the auto-restore process is executed.
12) ***Status*** – BER tester synchronization status (sync|nosync) or n/a when there is no active link to the remote side or free capacity left for the BER tester
13) ***Actual Tx Speed*** – shows reserved transmission speed for BER tester. This value roughly equals to half of the unassigned capacity which is used for the BER tester
14) ***TX Pattern*** – shows transmission pattern for BER tester frames
15) ***RX Pattern*** – shows receiving pattern of BER tester frames
16) ***Rx Bit Count*** – shows number of received bits (BER)
17) ***RX Err Count*** – shows number of received error bits (BER)
18) ***Rx Sync Count*** – number of synchronizations of the BER tester
19) ***BER*** – ratio of Rx Bit Count and Rx Err Count
20) ***TLE*** – time since last BER error; a number of seconds from the last error occurrence. It should correspond to time since pressing the Clear button
21) ***TBE*** – time between the last two BER error events
22) ***EFS*** – error free seconds of the BER tester; it should correspond to time since pressing the Clear button
23) ***ERS*** – error seconds; number of seconds during which a BER error occurred

By pressing the Clear button, the values of counters will be cleared. By pressing the Clear All button, the values of counters on all Counter pages will be cleared.

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

Status → Counters → Traffic

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

By pressing the Clear button, the values of counters will be cleared. By pressing the Clear All button, the values of counters on all Counter pages will be cleared.

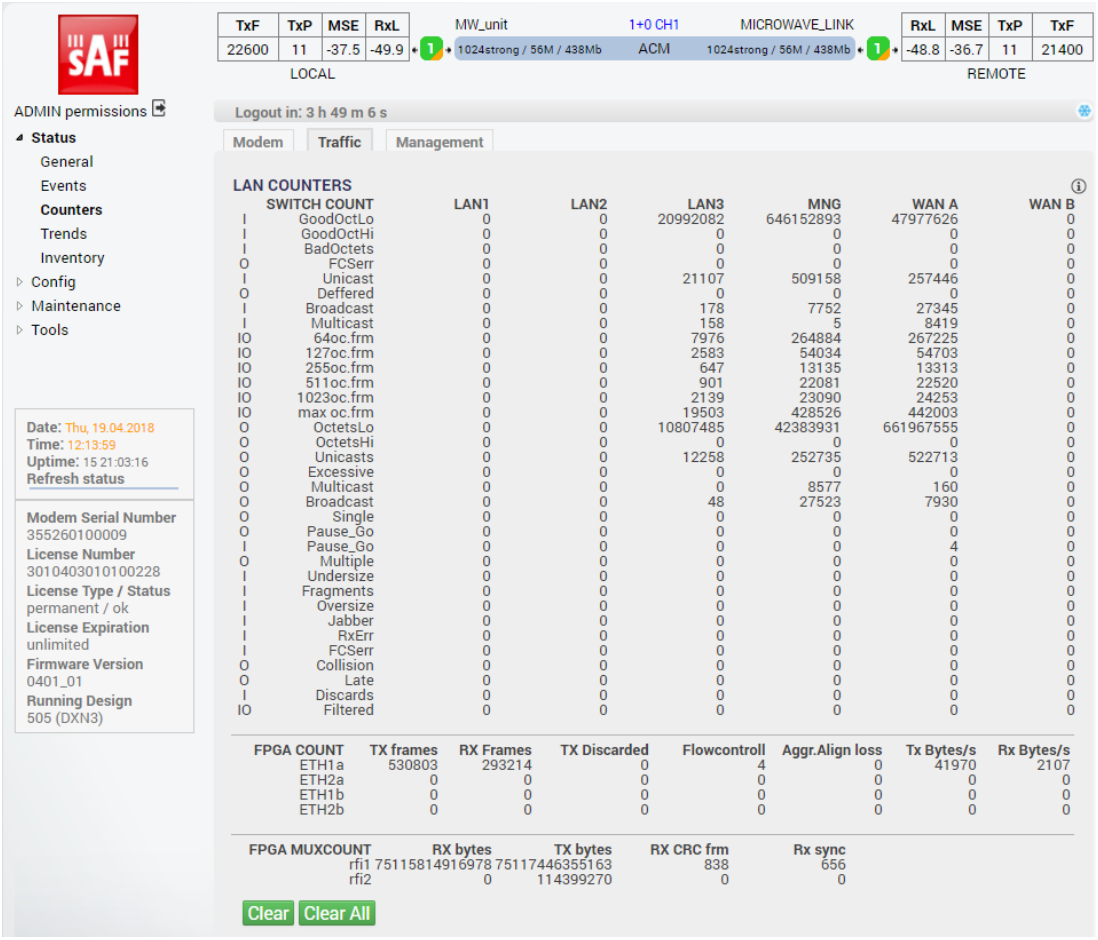


***Figure 3.19** "Status → Counters → Traffic" page*

Status → Counters → Management

This section displays IP statistics of IDU's interfaces.

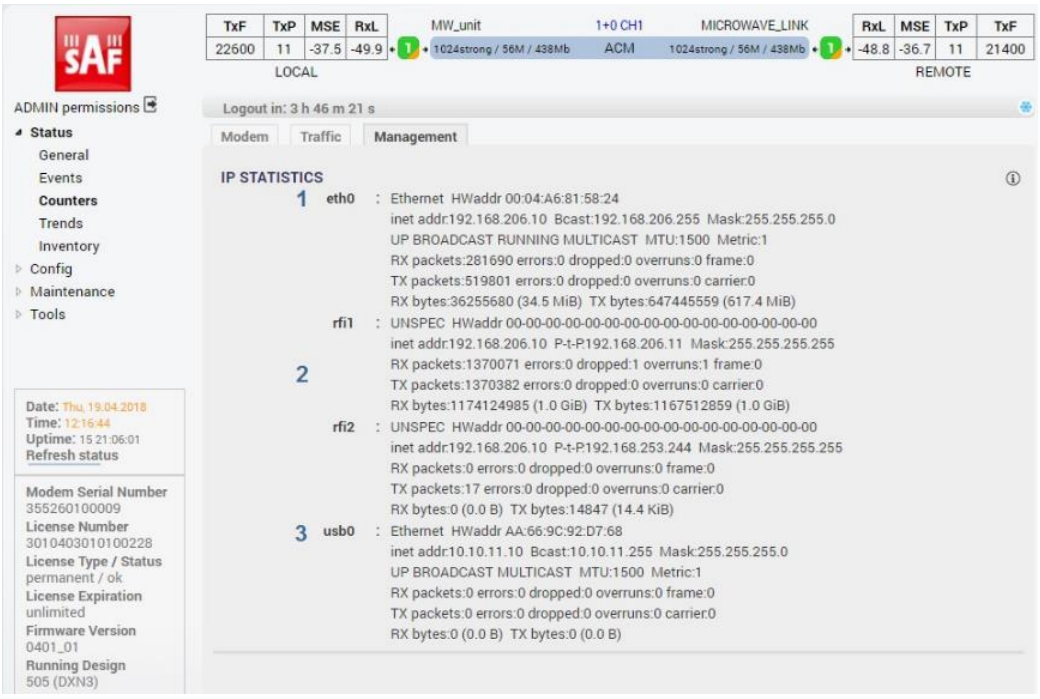


***Figure 3.20** "Status → Counters → Management" page*

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

Status → Counters → EMM

ASI EMM Counters:

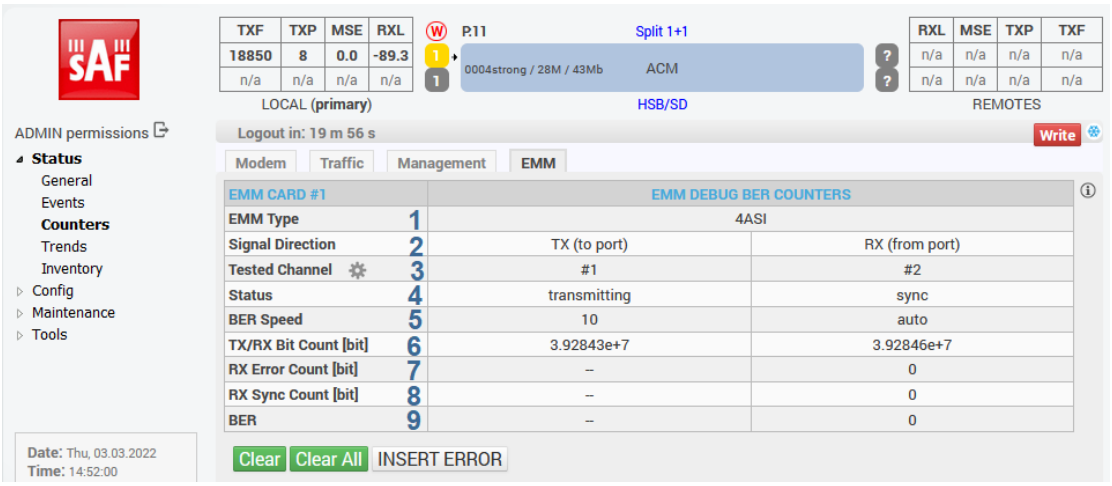


Figure 3.21 *"Status → Counters → EMM" page*

1) ***EMM Type*** – indicates type of connected EMM module
2) ***Signal Direction*** – indicates ASI signal directions Tx and Rx
3) ***Tested Channel*** – channel number on which BER is enabled. Pressing on ⚙ button the *Config →Ports →EMM* page will open
4) ***Status*** – indicates current BER status. The indicated options can be as follows:
   - ***sync*** – the port is receiving BER signal
   - ***nsync*** – no BER signal detected
   - ***transmitting*** – the port is transmitting BER signal
   - ***idle*** – the received signal is homologous. Usually it is indication of error
5) ***BER Speed*** – indicates current Tx/Rx speed of BER tester
6) ***TX/RX Bit Count*** – indicates the overall BER tester bit count. It can be cleared manually
7) ***RX Error Count*** – indicates the number of detected errors in the receiving BER stream
8) ***RX Sync Count*** – indicates the number of re-sync events during the BER test
9) ***BER*** – indicates the actual Bit Error Ratio (BER)

⚠ Some rows may not be available due to current settings or used EMM HW revision. BER counter is supported in ASI EMM Hardware revision 12AT**20486**_01_02 or later.

By pressing the Clear button, the values of counters will be cleared. By pressing the Clear All button, the values of counters on all Counter pages will be cleared.

By pressing the Insert Error button, one error will be inserted into data stream.

Status → Trends → Actual

The graph displays the selected values in dependence on time. If the connection with the remote is established, the values from the remote unit are also displayed. This graph is dynamic and thus updated with the newest values with each GUI auto-refresh. The refresh interval is computed dynamically from server response time.

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

- **TxPower** – depicts the transmitter signal output level
- **RxL/MSE** – received signal level/quality of the received signal
- **Temperature** – displays the temperature of modem and radio

It is possible to zoom the graph by means of mouse scrolling.



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



***Figure 3.22** "Status → Trends → Actual" page*

Status → Trends → Historical

The graph in this section displays the selected values in dependence on time. If the connection with remote side is established, the values from the remote unit will be displayed.

For depiction it is possible to choose from following options:

- ***TxPower*** – depicts the transmitter signal output level
- ***RxL/MSE*** – received signal level/quality of the received signal
- ***Temperature*** – displays the temperature of modem and radio
- ***Throughput*** – displays the transmission capacity for the transmission and admission on the selected ports of the IDU. Both the Ethernet port and EMM port throughput is displayed
- ***Sync/QAM*** – value MLOCK = 1 displays modem synchronization, value MLOCK = 0 shows that there was no synchronization. If ACM is active, the most appropriate

modulation for signal transmission or admission is found. Individual modulations are indicated by their amount of states.

It is possible to zoom the graph by means of mouse scrolling.

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



***Figure 3.23** "Status → Trends → Historical" page*

Status → Inventory

This section shows the device hardware/software information as well as radio part information.

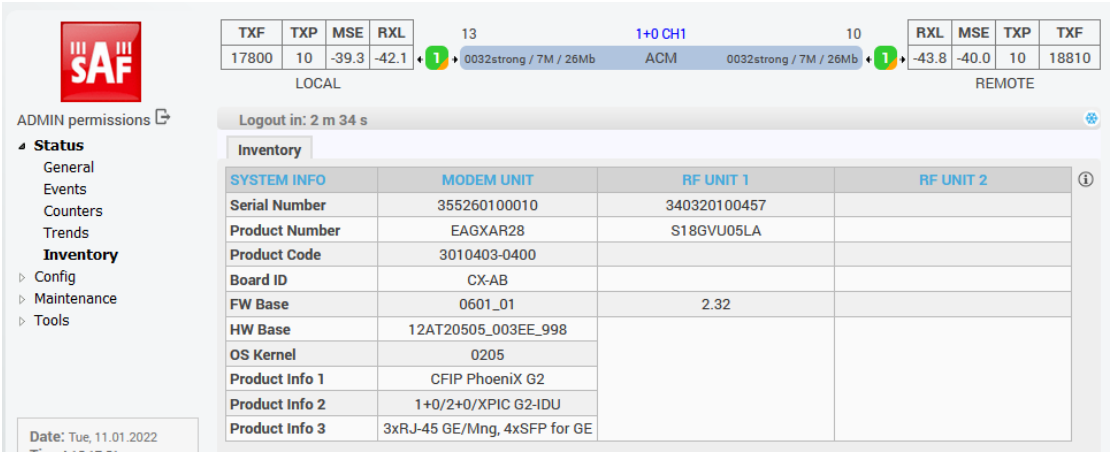


***Figure 3.24** "Status → Inventory" page*

If any of EMM modules are connected to the IDU and enabled, additional EMM information will appear in this section:

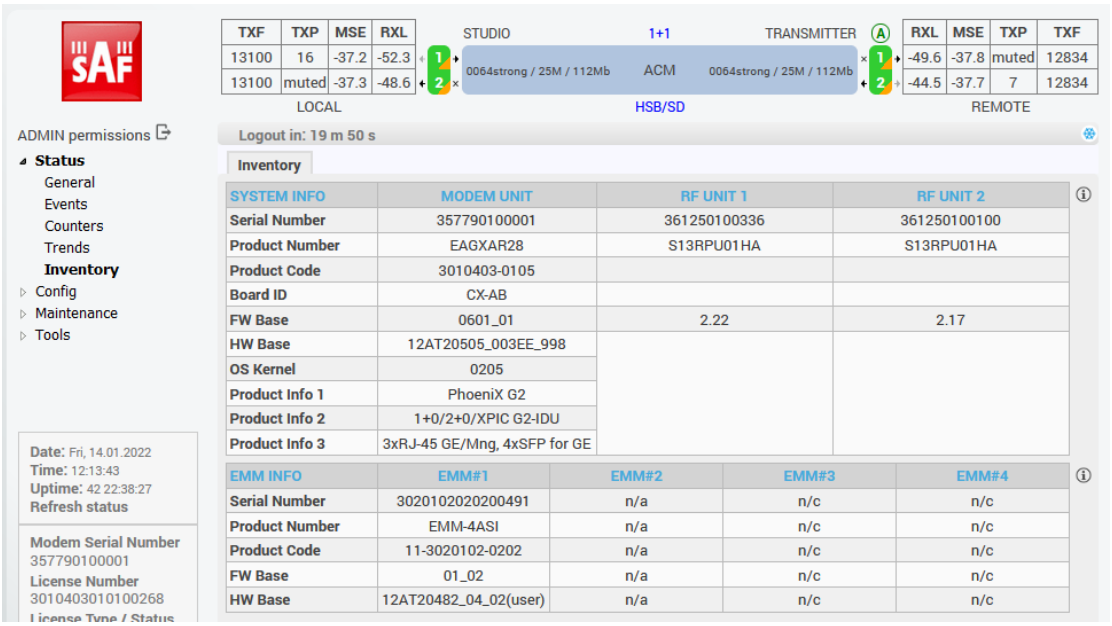


***Figure 3.25** "Status → Inventory" page*

Config

Config → System → Mode

In this section the user can select specific Design Type which specifies the main function of the system/link.

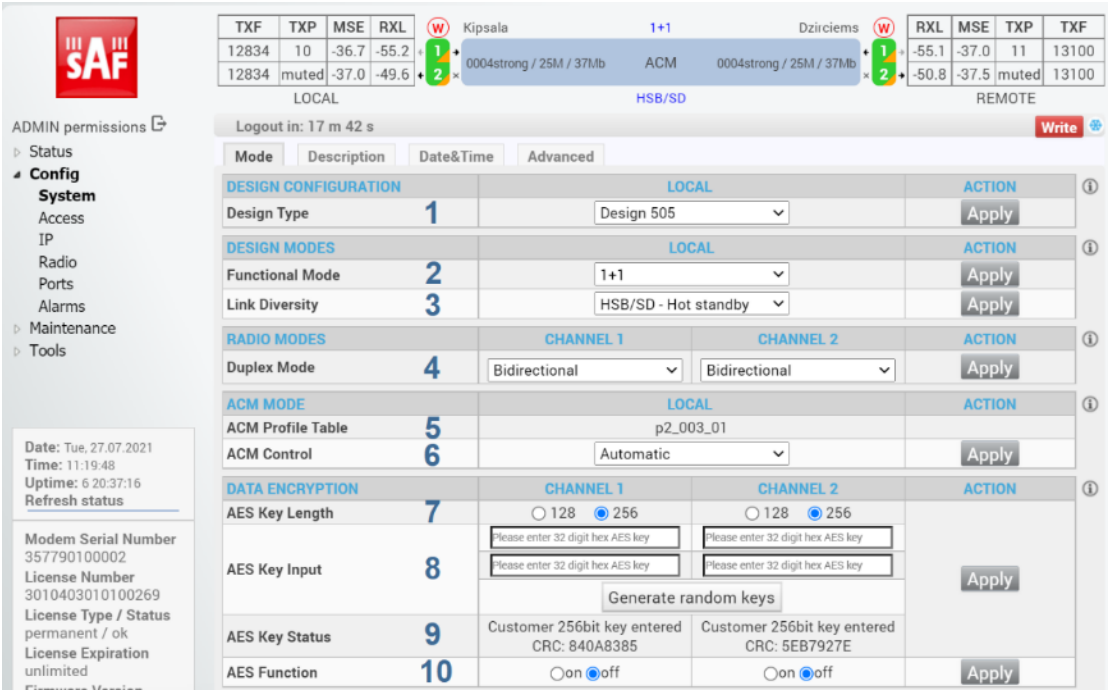


***Figure 3.26** "Config → System → Mode" page, Design 505 configuration*

1) ***Design Type*** **–** following two design types are supported (depending on the license):

a) ***Design 505*** – a single IDU on each side of the link. Available modes are 1+0 (ch1, ch2, dual FD and dual XPIC), 1+1 (FD, HSB, SD, XPIC) and 2+0 (FD, XPIC). This design supports AES encryption if licensed.

b) ***Design 511*** – two IDUs on each side of the link. This design type should be selected for application where full protection is required. Two interconnected IDUs are used on each side of a link in this configuration. This design supports following modes: Split 1+1 (FD, HSB, SD), Split 2+2 (FD, HSB, SD) and 1+1/2+2 Repeater modes. Note that the AES encryption is not available in this design.

c) ***Design 513*** – two IDUs on each side of the link. This design type should be selected for applications where full protection is required. This design supports 1+1 Repeater mode. The Repeater mode can be used for split 1+1 protection multi-hop links, as only one-channel modem configurations are supported. It allows for the transparent transfer of the EMM data streams over retranslation stations without EMM module installation in retranslation point. There are Split 1+1 (FD, HSB, SD) modes available. This design supports AES encryption.



The design change will load a configuration pre-sets for the given design. That means the device should be re-configured by the user after each design type change. It is recommended to reboot the device after such re-configuration.



It may happen that the link to the remote side will be lost after design type change. In this case local access to all devices must be ensured before design type change. The remote side IDU/ODU has to be configured separately.

Following configuration fields will appear when Design type ***Design 505*** will be chosen:

2) ***Functional Mode*** – above mentioned Radio modes in ***Design 505*** can be combined with following Functional modes:
   a) ***1+0 Ch1/2*** – simple one channel end station which uses physical channel Nr.1/2
   b) ***1+0 Dual*** – advanced 1+0 mode which separately uses both physical channels. Can be used also as repeater configuration.
   c) ***1+0 Star*** – advanced repeater mode where Channel 1 is directed to one direction (East) and Channel 2 is directed to other direction (West)
   d) ***2+0*** – capacity aggregation mode which combines the capacity of both physical channels.
   e) ***1+1*** – protection mode which combines the capacity of both physical channels.
3) ***Link Diversity*** modes – those modes are available when choosing above mentioned **1+1** or **2+0** Functional modes:
   a) ***FD*** – frequency diversity configuration with frequency separation in both physical channels of the system. Supported by **2+0** and **1+1** functional modes
   b) ***SD*** – space diversity configuration with single Tx channel, two Rx channels and two antennas in both directions. Supported by **1+1** functional mode. This mode does not support Tx switch-over.
   c) ***HSB/SD*** – hot standby/space diversity configuration with single Tx channel at a time and two Rx channels in both directions. Supported by **1+1** functional mode. This mode will switchover the Tx in case of Primary Tx failure



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*

   d) ***XPIC*** – cross-polarization diversity with automatic attenuation of interfering signal from the X-polarized channel. Supported by **2+0** and **1+1** functional modes



The following AES settings will be available if they are included in the license. Those settings may be available for one or two channels depending on the configuration of the Functional Mode.

4) ***Duplex Mode*** – this setting determinates duplex/simplex function of the configured link and has an essential influence on whole system function:

a) ***Rx Only*** – half-duplex/simplex link with only Rx channel. In this case the automatic ACM function should be set to the manual profile by the user.
b) ***Tx Only*** – half-duplex/simplex link with Tx only channel. In this case the automatic ACM function should be set to the manual profile by the user.



The simplex configuration considerably limits the functionality of the system. The ACM function will not work as well as remote side monitoring from Tx only side, etc.

c) ***Bidirectional*** – full duplex link with Tx and Rx channels

5) ***ACM Profile table*** – indicates currently used ACM profile
6) ***ACM control*** – allows choosing among following available ACM modes:
   a) ***Automatic*** – automatic change of QAM/FEC according to channel with worse receive signal quality, guarantees hitless protection in 1+1 mode, recommended for all configurations except unidirectional duplex mode
   b) ***Manual*** – disabled ACM, fixed QAM/FEC for RX and TX directions, applicable for all functional and duplex modes
   c) ***Automatic advanced*** – designed specifically for protection modes for automatic change of QAM/FEC according to channel with better receive signal quality. It guarantees the highest throughput in 1+1 and 2+2 configurations, recommended only for protection modes
   d) ***Semi-manual*** – designed specifically for unidirectional duplex mode. It has fixed QAM/FEC for TX direction, while the receiver can sync to any QAM/FEC. Recommended only for unidirectional duplex mode
7) ***AES key length*** – One of two ASI key lengths can be selected for the AES encryption: 32 hex digits key (128 bits) or 64 hex digit key (256 bits). If there is no specific requirement of 128-bit key usage, the 256-bit key is recommended.
8) ***AES key input*** – A 32 hex digit key (128 bits) or 2x 32 hex digit keys (256 bits) must be entered for each channel in order to properly initialize the AES function. The same key have to be entered on local and remote channels. It is possible to use the Generate random keys button to generate a random key(s).
9) ***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.
10) ***AES function*** – Allows enabling or disabling AES encryption function. When enabled, the whole traffic stream from packet processor is encrypted by provided AES key. It is required to define valid AES key(s) in order to enable the AES function.

When choosing Design type ***Design 511*** or ***Design 513*** following additional configuration options will appear in this same section:

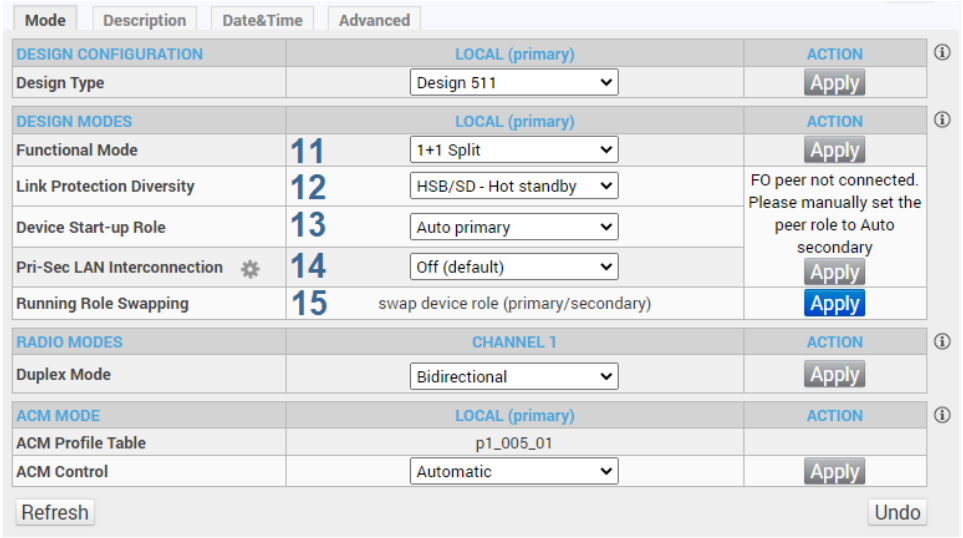


Figure 3.27 *"Config → System → Mode" page, Design 511 configuration*

11) ***Functional Mode*** – above mentioned Radio modes in ***Design 511*** and ***Design 513*** 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. Supported by ***Design 511*** and ***Design 513***
    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. Supported only by ***Design 511***



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

    c) ***1+1 Repeater –*** full protection repeater mode, must be set for IDUs in retranslation site. Two IDUs must be used on each side of each link. Supported by ***Design 511*** and ***Design 513***
    d) ***2+2 Repeater –*** aggregation protection repeater mode, must be set for IDUs in retranslation site. Two IDUs must be used on each side of each link. Supported by ***Design 511***
12) ***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.
13) ***Device Start-up 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).
14) ***Pri-Sec LAN Interconnection*** – when enabled, allows two independent simultaneous IP traffics (IP traffic 1 and IP traffic 2) in 1+1 Split Protection link – one over the Primary IDUs and the second over the Secondary IDUs. It must be configured identically on both Primary and Secondary IDUs. Following settings are available:
    a) ***Off (default)*** – the specific Pri-Sec LAN interconnection mode is disabled, all LAN ports operate as configured in standard Split 1+1 mode
    b) ***Summed mode1*** – enables Pri-Sec LAN interconnection mode. LAN1, LAN2, LAN3 and MNG ports are active and grouped, enabling LAN interconnection between the Primary and Secondary IDUs. It supports Out-band and In-band management access



For more details about this functionality and its configuration refer to *Example19 – Summed modes configuration*

15) ***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 appear. Following additional configuration options will appear in this same section:

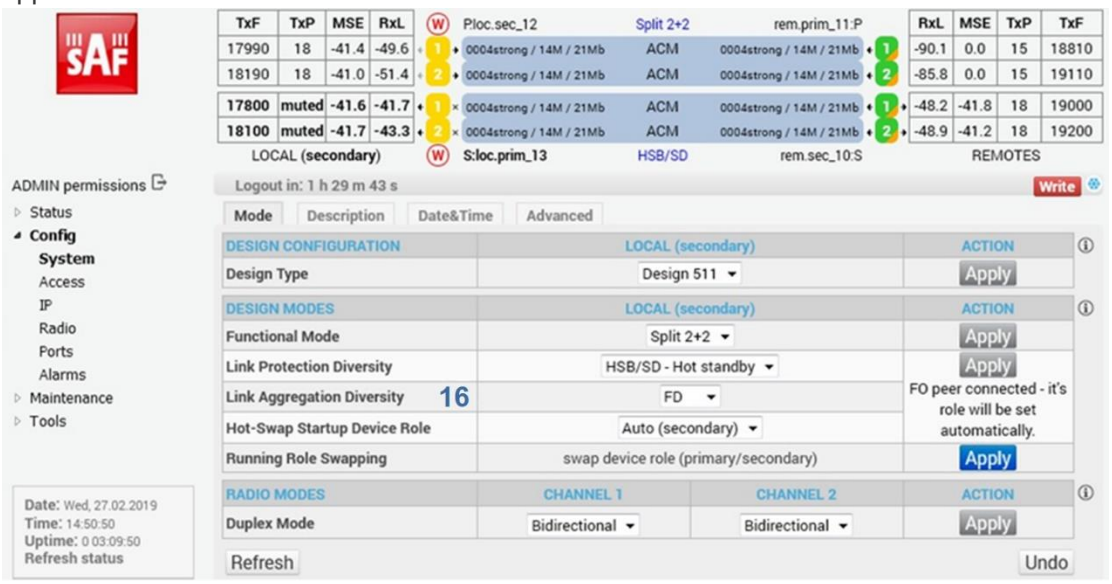


Figure 3.28 *"Config → System → Mode" page, 2+2 mode configuration*

16) ***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.

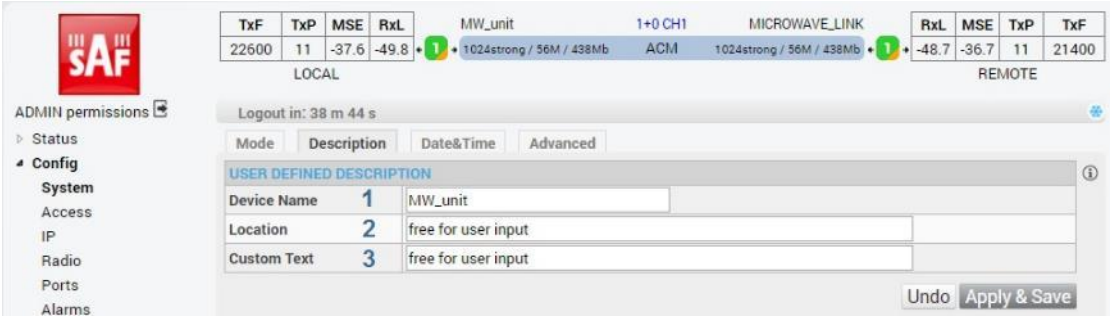


Figure 3.29 *"Config → System → Description" page*

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.

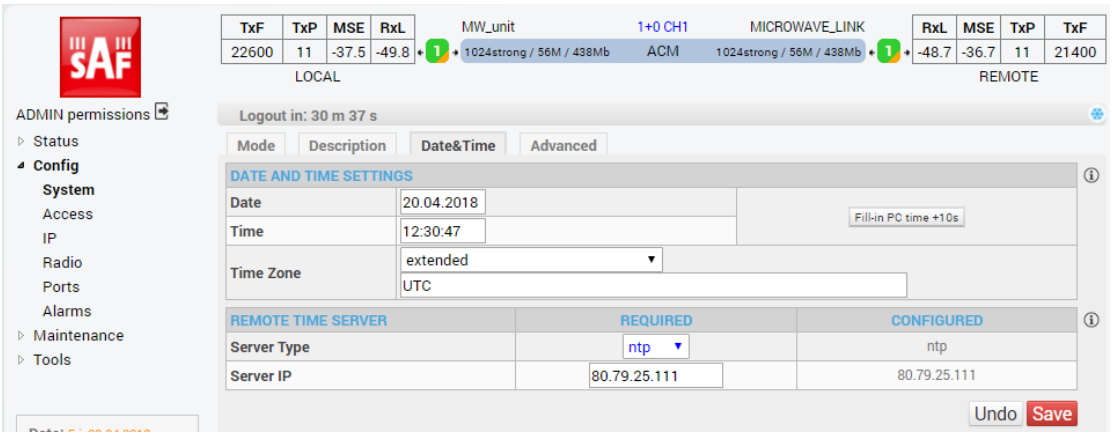


***Figure 3.30** "Config → System → Time&Date" page*

Config → System → Advanced

This section contains following advanced settings:

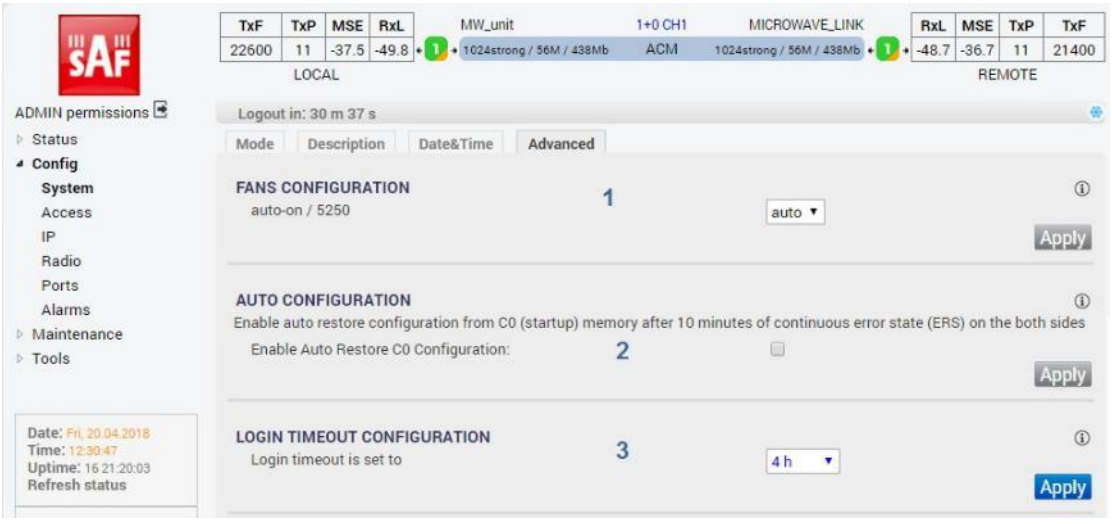


***Figure 3.31** "Config → System → Advanced" page*

1) ***Fans 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

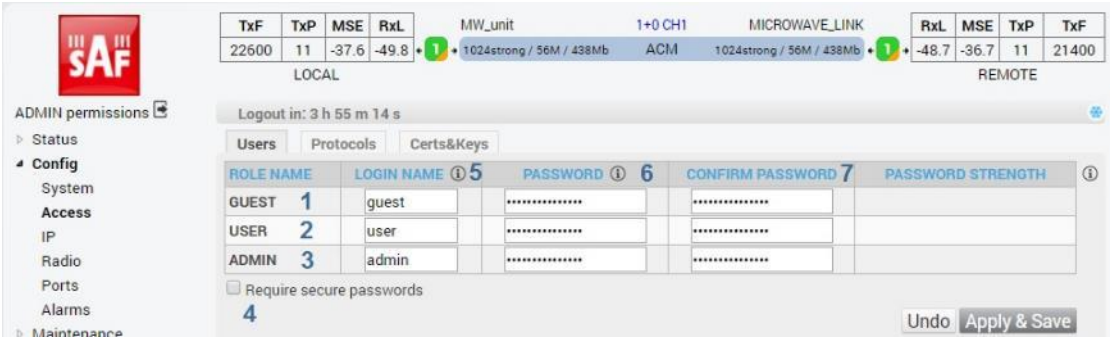


Figure 3.32 *"Config → Access → Users" page*

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*** – username 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 usernames 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.

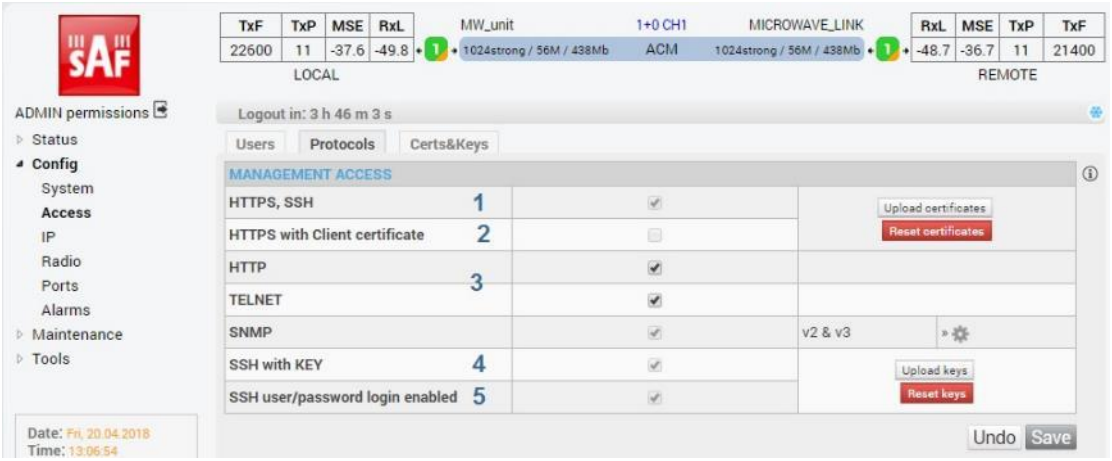


***Figure 3.33** "Config → Access → Protocols" page*

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

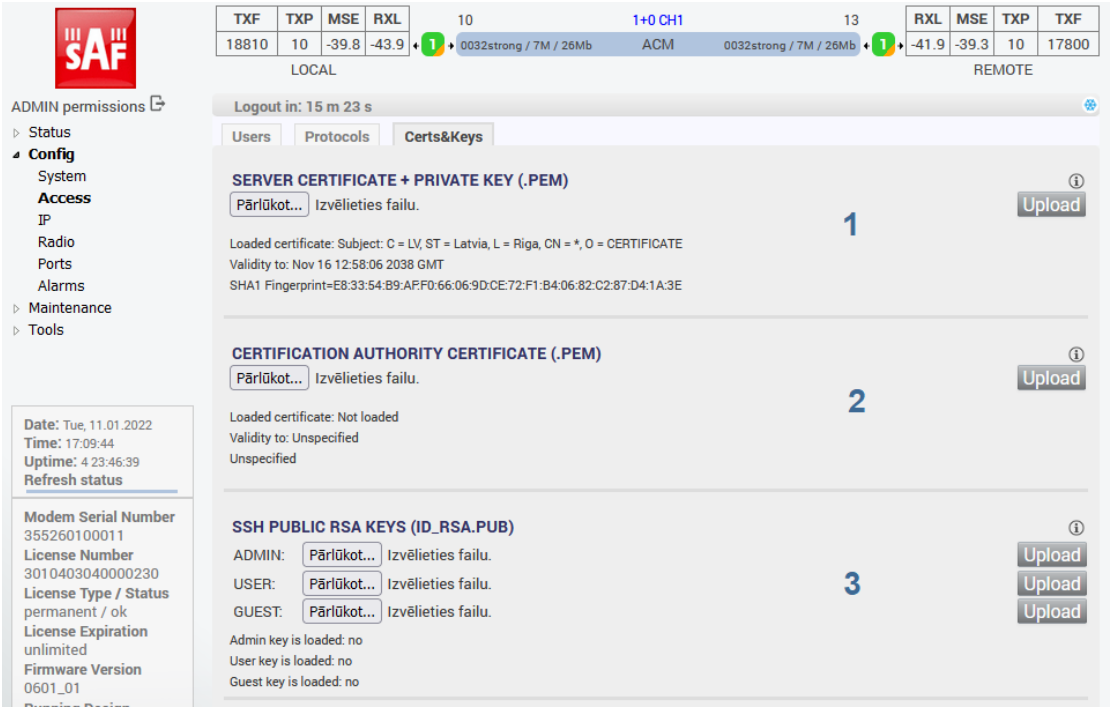


***Figure 3.34** "Config → Access → Certs&Keys" page*

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 3.35** "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

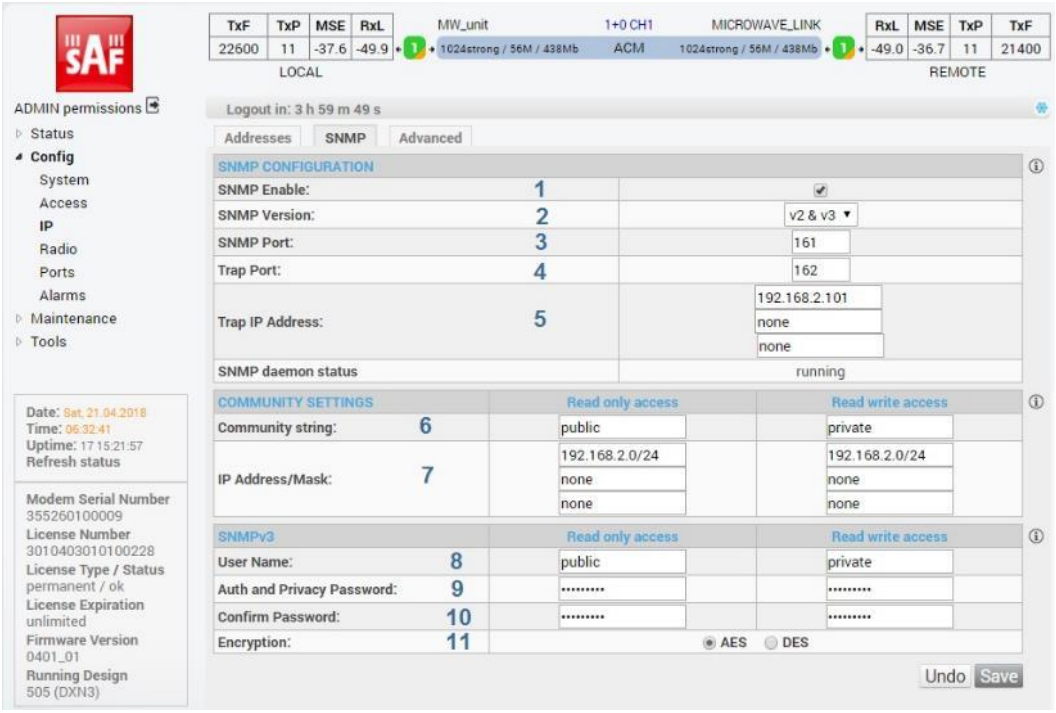


***Figure 3.36** "Config → IP → SNMP" page*

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

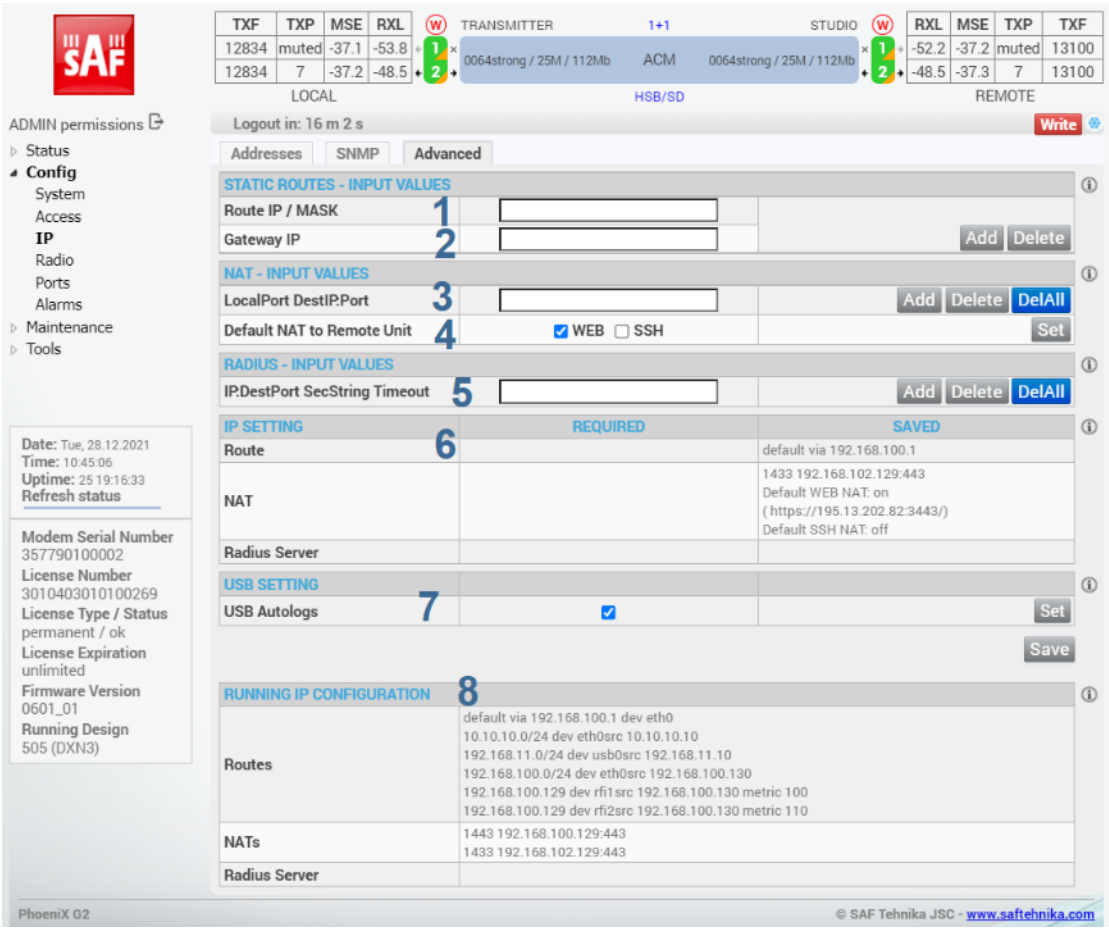


***Figure 3.37** "Config → IP → Advanced" page*

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 targeted 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) ***USB Autologs*** – enables auto save logs on USB flash just after inserting it.
8) 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.

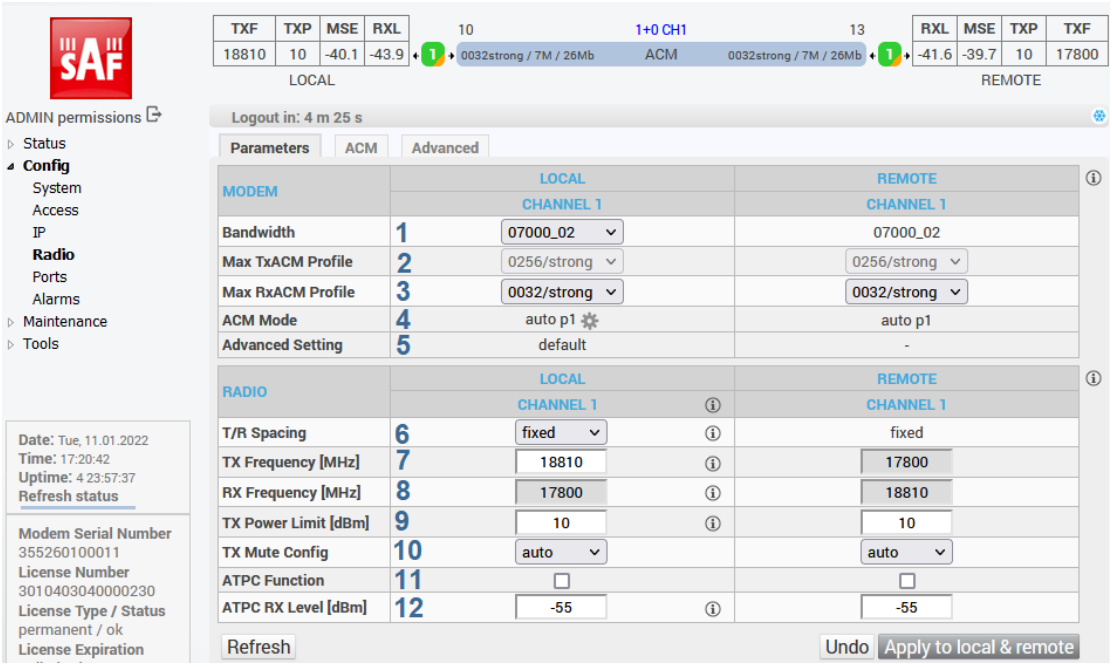


***Figure 3.38** "Config → Radio → Parameters" page*

1) ***Bandwidth*** – the bandwidth of the transmitting modulation. The number after the underscore indicates the modulation variant.
2) ***Max TxACM Profile*** – the highest possible Tx modulation at a given bandwidth. While the automatic ACM mode is enabled, this value will be the highest possible modulation. Otherwise, the value set will be the actual Tx modulation. Will become active if "Manual" or "Semi-manual" ACM Control option will be chosen in *Config →System →Mode* page
3) ***Max RxACM Profile –*** The highest possible Rx modulation at a given bandwidth. While the Semi-Manual ACM mode is enabled, this value will be the highest possible modulation. Otherwise, the value set will be the actual Rx modulation. Will become active if "Automatic" or "Automatic-advanced" ACM Control option will be chosen in *Config →System →Mode* page

Each modulation can have multiple Forward Error Correction variants:

- medium – optimal FEC, medium throughput speed
- strong – strong FEC, lowest throughput speed

4) ***ACM Mode*** – 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.
5) ***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.
6) ***T/R Spacing*** – TX / RX frequency distance mode. Note that available options depends on the attached radio type and it's capabilities.
7) ***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.
8) ***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.

9) ***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)
10) ***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.
11) ***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).
12) ***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

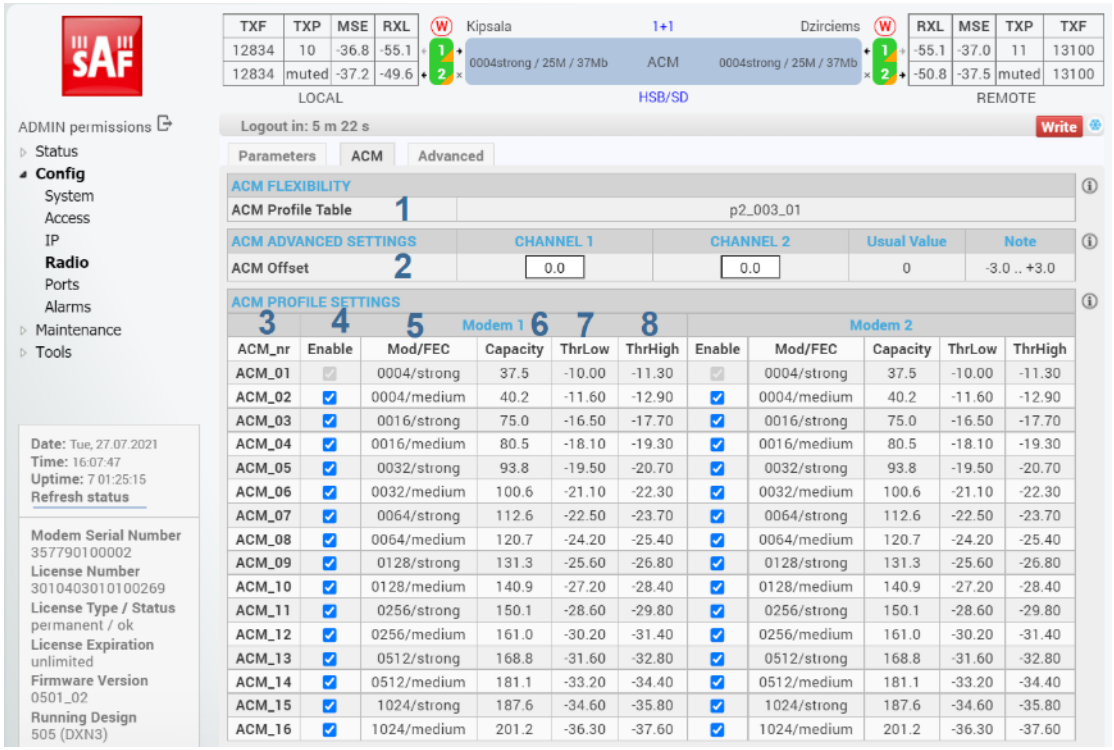


Figure 3.39 *"Config → Radio → ACM" page*

1) ***ACM Profile Table*** – specifies currently used ACM calibration table

2) ***ACM Offset*** – the MSE offset off the pre-set thrLow and thrHigh constants (see ACM profiles)
3) ***ACM_nr*** – designation of the modulation
4) ***Enable*** – enables a modulation for ACM switching
   - "I" means unlicenced modulation
   - "e" means error setting
   - "D" means not available in the selected profile
5) ***Mod/Fec*** – bandwidth/forward error correction level
6) ***Capacity*** – maximal throughput
7) ***ThrLow*** – the MSE threshold value for switching from this respective modulation to a lower Rx modulation
8) ***ThrHigh*** – the MSE threshold value for switching to this respective modulation



The ACM settings of local and remote devices should match.

Config → Radio → Advanced

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

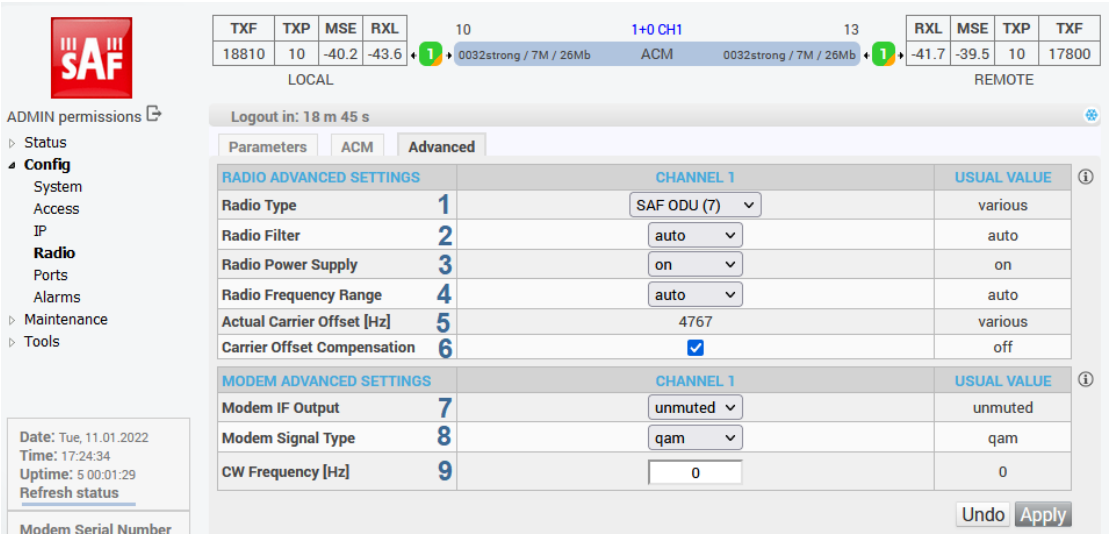


Figure 3.40 *"Config → Radio → Advanced" page*

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) ***Actual Carrier Offset –*** the current radio carrier offset. For the 3.5MHz bandwidth, it must be in the range from -40 000 to +40 000. This value will differ with each refresh
6) ***Carrier Offset Compensation*** – this option enables the automatic radio carrier offset calibration. The calibration is bound to the currently attached ODU only and should be repeated when the ODU is replaced by means of disabling and re-enabling this checkbox. Use this option when there is no modem synchronization on very narrow bandwidths (3.5MHz). Unchecking this option resets the calibration. Enabling the auto-calibration will cause data drop for about 3 sec. The calibration requires modem sync. The calibration may be done on a higher bandwidth or on the 4QAM modulation when there is not possible to achieve the synchronization on the desired narrow modulation.
7) ***Modem IF Output*** options are following:
   - **unmuted** – modem IF Tx is transmitting
   - **muted** – modem IF Tx is muted
8) ***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
9) ***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 protection/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.

Basically, the traffic ports (SFP, LAN) located on the front panel must be interconnected with internal traffic channels (Eth1a, Eth1b, EMM or PTP) for passing the data over the air. The internal traffic channels are main data transport over the air between both sides of the link. The interconnection of the traffic ports with internal traffic channels is done in built-in FPGA. SFP ports can be connected directly to traffic channels, the LAN ports is part of the internal Ethernet switch and can be connected to the traffic channels via WAN ports. The simplified diagram of traffic port interconnection with traffic channels is given below:

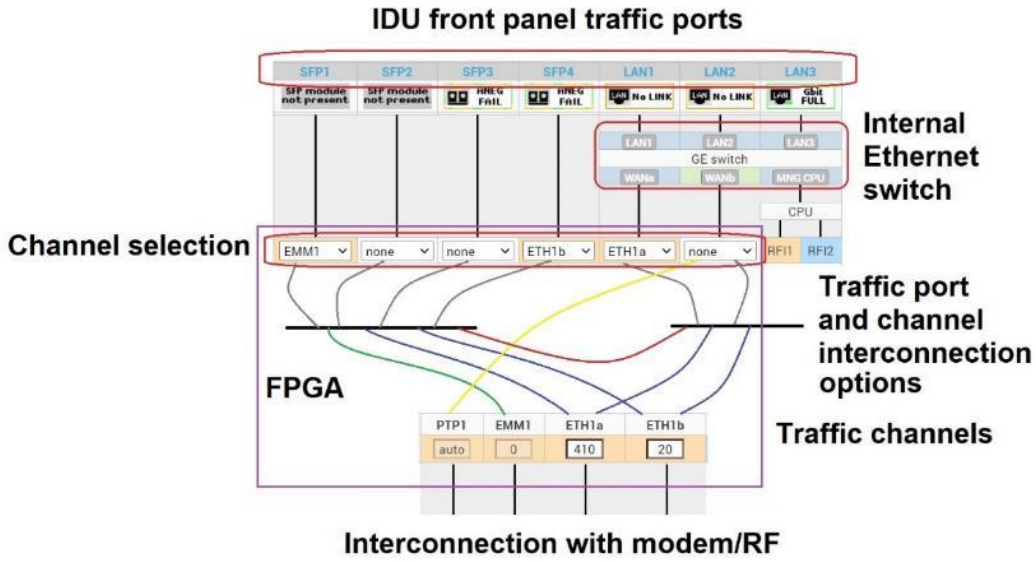


Figure 3.41 Traffic port and channel interconnection diagram

IDU front panel traffic ports are located on the Phoenix G2 IDU front panel and are used for user traffic interconnection with customer network equipment. There are 4x SFP ports for Ethernet and EMM traffic, and 3x LAN ports for Ethernet traffic.

Internal Ethernet switch contains 6 Ethernet ports – 3x LAN Ethernet ports and 2xWAN Ethernet ports for user and management traffic, and 1x MNG CPU Ethernet port for management access.

Channel selection is configuration part for ***traffic port and channel interconnection*** in ***FPGA***. Here it is possible to interconnect the user traffic ports with internal traffic channels to pass the data over the air. Each SFP port can be directly interconnected to Ethernet Eth1a and Eth1b channels and to EMM channel. From the switch side both WAN ports can be connected to any of Ethernet Eth1a and Eth1b channels. WANb port can be also connected to PTP channel. Any of SFP ports also can be interconnected to any of WAN ports thus interconnecting the SFP ports with internal Ethernet switch. For correct LAN and WAN port interconnection in the Ethernet switch port grouping must be properly configured. For port grouping configuration refer to page *Config →Ports →EthVLAN*

Traffic channels are 4 internal traffic channels which transport the data to the modem and over the air. Each traffic channel between local and remote IDU (over the air) is permanently interconnected: Eth1a<--->Eth1a, Eth1b<--->Eth1b, EMM<--->EMM and PTP<--->PTP. All traffic channels are prioritized in following sequence from Highest priority to Lowest priority: PTP, EMM, Eth1a, Eth1b. It is possible to specify speed limit for each Traffic port. The ***channel selection*** allows to interconnect different traffic ports to traffic channels on each side of the link. Some examples:

1) WANa port connected to Eth1a channel in IDU1, and WANb port connected to Eth1a channel in IDU2. With correct LAN and WAN port grouping in internal Ethernet switch in both IDUs, the traffic can be passed in following way over the link: LAN1<->WANa<->Eth1a<->RF<->Eth1a<->WANb<->LAN2
2) SFP1 port connected directly to Eth1a channel in IDU1, and WANa port connected to Eth1a channel in IDU2. In this case in IDU1 traffic will not be passed via the internal Ethernet switch, but in IDU2 the traffic will be passed via the internal Ethernet switch.

With correct LAN and WAN port grouping in internal Ethernet switch of IDU2, the traffic can be passed in following way over the link: SFP1<->Eth1a<->RF<->Eth1a<->WANa<->LAN1

3) SFP1 port interconnected with the internal switch in IDU1, and WANa port connected to Eth1a channel in IDU2. In this case in IDU1 the SFP1 port can be connected to the internal Ethernet switch only via one of WAN ports. The second WAN port will be interconnected to Eth1a traffic channel. Both WAN ports must be in the same one port group. So, with correct LAN and WAN port grouping in internal Ethernet switch in both IDUs, the traffic can be passed in following way over the link: SFP1<->WANa<->WANb<->Eth1a<->RF<->Eth1a<->WANa<->LAN1

Following is the description of port configuration in web GUI:

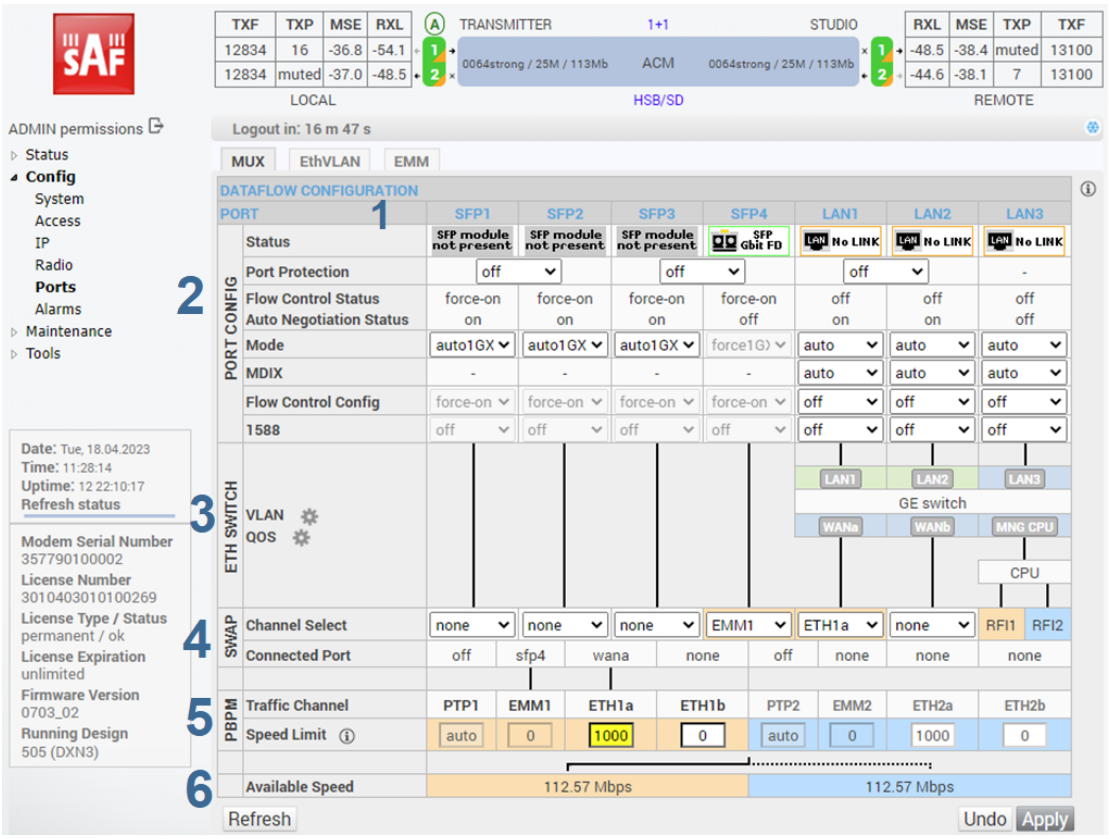


***Figure 3.42** "Config → Ports → MUX" page*

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) ***Port Protection*** – automatic switch over between ports according to actual link status or a mandatory LAN port mirroring settings in split protection repeater modes.

In case of configuring the IDU as 1+1 Repeater IDU supported by Design 513, 'mirror' option will appear and can be chosen for mentioned configuration if needed. Design 513 and Functional mode '1+1 Repeater' can be configured in page *Config → System → Mode*. Both

the Port Protection & Port Mirroring on LAN ports requires the bounded ports to be set in the same group for correct function

c) ***Flow Control Status*** – displays the actual duplex flow control mechanism settings.
d) ***Auto Negotiation Status*** – displays actual auto negotiation status for each port
e) ***Mode*** – displays and defines port mode (speed/duplex, administrative down)
f) ***MDIX*** – set particular ETH cable crossing option like auto/mdi/mdx
g) ***Flow Control Config*** – displays and defines duplex flow control mechanism settings.
h) ***1588*** – Precision time protocol (PTP) 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*

a) ***VLAN*** – pressing on icon will navigate to *Config → Ports → EthVLAN* for VLAN and port group configuration

b) ***QOS*** – pressing on icon will navigate to *Config → Ports → EthVLAN* for QoS configuration

4) ***SWAP:***

a) ***Channel Select*** – settings of data multiplexer. By those settings it is possible to cross connect a particular Switch port with a Mux Channel. Following channel options can be selected:

- For SFP1-4 ports:
  - ***ETH1a/ETH1b*** – connecting of particular SFP port directly to high or low priority data channel. One of those options should be chosen in case if SFP port is used for passing the Gigabit Ethernet traffic. In this case the built-in switch is not used for processing the Ethernet traffic
  - ***EMM1/EMM2*** – connecting of particular SFP port to EMM channel. EMM option must be chosen in case if EMM module is connected to the IDU via particular SFP port
  - ***WANA/WANB*** – connecting of particular SFP port to the built-in switch via one of WAN ports. This option can be chosen if SFP port is used for Gigabit Ethernet traffic and IDU management access. In this case the traffic will be processed via built-in switch
  - ***None*** – no channel selected

In 511 Design SFP1 and SFP2 ports are used only for interconnection between Primary and Secondary IDUs. In 513 Design only SFP1 port is used for Primary-Secondary IDU interconnection.

- For WANa port:
  - ***ETH1a/ETH1b*** – connecting of WANa port to high or low priority data channel
  - ***SFP1-4*** – connecting of WANa port to one of SFP ports; intended for interconnection of SFP port with built-in switch
  - ***None*** – no channel selected
- For WANb port:
  - ***ETH1a/ETH1b*** – connecting of WANa port to high or low priority data channel
  - ***SFP1-4*** – connecting of WANa port to one of SFP ports; intended for interconnection of SFP port with built-in switch
  - ***PTP1/PTP2*** – connecting of WANb port to Precision Time Protocol 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
      - **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

This section allows configuring VLAN 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.

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 3.43** "Config → Ports → EthVLAN" 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 and 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.
   a) **All** – all supported priority policies (Port, Tagged, IPv4/6) are taken into consideration in following order Tagged->IPv4/6->Port
   b) **Port only** – selects Priority policy only for LAN/WAN ports of the IDU
   c) **Tagged only** – when choosing this option of Priority policy, the priority contained in VLAN tag of the packet is considered. VLAN tag priority information can be already present in the VLAN packet (incoming from the external equipment), or can be inserted during VLAN tagging in the IDU (EthVLAN/VTU settings/QOS Pri) in *Config →Ports →EthVLAN* page
   d) **IPv4/6 only** – when choosing this option of Priority policy, the priority is taken from the incoming IP frame header
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) ***MAC Learning*** – allows disabling of MAC learning on a particular port. Note, the ATU table is cleared on this setting change
6) ***Port State*** – indicates the current port state settings. Possible values are *Active* and *Standby*. Used mainly for the split-protection modes with Pri-Sec LAN interconnection. Refer to web GUI page *Config →System →Mode*
7) ***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 does not 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 does not 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.
8) ***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.
9) ***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.

10) ***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.
11) ***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
12) ***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.
13) ***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).
14) ***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

15) ***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 → EMM

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

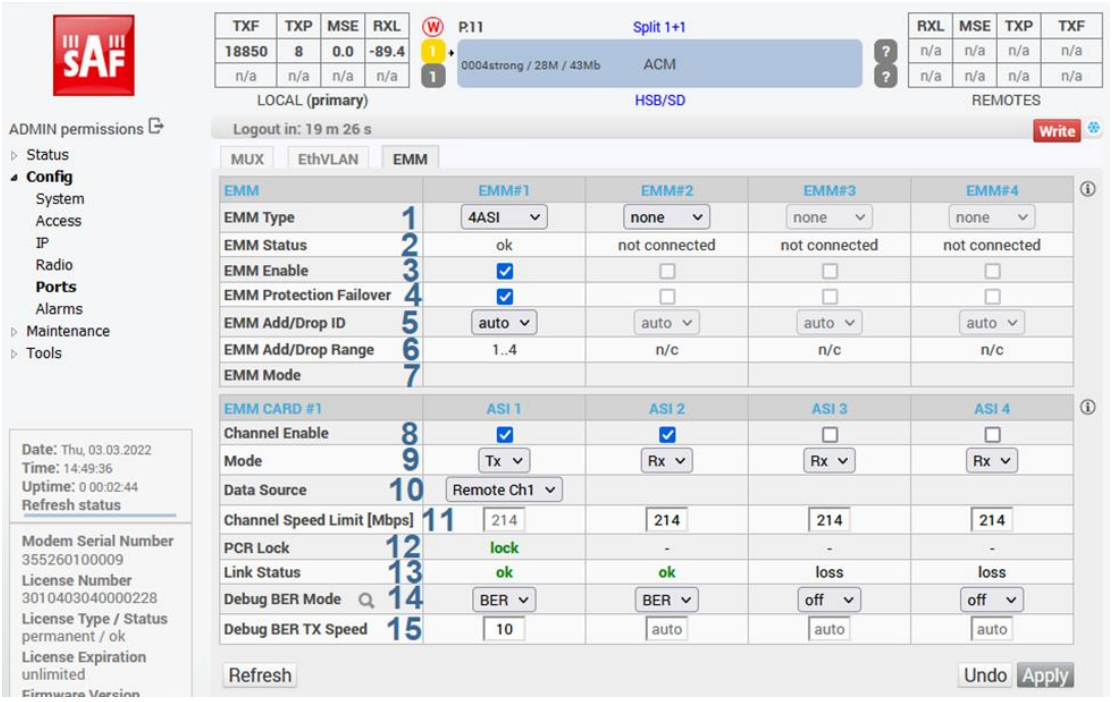


***Figure 3.44** "Config → Ports → EMM" ASI EMM configuration page*

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 Status*** – current EMM status indication. Possible values are:
    a) **ok** – EMM card is operational
    b) **warning** – EMM card has an active alarm
    c) **not connected** – no EMM detected in this position
    d) **offline** – EMM card is configured, but not connected
    e) **bad type** – EMM card configured as another type than actually connected
    f) **bad fw** – incompatible FW loaded in this card. Use the inbuilt FW wizard for FW upgrade
3) ***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).
4) ***EMM Protection Failover*** – this option will appear in case of ***Design 511*** and **Split 1+1** or **Split 2+2** modes are used. 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.
5) ***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.
6) ***EMM Add/Drop Range*** – displays appropriate port-channel range according to the EMM card position and EMM Add/Drop ID setting.
7) ***EMM Mode*** – it selects the mode of connected EMM 16E1/T1 card
8) ***Channel 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.

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) ***Channel Speed Limit*** – maximal data rate for inbound traffic to avoid overloading of overall link capacity. This setting is available in **Rx mode** only.
12) ***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
13) ***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.
14) ***Debug BER Mode*** – enables BER debugging tool which allows to test ASI transmission without need of actual ASI stream. Only one Tx and one Rx port can be set to BER mode. Pressing the 🔍 button will open *Status →Counters →EMM* page



BER debugging mode is supported in ASI EMM Hardware revision 12AT**20486**_01_02 or later. Enabling the BER mode will cause ASI user data drop and should be used only for debugging purposes.

15) ***Debug BER TX Speed*** – setting of requested ASI Tx BER speed

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

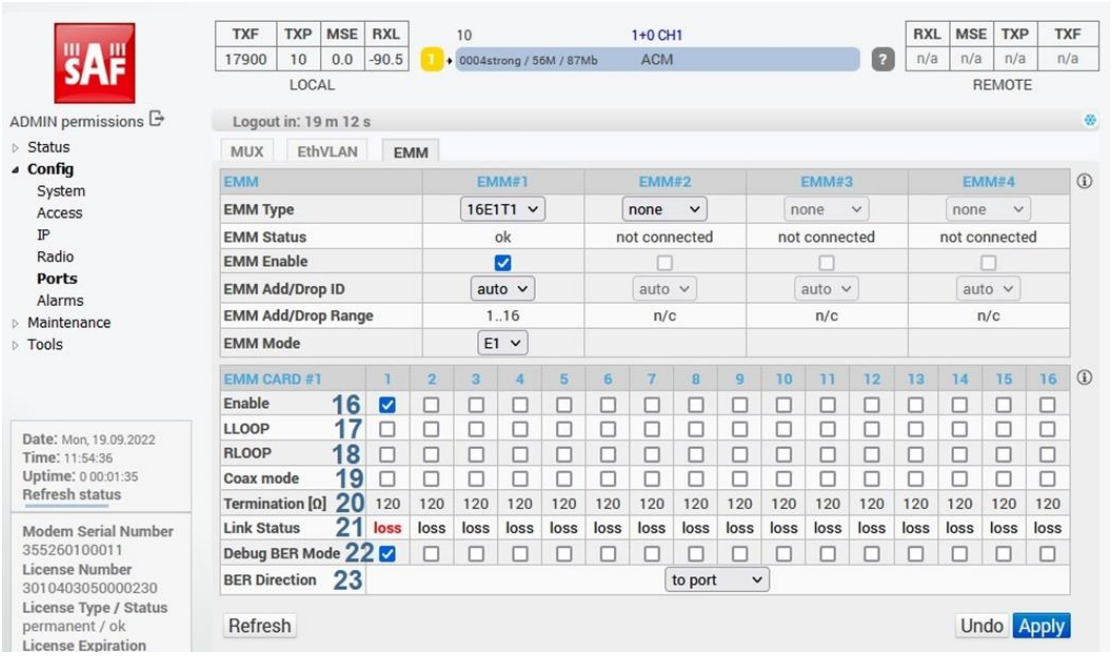


Figure 3.45 *"Config → Ports → EMM" E1/T1 EMM configuration page*

16) ***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).
17) ***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.
18) ***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.
19) ***Coax Mode*** –changes the E1/T1 mode from standard 120Ω balanced to 75Ω unbalanced.
20) ***Termination*** – displays the actual impedance matching of E1/T1 port according to Coax mode setting.
21) ***Link Status*** – it displays the actual status of E1/T1 port or appropriate internal traffic channel.
22) ***Debug BER Mode*** – the BER debugging tool allowing to test the E1/T1 transmission without the need for an actual E1/T1 stream. Only one port of 16 can be switched to the BER mode. For BER monitoring during this test refer *Status →Counters →EMM* page



BER debugging mode is supported in E1/T1 EMM Hardware revision 12AT**20484**_01_02 or later. Enabling the BER mode will cause E1/T1 user data drop and should be used only for debugging purposes.

23) ***BER Direction*** – the BER debugging tool can be routed either to the port or to the channel. In case of channel the BER stream will be transmitted through the link. Result of BER stream is detected on the same port/channel.

Config → Alarms → General

This section contains possible events/alarms with direct and immediate impact on the link operability. Following labels are used for alarm indication:

DEF - static recommended default alamrs. These alarms can be activated after pressing the ADD DEFAULTS button

PRT - the alarms indicated with this label, when enabled and activated, invokes the IDU Pri/Sec role switching in auto split protection modes

> For correct switching of protection role, the user must appropriately configure all the PRT labelled switch alarms. Only those alarm which are enabled and listed as PRT will be used for protection switching, taking in account that there are no protection alarms active on the peer IDU.

Following alarms configuration is available in this page:

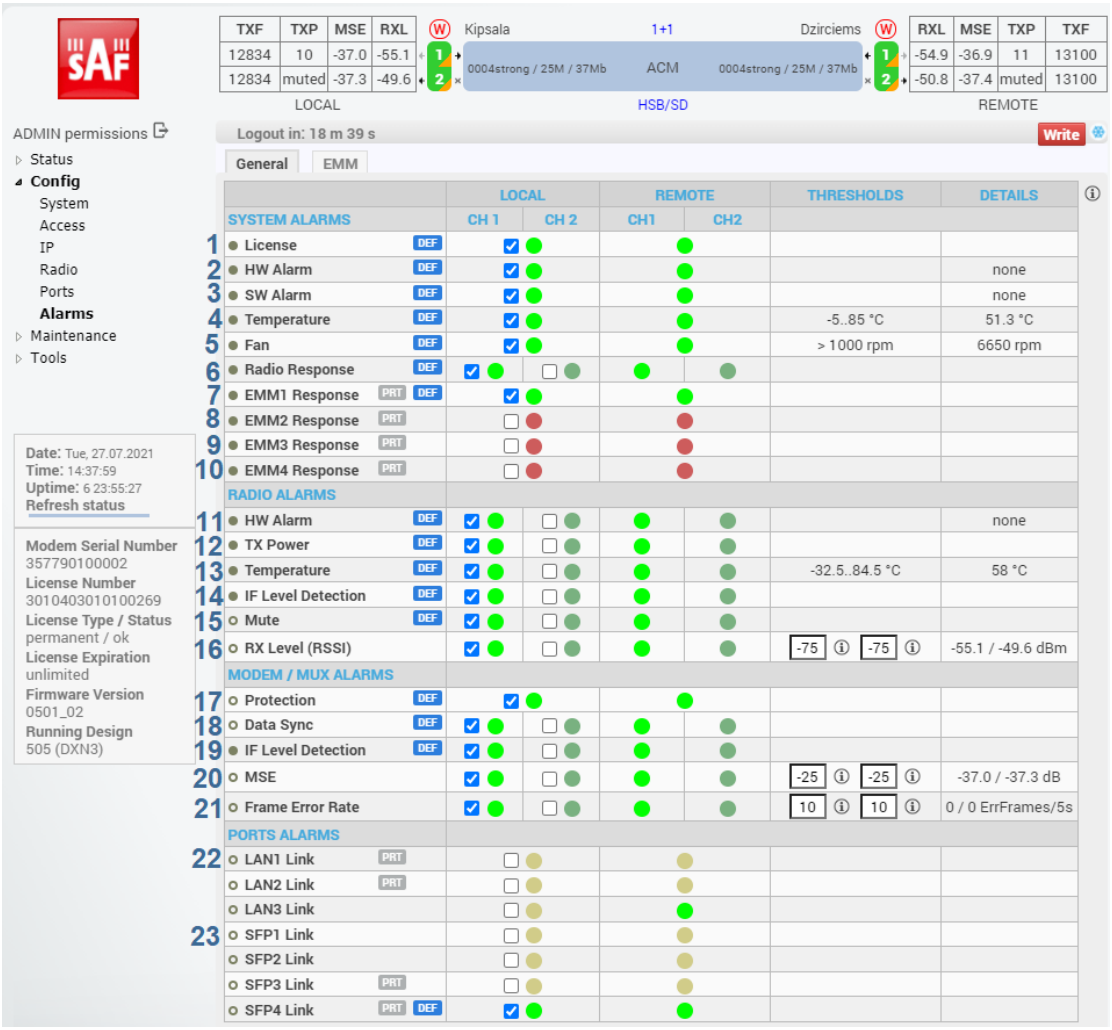


***Figure 3.46** "Config → Alarms → General" page*

1) ***License*** – this alarm will be raised when the license file is about to expire or is expired already, or contains an invalid data
2) ***HW Alarm*** – a hardware problem (for example non-working fan)
3) ***SW Alarm*** – a software problem (for example incompatible mode selection on local and remote side)
4) ***Temperature*** – temperature of the modem part
5) ***Fan*** – detected fan rounds are under the threshold value
6) ***Radio Response*** – the status of communication with the radio part
7) ***EMM1 Response*** – the status of bidirectional FO communication with EMM1 card

8) ***EMM2 Response*** – the status of bidirectional FO communication with EMM2 card
9) ***EMM3 Response*** – the status of bidirectional FO communication with EMM3 card
10) ***EMM4 Response*** – the status of bidirectional FO communication with EMM4 card
11) ***HW Alarm*** – the status of the radio part
12) ***TX Power*** – transmitting power status
13) ***Temperature*** – temperature of the radio part
14) ***IF Level Detection*** – indicates low radio IF input (350MHz)
15) ***Mute*** – the configured value does not match with the actual radio Tx mute status
16) ***RX Level (RSSI)*** – receiving level threshold configuration and status
17) ***Protection*** – one or more protection lines do not work
18) ***Data Sync*** – indicates the actual status of packet processor (PBPS) synchronization
19) ***IF Level Detection*** – indicates low or high level of modem input (140 MHz)
20) ***MSE*** – link quality indicator threshold settings and status. Actual MSE values can be observed in the ACM profile table in *Config->Radio->ACM* page
21) ***Frame Error Rate*** – threshold configuration for error frames per 5 seconds
22) ***LAN1/2/3 Link*** – link status of LAN ports
23) ***SFP1/2/3/4 Link*** – link status of SFP ports

Config → Alarms → EMM

This section will differ depending on EMM module type connected to Phoenix G2 IDU – ASI EMM or E1/T1 EMM.

In case of ASI EMM enabled, the ASI related alarms will be displayed:

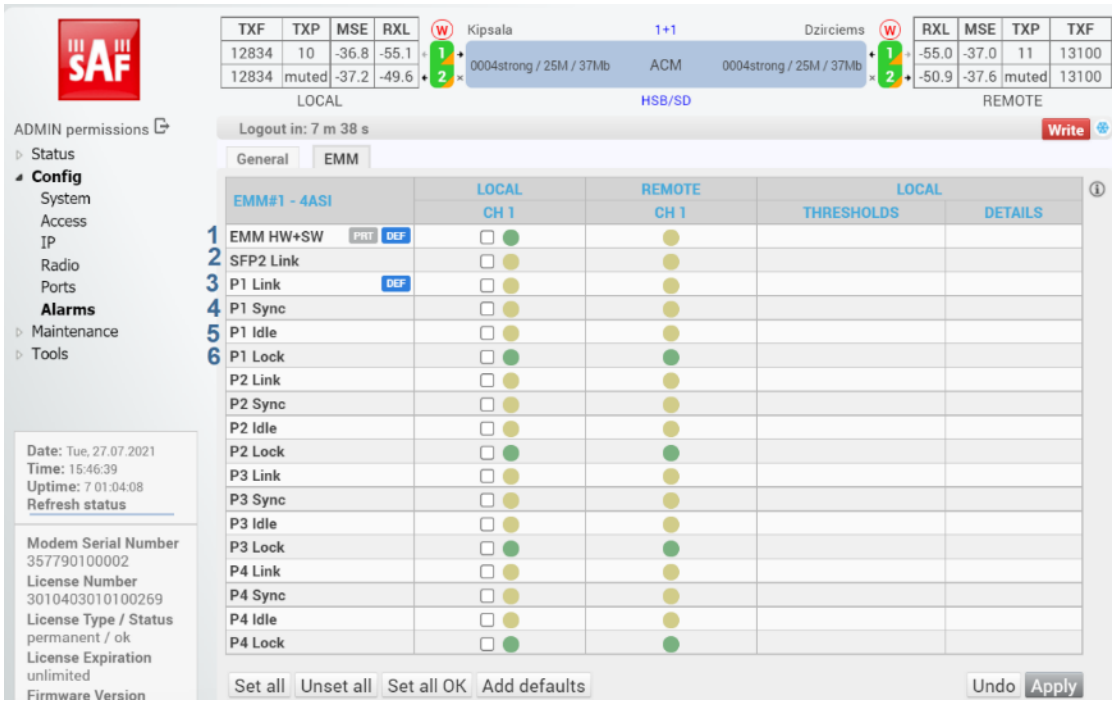


Figure 3.47 *"Config → Alarms → EMM" page for ASI EMM*

1) ***EMM HW+SW*** – indicates ASI EMM status. Possible values are:
   - **fifo overflow** – indicates that EMM Rx stream speed exceeds the available link throughput

- **src ID** – mismatch with remote EMM settings. For example, when trying to operate ASI EMM against a E1/T1 EMM

2) ***SFP2 Link*** – status of the secondary SFP port link.
3) ***P(1-4) Link:***
   - For Tx it will be always 'ok' status
   - For Rx – status of ASI Rx port link
4) ***P(1-4) Sync*** – indicates a synchronisation status to current ASI signal. The alarm can occur when there is RF link synchronization loss event or when ASI data are corrupted
5) ***P(1-4) Idle*** – indication of an unexpected pause in user data (MPEG stream is missing)
6) ***P(1-4) Lock:***
   - For Tx – indicates ASI PCR lock status. The alarm may occur in following cases: during ACM modulation shifting, during Protection switchover, due to variable ASI stream speed or link errors. It can also appear after establishing of synchronization when it can take up to a minute until it is correctly aligned and alarm cleared
   - For Rx it will be always 'ok' status

In case of E1/T1 EMM enabled, the E1/T1 related alarms will be displayed:

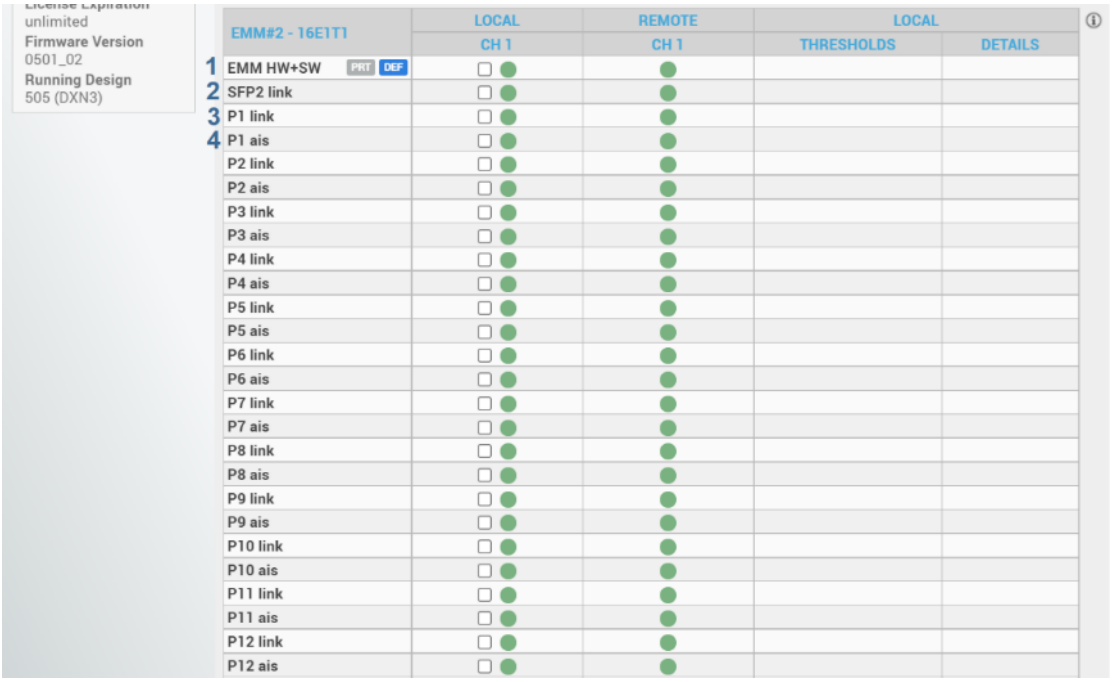


Figure 3.48 *"Config → Alarms → EMM" page for E1/T1 EMM*

1) ***EMM HW+SW*** – indicates E1/T1 EMM status. Possible values are:
   - **clk recovery** – indicates about no data to transfer; generating AIS instead
   - **fifo overflow** – indicates that EMM Rx stream speed exceeds the available link throughput
   - **src ID** – mismatch with remote EMM settings. For example, when trying to operate E1/T1 EMM against an ASI EMM
2) ***SFP2 Link*** – status of the secondary SFP port link.
3) ***P(1-16) link –*** status of E1/T1 port link
4) ***P(1-16) ais –*** indicates about the receiving of AIS signal. This alarm indicates a problem in the E1/T1 source device attached to particular E1/T1 port:

- For E1: two or less ‘0’ in each of two consecutive 512-bit streams received
- For T1: less than nine ‘0’ contained in 8192 bits

Maintenance

Maintenance → Configuration → Save&Run

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

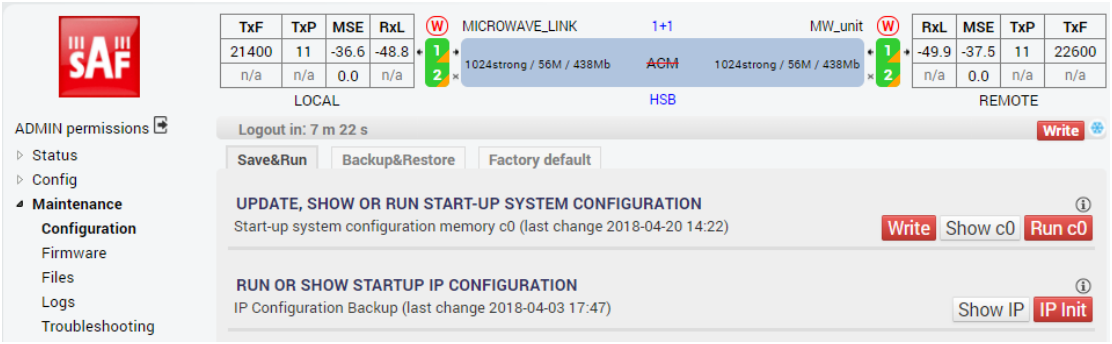


***Figure 3.49** “Maintenance → Configuration → Save&Run” page*

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

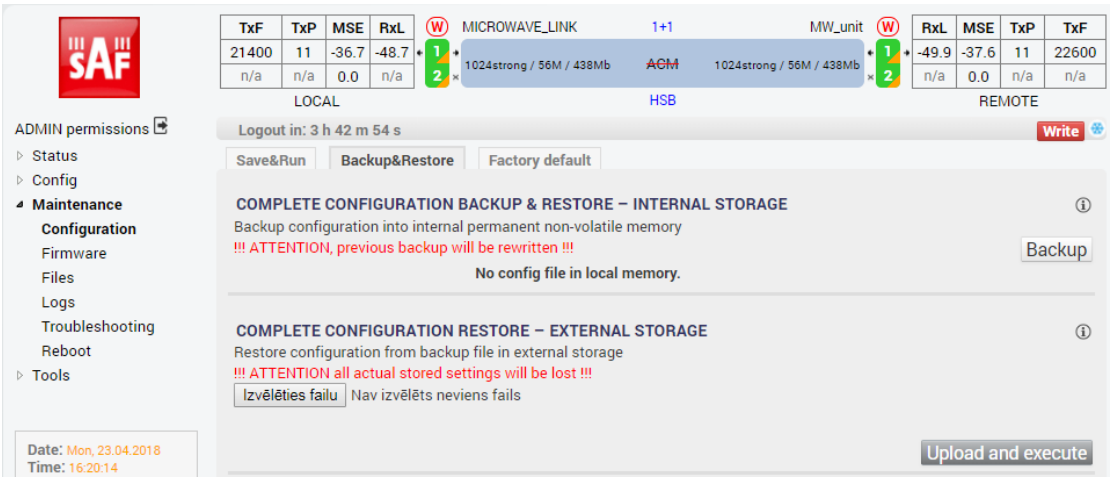


***Figure 3.50** "Maintenance → Configuration → Backup&Restore" page*

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.

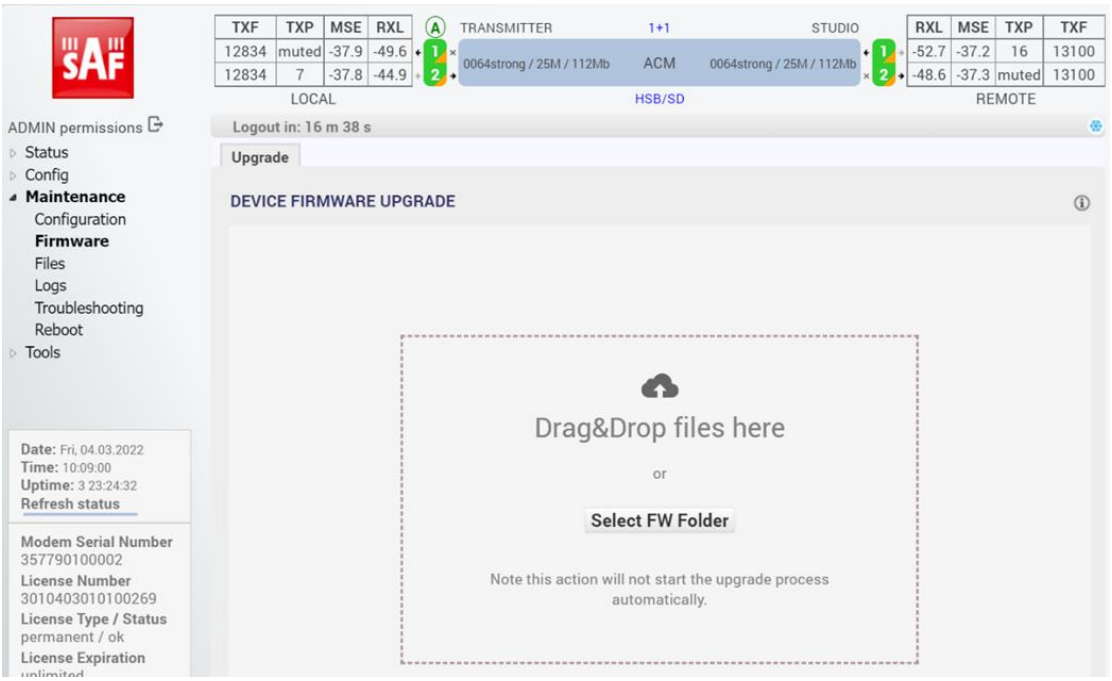


***Figure 3.52** "Maintenance → Firmware → Upgrade" page*

The firmware file upload can be done in 2 ways:

- By Drag&Drop all firmware files simultaneously into the indicated field
- By pressing the "Select FW Folder" button to choose the folder where all firmware files are located

Once the firmware files will be uploaded, next information will appear automatically:

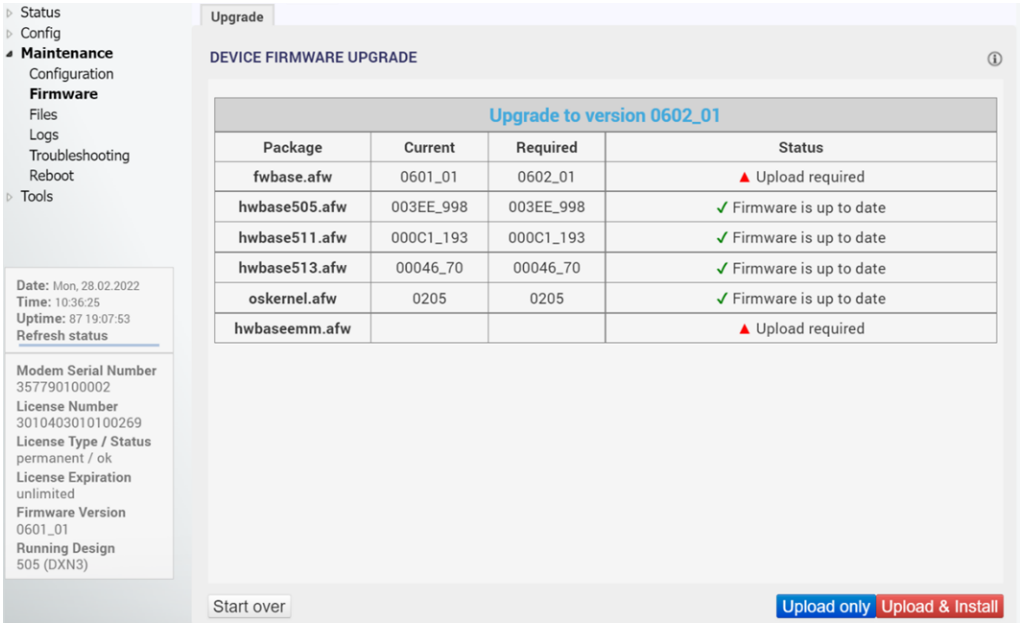


***Figure 3.53** "Maintenance → Firmware → Upgrade" page when FW files uploaded*

Following buttons will appear to continue with the upgrade process:

- Upload & Install – by pressing this button the required files will by uploaded and installed in the IDU. This process will automatically reboot the IDU after the installation and finish the FW upgrade process. During the reboot the traffic will be stopped
- Upload only – pressing this button uploads all the required FW parts into the device internal storage but will not start the upgrade procedure, so that it can be invoked manually later by the Install button. Pressing the Install button will complete the upgrade process, the IDU will be rebooted automatically. During the reboot the traffic will be stopped
- Start over – pressing this button will revert back to the beginning of the firmware upgrade procedure. This action can be done in case of any issues or indication about missing any of firmware files

> ⚠ 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 → 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 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):

- oskernel.afw – operating system
- hwbase505.afw, hwbase511.afw – software for internal HW parts
- 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.

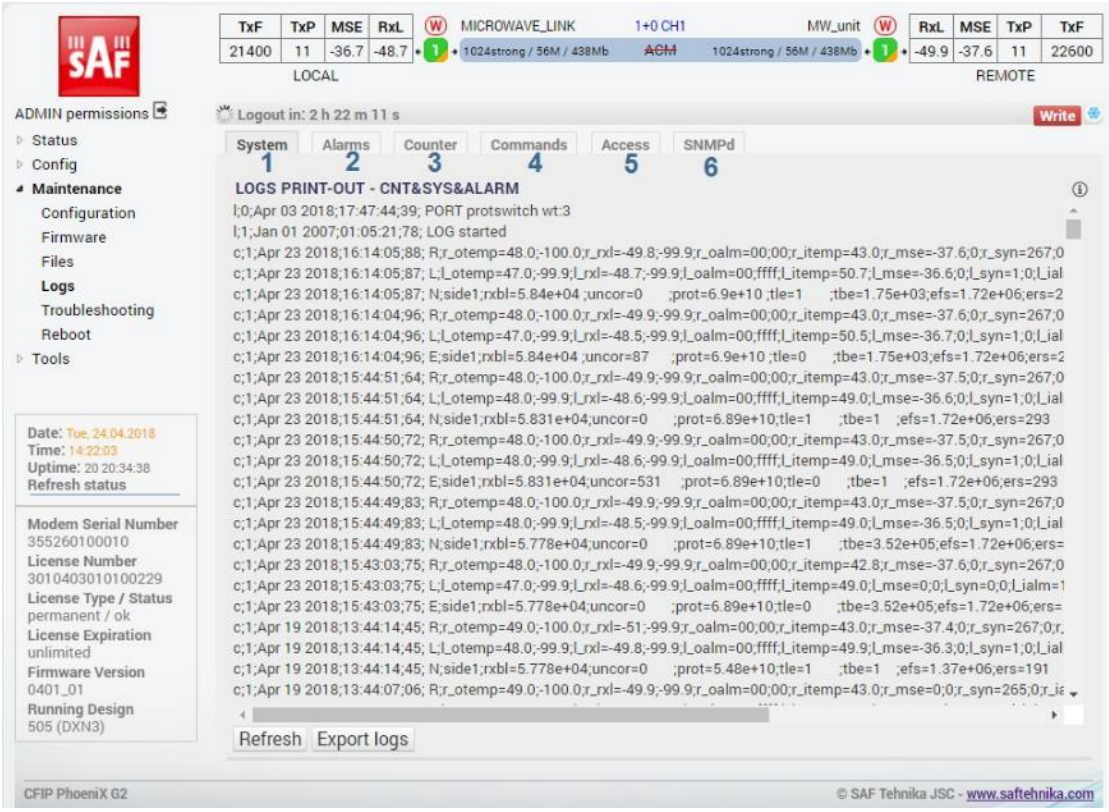


Figure 3.56 *"Maintenance → Logs" page*

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.

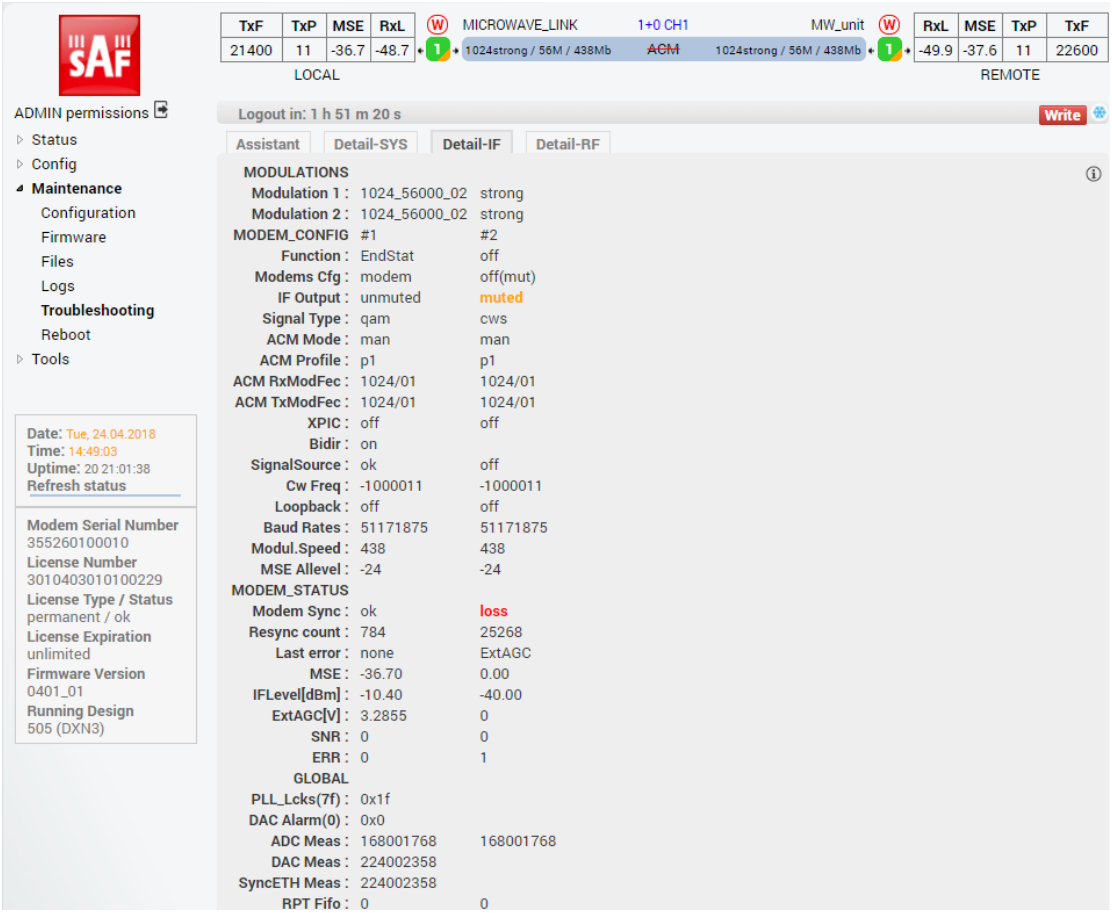


***Figure 3.59** "Maintenance → Troubleshooting → Detail-IF" page*

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.

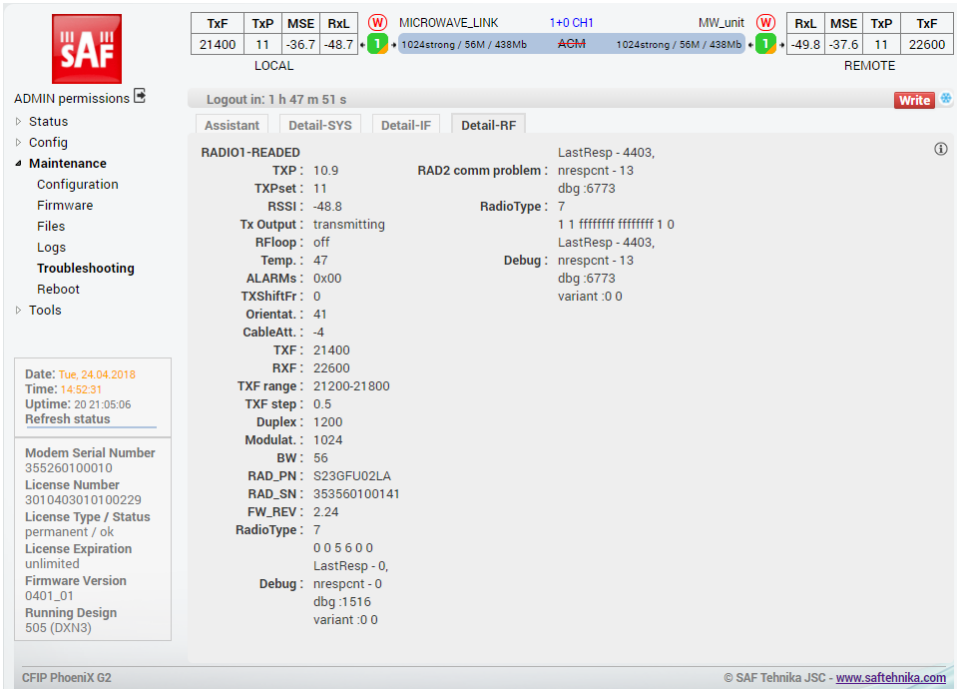


***Figure 3.60** "Maintenance → Troubleshooting → Detail-RF" page*

Maintenance → Reboot

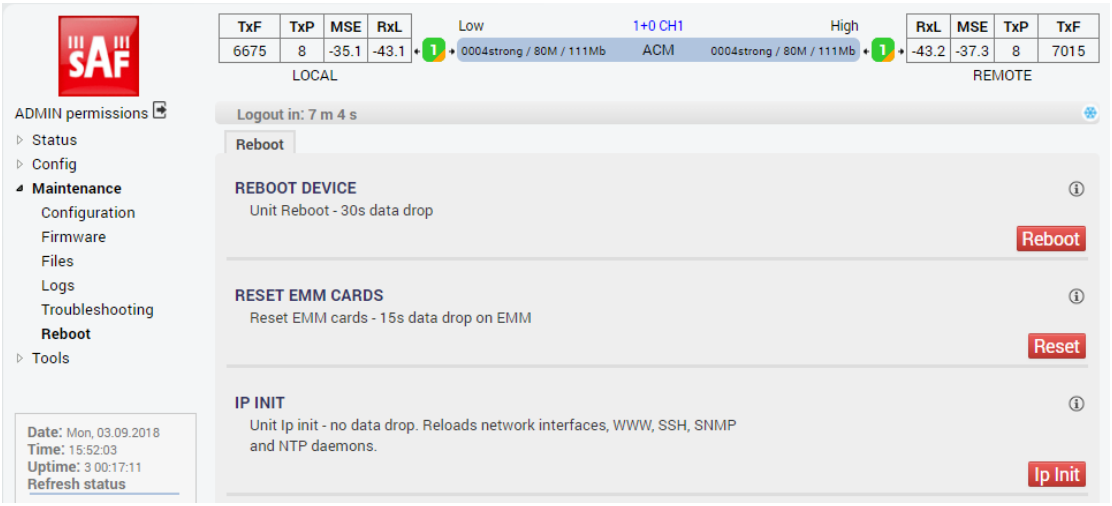


***Figure 3.61** "Maintenance → Reboot" page*

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

Reset - 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.

Ip Init - 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.

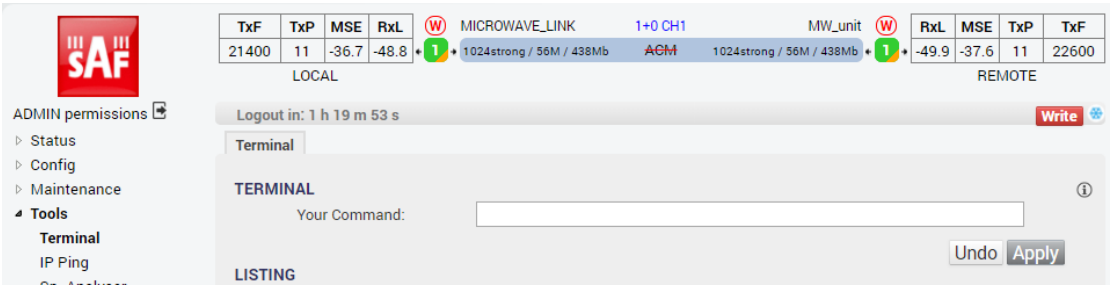


***Figure 3.62** "Tools → Terminal" page*

Tools → IP Ping

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

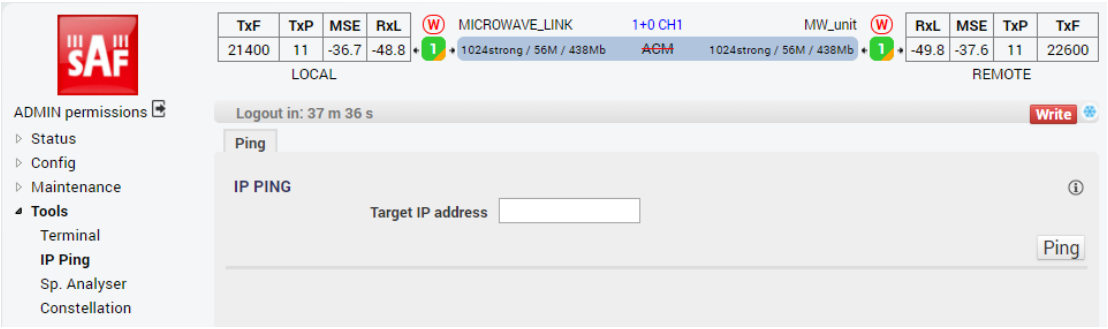


Figure 3.63 *"Tools → IP Ping" page*

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

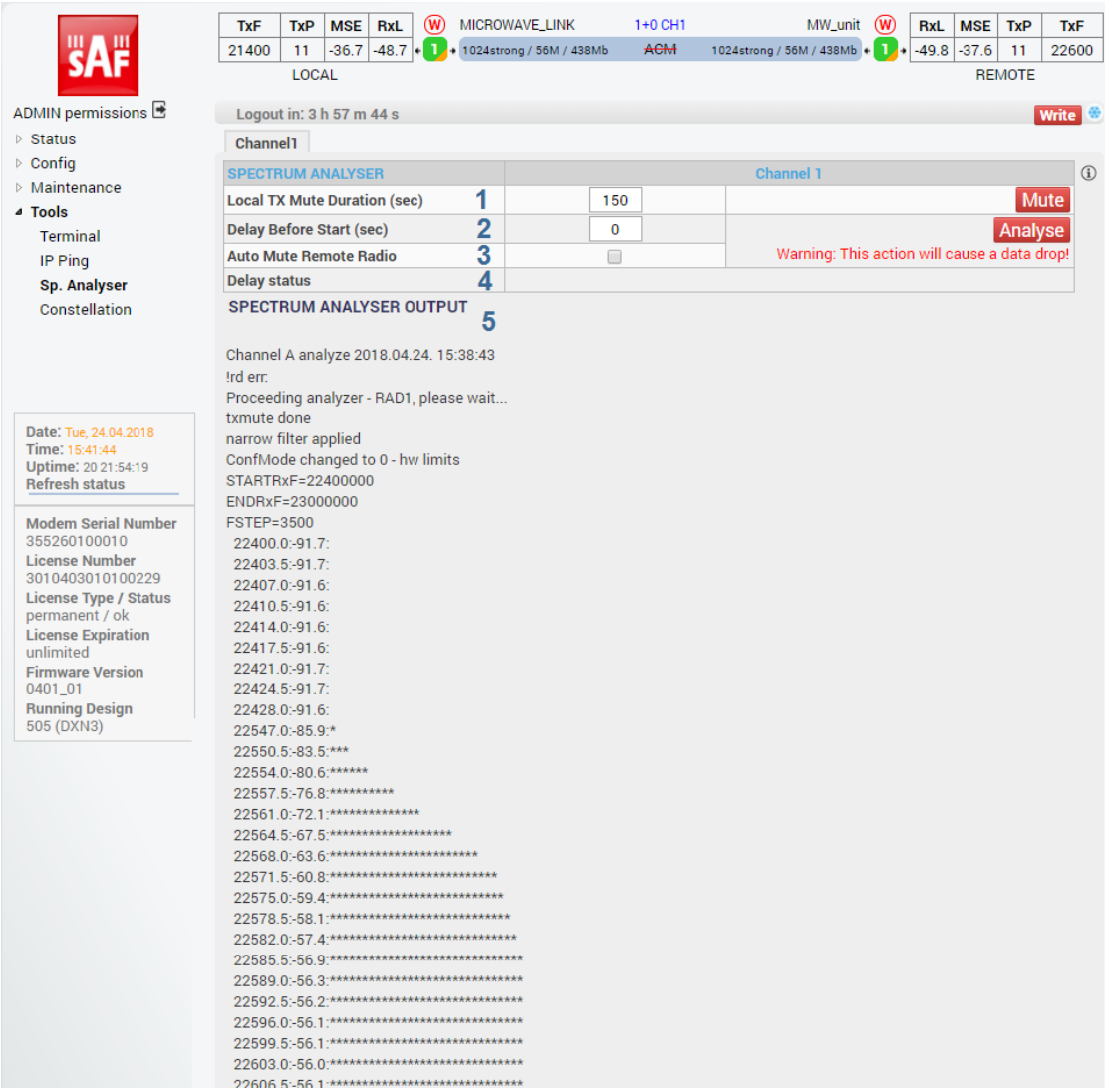


Figure 3.64 *"Tools → Sp. Analyser" page*

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 Analyse 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.

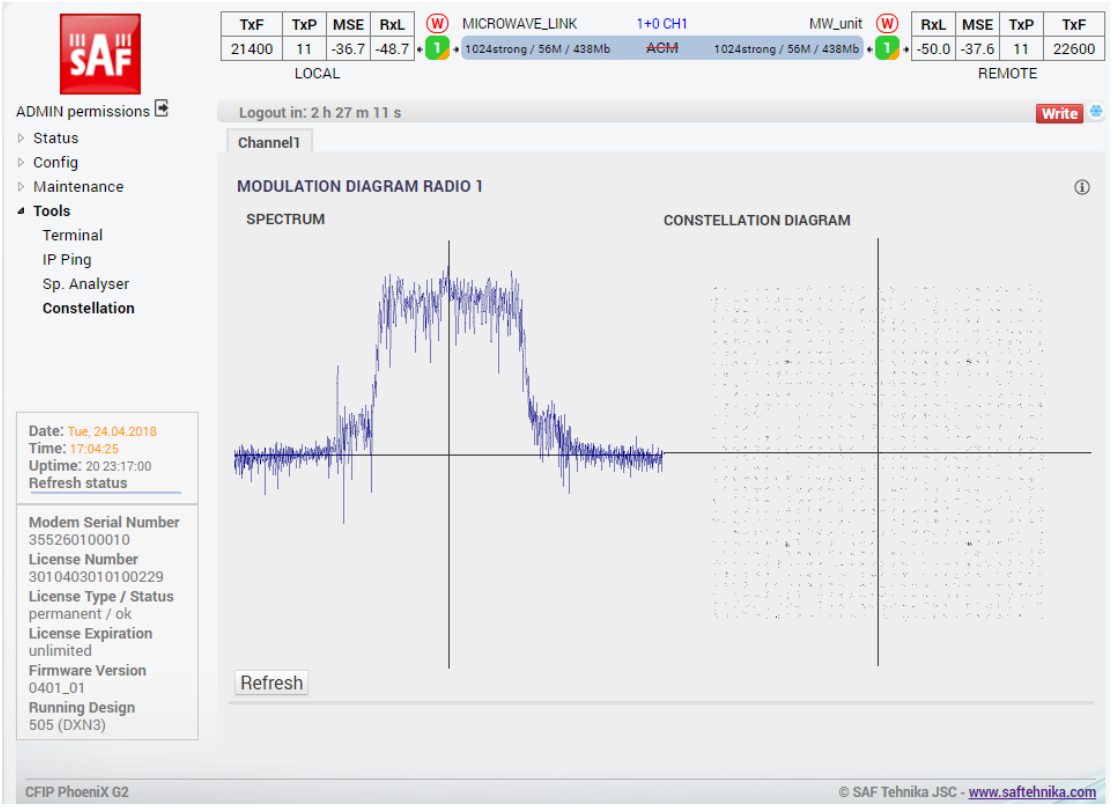
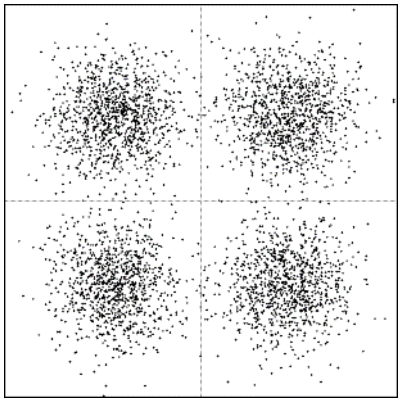


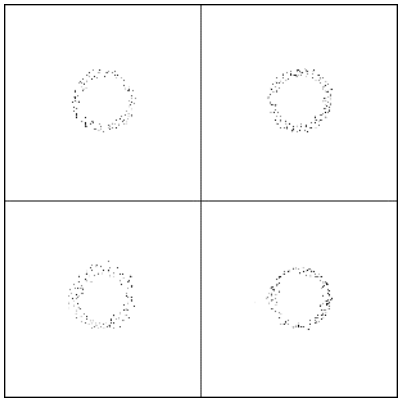
Figure 3.65 *"Tools → Constellation" page*

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

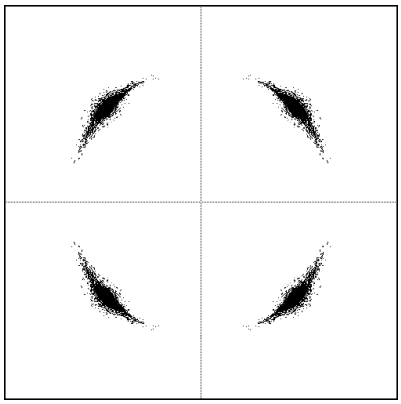
1) Gaussian noise is displayed as fuzzy constellation points:



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:

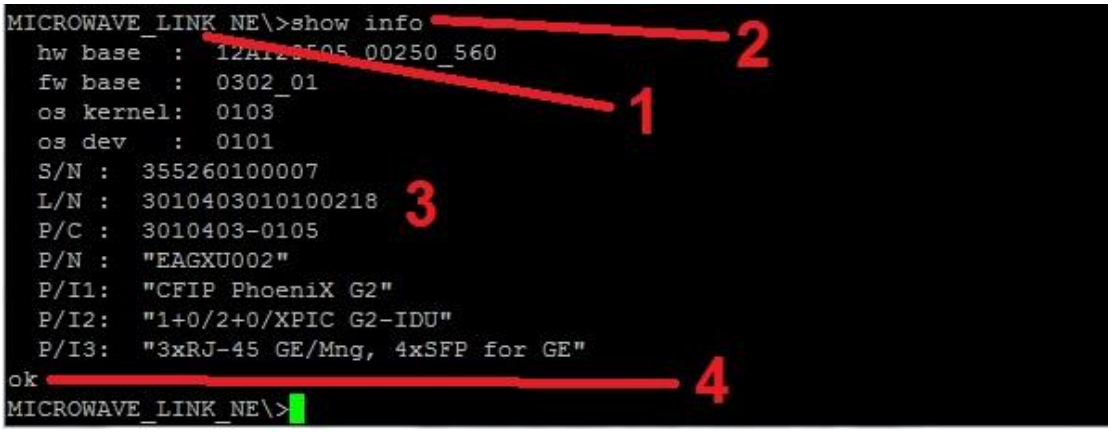


Figure 4.1 *CLI command structure*

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.

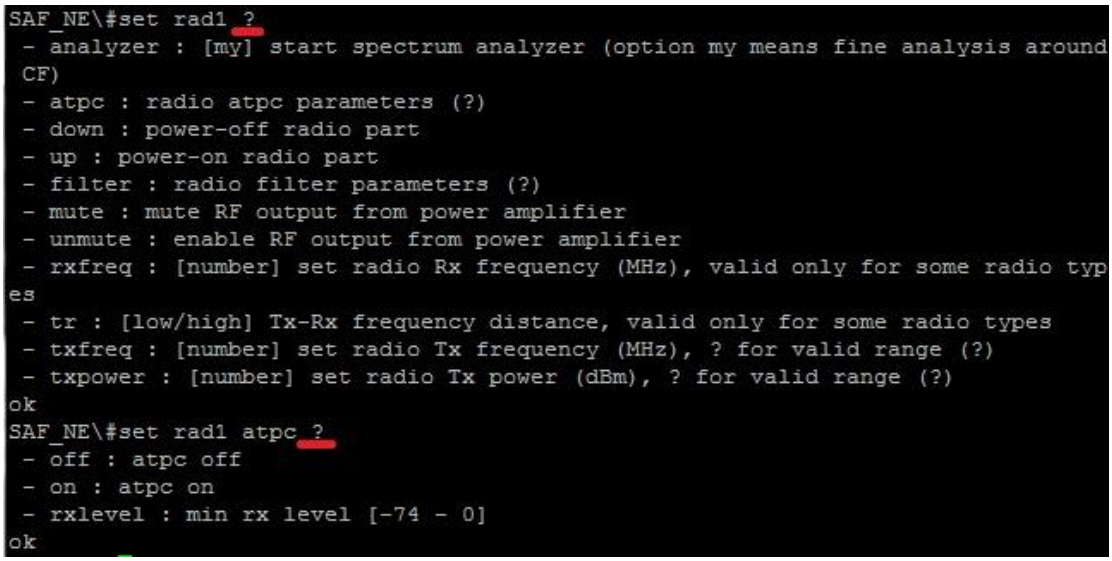


Figure 4.4 *CLI online help*

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):

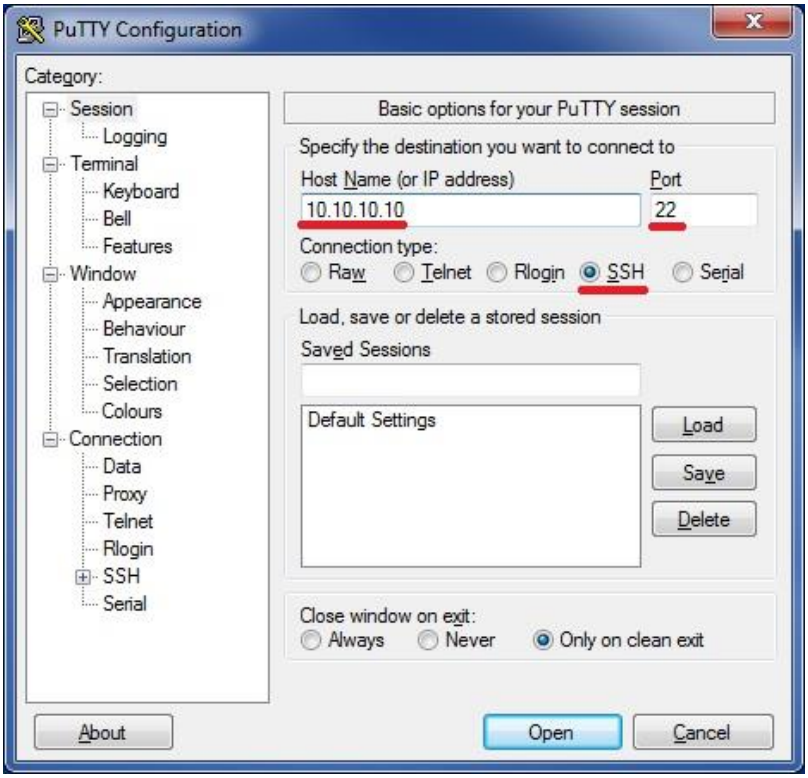


Figure 4.5 *PuTTY configuration*

2. Press “Open”, enter login credentials (default username 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):

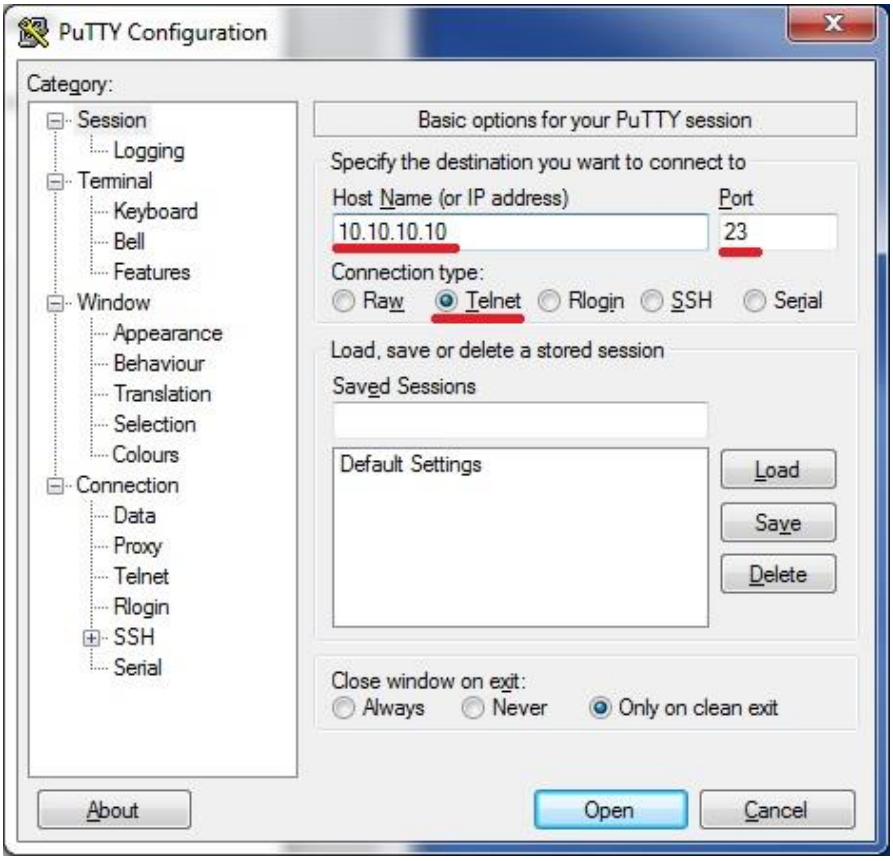


Figure 4.7 *PuTTY confguration*

2. Press “Open”, enter login credentials (default username 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.

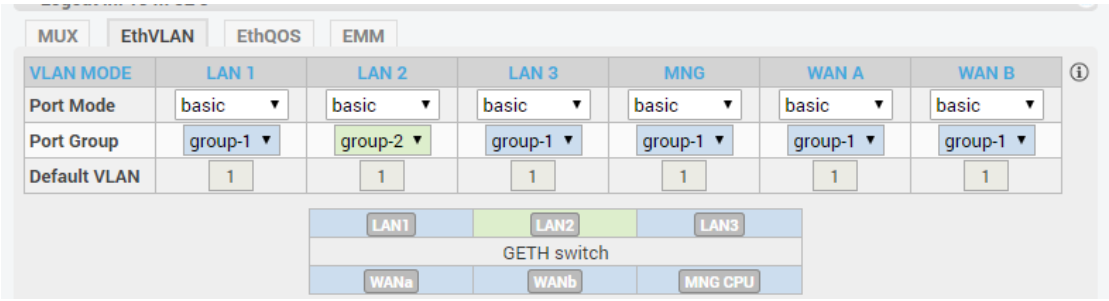


Figure 5.1 *Example of group configuration for WANA and WANB ports*

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.

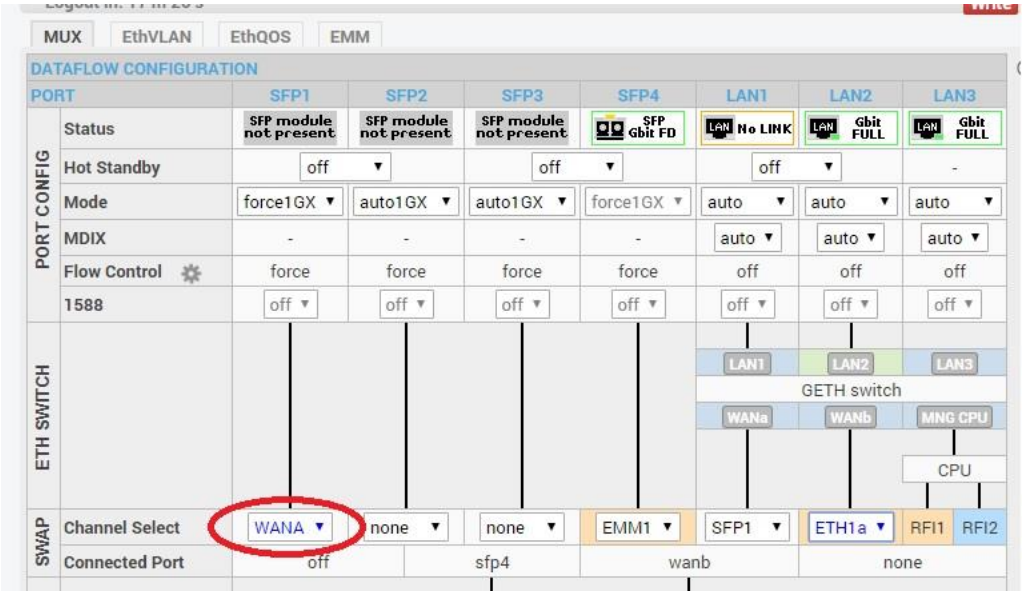


Figure 5.2 *Example of SFP port and WAN port interconnection*

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***).

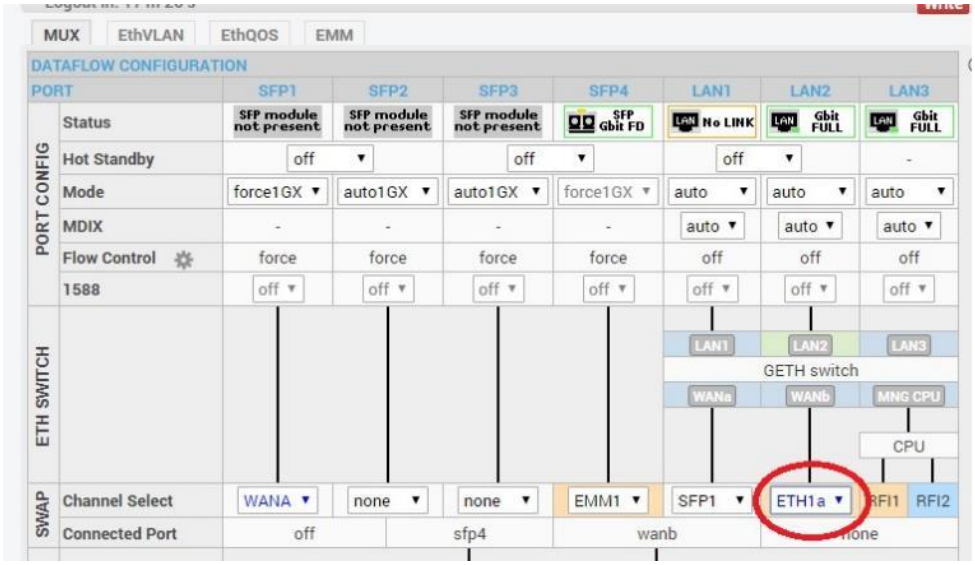


Figure 5.3 *Example of WAN port and data channel interconnection*

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

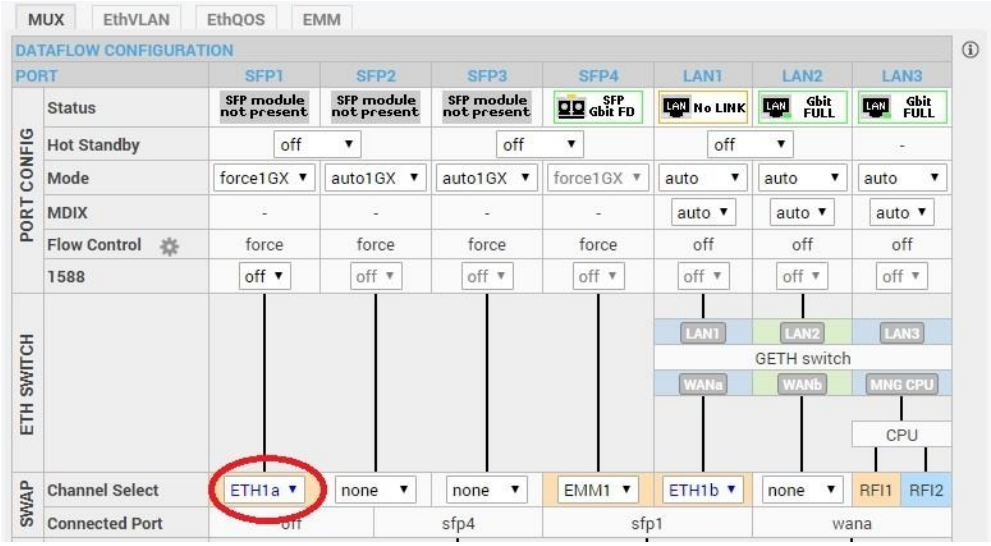


Figure 5.4 *Example of SFP port and data channel interconnection*

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

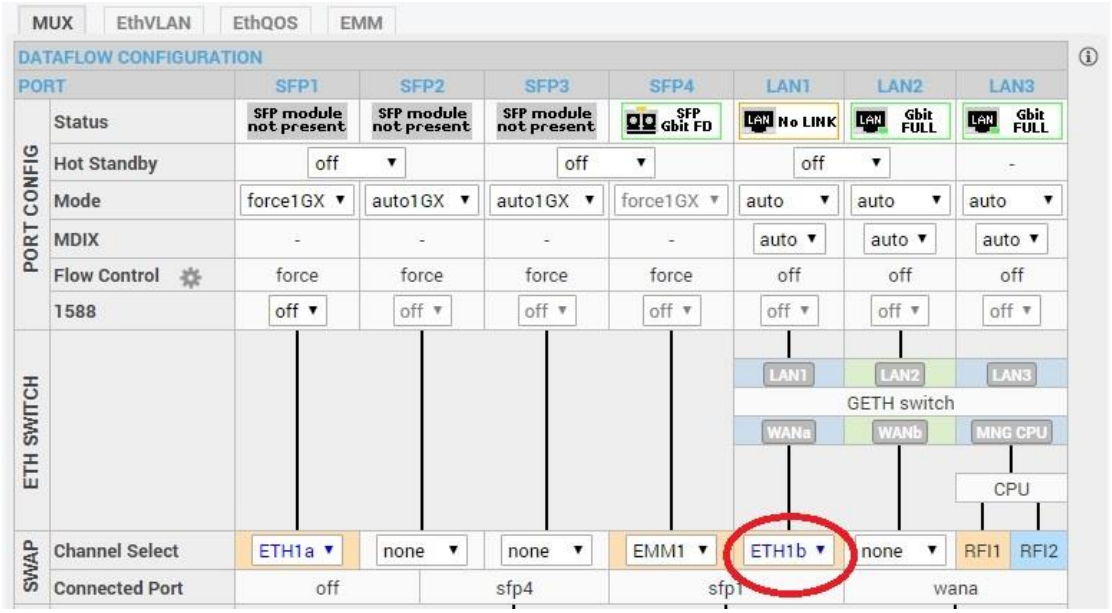


Figure 5.5 *Example of WAN port and data channel interconnection*

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

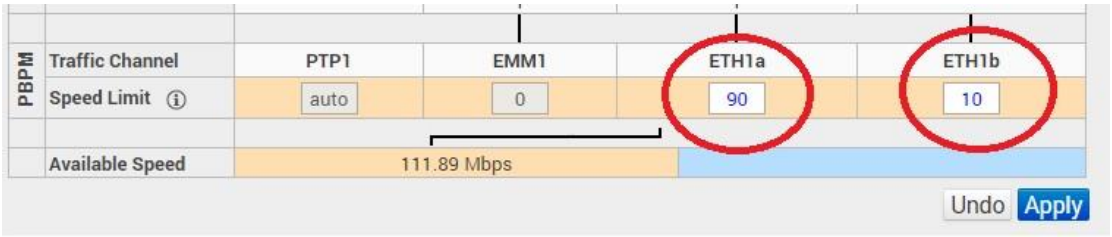


Figure 5.6 *Example of data channel speed limit configuration*

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

Example 2 – 1+1 HSB/SD mode (Design 505)

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.

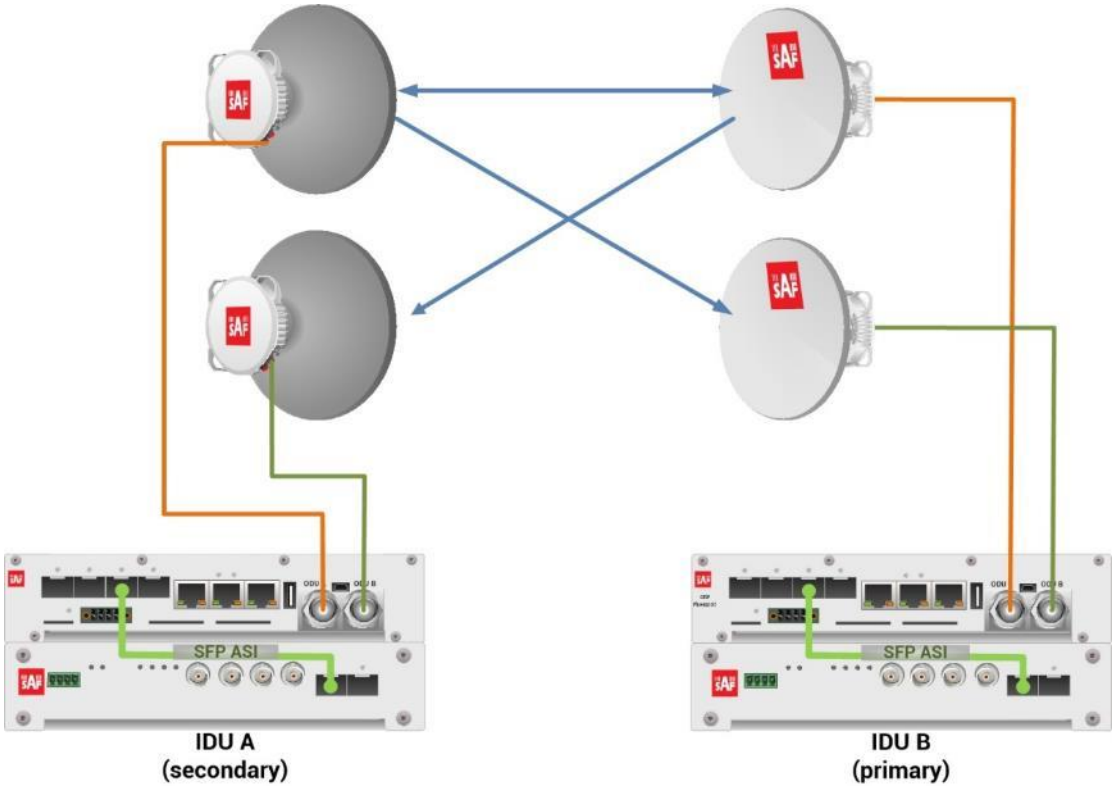


Figure 5.7 *Example of 1+1 SD mode*

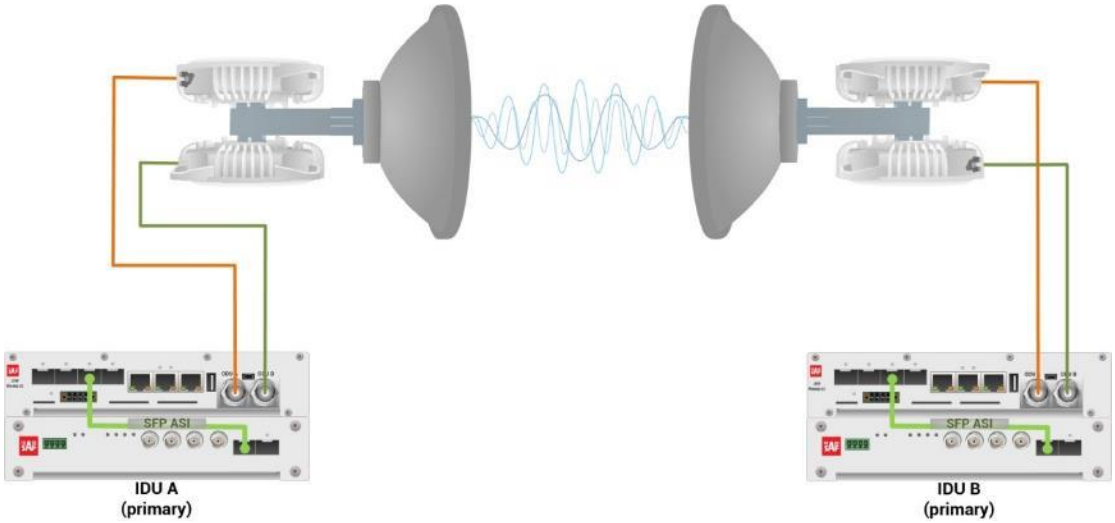


Figure 5.8 *Example of 1+1 HSB mode*

This 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:

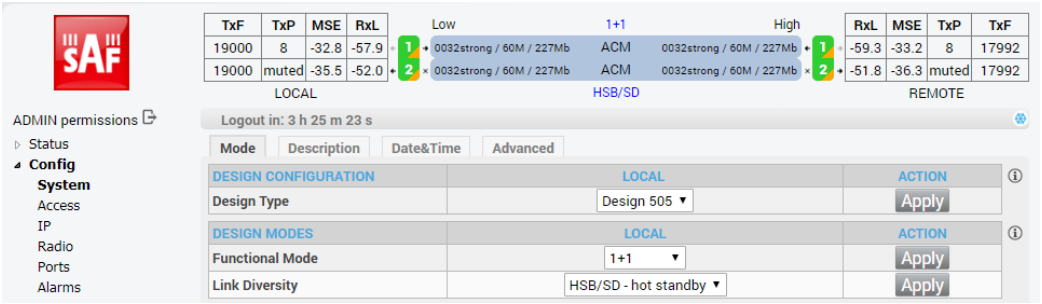


Figure 5.9 *Example of System configuration*

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:

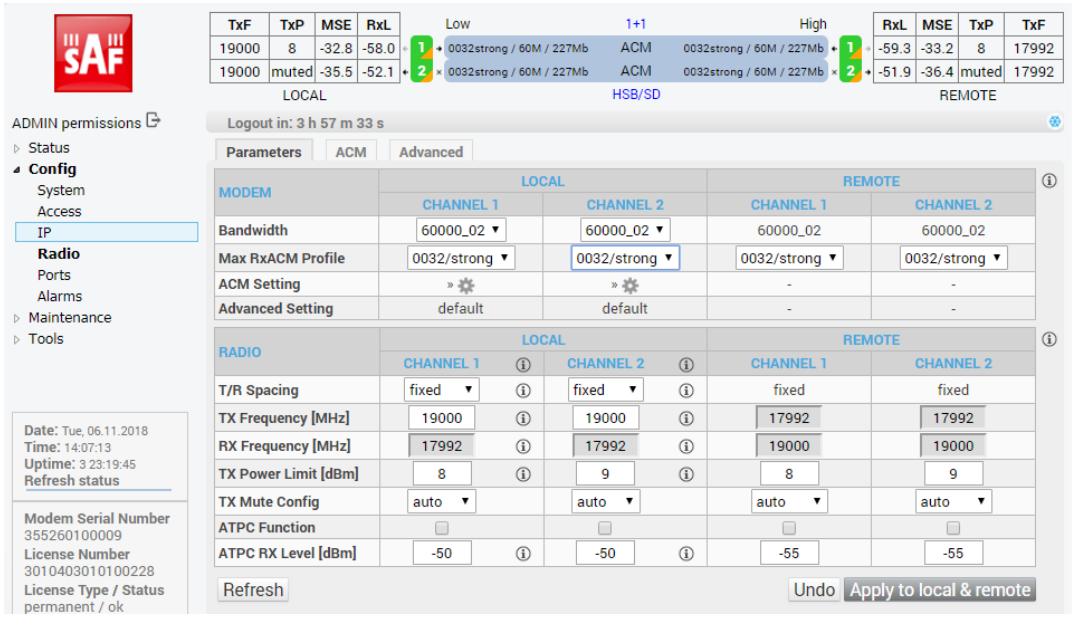


Figure 5.10 *Example of basic Radio parameters configuration*

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.

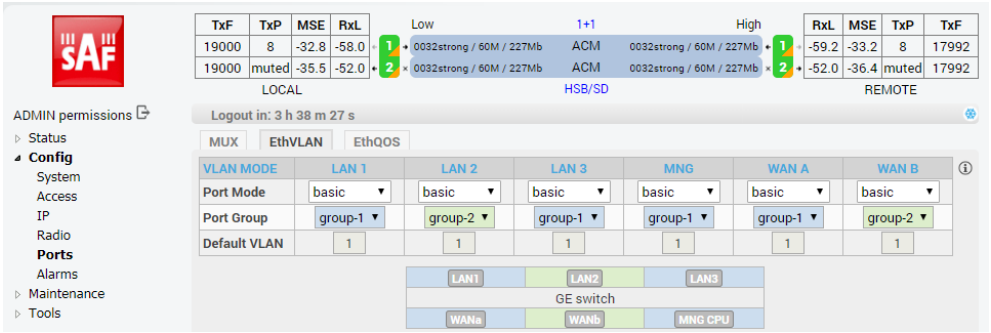


Figure 5.11 *Example of port grouping*

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.

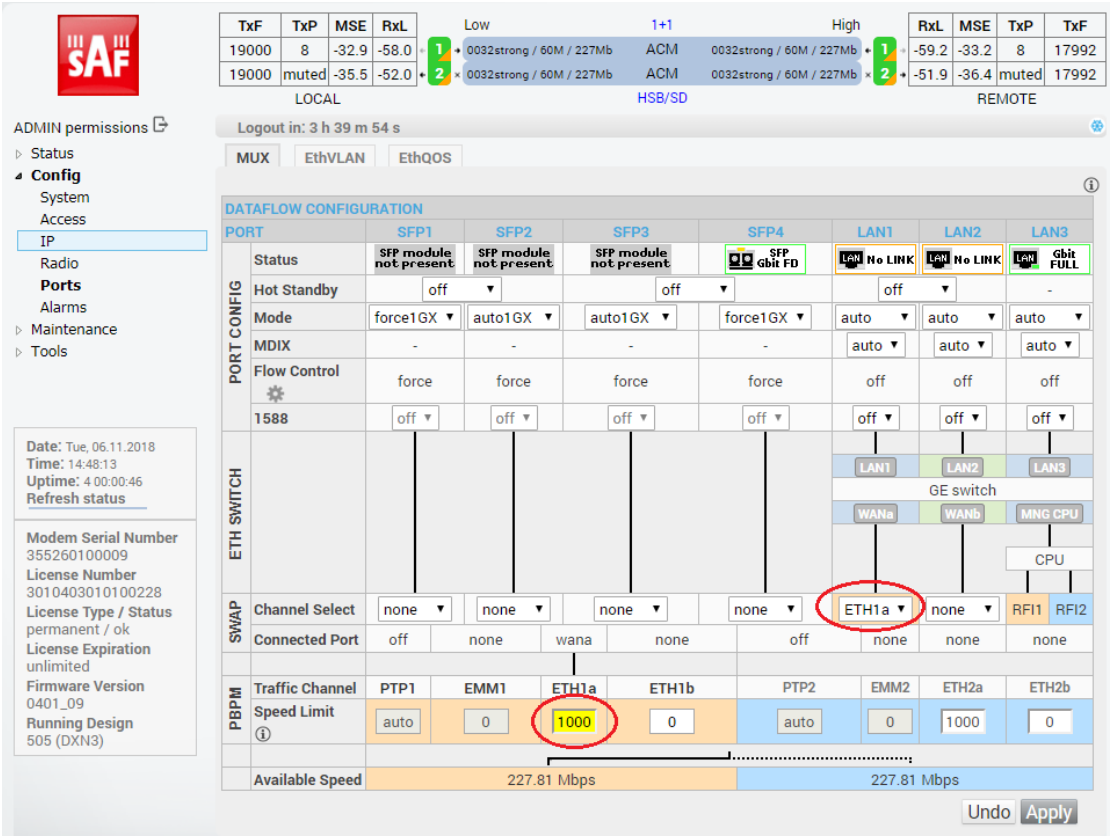


Figure 5.12 *Example of port configuration*

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 Write button.

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

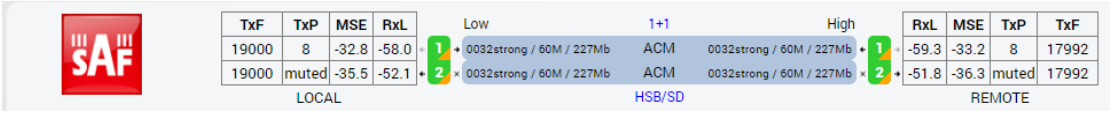


Figure 5.13 *Status of 1+1 HSB/SD mode*

Example 3 – 1+1 FD mode (Design 505)

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.

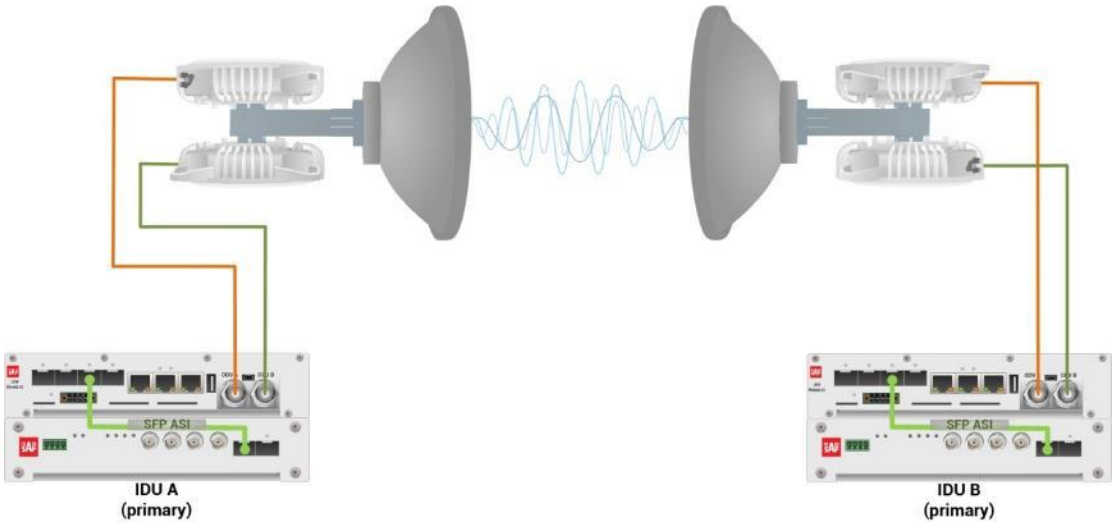


Figure 5.14 *Example of 1+1 FD mode*

This 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:

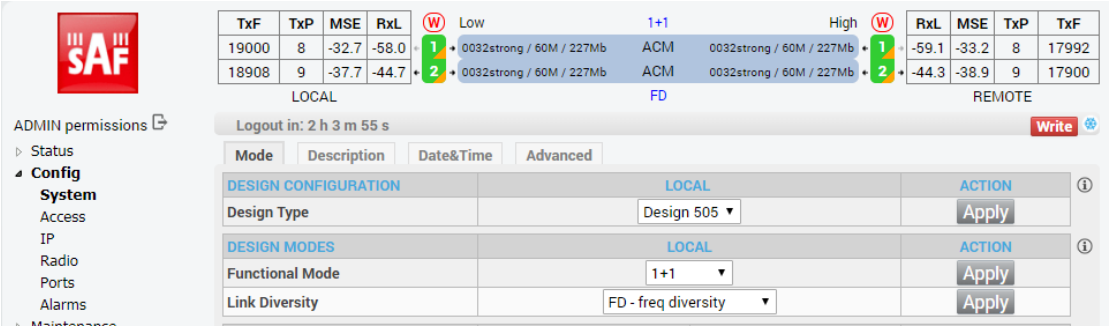


Figure 5.15 *Example of System configuration*

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:

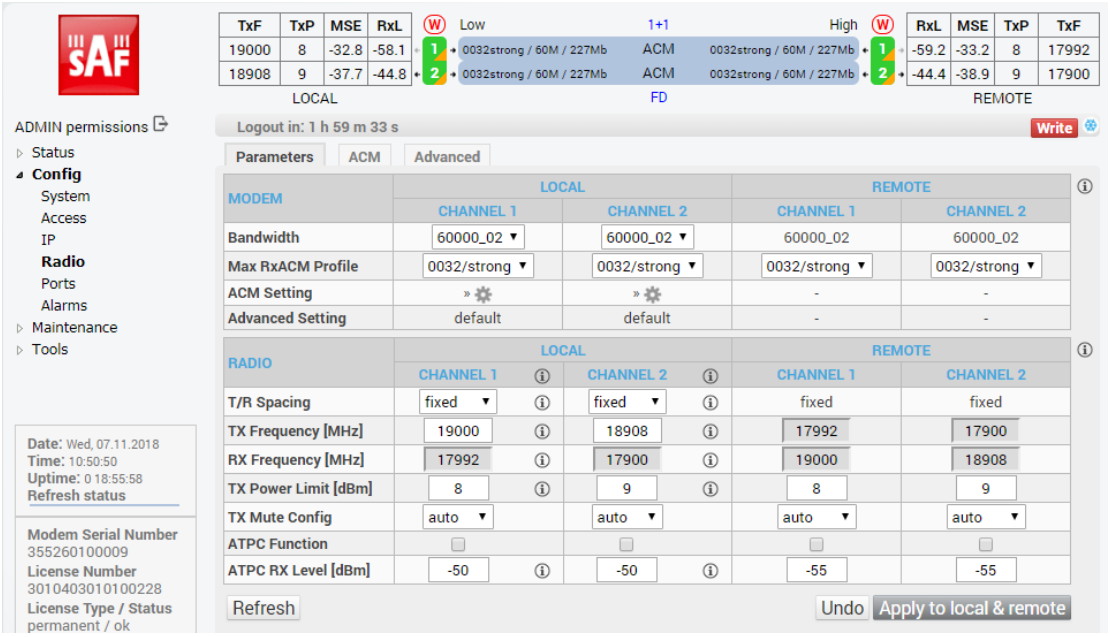


Figure 5.16 *Example of basic Radio parameters configuration*

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.

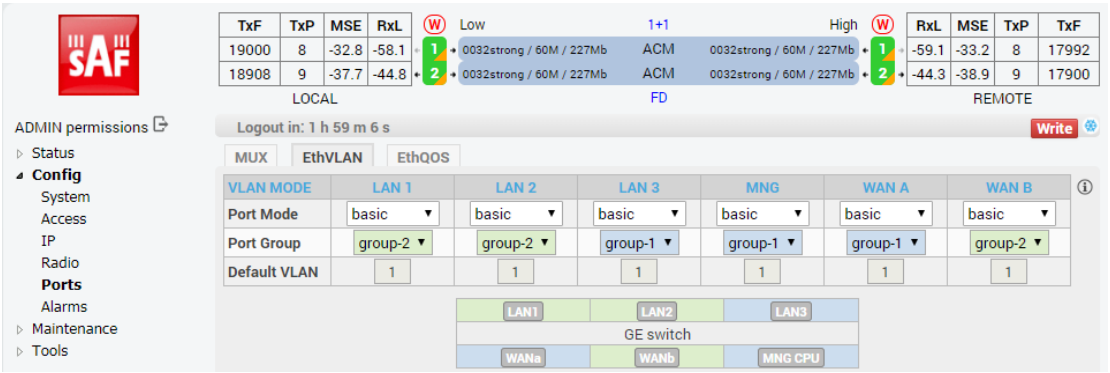


Figure 5.17 *Example of port grouping*

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.

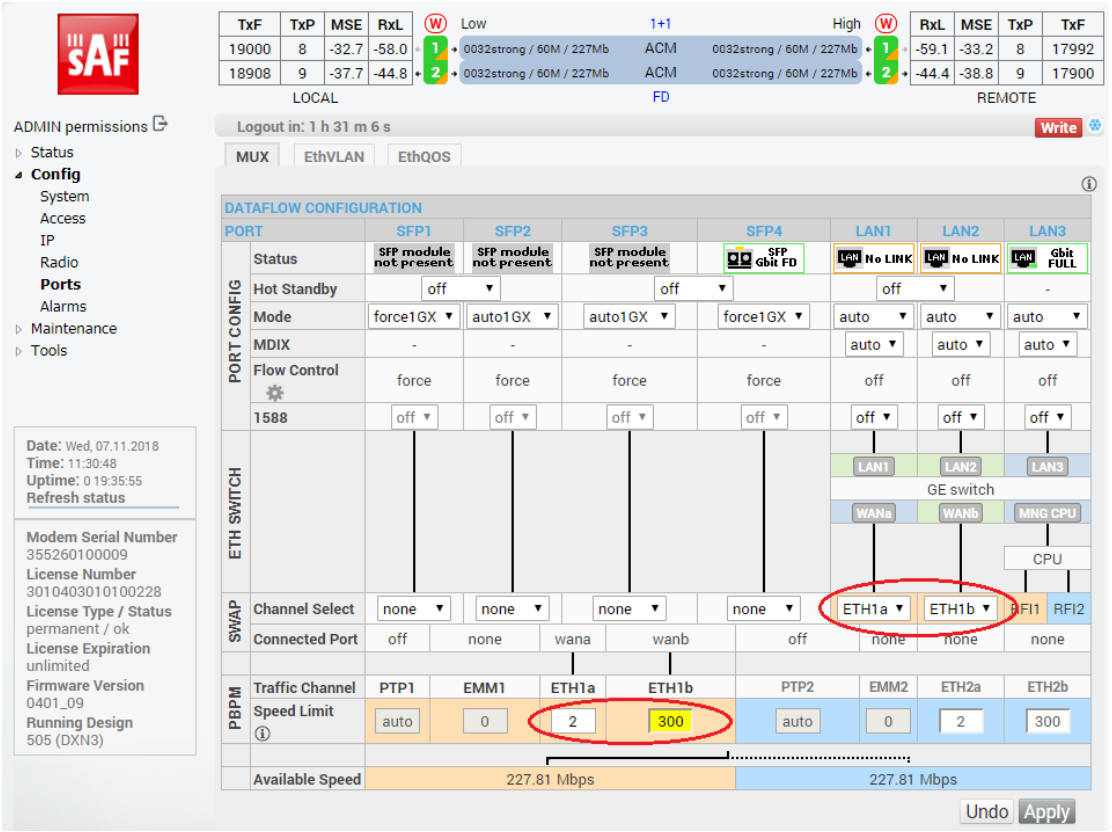


Figure 5.18 *Example of port configuration*

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 Write button.

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

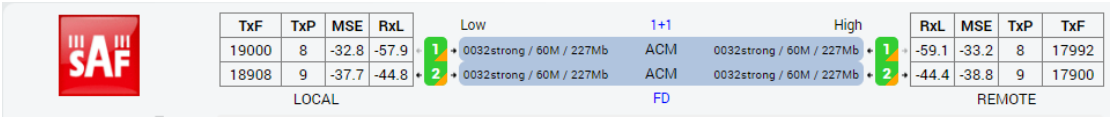


Figure 5.19 *Status of 1+1 FD mode*

Example 4 – 2+0 FD mode (Design 505)

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.

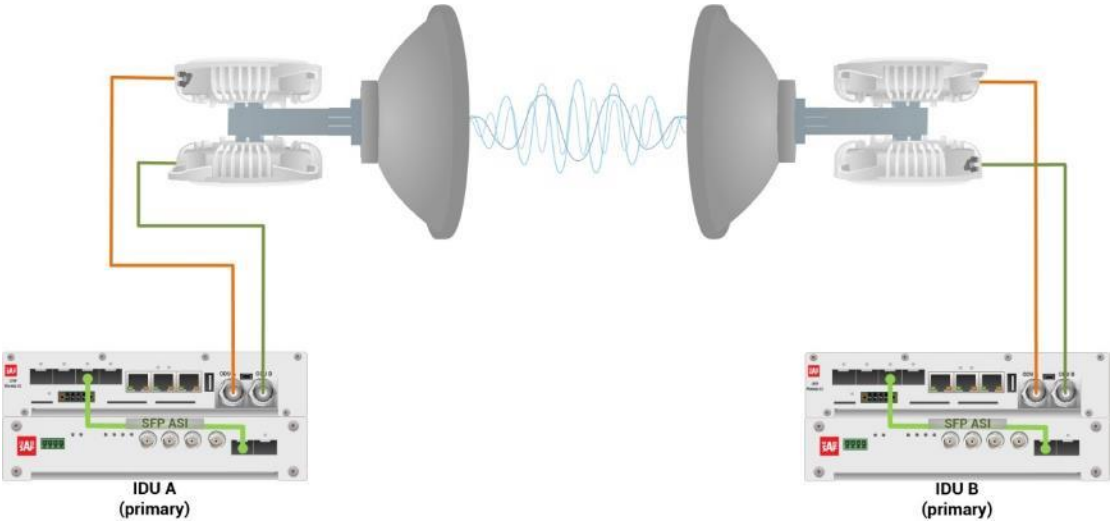


Figure 5.20 *Example of 2+0 FD mode*

This 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:

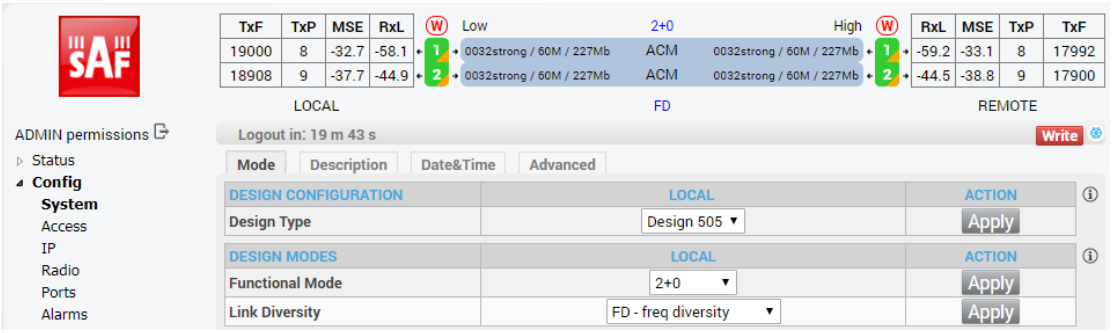


Figure 5.21 *Example of System configuration*

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:

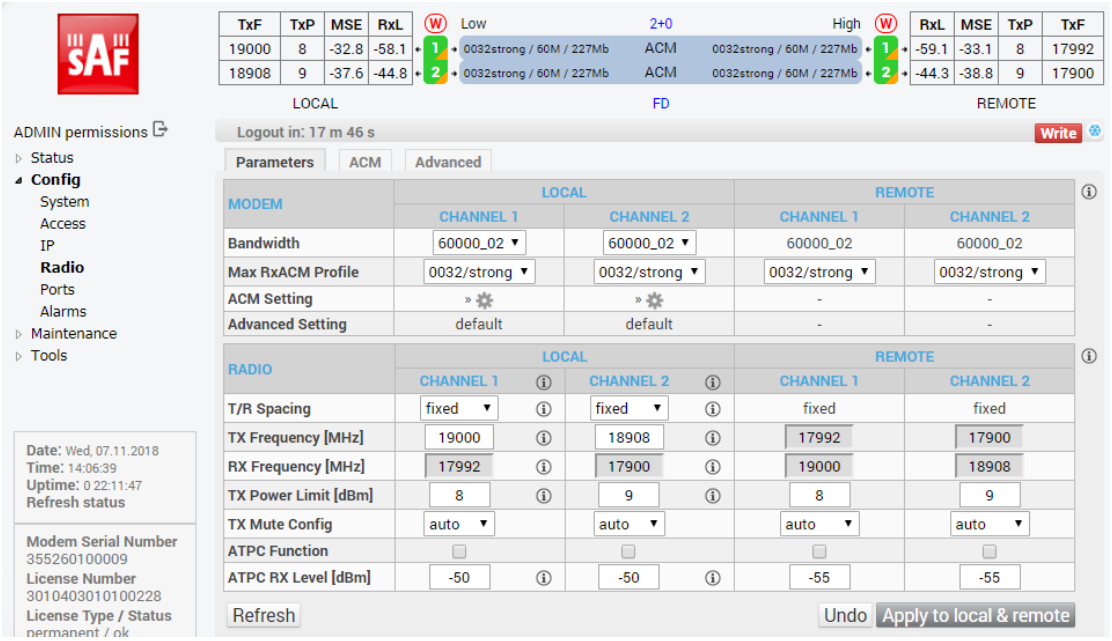


Figure 5.22 *Example of basic Radio parameters configuration*

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.

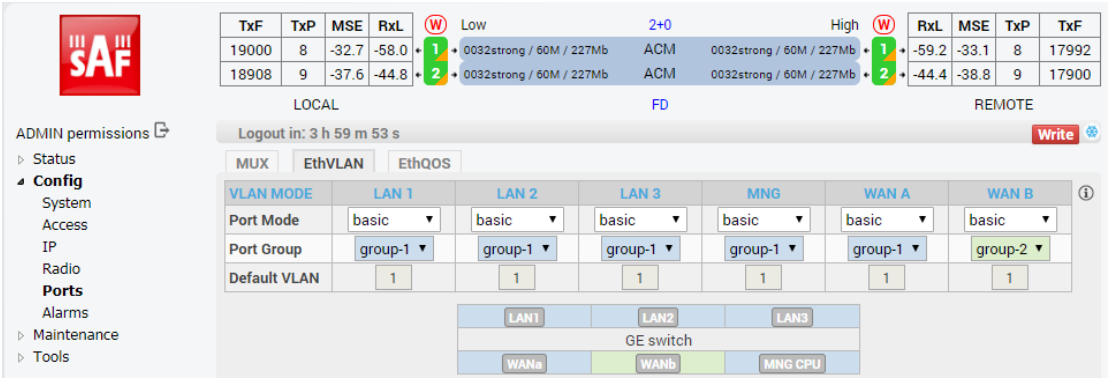


Figure 5.23 *Example of port grouping*

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.

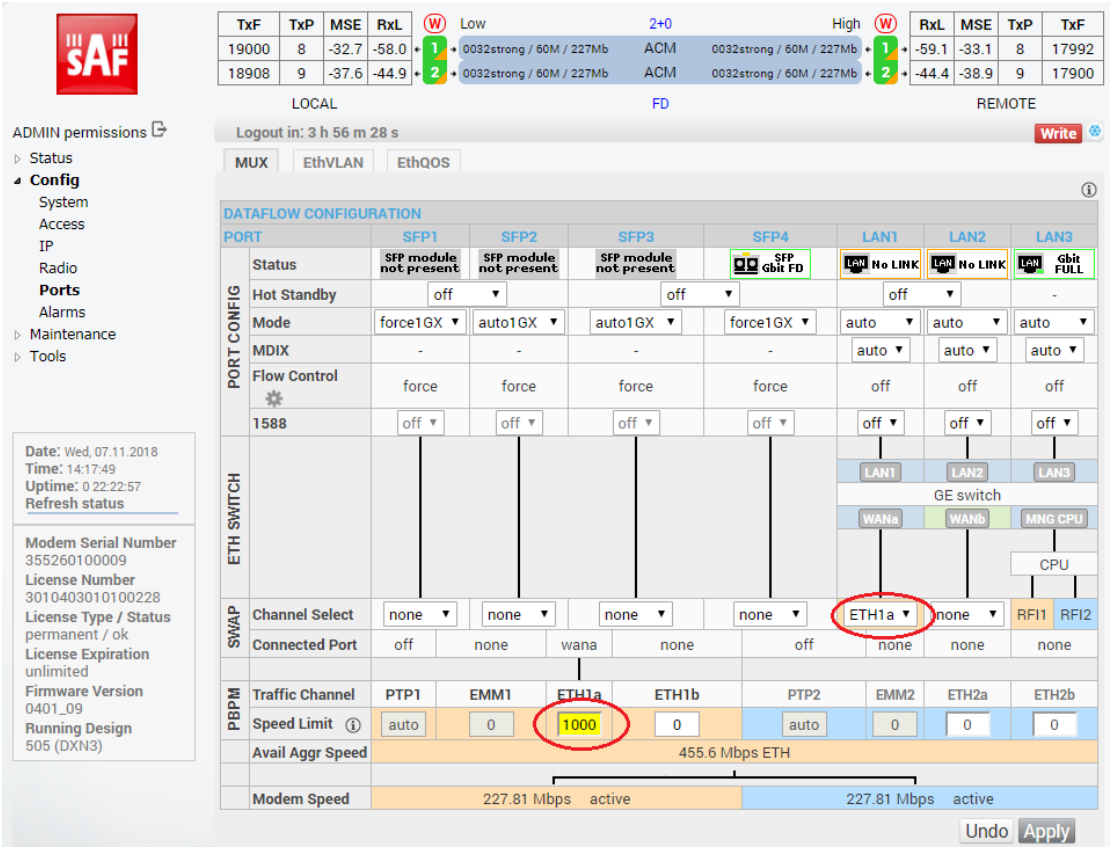


Figure 5.24 *Example of port configuration*

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 Write button.

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

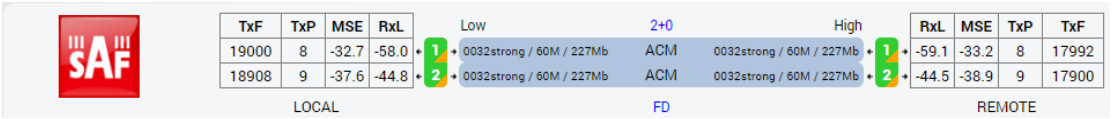


Figure 5.25 *Status of 2+0 FD mode*

Example 5 – 2+0 XPIC mode (Design 505)

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.

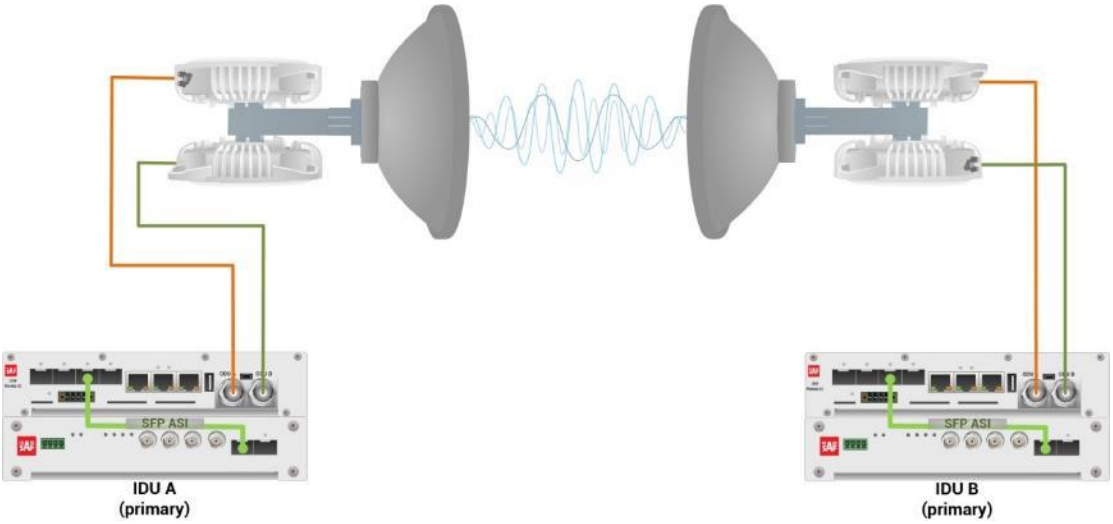


Figure 5.26 *Example of 2+0 XPIC mode*

This 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:

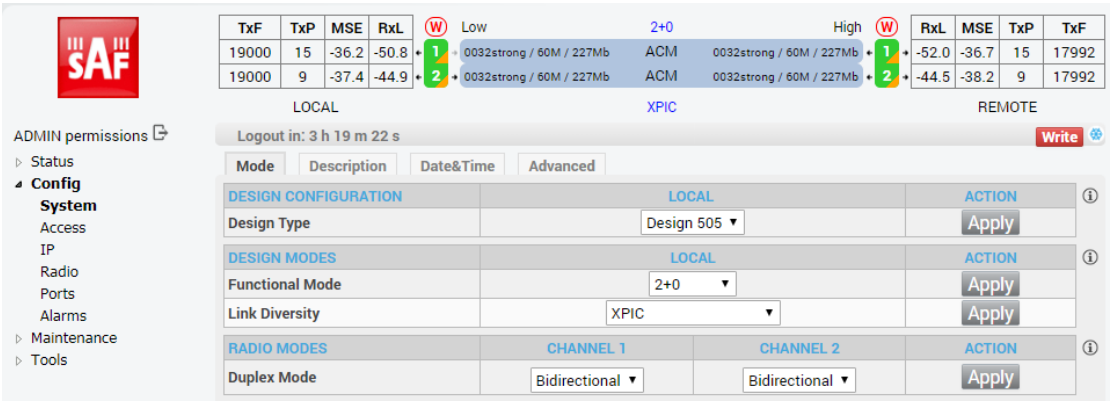


Figure 5.27 *Example of System configuration*

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:

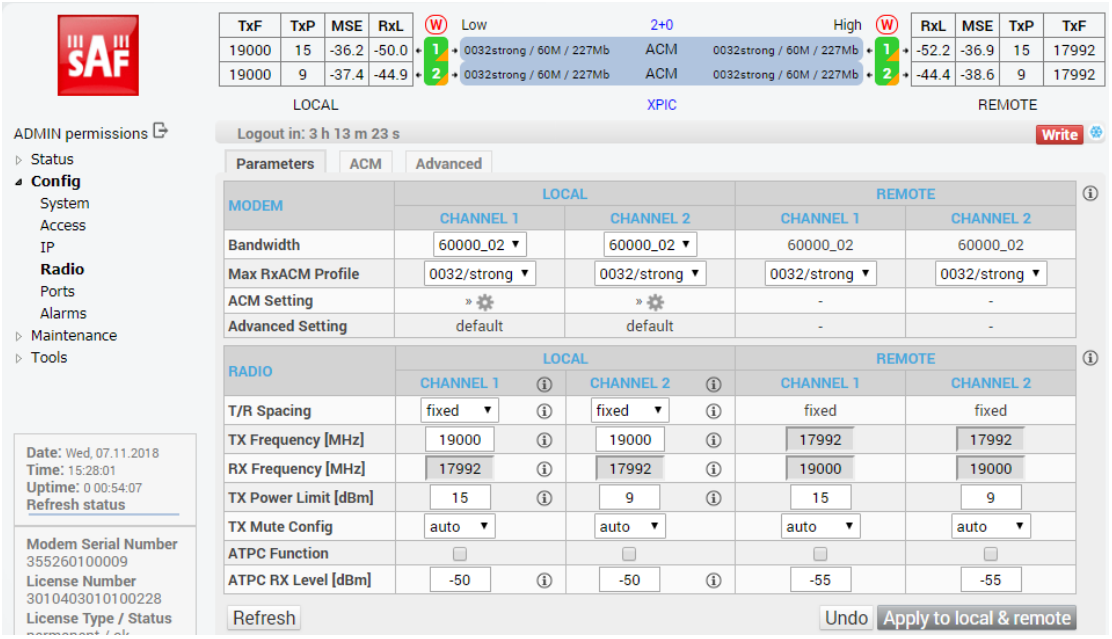


Figure 5.28 *Example of basic Radio parameters configuration*

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.

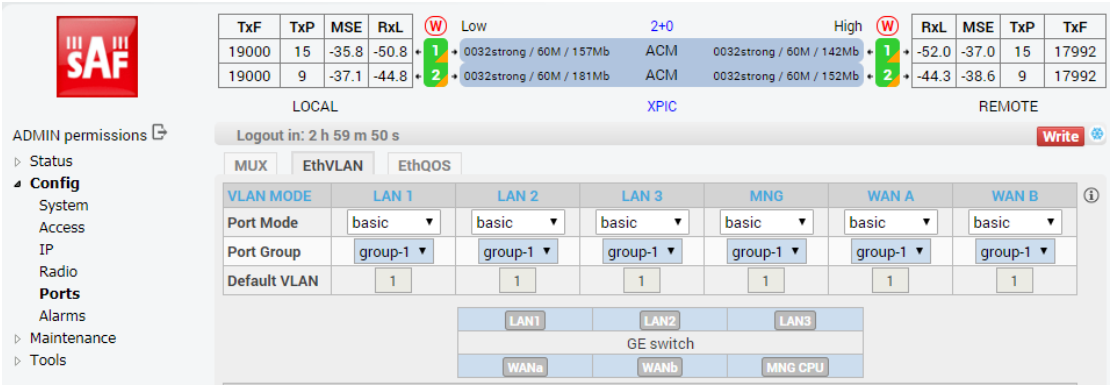


Figure 5.29 *Example of port grouping*

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.

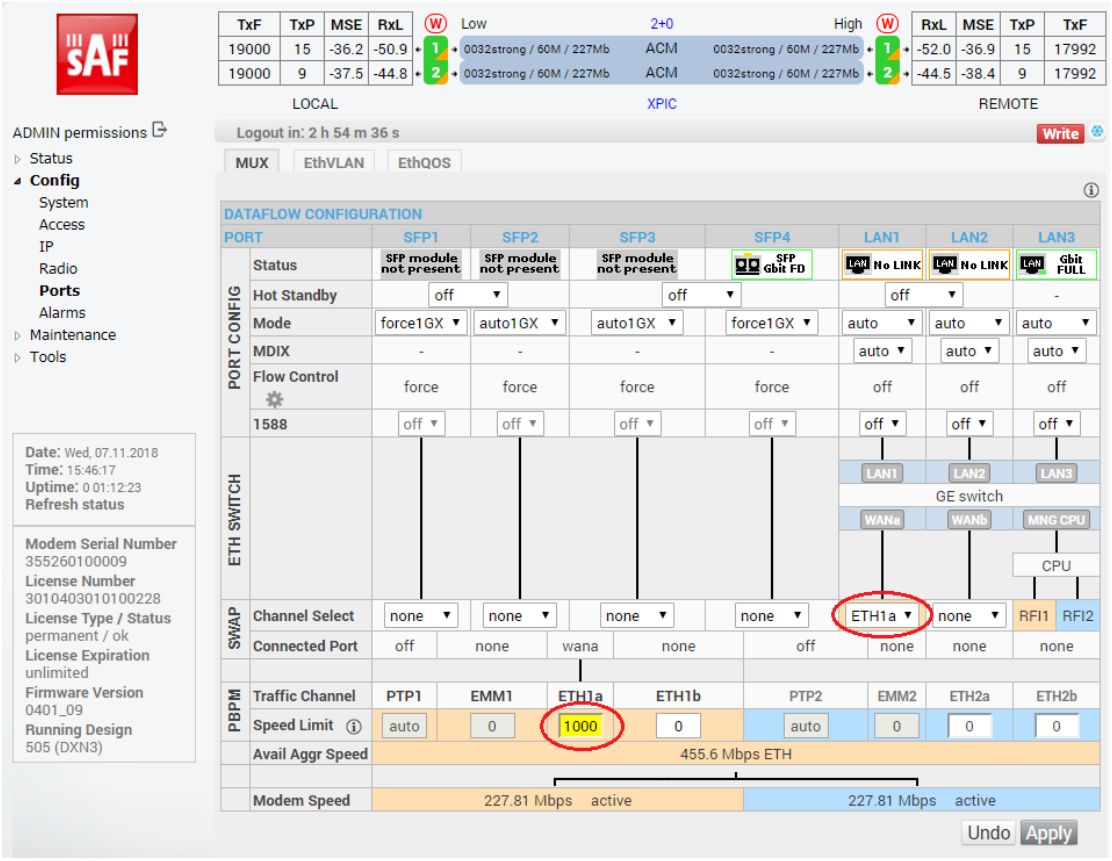


Figure 5.30 *Example of port configuration*

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:

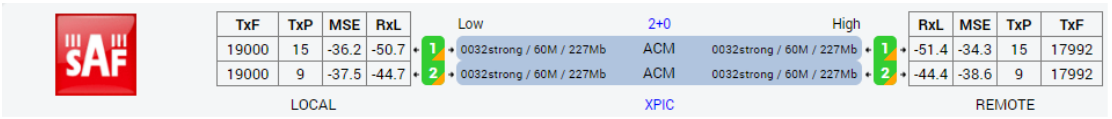


Figure 5.31 *Status of 2+0 XPIC mode*

Example 6 – 1+0 Dual FD mode (Design 505)

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.

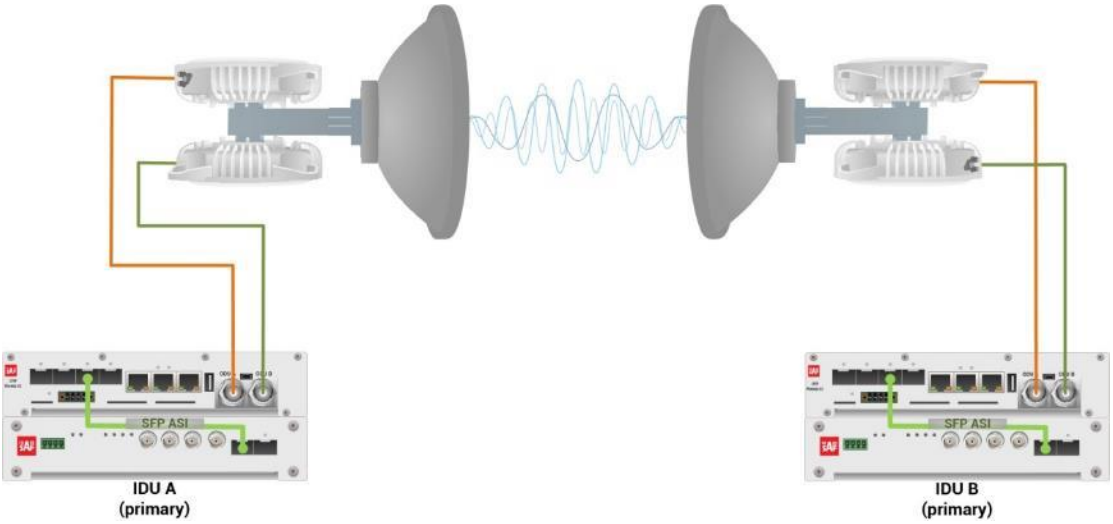


Figure 5.32 *Example of 1+0 Dual FD mode for link capacity increasing*

This 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:

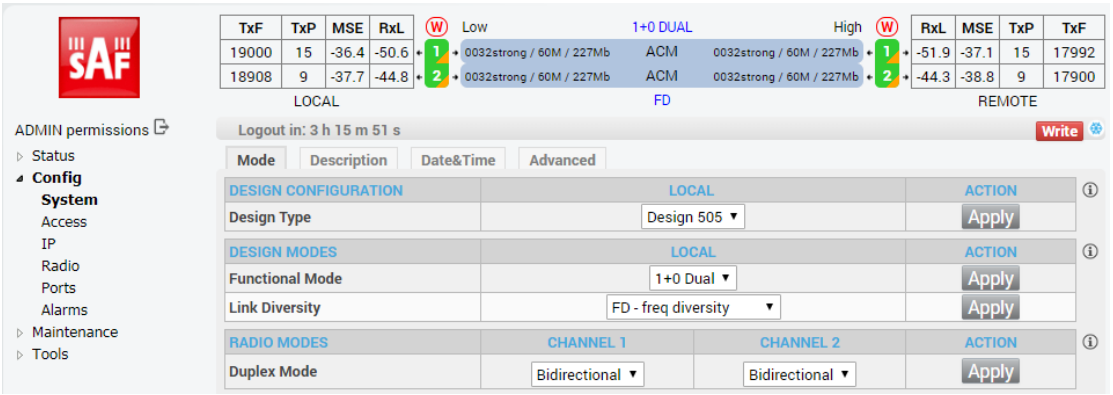


Figure 5.33 *Example of System configuration*

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:

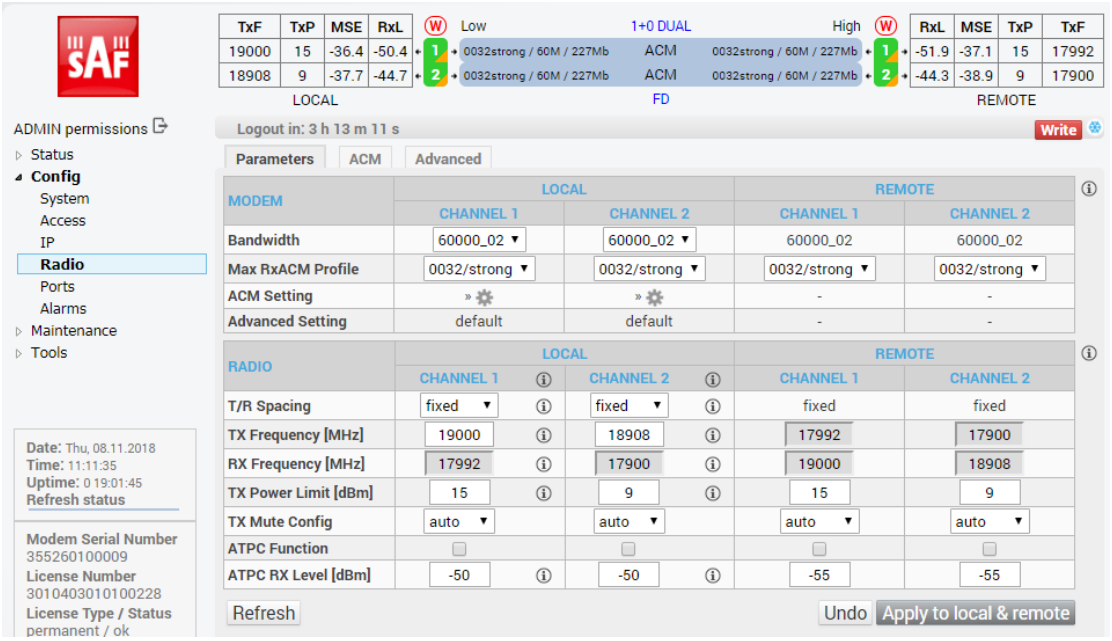


Figure 5.34 *Example of basic Radio parameters configuration*

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.

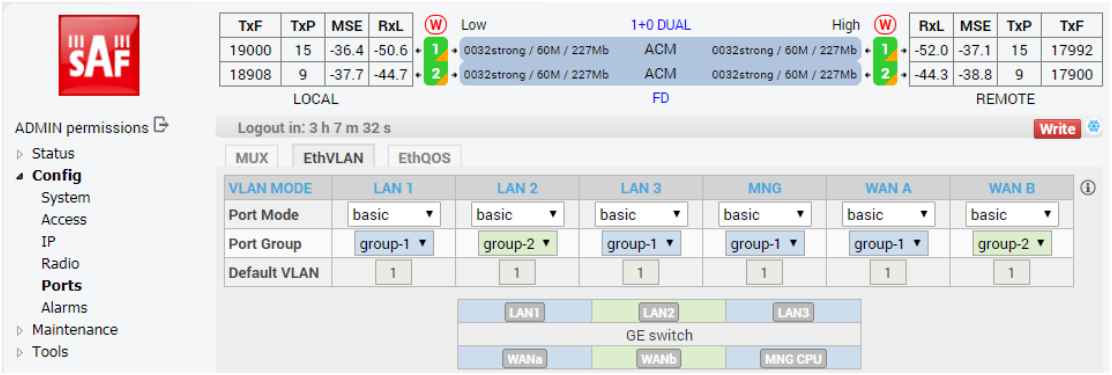


Figure 5.35 *Example of port grouping*

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.

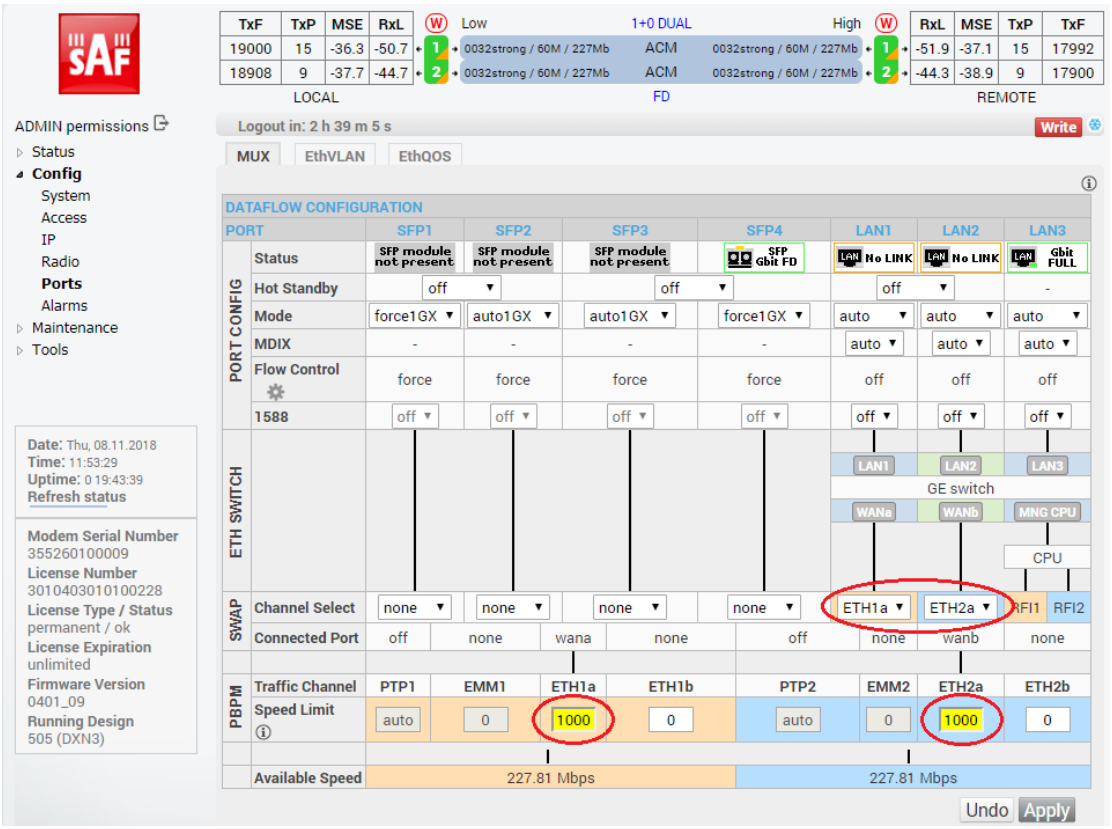


Figure 5.36 *Example of port configuration*

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 Write button.

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

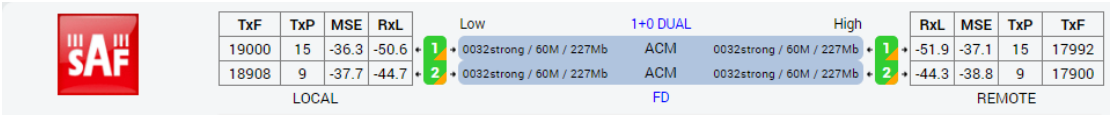


Figure 5.37 *Status of 1+0 Dual FD mode*

Example 7 – 1+0 Dual XPIC mode (Design 505)

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.

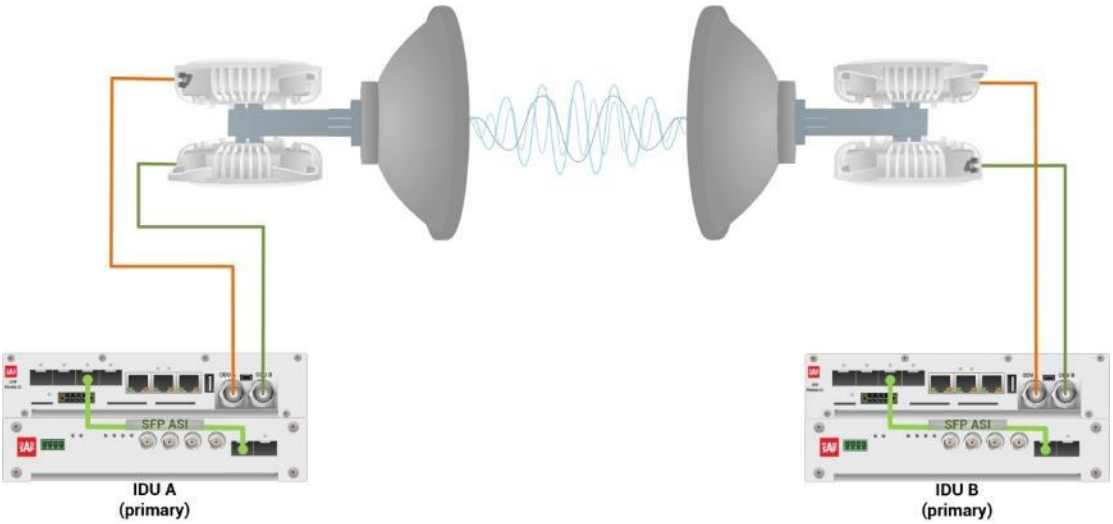


Figure 5.38 *Example of 1+0 Dual XPIC mode for link capacity increasing*

This 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:

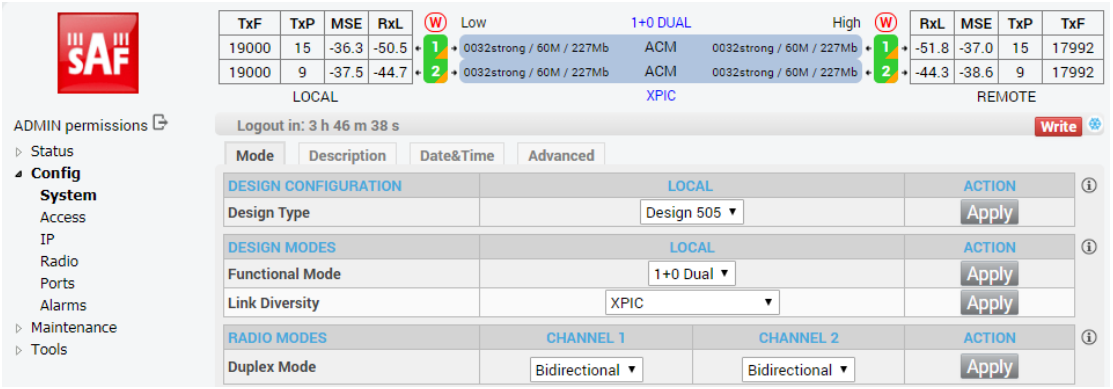


Figure 5.39 *Example of System configuration*

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:

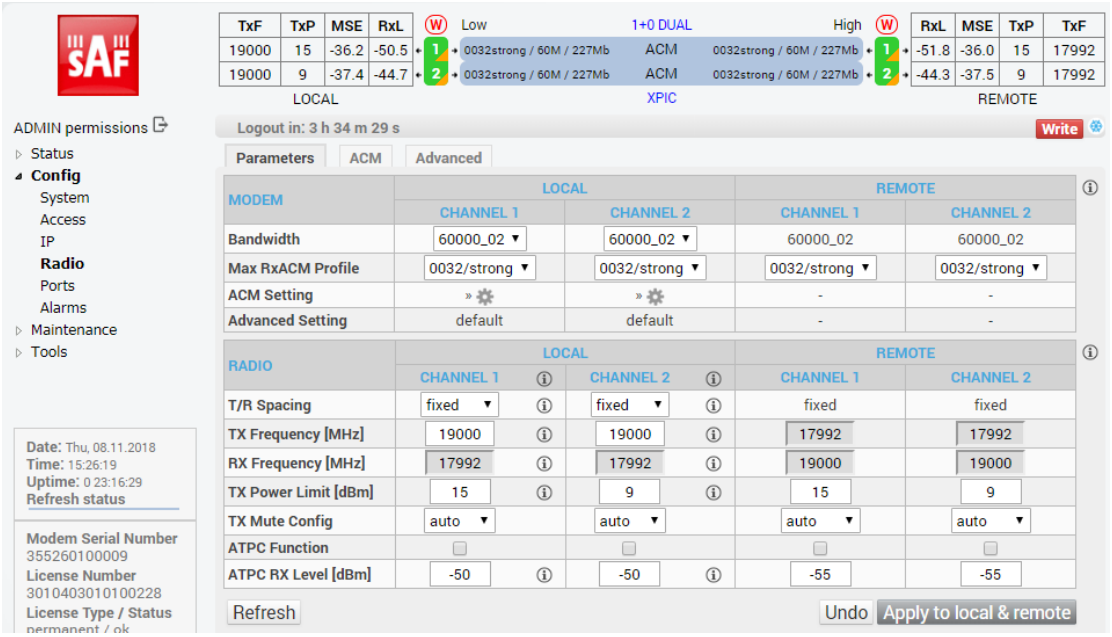


Figure 5.40 *Example of basic Radio parameters configuration*

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.

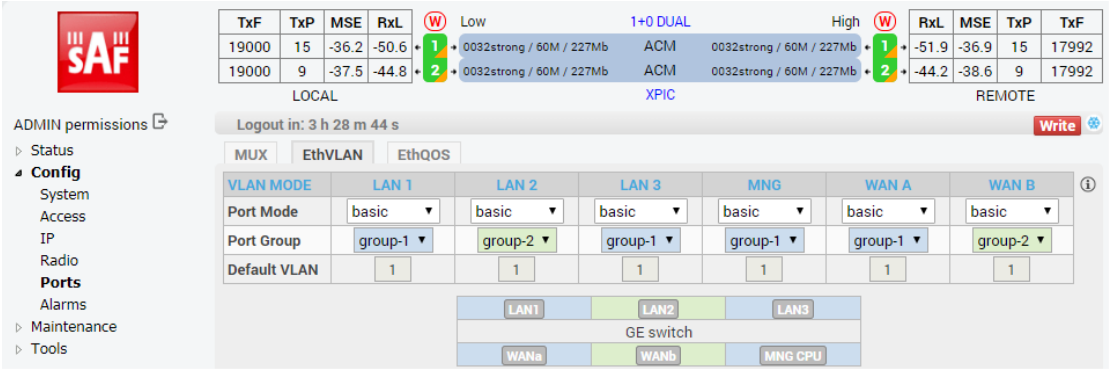


Figure 5.41 *Example of port grouping*

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.

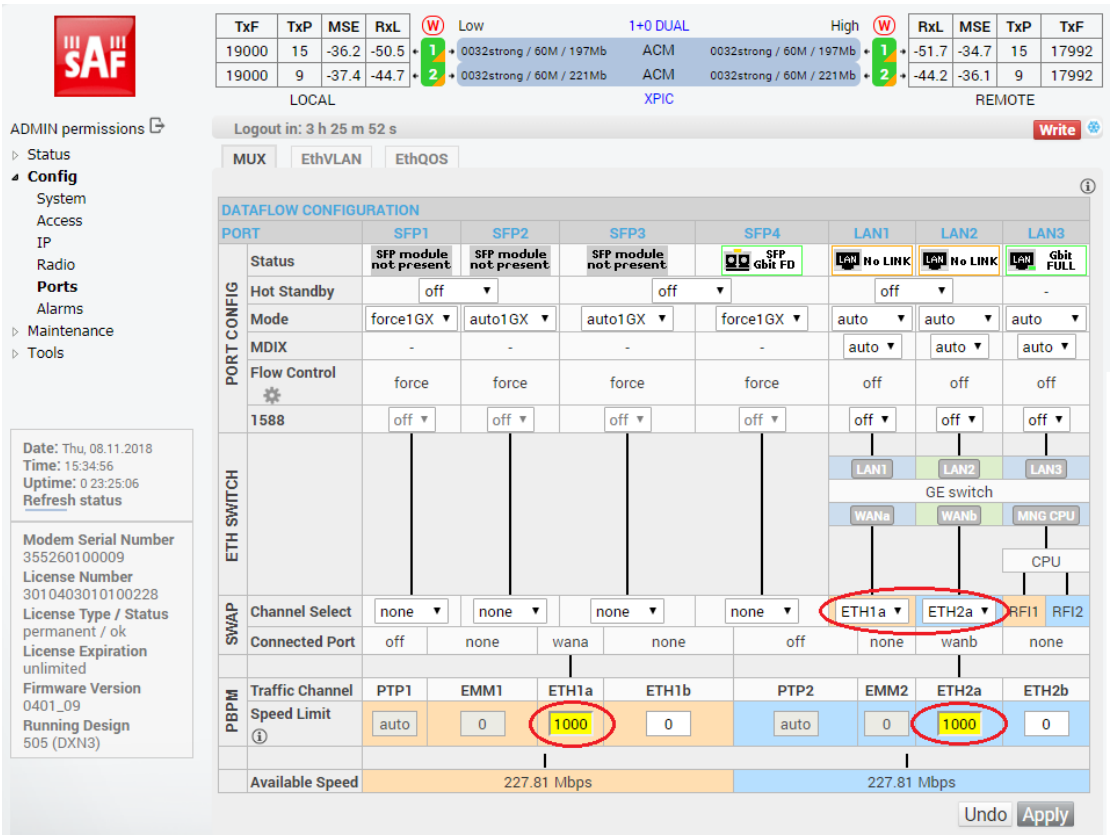


Figure 5.42 *Example of port configuration*

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 Write button.

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

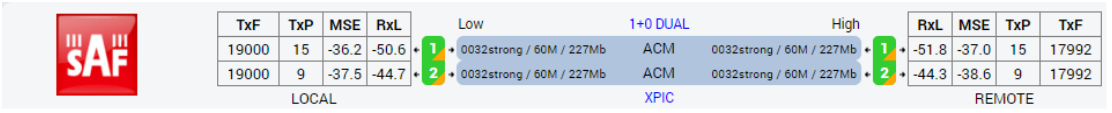


Figure 5.43 *Status of 1+0 Dual XPIC mode*

Example 8 – 1+0 Star mode (Design 505)

The 1+0 Star 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.

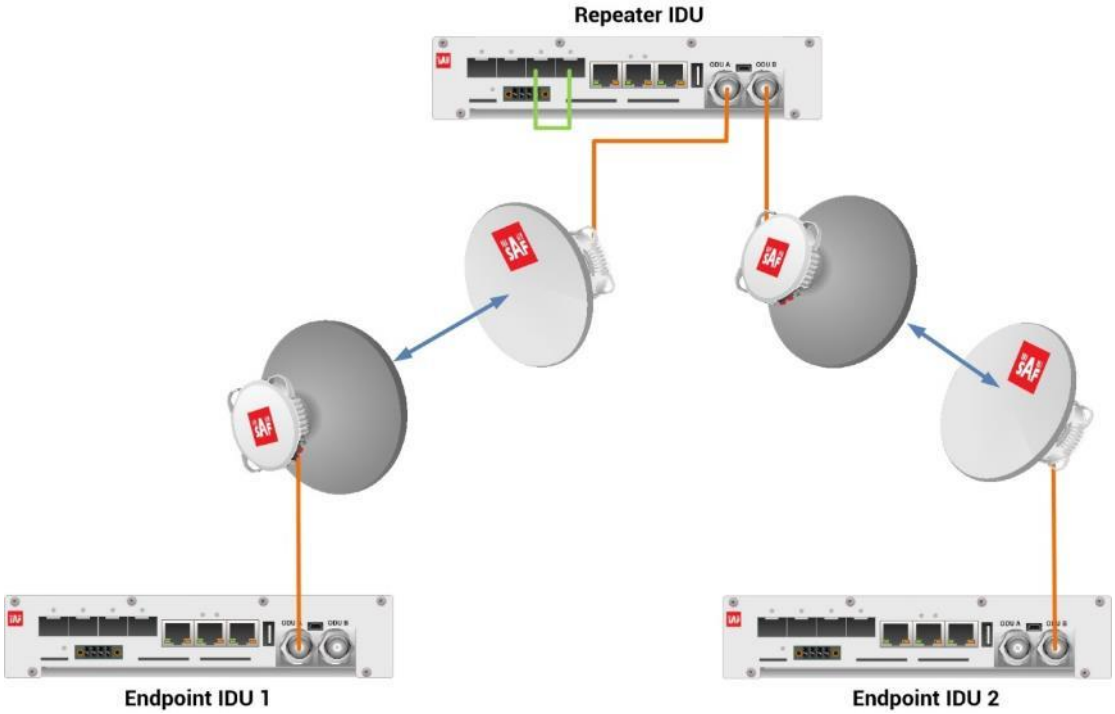


Figure 5.44 *Example of 1+0 Star repeater configuration*

As the 1+0 Star 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 Star repeater configuration does not support ASI/E1 EMM traffic.

This example describes an application where the Design Type 'Design 505', Functional mode '1+0 Star' 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 1024QAM 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 Star mode are following:

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

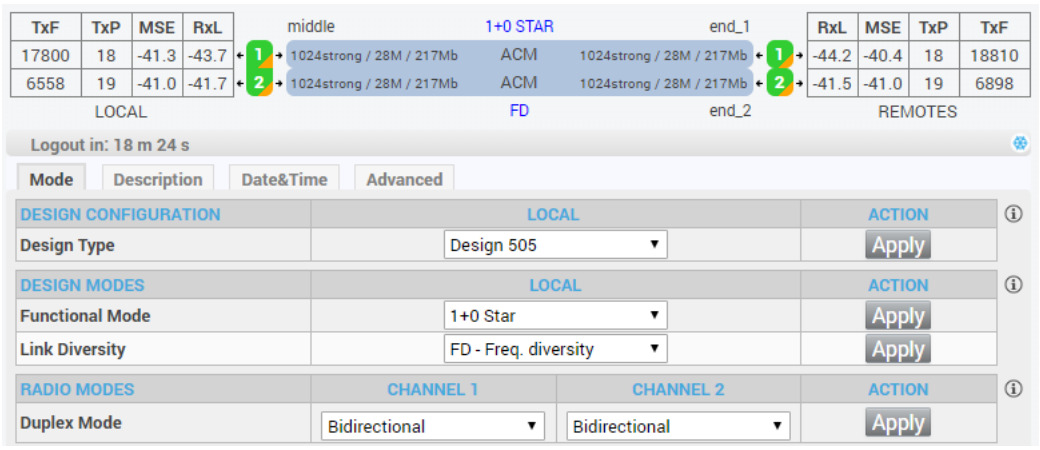


Figure 5.45 *Example of System configuration of Repeater IDU*

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

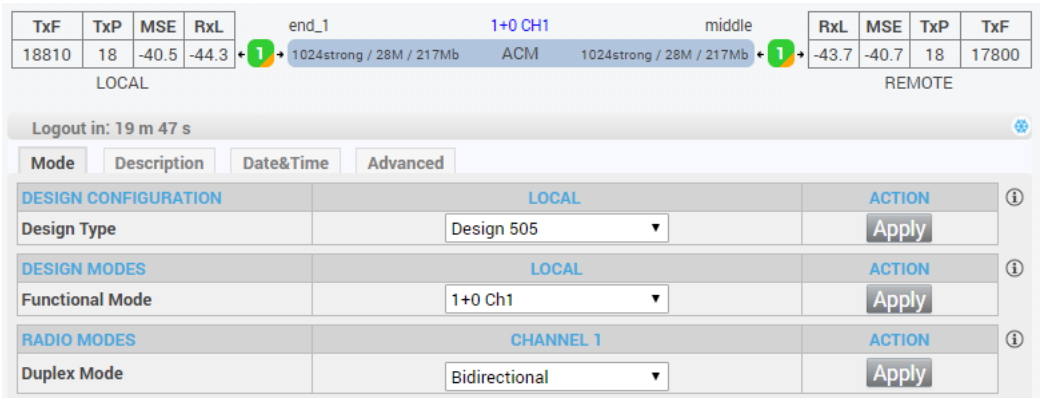


Figure 5.46 *Example of System configuration of Endpoint IDU 1*

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

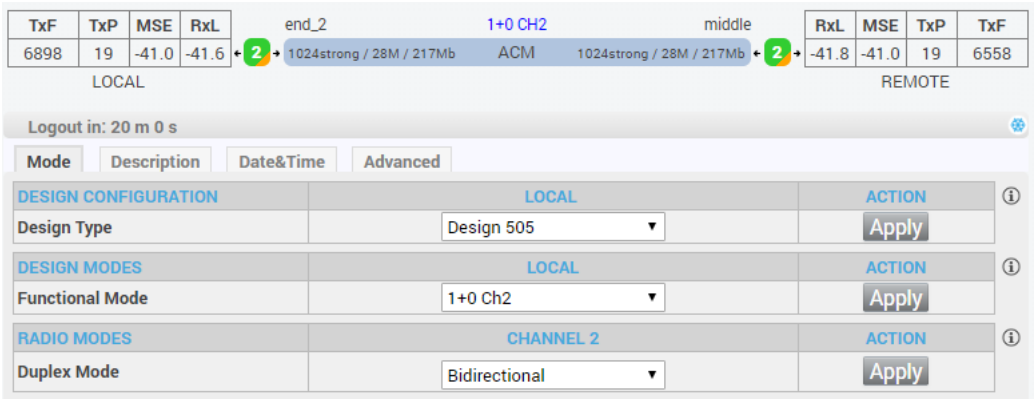


Figure 5.47 *Example of System configuration of Endpoint IDU 2*

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

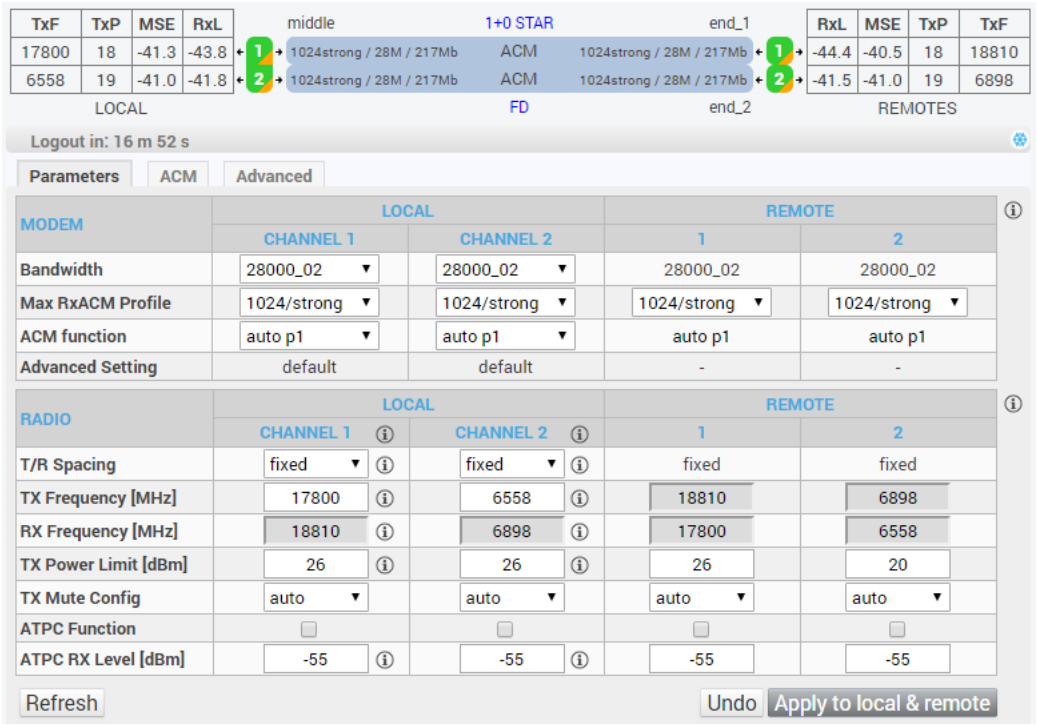


Figure 5.48 *Example of basic Radio parameters configuration of the Repeater IDU*

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

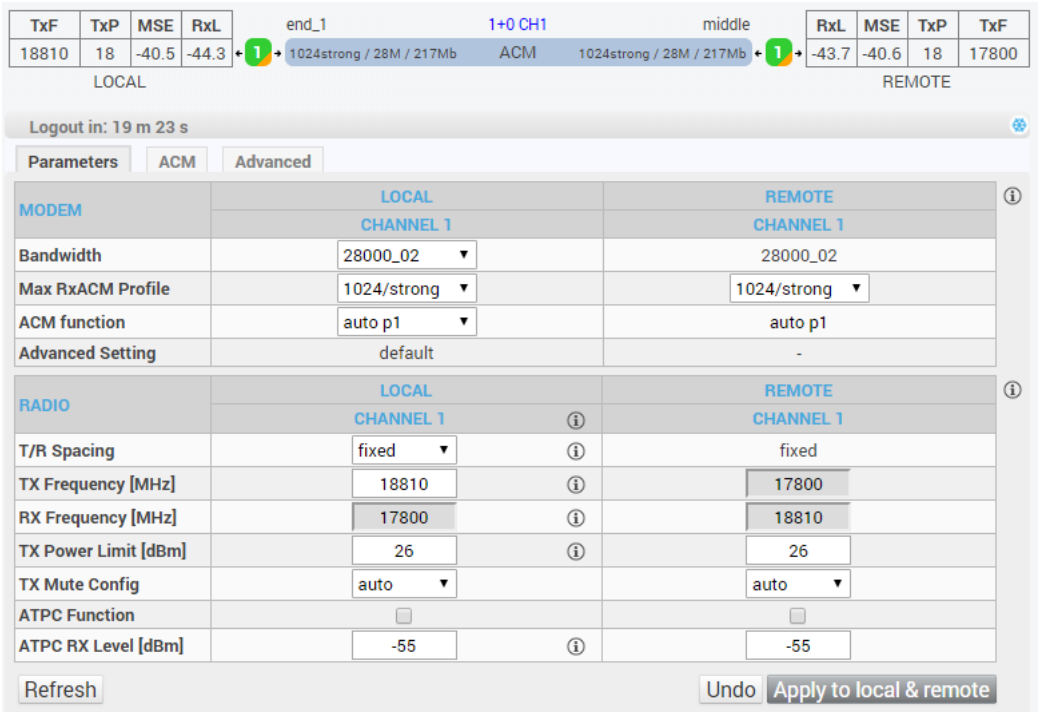


Figure 5.48 *Example of basic Radio parameters configuration of the Endpoint IDU 1*

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

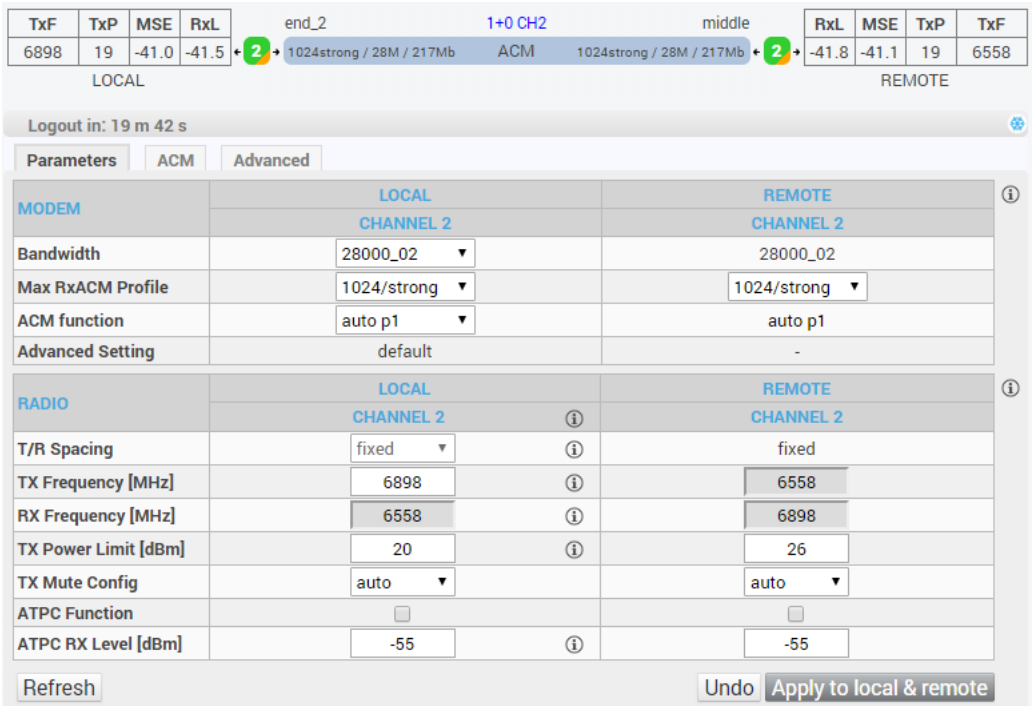


Figure 5.49 *Example of basic Radio parameters configuration of the Endpoint IDU 2*

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*':

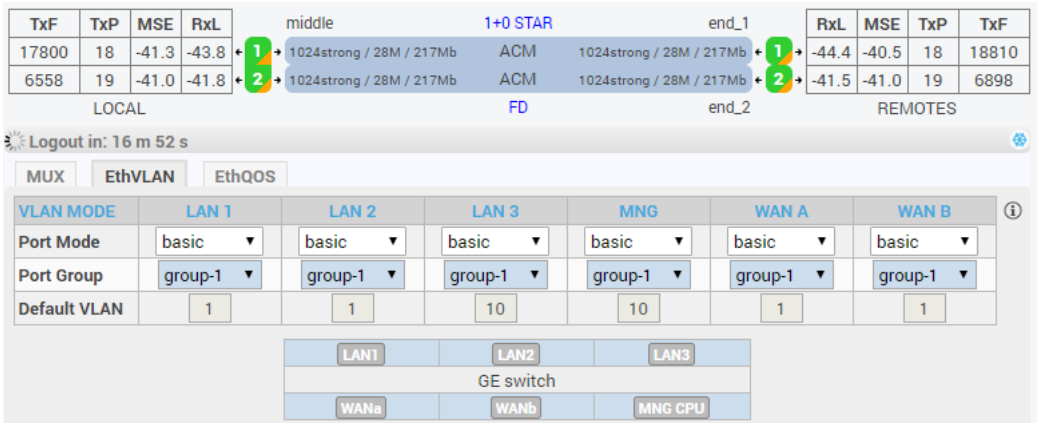


Figure 5.50 *Example of port grouping in the Repeater IDU*



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:

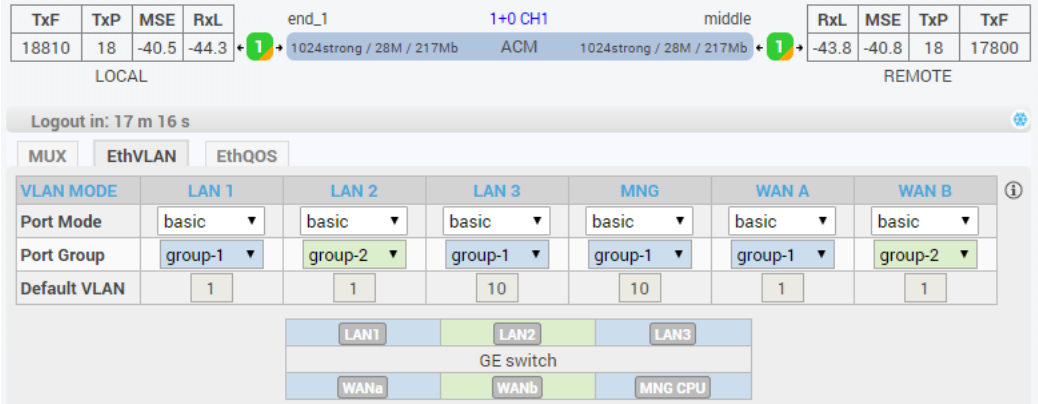


Figure 5.51 *Example of port grouping in the Endpoint IDU 1*

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:

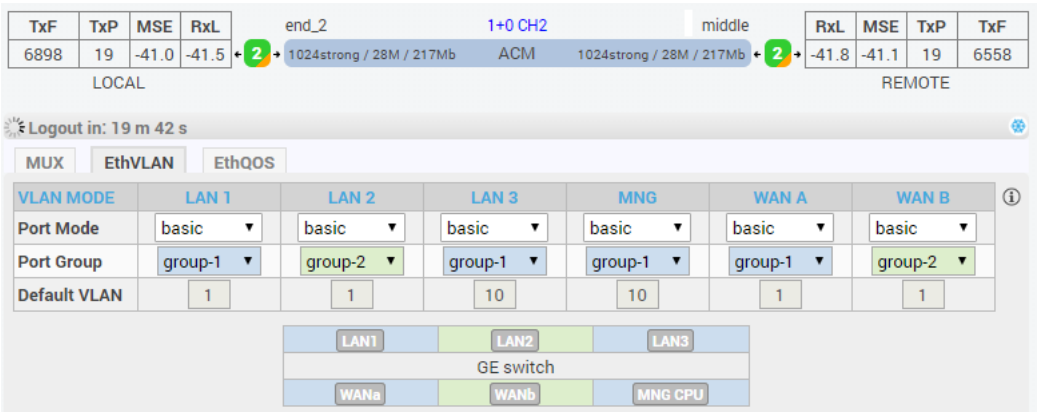


Figure 5.52 *Example of port grouping in the Endpoint IDU 2*

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.

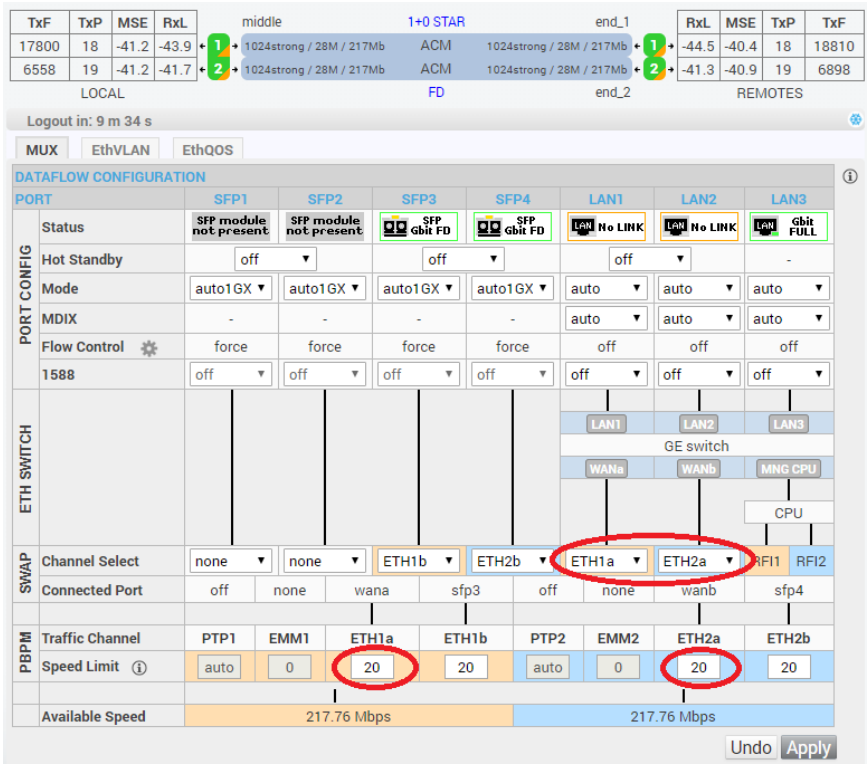


Figure 5.53 *Example of port configuration in Repeater IDU*

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

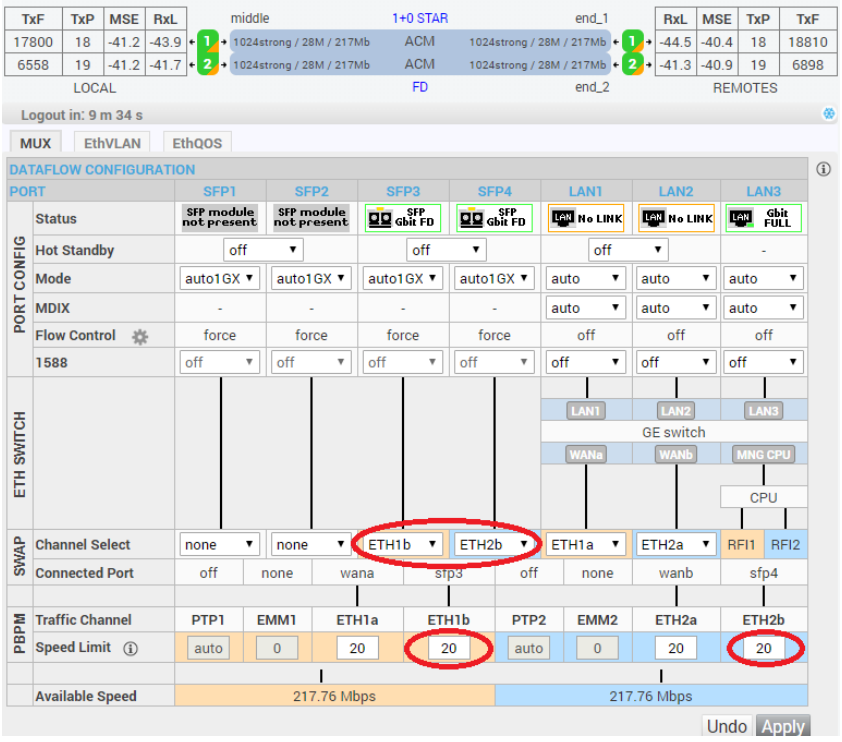


Figure 5.54 *Example of port configuration in Repeater IDU*

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

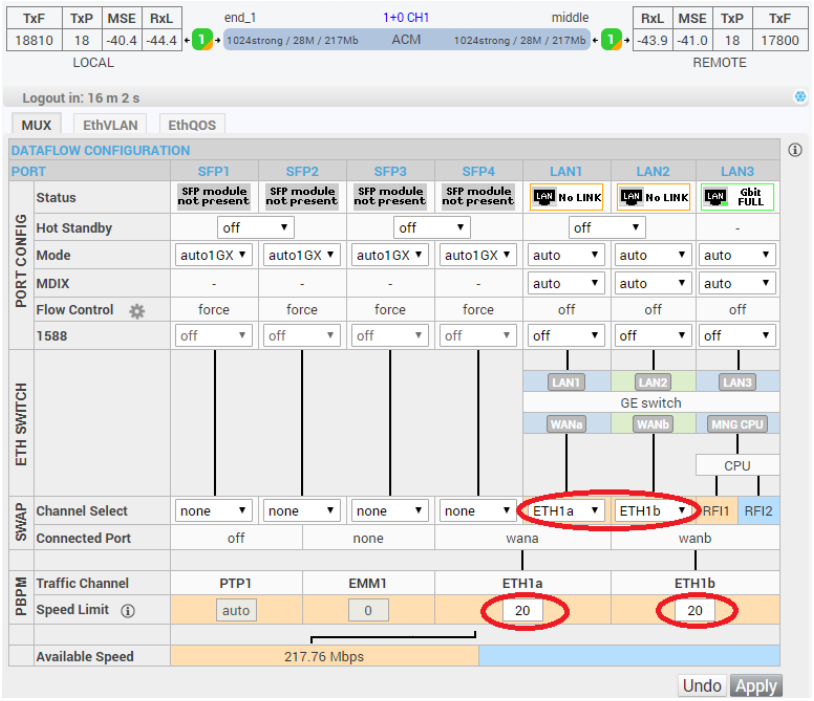


Figure 5.55 *Example of port configuration in Endpoint IDU 1*

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

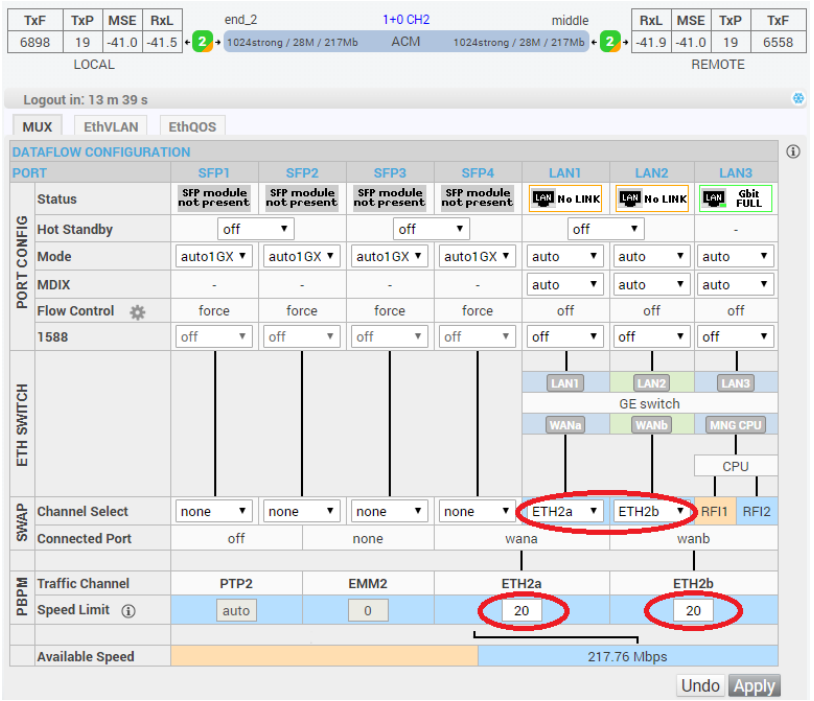


Figure 5.56 *Example of port configuration in Endpoint IDU 2*

13) Save new settings by pressing Write button.

The status of 1+0 Star configuration is displayed in the header of the web GUI of the Repeater IDU:

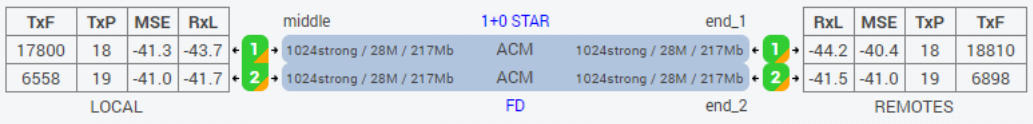


Figure 5.57 *Status of 1+0 Star mode in Repeater IDU*

The status of the Endpoint IDU 1 is displayed in the header of the web GUI:

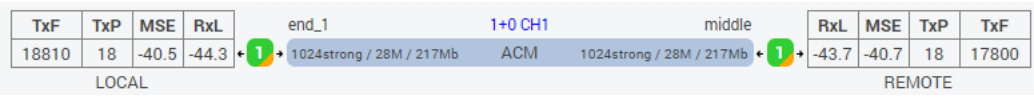


Figure 5.58 *Status of 1+0 Ch1 mode in Endpoint IDU 1*

The status of the Endpoint IDU 2 is displayed in the header of the web GUI:

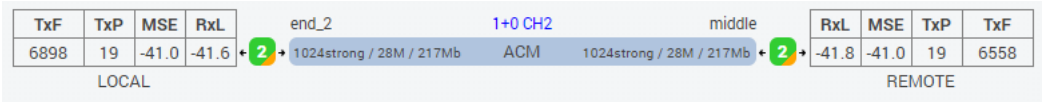


Figure 5.59 *Status of 1+0 Ch2 mode in Endpoint IDU 2*

Example 9 – 1+1 HSB/SD Dual-band configuration (Design 511)

The 1+1 HSB/SD (Hot Standby/Space Diversity) Dual-band frequency protection mode is specific mode which supports data transmission to one direction using one frequency channel/band, and for opposite direction another frequency channel/band. This mode allows even to have frequency channels of each direction in different frequency bands (for example – 7 GHz and 13 GHz frequency bands). Each frequency channel works in Simplex mode and is protected.

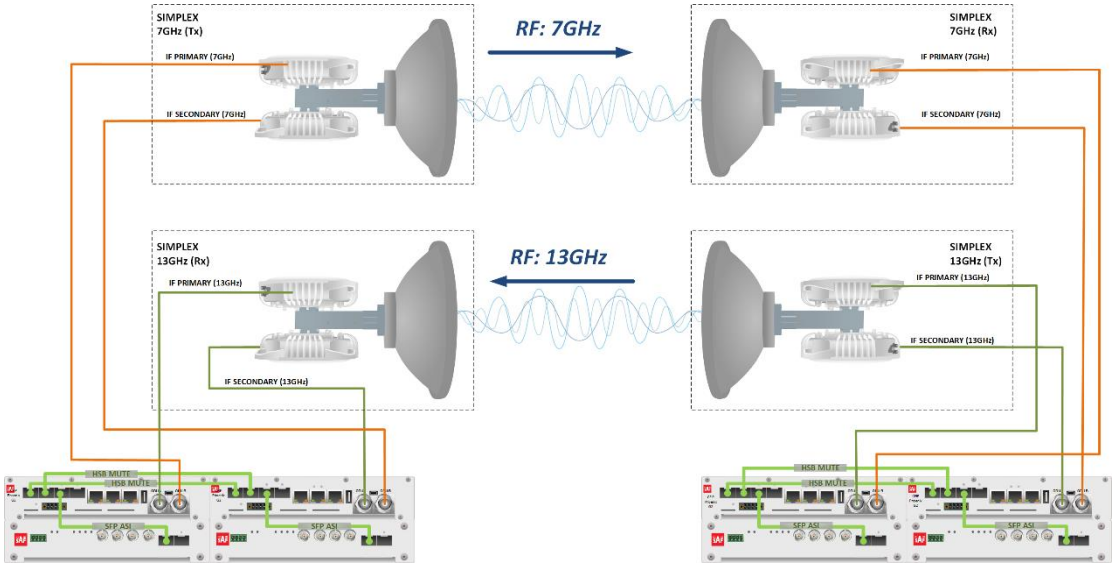


Figure 5.60 *Example of 1+1 HSB/SD Dual-band frequency protection*

In above mentioned scheme the ODUs and couplers can be substituted with IRFUs and IBUs combination if required by customer.

This example describes an application where the Design Type 'Design 511', Functional mode 'Split 2+2' and Link diversity 'HSB/SD – hot standby' are selected on both link sides. One frequency channel works on Tx-only mode, but the second frequency channel woks in Rx-only mode. The modulation is 32QAM in BW 60 MHz and the appropriate maximal data speed is about 227 Mbps per channel. ASI traffic is passed through the link. **This scheme requires four Phoenix G2 IDUs and eight ODUs per link.**



Both IDUs in each side of the link are interconnected with 2 optical cables on ports SFP1 and SFP2. 2.5 GB SFP modules must be used for this interconnection. SFP3 port is used for the IDU interconnection with ASI EMM module.

Configuration steps for 1+1 HSB/SD Dual-band frequency protection are following:

1) **IDU A (primary)**:
   a) In web GUI '*Config->System->Mode*' choose design type 'Design 511', Functional mode 'Split 2+2', Link Protection Diversity 'HSB/SD – Hot standby', Link Aggregation Diversity 'FD'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed primary'. As the link will use different frequency channels/bands for each direction then the Duplex Mode must be configured so that one of channels is in Tx mode, but the second channel is in Rx mode. In the example on Side A the Channel 1 is 'Tx-only' mode, and the Channel 2 is in 'Rx-only' mode.

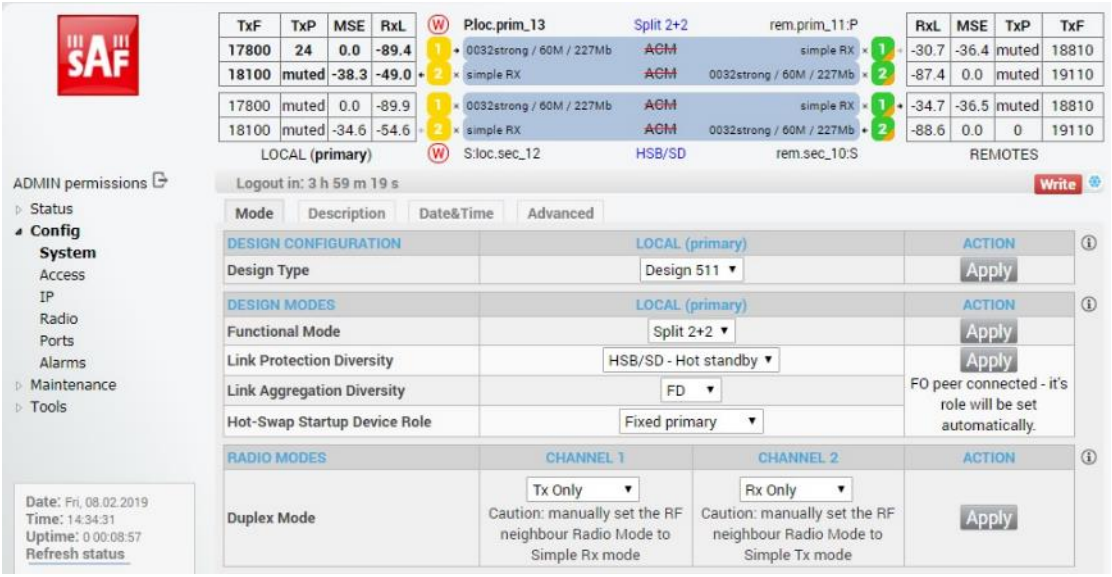


Figure 5.61 *Example of Side A Primary IDU system configuration*

   b) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters. Frequency channel/band must be different for Channel 1 and Channel 2, and correspond to 'Tx-only' and 'Rx-only' Duplex mode settings in '*Config->System->Mode*' page.

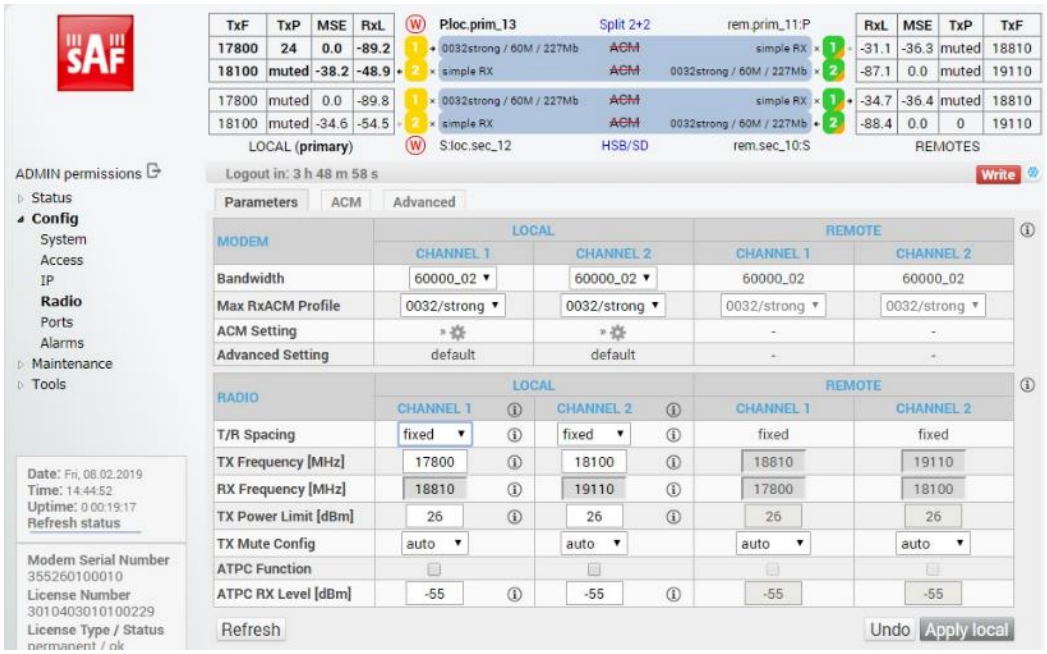


Figure 5.62 *Example of Side A Primary IDU radio configuration*

c) The ACM (Adaptive Coding and Modulation) must be disabled if Duplex modes "Tx only" and "Rx only" are used. In order to disable it, navigate to '*Config →System →Mode*' in the web GUI and set ACM Control to "Manual". This setting disables the ACM



Figure 5.63 *Example of Side A Primary IDU ACM configuration*

d) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU



Figure 5.64 *Example of Side A Primary IDU IP configuration*

e) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote. This will enable management access to other IDUs in the link via NAT.

With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible: 2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the local secondary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:2443

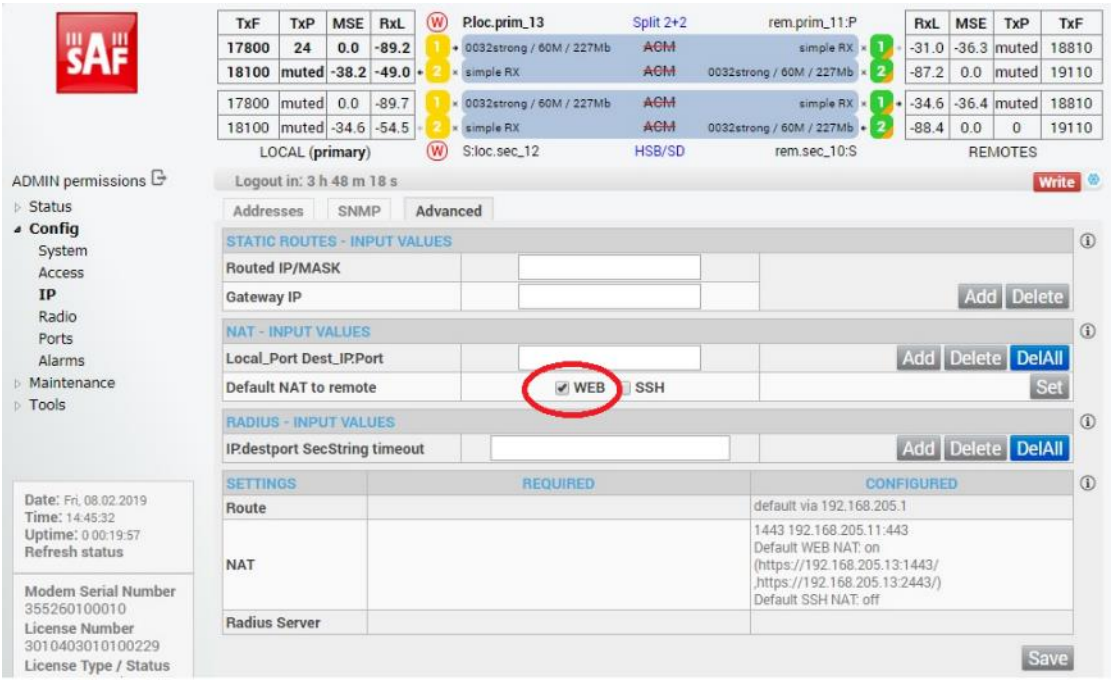


Figure 5.65 *Example of Side A Primary IDU IP NAT configuration*

f) Port group configuration must be done according to customer requirements. In this configuration when the Duplex modes “Tx-only” and “Rx-only” are used the remote management access via WAN port is not supported. That is why NAT configuration is required. In this example LAN1 port is used for the traffic, so LAN1 and WANa are grouped in the same group (Group 1). LAN2 and WANb are grouped in Group 2 and will not be used or can be intended for any other independent and separated user data traffic. LAN3 and MNG ports are grouped in Group3 for management access only via LAN3 port. Port grouping configuration is available in web GUI ‘*Config->Ports->EthVLAN*’ section

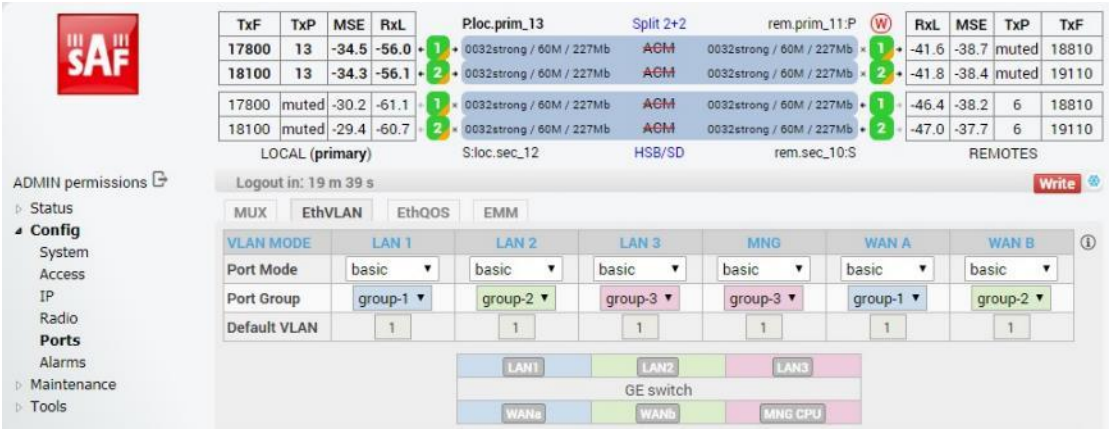


Figure 5.66 *Example of Side A Primary IDU port grouping*

g) In web GUI ‘*Config->Ports->MUX*’ specify Data channel and port speed for WAN (radio direction) port and SFP ports. In the example WANa port is connected to

high priority data channel ‘ETH1a’ and is set on full speed limit 1000 Mbps. The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary) are interconnected successfully, the SFP1 and SFP2 ports must be automatically indicated as connected in Mode ‘force2G5’

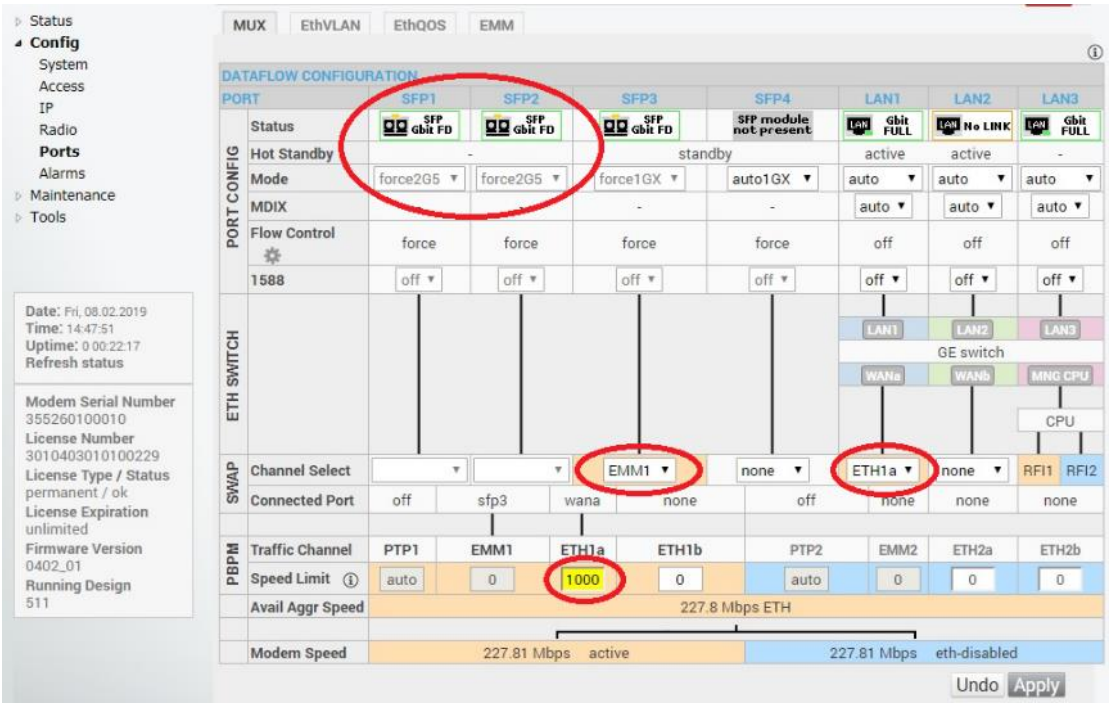


Figure 5.67 *Example of Side A Primary IDU port configuration*

h) In web GUI ‘*Config->Ports->EMM*’ configure the ASI traffic according to customer requirements. In the example one ASI traffic stream via ASI1 port is sent from side A to side B. In this case the ASI EMM configuration will be following: ‘EMM Enable’ and ‘EMM Protection Failover’ check-boxes must be checked. Also ASI EMM module ‘Enable’ check-box must be checked and ‘Mode’ set as ”Rx”

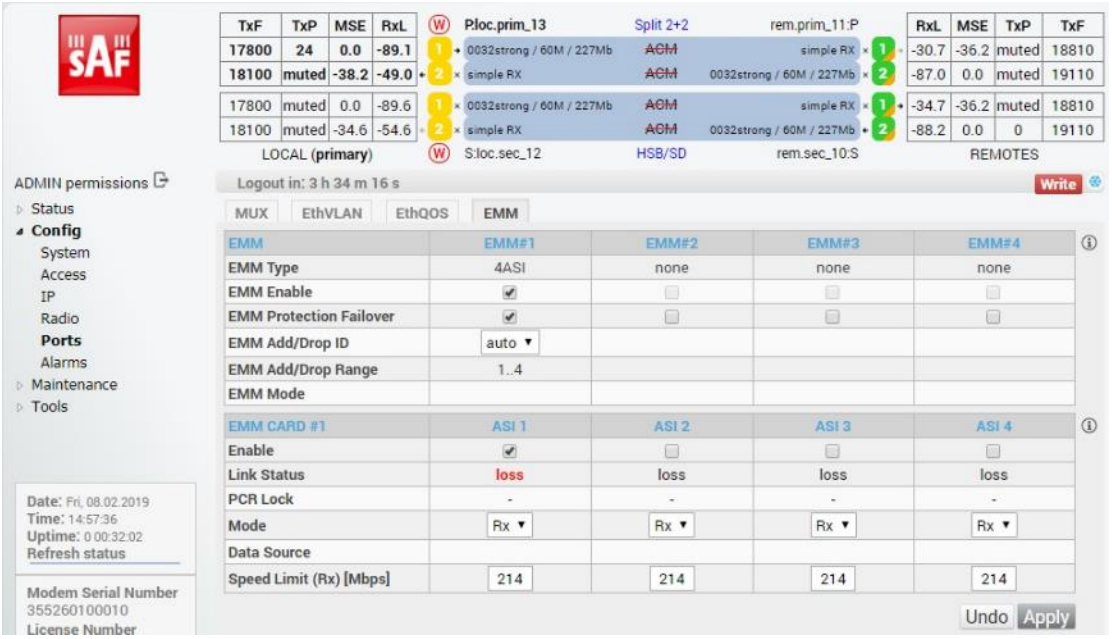


Figure 5.68 *Example of Side A Primary IDU EMM configuration*

i) In web GUI '*Config →Alarms →General*' configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label). In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

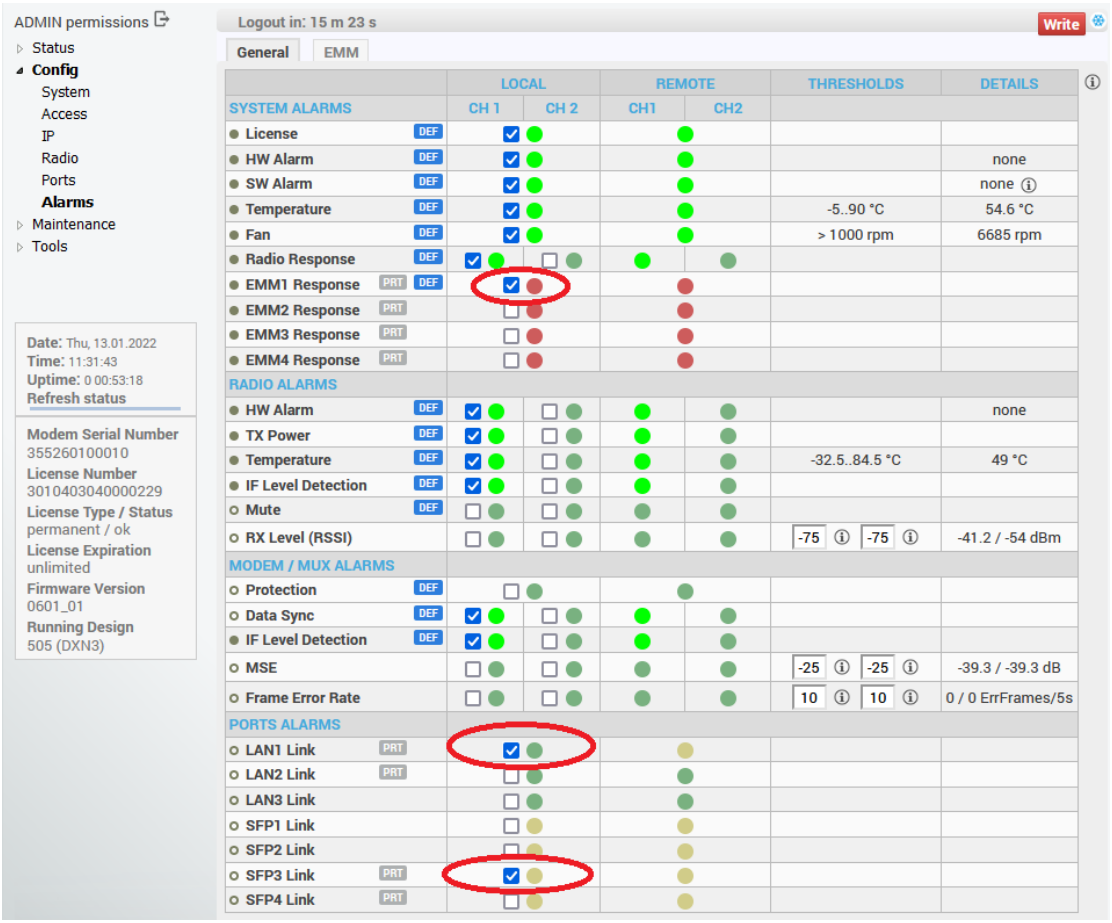


Figure 5.69a *Example of Side A Primary IDU alarm configuration*

j) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

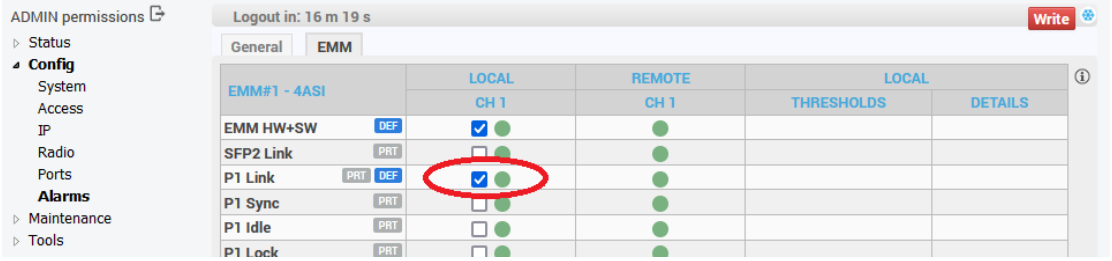


Figure 5.69b *Example of Side A Primary IDU alarm configuration*

k) Save new settings by pressing Write button.

2) **IDU A (secondary)**:

a) In web GUI '*Config->System->Mode*' choose design type 'Design 511', Functional mode 'Split 2+2', Link Protection Diversity 'HSB/SD – Hot standby', Link Aggregation Diversity 'FD'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed secondary'. As the link will use different

frequency channels/bands for each direction then the Duplex Mode must be configured so that one of channels is in Tx mode, but the second channel is in Rx mode. In the example on Side A the Channel 1 is 'Tx-only' mode, and the Channel 2 is in 'Rx-only' mode

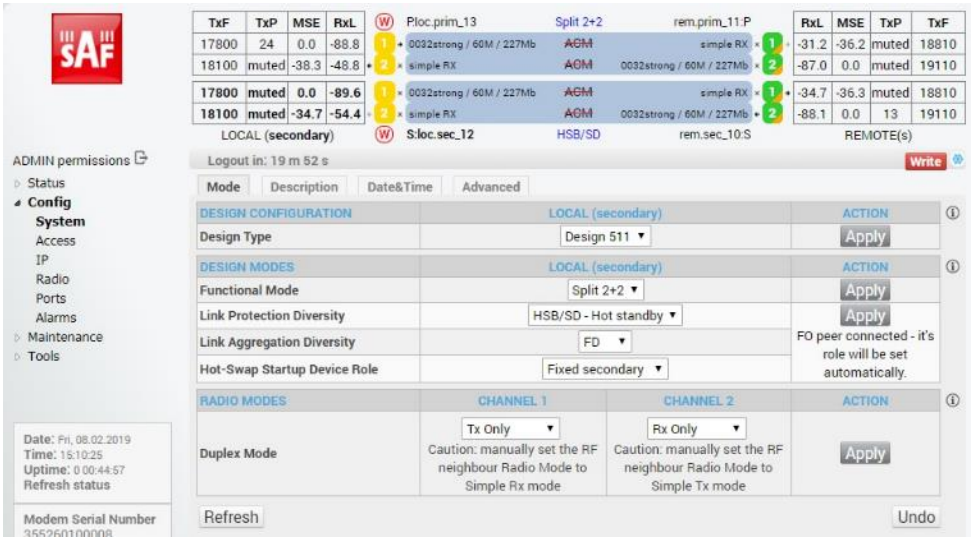


Figure 5.70 *Example of Side A Secondary IDU system configuration*

b) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters. Frequency channel/band must be different for Channel 1 and Channel 2, and correspond to 'Tx-only' and 'Rx-only' Duplex mode settings in '*Config->System->Mode*' page.

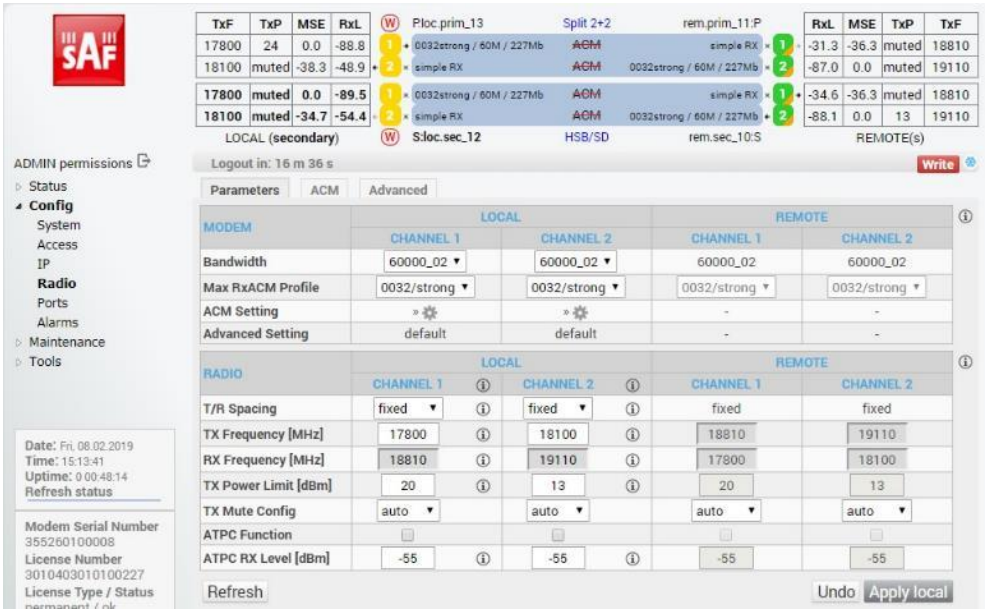


Figure 5.71 *Example of Side A Secondary IDU radio configuration*

c) The ACM (Adaptive Coding and Modulation) must be disabled if Duplex modes "Tx only" and "Rx only" are used. In order to disable it, navigate to '*Config →System →Mode*' in the web GUI and set ACM Control to "Manual". This setting disables the ACM



Figure 5.72 *Example of Side A Secondary IDU ACM configuration*

d) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU



Figure 5.73 *Example of Side A Secondary IDU IP configuration*

e) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote. This will enable management access to other IDUs in the link via NAT.



With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible: 2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the local secondary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:2443

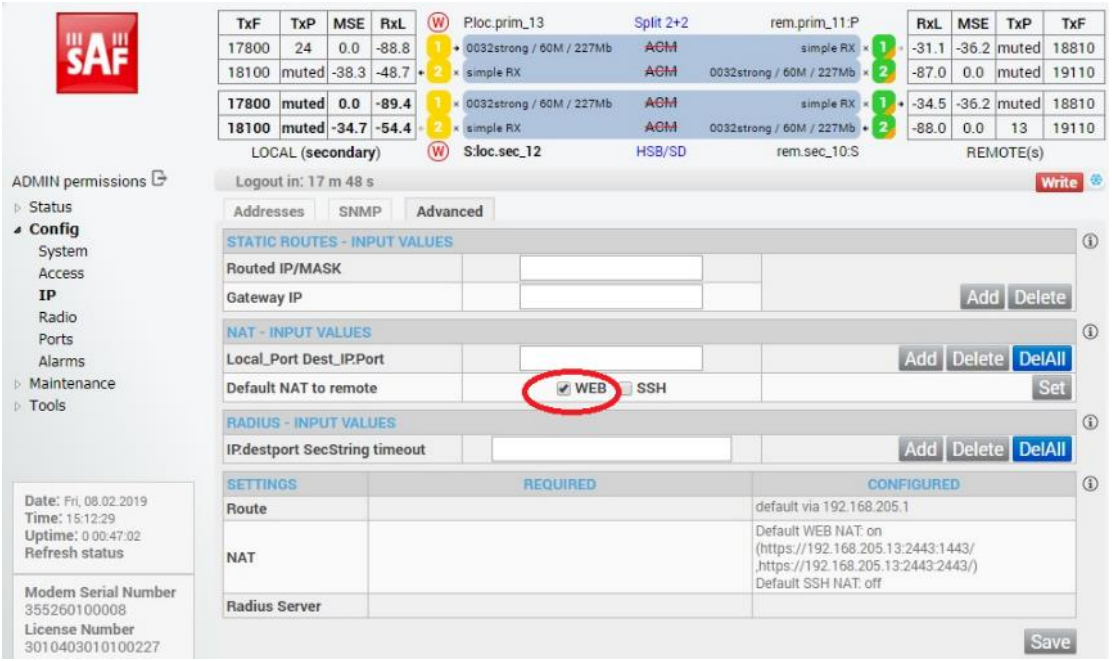


Figure 5.74 *Example of Side A Secondary IDU IP NAT configuration*

f) Port group configuration must be done according to customer requirements. In this configuration when the Duplex modes “Tx-only” and “Rx-only” are used the remote management access via WAN port is not supported. That is why NAT configuration is required. In this example LAN1 port is used for the traffic, so LAN1 and WANa are grouped in the same group (Group 1). LAN2 and WANb are grouped in Group 2 and will not be used or can be intended for any other independent and separated user data traffic. LAN3 and MNG ports are grouped in Group3 for management access only via LAN3 port. Port grouping configuration is available in web GUI ‘*Config->Ports->EthVLAN*’ section

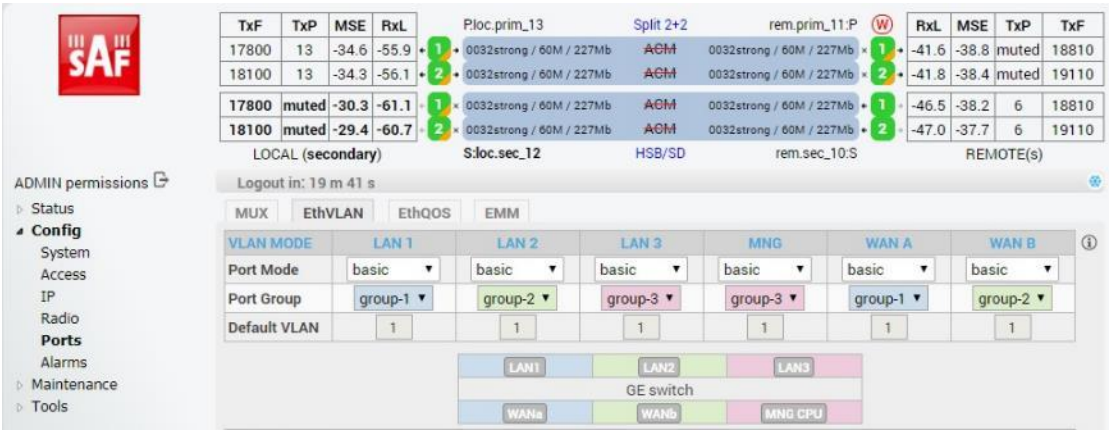


Figure 5.75 *Example of Side A Secondary IDU port grouping*

g) In web GUI ‘*Config->Ports->MUX*’ specify Data channel and port speed for WAN (radio direction) port and SFP ports. In the example WANa port is connected to high priority data channel ‘ETH1a’ and is set on full speed limit 1000 Mbps. The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary) are interconnected successfully, the SFP1 and SFP2 ports must be automatically indicated as connected in Mode ‘force2G5’

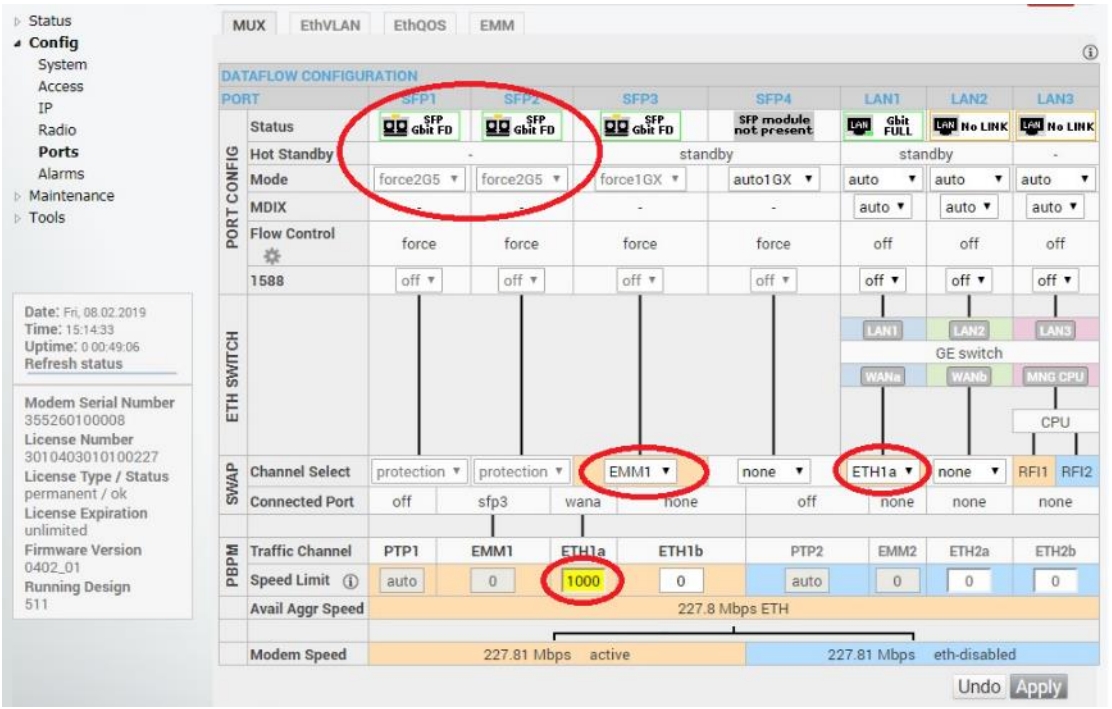


Figure 5.76 *Example of Side A Secondary IDU port configuration*

h) In web GUI '*Config->Ports->EMM*' configure the ASI traffic according to customer requirements. In the example one ASI traffic stream via ASI1 port is sent from side A to side B. In this case the ASI EMM configuration will be following: 'EMM Enable' and 'EMM Protection Failover' check-boxes must be checked. Also ASI EMM module 'Enable' check-box must be checked and 'Mode' set as "Rx"

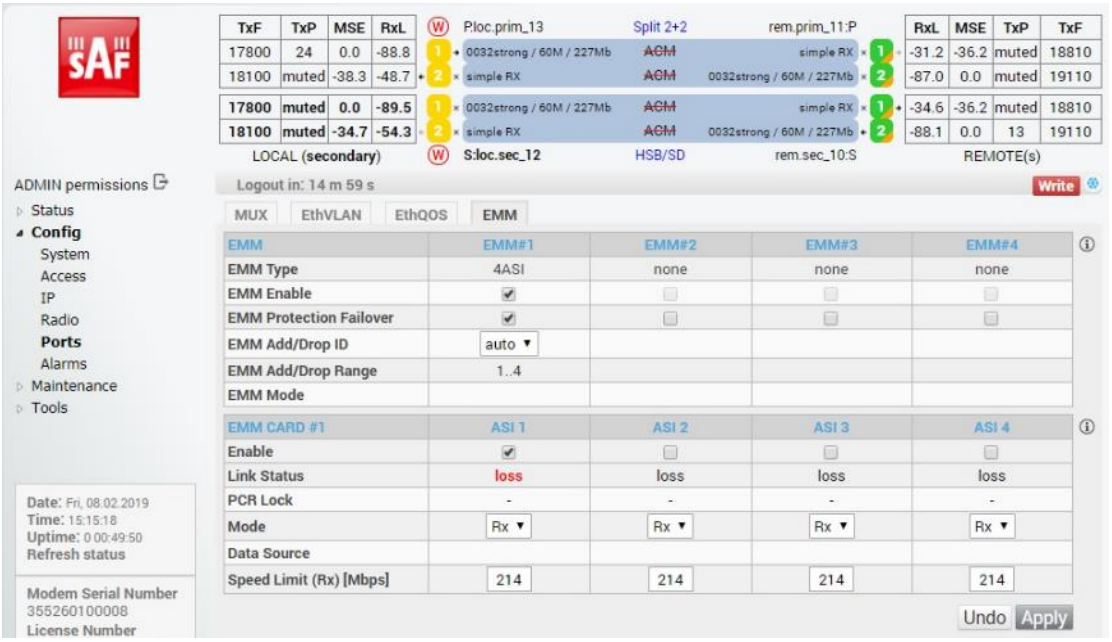


Figure 5.77 *Example of Side A Secondary IDU EMM configuration*

i) In web GUI '*Config →Alarms →General*' configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label). In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

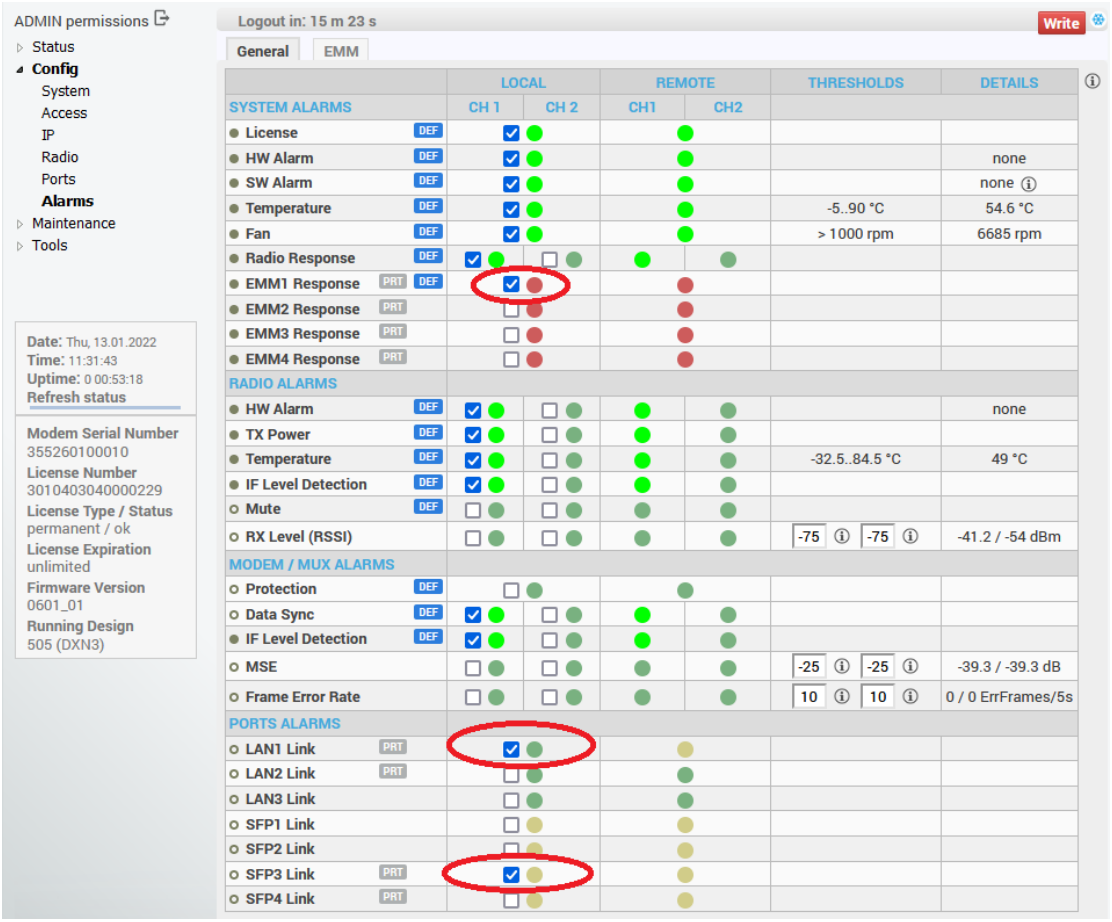


Figure 5.78a *Example of Side A Secondary IDU alarm configuration*

j) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

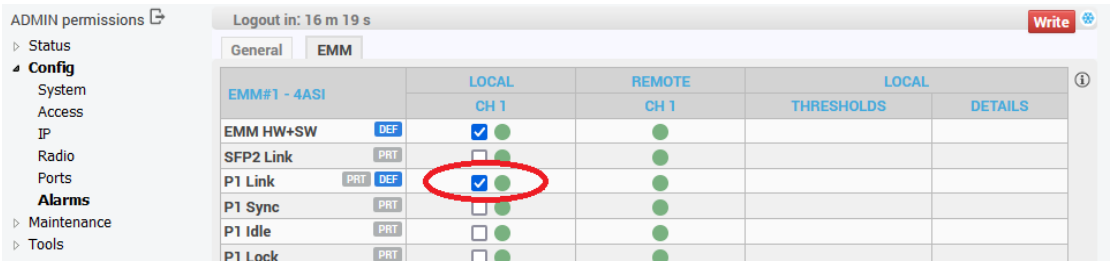


Figure 5.78b *Example of Side A Secondary IDU alarm configuration*

k) Save new settings by pressing Write button.

3) **IDU B (primary)**:

a) In web GUI '*Config->System->Mode*' choose design type 'Design 511', Functional mode 'Split 2+2', Link Protection Diversity 'HSB/SD – Hot standby', Link Aggregation Diversity 'FD'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed primary'. As the link will use different frequency channels/bands for each direction then the Duplex Mode must be configured so that one of channels is in Tx mode, but the second channel is in Rx mode. In the example on Side B the Channel 1 is 'Rx-only' mode, and the Channel 2 is in 'Tx-only' mode

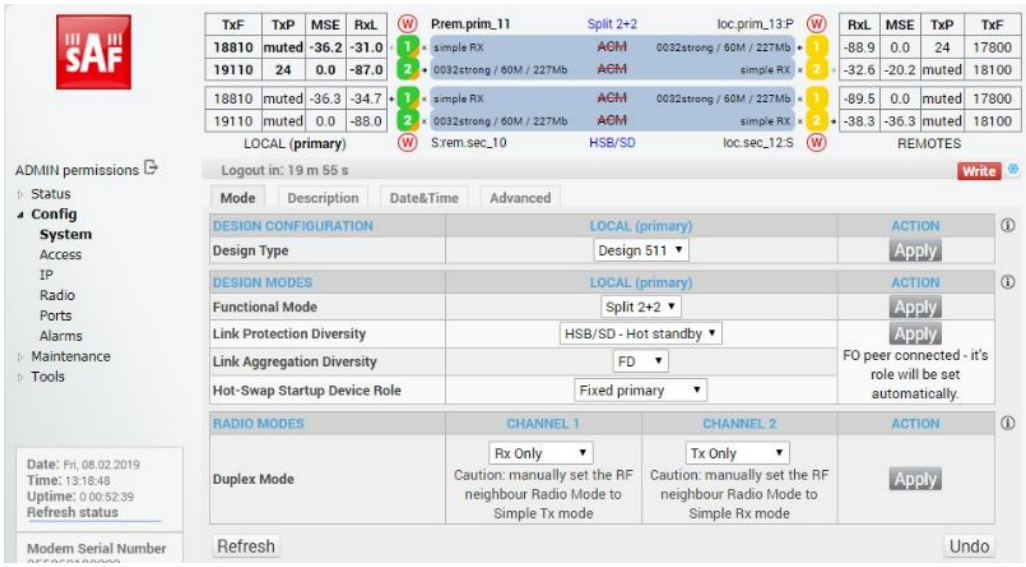


Figure 5.79 *Example of Side B Primary IDU system configuration*

b) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters. Frequency channel/band must be different for Channel 1 and Channel 2, and correspond to 'Tx-only' and 'Rx-only' Duplex mode settings in '[Config->System->Mode](#)' page.

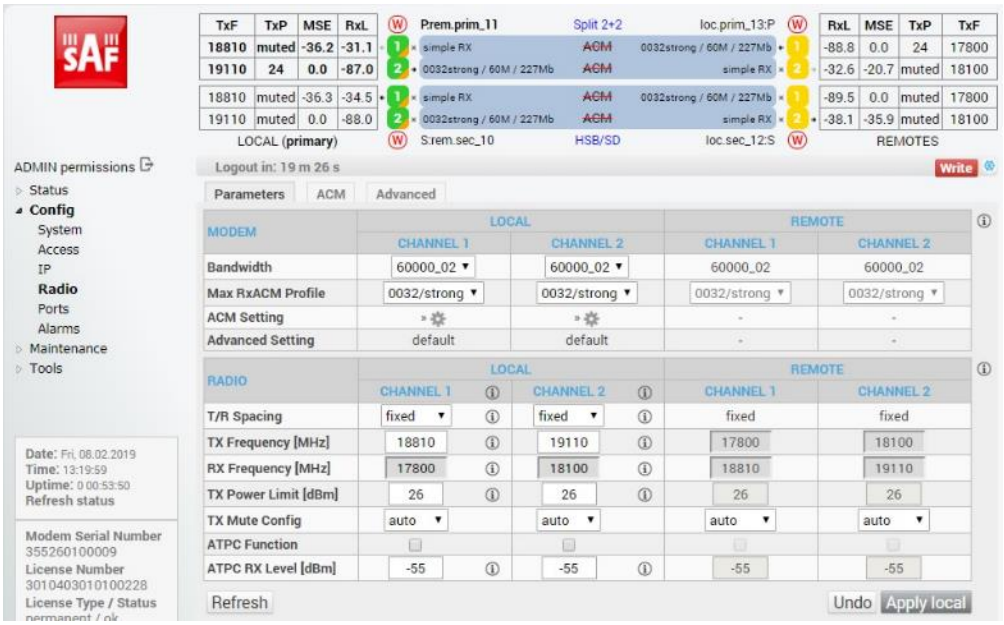


Figure 5.80 *Example of Side B Primary IDU radio configuration*

c) The ACM (Adaptive Coding and Modulation) must be disabled if Duplex modes "Tx only" and "Rx only" are used. In order to disable it, navigate to '*Config →System →Mode*' in the web GUI and set ACM Control to "Manual". This setting disables the ACM



Figure 5.81 *Example of Side B Primary IDU ACM configuration*

d) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU



Figure 5.82 *Example of Side B Primary IDU IP configuration*

e) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote. This will enable management access to other IDUs in the link via NAT.



With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible: 2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the remote primary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:1443

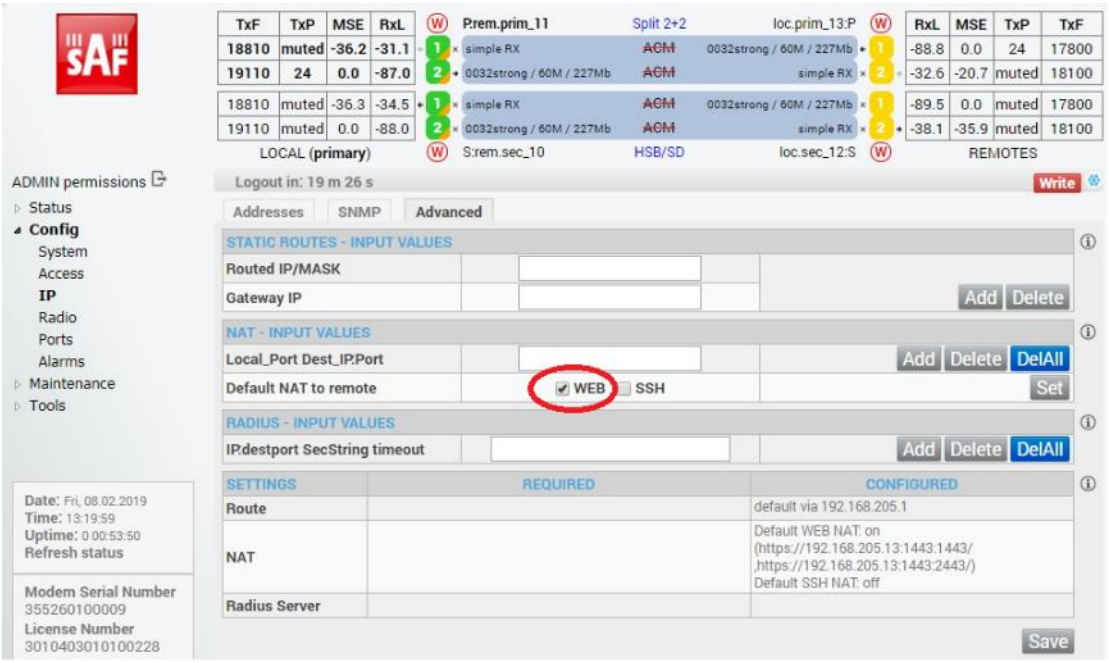


Figure 5.83 *Example of Side B Primary IDU IP NAT configuration*

f) Port group configuration must be done according to customer requirements. In this configuration when the Duplex modes "Tx-only" and "Rx-only" are used the remote management access via WAN port is not supported. That is why NAT configuration is required. In this example LAN1 port is used for the traffic, so LAN1 and WANa are grouped in the same group (Group 1). LAN2 and WANb are grouped in Group 2 and will not be used or can be intended for any other independent and separated user data traffic. LAN3 and MNG ports are grouped in

Group3 for management access only via LAN3 port. Port grouping configuration is available in web GUI '*Config->Ports->EthVLAN*' section

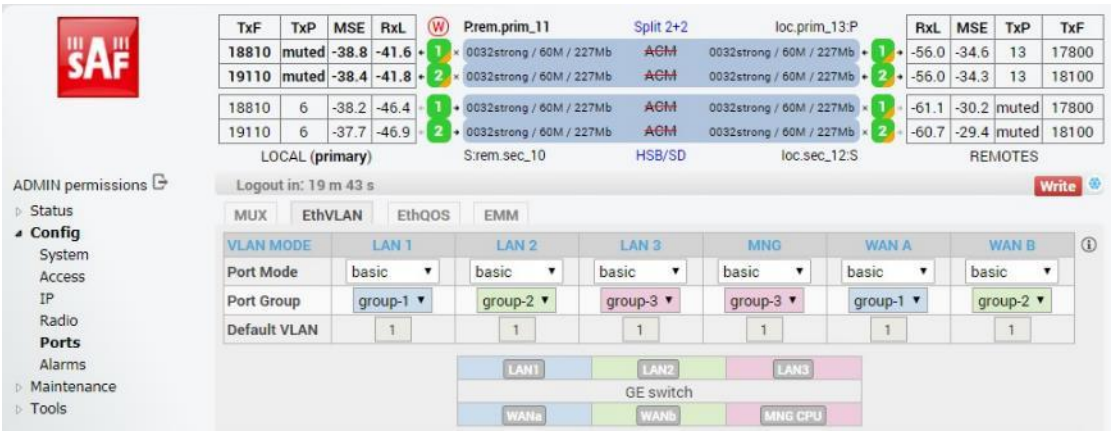


Figure 5.84 *Example of Side B Primary IDU port grouping*

g) In web GUI '*Config->Ports->MUX*' specify Data channel and port speed for WAN (radio direction) port and SFP ports. In the example WANa port is connected to high priority data channel 'ETH1a' and is set on full speed limit 1000 Mbps. The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary) are interconnected successfully, the SFP1 and SFP2 ports must be automatically indicated as connected in Mode 'force2G5'

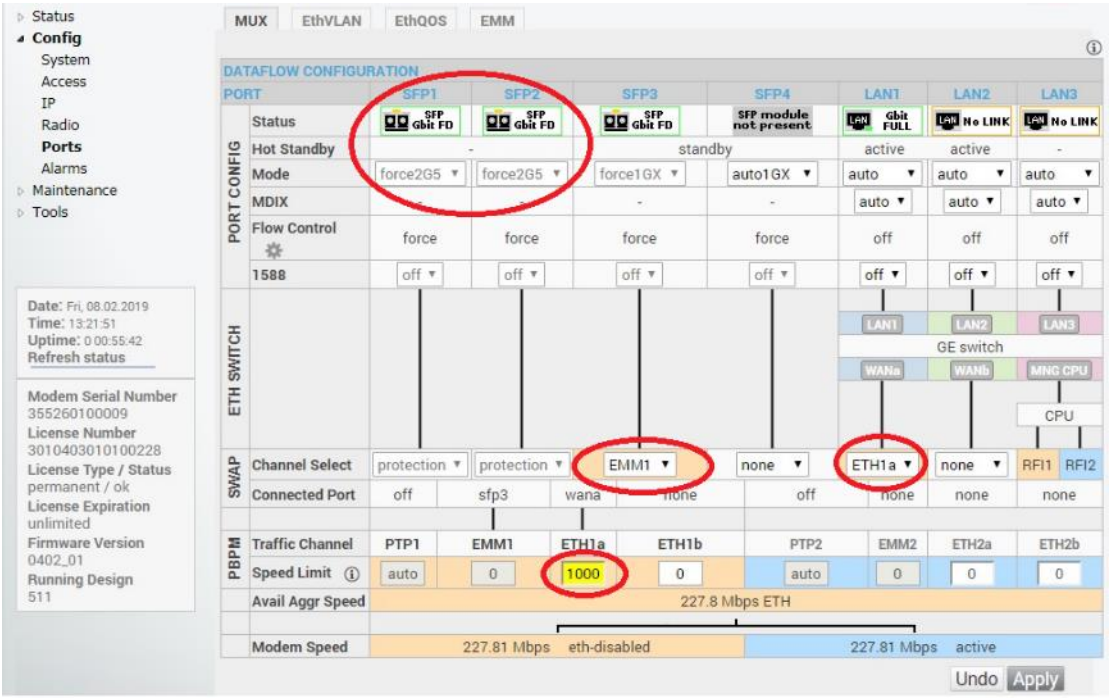


Figure 5.85 *Example of Side B Primary IDU port configuration*

h) In web GUI '*Config->Ports->EMM*' configure the ASI traffic according to customer requirements. In the example one ASI traffic stream via ASI1 port is sent from side A to side B. In this case the ASI EMM configuration will be following: 'EMM Enable' and 'EMM Protection Failover' check-boxes must be checked. Also ASI EMM module 'Enable' check-box must be checked and 'Mode' set as "Tx". The Data Source in this case must be specified as 'Remote Ch1'

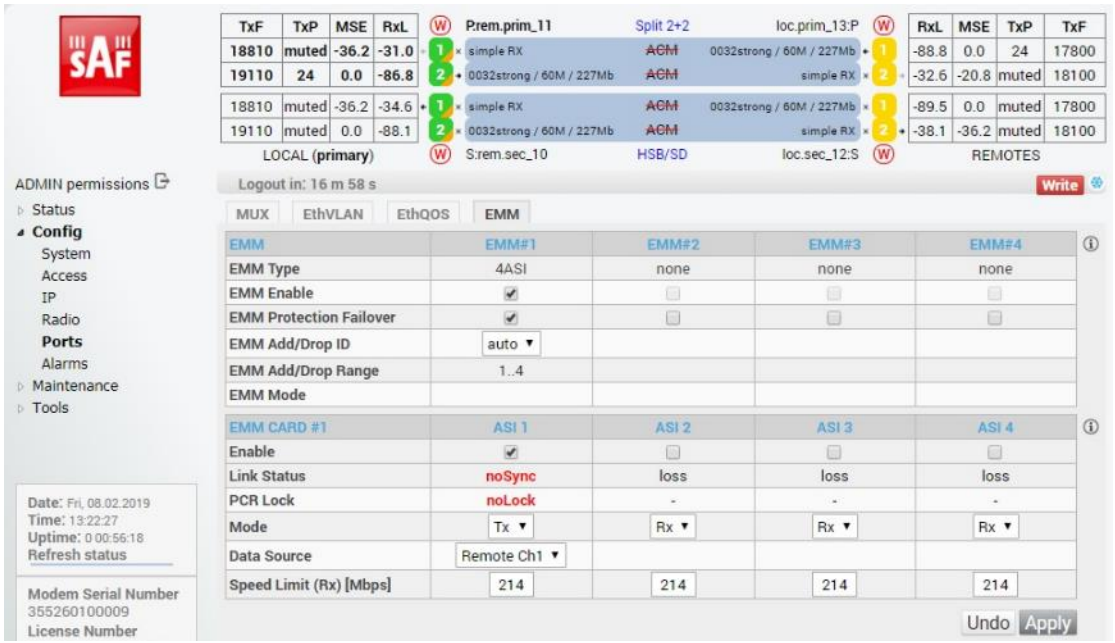


Figure 5.86 *Example of Side B Primary IDU EMM configuration*

i) In web GUI '*Config →Alarms →General*' configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label). In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

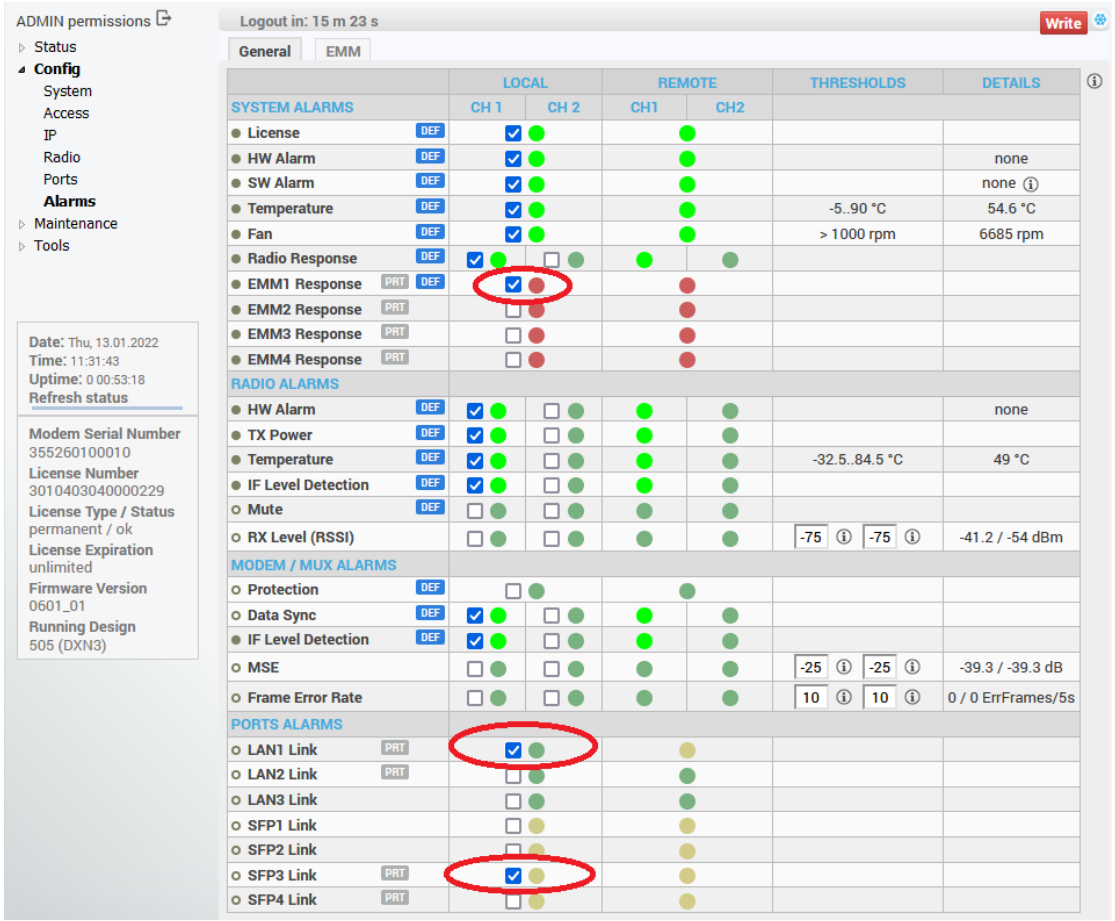


Figure 5.87a *Example of Side B Primary IDU alarm configuration*

j) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

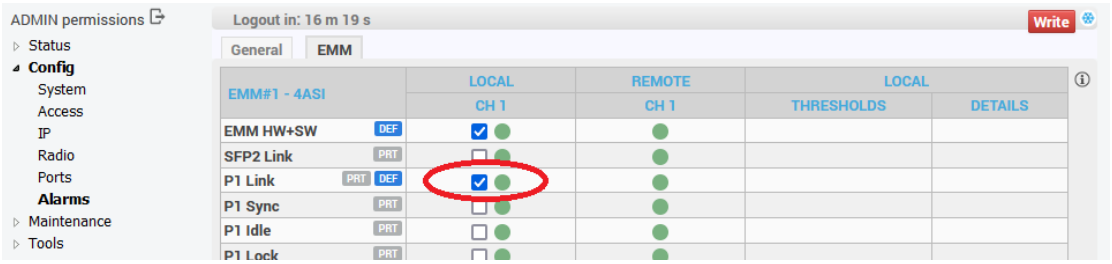


Figure 5.87b *Example of Side B Primary IDU alarm configuration*

k) Save new settings by pressing Write button.

4) **IDU B (secondary)**:

a) In web GUI '*Config->System->Mode*' choose design type 'Design 511', Functional mode 'Split 2+2', Link Protection Diversity 'HSB/SD – Hot standby', Link Aggregation Diversity 'FD'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed secondary'. As the link will use different frequency channels/bands for each direction then the Duplex Mode must be configured so that one of channels is in Tx mode, but the second channel is in Rx mode. In the example on Side B the Channel 1 is 'Rx-only' mode, and the Channel 2 is in 'Tx-only' mode

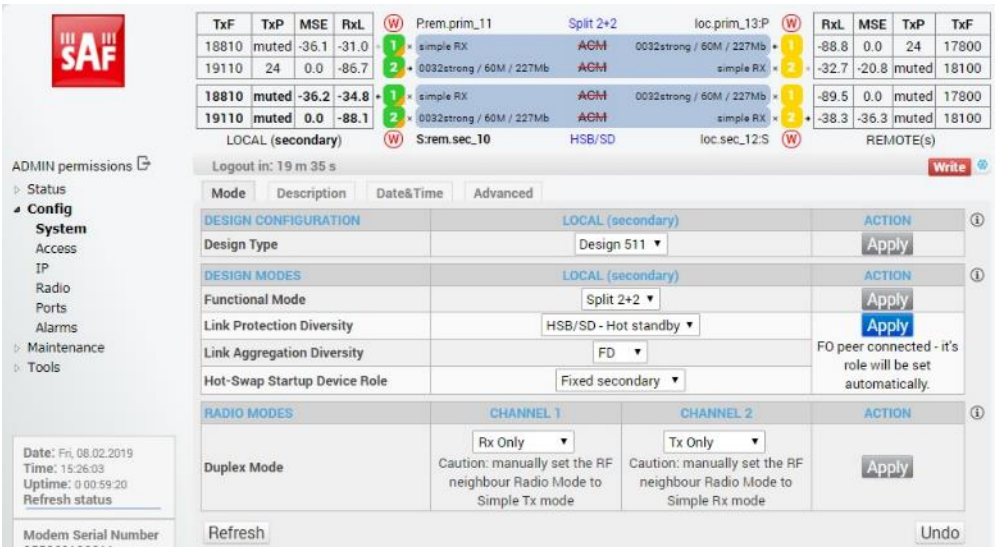


Figure 5.88 *Example of Side B Secondary IDU system configuration*

b) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters. Frequency channel/band must be different for Channel 1 and Channel 2, and correspond to 'Tx-only' and 'Rx-only' Duplex mode settings in '*Config->System->Mode*' page

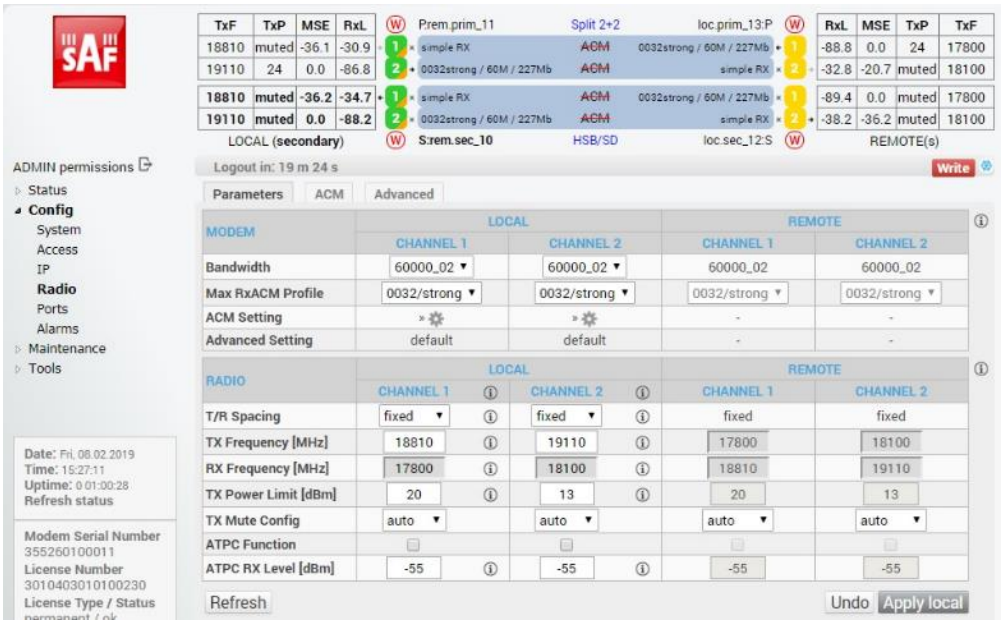


Figure 5.89 *Example of Side B Secondary IDU radio configuration*

c) The ACM (Adaptive Coding and Modulation) must be disabled if Duplex modes "Tx only" and "Rx only" are used. In order to disable it, navigate to '*Config →System →Mode*' in the web GUI and set ACM Control to "Manual". This setting disables the ACM



Figure 5.90 *Example of Side B Secondary IDU ACM configuration*

d) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU



Figure 5.91 *Example of Side B Secondary IDU IP configuration*

e) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote. This will enable management access to other IDUs in the link via NAT.

With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible:

2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the remote secondary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:3443

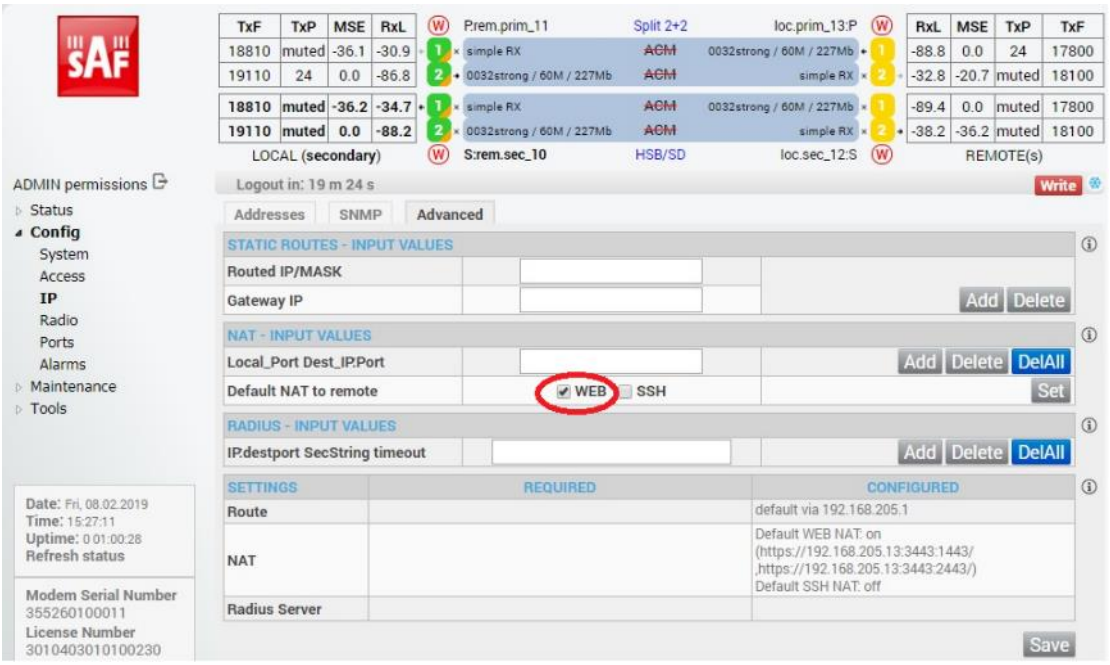


Figure 5.92 *Example of Side B Secondary IDU IP NAT configuration*

f) Port group configuration must be done according to customer requirements. In this configuration when the Duplex modes “Tx-only” and “Rx-only” are used the remote management access via WAN port is not supported. That is why NAT configuration is required. In this example LAN1 port is used for the traffic, so LAN1 and WANa are grouped in the same group (Group 1). LAN2 and WANb are grouped in Group 2 and will not be used or can be intended for any other independent and separated user data traffic. LAN3 and MNG ports are grouped in Group3 for management access only via LAN3 port. Port grouping configuration is available in web GUI ‘*Config->Ports->EthVLAN*’ section

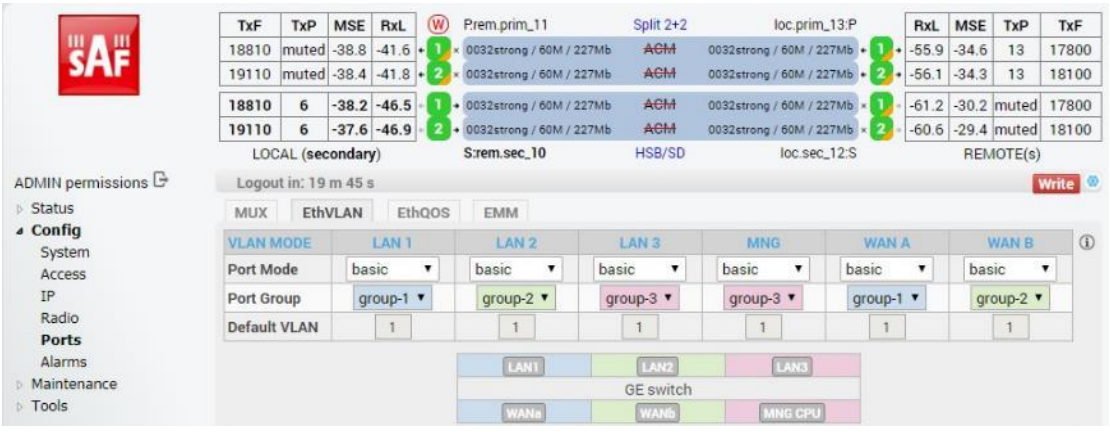


Figure 5.93 *Example of Side B Secondary IDU port grouping*

g) In web GUI ‘*Config->Ports->MUX*’ specify Data channel and port speed for WAN (radio direction) port and SFP ports. In the example WANa port is connected to high priority data channel ‘ETH1a’ and is set on full speed limit 1000 Mbps. The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary)

are interconnected successfully, the SFP1 and SFP2 ports must be automatically indicated as connected in Mode ‘force2G5’

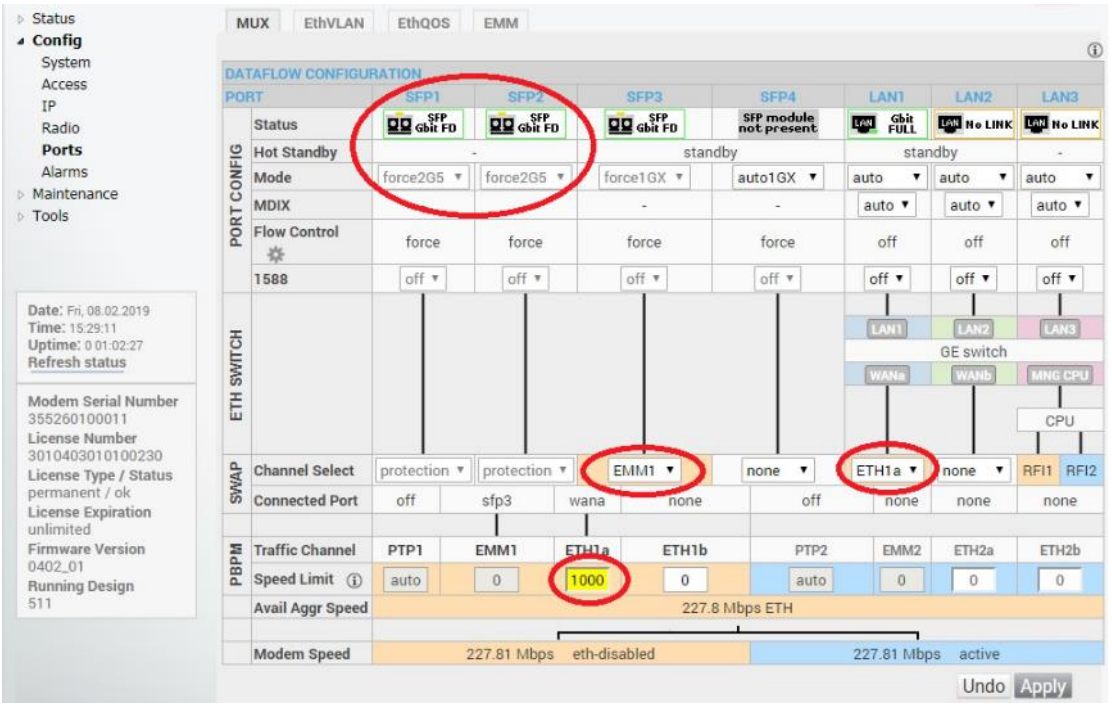


Figure 5.94 *Example of Side B Secondary IDU port configuration*

h) In web GUI ‘*Config->Ports->EMM*’ configure the ASI traffic according to customer requirements. In the example one ASI traffic stream via ASI1 port is sent from side A to side B. In this case the ASI EMM configuration will be following: ‘EMM Enable’ and ‘EMM Protection Failover’ check-boxes must be checked. Also ASI EMM module ‘Enable’ check-box must be checked and ‘Mode’ set as ”Tx”. The Data Source in this case must be specified as ‘Remote Ch1’

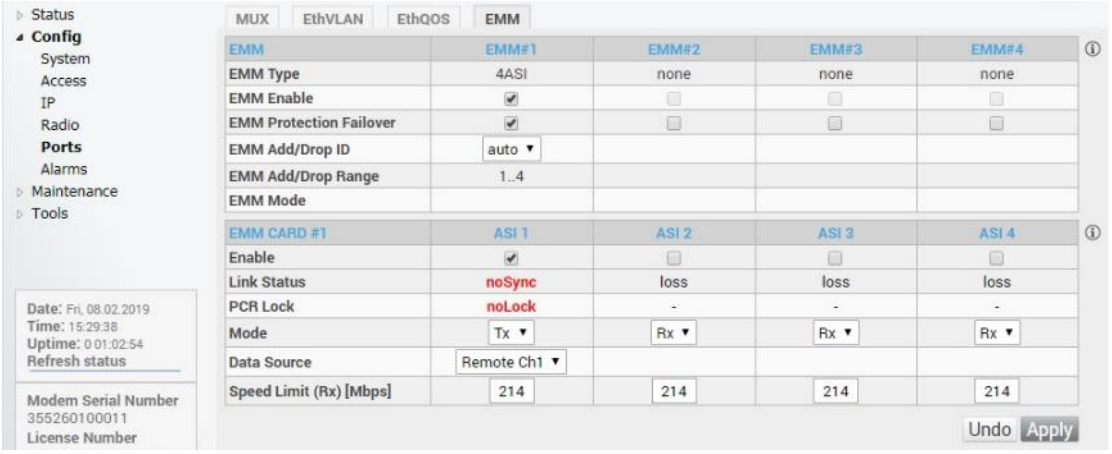


Figure 5.95 *Example of Side B Secondary IDU EMM configuration*

i) In web GUI ‘*Config →Alarms →General*’ configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label). In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

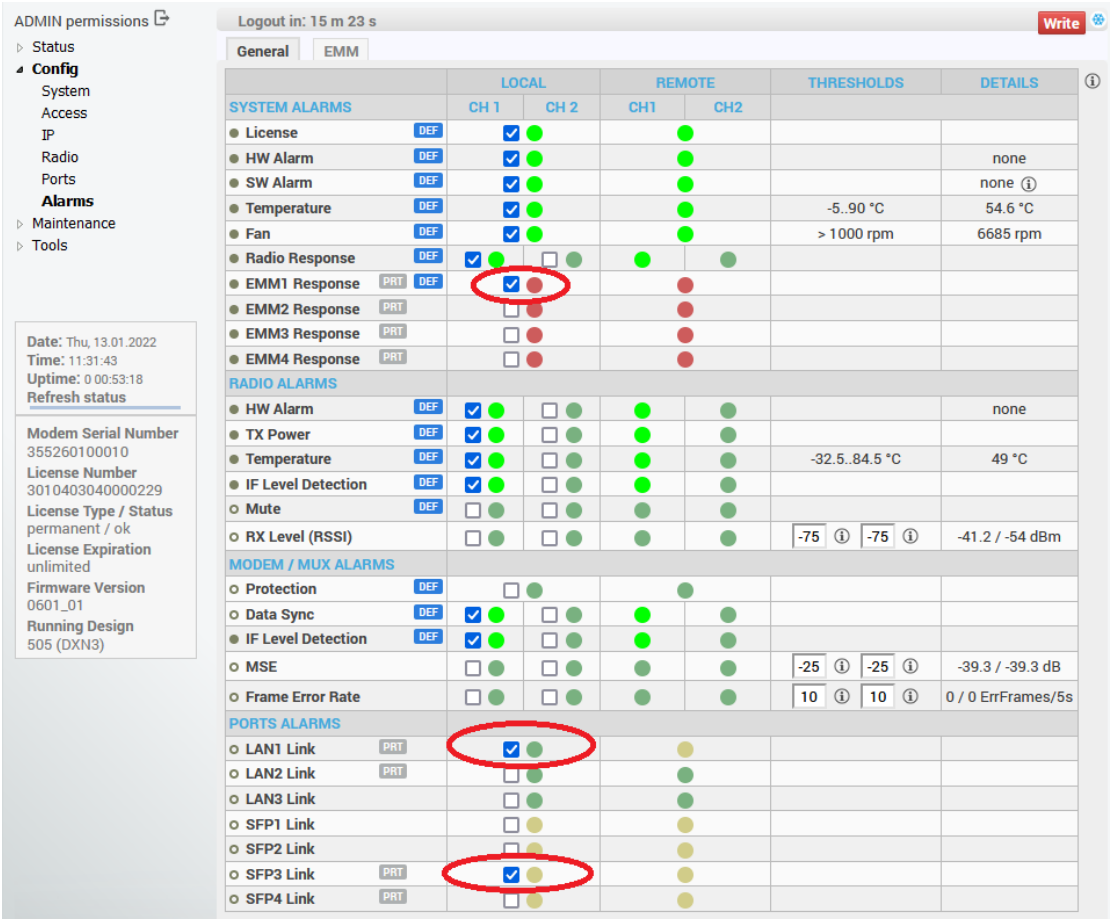


Figure 5.96a *Example of Side B Secondary IDU alarm configuration*

j) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

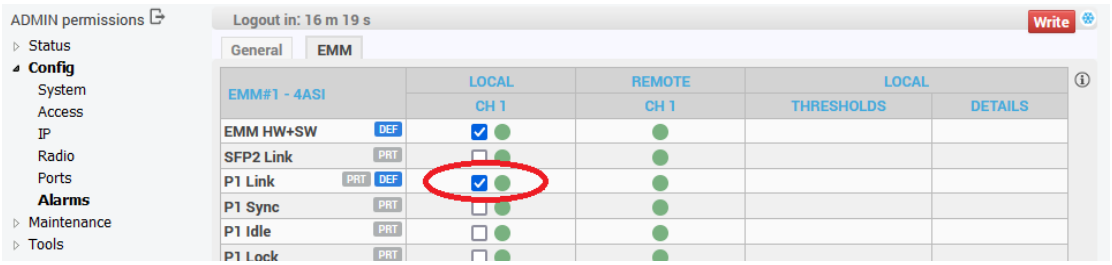


Figure 5.96b *Example of Side B Secondary IDU alarm configuration*

k) Save new settings by pressing Write button.

5) Reboot all 4 IDUs after successful reconfiguration
6) In web GUI '*Config->System->Mode*' set Hot-Swap Startup device Role to 'Auto primary' in both Primary IDUs in order to enable protection mode

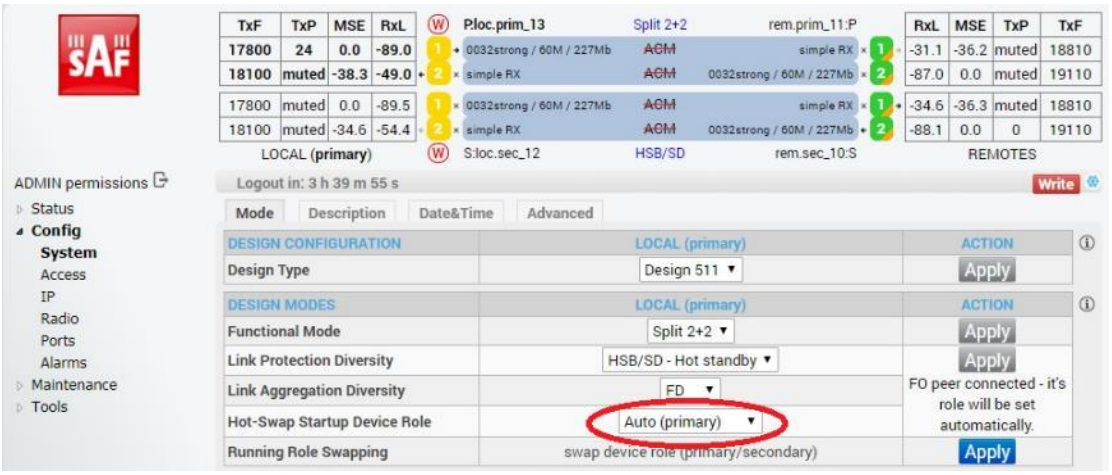


Figure 5.97 *Example of Primary IDUs system configuration in Auto mode*

7) In web GUI '*Config->System->Mode*' set Hot-Swap Startup device Role to 'Auto secondary' in both Secondary IDUs in order to enable protection mode

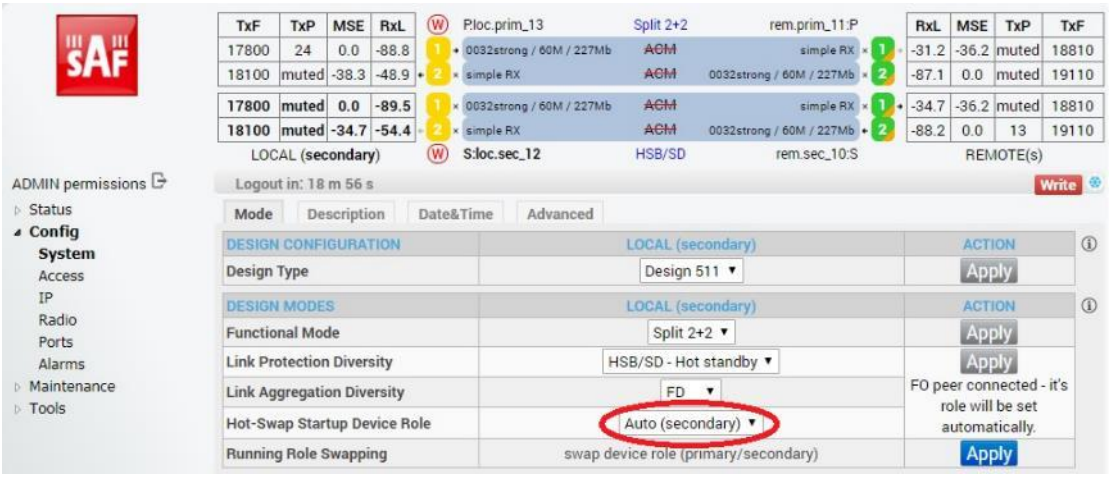


Figure 5.98 *Example of Secondary IDUs system configuration in Auto mode*

8) Save new settings by pressing Write button.

The status of the link and its configuration is displayed in the header of the web GUI. The status of the IDU which currently is monitored is displayed in Bold and is indicated as LOCAL (primary) or LOCAL (secondary):



Figure 5.99 *Status of 1+1 HSB/SD Dual-band frequency mode*

Example 10 – 2+2 FD aggregation HSB/SD protection mode (Design 511)

The 2+2 FD (Frequency Diversity) aggregation HSB/SD (Hot Standby/Space Diversity) protection mode is the mode supporting link aggregation which is protected using HSB/SD protection method. In this case two data Channels are used for data aggregation (Channel 1 and Channel 2). Each channel uses its own radio frequency channel (FD), and each channel is protected.

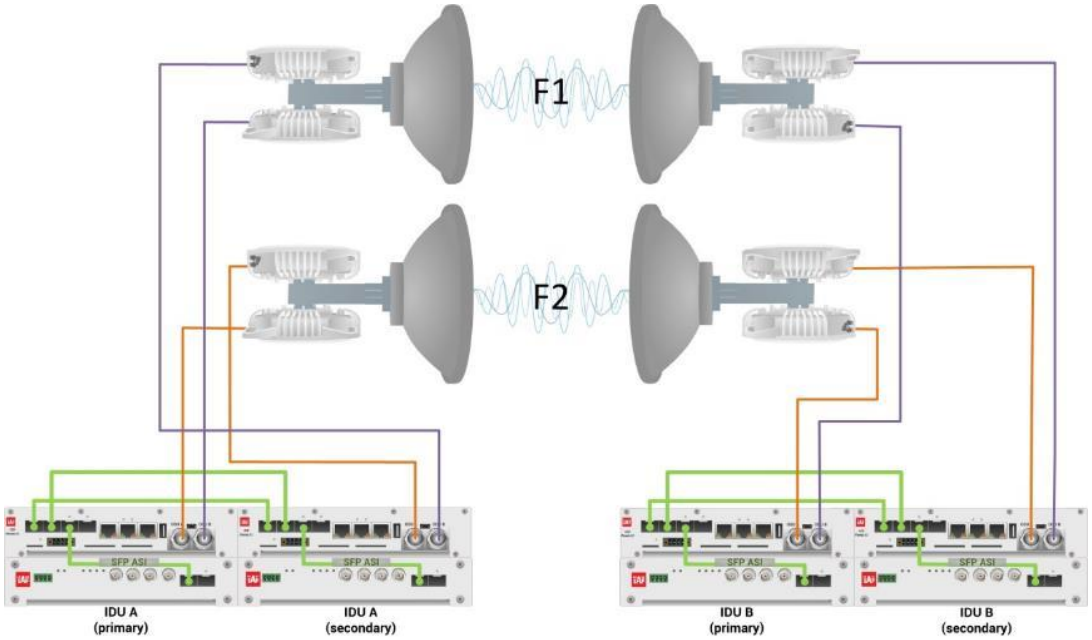


Figure 5.100a *Example of 2+2 FD aggregation HSB/SD protection scheme*

Figure 5.100a shows 2+2 FD aggregation HSB/SD protection scheme where IF interconnections between IDUs and ODUs provides HSB connection diagram. Two frequency channels are used in the same polarization. Couplers are used to interconnect 2 ODUs to one antenna.

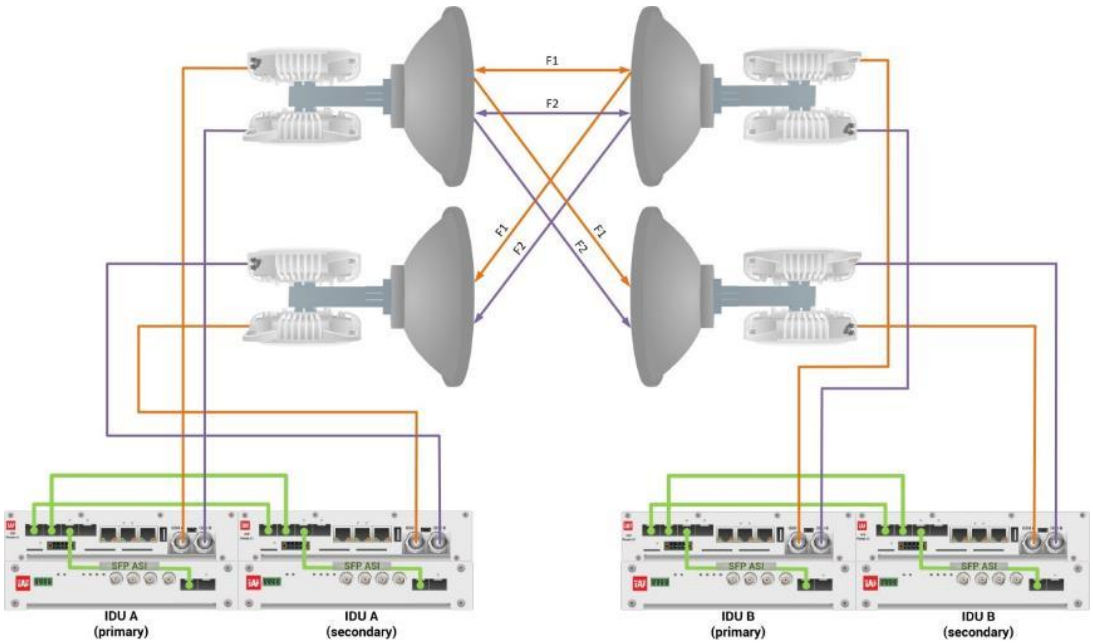


Figure 5.100b *Example of 2+2 FD aggregation HSB/SD protection scheme*

Figure 5.100b shows 2+2 FD aggregation HSB/SD protection scheme where IF interconnections between IDUs and ODUs provides SD connection diagram. Two frequency channels are used in the same polarization. Couplers are used to interconnect 2 ODUs to one antenna.

In both above mentioned schemes the ODUs and couplers can be substituted with IRFUs and IBUs combination if required by customer.

This example describes an application where the Design Type 'Design 511', Functional mode 'Split 2+2', Link Aggregation Diversity 'FD' and Link Protection Diversity 'HSB/SD – hot standby' are selected on both sides of the link. The modulation is 32QAM in BW 60 MHz and the appropriate maximal data speed is about 227 Mbps per channel. ASI traffic is passed through the link. **This scheme requires four Phoenix G2 IDUs and eight ODUs per link**.



Both IDUs in each side of the link are interconnected with 2 optical cables on ports SFP1 and SFP2. 2.5 GB SFP modules must be used for this interconnection. SFP3 or SFP4 port can be used for the IDU interconnection with ASI EMM module.

Configuration steps for 2+2 FD aggregation HSB/SD protection are following:

1) In web GUI '*Config->System->Mode*' choose design type 'Design 511', Functional mode 'Split 2+2', Link Protection Diversity 'HSB/SD – Hot standby', Link Aggregation Diversity 'FD'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed primary' on both Primary IDUs and as 'Fixed secondary' on both Secondary IDUs. The Duplex Mode must be set to 'Bidirectional' for both channels on all Phoenix G2 IDUs.

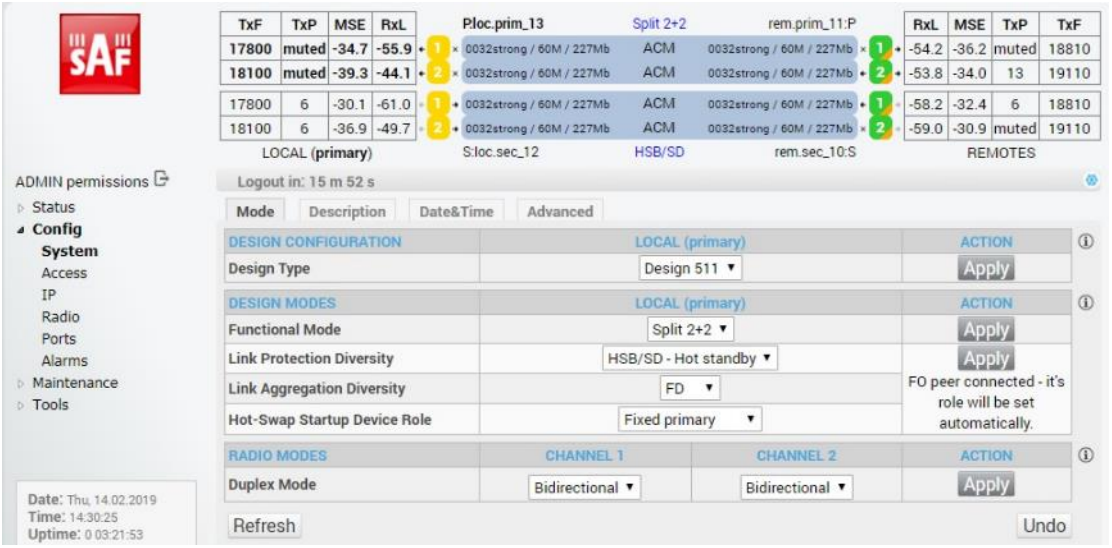


Figure 5.101 *Example of System configuration*

2) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters in all Phoenix G2 IDUs. Choose different frequency channels for Channel 1 and Channel 2

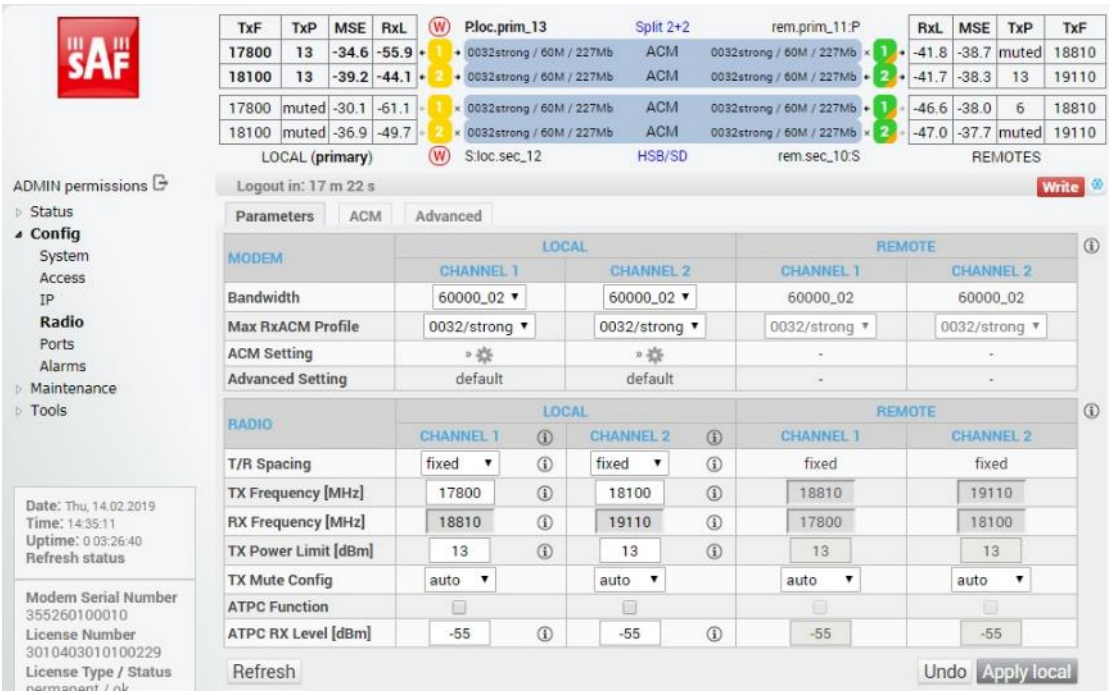


Figure 5.102 *Example of Radio configuration*

3) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU

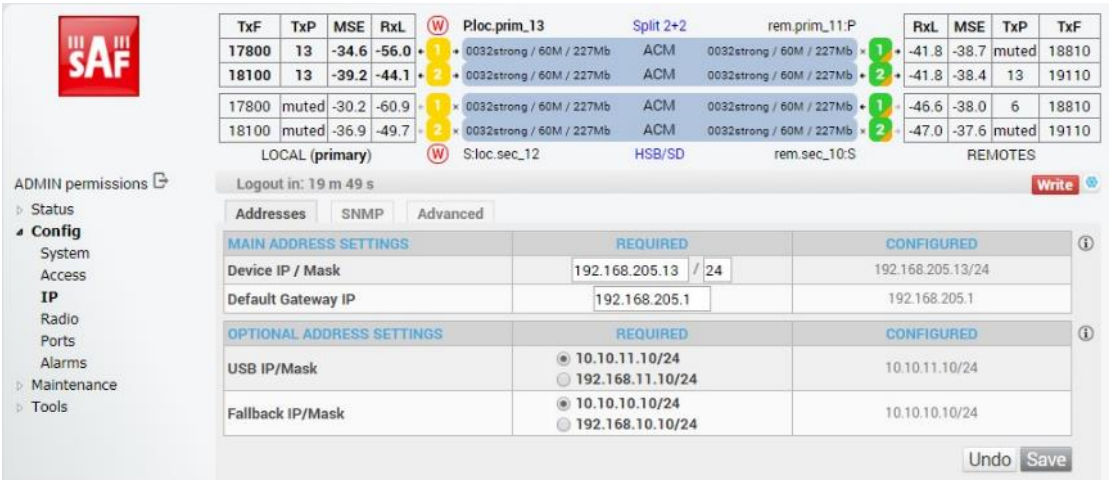


Figure 5.103 *Example of IP configuration*

4) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote in all Phoenix G2 IDUs. This will enable management access to other IDUs in the link via NAT.



With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible: 2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the local secondary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:2443

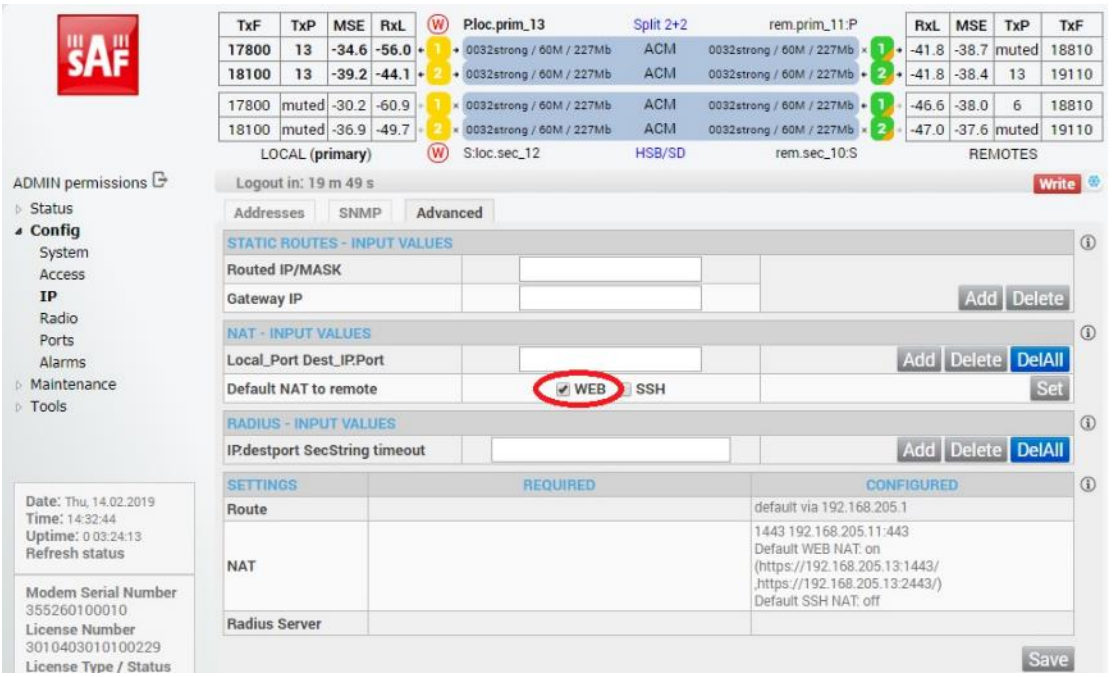


Figure 5.104 *Example of IP NAT configuration*

5) Port group configuration must be done according to customer requirements. The requirement in this example is to have one LAN port for Ethernet traffic. In this case LAN1 port will be used for the Ethernet traffic – it must be allocated in one group with one of WAN ports, in this case it is WANa port (Group1). LAN3 port will be used for management access, it is allocated in one group with MNG port (Group3). As the NAT is used for remote management access, it is not necessary to add management access ports to any of WAN ports. LAN2 and WANb ports will not be used in this example and will be allocated in Group2. Port grouping configuration is available in web GUI '*Config->Ports->EthVLAN*' section and must be done in all Phoenix G2 IDUs

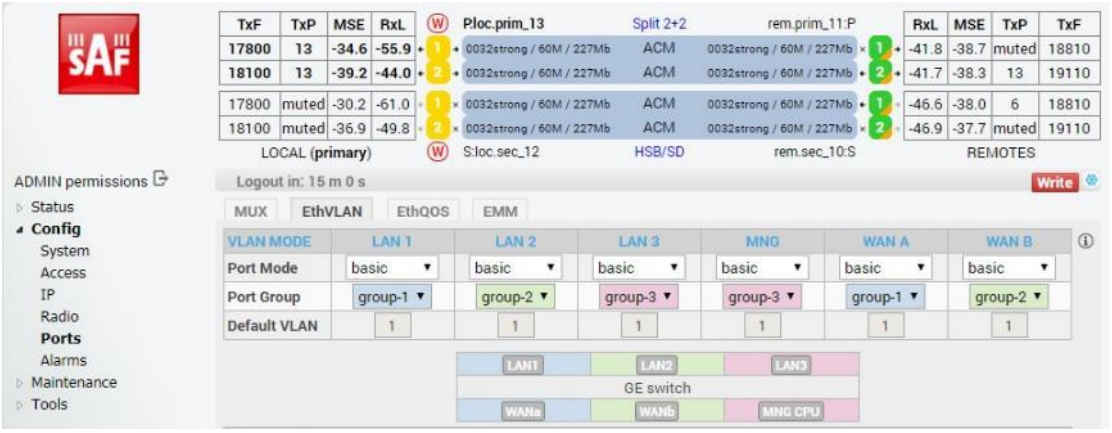


Figure 5.105 *Example of port grouping*

6) In web GUI '*Config->Ports->MUX*' specify Data channel and port speed for WAN (radio direction) port and SFP ports in all 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.The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary) are interconnected successfully, the SFP1 and SFP2 ports must be automatically indicated as connected in Mode 'force2G5'

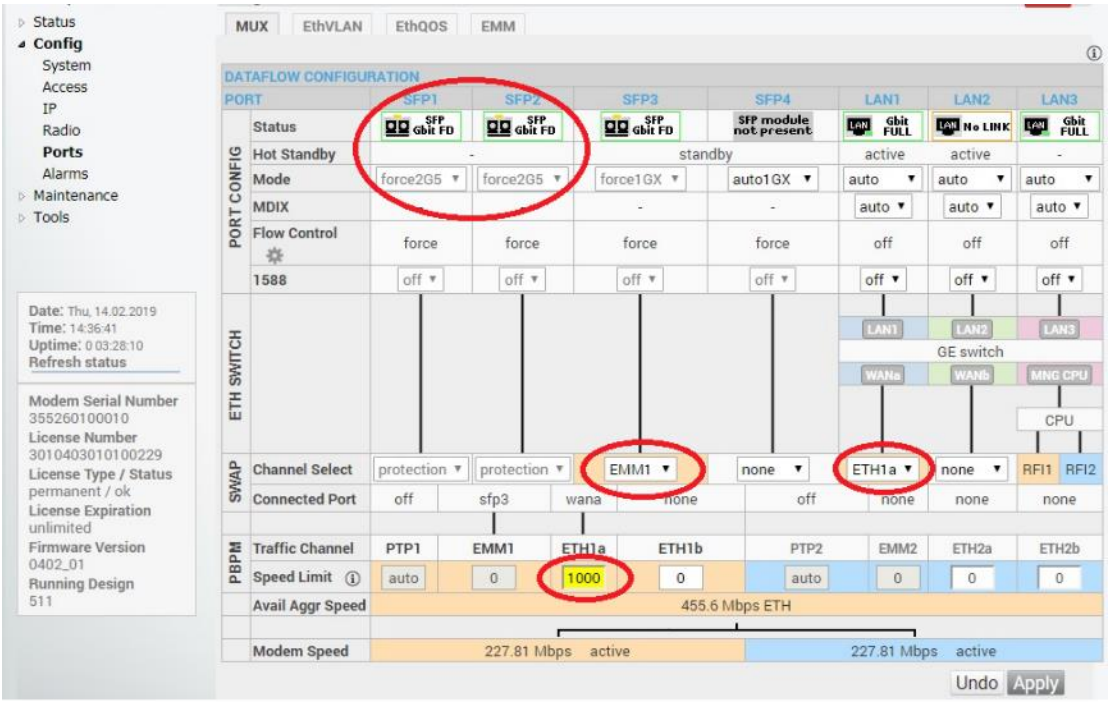


Figure 5.106 *Example of port configuration*

7) Configure EMM according to customer requirements and basing on EMM configuration description described in section '*Config->Ports->EMM*' in all Phoenix G2 IDUs.
8) In web GUI '*Config →Alarms →General*' configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label) in all Phoenix G2 IDUs. In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

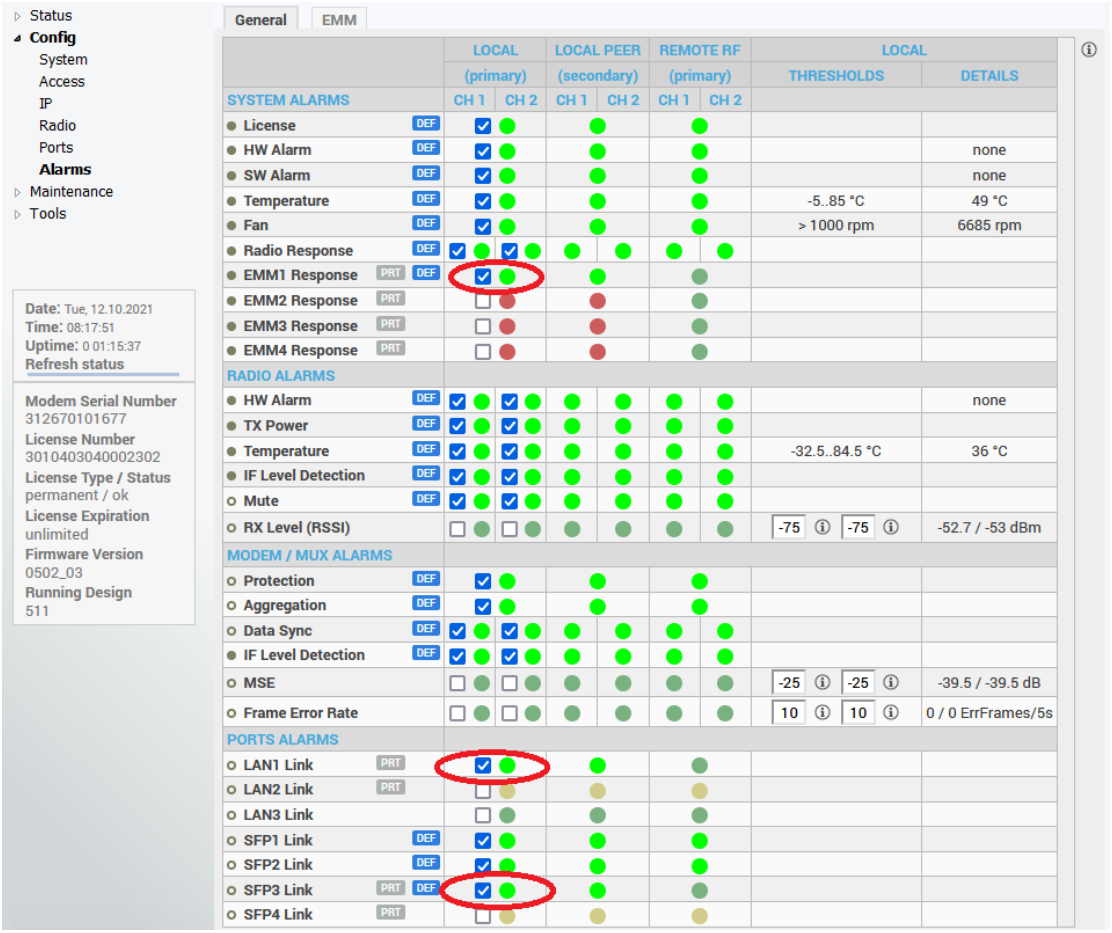


Figure 5.107a *Example of alarm configuration*

9) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

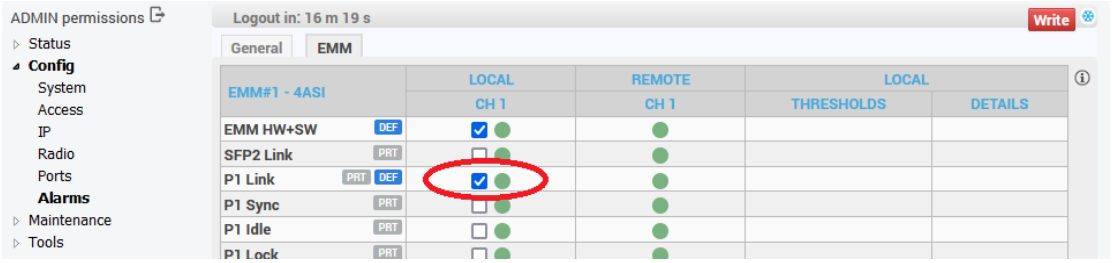


Figure 5.107b *Example of alarm configuration*

10) Save new settings by pressing Write button.
11) Reboot all 4 IDUs after successful reconfiguration
12) In web GUI '*Config->System->Mode*' set Hot-Swap Startup device Role to 'Auto primary' for both Primary IDUs and to 'Auto Secondary' for both Secondary IDUs in order to enable protection mode on all Phoenix G2 IDUs

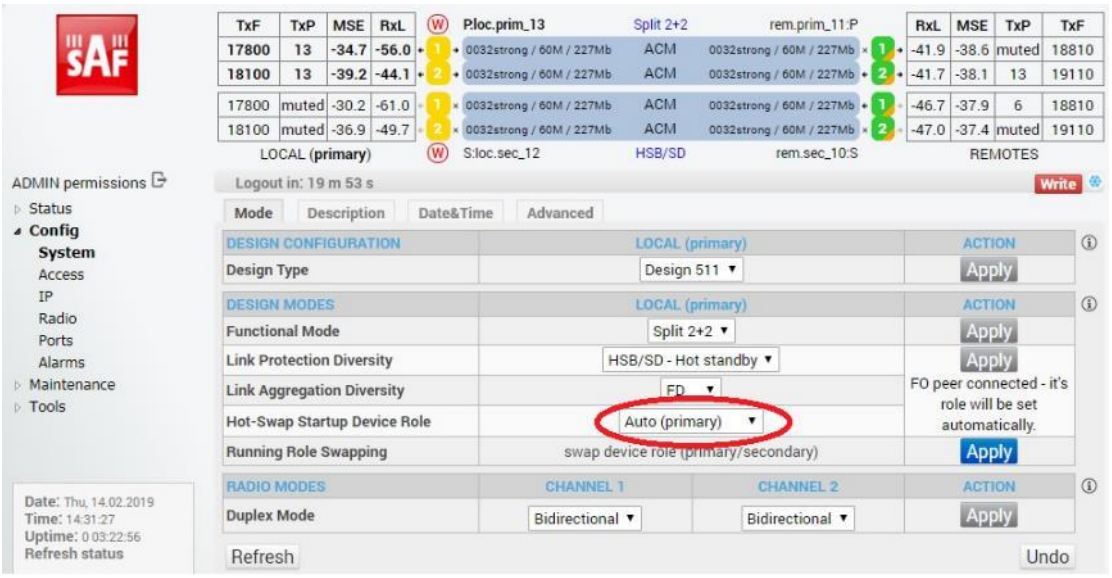


Figure 5.108 *Example of system configuration in Auto mode*

13) Save new settings by pressing Write button.

The status of the link and its configuration is displayed in the header of the web GUI. The status of the IDU which currently is monitored is displayed in Bold and is indicated as LOCAL (primary) or LOCAL (secondary):

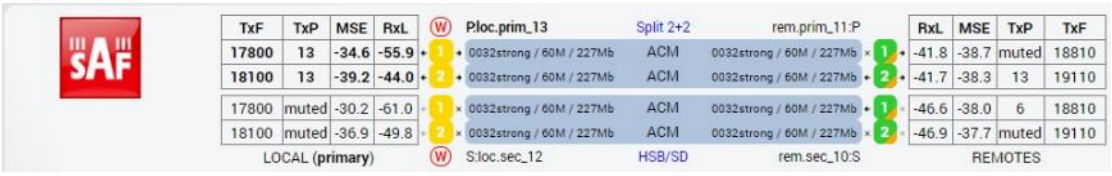


Figure 5.109 *Status of 2+2FD aggregation HSB/SD protection mode*

Example 11 – 2+2 FD aggregation FD protection mode (Design 511)

The 2+2 FD (Frequency Diversity) aggregation FD (Frequency Diversity) protection mode is the mode supporting link aggregation which is protected using FD protection method. In this case two data Channels are used for data aggregation (Channel 1 and Channel 2) and two Channels are used for protection of aggregation channels. Each channel – aggregation and protection uses its own radio frequency channel (FD), in total 4 frequency channels are used.

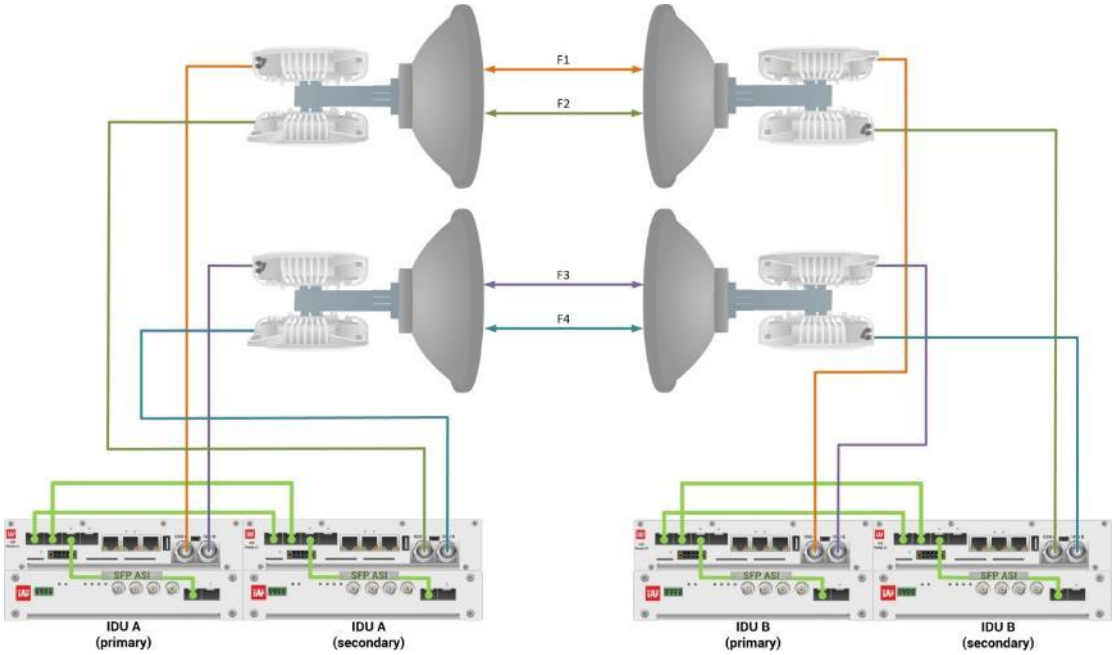


Figure 5.110a *Example of 2+2 FD aggregation FD protection scheme*

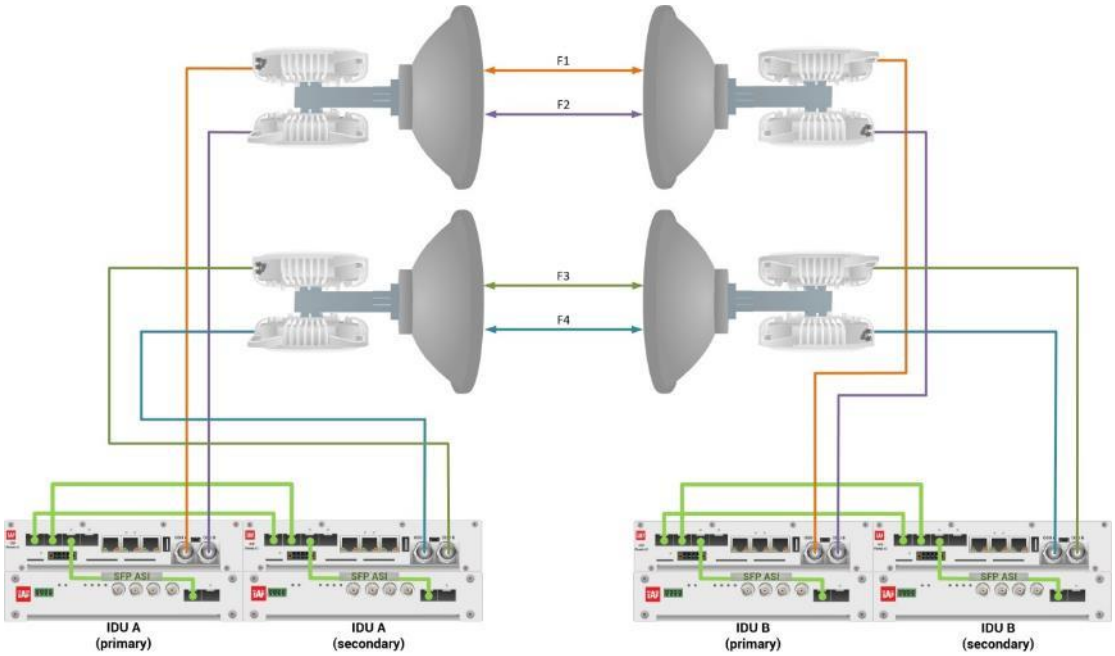


Figure 5.110b *Example of 2+2 FD aggregation FD protection scheme*

Figures 5.110a and 5.110b show 2+2 FD aggregation FD protection scheme where four frequency channels are used in the same polarization. Couplers are used to interconnect 2 ODUs to one antenna.

In both above mentioned schemes the ODUs and couplers can be substituted with IRFUs and IBUs combination if required by customer.

This example describes an application where the Design Type ‘Design 511’, Functional mode ‘Split 2+2’, Link Aggregation Diversity ‘FD’ and Link Protection Diversity ‘FD – Freq. diversity’ are selected on both sides of the link. The modulation is 1024QAM in BW 60 MHz and the appropriate maximal data speed is about 455 Mbps per channel. ASI traffic is passed through the link. **This scheme requires four Phoenix G2 IDUs and eight ODUs per link**.

Both IDUs in each side of the link are interconnected with 2 optical cables on ports SFP1 and SFP2. 2.5 GB SFP modules must be used for this interconnection. SFP3 or SFP4 port can be used for the IDU interconnection with ASI EMM module.

Configuration steps for 2+2 FD aggregation FD protection are following:

1) In web GUI '*Config->System->Mode*' choose design type 'Design 511', Functional mode 'Split 2+2', Link Protection Diversity 'FD – Freq. diversity', Link Aggregation Diversity 'FD'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed primary' on both Primary IDUs and as 'Fixed secondary' on both Secondary IDUs. The Duplex Mode must be set to 'Bidirectional' for both channels on all Phoenix G2 IDUs

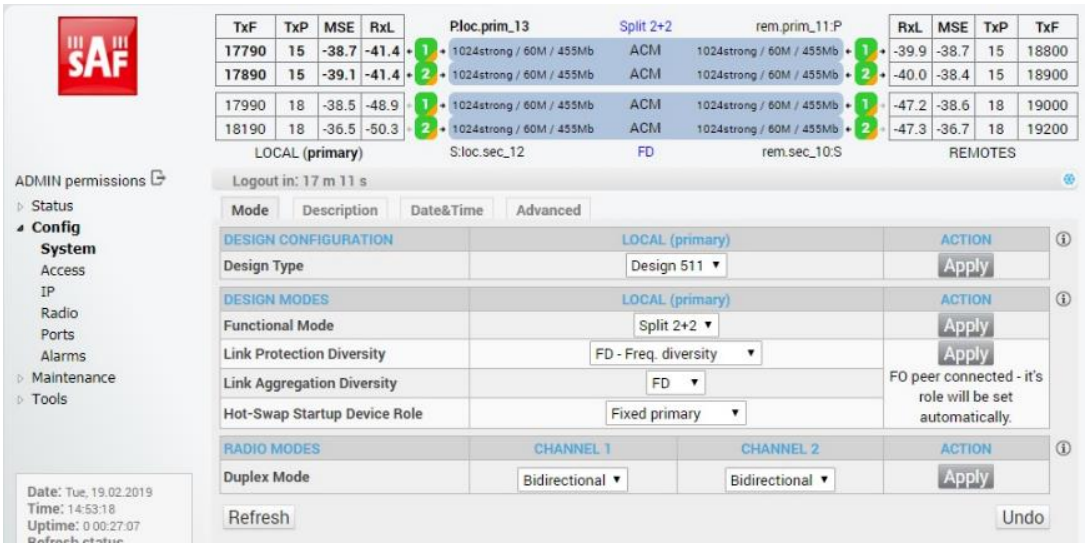


Figure 5.111 *Example of System configuration*

2) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters in all Phoenix G2 IDUs. Choose different frequency channels for Channel 1 and Channel 2 in both Primary IDUs and another different frequency channels for Channel 1 and Channel 2 in both secondary IDUs

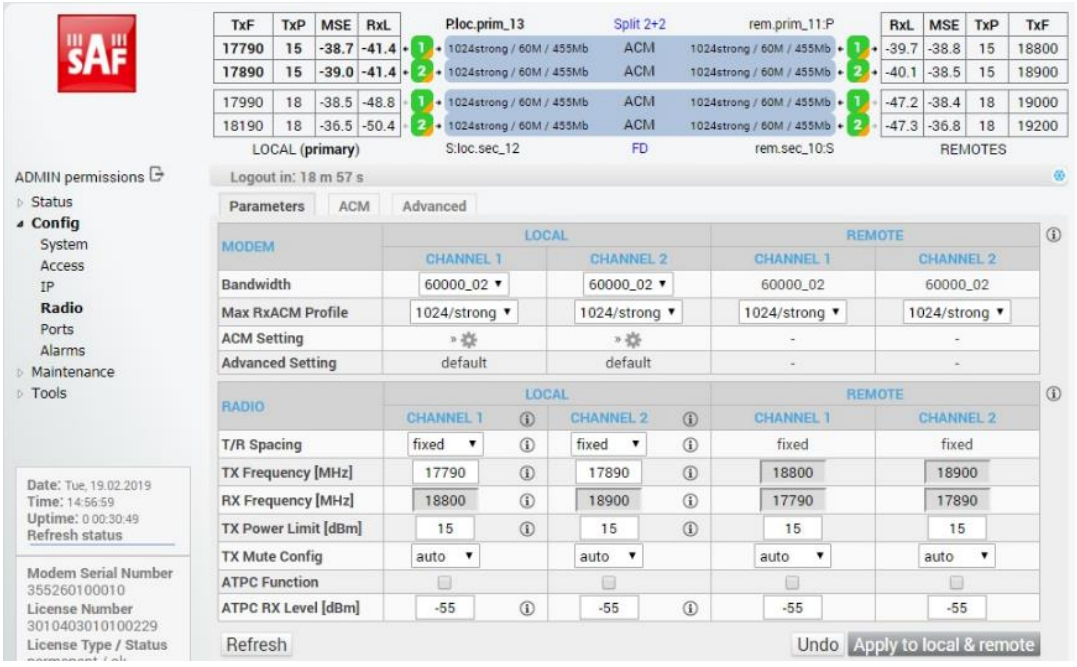


Figure 5.112 *Example of Primary IDU Radio configuration*

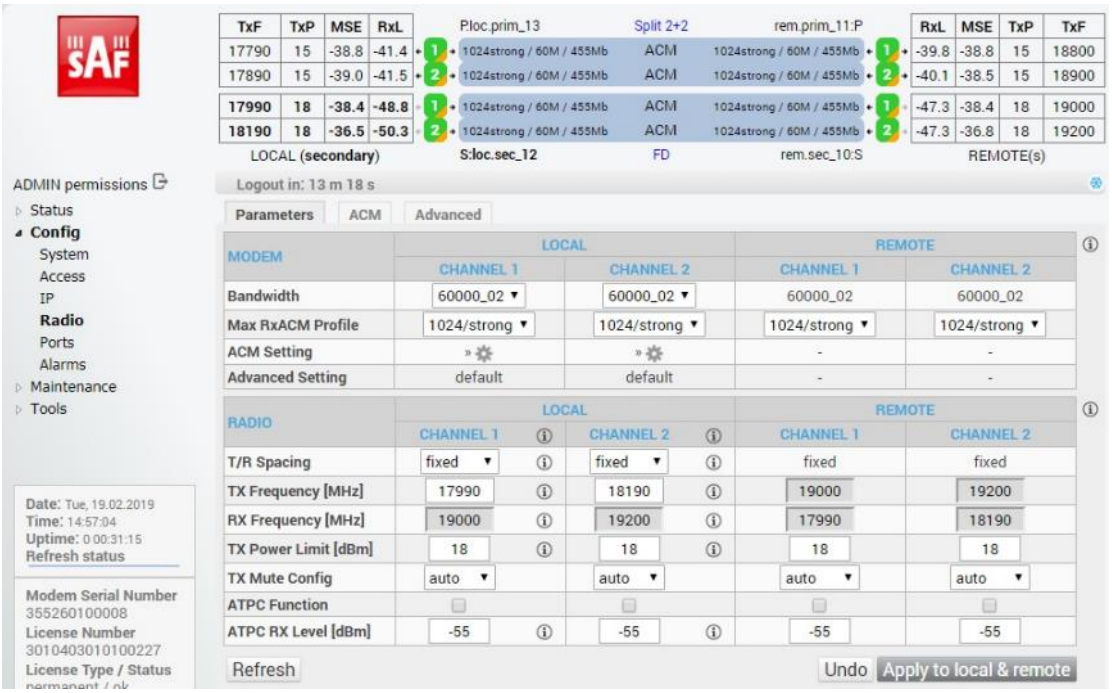


Figure 5.113 *Example of Secondary IDU Radio configuration*

3) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU



Figure 5.114 *Example of IP configuration*

4) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote in all Phoenix G2 IDUs. This will enable management access to other IDUs in the link via NAT.



With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible: 2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the local secondary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:2443

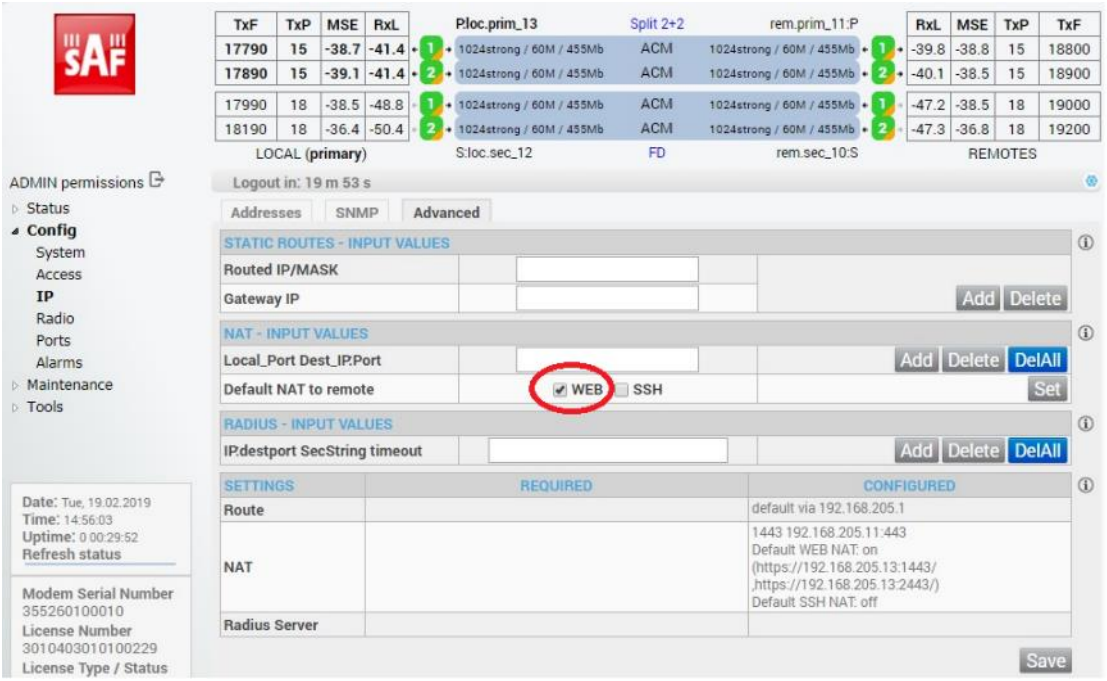


Figure 5.115 *Example of IP NAT configuration*

5) Port group configuration must be done according to customer requirements. The requirement in this example is to have one LAN port for Ethernet traffic. In this case LAN1 port will be used for the Ethernet traffic – it must be allocated in one group with one of WAN ports, in this case it is WANa port (Group1). LAN3 port will be used for management access, it is allocated in one group with MNG port (Group3). As the NAT is used for remote management access, it is not necessary to add management access ports to any of WAN ports. LAN2 and WANb ports will not be used in this example and will be allocated in Group2. Port grouping configuration is available in web GUI '*Config->Ports->EthVLAN*' section and must be done in all Phoenix G2 IDUs

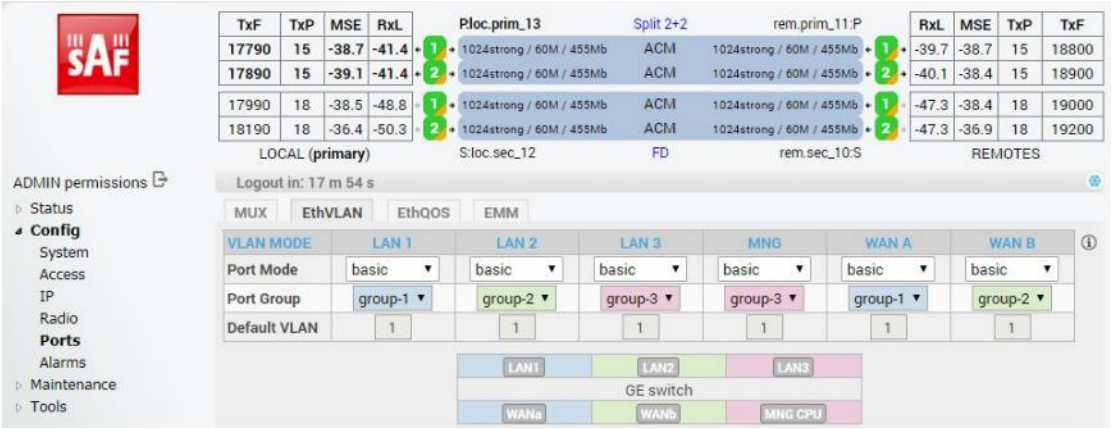


Figure 5.116 *Example of port grouping*

6) In web GUI '*Config->Ports->MUX*' specify Data channel and port speed for WAN (radio direction) port and SFP ports in all 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.The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary) are interconnected successfully, the SFP1 and SFP2 ports must be automatically indicated as connected in Mode 'force2G5'

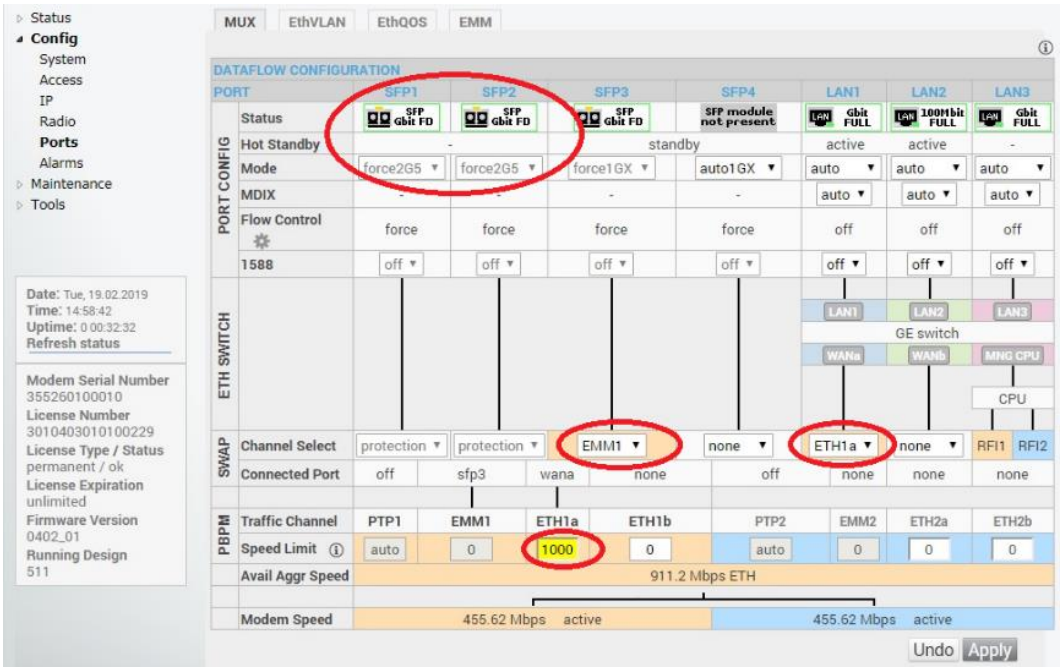


Figure 5.117 *Example of port configuration*

7) Configure EMM according to customer requirements and basing on EMM configuration description described in section '*Config->Ports->EMM*' in all Phoenix G2 IDUs.
8) In web GUI '*Config →Alarms →General*' configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label) in all Phoenix G2 IDUs. In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

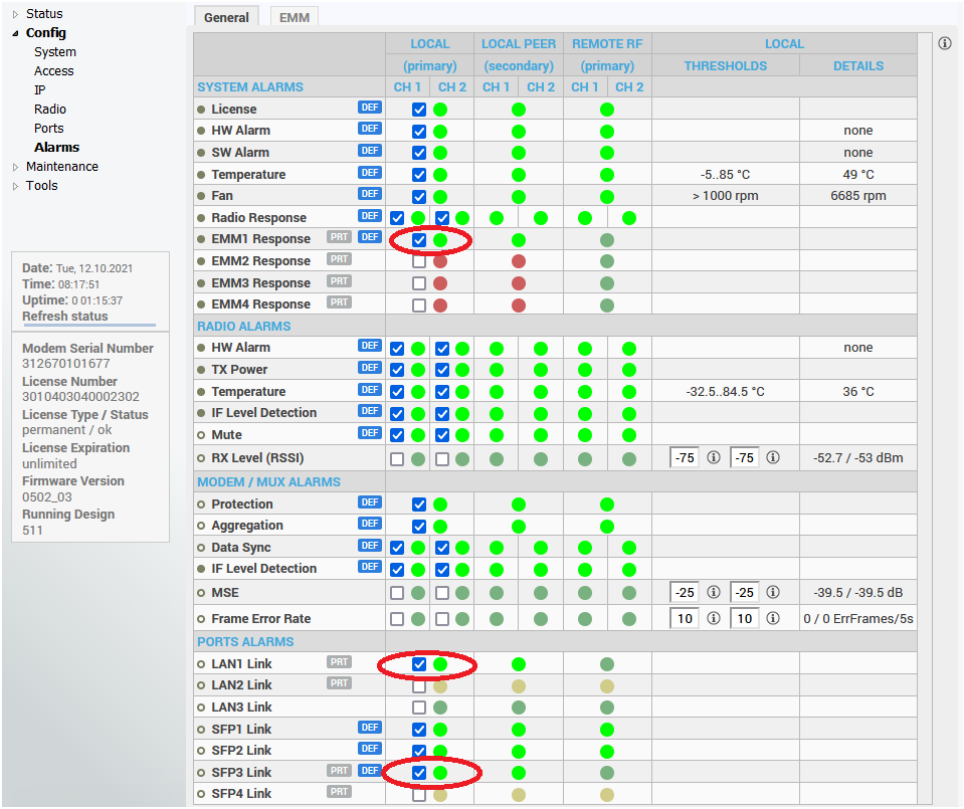


Figure 5.118a *Example of alarm configuration*

9) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

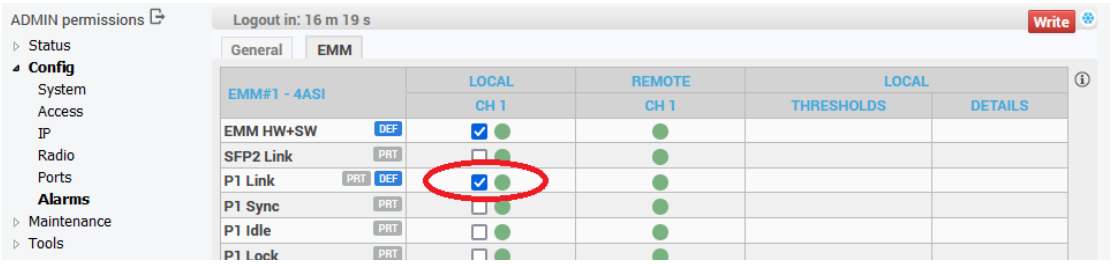


Figure 5.118a *Example of alarm configuration*

10) Save new settings by pressing Write button.
11) Reboot all 4 IDUs after successful reconfiguration
12) In web GUI '*Config->System->Mode*' set Hot-Swap Startup device Role to 'Auto primary' for both Primary IDUs and to 'Auto Secondary' for both Secondary IDUs in order to enable protection mode on all Phoenix G2 IDUs

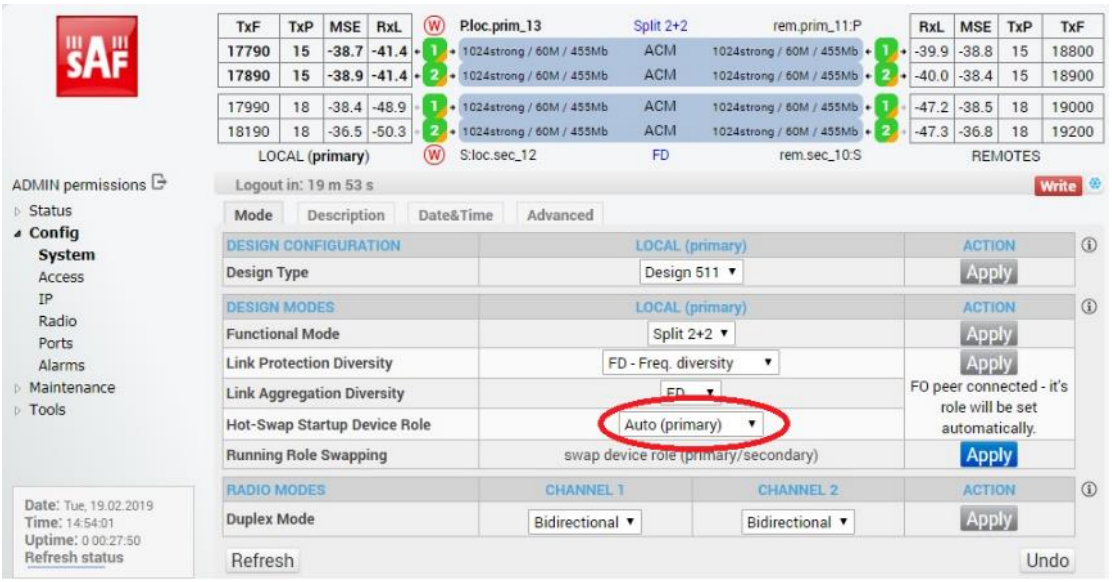


Figure 5.119 *Example of system configuration in Auto mode*

13) Save new settings by pressing Write button.

The status of the link and its configuration is displayed in the header of the web GUI. The status of the IDU which currently is monitored is displayed in Bold and is indicated as LOCAL (primary) or LOCAL (secondary):

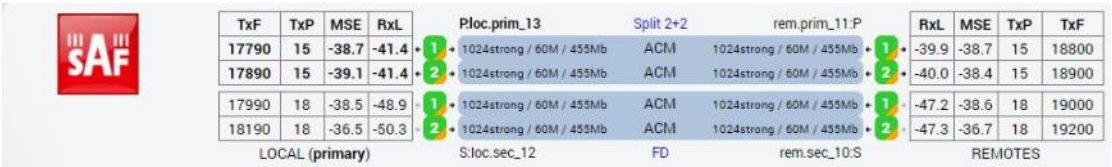


Figure 5.120 *Status of 2+2 FD aggregation FD protection mode*

Example 12 – 2+2 XPIC aggregation HSB/SD protection mode (Design 511)

The 2+2 XPIC (Cross-polarization Interference Cancellation) aggregation HSB/SD (Hot-standby/Space Diversity) protection mode is the mode supporting link aggregation which is protected using HSB/SD protection method. In this case two data Channels are used for data aggregation (Channel 1 and Channel 2) and two Channels are used for protection of aggregation channels. All channels – aggregation and protection works on the same one frequency channel.

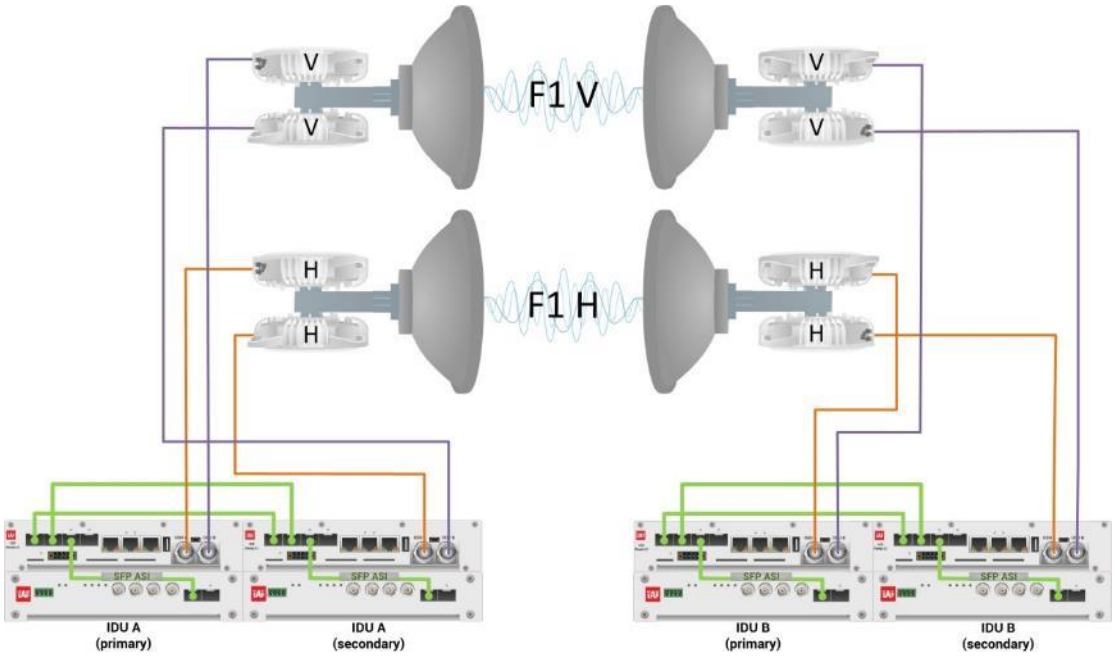


Figure 5.121a *Example of 2+2 XPIC aggregation HSB/SD protection scheme*

Figure 5.121a shows 2+2 XPIC aggregation HSB/SD protection scheme where IF interconnections between IDUs and ODUs provides HSB connection diagram. One frequency channel is used in both Horizontal and Vertical polarizations. Couplers are used to interconnect 2 ODUs to one antenna in this scheme. In this connection scheme the ODUs and couplers can be substituted with IRFUs and IBUs combination if required by customer.

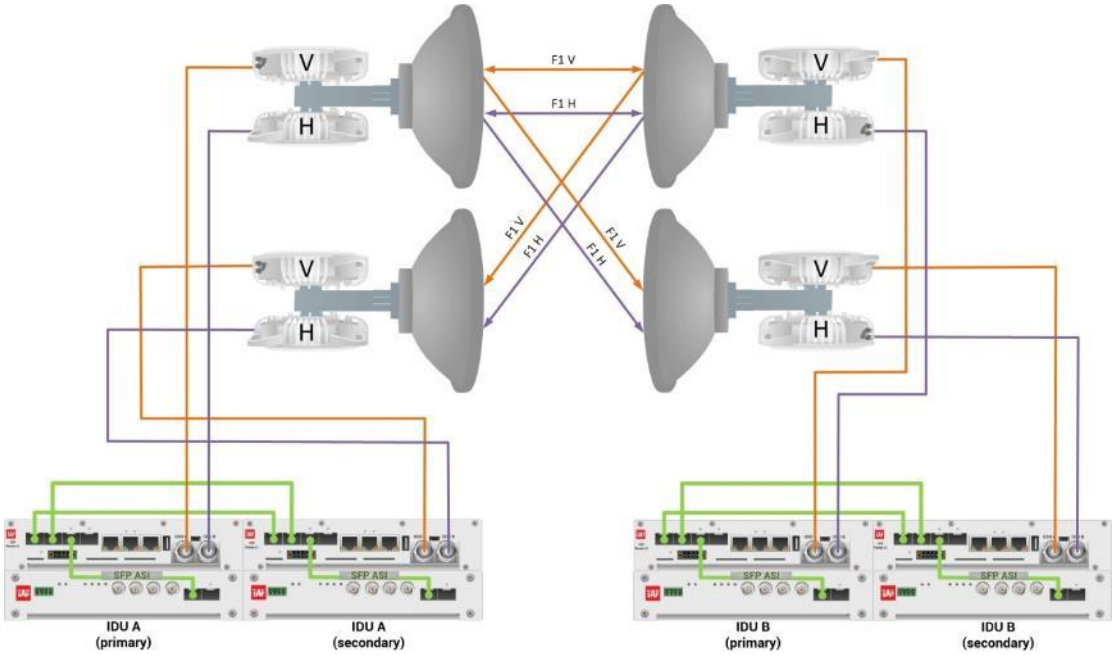


Figure 5.121b *Example of 2+2 XPIC aggregation HSB/SD protection scheme*

Figure 5.121b shows 2+2 XPIC aggregation HSB/SD protection scheme where IF interconnections between IDUs and ODUs provides SD connection diagram. One frequency channel is used in both Horizontal and Vertical polarizations. OMTs are used to interconnect 2 ODUs to one antenna in this scheme.

This example describes an application where the Design Type 'Design 511', Functional mode 'Split 2+2', Link Aggregation Diversity 'XPIC' and Link Protection Diversity 'HSB/SD-Hot standby' are selected on both sides of the link. The modulation is 1024QAM in BW 60 MHz and the appropriate maximal data speed is about 455 Mbps per channel. ASI traffic is passed through the link. **This scheme requires four Phoenix G2 IDUs and eight ODUs per link.**

Both IDUs in each side of the link are interconnected with 2 optical cables on ports SFP1 and SFP2. 2.5 GB SFP modules must be used for this interconnection. SFP3 or SFP4 port can be used for the IDU interconnection with ASI EMM module.

Configuration steps for 2+2 XPIC aggregation HSB/SD protection are following:

1) In web GUI '*Config->System->Mode*' choose design type 'Design 511', Functional mode 'Split 2+2', Link Protection Diversity 'HSB/SD – Hot standby', Link Aggregation Diversity 'XPIC'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed primary' on both Primary IDUs and as 'Fixed secondary' on both Secondary IDUs. The Duplex Mode must be set to 'Bidirectional' for both channels on all Phoenix G2 IDUs

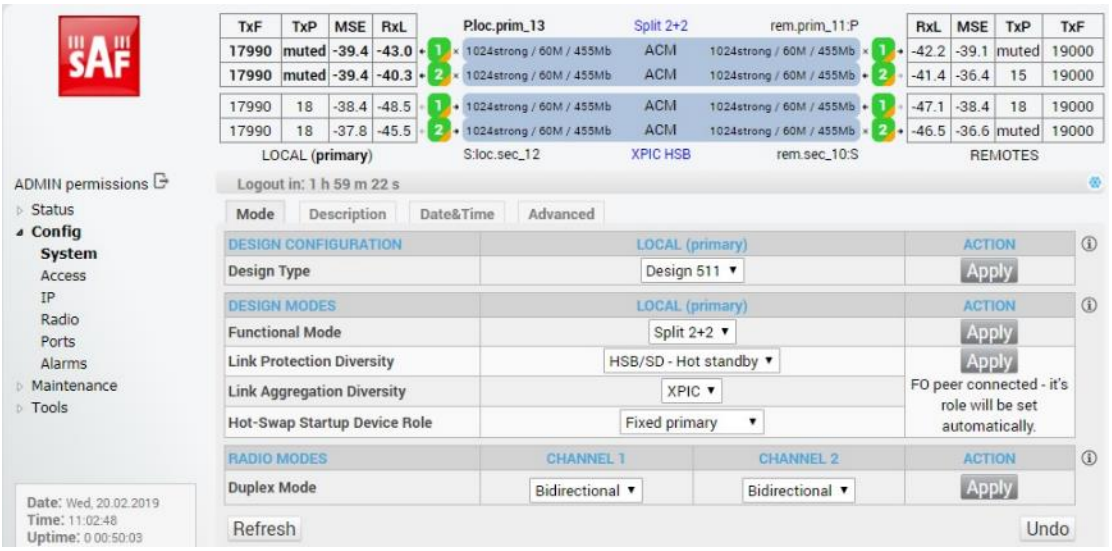


Figure 5.122 *Example of System configuration*

2) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters in all Phoenix G2 IDUs. Set the same one frequency channel for Channel 1 and Channel 2 in both Primary and Secondary IDUs.

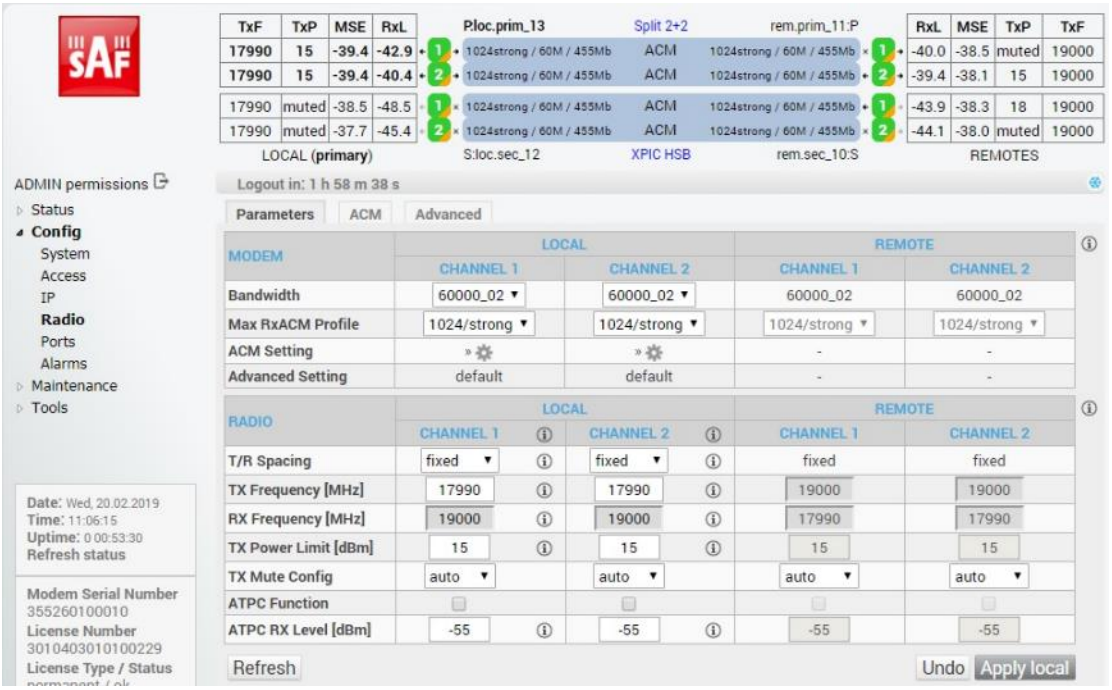


Figure 5.123 *Example of Radio configuration*

3) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU



Figure 5.124 *Example of IP configuration*

4) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote in all Phoenix G2 IDUs. This will enable management access to other IDUs in the link via NAT.

With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible: 2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the local secondary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:2443

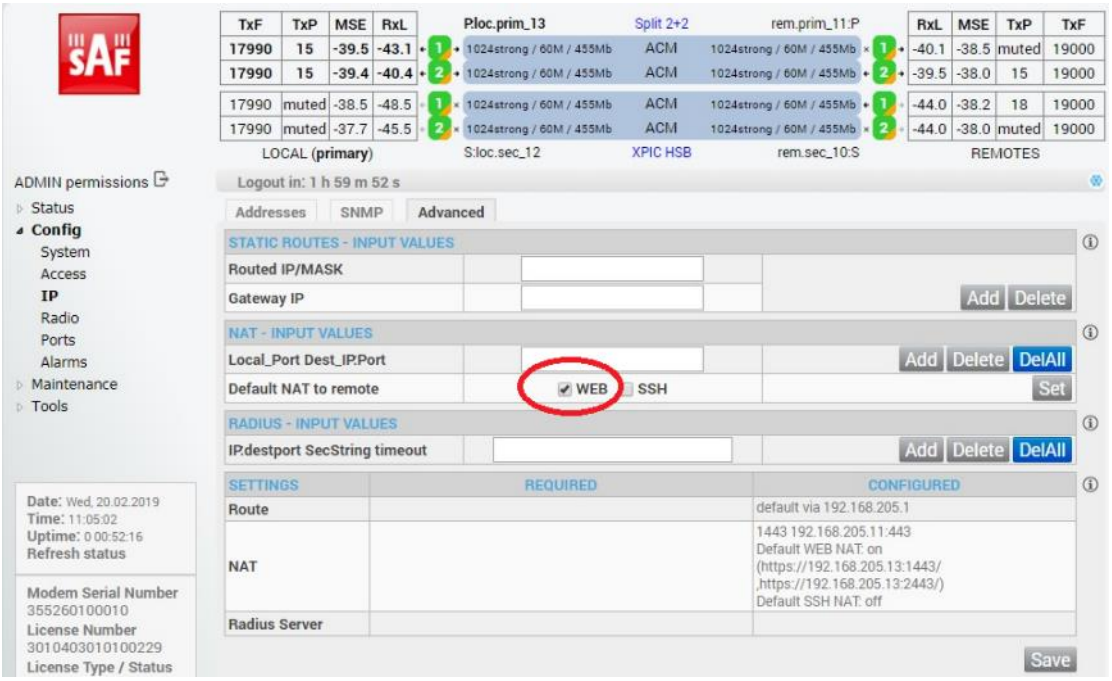


Figure 5.125 *Example of IP NAT configuration*

5) Port group configuration must be done according to customer requirements. The requirement in this example is to have one LAN port for Ethernet traffic. In this case LAN1 port will be used for the Ethernet traffic – it must be allocated in one group with one of WAN ports, in this case it is WANa port (Group1). LAN3 port will be used for management access, it is allocated in one group with MNG port (Group3). As the NAT

is used for remote management access, it is not necessary to add management access ports to any of WAN ports. LAN2 and WANb ports will not be used in this example and will be allocated in Group2. Port grouping configuration is available in web GUI '*Config->Ports->EthVLAN*' section and must be done in all Phoenix G2 IDUs

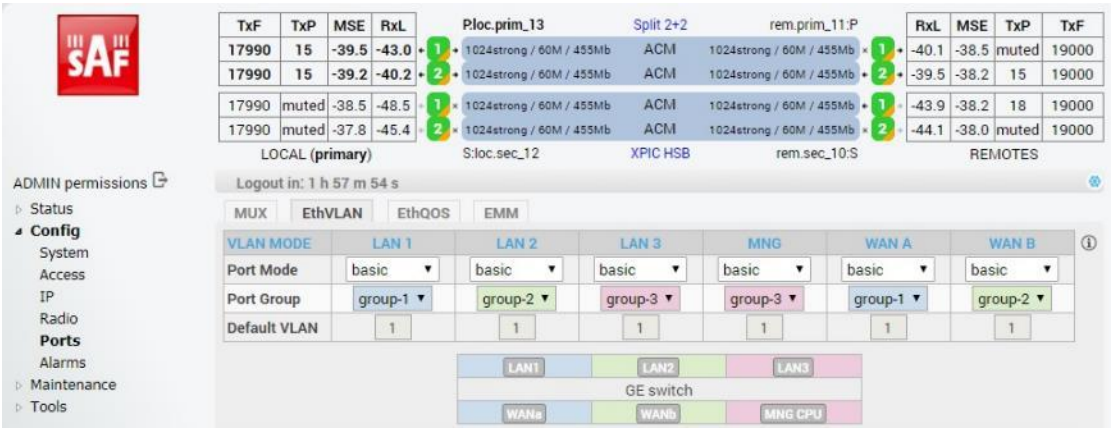


Figure 5.126 *Example of port grouping*

6) In web GUI '*Config->Ports->MUX*' specify Data channel and port speed for WAN (radio direction) port and SFP ports in all 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.The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary) are interconnected successfully, the SFP1 and SFP2 ports must be automatically indicated as connected in Mode 'force2G5'

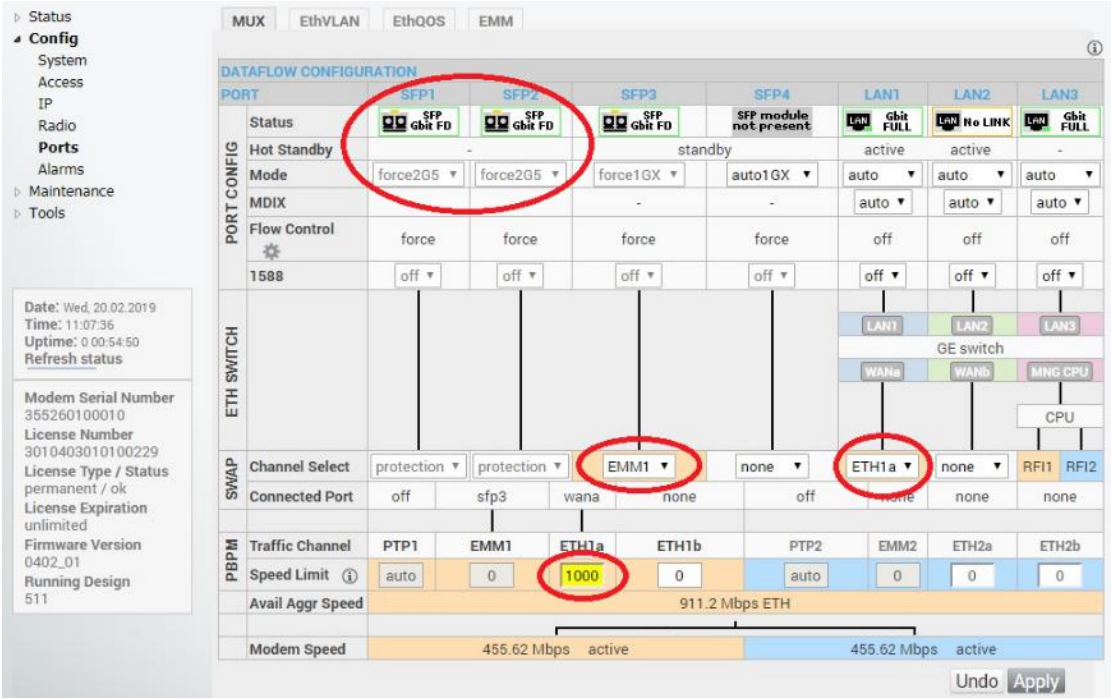


Figure 5.127 *Example of port configuration*

7) Configure EMM according to customer requirements and basing on EMM configuration description described in section '*Config->Ports->EMM*' in all Phoenix G2 IDUs.
8) In web GUI '*Config →Alarms →General*' configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label) in all Phoenix G2 IDUs. In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM

connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

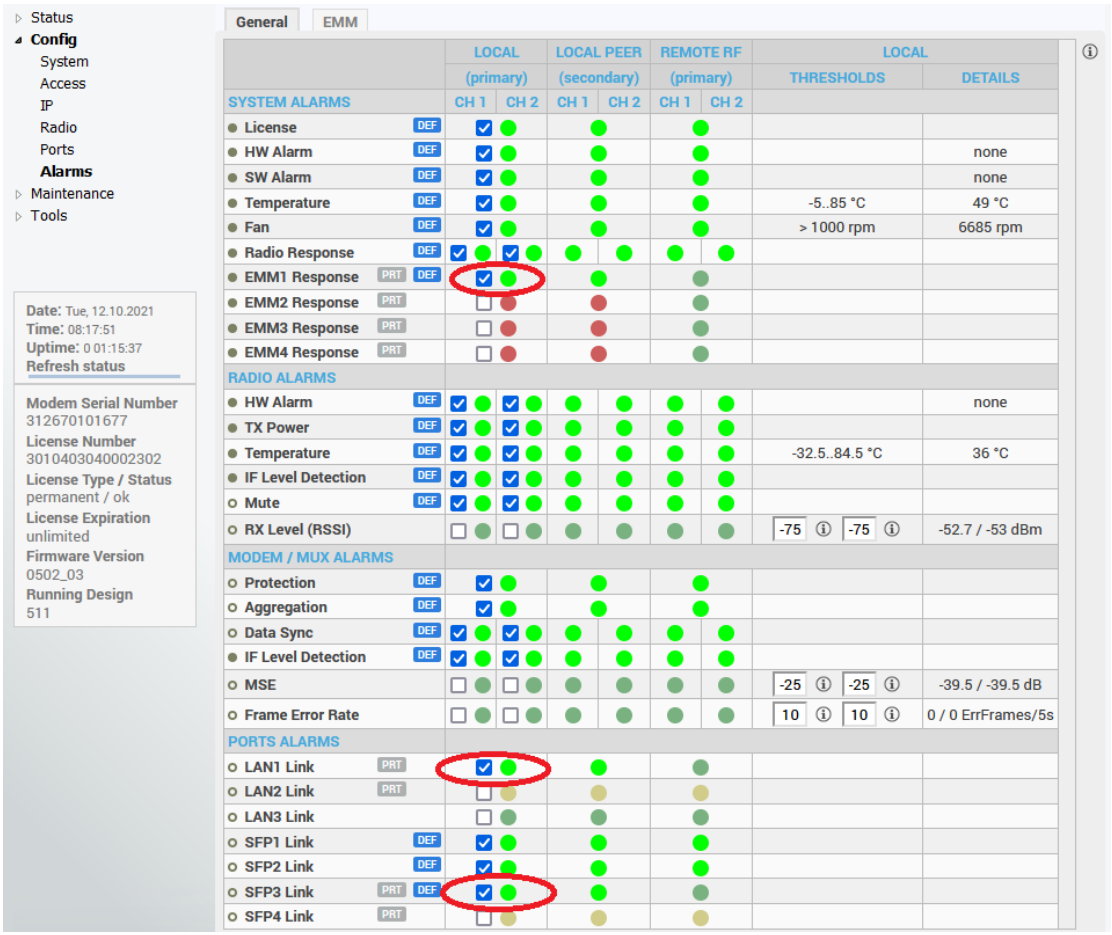


Figure 5.128a *Example of alarm configuration*

9) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

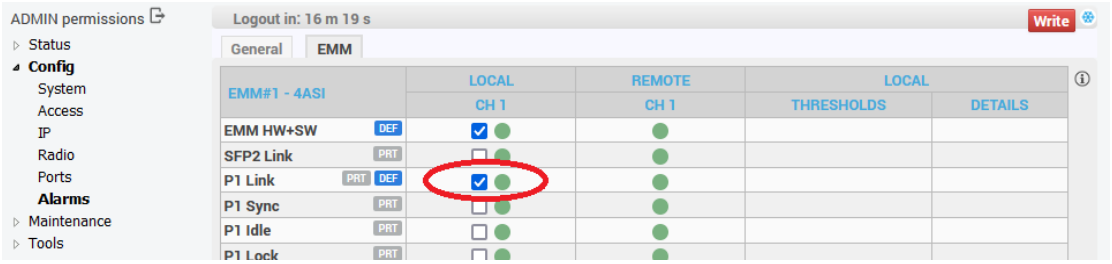


Figure 5.128b *Example of alarm configuration*

10) Save new settings by pressing Write button.
11) Reboot all 4 IDUs after successful reconfiguration
12) In web GUI '*Config->System->Mode*' set Hot-Swap Startup device Role to 'Auto primary' for both Primary IDUs and to 'Auto Secondary' for both Secondary IDUs in order to enable protection mode on all Phoenix G2 IDUs

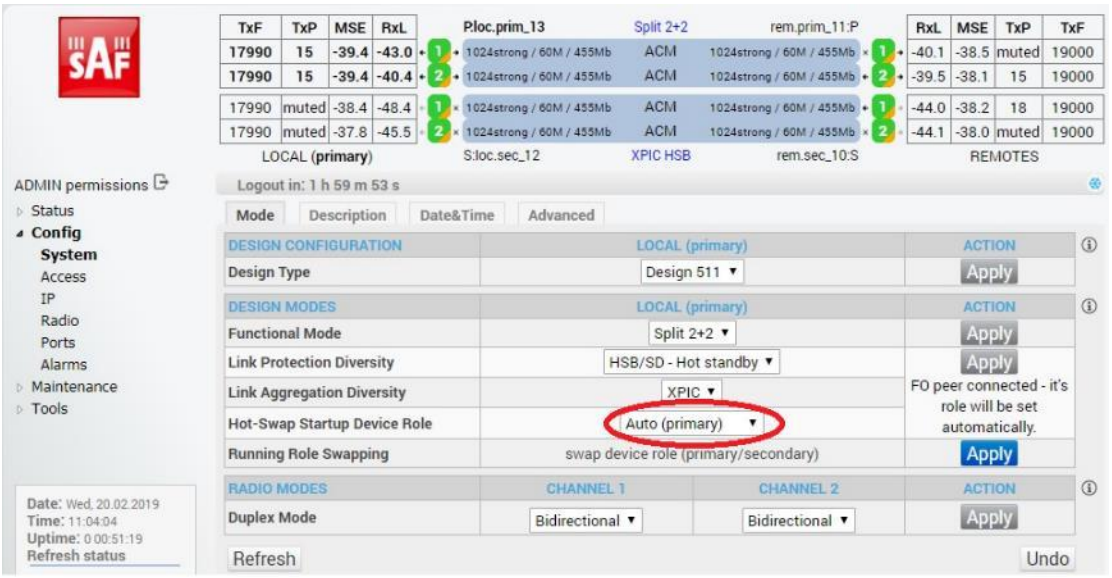


Figure 5.129 *Example of system configuration in Auto mode*

13) Save new settings by pressing Write button.

The status of the link and its configuration is displayed in the header of the web GUI. The status of the IDU which currently is monitored is displayed in Bold and is indicated as LOCAL (primary) or LOCAL (secondary):

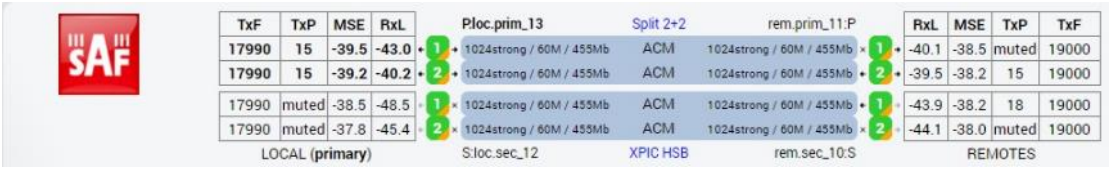


Figure 5.130 *Status of 2+2 XPIC aggregation HSB/SD protection mode*

Example 13 – 2+2 XPIC aggregation FD protection mode (Design 511)

The 2+2 XPIC (Cross-polarization Interference Cancellation) aggregation FD (Frequency Diversity) protection mode is the mode supporting link aggregation which is protected using FD protection method. In this case two data Channels are used for data aggregation (Channel 1 and Channel 2) and two Channels are used for protection of aggregation channels. Both Aggregation Channels use the same one frequency channel, both Protection channels use another frequency channel for FD protection.

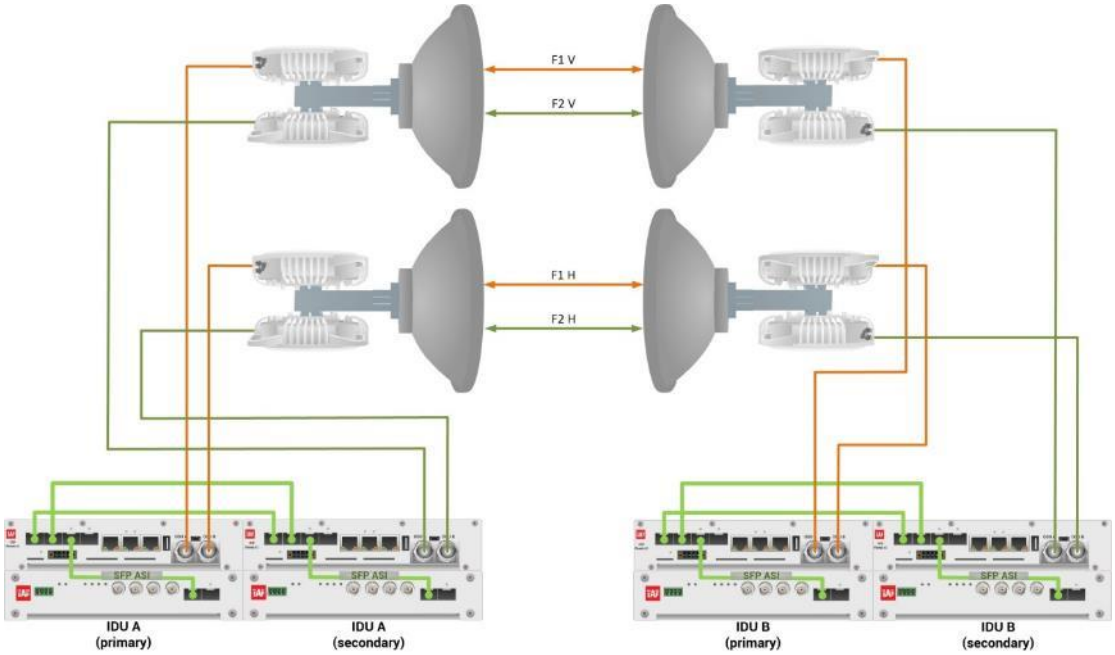


Figure 5.131a *Example of 2+2 XPIC aggregation FD protection scheme*

Figure 5.131a shows 2+2 XPIC aggregation FD protection scheme where one frequency channel is used in both Horizontal and Vertical polarizations for Primary IDU/ODUs, and another frequency channel is used in both polarizations for Secondary IDU/ODUs. Couplers are used to interconnect 2 ODUs to one antenna in this scheme. In this connection scheme the ODUs and couplers can be substituted with IRFUs and IBUs combination if required by customer.

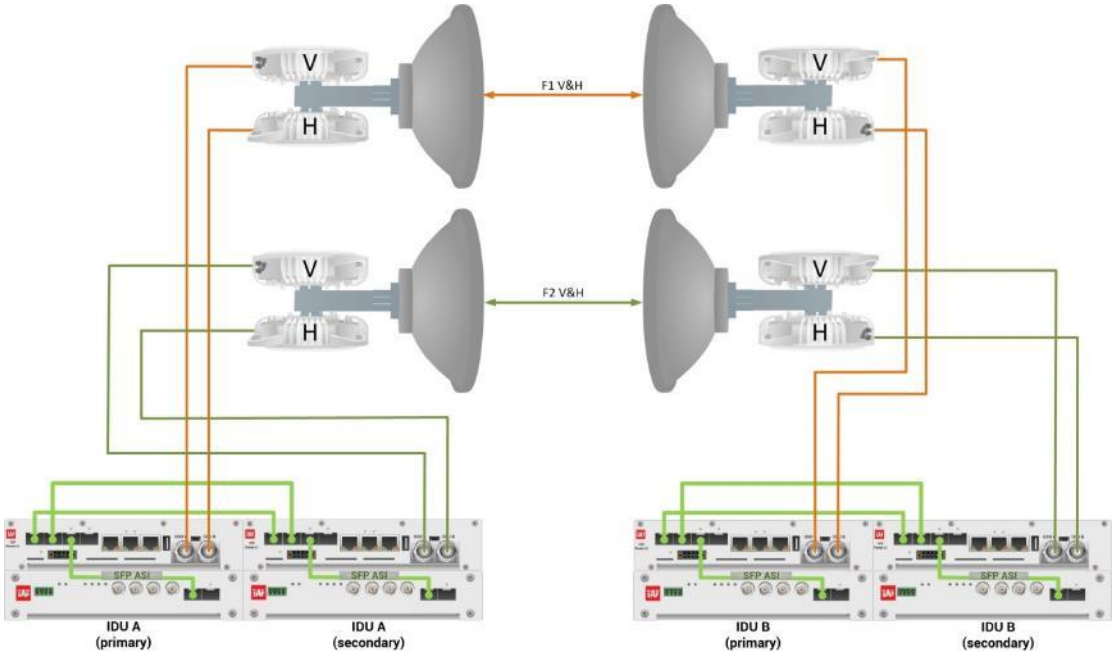


Figure 5.131b *Example of 2+2 XPIC aggregation FD protection scheme*

Figure 5.131b shows 2+2 XPIC aggregation FD protection scheme where one frequency channel is used in both Horizontal and Vertical polarizations for Primary IDU/ODUs, and another frequency channel is used in both polarizations for Secondary IDU/ODUs. OMTs are used to interconnect 2 ODUs to one antenna in this scheme.

This example describes an application where the Design Type 'Design 511', Functional mode 'Split 2+2', Link Aggregation Diversity 'XPIC' and Link Protection Diversity 'FD – Freq. diversity' are selected on both sides of the link. The modulation is 1024QAM in BW 60 MHz and the appropriate maximal data speed is about 455 Mbps per channel. ASI traffic is passed through the link. **This scheme requires four Phoenix G2 IDUs and eight ODUs per link.**



Both IDUs in each side of the link are interconnected with 2 optical cables on ports SFP1 and SFP2. 2.5 GB SFP modules must be used for this interconnection. SFP3 or SFP4 port can be used for the IDU interconnection with ASI EMM module.

Configuration steps for 2+2 XPIC aggregation FD protection is following:

1) In web GUI '*Config->System->Mode*' choose design type 'Design 511', Functional mode 'Split 2+2', Link Protection Diversity 'FD – Freq. diversity', Link Aggregation Diversity 'XPIC'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed primary' on both Primary IDUs and as 'Fixed secondary' on both Secondary IDUs. The Duplex Mode must be set to 'Bidirectional' for both channels on all Phoenix G2 IDUs

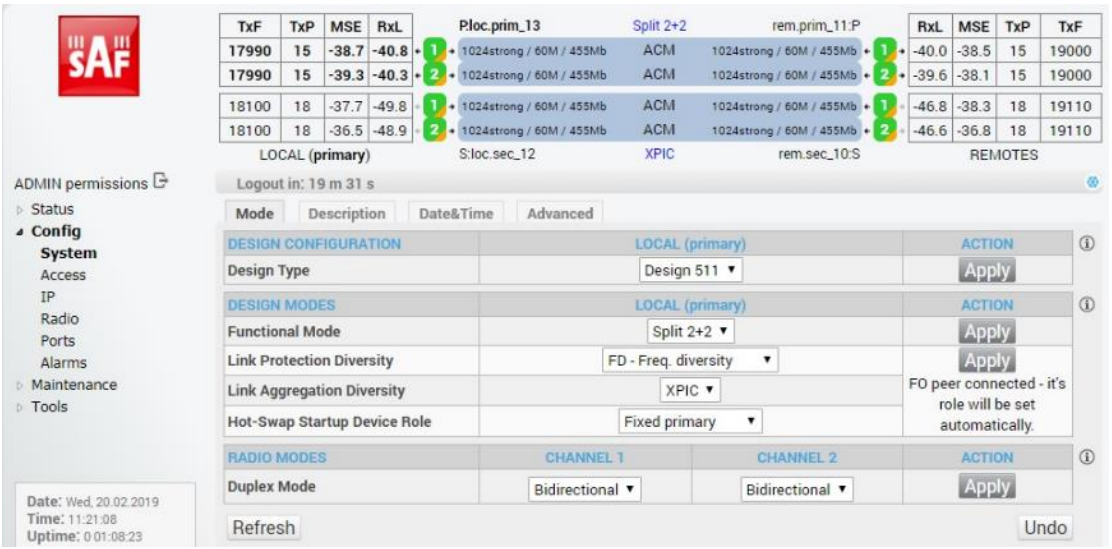


Figure 5.132 *Example of System configuration*

2) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters in all Phoenix G2 IDUs. Set the same one frequency channel for Channel 1 and Channel 2 in both the Primary IDUs and another frequency channel for Channel 1 and Channel 2 in the Secondary IDUs

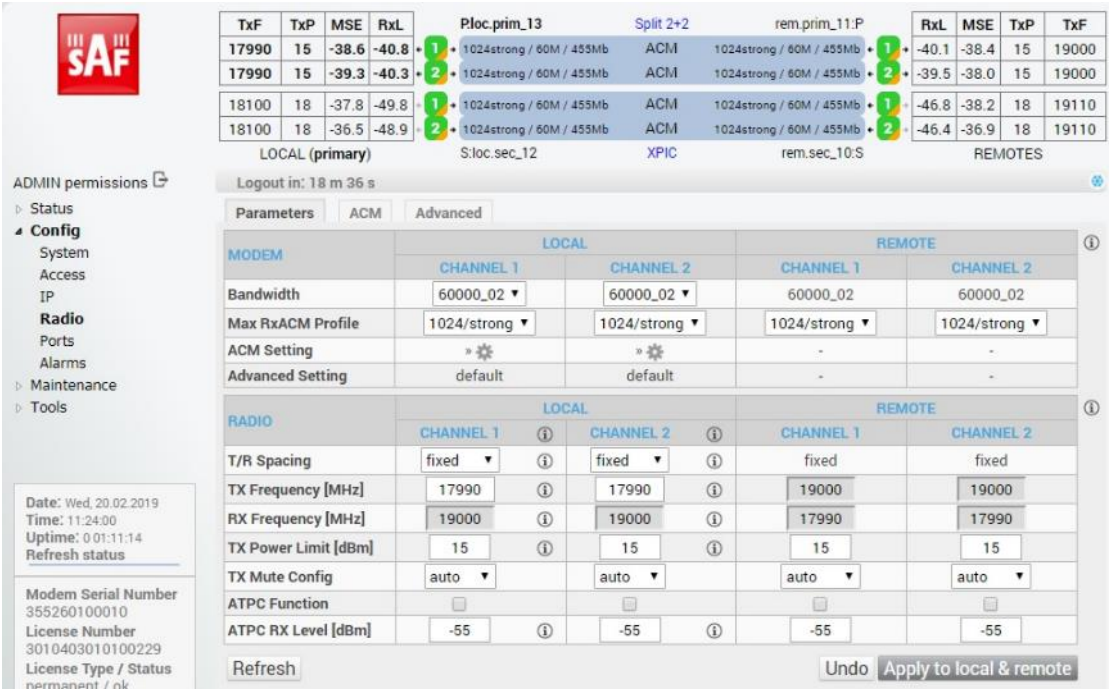


Figure 5.133 *Example of Primary IDU Radio configuration*

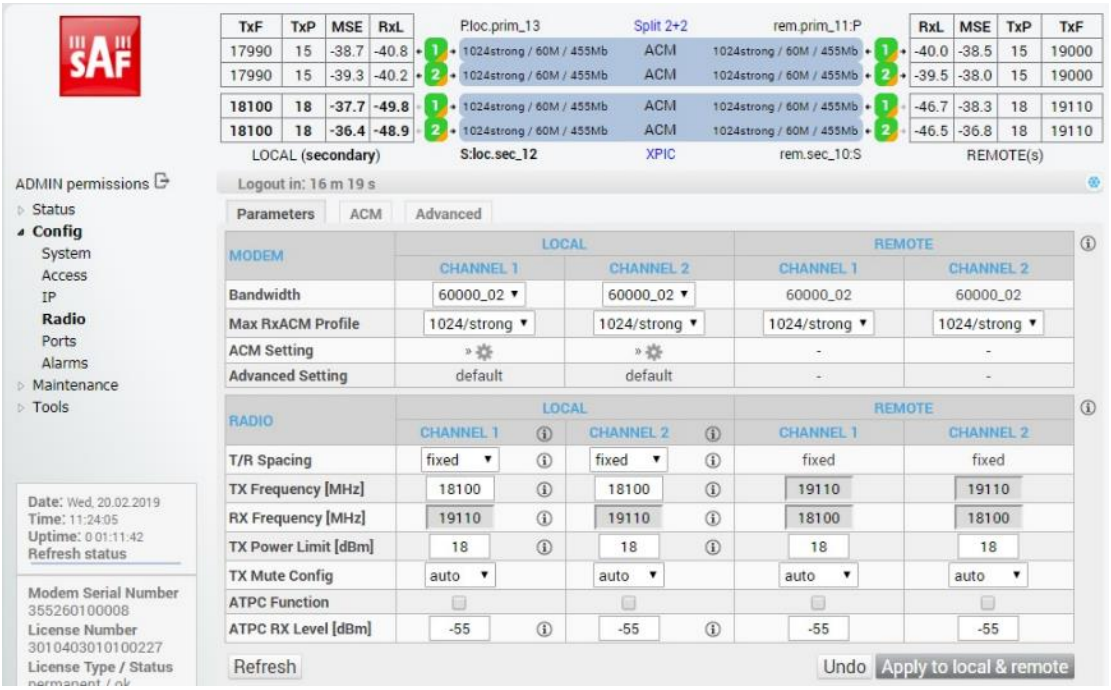


Figure 5.134 *Example of Secondary IDU Radio configuration*

3) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU



Figure 5.135 *Example of IP configuration*

4) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote in all Phoenix G2 IDUs. This will enable management access to other IDUs in the link via NAT.

With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible: 2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the local secondary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:2443

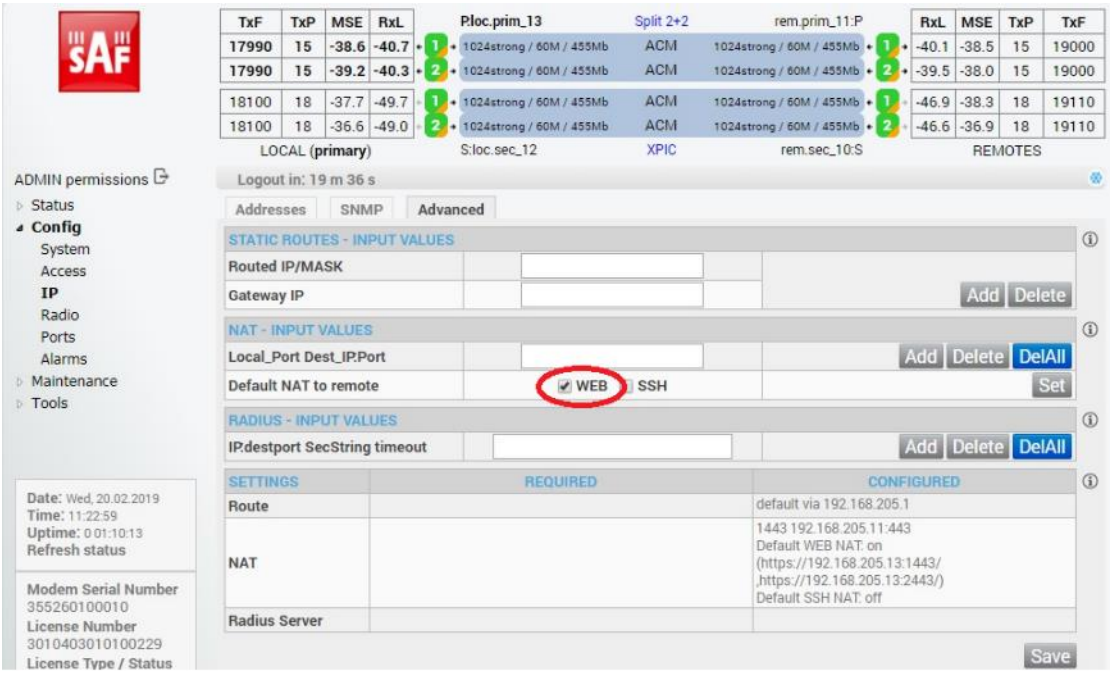


Figure 5.136 *Example of IP NAT configuration*

5) Port group configuration must be done according to customer requirements. The requirement in this example is to have one LAN port for Ethernet traffic. In this case LAN1 port will be used for the Ethernet traffic – it must be allocated in one group with one of WAN ports, in this case it is WANa port (Group1). LAN3 port will be used for management access, it is allocated in one group with MNG port (Group3). As the NAT is used for remote management access, it is not necessary to add management access

ports to any of WAN ports. LAN2 and WANb ports will not be used in this example and will be allocated in Group2. Port grouping configuration is available in web GUI '*Config->Ports->EthVLAN*' section and must be done in all Phoenix G2 IDUs

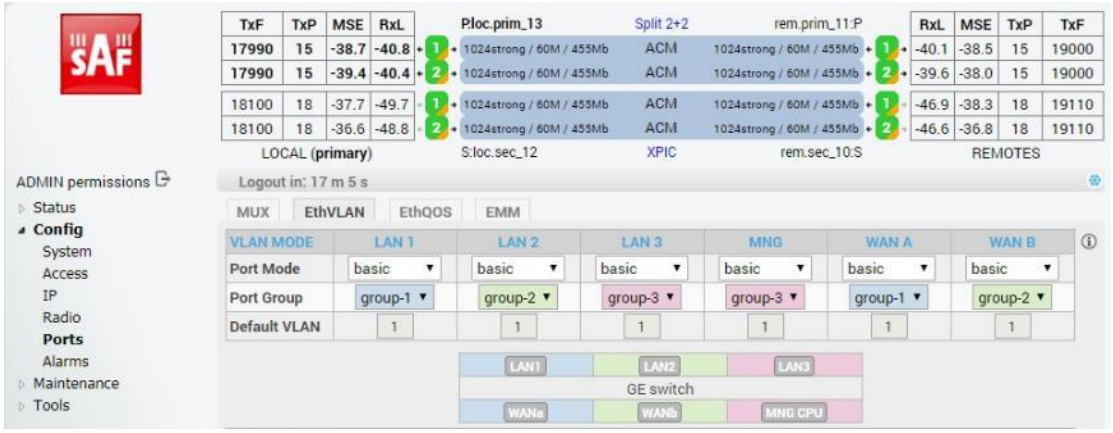


Figure 5.137 *Example of port grouping*

6) In web GUI '*Config->Ports->MUX*' specify Data channel and port speed for WAN (radio direction) port and SFP ports in all 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.The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary) are interconnected successfully, the SFP1 and SFP2 ports must be automatically indicated as connected in Mode 'force2G5'

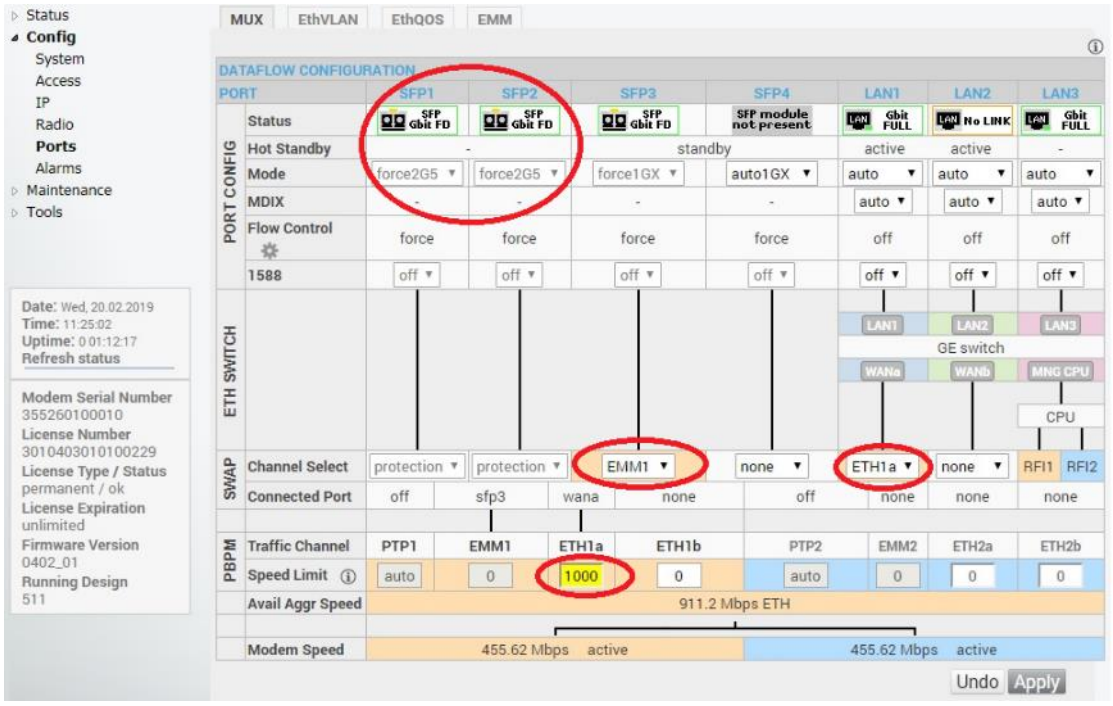


Figure 5.138 *Example of port configuration*

7) Configure EMM according to customer requirements and basing on EMM configuration description described in section '*Config->Ports->EMM*' in all Phoenix G2 IDUs.
8) In web GUI '*Config →Alarms →General*' configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label) in all Phoenix G2 IDUs. In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

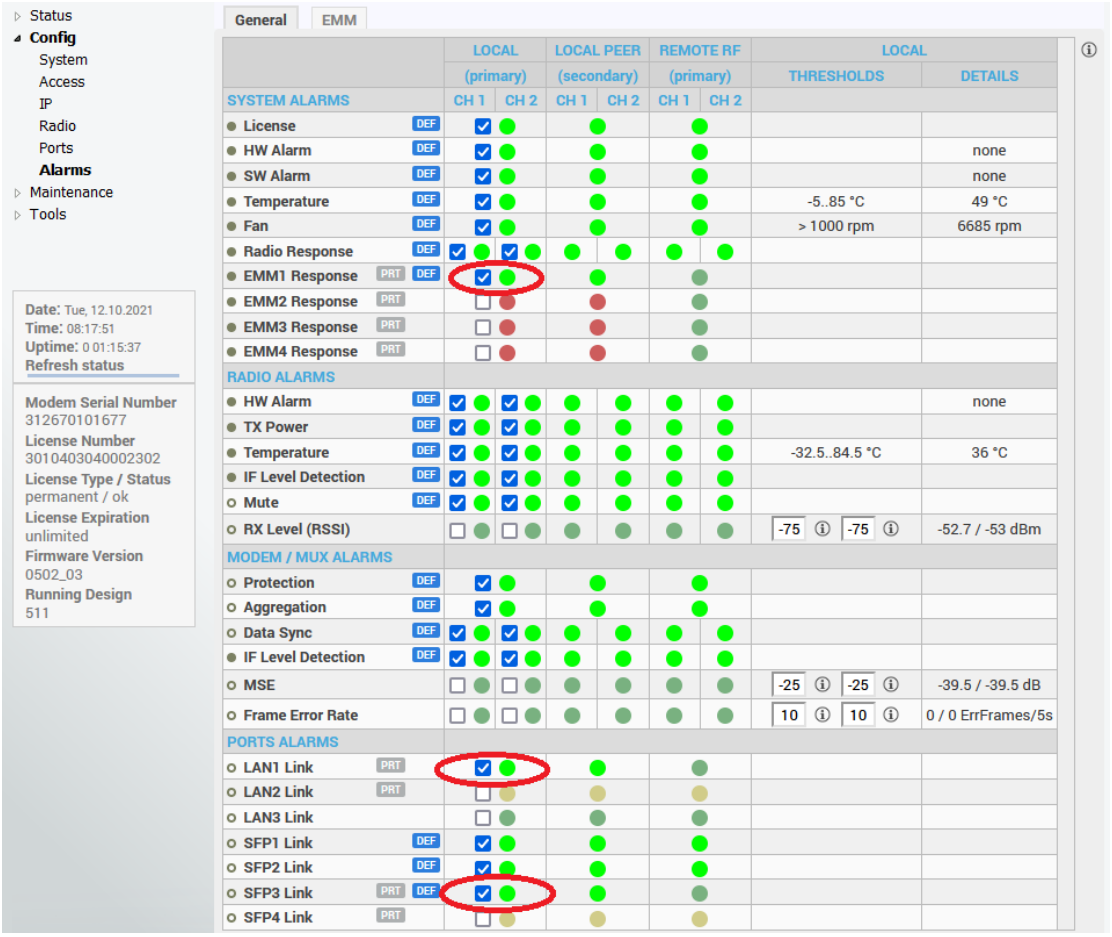


Figure 5.139a *Example of alarm configuration*

9) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

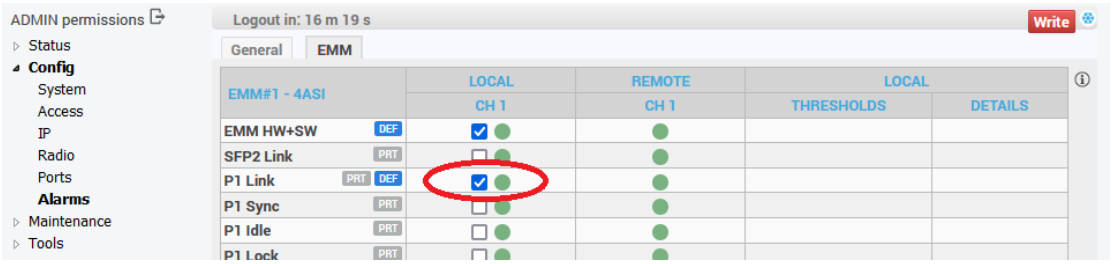


Figure 5.139b *Example of alarm configuration*

10) Save new settings by pressing Write button.
11) Reboot all 4 IDUs after successful reconfiguration
12) In web GUI '*Config->System->Mode*' set Hot-Swap Startup device Role to 'Auto primary' for both Primary IDUs and to 'Auto Secondary' for both Secondary IDUs in order to enable protection mode on all Phoenix G2 IDUs

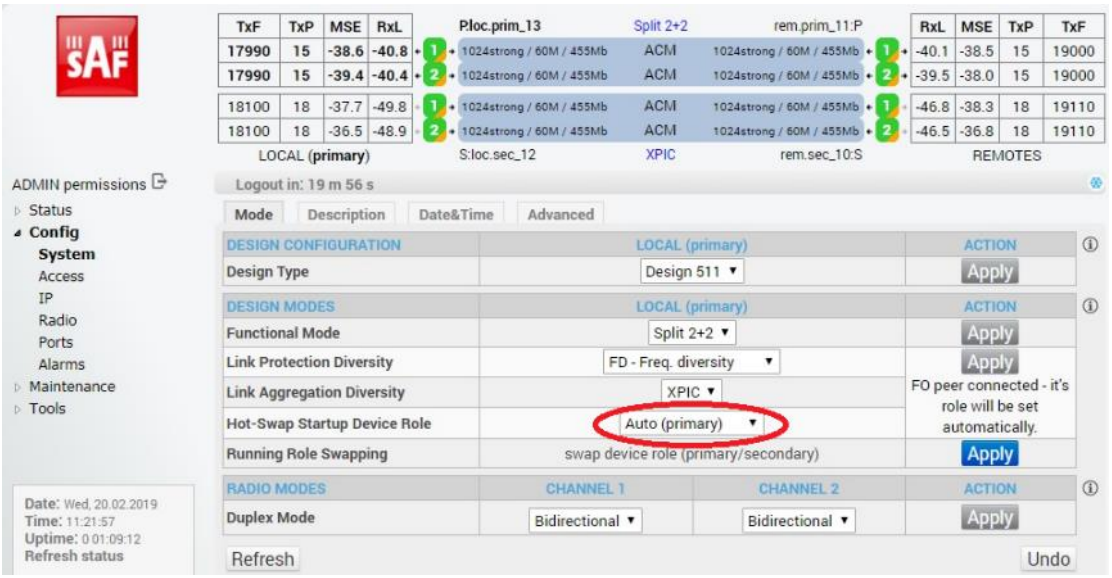


Figure 5.140 *Example of system configuration in Auto mode*

13) Save new settings by pressing Write button.

The status of the link and its configuration is displayed in the header of the web GUI. The status of the IDU which currently is monitored is displayed in Bold and is indicated as LOCAL (primary) or LOCAL (secondary):

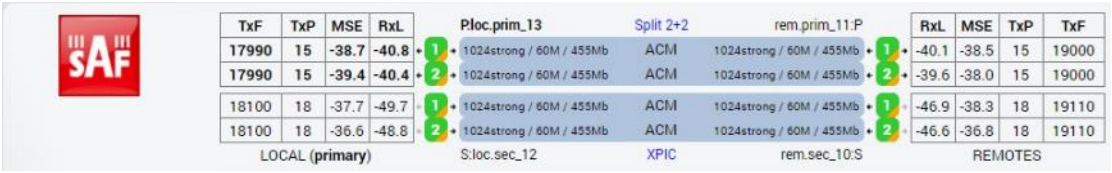


Figure 5.141 *Status of 2+2 XPIC aggregation FD protection mode*

Example 14 – 1+1 HSB/SD Full protection mode (Design 511/513)

The 1+1 HSB/SD (Hot Stnadby/Space Diversity) full protection mode besides the ODU, IDU-ODU cable and modem failure protection adds protection also against HW failures such as IDU power failure, ETH port failure, Primary-EMM and Secondary interconnection failure and EMM failure. When any of these events occurs the Secondary IDU is automatically reconfigured to become Primary IDU and its data ports are automatically enabled for traffic while the original primary, now the secondary, is simultaneously set so the Tx direction is still working but received data from EMM ports are dropped out.

The usage of an external ETH switch with automatic ARP table flushing is required for proper LAN and SFP2 data switch-over. To avoid an unnecessary data drop the new Primary unit will remain in its Primary role even when the original reason for switching has disappeared. Note that the LAN3 port is intended for management connection and it cannot be protected (automatically enabled/disabled) like other ports

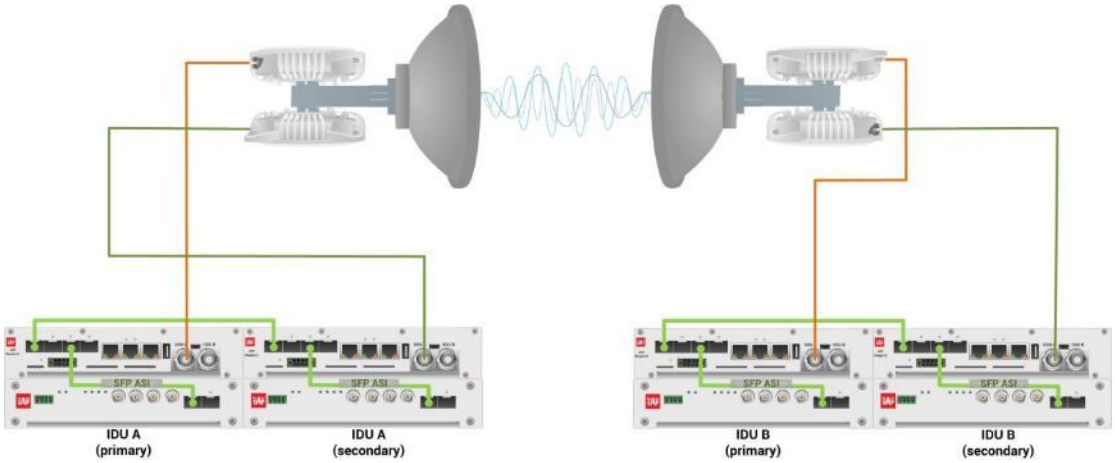


Figure 5.142a *Example of 1+1 HSB full protection scheme*

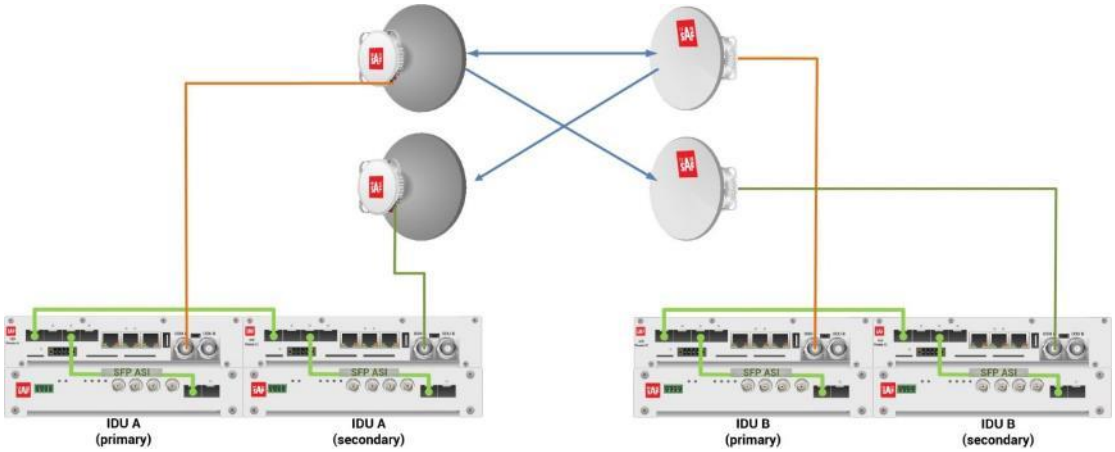


Figure 5.142b *Example of 1+1 SD full protection scheme*

This example describes an application where the Design Type 'Design 511' or 'Design 513', Functional mode 'Split 1+1', Link Protection Diversity 'HSB/SD – Hot standby' are selected on both sides of the link. The modulation is 1024QAM in BW 60 MHz and the appropriate maximal data speed is about 455 Mbps. ASI traffic is passed through the link. **This scheme requires four Phoenix G2 IDUs and eight ODUs per link.**

Both IDUs in each side of the link are interconnected with optical cable on ports SFP1. 2.5 GB SFP modules must be used for this interconnection. SFP3 or SFP4 port can be used for the IDU interconnection with ASI EMM module.

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

1) In web GUI '*Config->System->Mode*' choose design type 'Design 511' or 'Design 513', Functional mode 'Split 1+1', Link Protection Diversity 'HSB/SD – Hot standby'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed primary' on both Primary IDUs and as 'Fixed secondary' on both Secondary IDUs. The Duplex Mode must be set to 'Bidirectional' for both channels on all Phoenix G2 IDUs

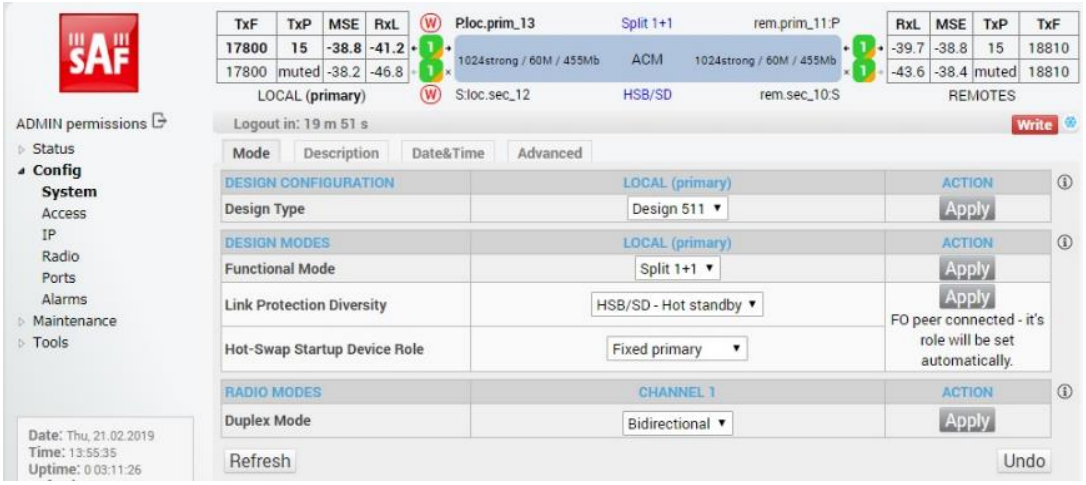


Figure 5.143 *Example of System configuration*

2) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters in all Phoenix G2 IDUs. Set the same one frequency channel in all Phoenix G2 IDUs



Figure 5.144 *Example of Radio configuration*

3) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU



Figure 5.145 *Example of IP configuration*

4) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote in all Phoenix G2 IDUs. This will enable management access to other IDUs in the link via NAT.



With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible: 2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the local secondary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:2443

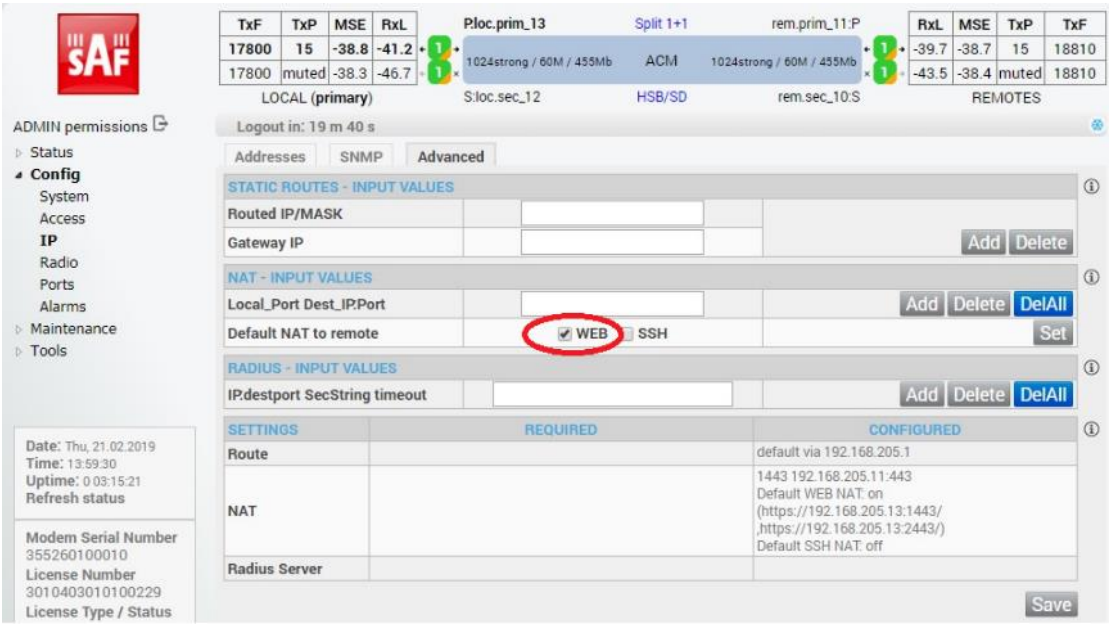


Figure 5.146 *Example of IP NAT configuration*

5) Port group configuration must be done according to customer requirements. The requirement in this example is to have one LAN port for Ethernet traffic. In this case LAN1 port will be used for the Ethernet traffic – it must be allocated in one group with one of WAN ports, in this case it is WANa port (Group1). LAN3 port will be used for management access, it is allocated in one group with MNG port (Group3). As the NAT is used for remote management access, it is not necessary to add management access ports to any of WAN ports. LAN2 and WANb ports will not be used in this example and will be allocated in Group2. Port grouping configuration is available in web GUI '*Config->Ports->EthVLAN*' section and must be done in all Phoenix G2 IDUs



Figure 5.147 *Example of port grouping*

6) In web GUI '*Config->Ports->MUX*' specify Data channel and port speed for WAN (radio direction) port and SFP ports in all 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.The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary) are interconnected successfully, the SFP1 port must be automatically indicated as connected in Mode 'force2G5'

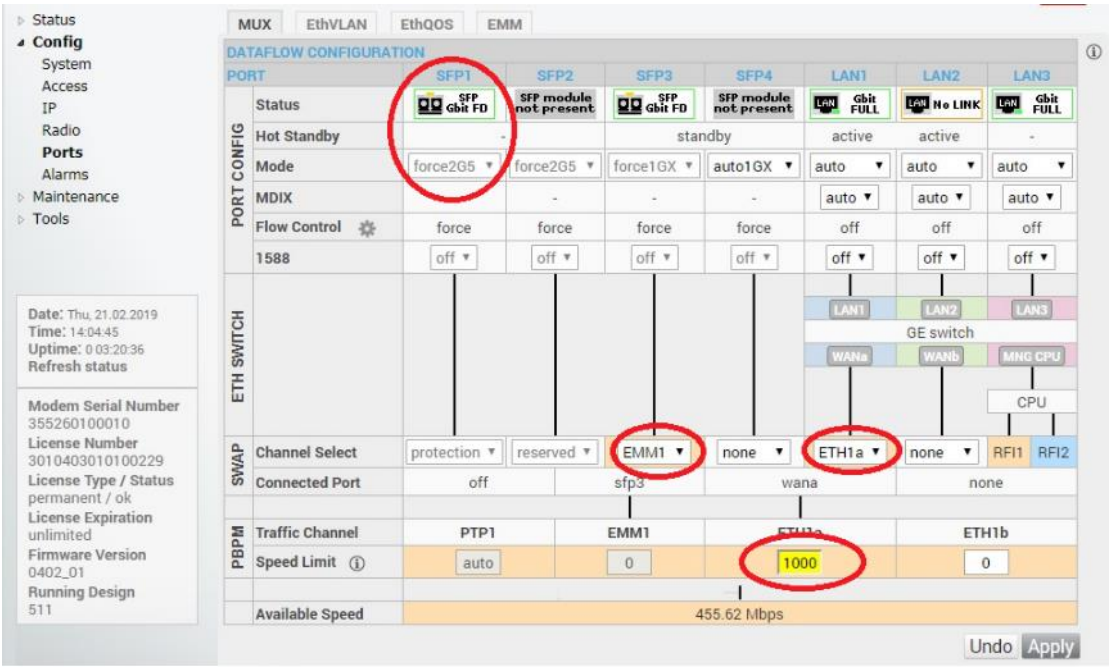


Figure 5.148 *Example of port configuration*

7) Configure EMM according to customer requirements and basing on EMM configuration description described in section '*Config->Ports->EMM*' in all Phoenix G2 IDUs.
8) In web GUI '*Config →Alarms →General*' configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label) in all Phoenix G2 IDUs. In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

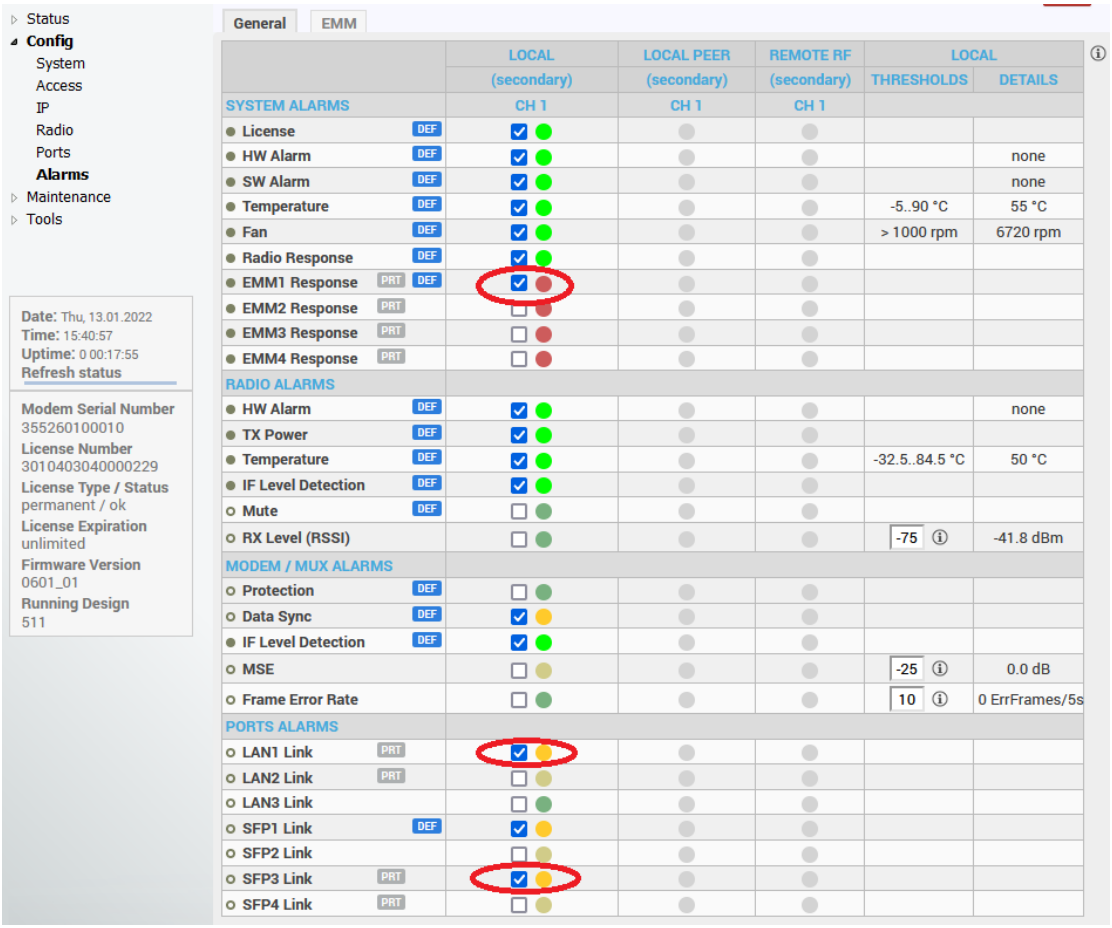


Figure 5.149a *Example of alarm configuration*

9) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

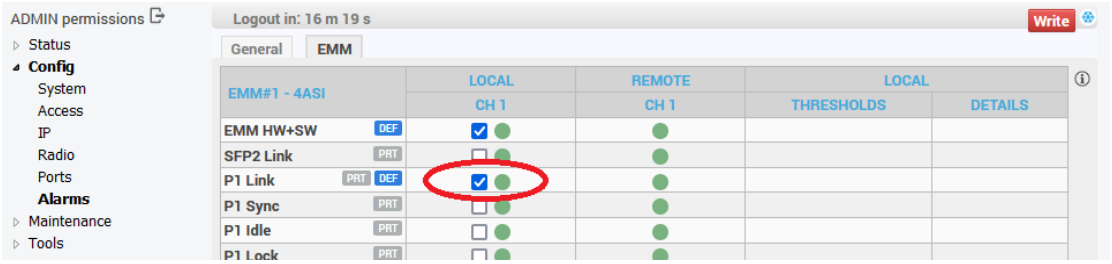


Figure 5.149b *Example of alarm configuration*

10) Save new settings by pressing Write button.
11) Reboot all 4 IDUs after successful reconfiguration
12) In web GUI '*Config->System->Mode*' set Hot-Swap Startup device Role to 'Auto primary' for both Primary IDUs and to 'Auto Secondary' for both Secondary IDUs in order to enable protection mode on all Phoenix G2 IDUs

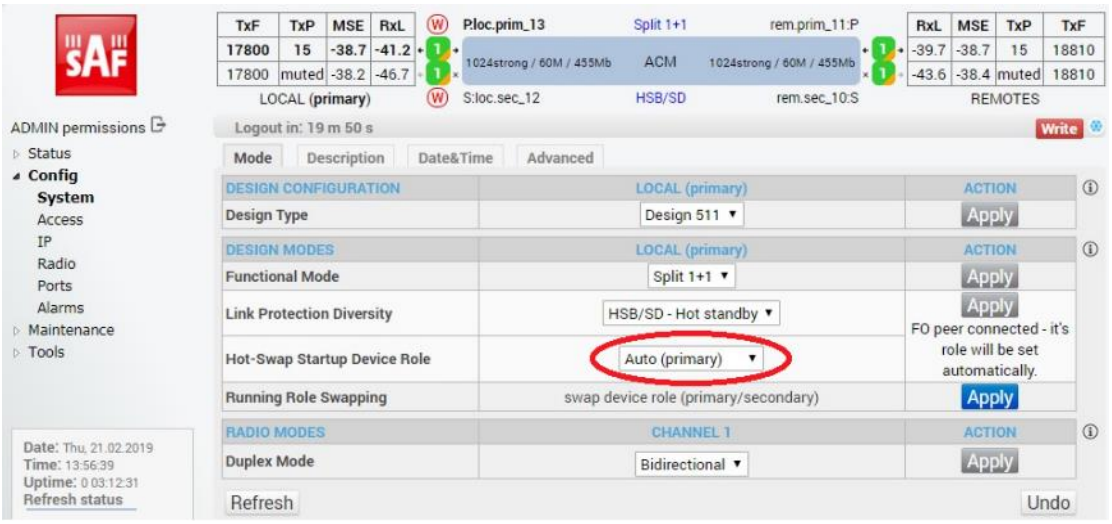


Figure 5.150 *Example of system configuration in Auto mode*

13) Save new settings by pressing Write button.

The status of the link and its configuration is displayed in the header of the web GUI. The status of the IDU which currently is monitored is displayed in Bold and is indicated as LOCAL (primary) or LOCAL (secondary):



Figure 5.151 *Status of 1+1 HSB/SD protection mode*

Example 15 – 1+1 FD Full protection mode (Design 511/513)

The 1+1 FD (Frequency Diversity) full protection mode besides the ODU, IDU-ODU cable and modem failure protection adds protection also against HW failures such as IDU power failure, ETH port failure, Primary-EMM and Secondary interconnection failure and EMM failure. When any of these events occurs the Secondary IDU is automatically reconfigured to become Primary IDU and its data ports are automatically enabled for traffic while the original primary, now the secondary, is simultaneously set so the Tx direction is still working but received data from EMM ports are dropped out.

The usage of an external ETH switch with automatic ARP table flushing is required for proper LAN and SFP2 data switch-over. To avoid an unnecessary data drop the new Primary unit will remain in its Primary role even when the original reason for switching has disappeared. Note that the LAN3 port is intended for management connection and it cannot be protected (automatically enabled/disabled) like other ports

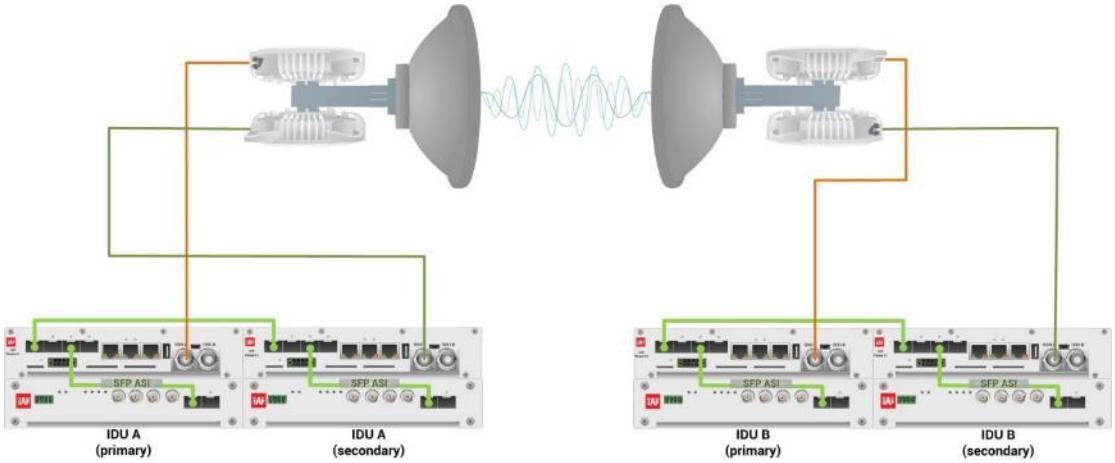


Figure 5.152 *Example of 1+1 FD full protection scheme*

This example describes an application where the Design Type 'Design 511' or 'Design 513', Functional mode 'Split 1+1', Link Protection Diversity 'FD – Freq. diversity' are selected on both sides of the link. The modulation is 1024QAM in BW 60 MHz and the appropriate maximal data speed is about 455 Mbps. ASI traffic is passed through the link. **This scheme requires four Phoenix G2 IDUs and eight ODUs per link.**

Both IDUs in each side of the link are interconnected with optical cable on ports SFP1. 2.5 GB SFP modules must be used for this interconnection. SFP3 or SFP4 port can be used for the IDU interconnection with ASI EMM module.

Configuration steps for 1+1 FD full protection are following:

1) In web GUI '*Config->System->Mode*' choose design type 'Design 511' or 'Design 513', Functional mode 'Split 1+1', Link Protection Diversity 'FD – Freq. diversity'. The setting Hot-Swap Startup device Role during the configuration must be set as 'Fixed primary' on both Primary IDUs and as 'Fixed secondary' on both Secondary IDUs. The Duplex Mode must be set to 'Bidirectional' for both channels on all Phoenix G2 IDUs



Figure 5.153 *Example of System configuration*

2) In web GUI '*Config->Radio->Parameters*' configure basic radio and modem parameters in all Phoenix G2 IDUs. Set one frequency channel on the Primary link and another frequency channel for the Secondary link (FD) in all Phoenix G2 IDUs

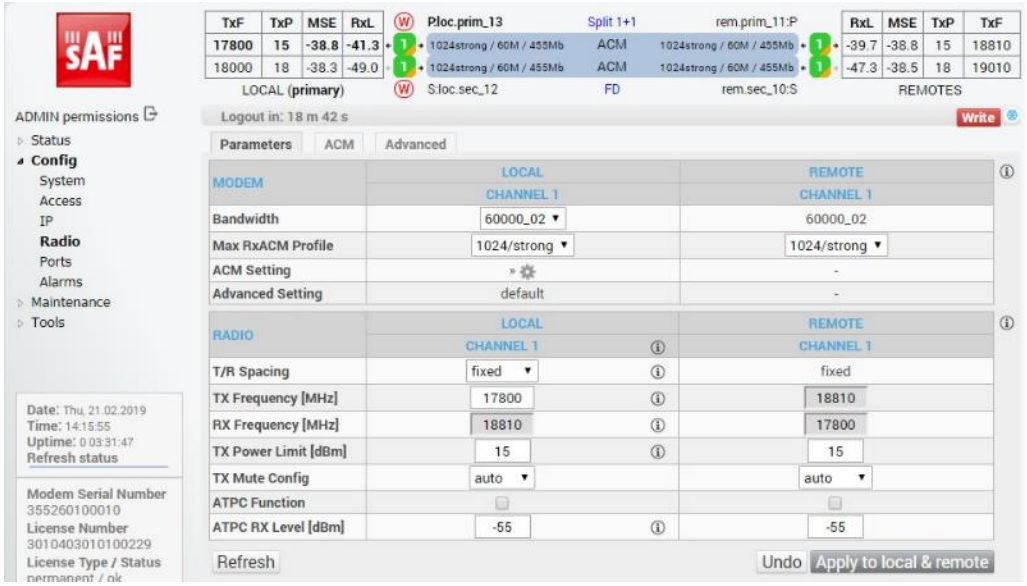


Figure 5.154 *Example of Primary Radio configuration*

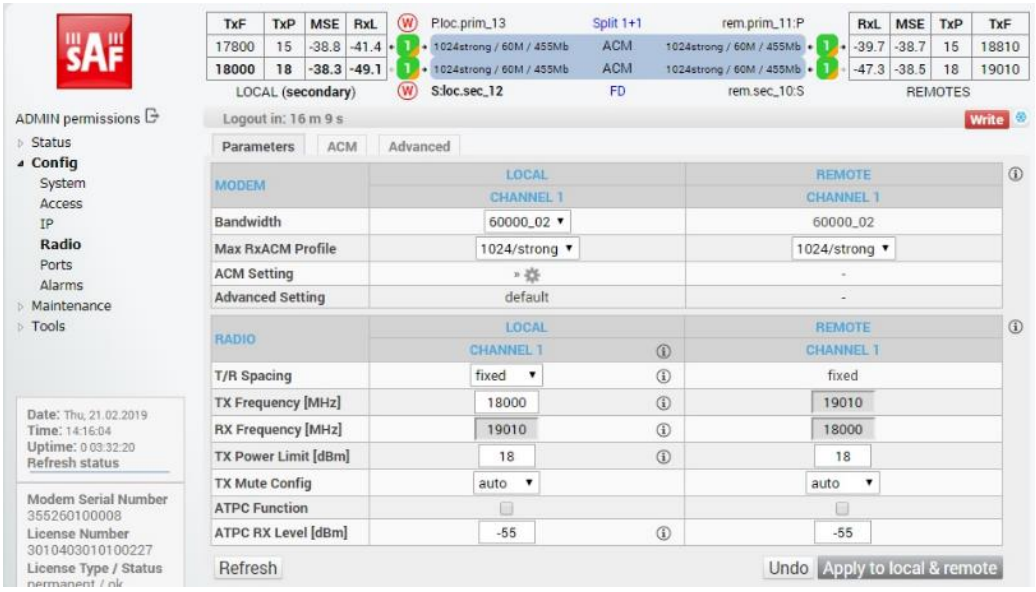


Figure 5.155 *Example of Secondary Radio configuration*

3) In web GUI '*Config->IP->Addresses*' set the IP address of the device. The IP address must be different for each IDU



Figure 5.156 *Example of IP configuration*

4) In web GUI '*Config->IP->Advanced*' set 'WEB' option as Default NAT to remote in all Phoenix G2 IDUs. This will enable management access to other IDUs in the link via NAT.



With NAT configured it is possible to access other IDUs management in the link via IP address of one of IDUs and default NAT ports. Following default NAT ports are possible: 2443 (for local secondary IDU), 1443 (for remote primary IDU), 3443 (for remote secondary IDU). The example of accessing the local secondary IDU via the local primary IDU IP address in this case is: https://192.168.205.13:2443

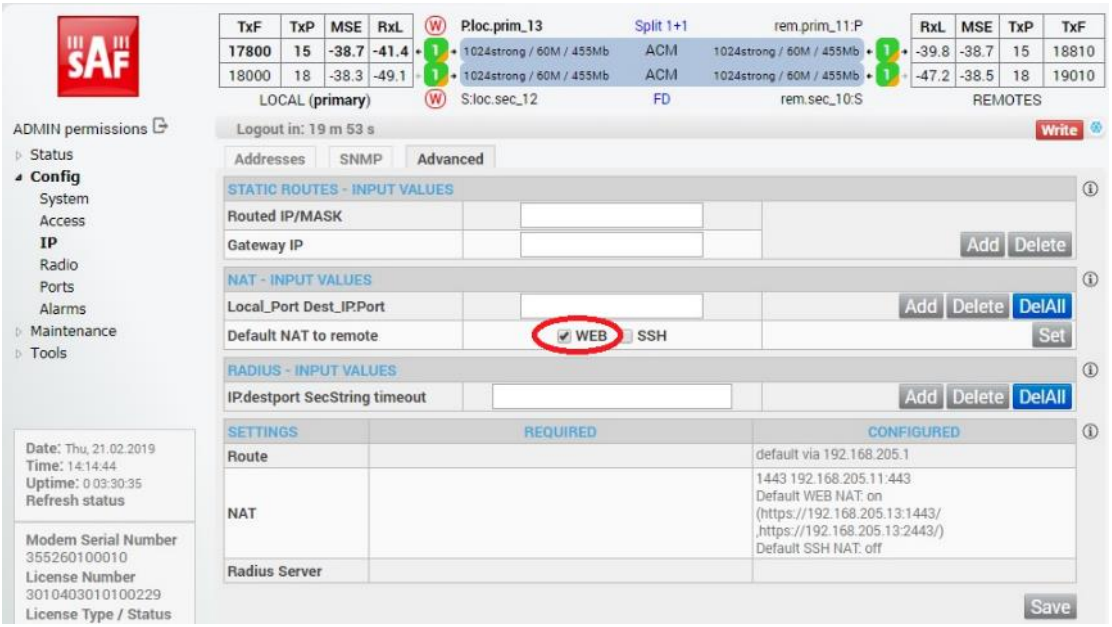


Figure 5.157 *Example of IP NAT configuration*

5) Port group configuration must be done according to customer requirements. The requirement in this example is to have one LAN port for Ethernet traffic. In this case LAN1 port will be used for the Ethernet traffic – it must be allocated in one group with one of WAN ports, in this case it is WANa port (Group1). LAN3 port will be used for management access, it is allocated in one group with MNG port (Group3). As the NAT is used for remote management access, it is not necessary to add management access ports to any of WAN ports. LAN2 and WANb ports will not be used in this example and will be allocated in Group2. Port grouping configuration is available in web GUI '*Config->Ports->EthVLAN*' section and must be done in all Phoenix G2 IDUs

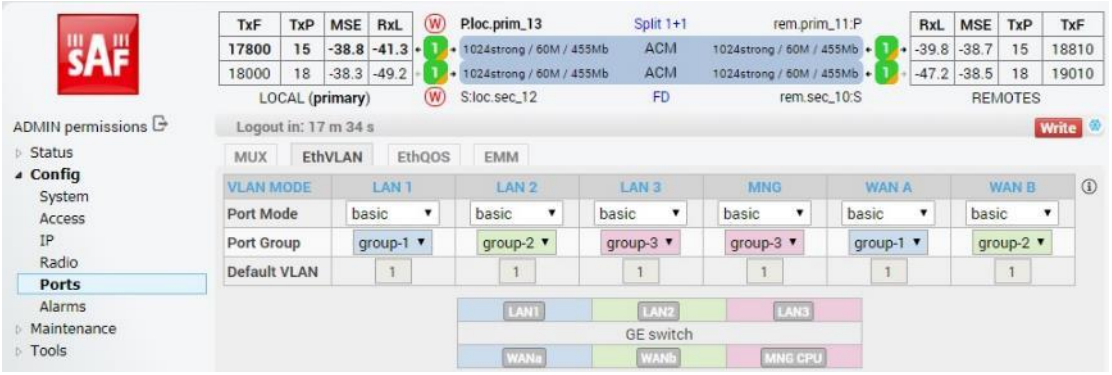


Figure 5.158 *Example of port grouping*

6) In web GUI '*Config->Ports->MUX*' specify Data channel and port speed for WAN (radio direction) port and SFP ports in all 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.The SFP3 port is connected to EMM channel. If both IDUs (Primary and Secondary) are interconnected successfully, the SFP1 port must be automatically indicated as connected in Mode 'force2G5'

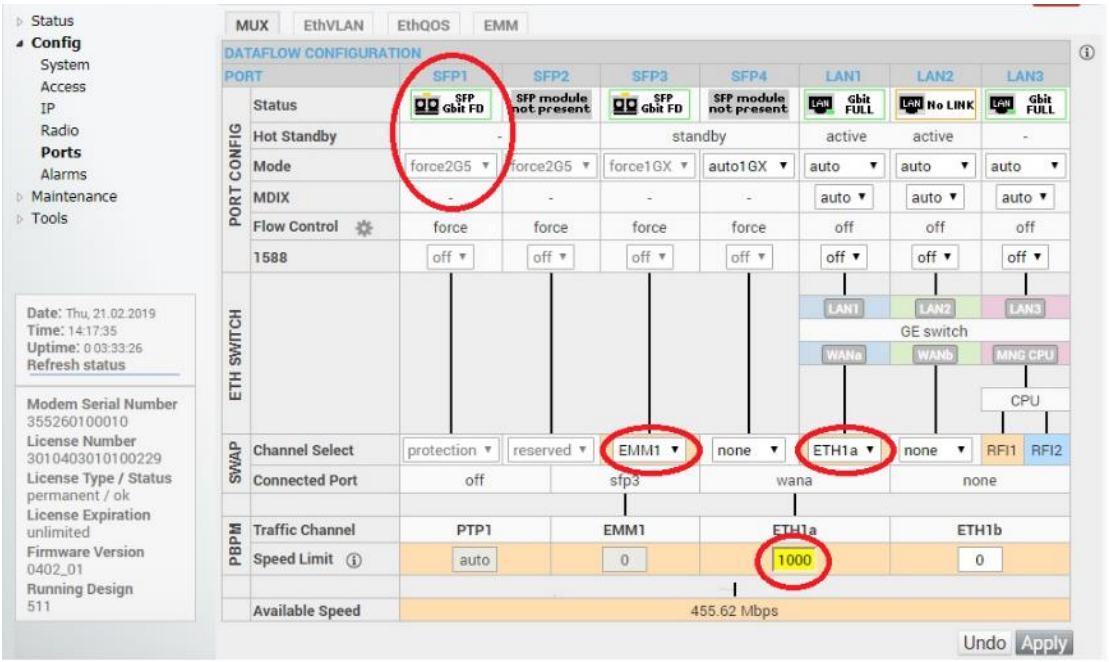


Figure 5.159 *Example of port configuration*

7) Configure EMM according to customer requirements and basing on EMM configuration description described in section '*Config->Ports->EMM*' in all Phoenix G2 IDUs.
8) In web GUI '*Config →Alarms →General*' configure interface (LAN, SFP and EMM1) alarms which will be used for protection switchover (marked with PRT label) in all Phoenix G2 IDUs. In the example LAN1 (for Ethernet traffic) and SFP3 (for ASI EMM connection) are used. Those interface port alarm check-boxes must be checked in order to initiate the switch-over in case of failure of any of those interfaces

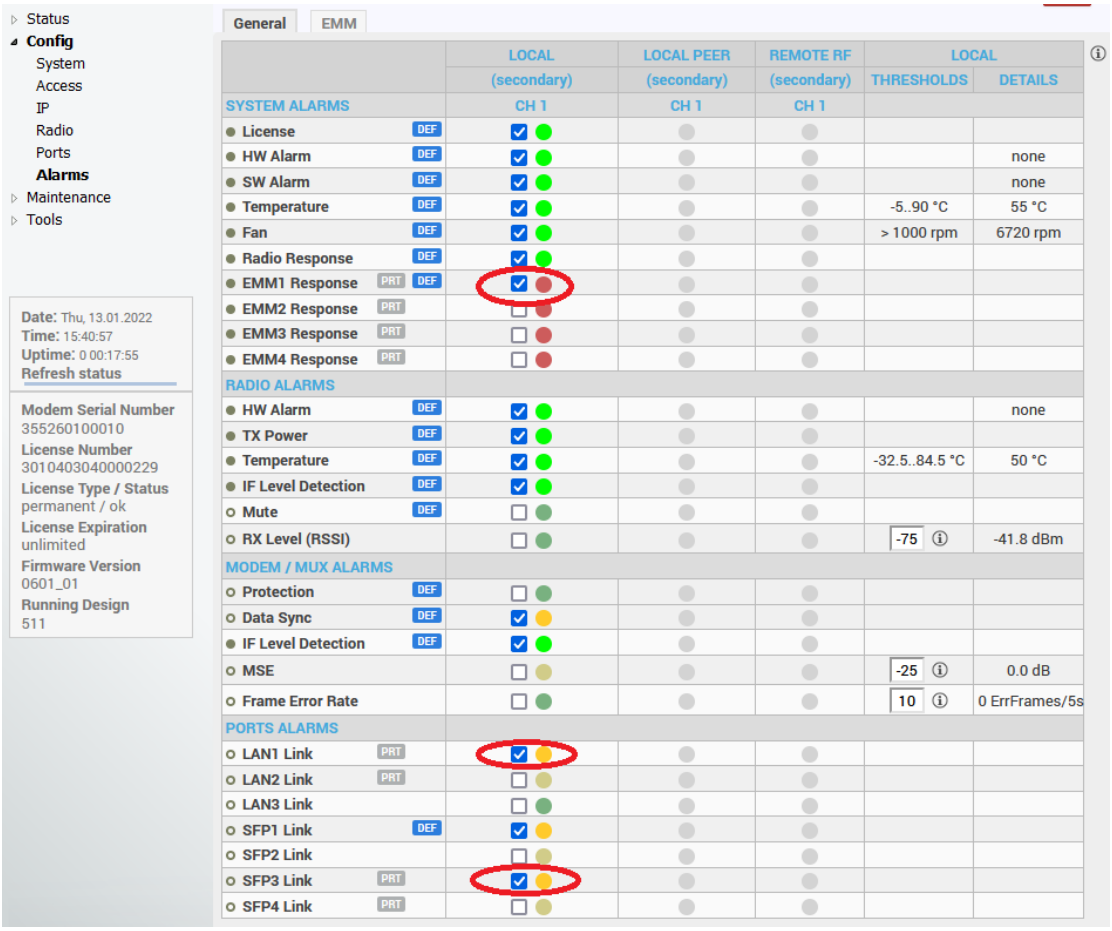


Figure 5.160a *Example of alarm configuration*

9) In web GUI '*Config →Alarms →EMM*' configure EMM port alarms which will be used for protection switchover (marked with PRT label). In the example ASI1 port is used. This port alarm check-box must be checked in order to initiate the switch-over in case of failure of ASI port

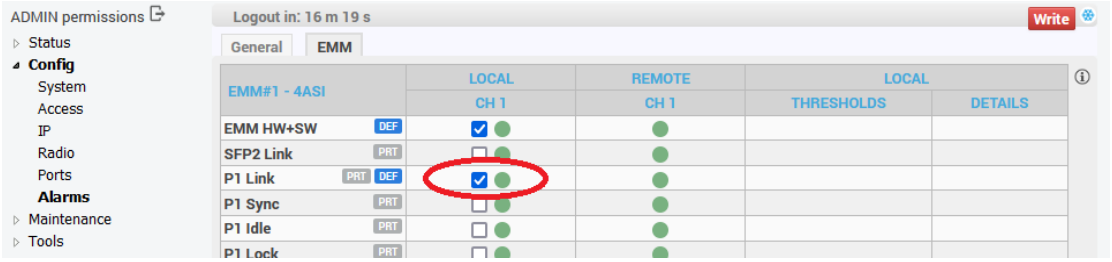


Figure 5.160b *Example of alarm configuration*

10) Save new settings by pressing Write button.
11) Reboot all 4 IDUs after successful reconfiguration
12) In web GUI '*Config->System->Mode*' set Hot-Swap Startup device Role to 'Auto primary' for both Primary IDUs and to 'Auto Secondary' for both Secondary IDUs in order to enable protection mode on all Phoenix G2 IDUs

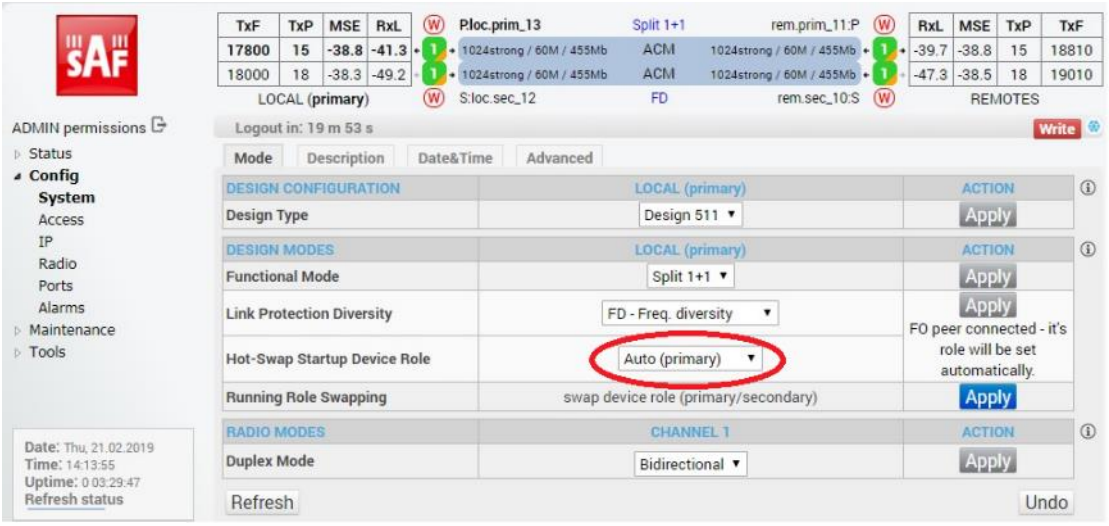


Figure 5.161 *Example of system configuration in Auto mode*

1) Save new settings by pressing Write button.

The status of the link and its configuration is displayed in the header of the web GUI. The status of the IDU which currently is monitored is displayed in Bold and is indicated as LOCAL (primary) or LOCAL (secondary):



Figure 5.162 *Status of 1+1 FD protection mode*

Example 16 – Full protection 1+1 Repeater mode (Design 513)

The example will describe 4 scenarios of Full protection 1+1 Repeater link configuration and interconnection schemes. The focus of this example is on Phoenix G2 IDUs interconnection options in Repeater site and configuration specifics of Endpoint IDUs and Repeater site IDUs. Full protection 1+1 Repeater mode is supported only by Design 513. The Functional mode for IDUs installed in Repeater site must be set as '1+1 Repeater mode', but for IDUs installed in Endpoints it must be set as '1+1 Split'.

In the Repeater site 4 IDUs/ODUs must be installed – one Primary/Secondary IDU pair to one direction, and second Primary/Secondary IDU pair to another direction. In each Endpoint site 2 IDUs/ODUs must be installed

Scenario 1

This is Full protection 1+1 Repeater scenario with Ethernet traffic and in-band management access via all LAN ports. PTP traffic, ASI or E1/T1 EMM traffic can be supported in this scenario.

Traffic port usage in this scenario is following: SFP1 port is used for 1+1 redundancy IDU interconnection; SFP3 and SFP4 ports are used for ASI or E1/T1 EMM traffic; LAN ports are used for Ethernet (High Priority ETH) and/or for PTP traffic. This scenario does not require external switch on Repeater site.

Full protection 1+1 Repeater IDU interconnection example in Repeater site is following:

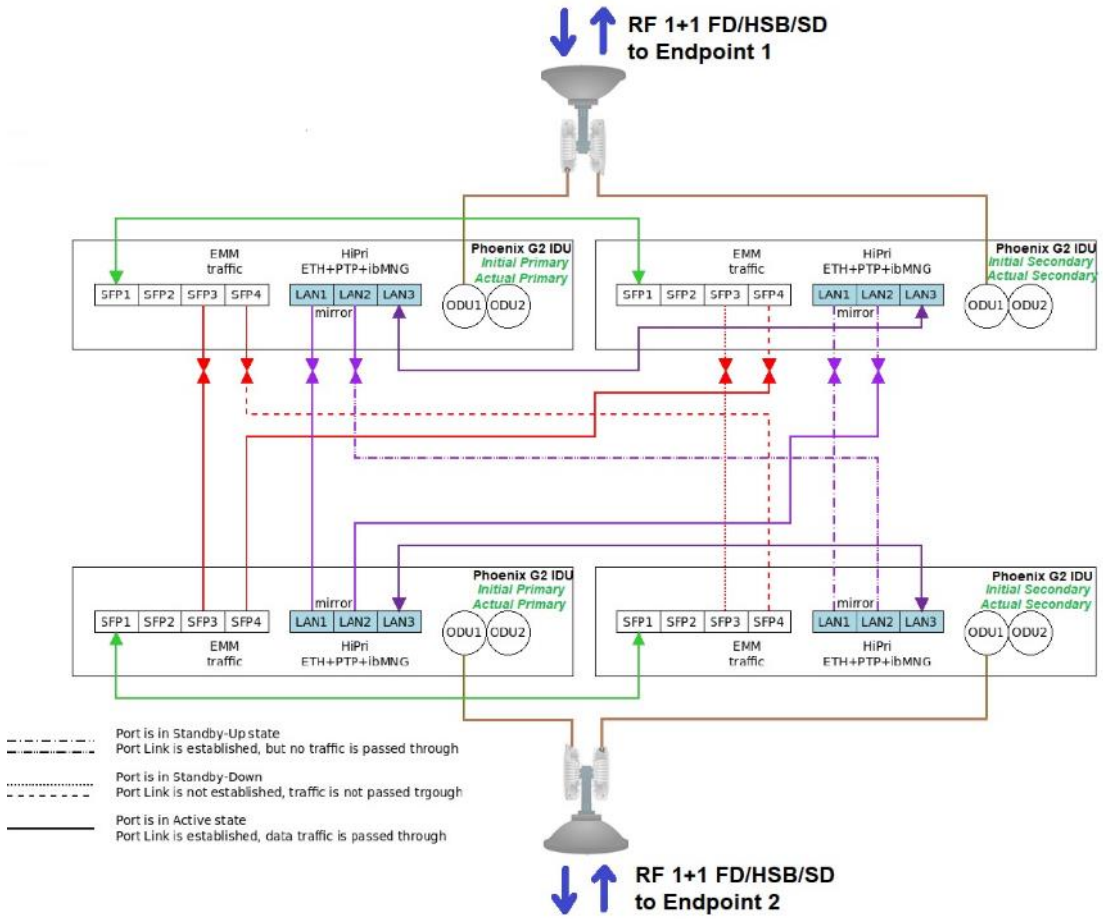


Figure 5.163 *Full protection 1+1 Repeater site interconnection scheme (scenario 1)*

Endpoint Primary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Split', Hot-Swap Startup Role 'Auto (primary)':

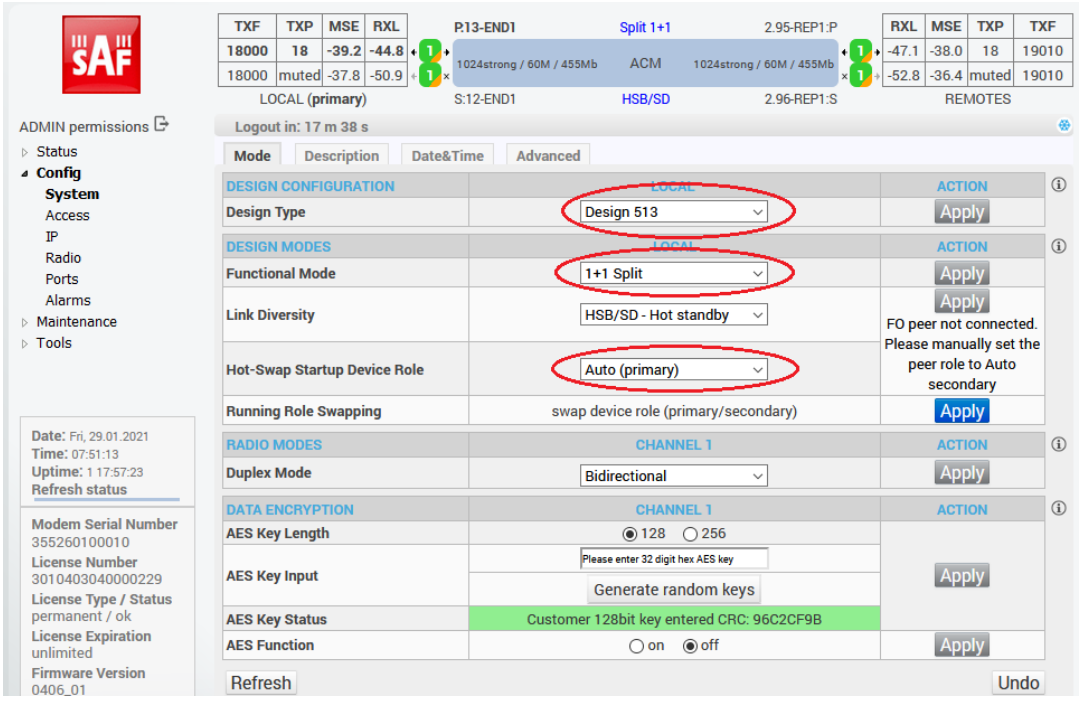


Figure 5.164 *Endpoint Primary IDU System configuration (scenario 1)*

Endpoint Primary IDU port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports must be configured in the same port group (it can be done in *Config →Ports →EthVLAN* page), any of WAN ports must be connected to High priority Ethernet data channel (ETH1a), SFP3/SFP4 ports must be connected to EMM channel (if ASI or E1/T1 EMM is used):

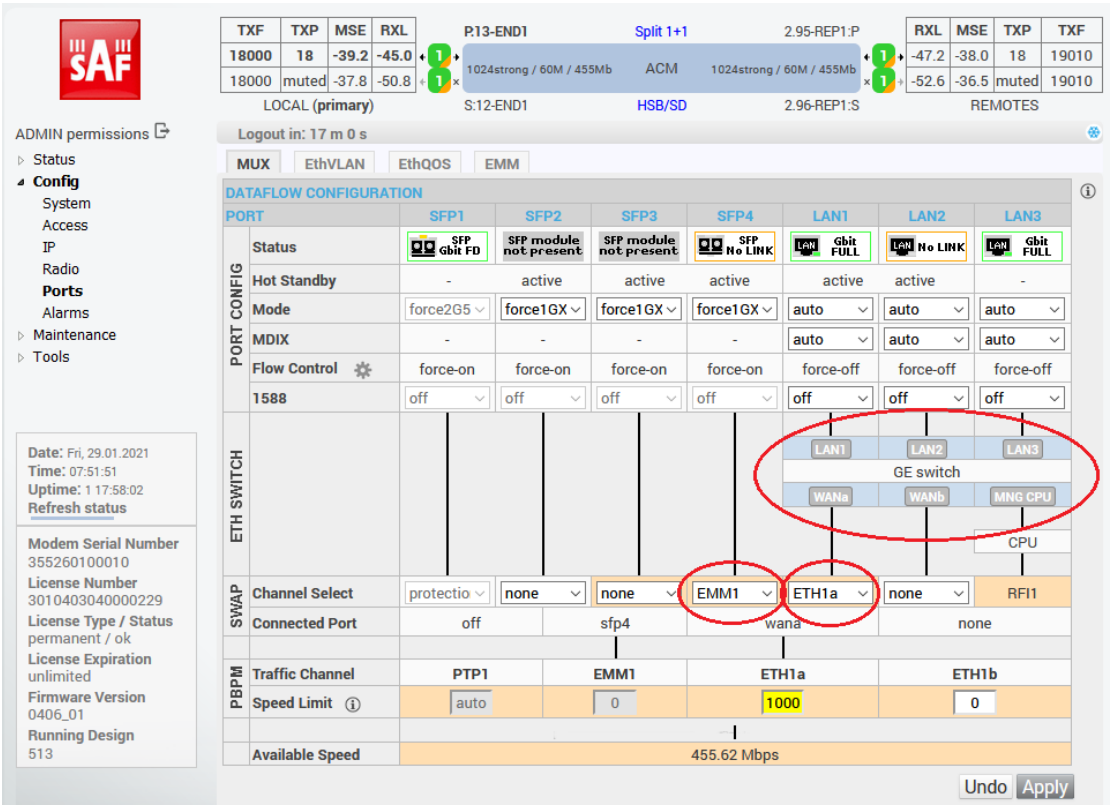


Figure 5.165 *Endpoint Primary IDU Port configuration (scenario 1)*

Endpoint Secondary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Split', Hot-Swap Startup Role 'Auto (secondary)':

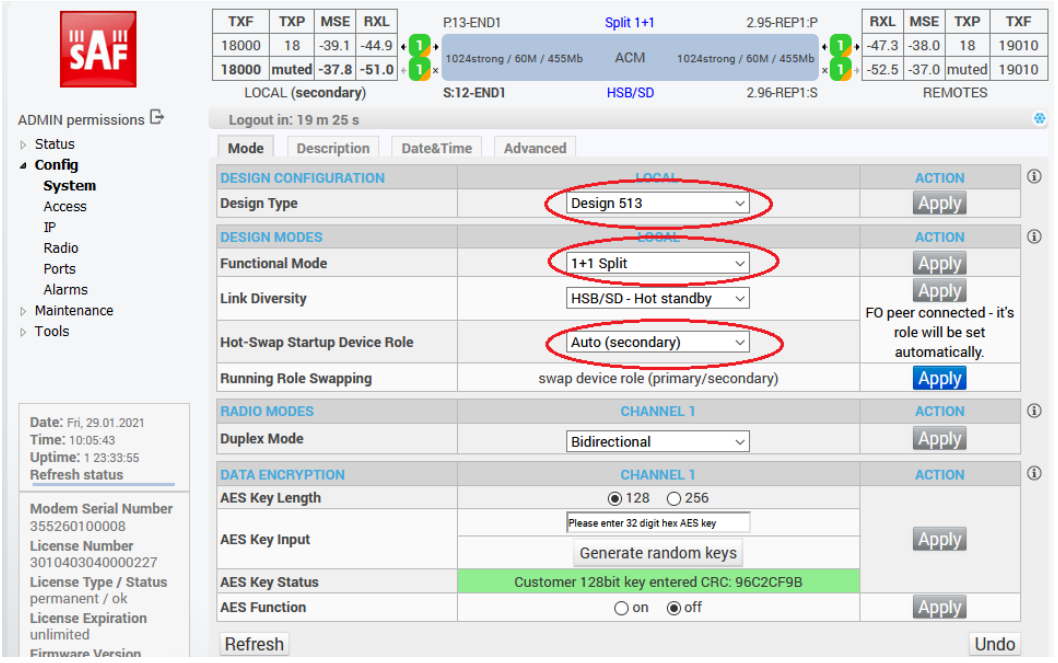


Figure 5.166 *Endpoint Secondary IDU System configuration (scenario 1)*

Endpoint Secondary IDU port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports must be configured in the same port group (it can be done in *Config →Ports →EthVLAN* page), any of WAN ports must be connected to High priority Ethernet data channel (ETH1a), SFP3/SFP4 ports must be connected to EMM channel (if ASI or E1/T1 EMM is used):

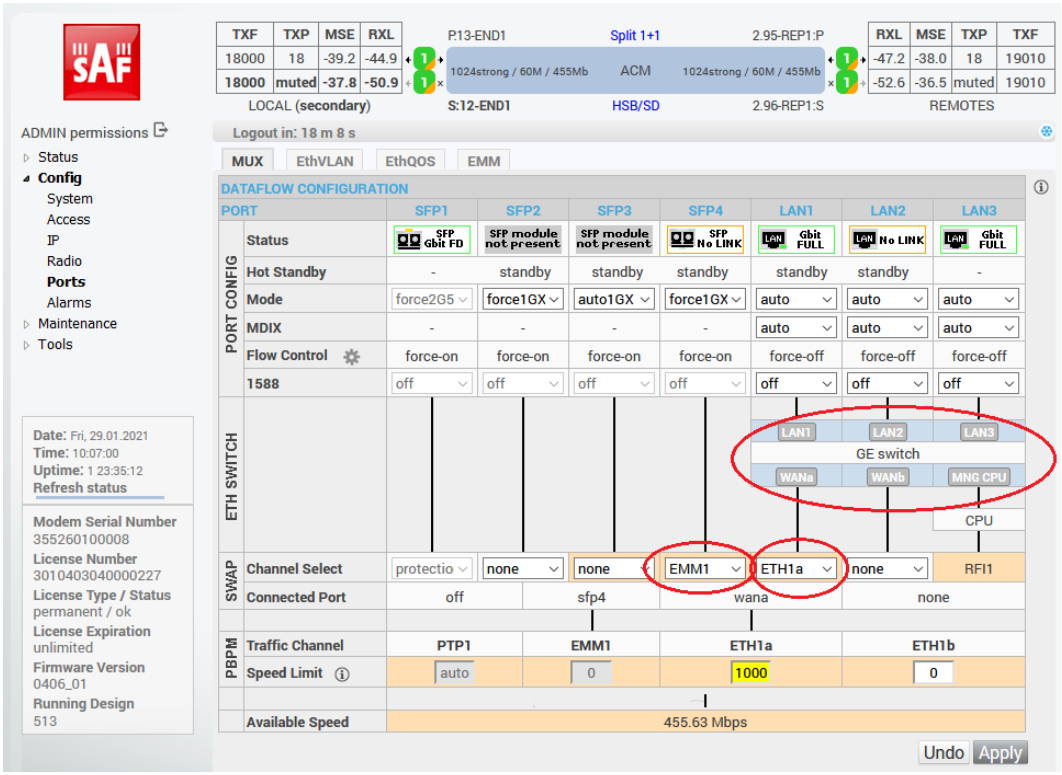


Figure 5.167 *Endpoint Secondary IDU Port configuration (scenario 1)*

Both Repeater site Primary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Repeater', Hot-Swap Startup Role 'Auto (primary)':

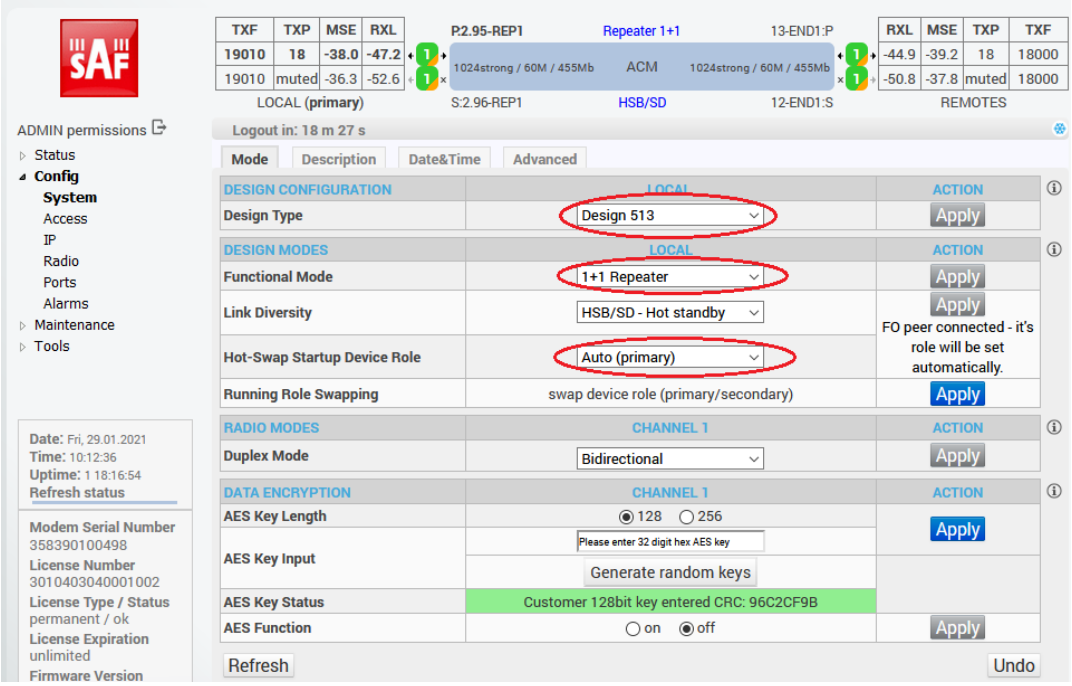


Figure 5.168 *Repeater Primary IDU System configuration (scenario 1)*

Repeater site both Primary IDUs port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports must be configured in the same port group (it can be done in *Config →Ports →EthVLAN* page), any of WAN ports must be connected to High priority Ethernet data channel (ETH1a), Hot Standby option for LAN1/LAN2 ports must be set to 'mirror'. SFP3/SFP4 ports will automatically be dedicated to EMM channel (if ASI or E1/T1 EMM is used):

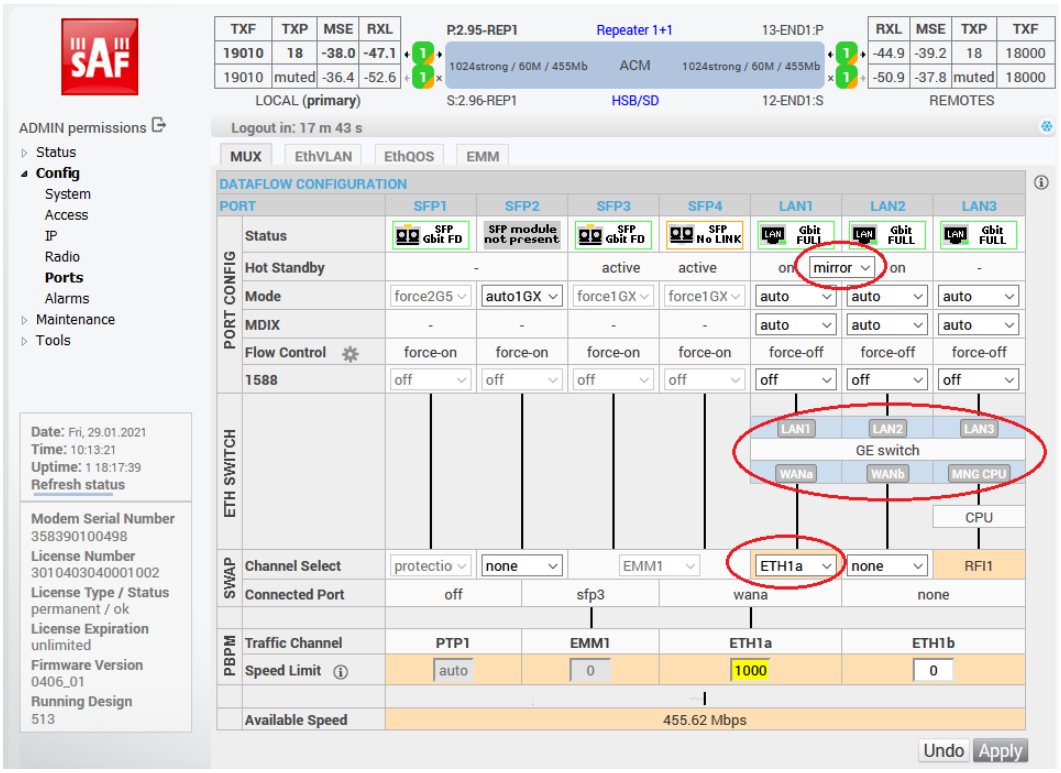


Figure 5.169 *Repeater Primary IDU Port configuration (scenario 1)*

Both Repeater site Secondary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Repeater', Hot-Swap Startup Role 'Auto (secondary)':

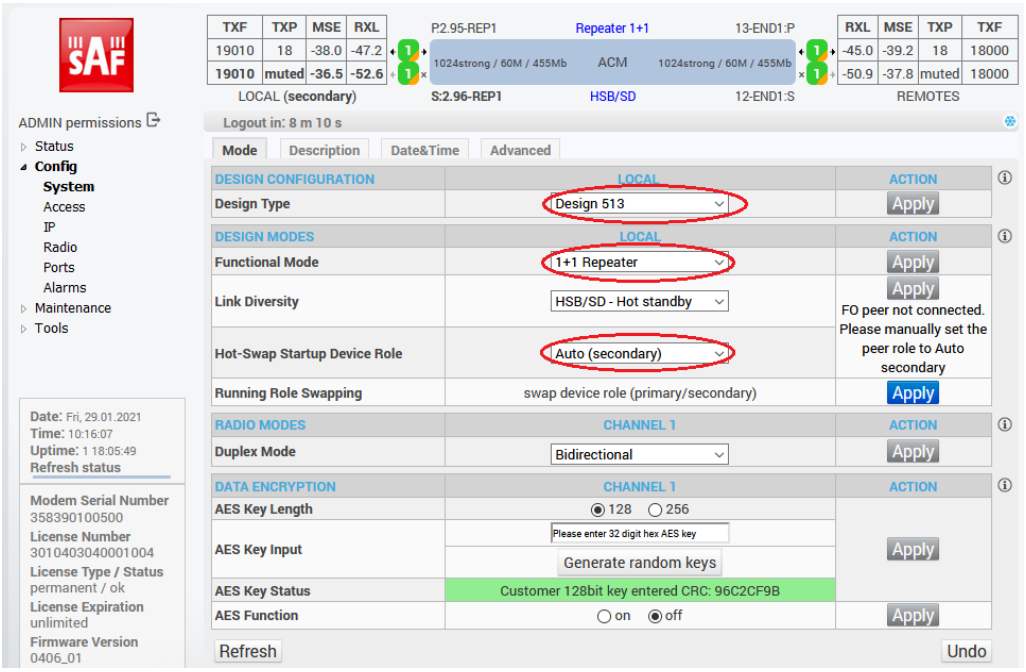


Figure 5.170 *Repeater Secondary IDU System configuration (scenario 1)*

Repeater site both Secondary IDUs port configuration is following (in *Config →Ports →MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports must be configured in the same port group (it can be done in *Config →Ports →EthVLAN* page), any of WAN ports must be connected to High priority Ethernet data channel (ETH1a), Hot Standby option for LAN1/LAN2 ports must be set to 'mirror'. SFP3/SFP4 ports will automatically be dedicated to EMM channel (if ASI or E1/T1 EMM is used):

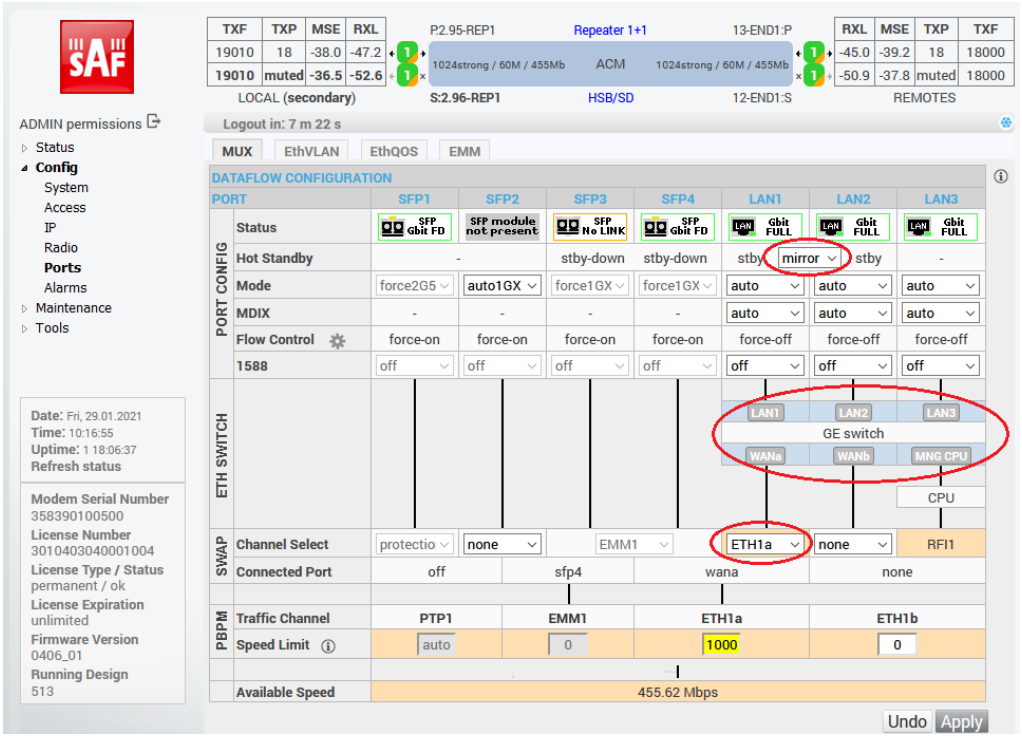


Figure 5.171 *Repeater Secondary IDU Port configuration (scenario 1)*

Alarm configuration is mandatory for all IDUs in Endpoint and in Repeater site as part of alarms are used as initiation of 1+1 switchover (Primary/Secondary role switch). The alarms which are used as criteria for IDU role switch are indicated with PRT label. Those alarms must be enabled according to customer needs for each IDU. Alarm configuration can be done in page *Config →Alarms →General*:

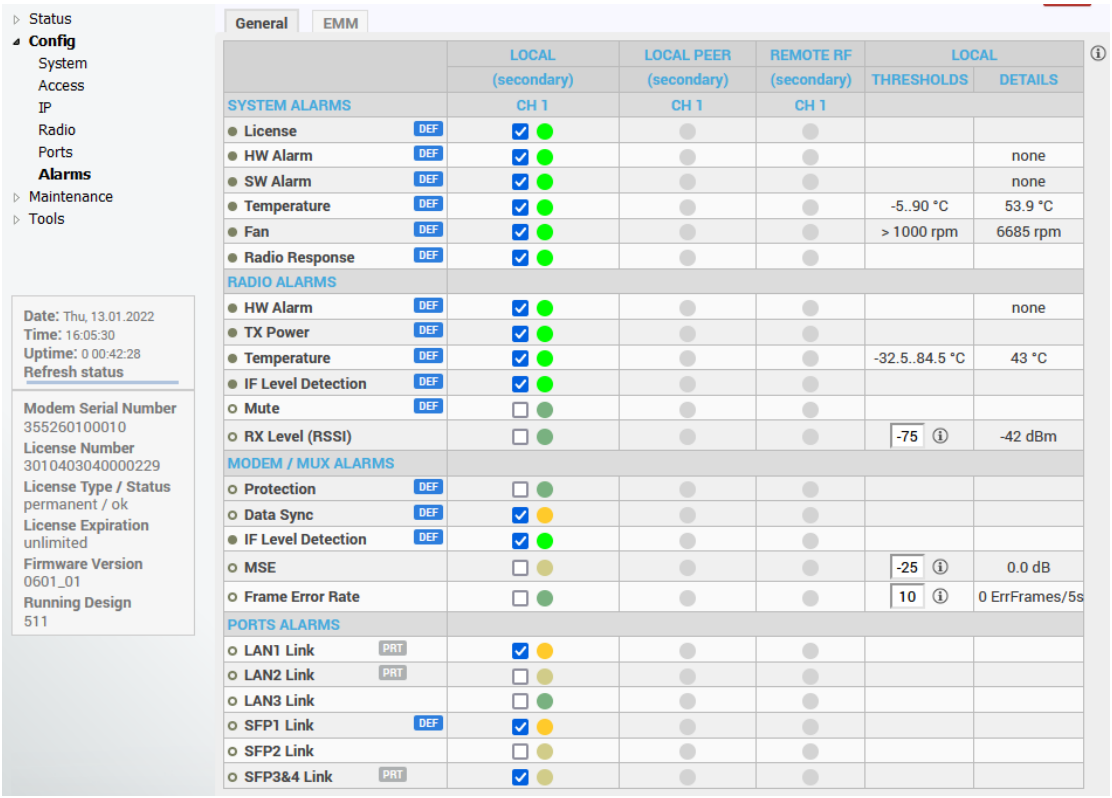


Figure 5.172 *IDU alarm configuration (scenario 1)*

In all the Repeater site IDUs the SFP3 Link and SFP4 Link alarms are merged, so that the alarms will be initiated for both ports together. The alarm configuration can be done for SFP3 Link, but the SFP4 Link alarms will be automatically set

Scenario 2

This is Full protection 1+1 Repeater scenario with Ethernet traffic in LAN1, LAN2 and SFP2 ports, out-band management access in LAN3 port. The scenario allows also configure LAN3 port as in-band management and traffic port. PTP traffic, ASI or E1/T1 EMM traffic can be supported in this scenario.

Traffic port usage is following: SFP1 port is used for 1+1 redundancy IDU interconnection; SFP2 port is used for Ethernet (Low Priority ETH) traffic, SFP3 and SFP4 ports are used for ASI or E1/T1 EMM traffic; LAN1, LAN2 ports are used for Ethernet (High Priority ETH) and/or for PTP traffic; LAN3 port is used for out-band management access (local management access only). This scenario example requires external switches for Low Priority Ethernet traffic and for out-band management traffic on Repeater site.

Endpoint IDU traffic ports can be configured in following way: SFP1 port is used for 1+1 redundancy IDU interconnection; SFP2 port is used for Ethernet (Low Priority ETH) traffic, SFP3 and SFP4 ports are used for ASI or E1/T1 EMM traffic; LAN1, LAN2 ports are used for Ethernet (High Priority ETH) and/or for PTP traffic; LAN3 port can be used for out-band management access (local management access only), as well as for in-band management access.

Full protection 1+1 Repeater IDU interconnection example in Repeater site is following:

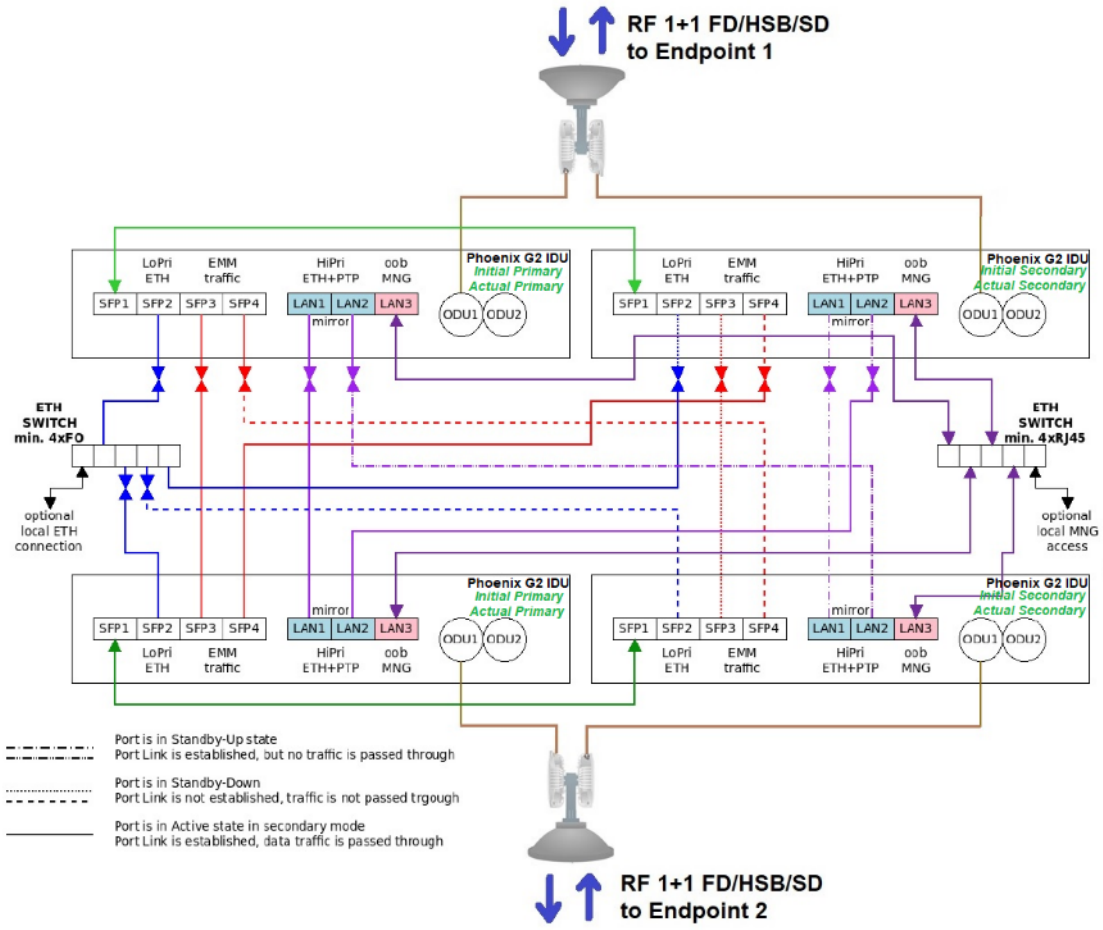


Figure 5.173 *Full protection 1+1 Repeater site interconnection scheme (scenario 2)*

Endpoint Primary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Split', Hot-Swap Startup Role 'Auto (primary)':

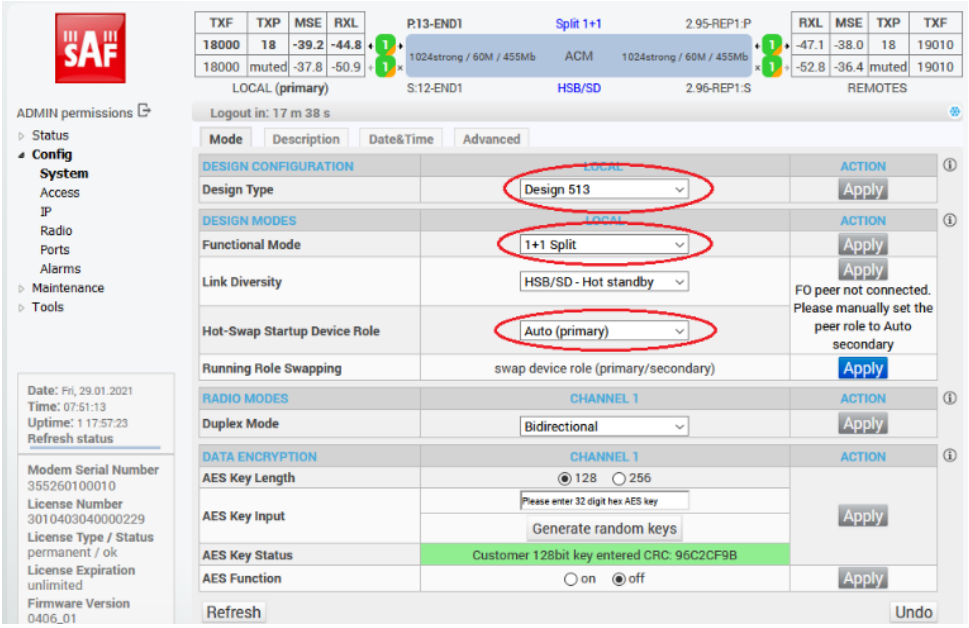


Figure 5.174 *Endpoint Primary IDU System configuration (scenario 2)*

Endpoint Primary IDU port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports can be configured in the same port group (it can be done in *Config →Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in different port group in order to have out-band management access (in this case it will be only local management access).

Any of WAN ports must be connected to High priority Ethernet data channel (ETH1a), SFP2 port must be connected to Low priority Ethernet data channel (ETH1b), SFP3/SFP4 ports must be connected to EMM channel (if ASI or E1/T1 EMM is used):

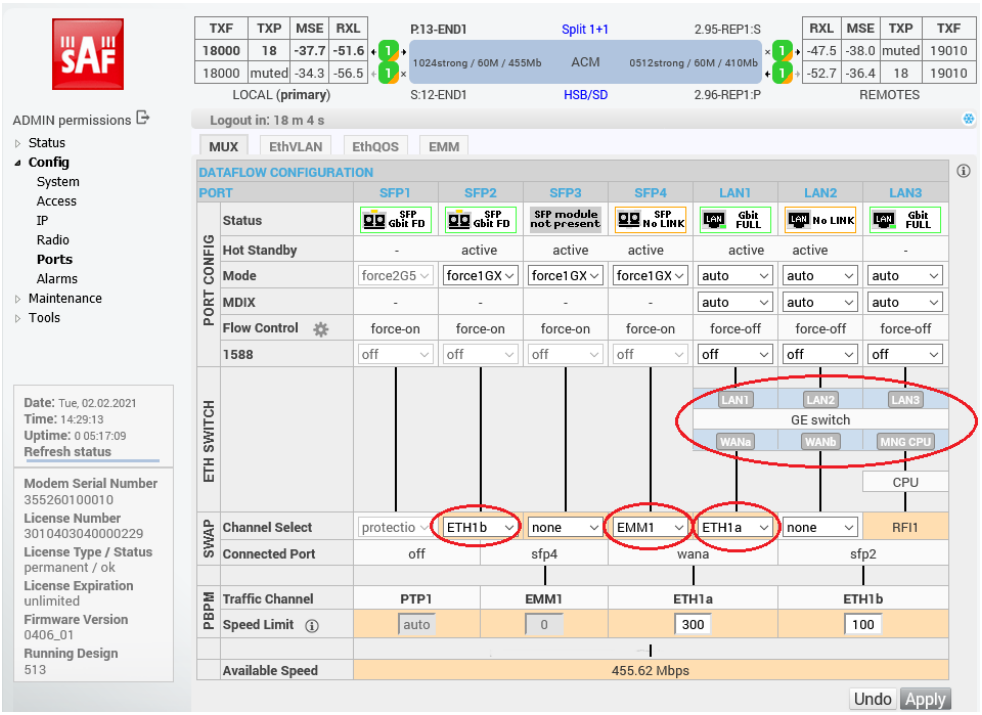


Figure 5.175 *Endpoint Primary IDU Port configuration (scenario 2)*

Endpoint Secondary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Split', Hot-Swap Startup Role 'Auto (secondary)':

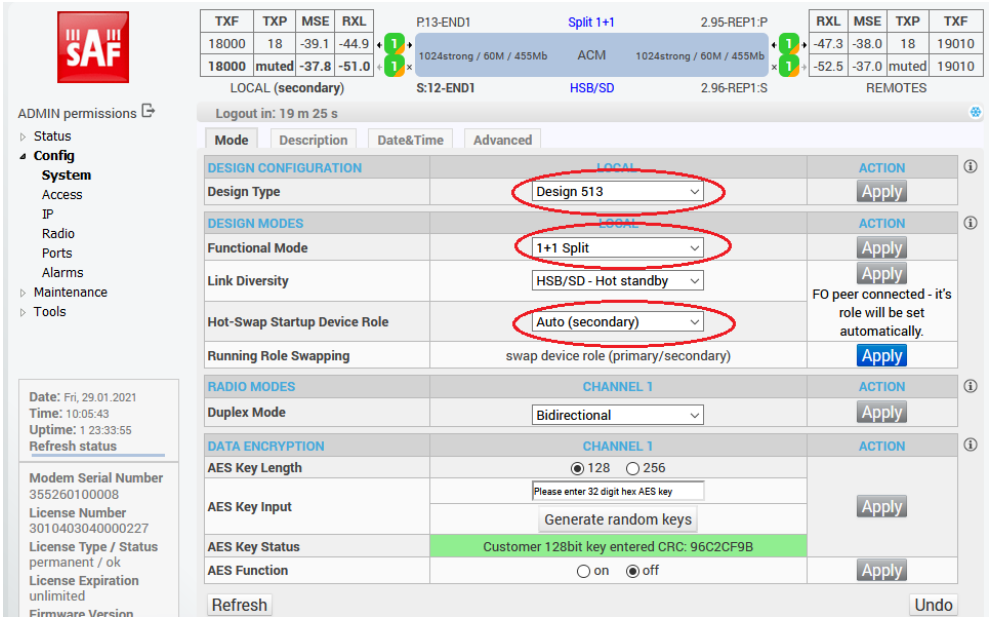


Figure 5.176 *Endpoint Secondary IDU System configuration (scenario 2)*

Endpoint Secondary IDU port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports can be configured in the same port group (it can be done in *Config →Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in different port group in order to have out-band management access (in this case it will be only local management access).

Any of WAN ports must be connected to High priority Ethernet data channel (ETH1a), SFP2 port must be connected to Low priority Ethernet data channel (ETH1b), SFP3/SFP4 ports must be connected to EMM channel (if ASI or E1/T1 EMM is used):

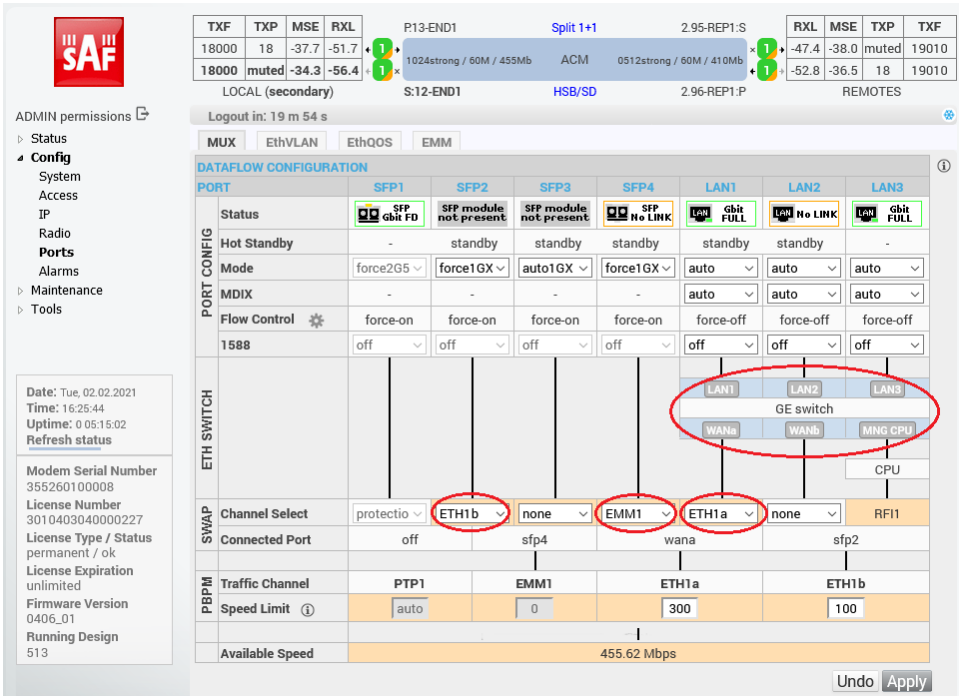


Figure 5.177 *Endpoint Secondary IDU Port configuration (scenario 2)*

Both Repeater site Primary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Repeater', Hot-Swap Startup Role 'Auto (primary)':

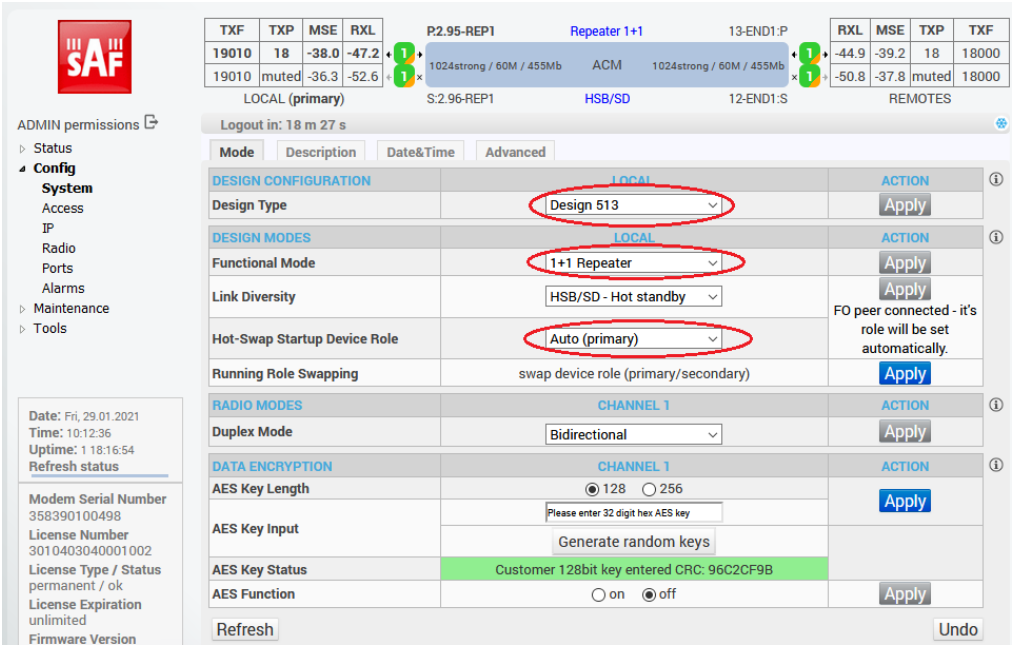


Figure 5.178 *Repeater Primary IDU System configuration (scenario 2)*

Repeater site both Primary IDUs port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, WANa and WANb ports must be configured in the same port group, LAN3 and MNG ports must be configured in different port group in order to have out-band management access (for local management access only in this case). It can be done in *Config →Ports →EthVLAN* page.



As an alternative LAN3 and MNG ports can be configured in the same port group with other LAN and WAN ports in order to have in-band management access and remote management connection.

Any of WAN ports must be connected to High priority Ethernet data channel (ETH1a) and SFP2 port must be connected to Low priority Ethernet data channel (ETH1b). Hot Standby option for LAN1/LAN2 ports must be set to 'mirror'. SFP3/SFP4 ports will automatically be dedicated to EMM channel (if ASI or E1/T1 EMM is used):

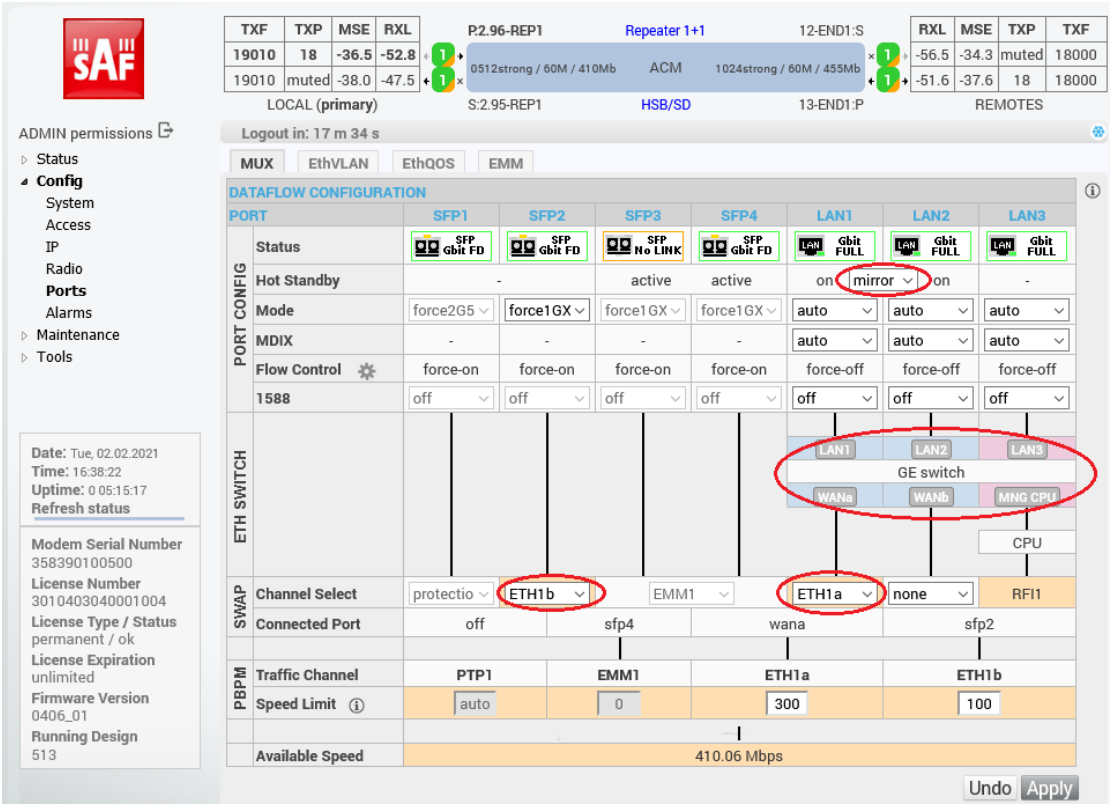


Figure 5.179 *Repeater Primary IDU Port configuration (scenario 2)*

Both Repeater site Secondary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Repeater', Hot-Swap Startup Role 'Auto (secondary)':

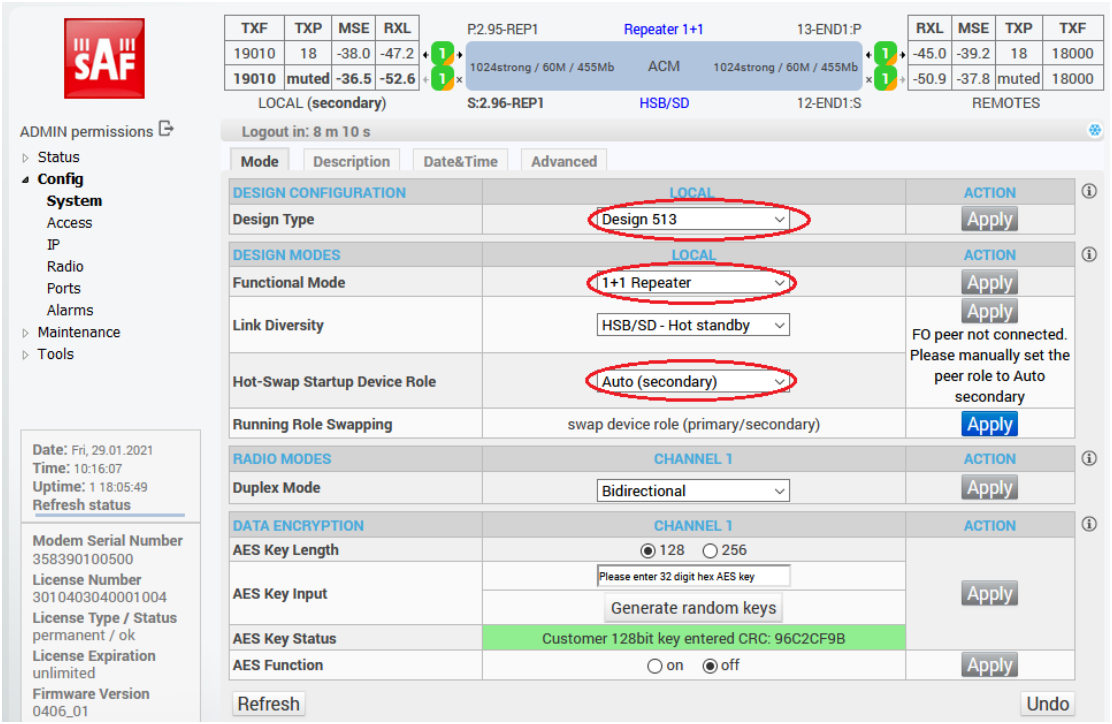


Figure 5.180 *Repeater Secondary IDU System configuration (scenario 2)*

Repeater site both Secondary IDUs port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, WANa and WANb ports must be configured in the same port group, LAN3 and MNG ports must be configured in different port group in order to have out-band management access (for local management access only in this case). It can be done in *Config →Ports →EthVLAN* page.



As an alternative LAN3 and MNG ports can be configured in the same port group with other LAN and WAN ports in order to have in-band management access and remote management connection.

Any of WAN ports must be connected to High priority Ethernet data channel (ETH1a) and SFP2 port must be connected to Low priority Ethernet data channel (ETH1b). Hot Standby option for LAN1/LAN2 ports must be set to 'mirror'. SFP3/SFP4 ports will automatically be dedicated to EMM channel (if ASI or E1/T1 EMM is used):

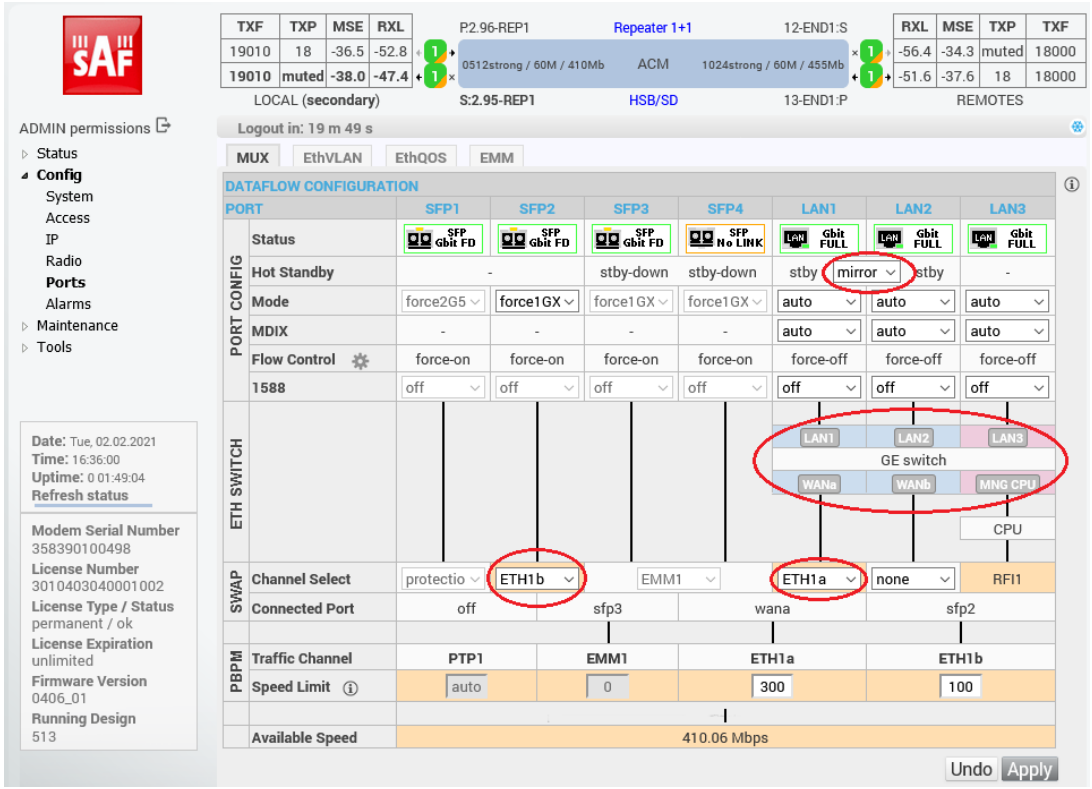


Figure 5.181 *Repeater Secondary IDU Port configuration (scenario 2)*

Alarm configuration is mandatory for all IDUs in Endpoint and in Repeater site as part of alarms are used as initiation of 1+1 switchover (Primary/Secondary role switch). The alarms which are used as criteria for IDU role switch are indicated with PRT label. Those alarms must be enabled according to customer needs for each IDU. Alarm configuration can be done in page *Config →Alarms →General*:

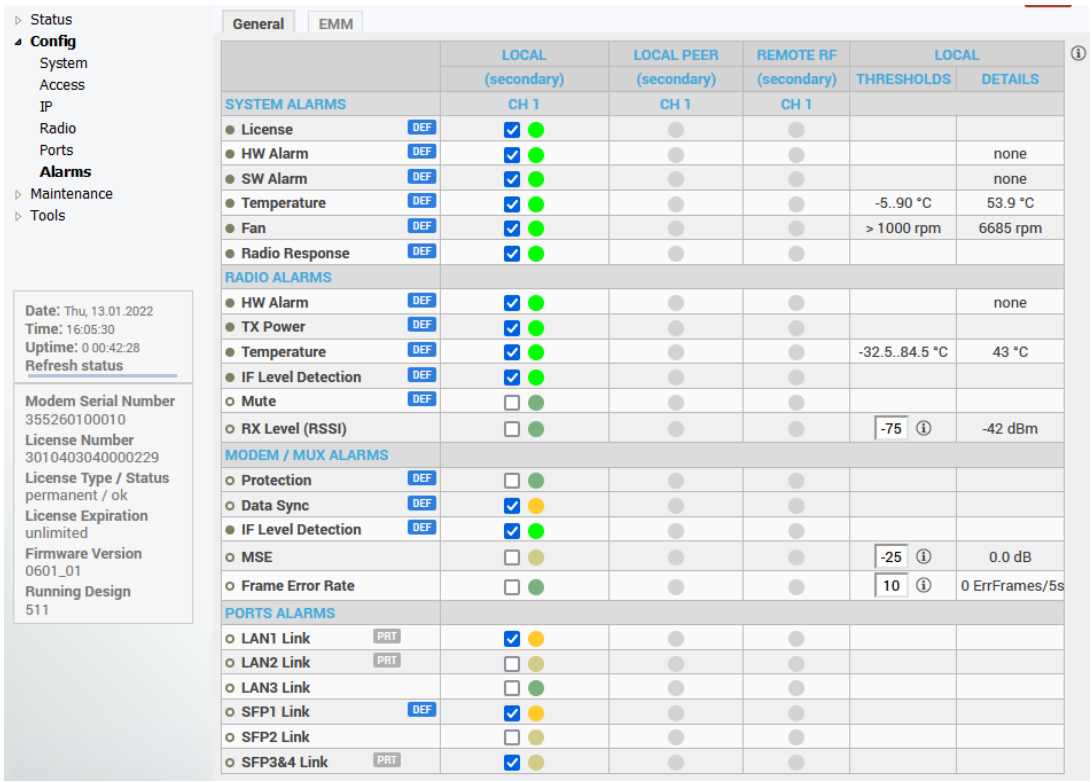


Figure 5.182 *IDU alarm configuration (scenario 2)*

In all the Repeater site IDUs the SFP3 Link and SFP4 Link alarms are merged, so that the alarms will be initiated for both ports together. The alarm configuration can be done for SFP3 Link, but the SFP4 Link alarms will be automatically set

Scenario 3

This is Full protection 1+1 Repeater scenario with Ethernet traffic in LAN1, LAN2 and SFP2 ports, out-band management access in LAN3 port. The scenario allows also configure LAN3 port as in-band management and traffic port. PTP traffic, ASI or E1/T1 EMM traffic can be supported in this scenario.

Traffic port usage is following: SFP1 port is used for 1+1 redundancy IDU interconnection; SFP2 port is used for Ethernet (High Priority ETH) traffic and/or for PTP traffic, SFP3 and SFP4 ports are used for ASI or E1/T1 EMM traffic; LAN1, LAN2 ports are used for Ethernet (Low Priority ETH); LAN3 port is used for out-band management access (local management access only). This scenario example requires external switches for High Priority Ethernet traffic on Repeater site.

Endpoint IDU traffic ports can be configured in following way: SFP1 port is used for 1+1 redundancy IDU interconnection; SFP2 port is used for Ethernet (High Priority ETH) traffic and/or for PTP traffic, SFP3 and SFP4 ports are used for ASI or E1/T1 EMM traffic; LAN1, LAN2 ports are used for Ethernet (Low Priority ETH); LAN3 port can be used for out-band management access (local management access only), as well as for in-band management access.

Full protection 1+1 Repeater IDU interconnection example in Repeater site is following:

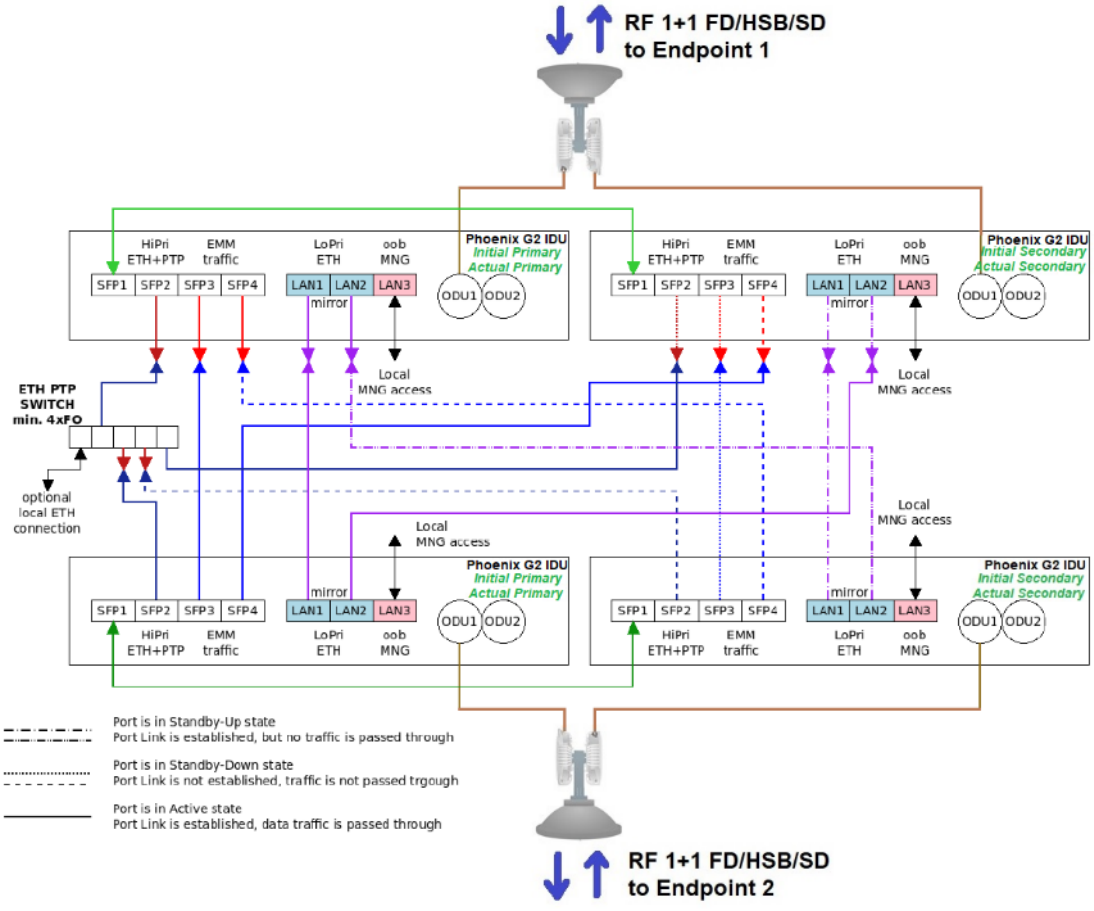


Figure 5.183 *Full protection 1+1 Repeater site interconnection scheme (scenario 3)*

Endpoint Primary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Split', Hot-Swap Startup Role 'Auto (primary)':

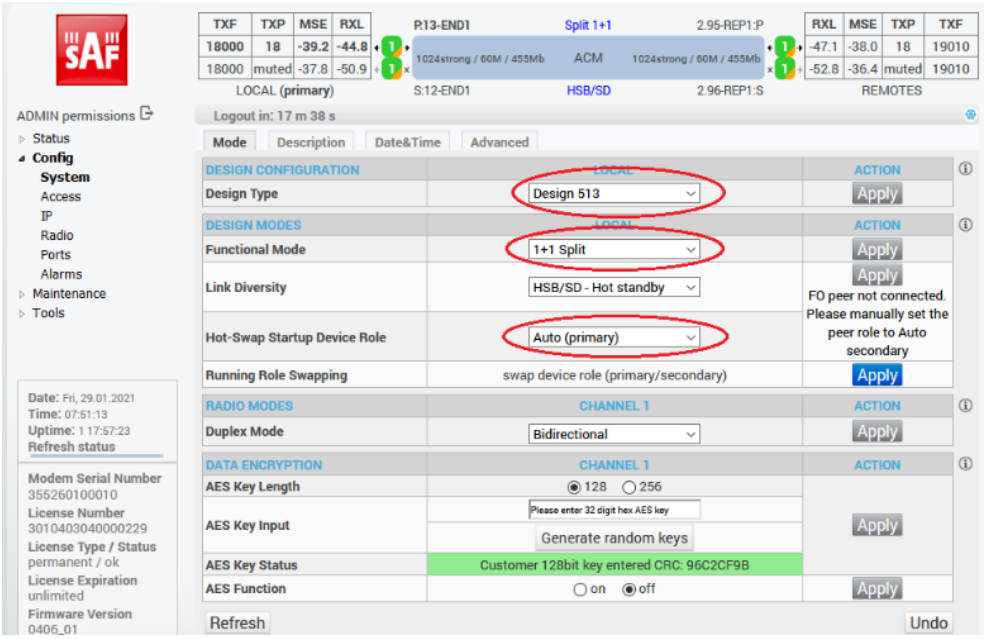


Figure 5.184 *Endpoint Primary IDU System configuration (scenario 3)*

Endpoint Primary IDU port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports can be configured in the same port group (it can be done in *Config →Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in different port group in order to have out-band management access (in this case it will be only local management access).

Any of WAN ports must be connected to Low priority Ethernet data channel (ETH1b), SFP2 port must be connected to High priority Ethernet data channel (ETH1a), SFP3/SFP4 ports must be connected to EMM channel (if ASI or E1/T1 EMM is used):

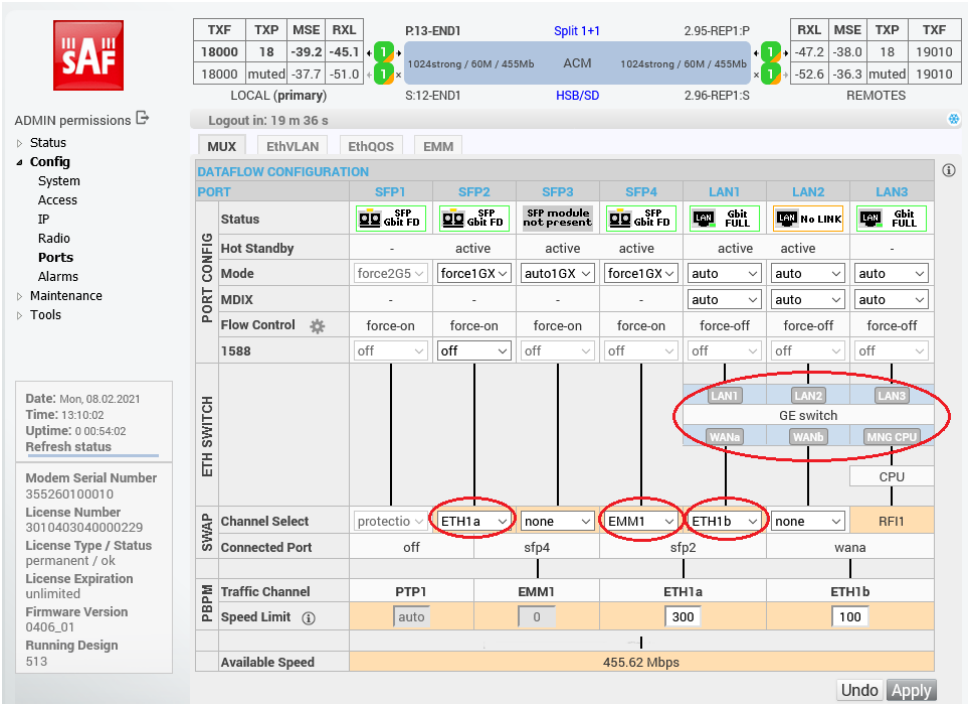


Figure 5.185 *Endpoint Primary IDU Port configuration (scenario 3)*

Endpoint Secondary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Split', Hot-Swap Startup Role 'Auto (secondary)':



Figure 5.186 *Endpoint Secondary IDU System configuration (scenario 3)*

Endpoint Secondary IDU port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports can be configured in the same port group (it can be done in *Config →Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in different port group in order to have out-band management access (in this case it will be only local management access).

Any of WAN ports must be connected to Low priority Ethernet data channel (ETH1b), SFP2 port must be connected to High priority Ethernet data channel (ETH1a), SFP3/SFP4 ports must be connected to EMM channel (if ASI or E1/T1 EMM is used):

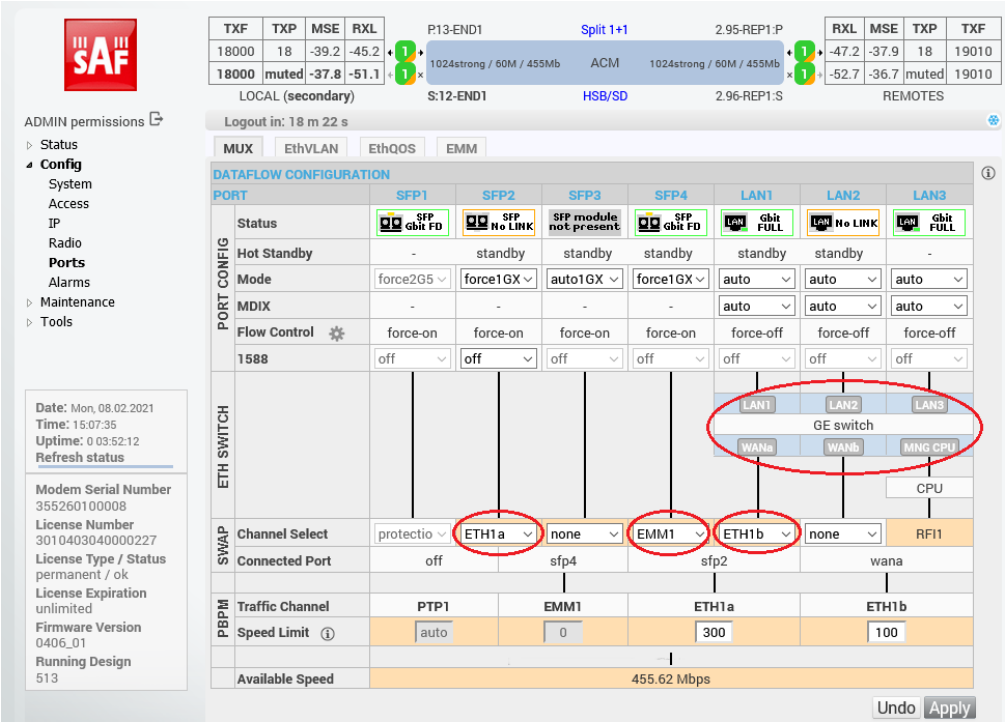


Figure 5.187 *Endpoint Secondary IDU Port configuration (scenario 3)*

Both Repeater site Primary IDUs must be configured in following way (in *Config → System → Mode* page): Design type ‘Design 513’, Functional mode ‘1+1 Repeater’, Hot-Swap Startup Role ‘Auto (primary)’:

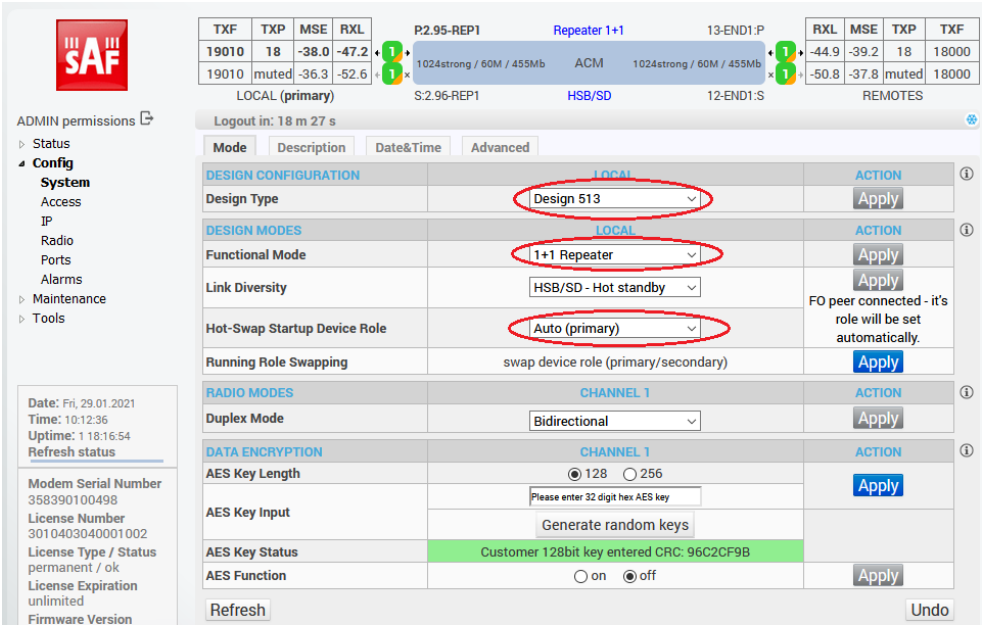


Figure 5.188 *Repeater Primary IDU System configuration (scenario 3)*

Repeater site both Primary IDUs port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports can be configured in the same port group (it can be done in *Config→Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in different port group in order to have out-band management access (in this case it will be only local management access).

Any of WAN ports must be connected to Low priority Ethernet data channel (ETH1b) and SFP2 port must be connected to High priority Ethernet data channel (ETH1a). Hot Standby option for LAN1/LAN2 ports must be set to ‘mirror’. SFP3/SFP4 ports will automatically be dedicated to EMM channel (if ASI or E1/T1 EMM is used):

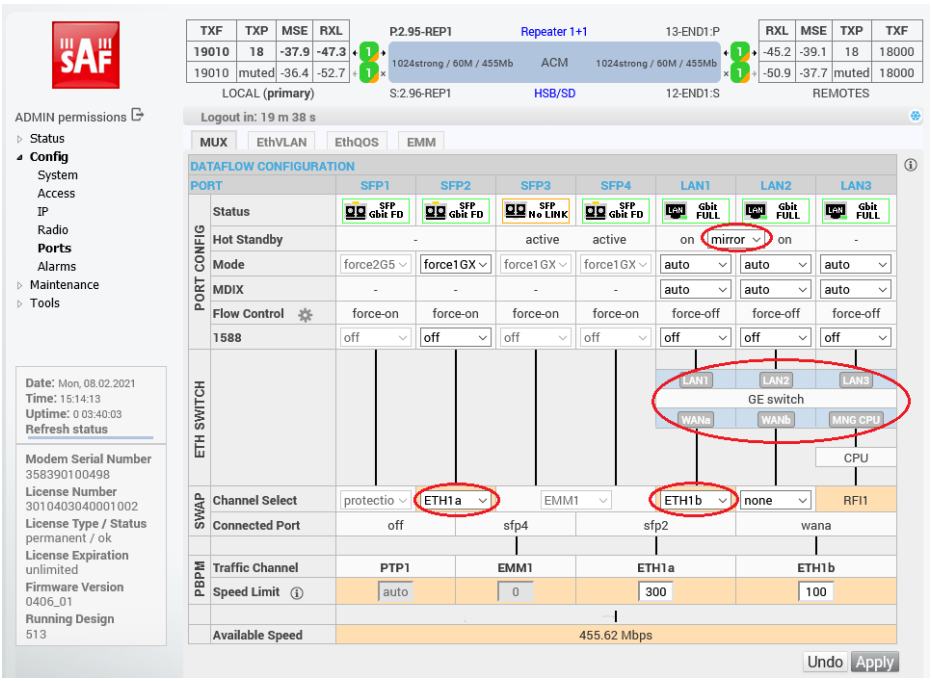


Figure 5.189 *Repeater Primary IDU Port configuration (scenario 3)*

Both Repeater site Secondary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Repeater', Hot-Swap Startup Role 'Auto (secondary)':

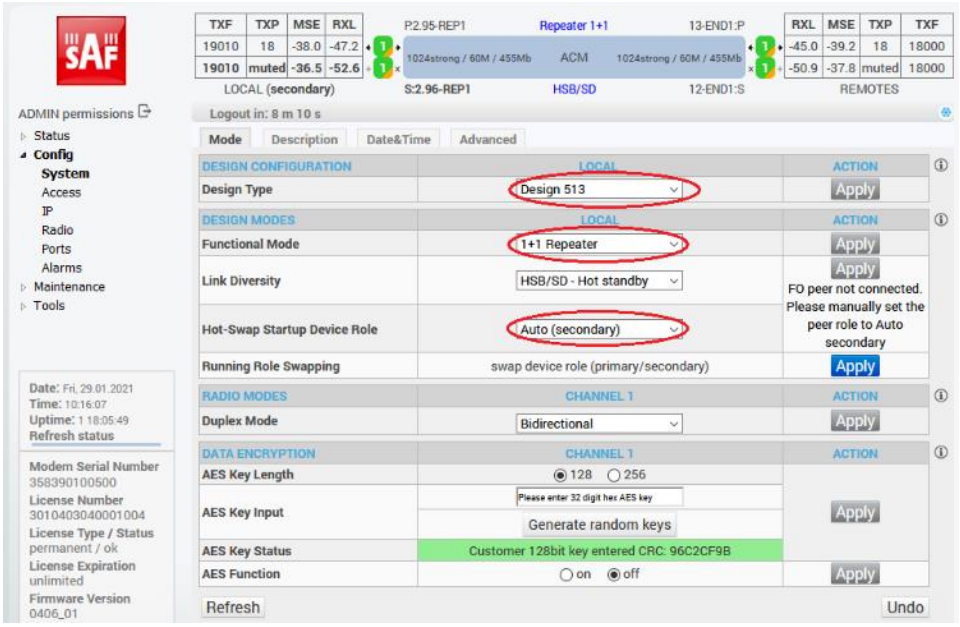


Figure 5.190 *Repeater Secondary IDU System configuration (scenario 3)*

Repeater site both Secondary IDUs port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN2, LAN3, WANa, WANb and MNG ports can be configured in the same port group (it can be done in *Config →Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in different port group in order to have out-band management access (in this case it will be only local management access).

Any of WAN ports must be connected to Low priority Ethernet data channel (ETH1b) and SFP2 port must be connected to High priority Ethernet data channel (ETH1a). Hot Standby option for LAN1/LAN2 ports must be set to 'mirror'. SFP3/SFP4 ports will automatically be dedicated to EMM channel (if ASI or E1/T1 EMM is used):

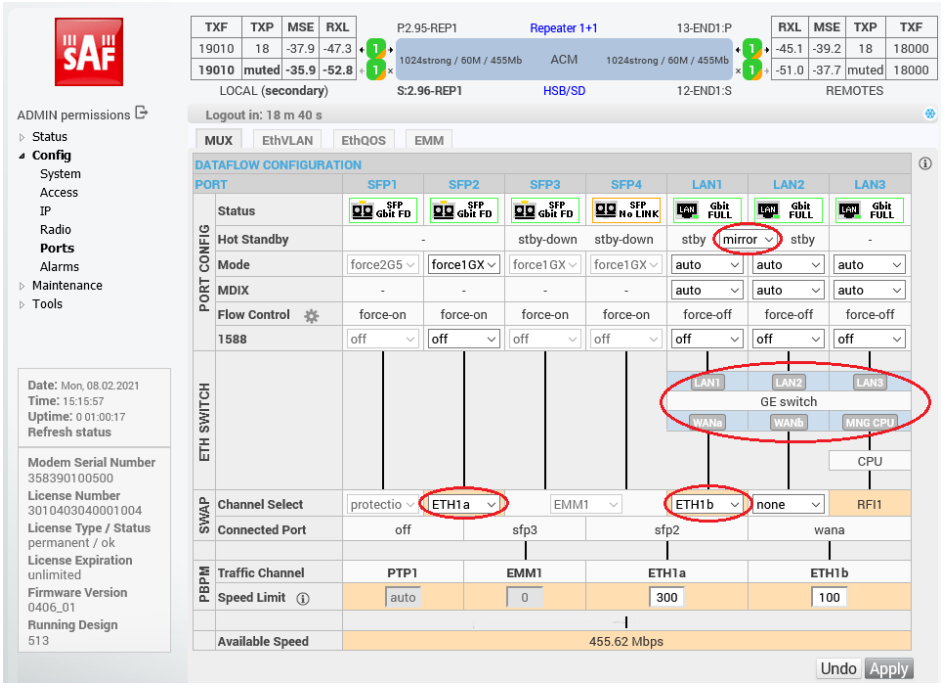


Figure 5.191 *Repeater Secondary IDU Port configuration (scenario 3)*

Alarm configuration is mandatory for all IDUs in Endpoint and in Repeater site as part of alarms are used as initiation of 1+1 switchover (Primary/Secondary role switch). The alarms which are used as criteria for IDU role switch are indicated with PRT label. Those alarms must be enabled according to customer needs for each IDU. Alarm configuration can be done in page *Config →Alarms →General*:

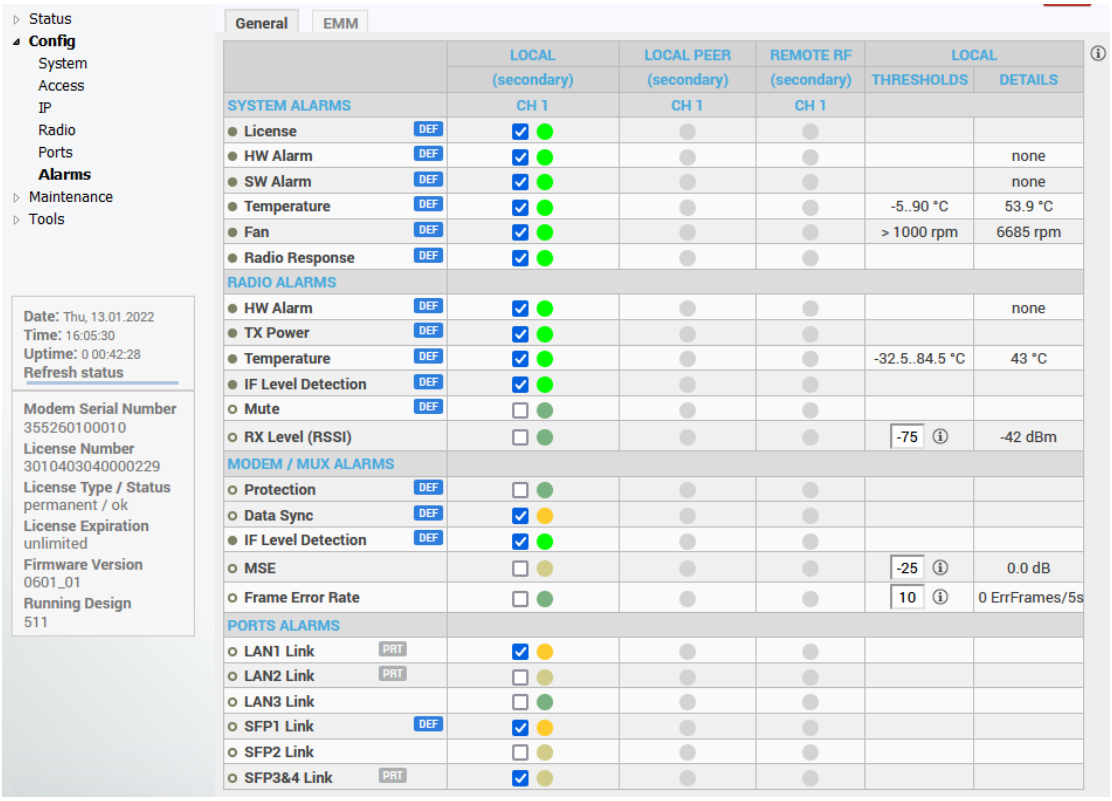


Figure 5.192 *IDU alarm configuration (scenario 3)*



In all the Repeater site IDUs the SFP3 Link and SFP4 Link alarms are merged, so that the alarms will be initiated for both ports together. The alarm configuration can be done for SFP3 Link, but the SFP4 Link alarms will be automatically set

Scenario 4

This is Full protection 1+1 Repeater scenario with Ethernet traffic in LAN1 and LAN2 ports, out-band management access in LAN3 port. The scenario allows also configure LAN3 port as in-band management and traffic port. ASI or E1/T1 EMM traffic can be supported in this scenario.

Traffic port usage is following: SFP1 port is used for 1+1 redundancy IDU interconnection; SFP3 and SFP4 ports are used for ASI or E1/T1 EMM traffic; LAN1 port is used for Ethernet (Hight Priority ETH) traffic; LAN2 port is used for Ethernet (Low Priority ETH) traffic; LAN3 port is used for out-band management access (local management access only). This scenario example requires external switches for High Priority Ethernet traffic and for Low Priority Ethernet traffic on Repeater site.

Endpoint IDU traffic ports can be configured in following way: SFP1 port is used for 1+1 redundancy IDU interconnection; SFP3 and SFP4 ports are used for ASI or E1/T1 EMM traffic; LAN1 port is used for Ethernet (Hight Priority ETH) traffic; LAN2 port is used for Ethernet (Low Priority ETH) traffic; LAN3 port can be used for out-band management access (local management access only), as well as for in-band management access.

Full protection 1+1 Repeater IDU interconnection example in Repeater site is following:

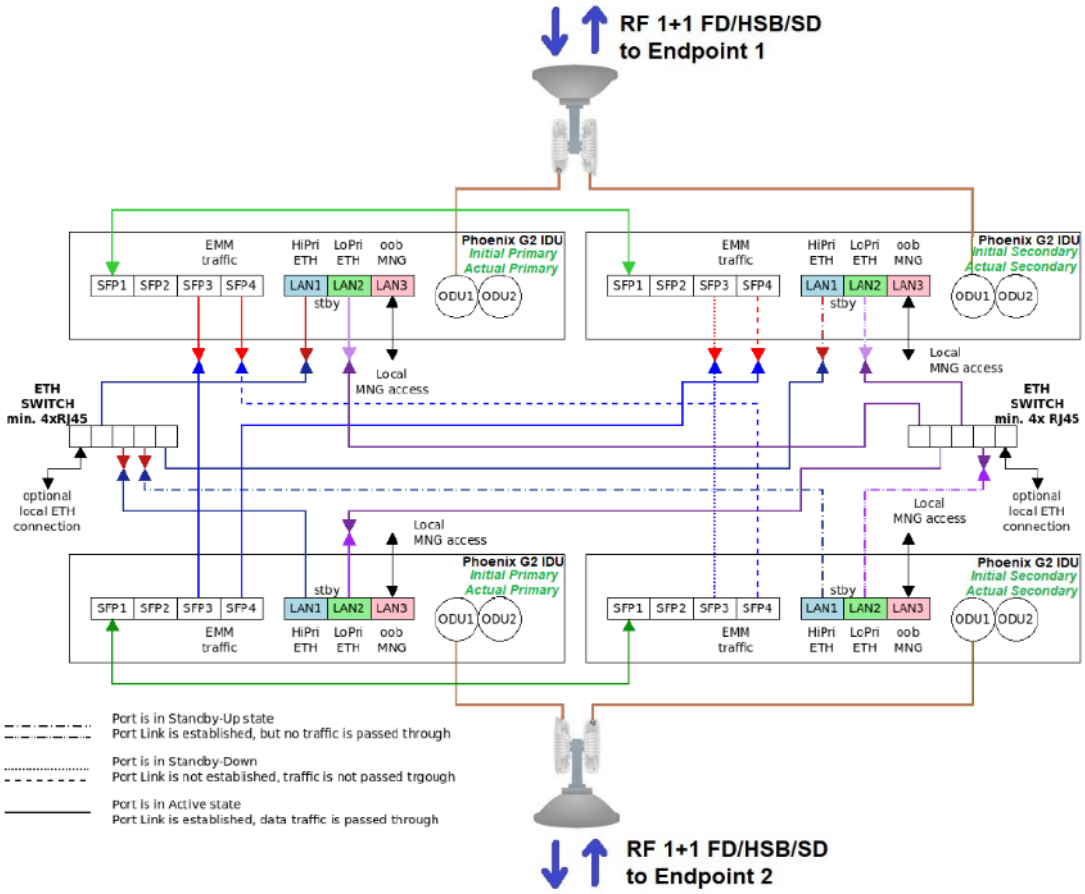


Figure 5.193 *Full protection 1+1 Repeater site interconnection scheme (scenario 4)*

Endpoint Primary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Split', Hot-Swap Startup Role 'Auto (primary)':

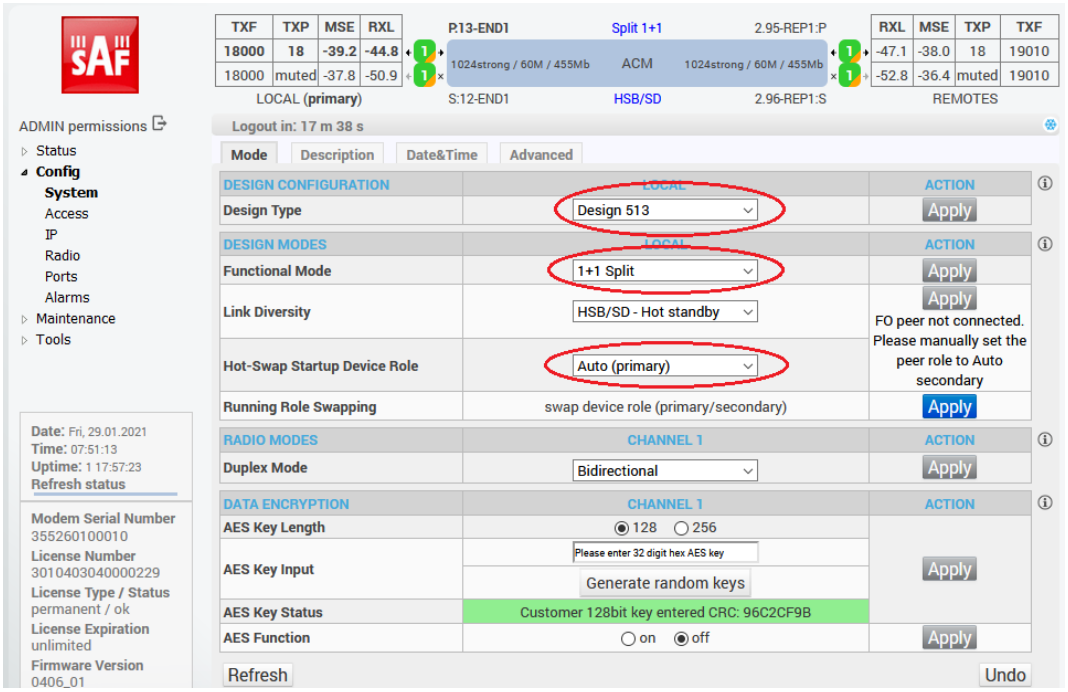


Figure 5.194 *Endpoint Primary IDU System configuration (scenario 4)*

Endpoint Primary IDU port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN3, WANa and MNG ports should be configured in the same port group; LAN2 and WANb ports should be configured in another port group (it can be done in *Config →Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in third port group in order to have out-band management access (in this case it will be only local management access).

WANa port must be connected to High priority Ethernet data channel (ETH1b), WANb port must be connected to Low priority Ethernet data channel (ETH1a), SFP3/SFP4 ports must be connected to EMM channel (if ASI or E1/T1 EMM is used):

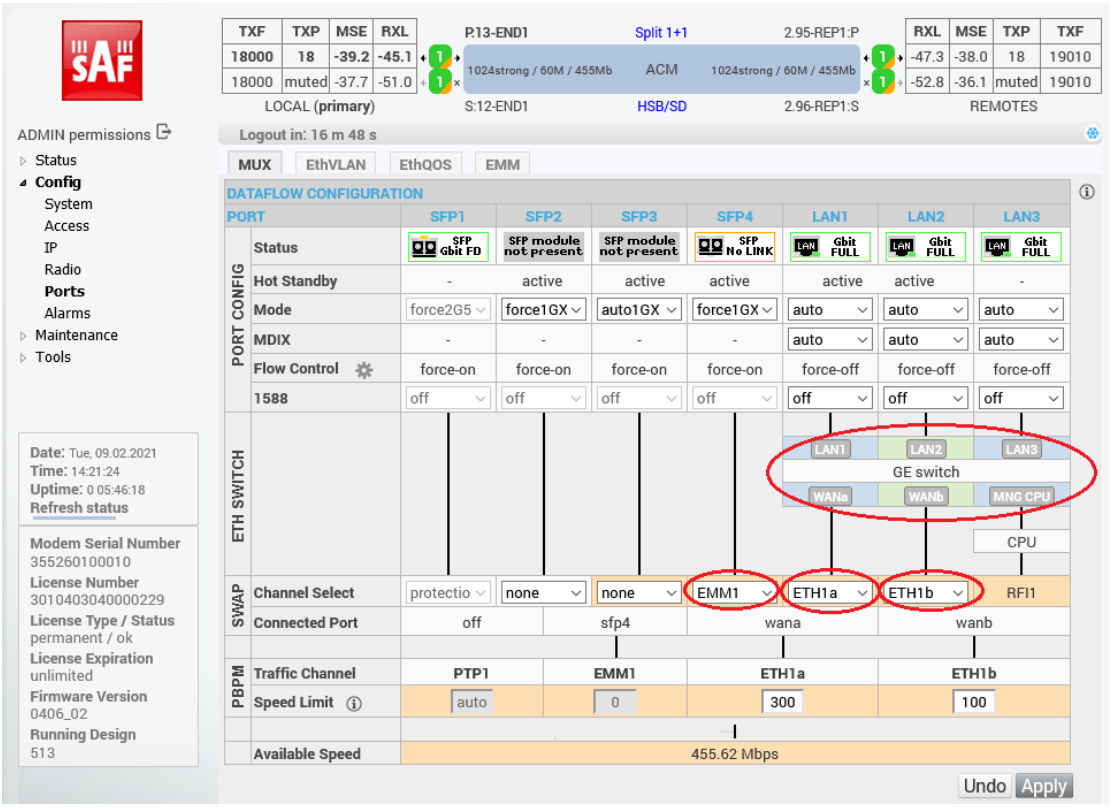


Figure 5.195 *Endpoint Primary IDU Port configuration (scenario 4)*

Endpoint Secondary IDUs must be configured in following way (in *Config → System → Mode* page): Design type ‘Design 513’, Functional mode ‘1+1 Split’, Hot-Swap Startup Role ‘Auto (secondary)’:



Figure 5.196 *Endpoint Secondary IDU System configuration (scenario 4)*

Endpoint Secondary IDU port configuration is following (in *Config →Ports →MUX* page): LAN1, LAN3, WANa and MNG ports should be configured in the same port group; LAN2 and WANb ports should be configured in another port group (it can be done in *Config →Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in third port group in order to have out-band management access (in this case it will be only local management access).

WANa port must be connected to High priority Ethernet data channel (ETH1b), WANb port must be connected to Low priority Ethernet data channel (ETH1a), SFP3/SFP4 ports must be connected to EMM channel (if ASI or E1/T1 EMM is used):

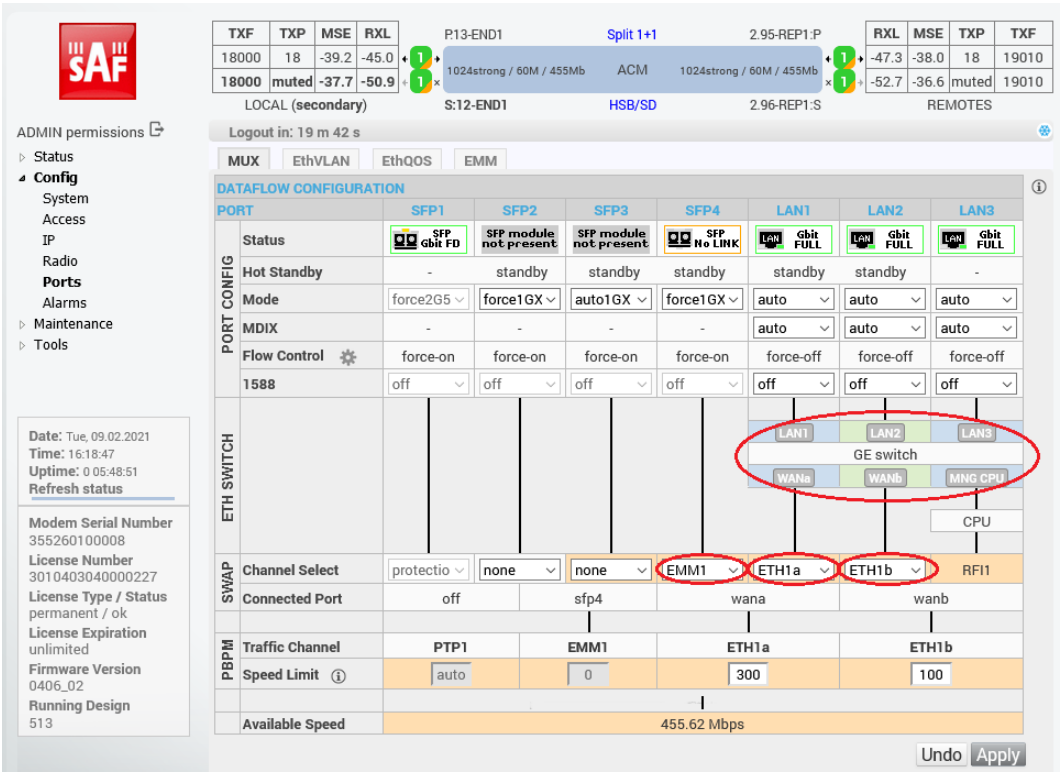


Figure 5.197 *Endpoint Secondary IDU Port configuration (scenario 4)*

Both Repeater site Primary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Repeater', Hot-Swap Startup Role 'Auto (primary)':

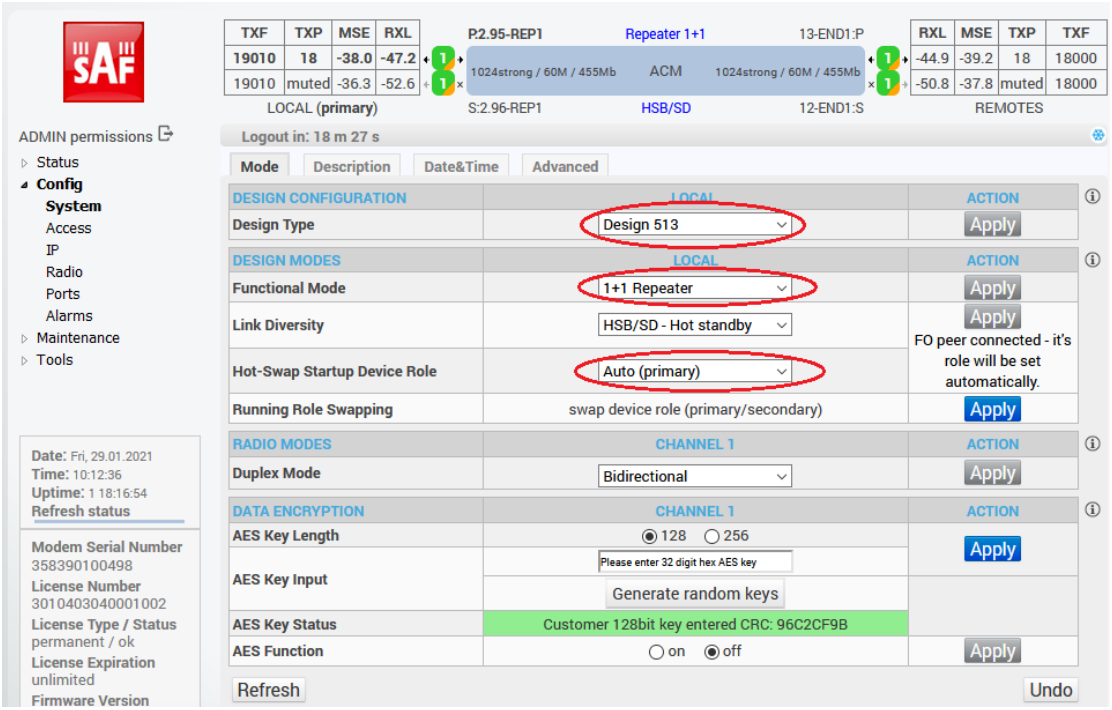


Figure 5.198 *Repeater Primary IDU System configuration (scenario 4)*

Repeater site both Primary IDUs port configuration is following (in *Config → Ports → MUX* page): LAN1, LAN3, WANa and MNG ports should be configured in the same port group; LAN2 and WANb ports should be configured in another port group (it can be done in *Config →Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in third port group in order to have out-band management access (in this case it will be only local management access).

WANa port must be connected to High priority Ethernet data channel (ETH1b), WANb port must be connected to Low priority Ethernet data channel (ETH1a). Hot Standby option for LAN1/LAN2 ports must be set to 'off'. SFP3/SFP4 ports will automatically be dedicated to EMM channel (if ASI or E1/T1 EMM is used):

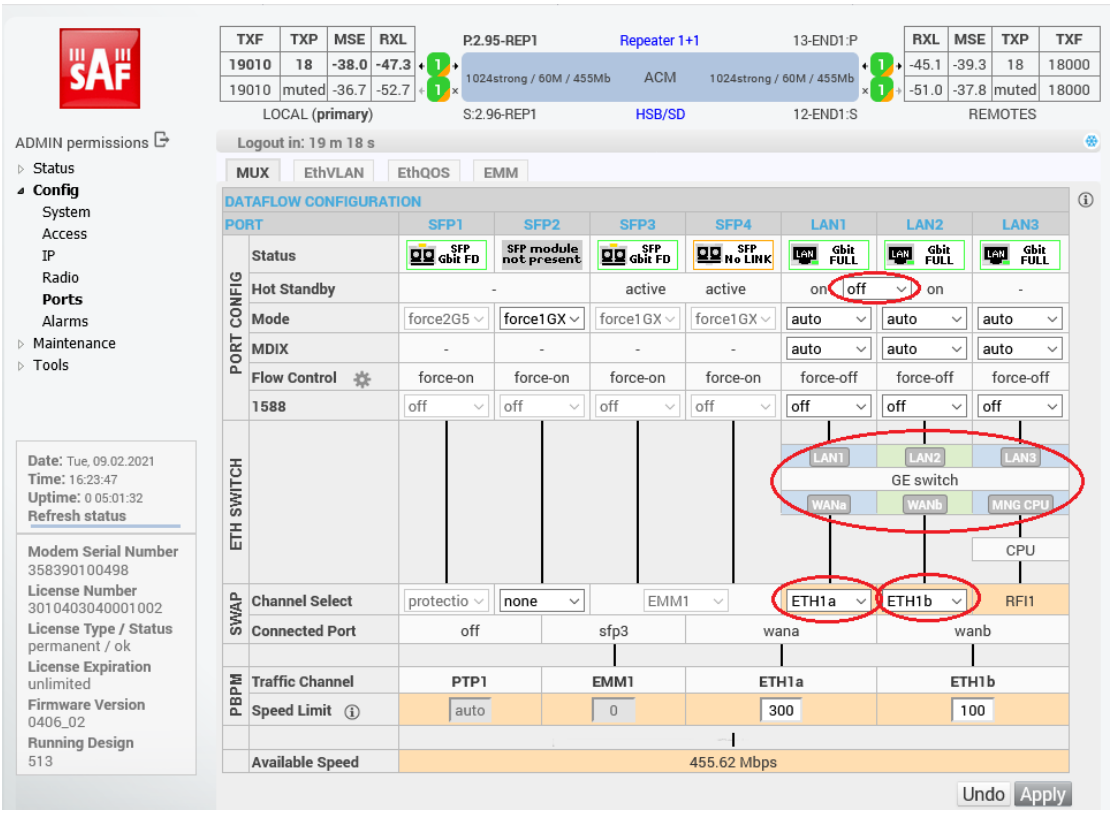


Figure 5.199 *Repeater Primary IDU Port configuration (scenario 4)*

Both Repeater site Secondary IDUs must be configured in following way (in *Config → System → Mode* page): Design type 'Design 513', Functional mode '1+1 Repeater', Hot-Swap Startup Role 'Auto (secondary)':

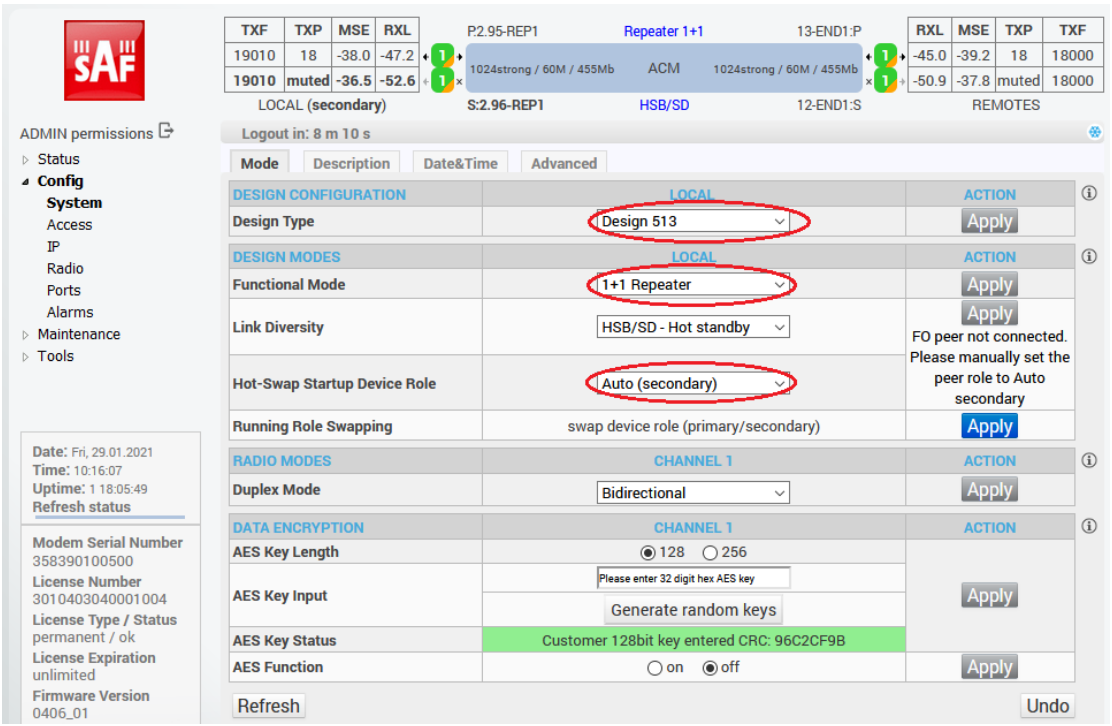


Figure 5.200 *Repeater Secondary IDU System configuration (scenario 4)*

Repeater site both Secondary IDUs port configuration is following (in *Config →Ports →MUX* page): LAN1, LAN3, WANa and MNG ports should be configured in the same port group; LAN2 and WANb ports should be configured in another port group (it can be done in *Config →Ports →EthVLAN* page).



As an alternative LAN3 and MNG ports can be configured in third port group in order to have out-band management access (in this case it will be only local management access).

WANa port must be connected to High priority Ethernet data channel (ETH1b), WANb port must be connected to Low priority Ethernet data channel (ETH1a). Hot Standby option for LAN1/LAN2 ports must be set to 'off'. SFP3/SFP4 ports will automatically be dedicated to EMM channel (if ASI or E1/T1 EMM is used):

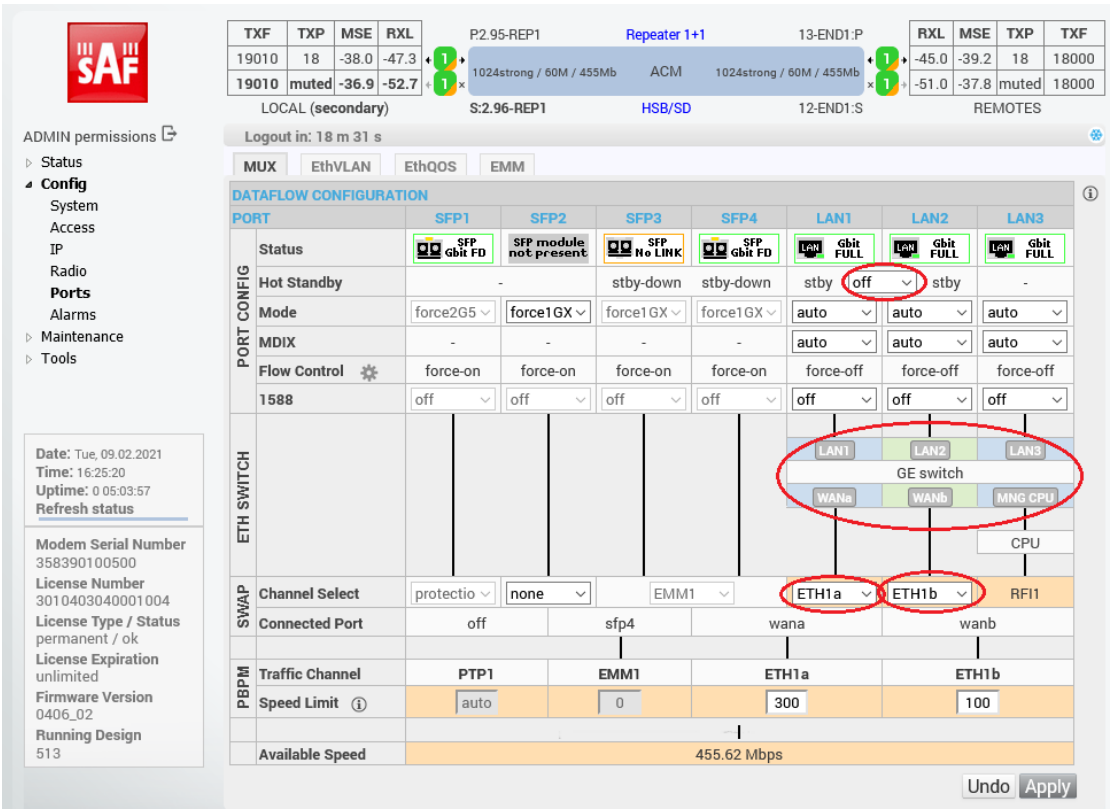


Figure 5.201 *Repeater Secondary IDU Port configuration (scenario 4)*

Alarm configuration is mandatory for all IDUs in Endpoint and in Repeater site as part of alarms are used as initiation of 1+1 switchover (Primary/Secondary role switch). The alarms which are used as criteria for IDU role switch are indicated with PRT label. Those alarms must be enabled according to customer needs for each IDU. Alarm configuration can be done in page *Config →Alarms →General*:

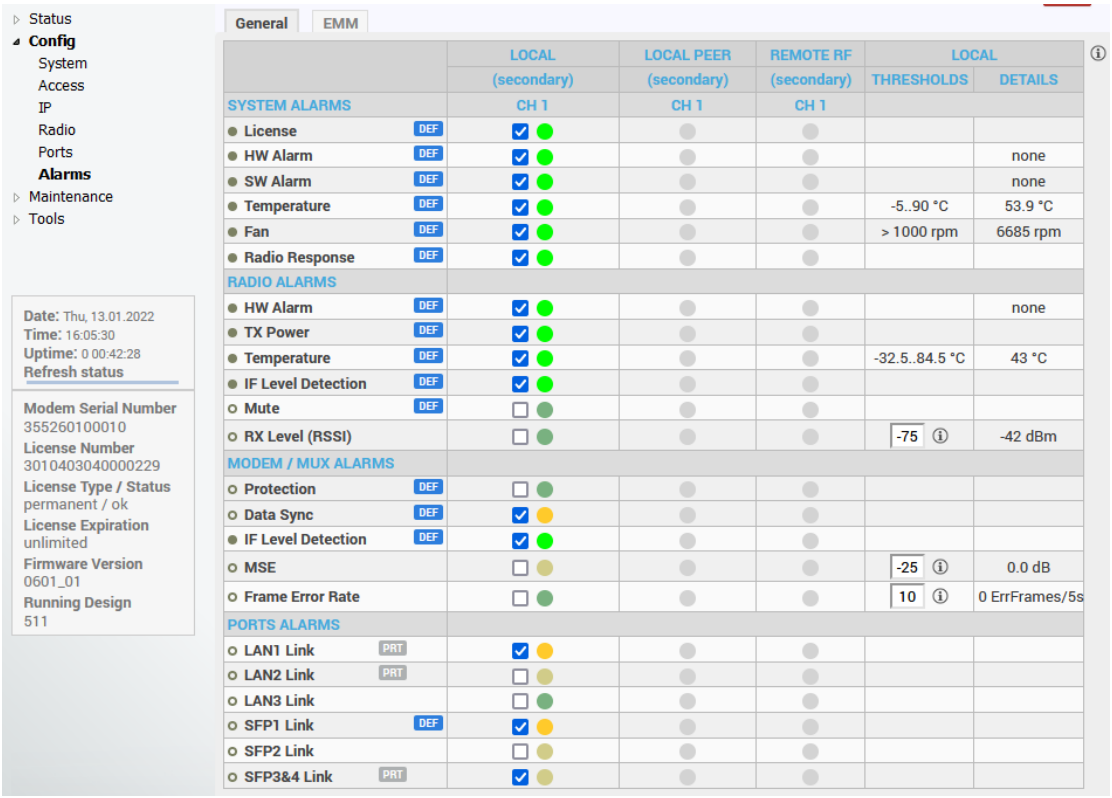


Figure 5.202 *IDU alarm configuration (scenario 4)*

In all the Repeater site IDUs the SFP3 Link and SFP4 Link alarms are merged, so that the alarms will be initiated for both ports together. The alarm configuration can be done for SFP3 Link, but the SFP4 Link alarms will be automatically set

Example 17 – VLAN configuration

The example will describe the VLAN configuration in Phoenix G2 IDUs. In this case the VLAN requirement is following: VLAN ID 100 will be user traffic via LAN1 port and trunked through the link; VLAN ID 200 will be used for Phoenix G2 management (MNG port) access via LAN1 port. WANa port will be used for radio/remote side access. All mentioned ports are grouped in Group 1. The same VLAN configuration must be applied on both side IDUs.

Configuration steps are following:

1) In web GUI *Config->System->EthVLAN* the 'Port Mode' for all ports must be set to "basic" option – this is transparent mode and VLAN mode is disabled:

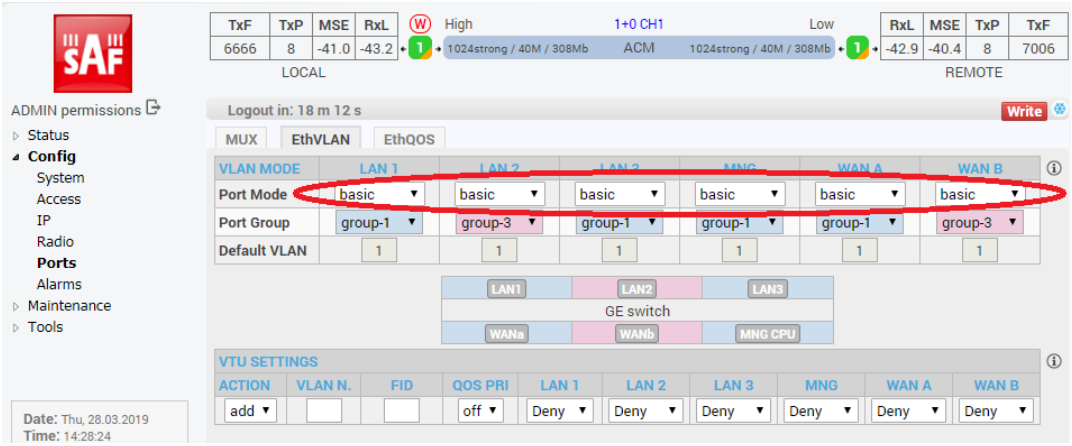


Figure 5.203 *Port mode configuration before VLAN ID configuration*

2) In the same web page in VTU Settings add user traffic VLAN ID 100 tag for LAN1 and WANa ports by choosing option “Tag” in appropriate dropdowns and press Apply button:

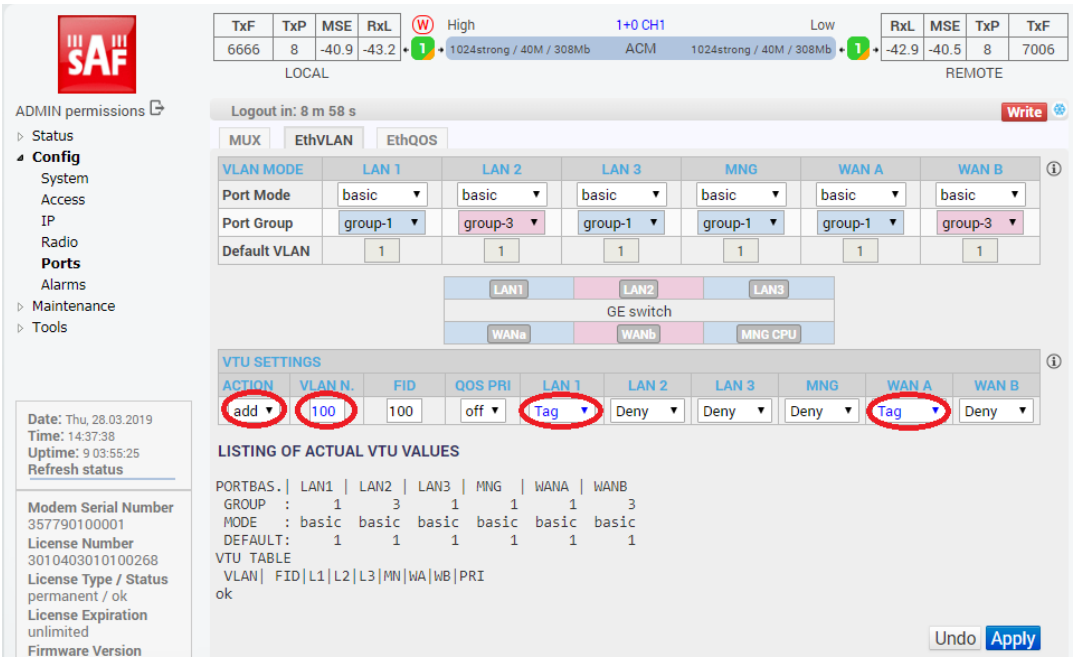


Figure 5.204 *Traffic VLAN configuration*

3) The new applied VLAN ID will be indicated in VTU table:

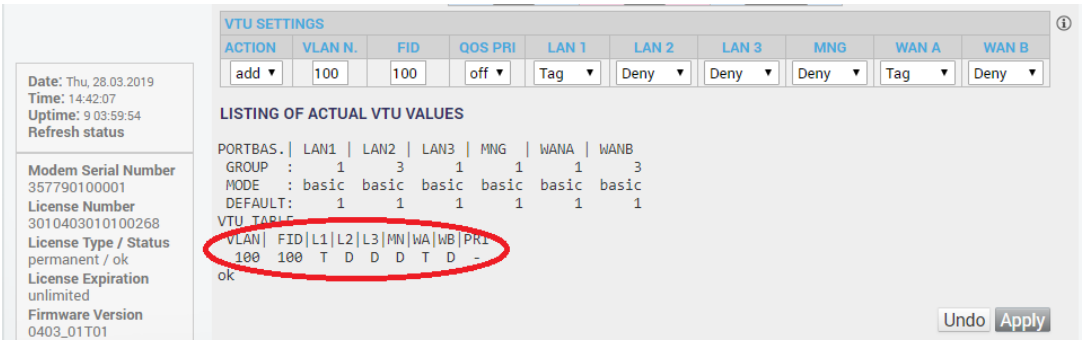


Figure 5.205 *Traffic VLAN configuration*

4) Add management VLAN ID 200 tag for LAN1 and WANa ports by choosing option “Tag” in appropriate dropdowns. Choose “Untag” in MNG port dropdown. Press Apply button. The new configured VLAN ID will be indicated in VTU table and VLAN ID 200 will be indicated as default VLAN for MNG port:

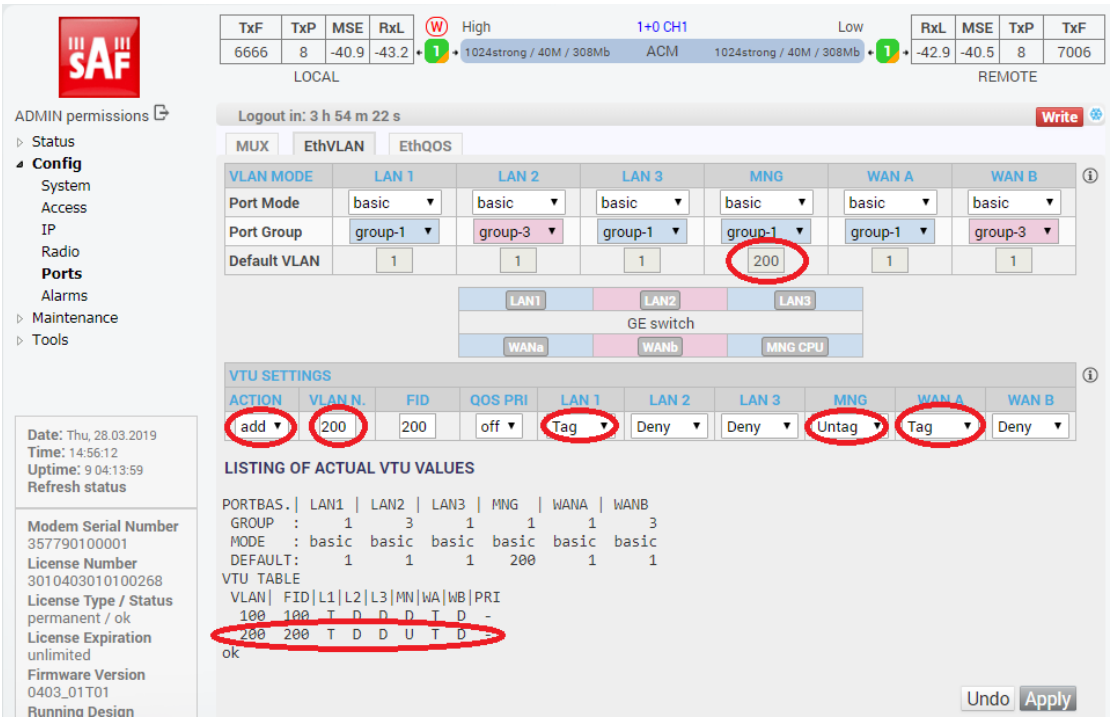


Figure 5.206 *Management VLAN configuration*

5) After configuring VLAN IDs, in the same page enable VLAN mode by setting “Port Mode” for each involved port: set “trunk” mode for LAN1 and WANa port, set “access” mode for MNG port and press Apply button:

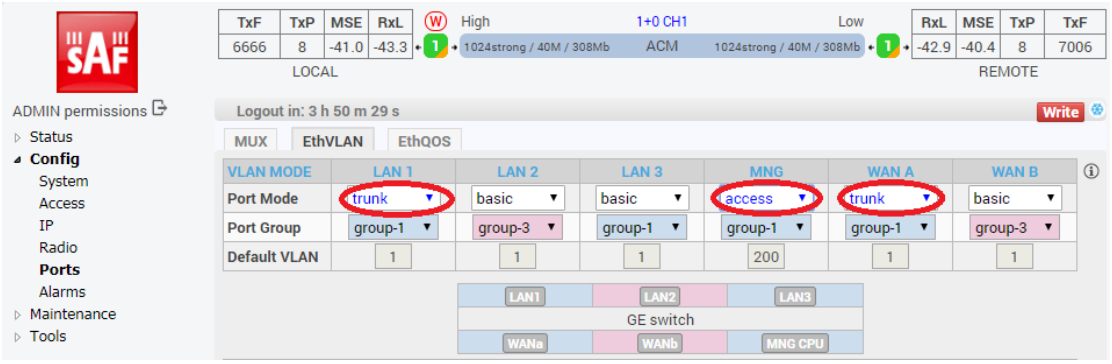


Figure 5.207 *VLAN mode enabling*

6) After applying those settings the management connection between the IDU and computer will be lost, reconnect to the IDU via external switch with appripriate VLAN configuration (VLAN ID 200 for management access)

7) After successful VLAN configuration save new settings by pressing Write button.

Example 18 – PTP channel configuration

PTP (Precision Time Protocol) is used to synchronize clocks over the link or several links. Phoenix G2 supports PTP over Ethernet with specific EtherType = 0x88FT. The purpose of PTP transmission is to keep the constant latency for the PTP signal.

The PTP transmission is supported by the built-in switch via LAN1 and LAN2 ports and is processed over the Phoenix G2 equipment in following way: in transmitting IDU the incoming Ethernet stream from LAN1 or LAN2 port is split into two streams at the input of the built-in switch. The first stream represents data for PTP 1588 identified by means of mentioned EtherType and is subsequently routed to WANb port. The second stream represents remaining standard Ethernet data and is subsequently routed to WANa port. Both data streams are further processed independently. A timestamp for PTP data stream is set when it is passed through the WANb port. The PTP data stream is further processed with the higher priority. In the receiving IDU both data streams are received into the built-in switch via the same WAN ports (PTP in WANb and Ethernet in WANa) and are merged into one data stream in LAN1 or LAN2 port.

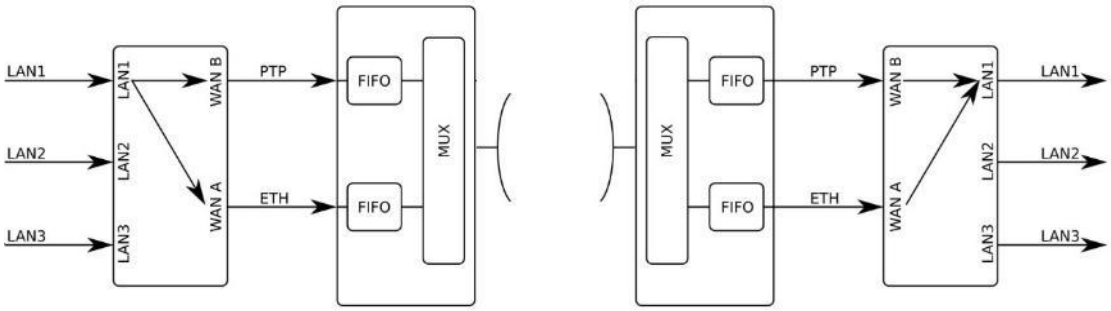


Figure 5.208 *PTP processing block-scheme*

The example will describe PTP 1588 configuration in Phoenix G2 IDUs. In this case LAN1 port will be used for PTP 1588 and Ethernet traffic stream. Management will be accessible via LAN1 and LAN3 ports. The same PTP 1588 configuration must be applied on both side IDUs.

Configuration steps are following:

1) In web GUI *Config->Ports->MUX* set “1588” option as “on” for LAN1 and press Apply button. This setting will automatically enable the Channel “PTP1” for WANb port. Channel “PTP1” can be set also manually for WANb port. The WANb cell indication will become yellow indicating Group 4 for WANb port. Select “ETH1a” channel for WANa port for passing Ethernet traffic over the link:

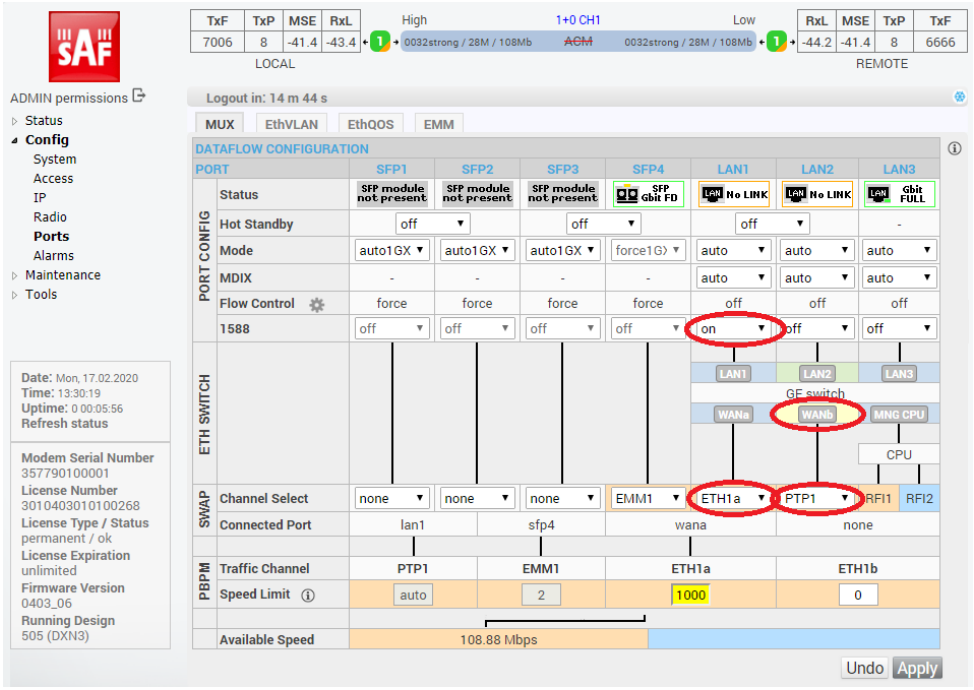


Figure 5.209 *PTP port configuration*

2) Group 4 (timing) for WANb port also will be indicated in web GUI *Config->Ports->EthVLAN* page. It will be set automatically, but can be set also manually when required. Set Group1 for WANa, LAN1, LAN3 and MNG CPU ports in this same page and press Apply button:

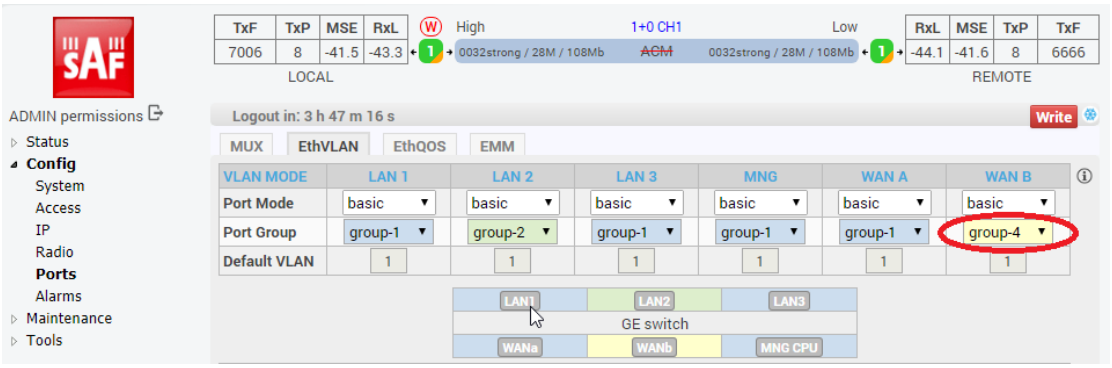


Figure 5.210 *PTP group configuration*

3) After successful PTP configuration save new settings by pressing Write button.

Example 19 – Pri-Sec interconnection (Summed mode) configuration

Pri-Sec interconnection functionality (further – Summed mode) can be used to get two independent simultaneous IP traffics (IP traffic 1 and IP traffic 2) over the 1+1 Split Protection (Full redundancy) link. Different port group configurations of Summed mode allow In-band management access (in the same cable/port with the IP traffic 1 or in the same cable/port with the IP traffic 2) and Out-band management access.

In-band management access: IP traffic 1 + MNG option

The utilization of IP traffic 1 and IP traffic 2 in this option is following:

1) IP traffic 1 (over ETH1a channel):
   a) IP traffic 1 from the external equipment is connected to Phoenix G2 Primary IDU LAN1 port
   b) LAN1 port must be configured in the same port group with WANA, LAN3 and MNG ports. WANA port must be interconnected with High priority ETH1a channel
   c) According to the 1+1 Protection algorithm the Primary IDU is the one which is passing the data over the link – so the IP traffic 1 is passed through the ETH1a channel of Primary IDUs
   d) LAN2 port of the Primary IDU and LAN1 port of the Secondary IDU are interconnected with Ethernet jumper cable
   e) In case of protection switchover and IDU role change: after the IDU role change the IP traffic 1 is passed via new Secondary IDU LAN1 port and internally copied to new Secondary IDU LAN2 port, and sent to the new Primary IDU LAN1 port via Ethernet jumper cable
2) IP traffic 2 (over ETH1b channel):
   a) IP traffic 2 from the external equipment is connected to the Phoenix G2 Secondary IDU LAN2 port
   b) In the Secondary IDU LAN2 port is internally copied to Secondary IDU LAN1 port. Secondary IDU LAN1 port is interconnected with Primary IDU LAN2 port with Ethernet jumper cable
   c) LAN2 port in Primary IDU must be configured in the same group with WANB which must be interconnected with Low Priority ETH1b channel
   d) According to the 1+1 Protection algorithm the Secondary IDU does not pass the data over the link – all the traffic is organized over the Primary link/IDUs
   e) In case of protection switchover and IDU role change: after the IDU role change, the IP traffic 2 is passed through the LAN2 port in the new Primary IDU

Instructions about IDU management access:

   a) The in-band management data is passed together with IP traffic 1 data through the ETH1a channel which is interconnected with WANA port. LAN1, LAN3, MNG and WANA ports in the Primary IDU are in the same port group
   b) LAN3 ports on Primary IDU and Secondary IDU must be interconnected with Ethernet jumper cable in order to have management data transmission between Primary and Secondary IDUs

Internal and external interconnection scheme of Summed mode with In-band management access option IP traffic 1 + MNG is as follows:

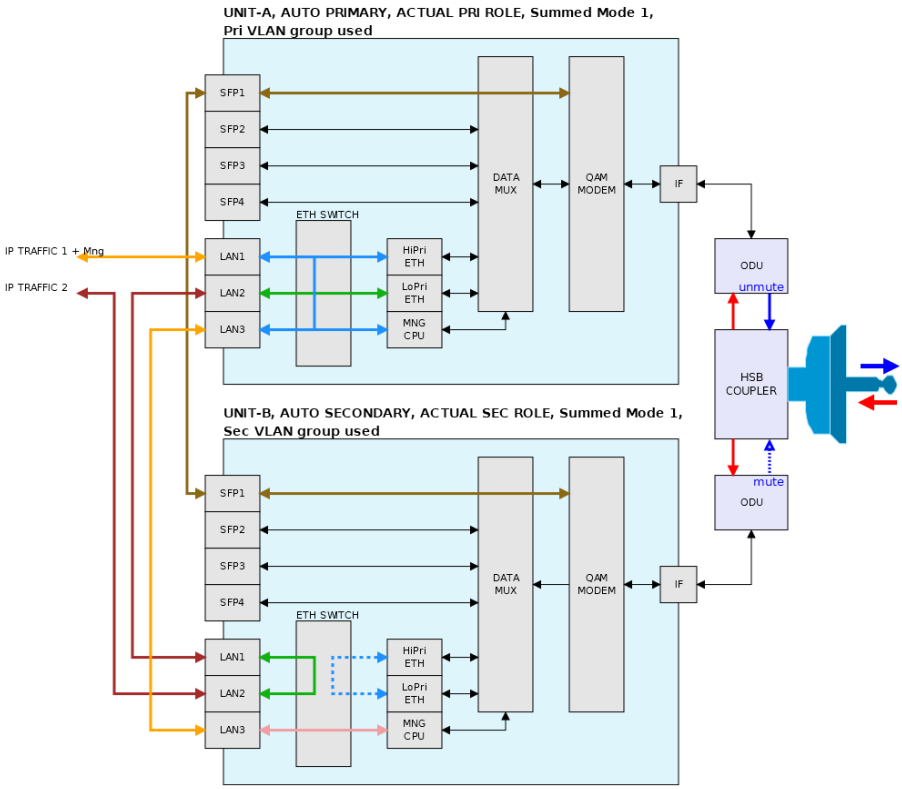


Figure 5.211 *Summed mode interconnection scheme IP traffic 1 + MNG*

Internal interconnection scheme of Summed mode with In-band management access option IP traffic 1 + MNG after IDU role change (1+1 switchover) is as follows:

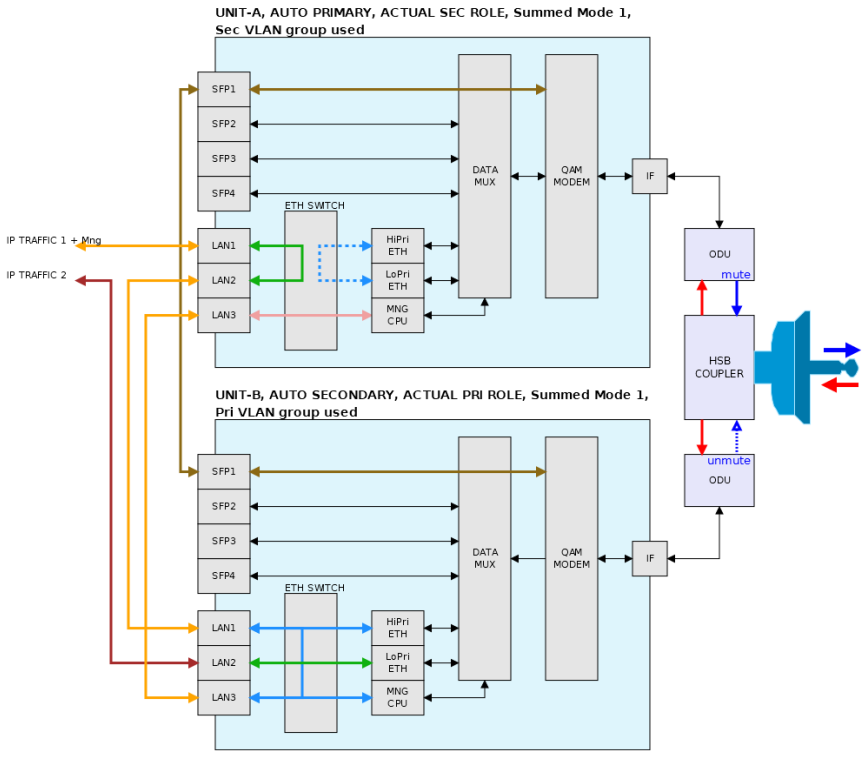


Figure 5.212 *Summed mode interconnection scheme IP traffic 1 + MNG after IDU role change*

The example will describe Summed mode configuration in Phoenix G2 IDUs. In this case Phoenix G2 link is already configured as 1+1 HSB/SD Full Redundancy link (refer to *Example 14 – 1+1 HSB/SD Full protection mode (Design 511/513)*).

Configuration steps for “Summed mode 1” with in-band management IP traffic 1+ MNG are following:

1) In web GUI page *Config->System->Mode* set “Pri-Sec LAN Interconnection” option as “Summed mode1” and press Apply button. This setting must be chosen in both IDUs – Primary and Secondary:

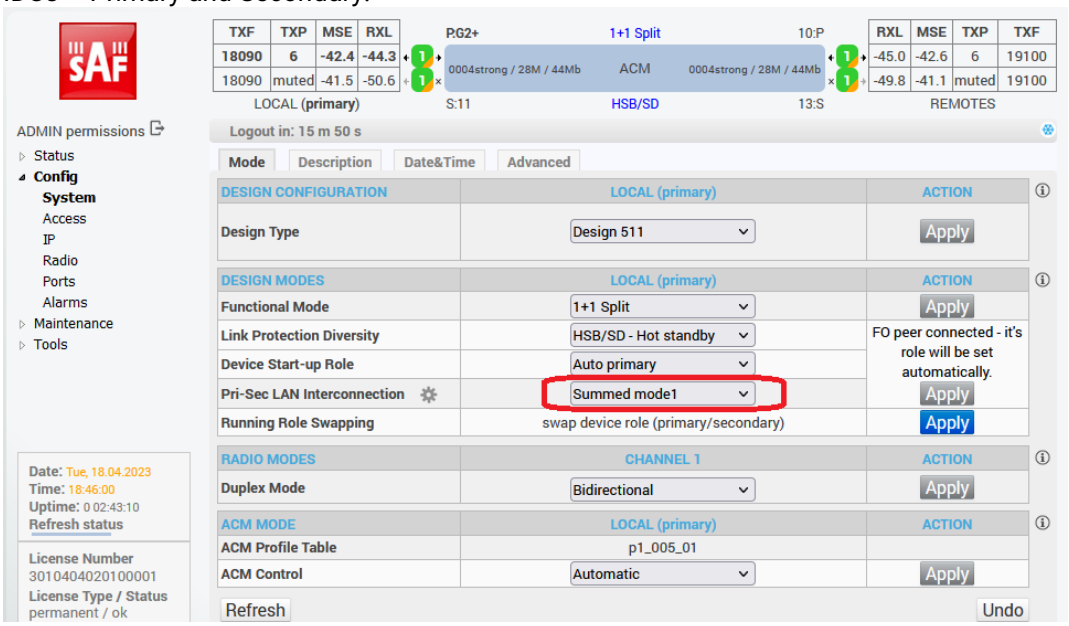


Figure 5.213 *Summed mode 1 configuration*

2) Navigate to *Config->Ports->EthVLAN* and configure the port groups as following: LAN1, LAN3, MNG and WANA ports in port group 1, LAN2 and WANB ports in port group 2. The same port grouping must be configured in both Primary and Secondary IDUs:

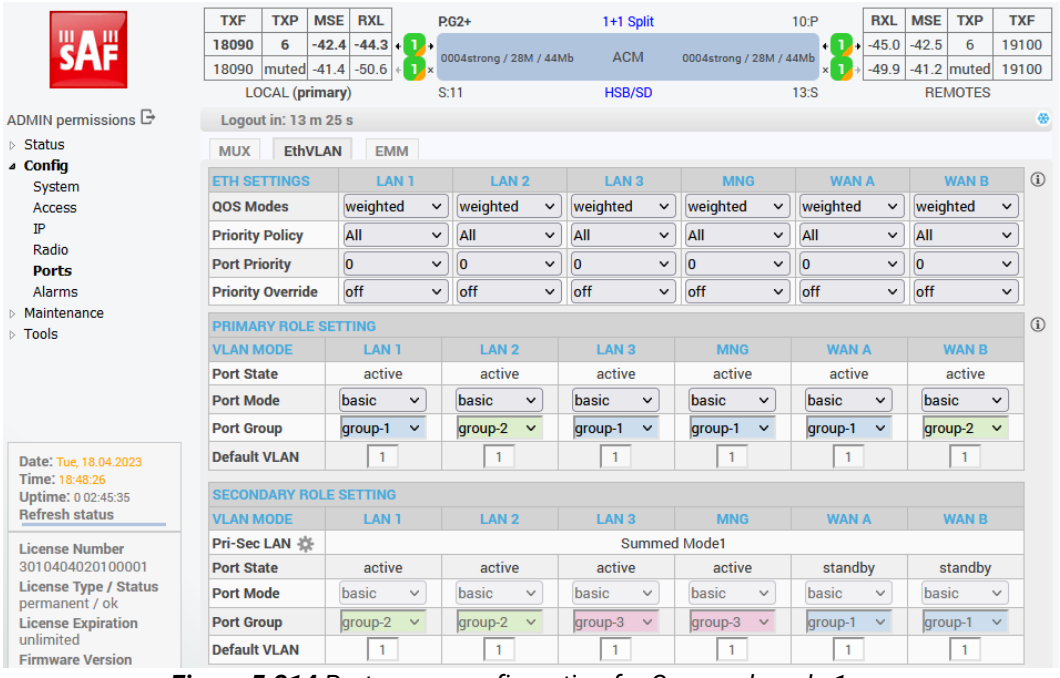


Figure 5.214 *Port group configuration for Summed mode 1*

3) Navigate to *Config->Ports->MUX* and interconnect WANA port with ETH1a High priority channel and WANB port with ETH1b Low priority channel. Make sure the speed limit is configured for each channel as per customer's requirements:

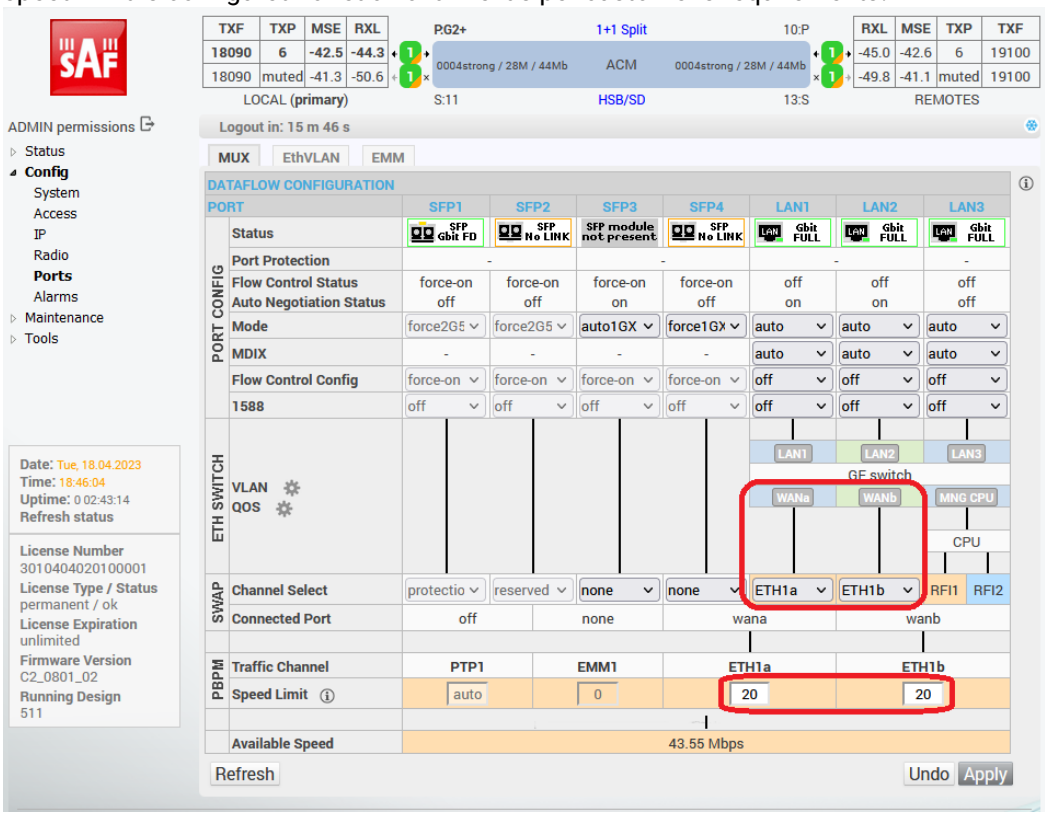


Figure 5.215 *Ethernet channel configuration for Summed mode 1*

4) Save the configuration by pressing Write button

In-band management access: IP traffic 2 + MNG option

The utilization of IP traffic 1 and IP traffic 2 in this option is following:

1) IP traffic 1 (over ETH1a channel):
   a) IP traffic 1 from the external equipment is connected to Phoenix G2 Primary IDU LAN1 port
   b) LAN1 port must be configured in the same port group with WANA port which must be interconnected with High priority ETH1a channel
   c) According to the 1+1 Protection algorithm the Primary IDU is the one which is passing the data over the link – so the IP traffic 1 is passed through the ETH1a channel of Primary IDUs
   d) LAN2 port of the Primary IDU and LAN1 port of the Secondary IDU are interconnected with Ethernet jumper cable
   e) In case of protection switchover and IDU role change: after the IDU role change the IP traffic 1 is passed via new Secondary IDU LAN1 port and internally copied to new Secondary IDU LAN2 port, and sent to the new Primary IDU LAN1 port via Ethernet jumper cable
2) IP traffic 2 (over ETH1b channel):
   a) IP traffic 2 from the external equipment is connected to the Phoenix G2 Secondary IDU LAN2 port
   b) In the Secondary IDU LAN2 port is internally copied to Secondary IDU LAN1 port. Secondary IDU LAN1 port is interconnected with Primary IDU LAN2 port with Ethernet jumper cable

c) LAN2 port in Primary IDU must be configured in the same group with LAN3, MNG and WANB ports. WANB port must be interconnected with Low Priority ETH1b channel
d) According to the 1+1 Protection algorithm the Secondary IDU does not pass the data over the link – all the traffic is organized over the Primary link/IDUs
e) In case of protection switchover and IDU role change: after the IDU role change, the IP traffic 2 is passed through the LAN2 port in the new Primary IDU

Instructions about IDU management access:

a) The in-band management data is passed together with IP traffic 2 data through the ETH1b channel which is interconnected with WANB port. LAN2, LAN3, MNG and WANB ports in the Primary IDU are in the same port group
b) LAN3 ports on Primary IDU and Secondary IDU must be interconnected with Ethernet jumper cable in order to have management data transmission between Primary and Secondary IDUs

Internal and external interconnection scheme of Summed mode with In-band management access option IP traffic 2 + MNG is as follows:

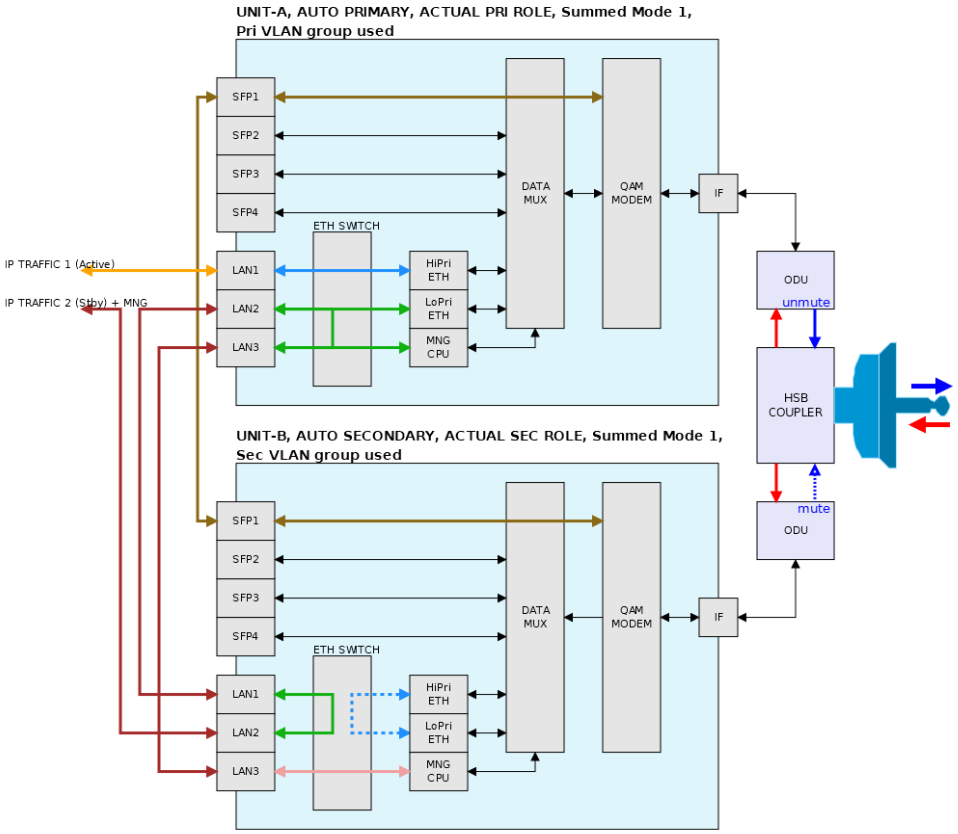


Figure 5.216 *Summed mode interconnection scheme IP traffic 2 + MNG*

Internal interconnection scheme of Summed mode with In-band management access option IP traffic 2 + MNG after IDU role change (1+1 switchover) is as follows:

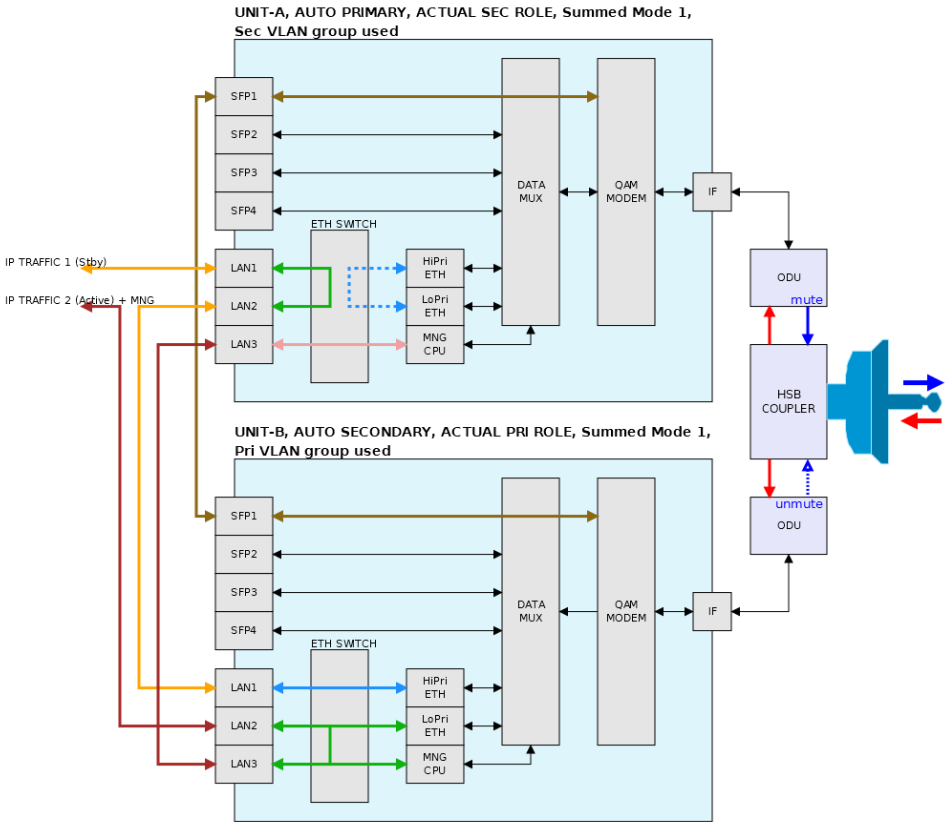


Figure 5.217 *Summed mode interconnection scheme IP traffic 2 + MNG after IDU role change*

The example will describe Summed mode configuration in Phoenix G2 IDUs. In this case Phoenix G2 link is already configured as 1+1 HSB/SD Full Redundancy link (refer to *Example 14 – 1+1 HSB/SD Full protection mode (Design 511/513)*).

Configuration steps for "Summed mode 1" with in-band management IP traffic 2 + MNG are following:

1) In web GUI page *Config->System->Mode* set "Pri-Sec LAN Interconnection" option as "Summed mode1" and press Apply button. This setting must be chosen in both IDUs – Primary and Secondary:

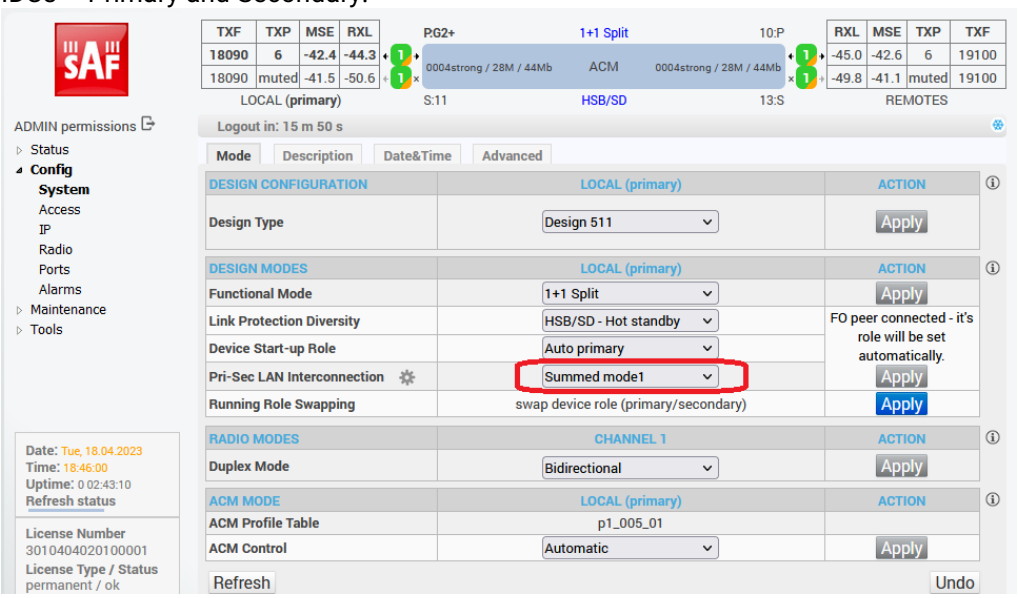


Figure 5.218 *Summed mode 1 configuration*

2) Navigate to *Config->Ports->EthVLAN* and configure the port groups as following: LAN1 and WANA ports in port group 1, LAN2, LAN3, MNG and WANB ports in port group 2. The same port grouping must be configured in both Primary and Secondary IDUs:

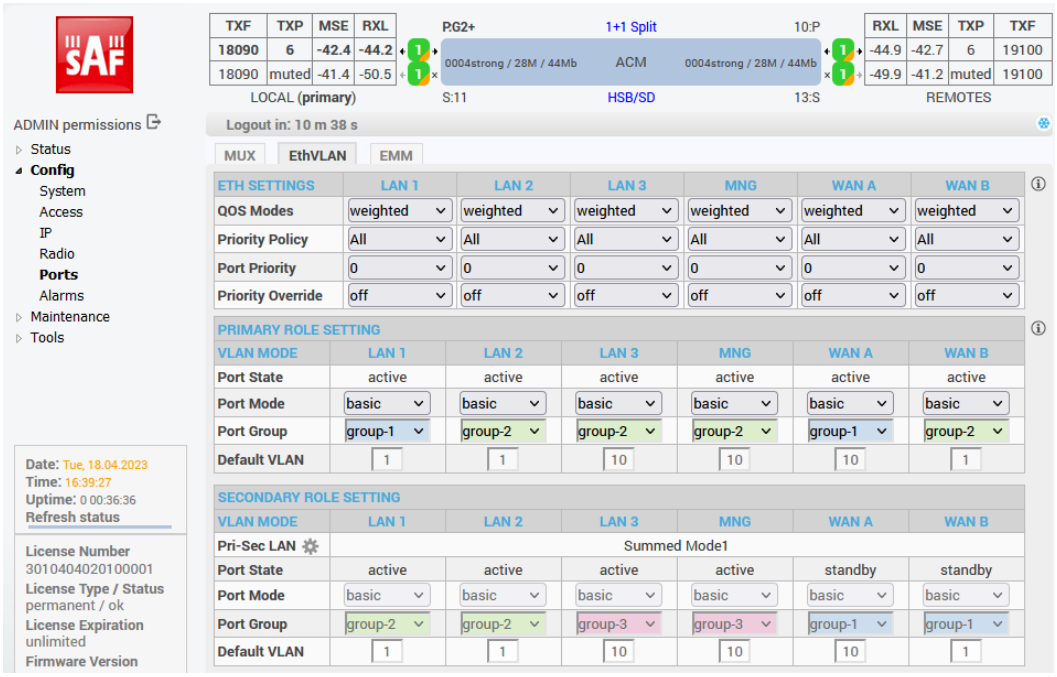


Figure 5.219 *Port group configuration for Summed mode 1*

3) Navigate to *Config->Ports->MUX* and interconnect WANA port with ETH1a High priority channel and WANB port with ETH1b Low priority channel. Make sure the speed limit is configured for each channel as per customer's requirements:

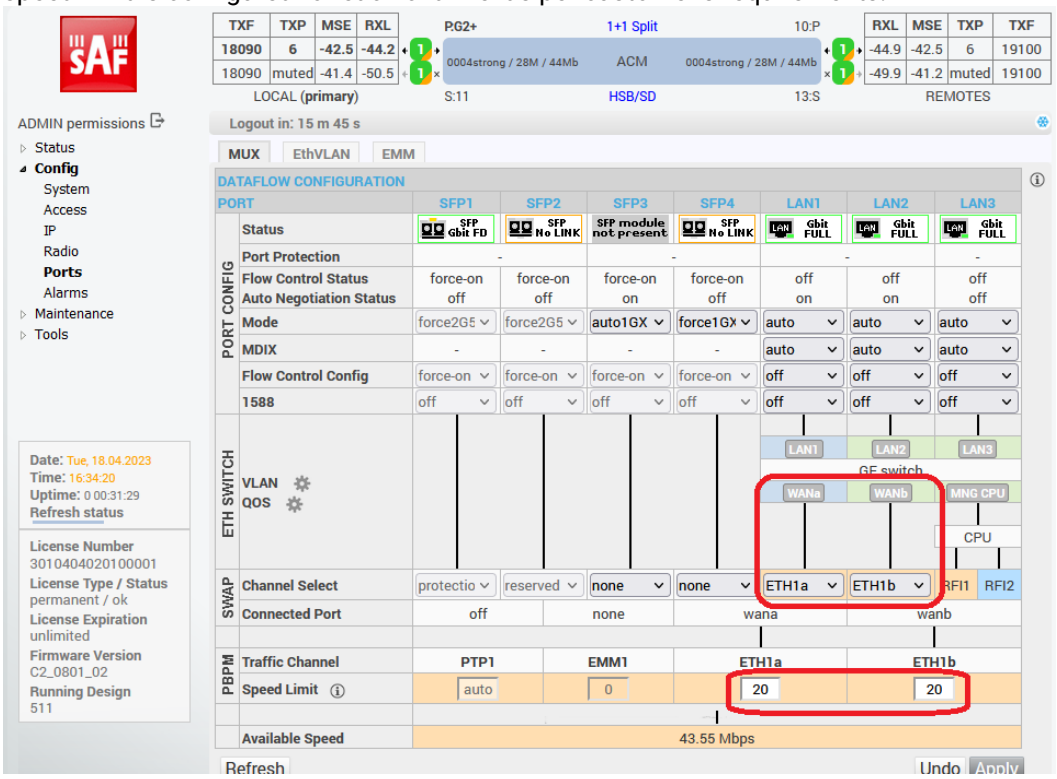


Figure 5.220 *Ethernet channel configuration for Summed mode 1*

4) Save the configuration by pressing Write button

Out-band management access

The utilization of IP traffic 1 and IP traffic 2 in this option is following:

1) IP traffic 1 (over ETH1a channel):
   a) IP traffic 1 from the external equipment is connected to Phoenix G2 Primary IDU LAN1 port
   b) LAN1 port must be configured in the same port group with WANA port which must be interconnected with High priority ETH1a channel
   c) According to the 1+1 Protection algorithm the Primary IDU is the one which is passing the data over the link – so the IP traffic 1 is passed through the ETH1a channel of Primary IDUs
   d) LAN2 port of the Primary IDU and LAN1 port of the Secondary IDU are interconnected with Ethernet jumper cable
   e) In case of protection switchover and IDU role change: after the IDU role change the IP traffic 1 is passed via new Secondary IDU LAN1 port and internally copied to new Secondary IDU LAN2 port, and sent to the new Primary IDU LAN1 port via Ethernet jumper cable
2) IP traffic 2 (over ETH1b channel):
   a) IP traffic 2 from the external equipment is connected to the Phoenix G2 Secondary IDU LAN2 port
   b) In the Secondary IDU LAN2 port is internally copied to Secondary IDU LAN1 port. Secondary IDU LAN1 port is interconnected with Primary IDU LAN2 port with Ethernet jumper cable
   c) LAN2 port in Primary IDU must be configured in the same group with WANB port which must be interconnected with Low Priority ETH1b channel
   d) According to the 1+1 Protection algorithm the Secondary IDU does not pass the data over the link – all the traffic is organized over the Primary link/IDUs
   e) In case of protection switchover and IDU role change: after the IDU role change, the IP traffic 2 is passed through the LAN2 port in the new Primary IDU

Instructions about IDU management access:

   a) The out-band management data is accessible through the LAN3 ports of Primary and Secondary IDUs only, separated from the IP traffic
   b) LAN3 port in the Primary IDU must be configured in the same group with MNG port
   c) LAN3 ports of Primary and Secondary IDUs must be connected to external customer's network device using Ethernet jumper cables in order to have management access to both Primary and Secondary IDUs
   d) In this configuration only local management access to both IDUs is available

Internal and external interconnection scheme of Summed mode with Out-band management access is as follows:

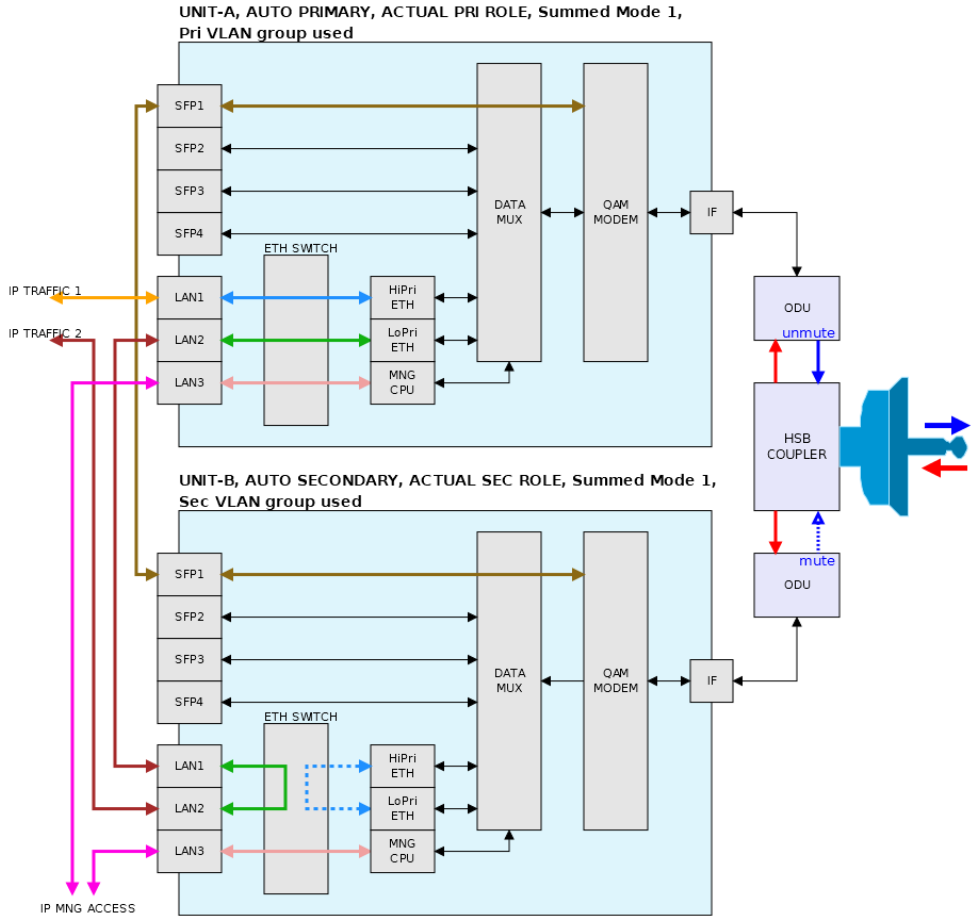


Figure 5.221 *Summed mode interconnection scheme out-band MNG*

Internal interconnection scheme of Summed mode with Out-band management access after IDU role change (1+1 switchover) is as follows:

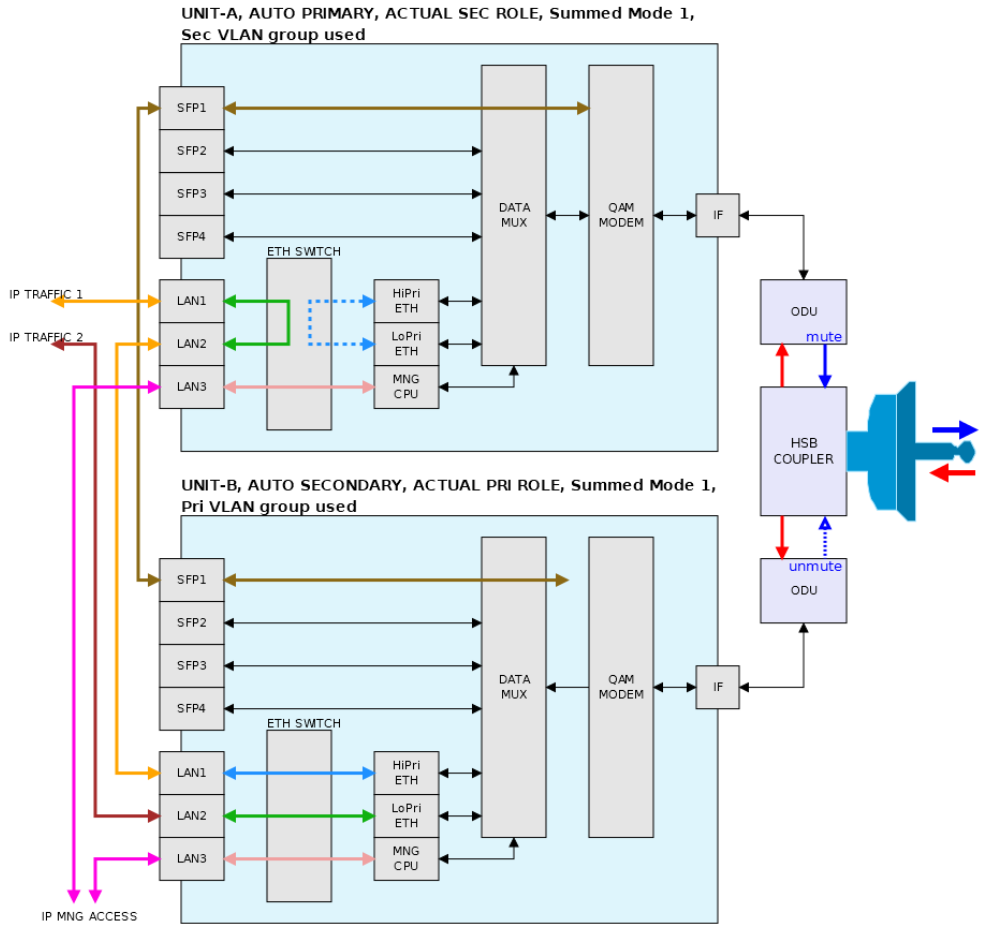


Figure 5.222 *Summed mode interconnection scheme out-band MNG after IDU role change*

The example will describe Summed mode configuration in Phoenix G2 IDUs. In this case Phoenix G2 link is already configured as 1+1 HSB/SD Full Redundancy link (refer to *Example 14 – 1+1 HSB/SD Full protection mode (Design 511/513)*).

Configuration steps for “Summed mode 1” with out-band management are following:

1) In web GUI page *Config->System->Mode* set “Pri-Sec LAN Interconnection” option as “Summed mode1” and press Apply button. This setting must be chosen in both IDUs – Primary and Secondary:

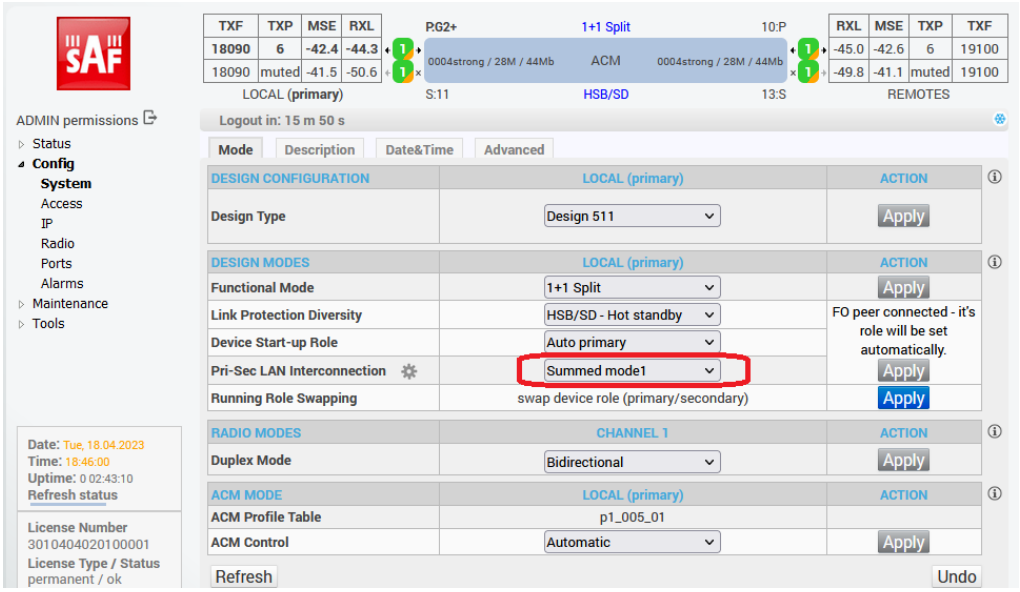


Figure 5.223 *Summed mode 1 configuration*

2) Navigate to *Config->Ports->EthVLAN* and configure the port groups as following: LAN1 and WANA ports in port group 1, LAN2 and WANB ports in port group 2, LAN3 and MNG ports in port group 3. The same port grouping must be configured in both Primary and Secondary IDUs:

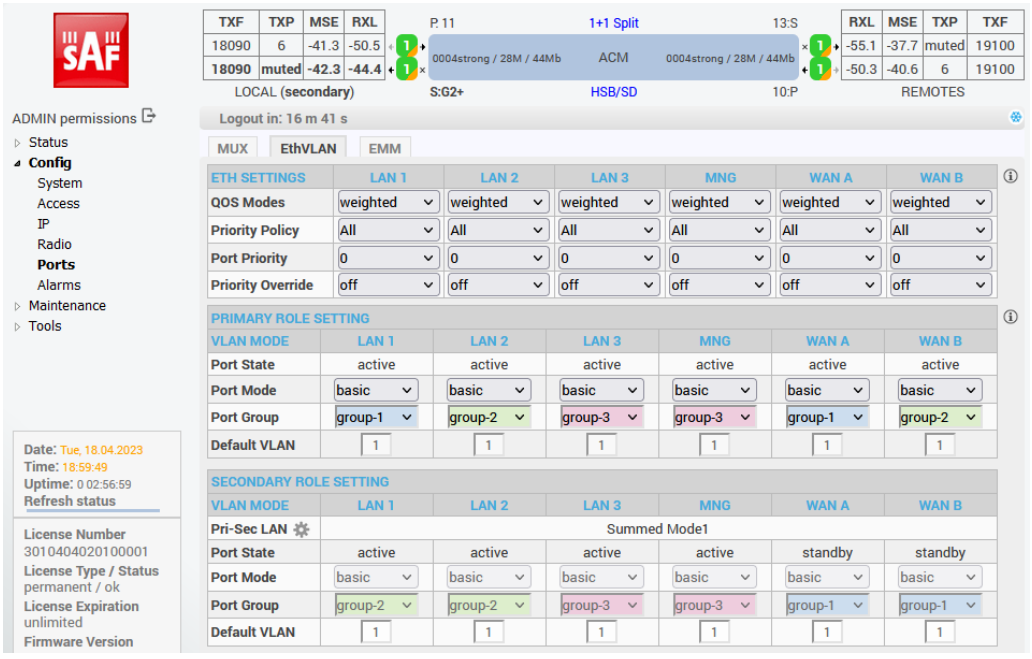


Figure 5.224 *Port group configuration for Summed mode 1*

3) Navigate to *Config->Ports->MUX* and interconnect WANA port with ETH1a High priority channel and WANB port with ETH1b Low priority channel. Make sure the speed limit is configured for each channel as per customer's requirements:

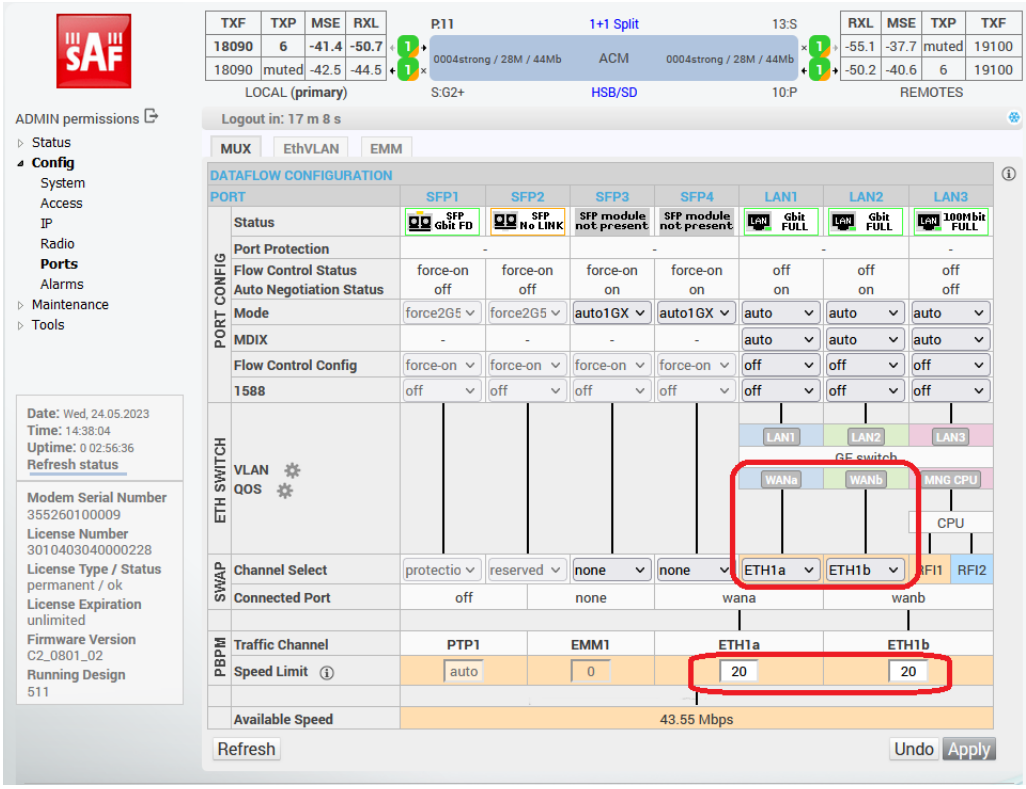


Figure 5.225 *Ethernet channel configuration for Summed mode 1*

4) Save the configuration by pressing  button

Example 20 – ASI traffic retranslation over repeater

This example describes the ASI traffic retranslation without connecting ASI EMM modules in the repeater site when both repeater links are configured in basic 1+1HSB/SD (Design 505) configuration. Similar configuration can be applied if using E1/T1 EMM modules and if both repeater links are configured in any other Design 505 configuration, like 1+0, 1+1SD and 1+1FD. Interconnection scheme of this setup will be following:

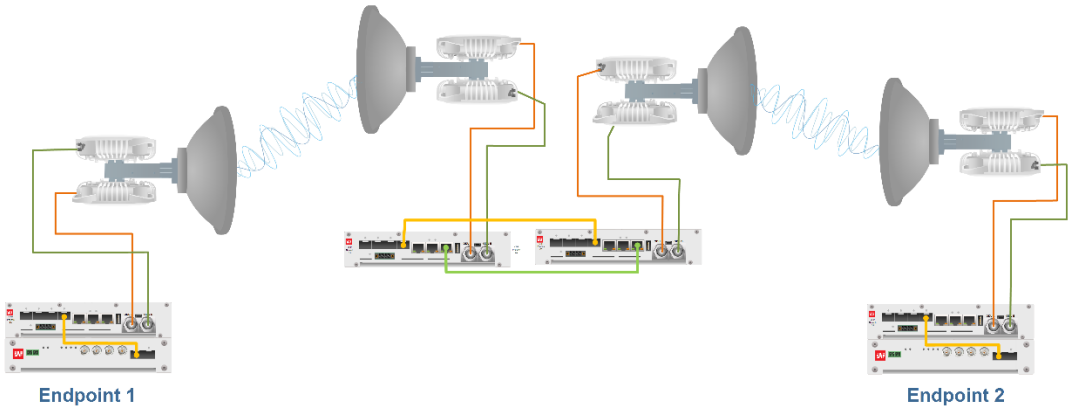


Figure 5.226 *ASI EMM retranslation in repeater link*

In the example both repeater links will be configured as basic 1+1HSB/SD (Design 505) configuration. As the reference for this configuration use *Example 2 – 1+1 HSB/SD mode*

(Design 505) in this document. ASI stream will be transmitted over the ASI 1 channel from Endpoint 1 to Endpoint 2.

Configuration steps for ASI EMM settings in endpoint IDUs and Repeater IDUs are following:

1) On both endpoints interconnect Phoenix G2 IDUs and ASI EMMs via SFP4 port on the IDUs and SFP1 port on the ASI EMMs. Use optical cable kit as described in *Cable requirements* section
2) On both endpoint IDUs web GUI navigate to *Config->Ports->MUX* page and select channel EMM1 for SFP4 ports as indicated in the following example:

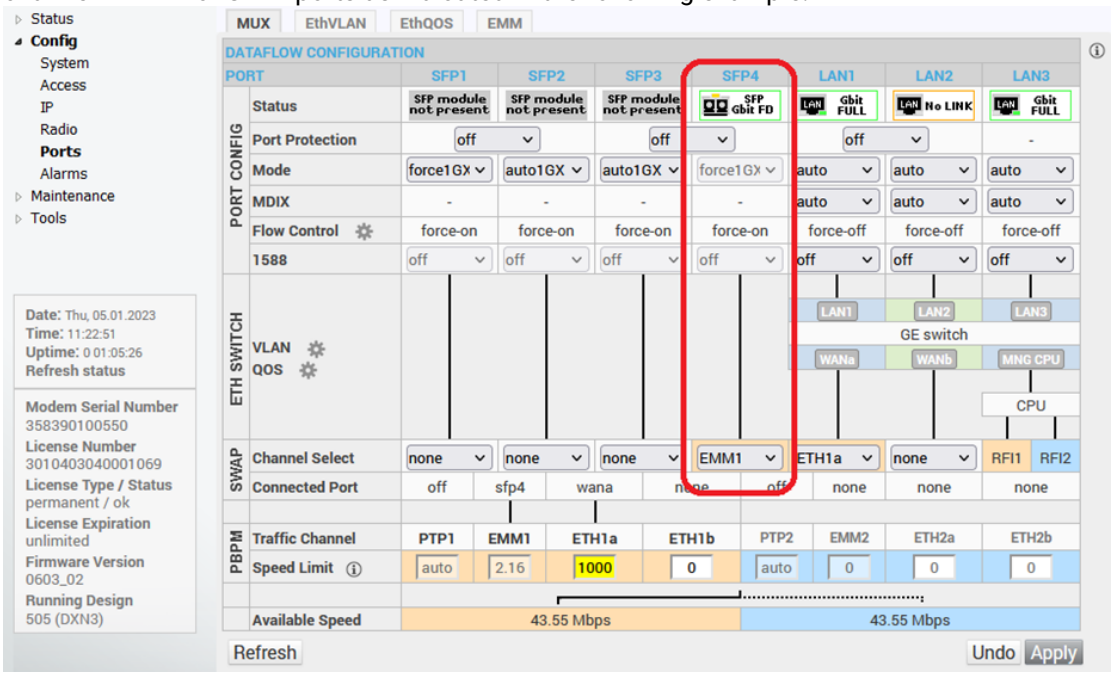


Figure 5.227 *SFP port configuration in endpoint IDUs*

3) On the Endpoint 1 IDU web GUI navigate to *Config->Ports->EMM* page and enable ASI EMM card as shown in following screenshot. Choose EMM type “4ASI”, enable ASI EMM and ASI1 channel, set ASI channel mode to Rx:

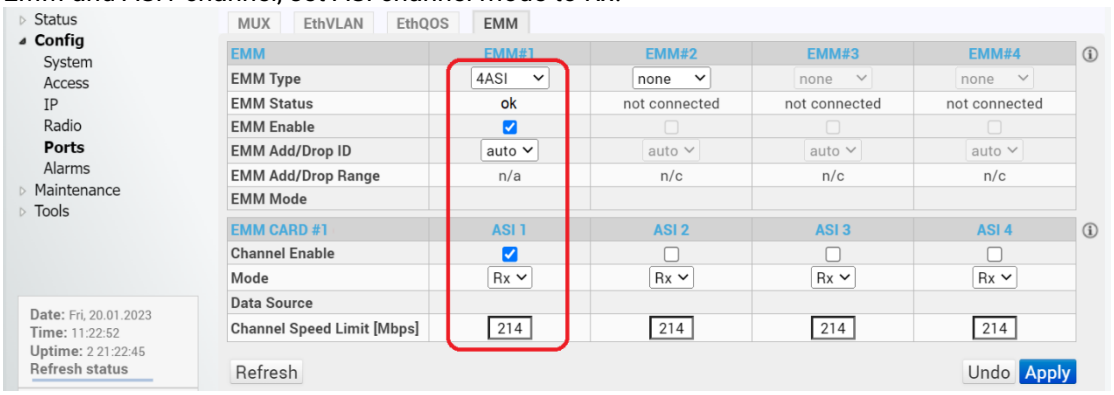


Figure 5.228 *ASI EMM configuration in Endpoint 1 IDU*

4) On the Endpoint 2 IDU web GUI navigate to *Config->Ports->EMM* page and enable ASI EMM card as shown in following screenshot. Choose EMM type “4ASI”, enable ASI EMM and ASI1 channel, set ASI channel mode to Tx, choose “Remote Ch1” as data source:

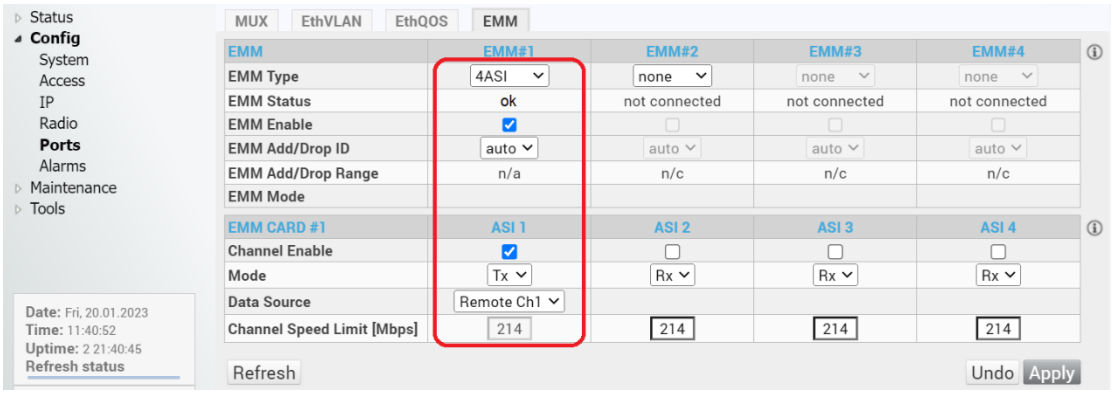


Figure 5.229 *ASI EMM configuration in Endpoint 2 IDU*

5) Interconnect both repeater IDUs via SFP4 ports. Use optical cable kit as described in *Cable requirements* section.
6) In both repeater IDUs web GUI navigate to *Config->Ports->MUX* and select channel EMM1 for SFP4 ports as indicated in the following example:

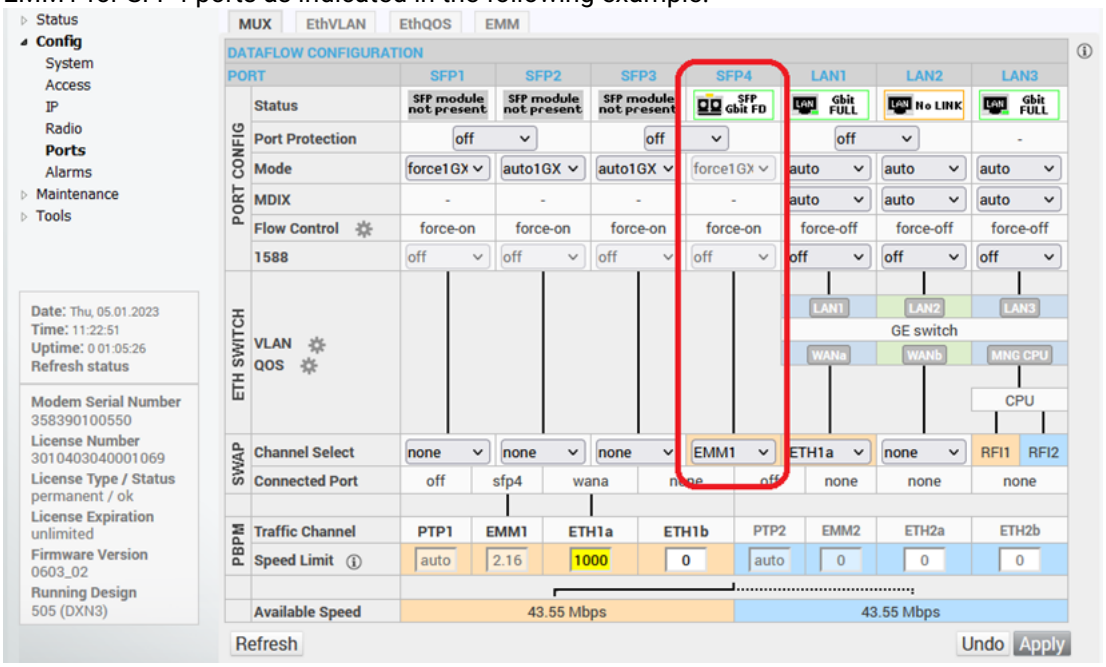


Figure 5.230 *SFP port configuration in repeater IDUs*

7) In boths repeater IDUs web GUI navigate to *Config->Ports->EMM* and check if EMM Status is indicated as “RELAY-SYS” as indicated in the following example:

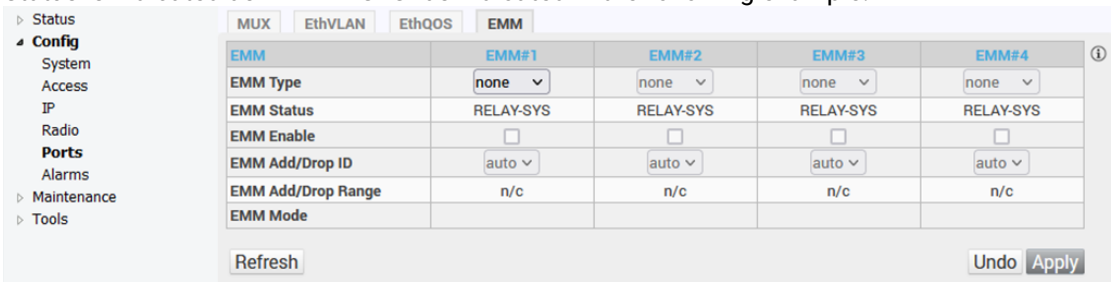


Figure 5.231 *EMM status in repeater IDUs*

8) Save the configuration by pressing Write button in all four IDUs.

Appendix A: TECHNICAL SPECIFICATION

		PhoeniX G2
General		
Concept / form factor		Split Mount
Frequency bands		2/2.3*GHz, 4GHz, U4GHz, L6GHz, U6GHz 7GHz, 8GHz, 11GHz, 13GHz, 18GHz, 23GHz, 38GHz
Capacity		Up to 900 Mbps in 2+0 configuration
		452 Mbps at 60 MHz 1024QAM 1+0
Max modulation		1024QAM
Configurations		1+0, 1+1 HSB/SD/FD, 2+0 (Layer 1 aggregation), 2+0 XPIC, 2+2 (with two IDUs), 1+1 HSB/SD/FD Full redundancy (with two IDUs)
ACM and ATPC		Yes
Channel bandwidth		ETSI: from 7 MHz, up to 56 MHz FCC: from 10 MHz, up to 60 MHz
Ports		
Ethernet traffic	3x RJ-45	10/100/1000Base-T
	4x SFP	1000BaseSX/LX 2x SFP ports also work as Extension/Protection ports
Ethernet Management Access		1x 10/100/1000Base-T, RJ-45
Serial port for configuration		USB B (alternative IP port)
Flash memory port		USB A
ODU port		2x N-Type Female
DC power port		Single block 4 pole
Ethernet		
Switch type		Managed Gigabit Ethernet Layer 2
Max frame size		64 to 2048 bytes, up to 10240 bytes for Jumbo mode
MAC table		8192 entries; automatic learning and aging
Packet buffer		125KB , non-blocking store&forward
Flow Control		802.3x
VLAN support		802.1Q, up to 4096 VLANs
QinQ (Double Tagging)		Yes
QoS		64 level DiffServ (DSCP) or 8 level 802.1p mapped in 4 prioritization queues with VLAN support, IPv6 Traffic Class
Synchronization		PTP 1588v2
Management features		
Protocols		via WEB GUI (HTTP/HTTPS), CLI (Telnet/SSH), NMS (SNMP v2c/v3), Serial interface (USB IP port)
Access		In-band (via VLAN) Out-of-band (115 kbps)

	PhoeniX G2
SNMP	Yes, SNMP traps, MIB, SNMP v2c/3
Element Management System (EMS)	Web based, HTTP/HTTPS
Mechanical & Electrical	
Temperature Range / Humidity	-5 °C to +45 °C / 23 °F to 113 °F / 0% to 95%
Dimensions: HxWxD	½ width 1U (44 x 220 x 240 mm) / (1.73 x 8.66x 9.45 in)
Weight	2.2 kg / 4.9 lb
Max. power consumption	IDU only: <30W IDU + 2xODU: <180W
IDU-ODU connection	Maximum permissible IF cable attenuation = 15dB, N-Type connectors
DC port	-40.5V to -57V DC
IDU compliance	
Operation	ETSI EN 300 019, Part 1-3, Class 3.2
Storage	ETSI EN 300 019, Part 1-1, Class 1.2
Transportation	ETSI EN 300 019, Part 1-2, Class 2.3
Power	EN 300 132-2
Radio frequency IDU+ODU	EN 302 217-2-2
EMC	EN 301 489-1, EN 301 489-3
Safety	IEC 60950-1/EN 60950-1

**2.3GHz radio unit complies with FCC part 27*

Maximum Tx Power [dBm] for PhoeniX G2*:

Modulation	2/2.3 GHz**	4/U4 GHz	L6/U6 GHz	7 GHz	8 GHz	11 GHz	13 GHz	18 GHz	23 GHz	38 GHz
4 QAM	+35	+33	+19/+27/+33	+19/+27/+32	+19/+27/+31	+19/+25/+29	+19/+25/+28	+19/+26	+19	+17
16 QAM	+34	+32	+18/+26/+32	+18/+26/+31	+18/+26/+30	+18/+24/+28	+18/+24/+27	+18/+25	+18	+16
32 QAM	+33	+31	+17/+25/+31	+17/+25/+30	+17/+25/+29	+17/+23/+27	+17/+23/+26	+17/+24	+17	+15
64 QAM	+32	+30	+16/+24/+30	+16/+24/+29	+16/+24/+28	+16/+22/+26	+16/+22/+25	+16/+23	+16	+14
128 QAM	+32	+30	+16/+24/+30	+16/+24/+29	+16/+24/+28	+16/+22/+26	+16/+22/+25	+16/+23	+16	+14
256 QAM	+31	+29	+15/+23/+29	+15/+23/+28	+15/+23/+27	+15/+21/+25	+15/+21/+24	+15/+22	+15	+13
512 QAM	+30	+28	+14/+22/+28	+14/+22/+27	+14/+22/+26	+14/+20/+24	+14/+20/+23	+14/+21	+14	+12
1024 QAM	+27	+25	+11/+19/+25	+11/+19/+24	+11/+19/+23	+11/+17/+21	+11/+17/+20	+11/+18	+11	+9

** Preliminary data*

*** 2.3GHz radio unit complies with FCC part 27*

PhoeniX G2 RSL Thresholds and Capacity for ETSI channels*

Bandwidth, MHz	Modulation	2/2.3 GHz**	U4GHz	L6GHz	U6GHz	7GHz	11GHz	13GHz	18GHz	23GHz	Capacity, Mbps
		Guaranteed RSL Threshold, dBm									
7	4QAM StrongFEC	-91	-92	-92	-89,5	-90,5	-87,5	-88,5	-91	-89	10
	16QAM StrongFEC	-85	-86	-86	-83	-84	-82	-82,5	-85	-82,5	20
	32QAM StrongFEC	-82	-83	-83	-80	-81,5	-79	-79	-81,5	-79	25
	64QAM StrongFEC	-79	-80	-80	-76,5	-78	-76	-76	-78,5	-76	30
	128QAM StrongFEC	-75.5	-76,5	-76,5	-72,5	-74,5	-73,5	-73	-74,5	-72,5	35
14	4QAM StrongFEC	-88	-89	-89	-87	-87,5	-85	-87	-89	-87	21
	16QAM StrongFEC	-81.5	-82,5	-82,5	-81	-81	-80	-80	-82	-80	42
	32QAM StrongFEC	-78.5	-79,5	-79,5	-77,5	-78	-76,5	-77	-79	-77,5	53
	64QAM StrongFEC	-75.5	-76,5	-76,5	-75	-75,5	-74	-74	-76	-74,5	63
	128QAM StrongFEC	-72.5	-73,5	-73,5	-72	-72,5	-71	-71,5	-73	-71,5	74
	256QAM StrongFEC	-69.5	-70,5	-70,5	-68,5	-69,5	-68,5	-68	-70	-68,5	85
20	4QAM StrongFEC	-86.5	-87,5	-87,5	-86	-86	-84	-85,5	-87,5	-85	30
	16QAM StrongFEC	-80.5	-81,5	-81,5	-79	-79,5	-79	-79	-81,5	-78,5	61
	32QAM StrongFEC	-77.5	-78,5	-78,5	-76	-77	-75,5	-76	-78	-75,5	76
	64QAM StrongFEC	-74.5	-75,5	-75,5	-73	-74	-72,5	-73	-75	-72,5	91
	128QAM StrongFEC	-71	-72	-72	-70	-71	-69,5	-69,5	-72	-69,5	107
	256QAM StrongFEC	-68	-69	-69	-67,5	-68,5	-66,5	-66,5	-69	-67	122
	512QAM StrongFEC	-65	-66	-66	-64,5	-65	-63,5	-64	-66	-63,5	137
	1024QAM StrongFEC	-62	-63	-63	-60,5	-61	-61	-60	-62	-59,5	152
28	4QAM StrongFEC	-85	-86	-86	-84	-84,5	-83,5	-84	-86,5	-83,5	43
	16QAM StrongFEC	-78.5	-79,5	-79,5	-77,5	-78	-78	-77,5	-79,5	-77,5	86
	32QAM StrongFEC	-75.5	-76,5	-76,5	-74,5	-75,5	-75	-74,5	-76	-74,5	108
	64QAM StrongFEC	-73	-74	-74	-71,5	-72,5	-72	-71,5	-73	-71,5	129
	128QAM StrongFEC	-69.5	-70,5	-70,5	-68,5	-69,5	-69	-68,5	-70,5	-68,5	151
	256QAM StrongFEC	-67	-68	-68	-66	-66,5	-66	-65,5	-67	-65,5	172
	512QAM StrongFEC	-63.5	-64,5	-64,5	-62,5	-63,5	-62,5	-63	-63,5	-62	194
	1024QAM StrongFEC	-61	-62	-62	-59,5	-60	-59,5	-59	-61	-59	216
40	4QAM StrongFEC	-83.5	-84,5	-84,5	-83	-83	-82	-82	-84	-82	61
	16QAM StrongFEC	-77	-78	-78	-76	-76,5	-76	-75,5	-77	-75,5	122
	32QAM StrongFEC	-74.5	-75,5	-75,5	-73	-73,5	-73	-72,5	-74,5	-72,5	152
	64QAM StrongFEC	-71.5	-72,5	-72,5	-70	-71	-70	-69,5	-71	-69,5	183
	128QAM StrongFEC	-68.5	-69,5	-69,5	-67	-68	-67	-66,5	-68,5	-66,5	214
	256QAM StrongFEC	-65.5	-66,5	-66,5	-64	-65	-64,5	-63,5	-65	-63,5	244
	512QAM StrongFEC	-62.5	-63,5	-63,5	-61,5	-62	-60,5	-60,5	-62	-60,5	275
	1024QAM StrongFEC	-59.5	-60,5	-60,5	-58,5	-58	-58	-57,5	-58,5	-57	305
56	4QAM StrongFEC	-82	-83	-83	-80,5	-81,5	-81	-81	-82	-80,5	87
	16QAM StrongFEC	-75.5	-76,5	-76,5	-74	-75	-74,5	-74,5	-75,5	-74	174
	32QAM StrongFEC	-73	-74	-74	-71,5	-72	-71,5	-71,5	-72,5	-71	217
	64QAM StrongFEC	-70	-71	-71	-68,5	-69	-68,5	-68	-69,5	-68,5	261
	128QAM StrongFEC	-67	-68	-68	-65,5	-66,5	-65,5	-65,5	-67	-65	304
	256QAM StrongFEC	-64	-65	-65	-62	-63,5	-63	-62	-63,5	-61,5	348
	512QAM StrongFEC	-60.5	-61,5	-61,5	-59,5	-60,5	-59,5	-59	-60,5	-58,5	392
	1024QAM StrongFEC	-57.5	-58,5	-58,5	-56	-56,5	-56,5	-56	-56,5	-55,5	435

** Preliminary data*

*** 2.3GHz radio unit complies with FCC part 27*

PhoeniX G2 RSL Thresholds and Capacity for FCC channels*

Bandwidth, MHz	Modulation	2GHz**	U4GHz	L6GHz	U6GHz	7GHz	11GHz	13GHz	18GHz	23GHz	Capacity, Mbps
		Guaranteed RSL Threshold, dBm									
10	4QAM StrongFEC	-89.5	-90.5	-88.5	-88.5	-87	-88	-90	-88	-89	15
	16QAM StrongFEC	-83.5	-84.5	-82	-82.5	-81	-81.5	-83.5	-82.5	-82.5	30
	32QAM StrongFEC	-80	-81	-79	-79.5	-78.5	-78.5	-80	-79	-79.5	38
	64QAM StrongFEC	-77.5	-78.5	-76	-76.5	-75.5	-75.5	-77	-76	-76.5	45

Bandwidth, MHz	Modulation	2GHz**	U4GHz	L6GHz	U6GHz	7GHz	11GHz	13GHz	18GHz	23GHz	Capacity, Mbps
		Guaranteed RSL Threshold, dBm									
	128QAM StrongFEC	-74.5	-75.5	-73.5	-73.5	-73	-72.5	-73.5	-72.5	-74	53
20	4QAM StrongFEC	-86.5	-87.5	-86	-86	-84	-85.5	-87.5	-85	-86	30
	16QAM StrongFEC	-80.5	-81.5	-79	-79.5	-79	-79	-81.5	-78.5	-79.5	61
	32QAM StrongFEC	-77.5	-78.5	-76	-77	-75.5	-76	-78	-75.5	-76.5	76
	64QAM StrongFEC	-74.5	-75.5	-73	-74	-72.5	-73	-75	-72.5	-73	91
	128QAM StrongFEC	-71	-72	-70	-71	-69.5	-69.5	-72	-69.5	-69.5	107
	256QAM StrongFEC	-68	-69	-67.5	-68.5	-66.5	-66.5	-69	-67	-67	122
	512QAM StrongFEC	-65	-66	-64.5	-65	-63.5	-64	-66	-63.5	-63.5	137
	1024QAM StrongFEC	-62	-63	-60.5	-61	-61	-60	-62	-59.5	-59.5	152
25	4QAM StrongFEC	-85.5	-86.5	-84.5	-85	-83.5	-85	-87.5	-84	-84.5	37
	16QAM StrongFEC	-79.5	-80.5	-78	-79	-78	-78	-81	-78	-78	74
	32QAM StrongFEC	-76.5	-77.5	-75	-75.5	-75	-75.5	-78	-75	-75	93
	64QAM StrongFEC	-73.5	-74.5	-72	-73	-72	-72	-75	-71.5	-72	111
	128QAM StrongFEC	-70.5	-71.5	-69	-70	-69.5	-69	-72	-69	-69.5	130
	256QAM StrongFEC	-67.5	-68.5	-66.5	-67	-66.5	-66	-68.5	-66	-66.5	148
	512QAM StrongFEC	-64.5	-65.5	-63.5	-64	-63	-63	-65.5	-63	-63.5	167
	1024QAM StrongFEC	-61.5	-62.5	-60	-61	-60	-59.5	-62	-59.5	-59.5	186
30	4QAM StrongFEC	-84.5	-85.5	-83.5	-84	-82.5	-83	-85	-83.5	-84.5	45
	16QAM StrongFEC	-78.5	-79.5	-77	-78	-77.5	-76.5	-78	-77	-77.5	91
	32QAM StrongFEC	-75.5	-76.5	-74	-75	-74	-74	-75	-74.5	-74.5	114
	64QAM StrongFEC	-72.5	-73.5	-71	-72	-71.5	-70.5	-73	-70.5	-71.5	137
	128QAM StrongFEC	-69.5	-70.5	-68.5	-69.5	-68.5	-68	-70	-68	-69	160
	256QAM StrongFEC	-66.5	-67.5	-65.5	-66	-66	-64.5	-66.5	-64.5	-66	183
	512QAM StrongFEC	-63.5	-64.5	-62.5	-63	-61.5	-61.5	-63.5	-61.5	-62.5	206
	1024QAM StrongFEC	-60.5	-61.5	-59	-59.5	-59.5	-58.5	-60	-59	-58.5	229
40	4QAM StrongFEC	-83.5	-84.5	-83	-83	-82	-82	-84	-82	-83	61
	16QAM StrongFEC	-77	-78	-76	-76.5	-76	-75.5	-77	-75.5	-76.5	122
	32QAM StrongFEC	-74.5	-75.5	-73	-73.5	-73	-72.5	-74.5	-72.5	-73	152
	64QAM StrongFEC	-71.5	-72.5	-70	-71	-70	-69.5	-71	-69.5	-70.5	183
	128QAM StrongFEC	-68.5	-69.5	-67	-68	-67	-66.5	-68.5	-66.5	-68	214
	256QAM StrongFEC	-65.5	-66.5	-64	-65	-64.5	-63.5	-65	-63.5	-64.5	244
	512QAM StrongFEC	-62.5	-63.5	-61.5	-62	-60.5	-60.5	-62	-60.5	-61	275
	1024QAM StrongFEC	-59.5	-60.5	-58.5	-58	-58	-57.5	-58.5	-57	-57.5	305
50	4QAM StrongFEC	-82.5	-83.5	-81.5	-82	-81.5	-81	-83	-81	-82	75
	16QAM StrongFEC	-76.5	-77.5	-75	-75.5	-75	-74.5	-76.5	-74.5	-75	151
	32QAM StrongFEC	-73.5	-74.5	-72	-73	-72	-71.5	-73.5	-71.5	-72.5	189
	64QAM StrongFEC	-70.5	-71.5	-69	-70	-69	-68.5	-71	-68.5	-69	227
	128QAM StrongFEC	-67.5	-68.5	-66	-67	-66	-65.5	-68	-65.5	-67	265
	256QAM StrongFEC	-64.5	-65.5	-63	-64	-63.5	-62.5	-64.5	-62.5	-63.5	303
	512QAM StrongFEC	-61.5	-62.5	-60.5	-61	-60	-60	-61.5	-59.5	-60.5	341
	1024QAM StrongFEC	-58.5	-59.5	-57	-57	-56.5	-56.5	-58	-56.5	-57.5	379
60	4QAM StrongFEC	-81.5	-82.5	-81	-81	-80.5	-81	-80.5	-80.5	-81	90
	16QAM StrongFEC	-75.5	-76.5	-74	-74	-74	-74.5	-74	-73.5	-74.5	180
	32QAM StrongFEC	-72.5	-73.5	-71	-71.5	-71	-71.5	-70.5	-70.5	-72	226
	64QAM StrongFEC	-69.5	-70.5	-68.5	-68.5	-68	-67.5	-68.5	-68	-69	271
	128QAM StrongFEC	-66.5	-67.5	-65.5	-63.5	-65	-64.5	-65.5	-65	-66	316
	256QAM StrongFEC	-64	-65	-62.5	-62.5	-62.5	-62	-62.5	-61.5	-63	361
	512QAM StrongFEC	-60.5	-61.5	-59.5	-59.5	-59	-59	-59.5	-58.5	-59.5	407
	1024QAM StrongFEC	-57.5	-58.5	-56.5	-56.5	-56	-55.5	-56	-55.5	-56	452

** Preliminary data*

*** 2.3GHz radio unit complies with FCC part 27*

Appendix B: ASI EMM TECHNICAL SPECIFICATION

CFIP-ASI-EXT	
EAGMEXA4	External ASI module for PhoeniX G2 IDU, 4x BNC, 2x SFP ports
ASI	Unbalanced, 75 ohm
Scalability	Cascading up to four external modules
Ports	
IDU connection	1x SFP port 1000Base-SX (proprietary GigE protocol)
Connection to next External module	1x SFP port 1000Base-SX (proprietary GigE protocol)
ASI ports	4x BNC
DC port	Industrial power connector
Mechanical & Electrical	
Dimensions: HxWxD	½ width 1U (45 x 210 x 240 mm) / (1.77 x 8.27 x 9.45 in)
Weight	1.3 kg / 2.87 lb
Max. power consumption	IDU: <9 W
DC port	-20V to -60V DC

Appendix C: E1/T1 EMM TECHNICAL SPECIFICATION

CFIP-16E1/T1-EXT	
EAGMEX16	16E1/T1 external module for PhoeniX G2 IDU, 16xRJ-45, 2xSFP ports
16xE1/T1	G.703-E1 balanced 120ohm for E1 mode G.703-E1 unbalanced 75 ohm for E1 mode T1.102-T1/100 ohm for T1 mode
Scalability	Cascading up to four external modules
Ports	
IDU connection	1x SFP port 1000Base-SX (proprietary GigE protocol)
Connection to next External module	1x SFP port 1000Base-SX (proprietary GigE protocol)
E1 ports	16x RJ-45
DC port	Industrial power connector
Mechanical & Electrical	
Dimensions: HxWxD	½ width 1U (45 x 210 x 240 mm) / (1.77 x 8.27 x 9.45 in)
Weight	1.3 kg / 2.87 lb
Max. power consumption	IDU: <9 W
DC port	-20V to -60V DC

Appendix D: IRFU TECHNICAL SPECIFICATION

Ports	
Antenna	A) N-Type or flange B) SMA Tx and Rx ports
IF to IDU	SMA
RSSI	2-port for multi-meter
Power	2-pin power port (alternative to IF port)
Mechanical & Electrical	
Operational use	Conforms to ETSI EN 300 019 Class 3.1E, IP20, NEMA 1
Temperature Range	-33°C to +55°C
Dimensions: HxWxD / weight	19” 2U rack 90x430x260 / 5.8 kg
IF port surge protection	Conforms to ETSI EN 301 489-1; EN 61000-4-5; IEC 61000-4-5
Input DC voltage	-40.5V to -57V DC (conforms to ETSI EN 300 132-2)
Max. power consumption	SP: 13-27 W; HP: 21-39 W; VHP: 39-55W

ABBREVIATIONS

ACM – Adaptive Coding and Modulation
AES – Advanced Encryption Standard
ANSI – American National Standards Institute
ASI – Asynchronous Serial Interface
ATPC – Automatic Transmit Power Control
AWG – American Wire Gauge
BER – Bit-Error Ratio
BNC – Bayonet Neill-Concelman connector
CDE – Cable Discharge Events
CLI – Command-Line Interface
CPE – Customer-premises equipment
CRC – Cyclic Redundancy Check
CW – Continuous Wave
DC – Direct Current
DSCP - Differentiated Services Code Point
DVB – Digital Video Broadcasting
EMM – External Multiplexer Module
ESD – Electrostatic Discharge
ETH - Ethernet
ETSI – European Telecommunications Standards Institute
FCC - The Federal Communications Commission
FD – Frequency Diversity
FEC – Forward Error Correction
FER – Frame Errors
FO – Fiber Optics
GND – Grounding
GUI – Graphical User Interface
HP – High Power
HSB – Hot Standby
HTTPS – Hypertext Transfer Protocol Secure
HW – Hardware
IDU – Indoor Unit
IF – Intermediate Frequency
IRFU – Indoor Radio Frequency Unit
ITU-T – International Telecommunication Union – Telecommunication Standardization Sector
JSC – Joint Stock Company
LAN – Local Area Network
LED – Light-Emitting Diode
MAC – Media Access Control
MDI/MDX – Medium Dependent Interface / Medium Dependent Interface Crossover
MIB – Management Information Base
M/N – Model Number
MNG – Management
MPEG – Moving Picture Experts Group

MSE – Mean Square Error
MUX – Multiplexer
NAT – Network Address Translation
NTP – Network Time Protocol
ODU – Outdoor Unit
OQPRI – Queue Priority override
PBPM – Priority Based Packet Multiplexer
PC – Personal Computer
P/N – Part Number
PRI – Priority
Pri/Sec – Primary/Secondary
PTP – Precision Time Protocol
RF – Radio Frequency
RSL – Received Signal Level
RSS – Radio Standards Specification
RSSI – Received Signal Strength Indicator
Rx – Receive
SD – Space Diversity
SFP – Small Form-factor Pluggable
SMA – SubMiniature version A connector
SNMP - Simple Network Management Protocol
S/N – Serial Number
SP – Standard Power
SSH – Secure Shell
SW – Software
SyncE – Synchronous Ethernet
QAM - Quadrature amplitude modulation
QoS – Quality of Service
QPRI – Queue Priority
QPSK – Quadrature Phase-shift Keying
TCP/IP – Internet Protocol Suite (Transmission Control Protocol / Internet Protocol)
TDM – Time-Division Multiplexing
Tx – Transmit
TV – Television
USB – Universal Serial Bus
VHP – Very High Power
VLAN – Virtual Local Area Network
VTU – VLAN rules table: VLAN Tagged/Untagged
XPIC – Cross-polar Interference Cancellation



SAF Tehnika JSC
24a, Ganibu dambis, Riga, LV-1005, Latvia, EU
sales@saftehnika.com
www.saftehnika.com