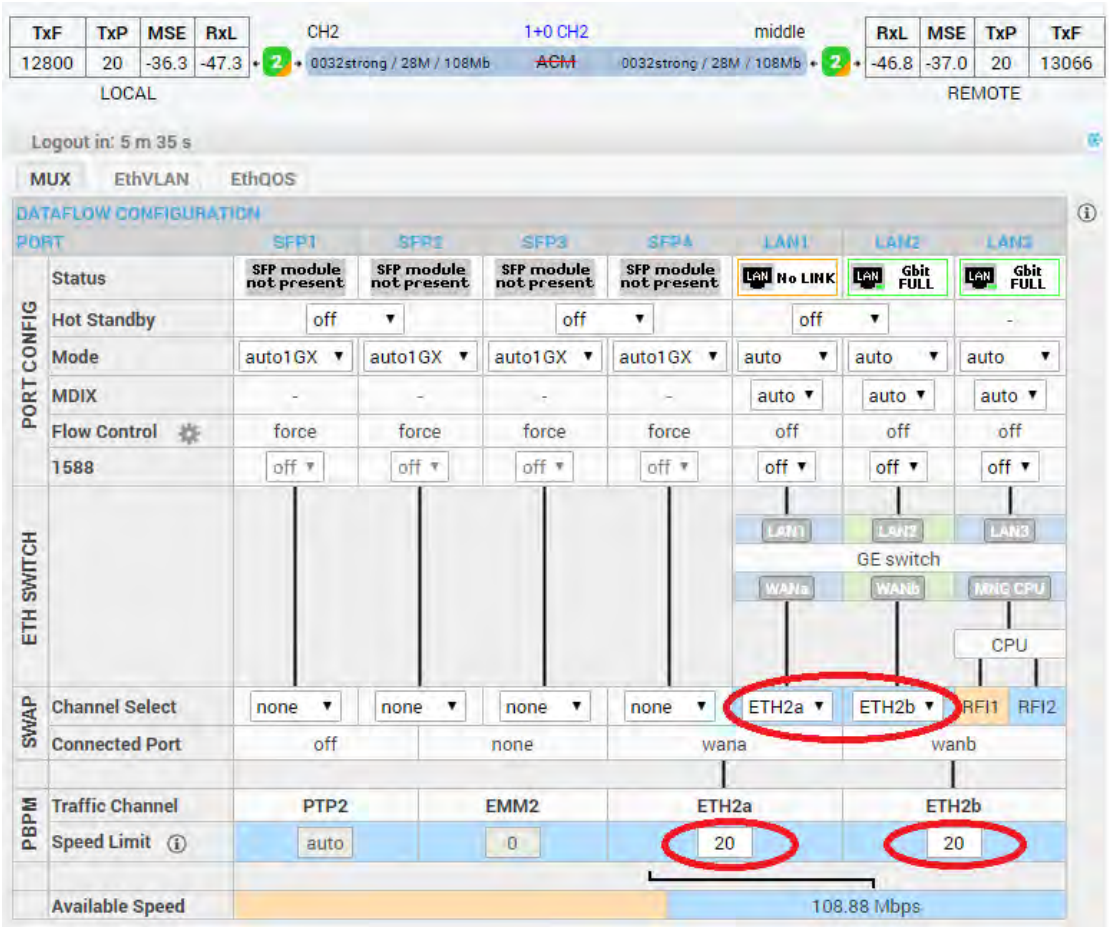


Figure 5.56 *Example of port configuration in Endpoint IDU 2*

13) Save new settings by pressing Write button.

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

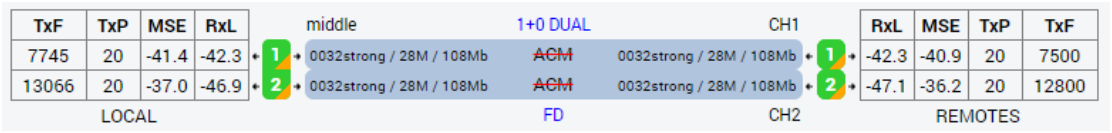


Figure 5.57 *Status of 1+0 Dual FD mode in Repeater IDU*

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:

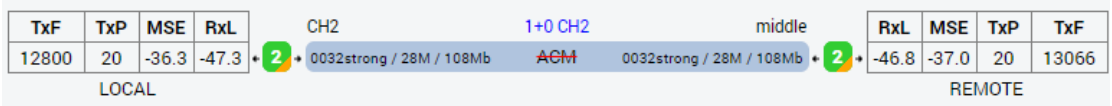


Figure 5.59 *Status of 1+0 Ch2 mode in Endpoint IDU 2*

Example 9 – 1+1 HSB/SD Dual-band frequency protection scheme

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.

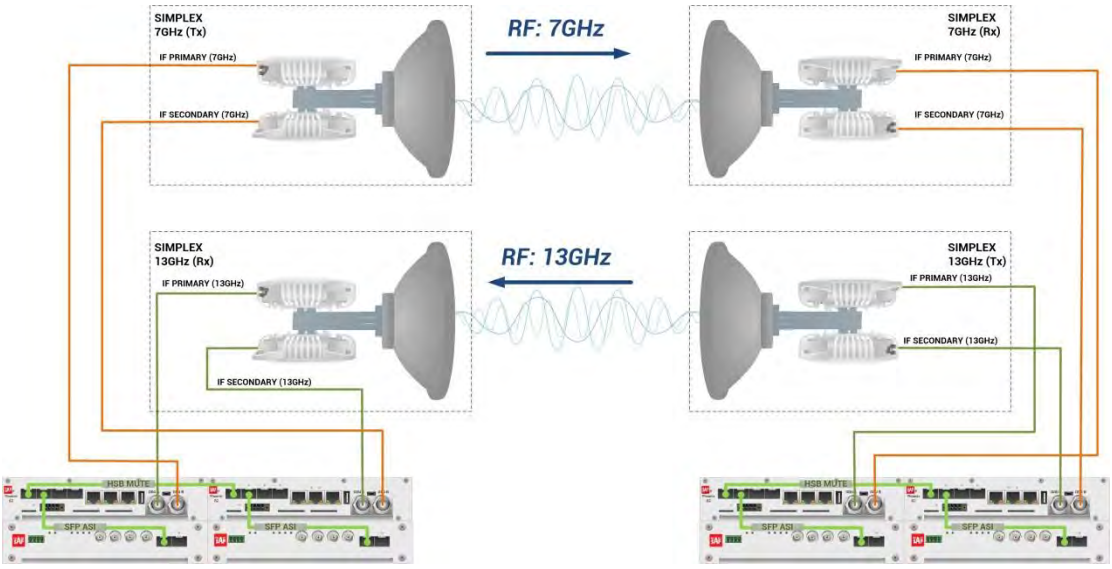


Figure 5.60 *Example of 1+1 HSB/SD Dual-band frequency protection*

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

This concrete 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.

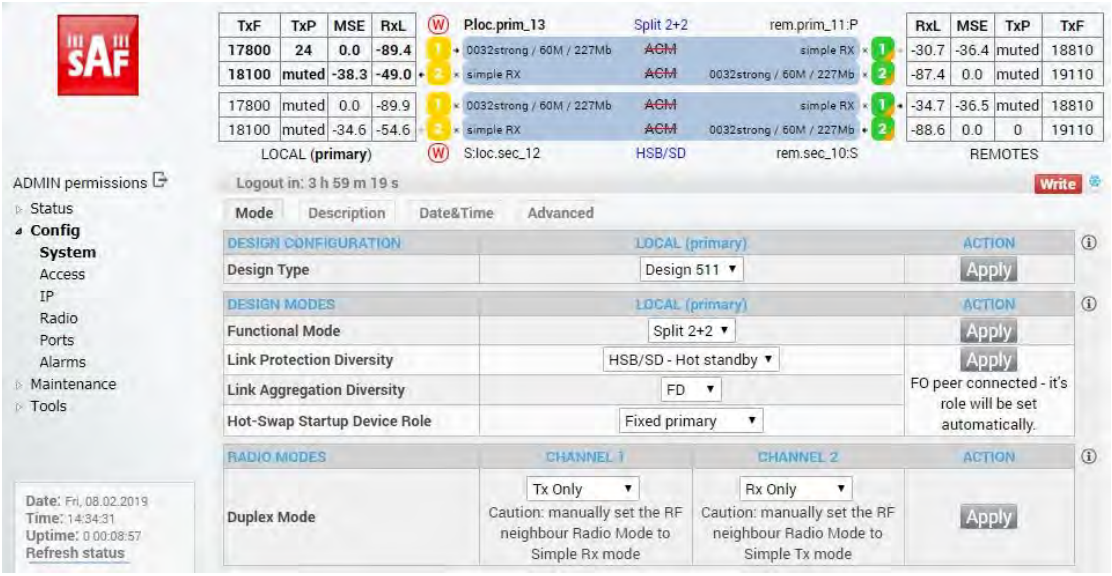


Figure 5.61 *Example of Side A Primary IDU system configuration*

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.

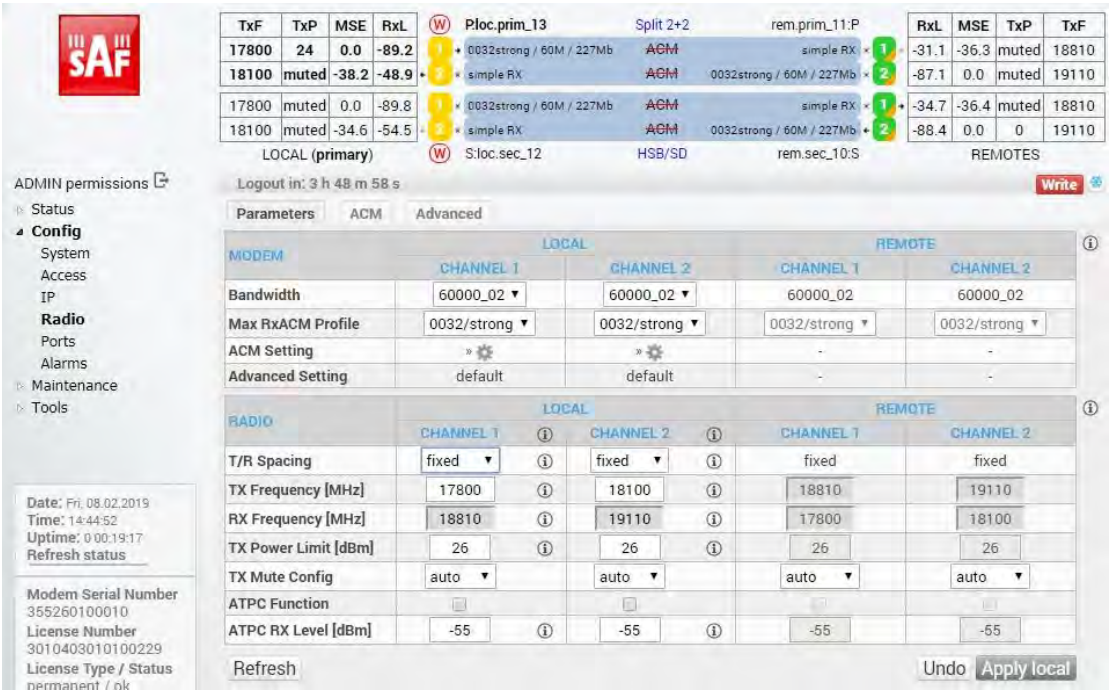


Figure 5.62 *Example of Side A Primary IDU radio configuration*

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->Radio->ACM' in the web GUI and set ACM function to "man p1" on both Channels. 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

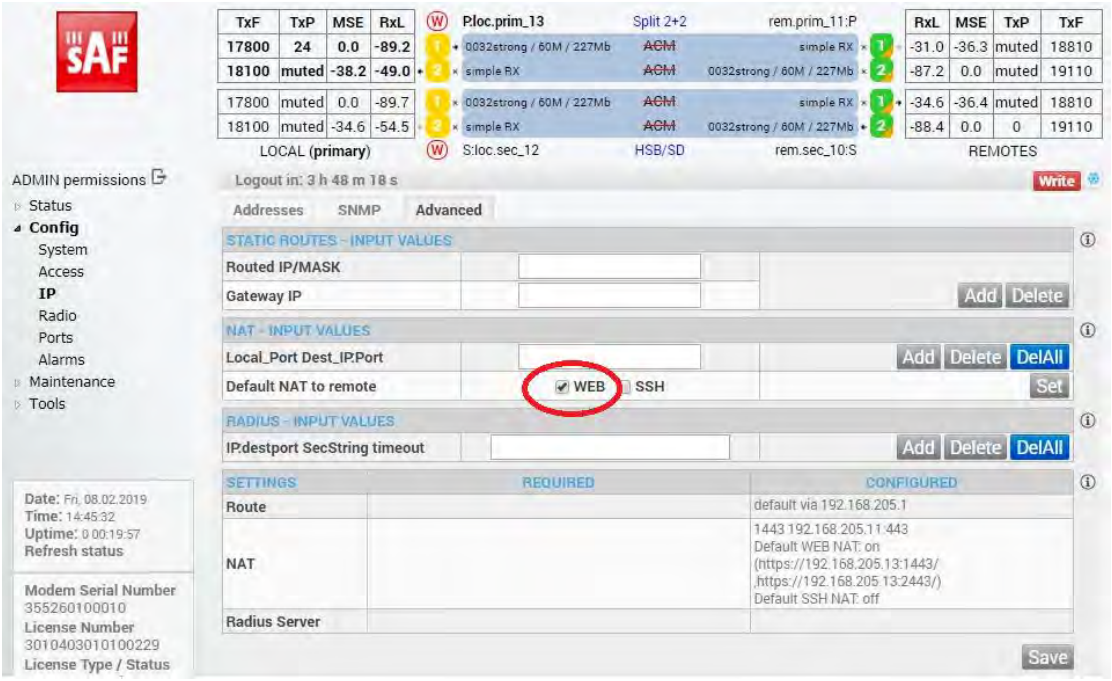


Figure 5.65 *Example of Side A Primary IDU IP NAT configuration*

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

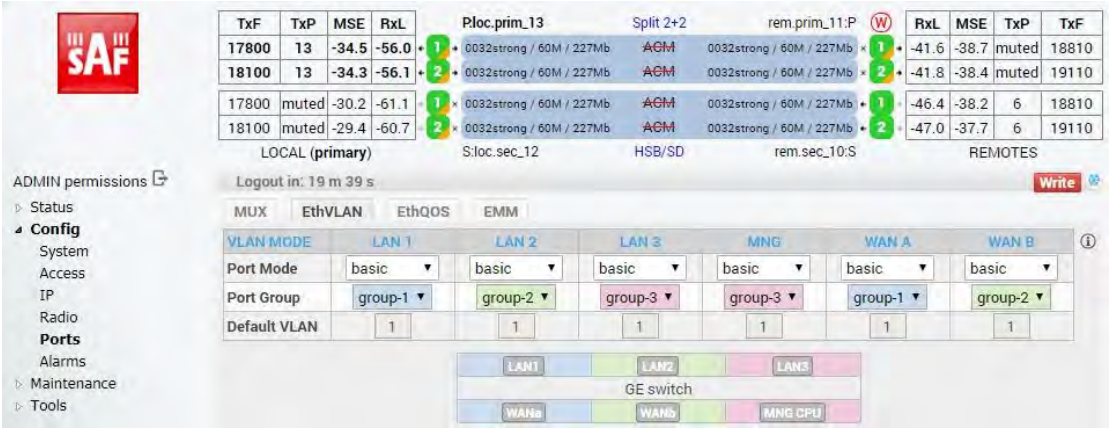


Figure 5.66 *Example of Side A Primary IDU port grouping*

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'

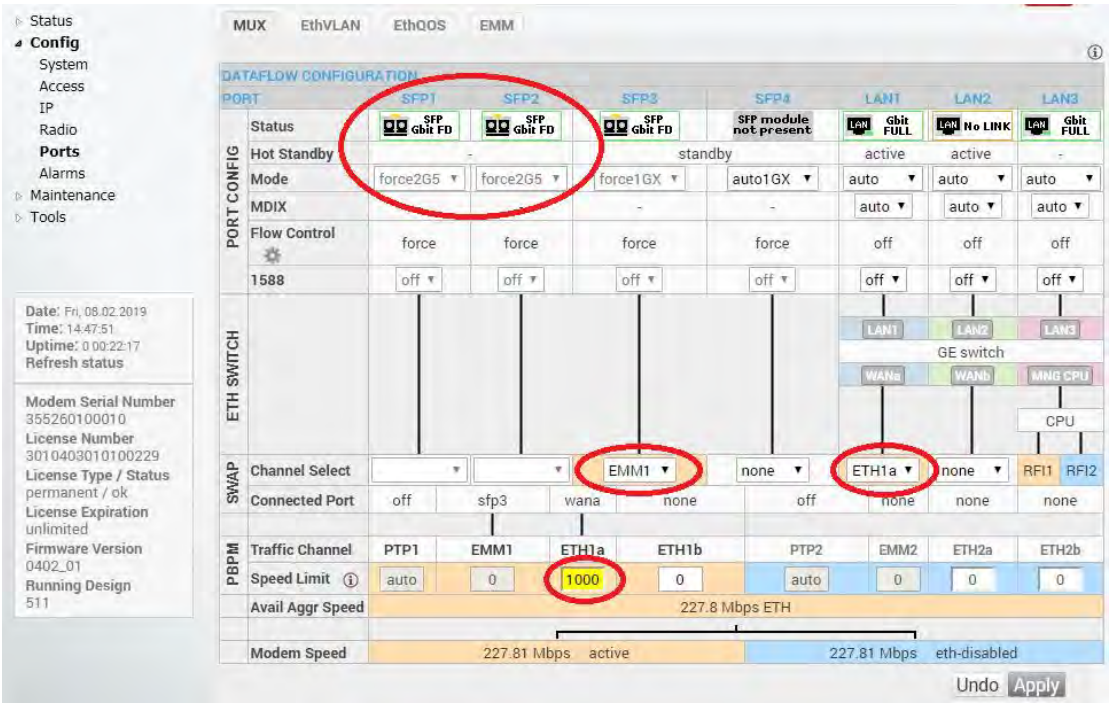


Figure 5.67 *Example of Side A Primary IDU port configuration*

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"

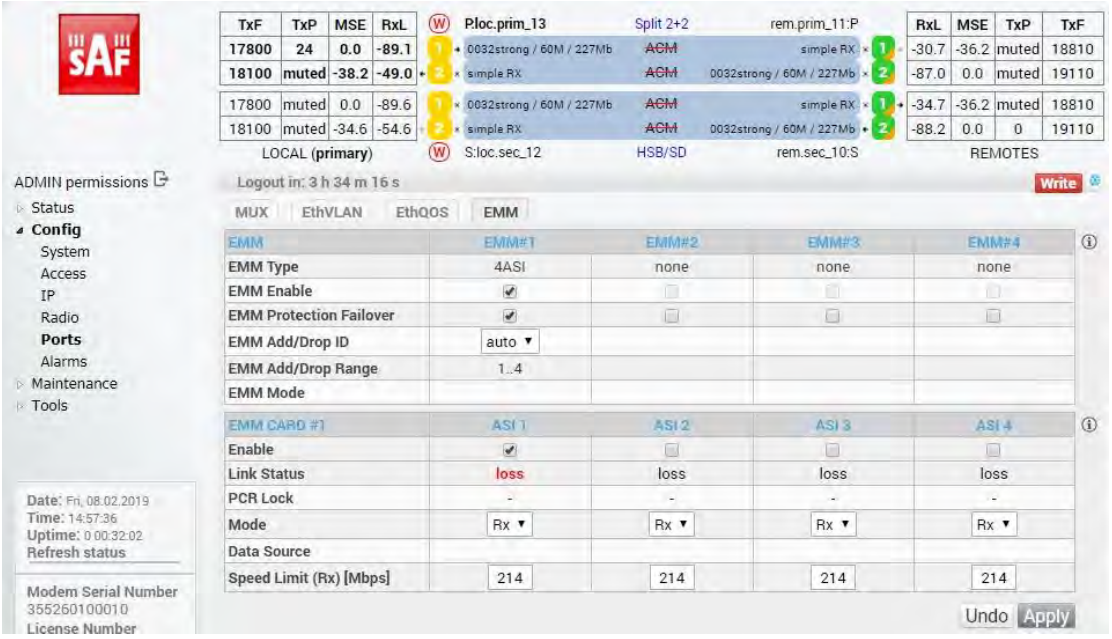


Figure 5.68 *Example of Side A Primary IDU EMM configuration*

i) In web GUI 'Config->Alarms->Minor' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover. In the example LAN1, SFP1, SFP2, SFP3 and ASI Port 1 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

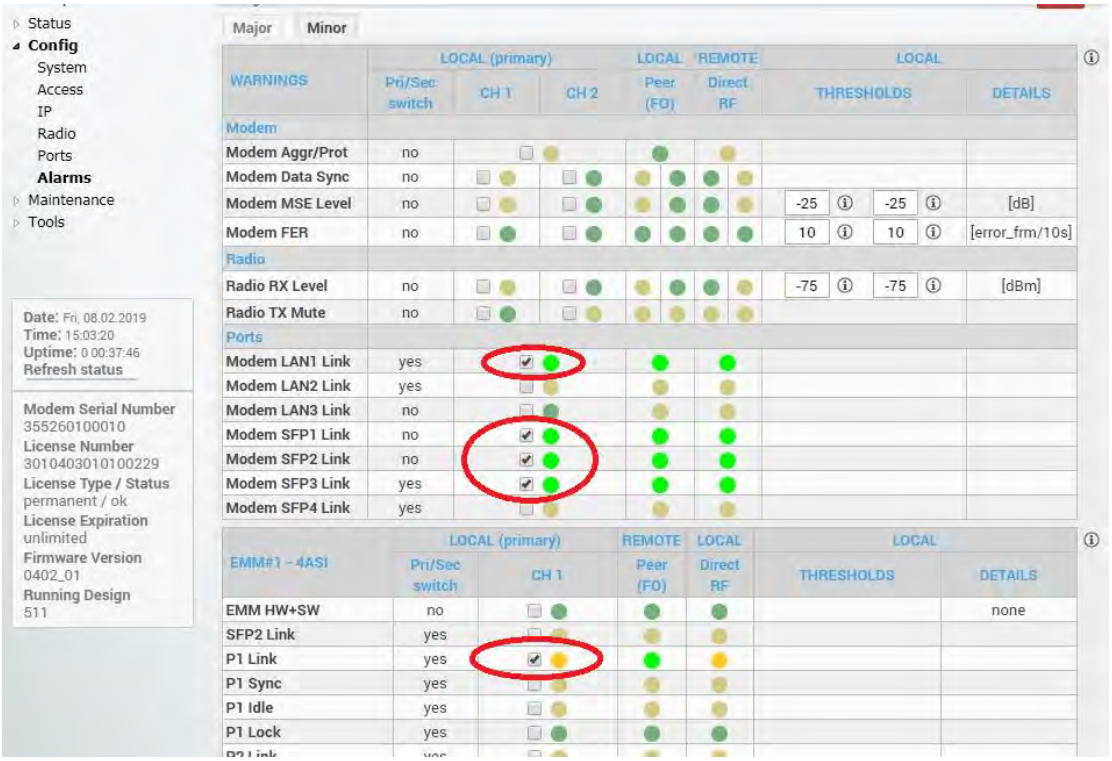


Figure 5.69 *Example of Side A Primary IDU alarm configuration*

j) Save new settings by pressing 

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

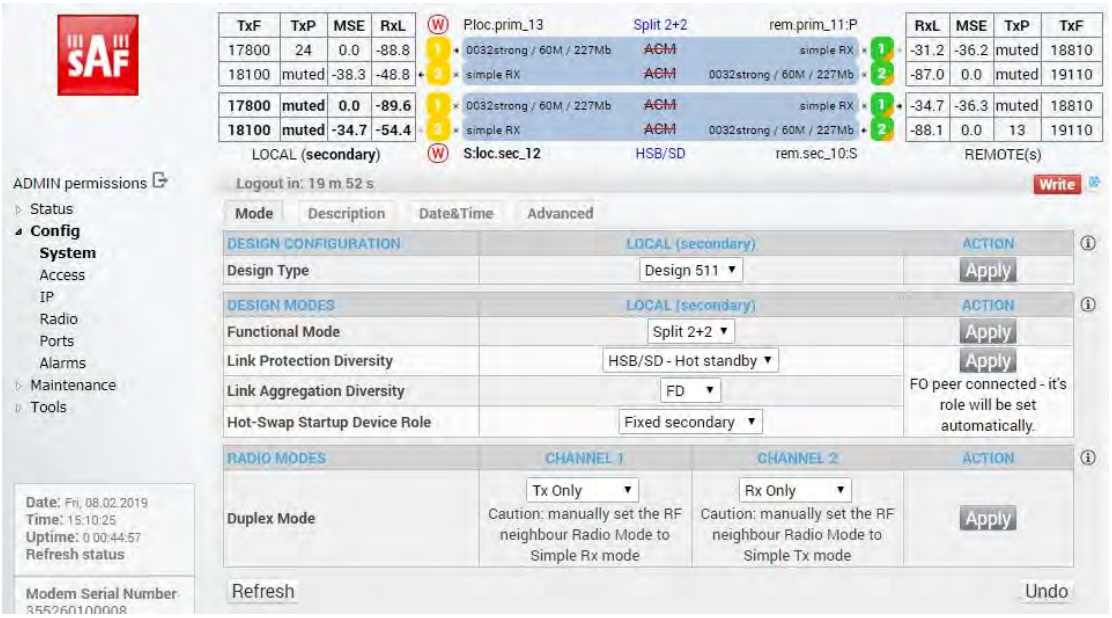


Figure 5.70 *Example of Side A Secondary IDU system configuration*

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.

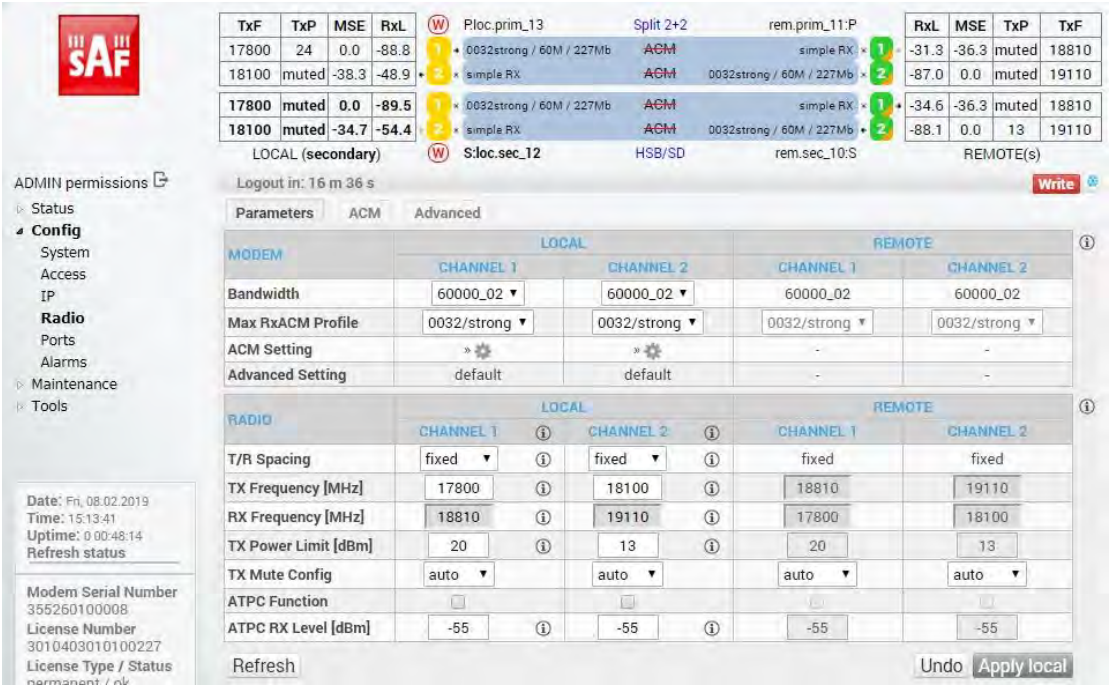


Figure 5.71 *Example of Side A Secondary IDU radio configuration*

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->Radio->ACM' in the web GUI and set ACM function to "man p1" on both Channels. 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

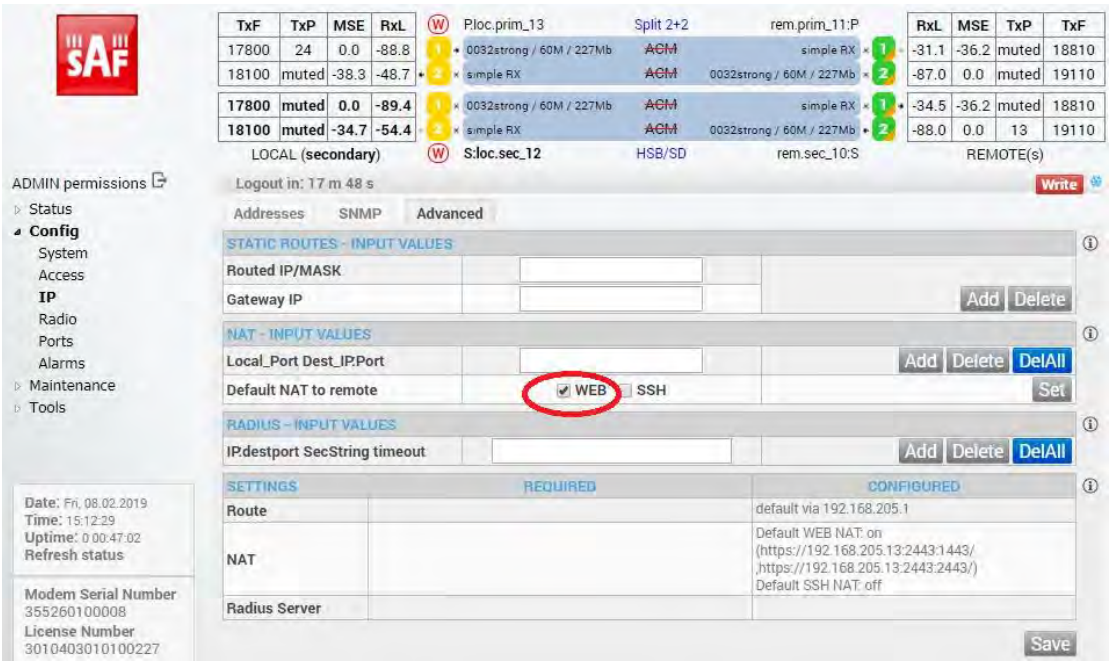


Figure 5.74 *Example of Side A Secondary IDU IP NAT configuration*

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

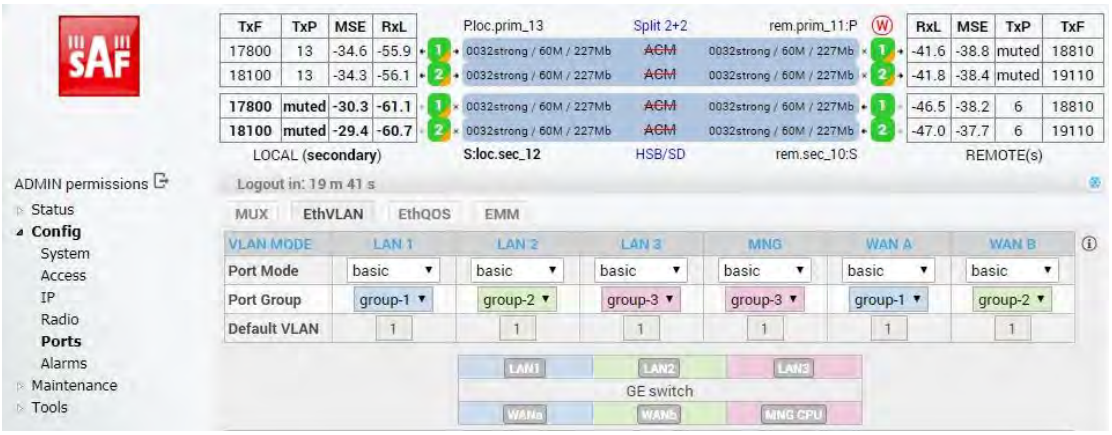


Figure 5.75 *Example of Side A Secondary IDU port grouping*

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'

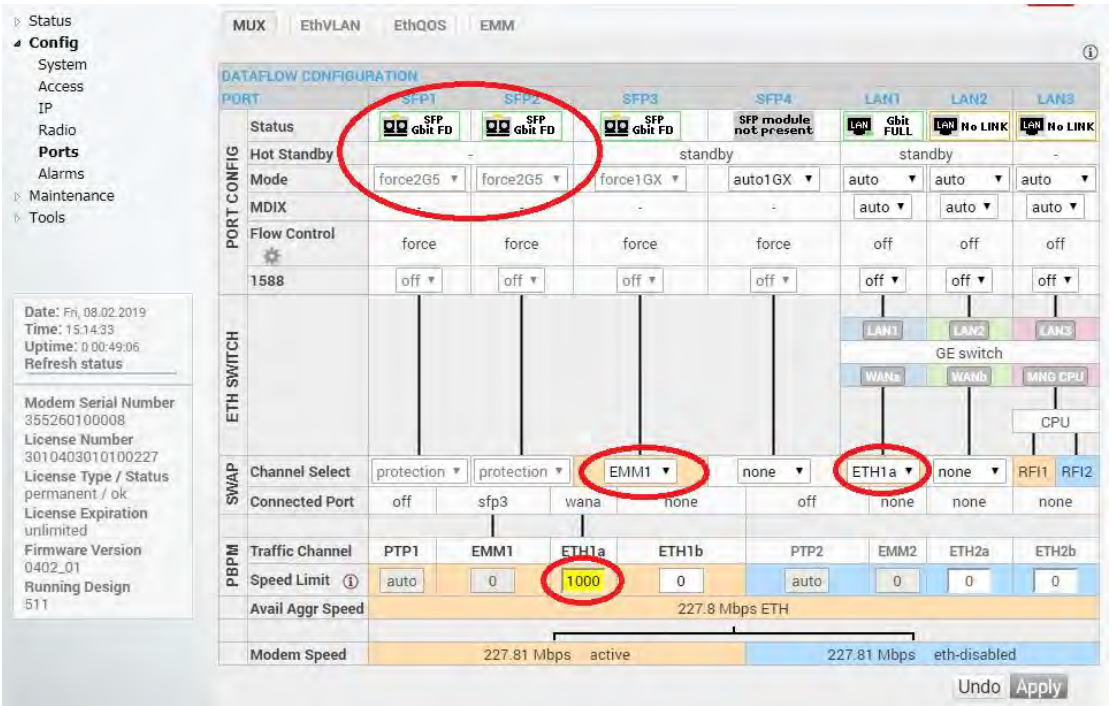


Figure 5.76 *Example of Side A Secondary IDU port configuration*

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"

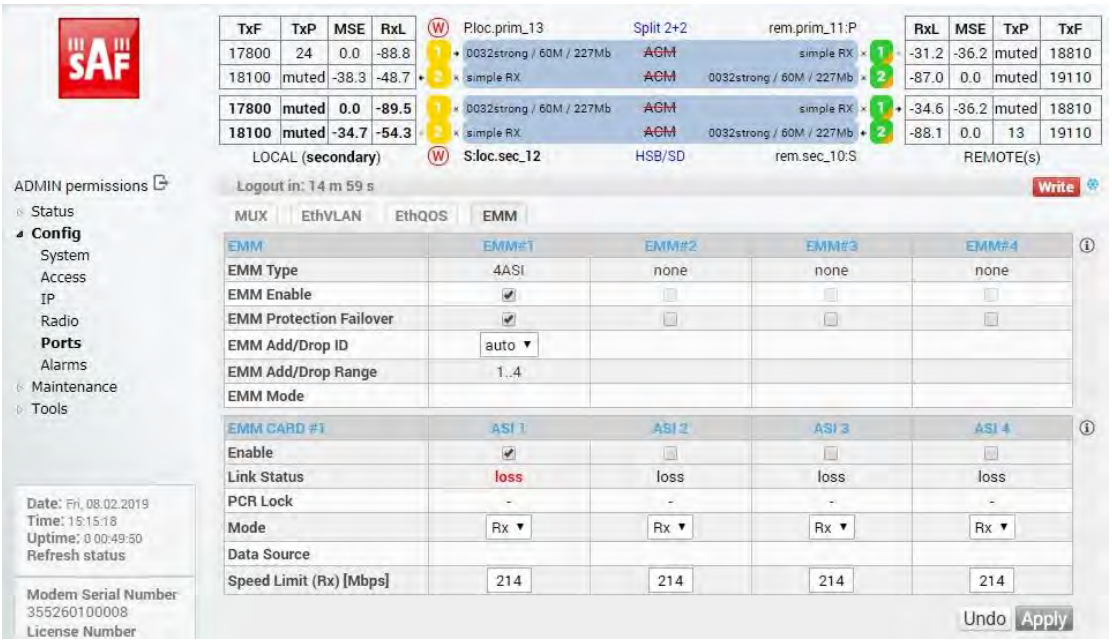


Figure 5.77 *Example of Side A Secondary IDU EMM configuration*

i) In web GUI '[Config->Alarms->Minor](#)' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover. In the example LAN1, SFP1, SFP2, SFP3 and ASI Port 1 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

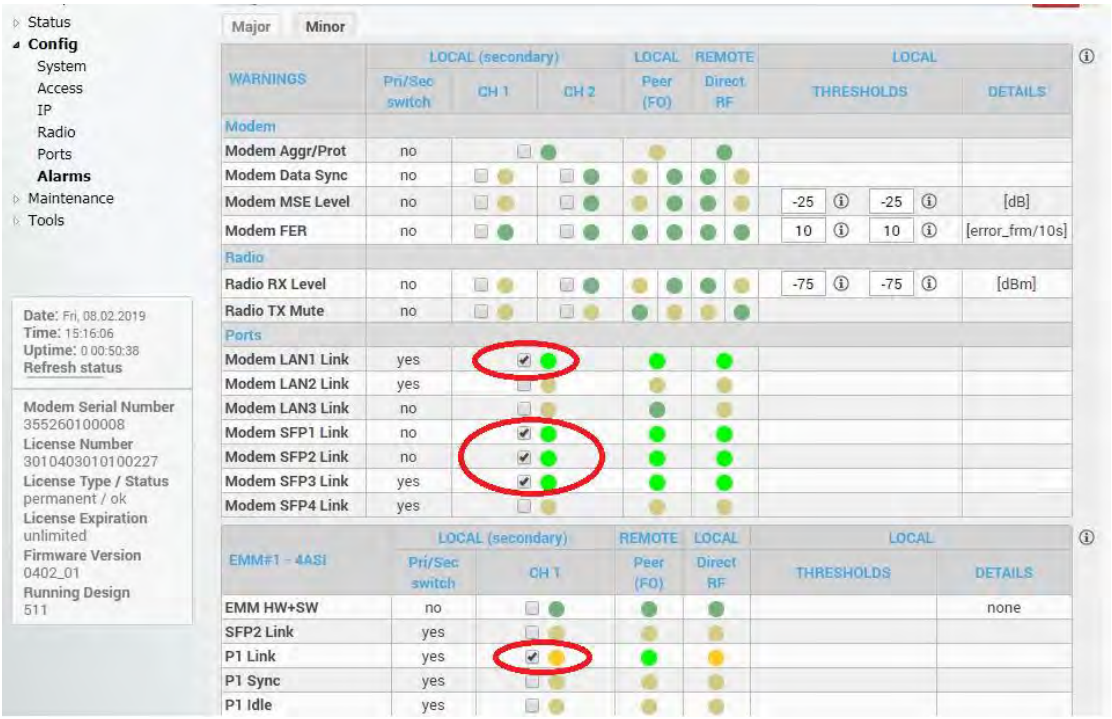


Figure 5.78 *Example of Side A Secondary IDU alarm configuration*

j) Save new settings by pressing 

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.

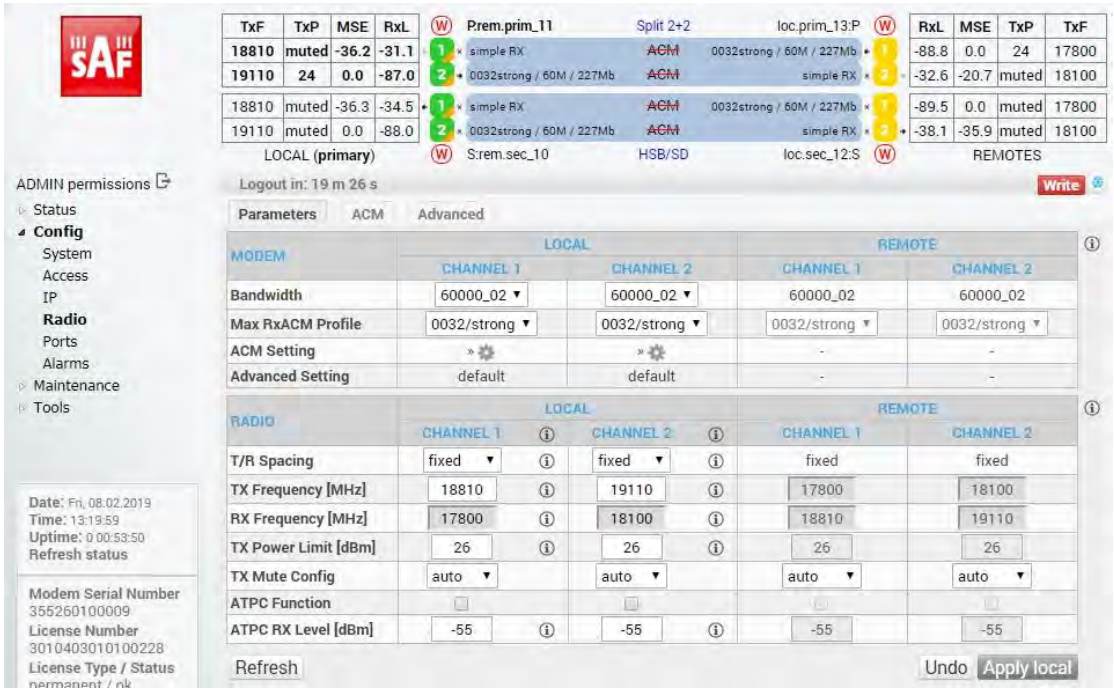


Figure 5.80 *Example of Side B Primary IDU radio configuration*

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->Radio->ACM' in the web GUI and set ACM function to "man p1" on both Channels. 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

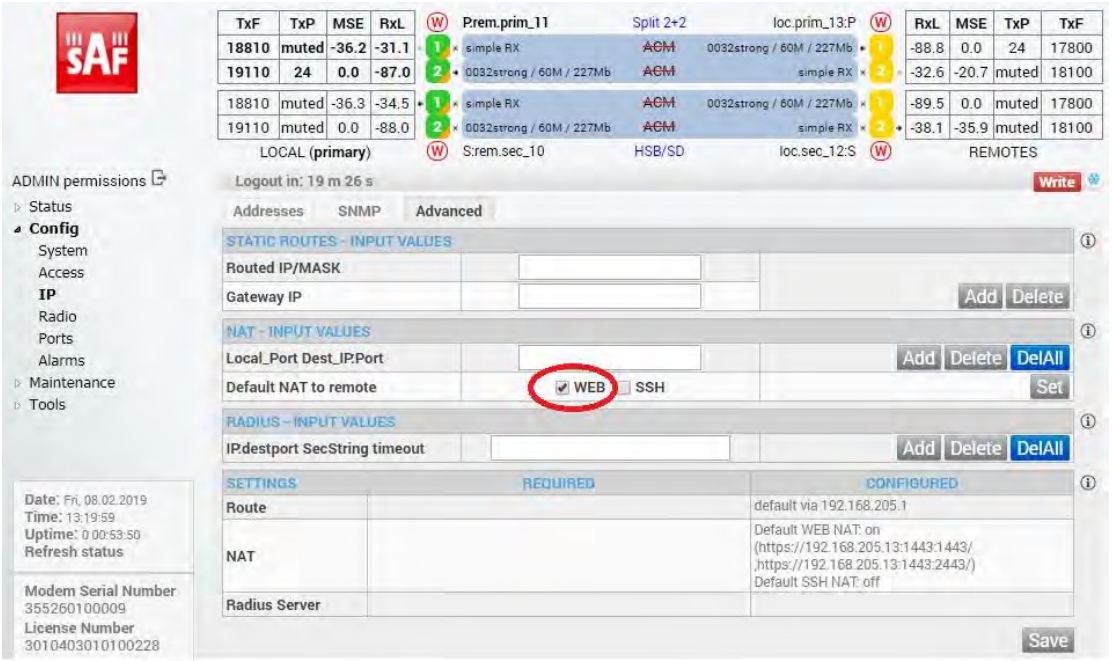


Figure 5.83 *Example of Side B Primary IDU IP NAT configuration*

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'

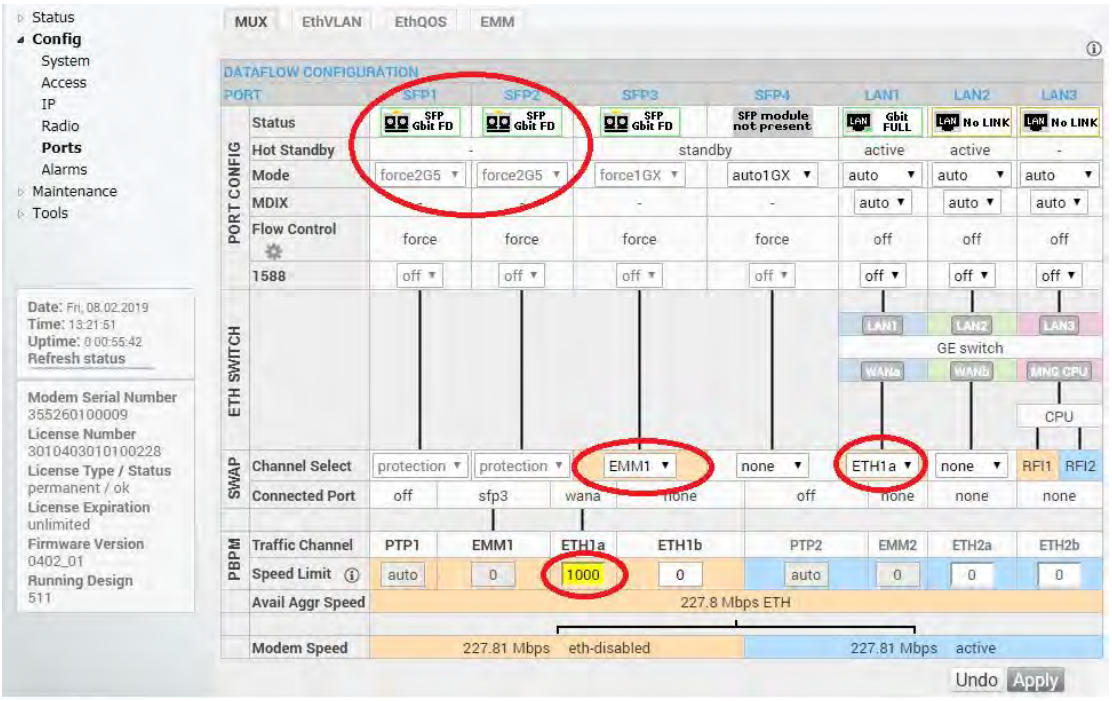


Figure 5.85 *Example of Side B Primary IDU port configuration*

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'

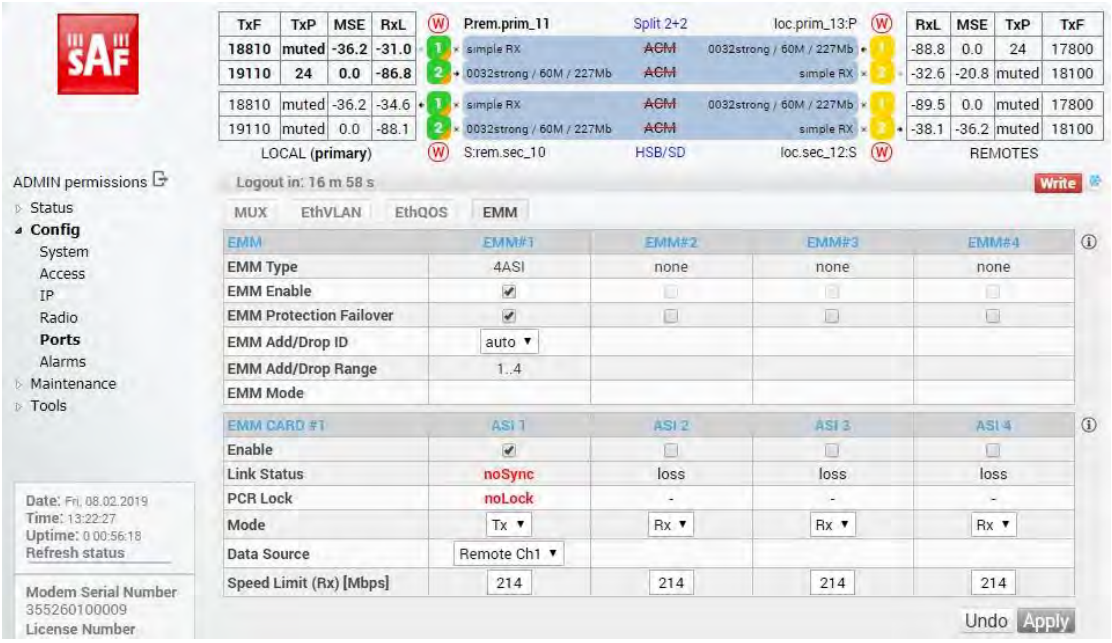


Figure 5.86 *Example of Side B Primary IDU EMM configuration*

i) In web GUI 'Config->Alarms->Minor' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover. In the example LAN1, SFP1, SFP2, SFP3 and ASI Port 1 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

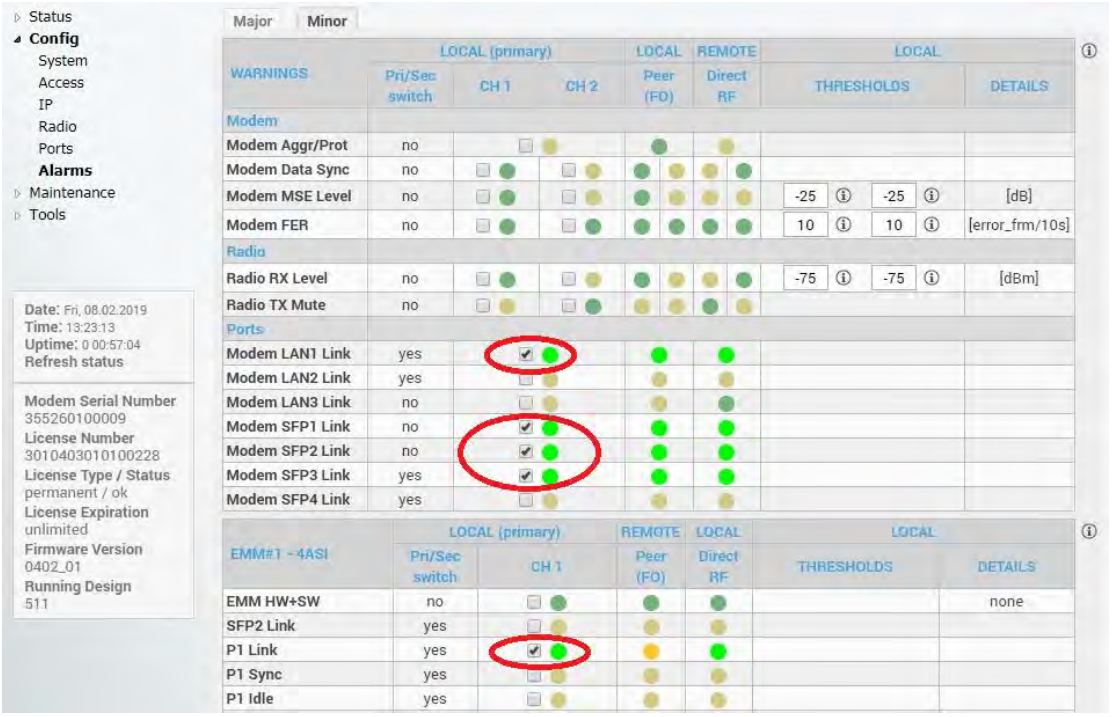


Figure 5.87 *Example of Side B Primary IDU alarm configuration*

j) Save new settings by pressing 

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

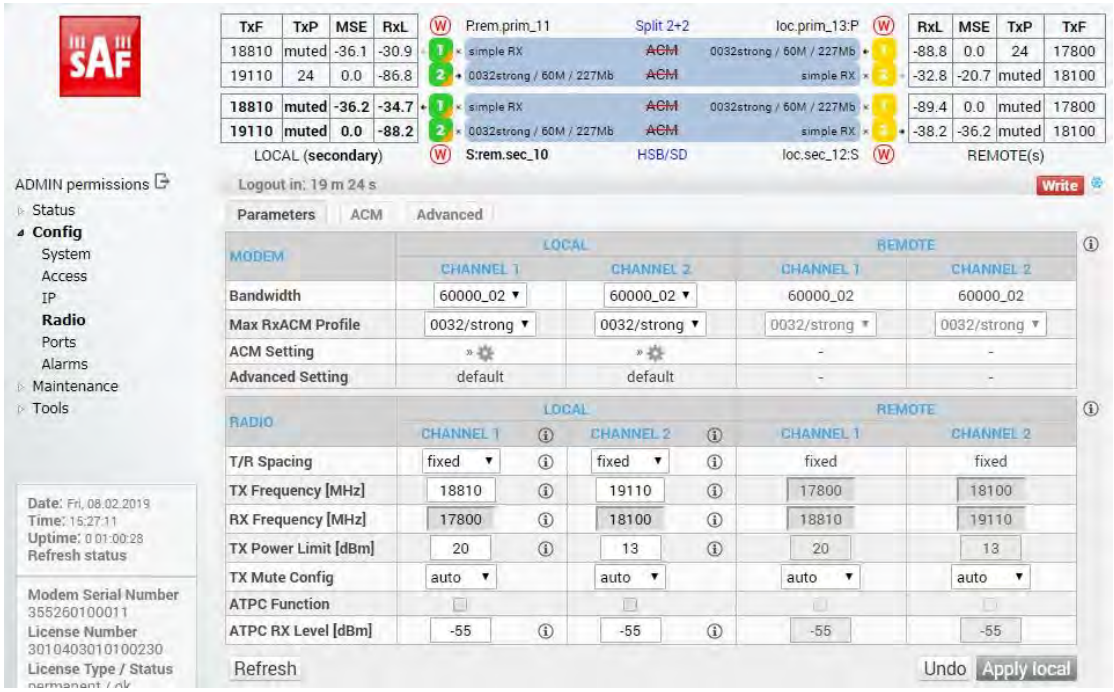


Figure 5.89 *Example of Side B Secondary IDU radio configuration*

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->Radio->ACM]' in the web GUI and set ACM function to "man p1" on both Channels. 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

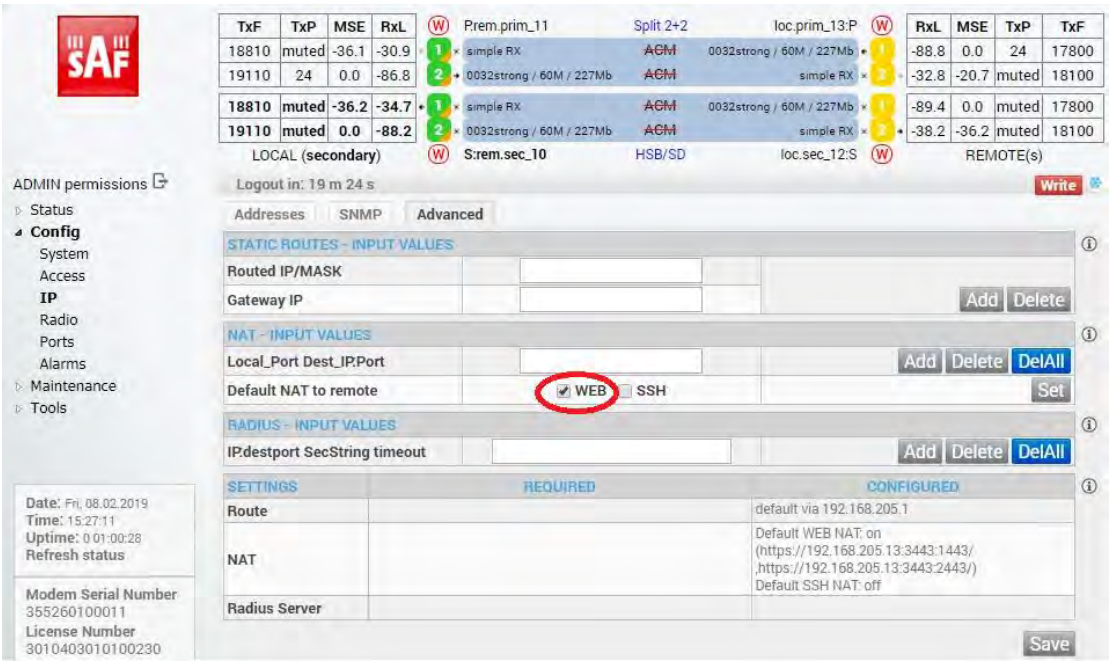


Figure 5.92 *Example of Side B Secondary IDU IP NAT configuration*

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

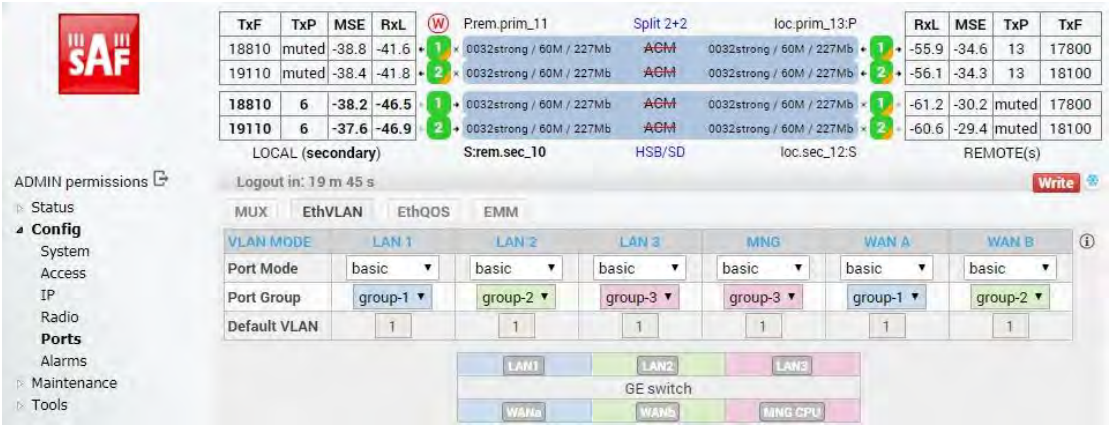


Figure 5.93 *Example of Side B Secondary IDU port grouping*

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’

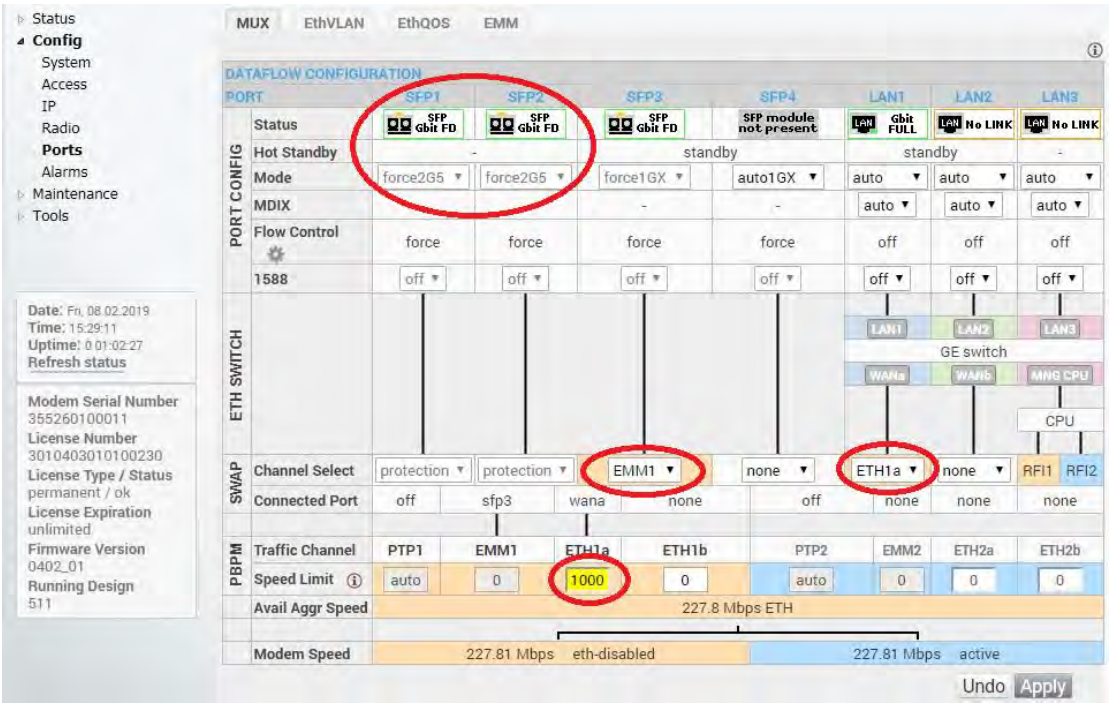


Figure 5.94 *Example of Side B Secondary IDU port configuration*

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->Minor' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover. In the example LAN1, SFP1, SFP2, SFP3 and ASI Port 1 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

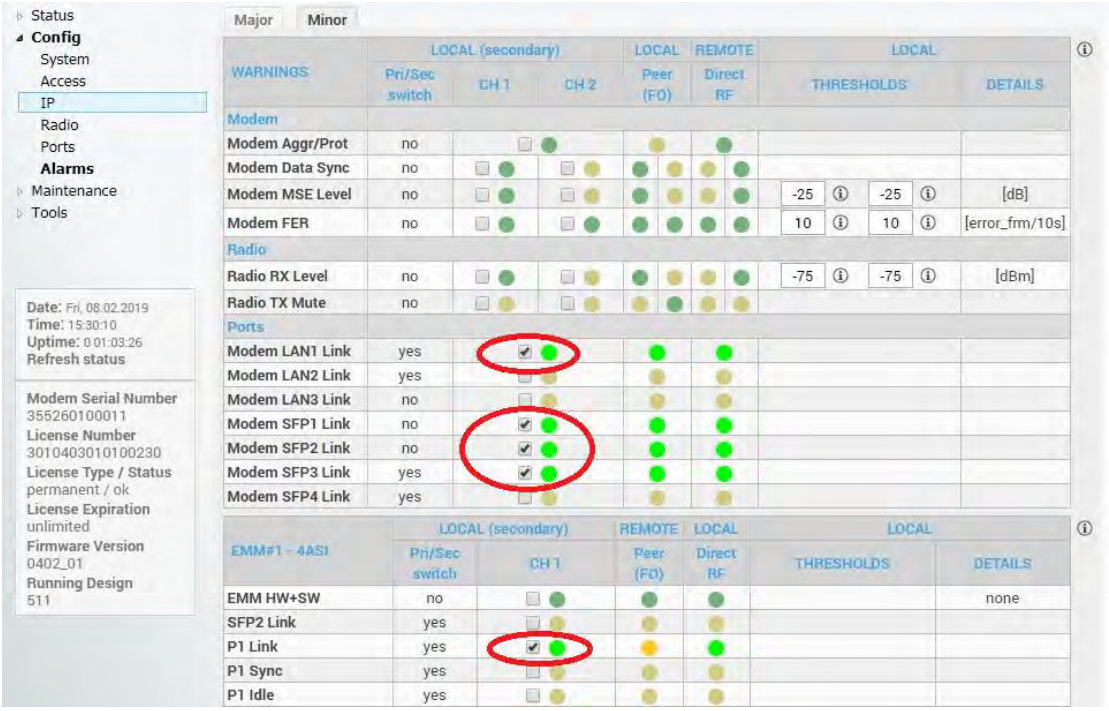


Figure 5.96 *Example of Side B Secondary IDU alarm configuration*

j) Save new settings by pressing 

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

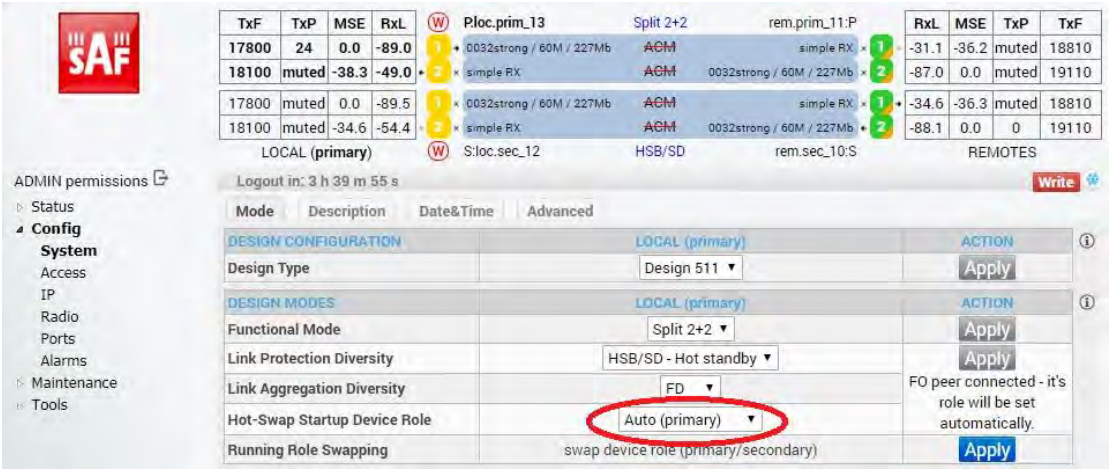


Figure 5.97 *Example of Primary IDUs system configuration in Auto mode*

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

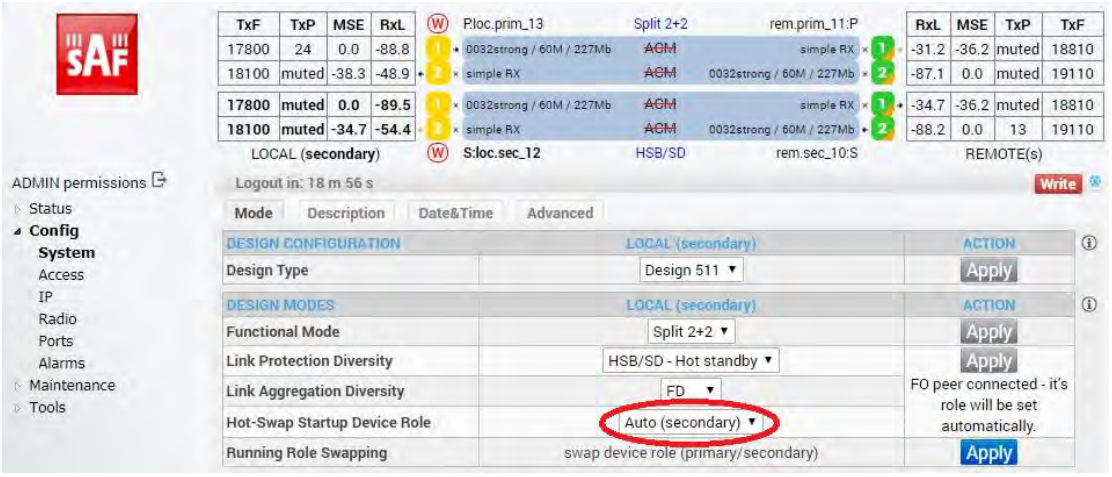


Figure 5.98 *Example of Secondary IDUs system configuration in Auto mode*

8) Save new settings by pressing  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):

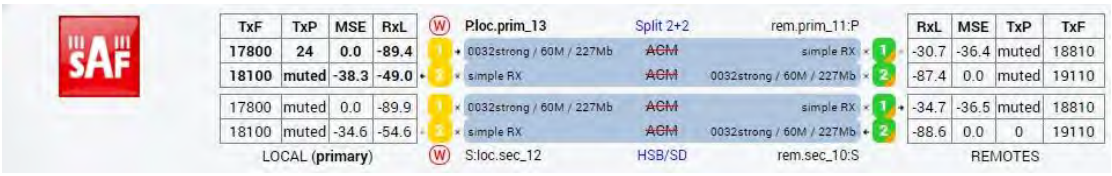


Figure 5.99 *Status of 1+1 HSB/SD Dual-band frequency mode*

Example 10 – 2+2 FD aggregation HSB/SD protection scheme

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.

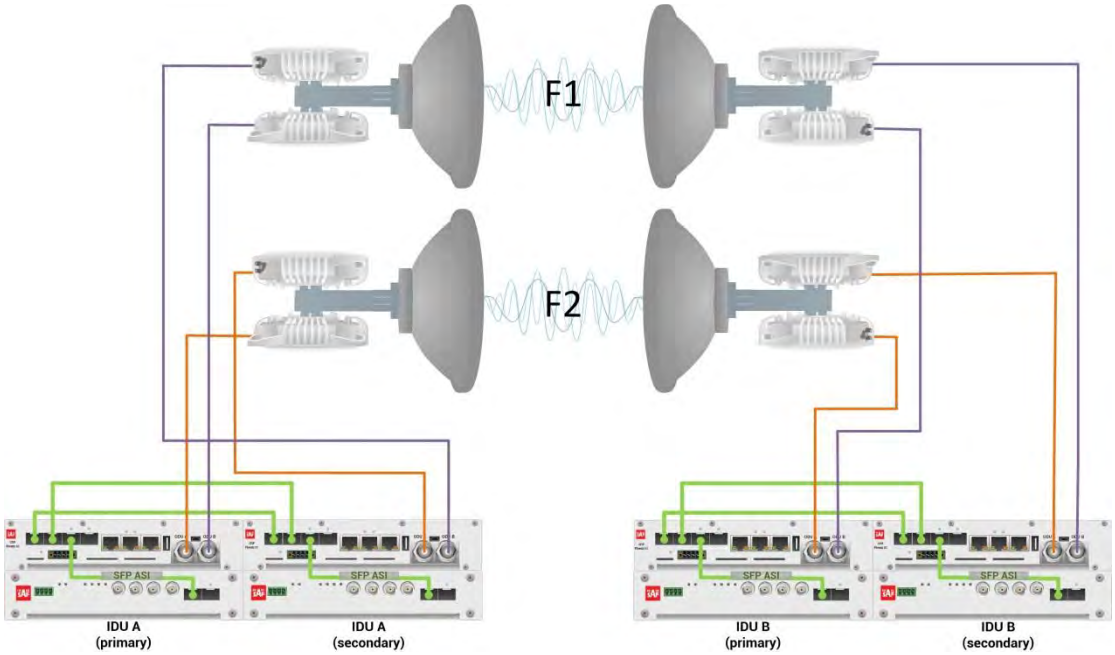


Figure 5.100a *Example of 2+2 FD aggregation HSB/SD protection scheme*

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.

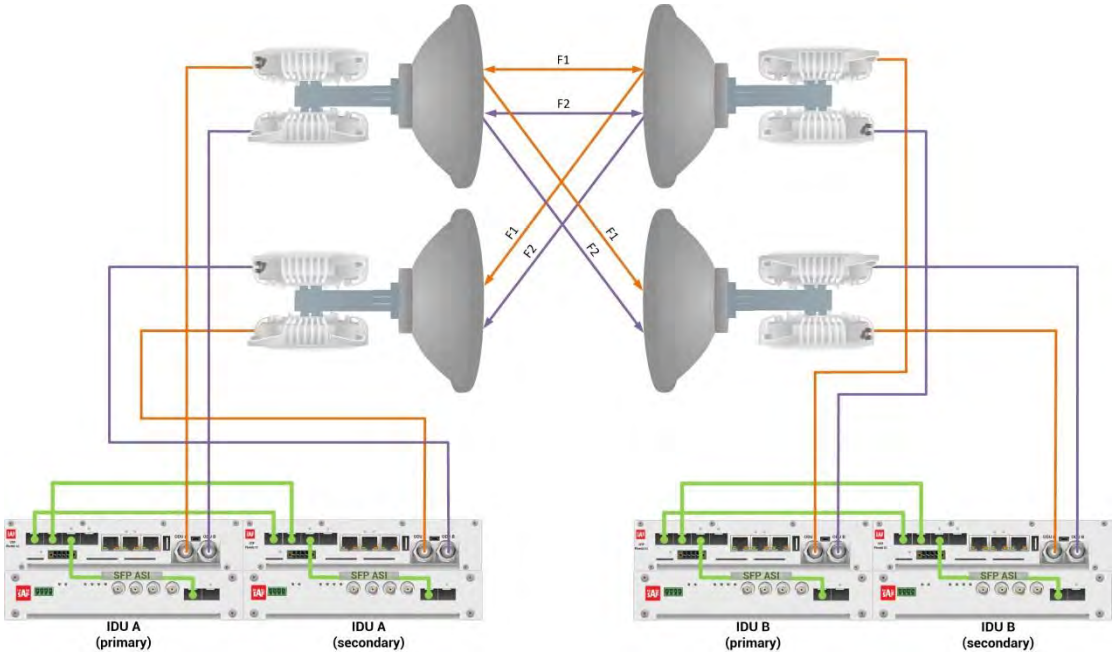


Figure 5.100b *Example of 2+2 FD aggregation HSB/SD protection scheme*

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 concrete 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

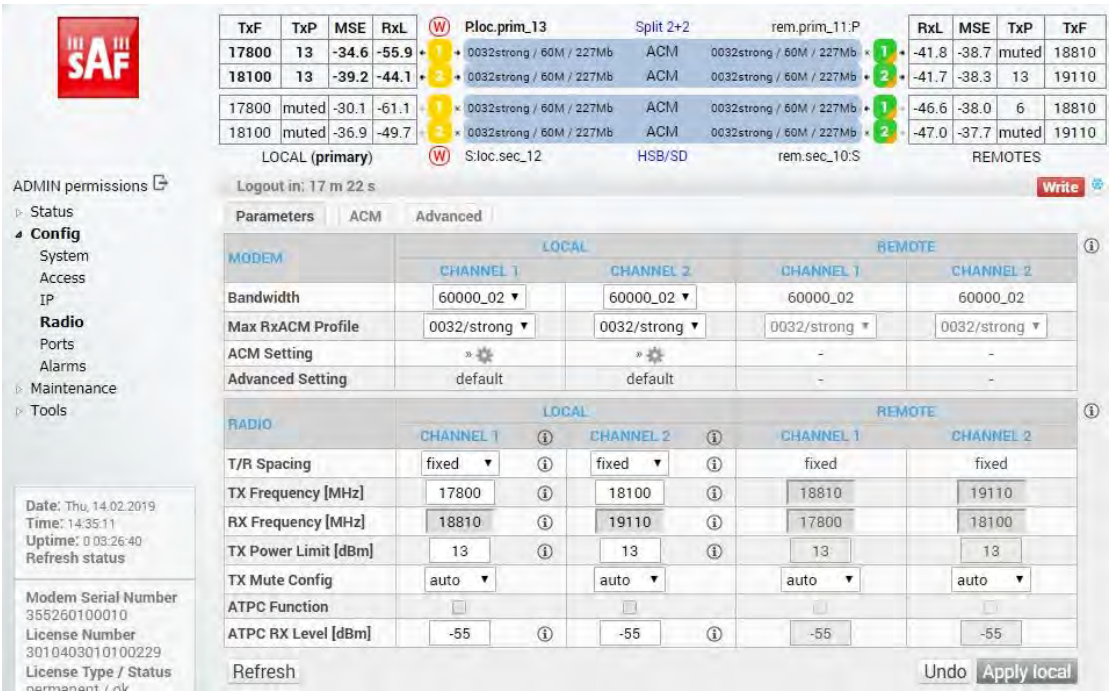


Figure 5.102 *Example of Radio configuration*

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

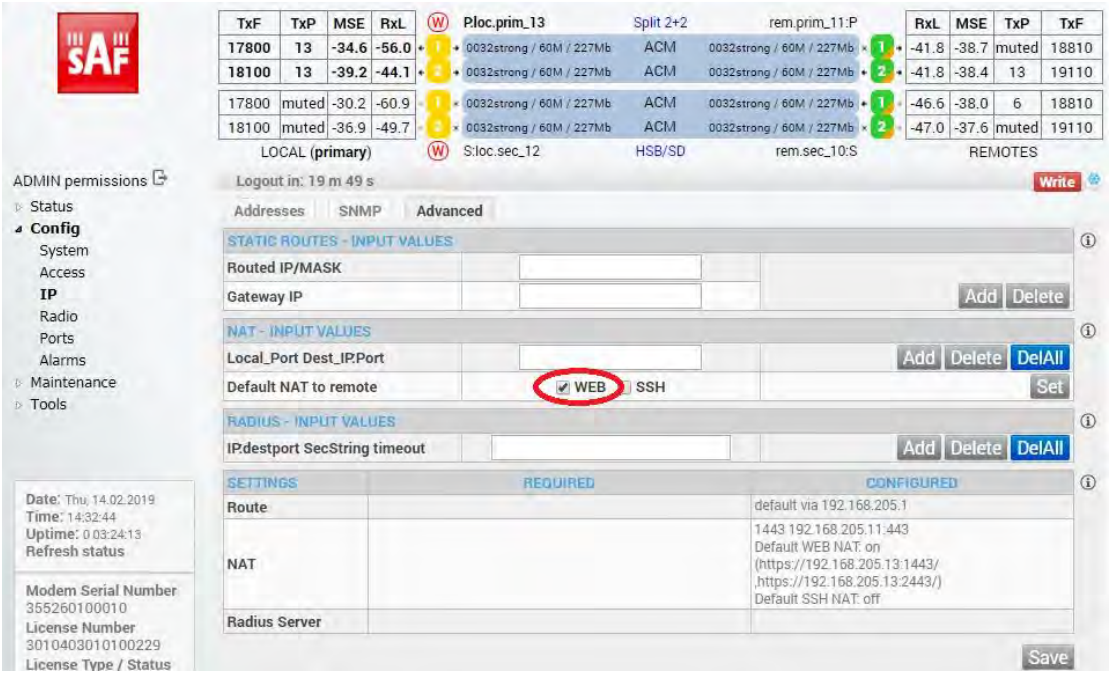


Figure 5.104 *Example of IP NAT configuration*

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

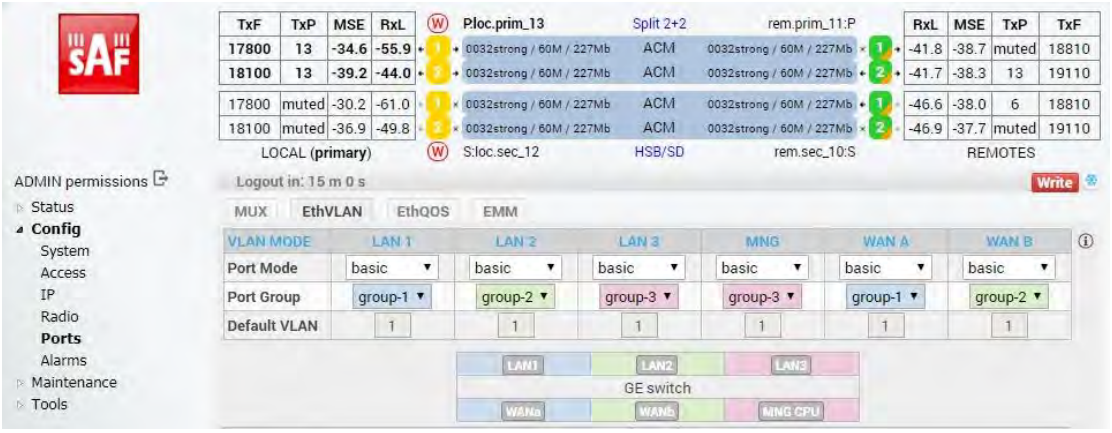


Figure 5.105 *Example of port grouping*

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'

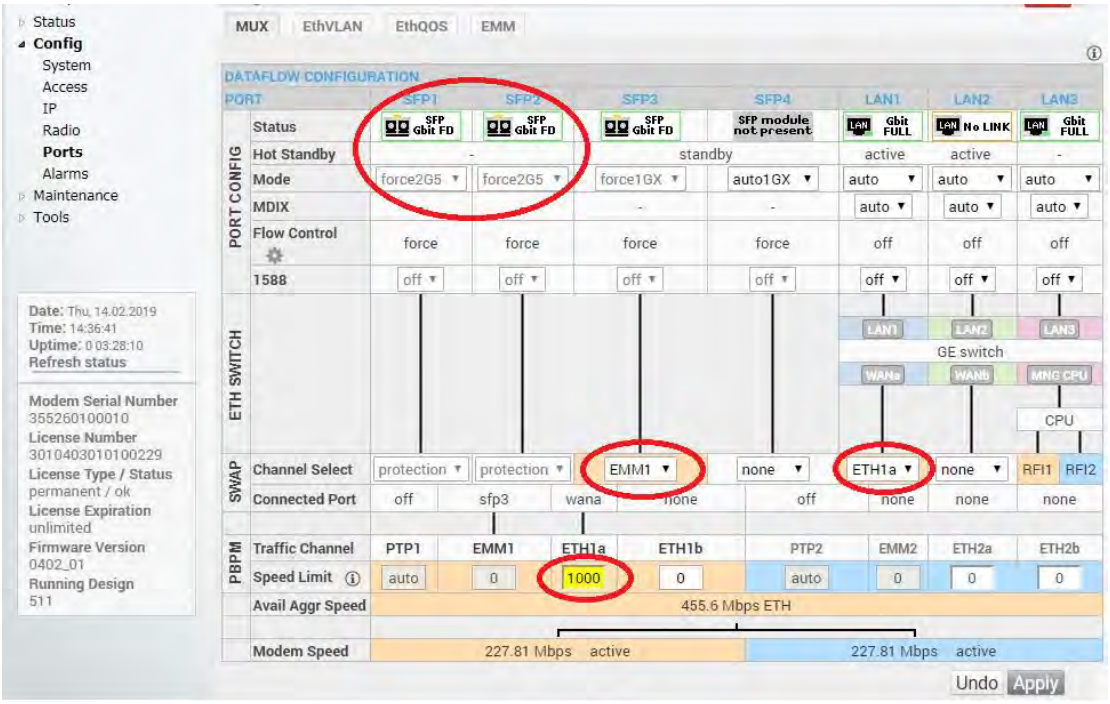


Figure 5.106 *Example of port configuration*

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->Minor]' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover in all Phoenix G2 IDUs. In the example LAN1, SFP1, SFP2, SFP3 and ASI Port 1 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

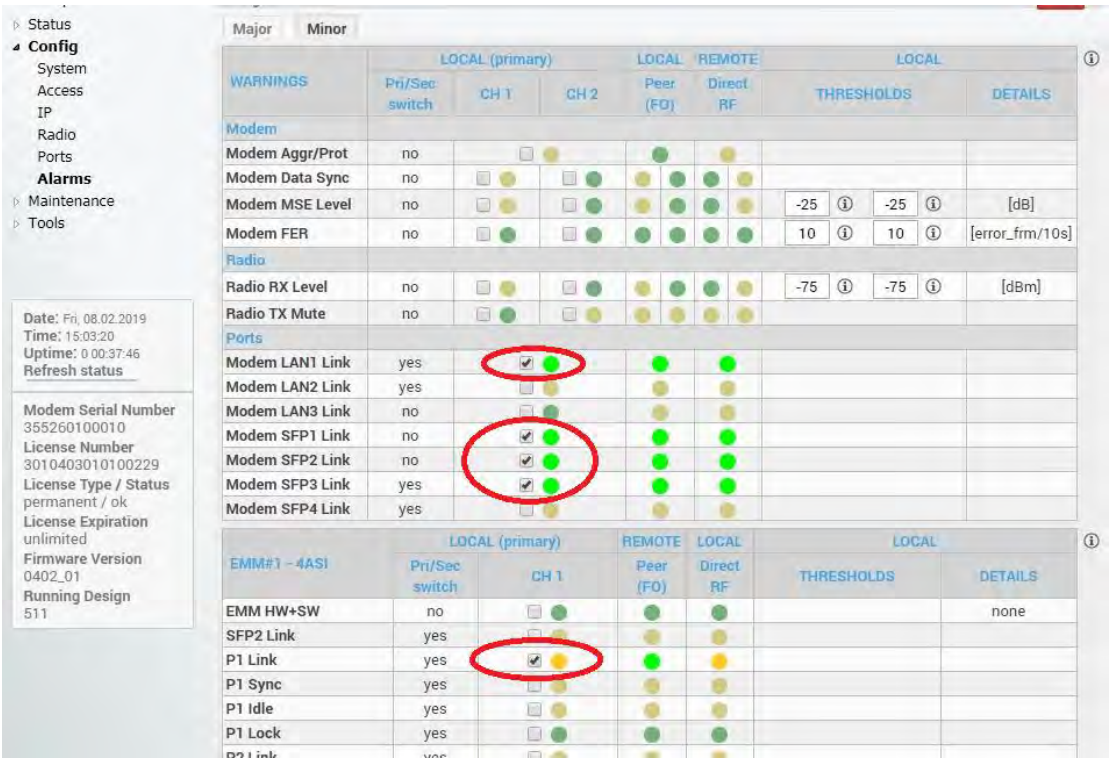


Figure 5.107 *Example of alarm configuration*

9) Save new settings by pressing Write button.
10) Reboot all 4 IDUs after successful reconfiguration
11) 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

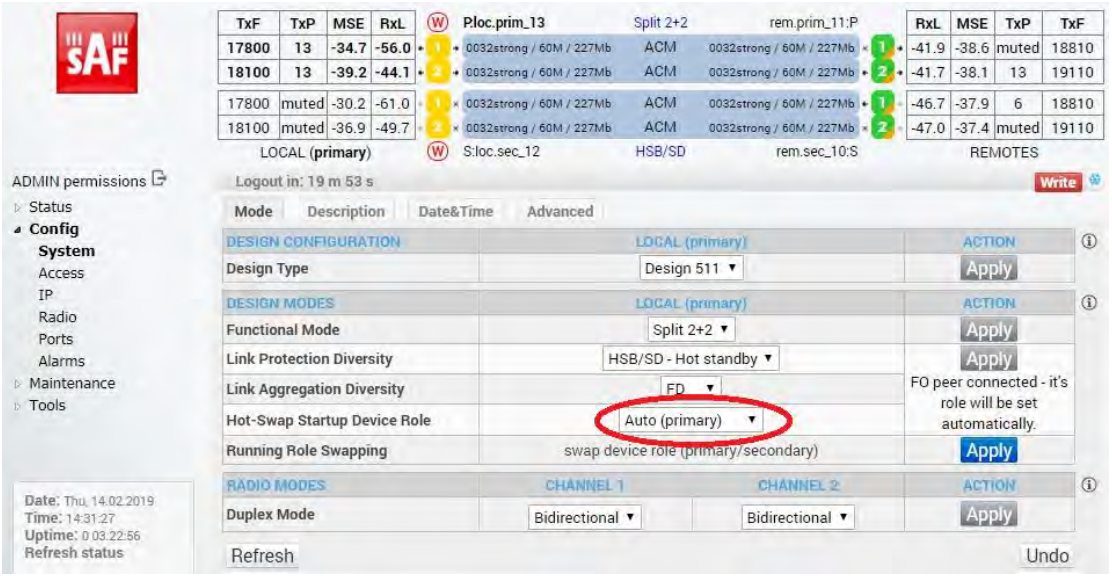


Figure 5.108 *Example of system configuration in Auto mode*

12) 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):

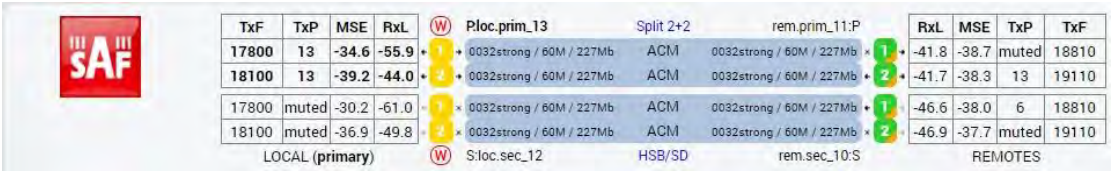


Figure 5.109 *Status of 2+2FD aggregation HSB/SD protection mode*

Example 11 – 2+2 FD aggregation FD protection scheme

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.

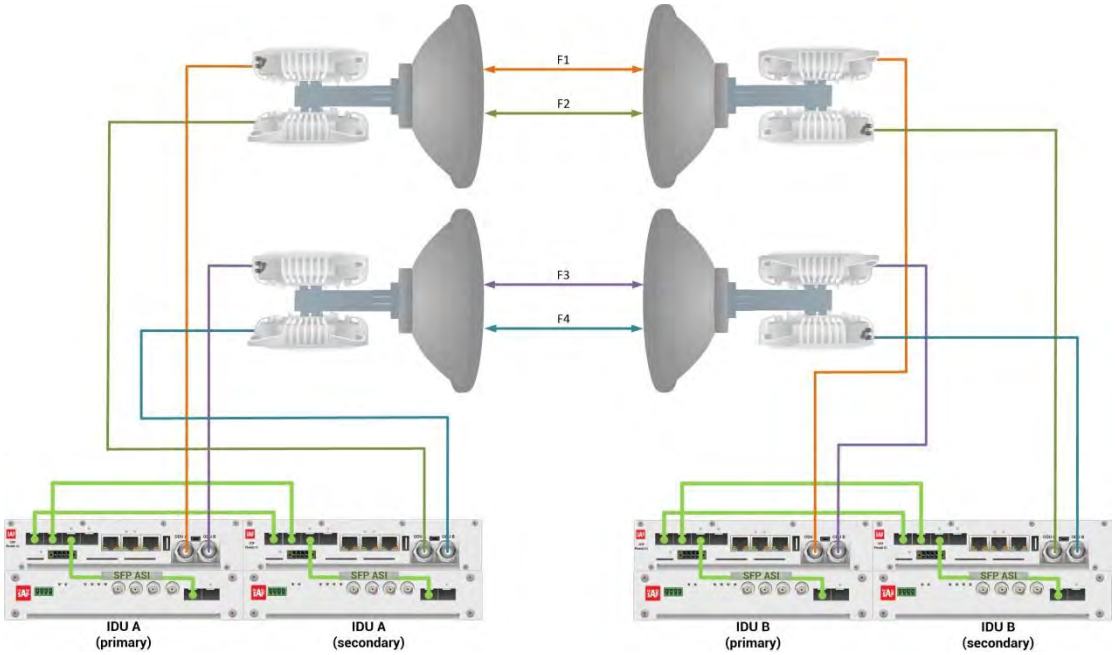


Figure 5.110a *Example of 2+2 FD aggregation FD protection scheme*

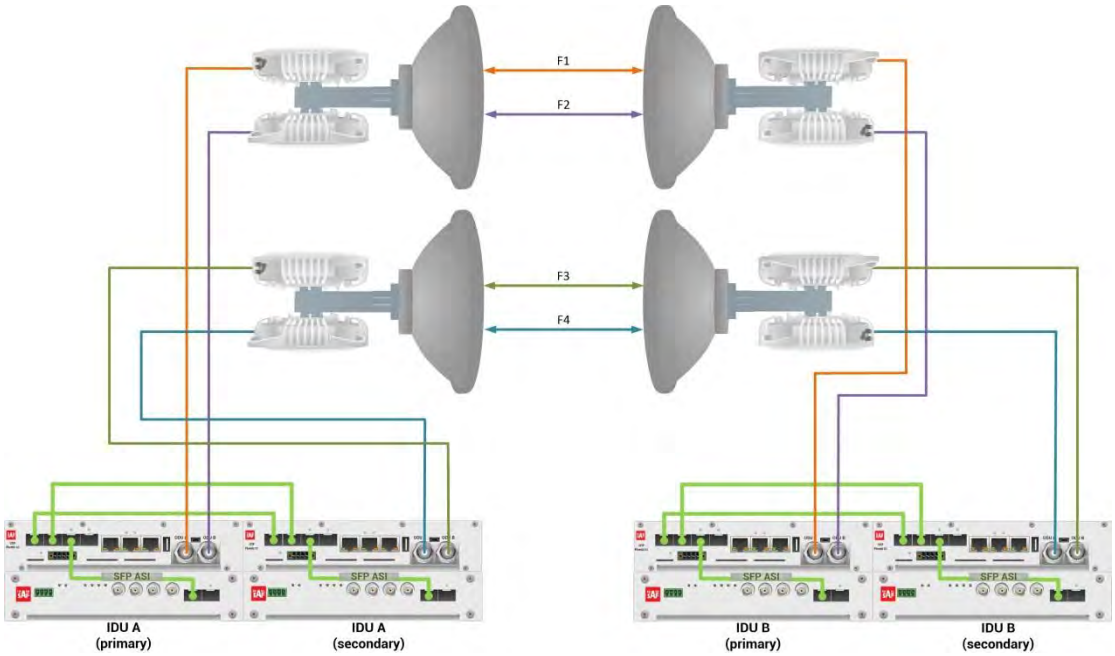


Figure 5.110b *Example of 2+2 FD aggregation FD protection scheme*

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 concrete 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

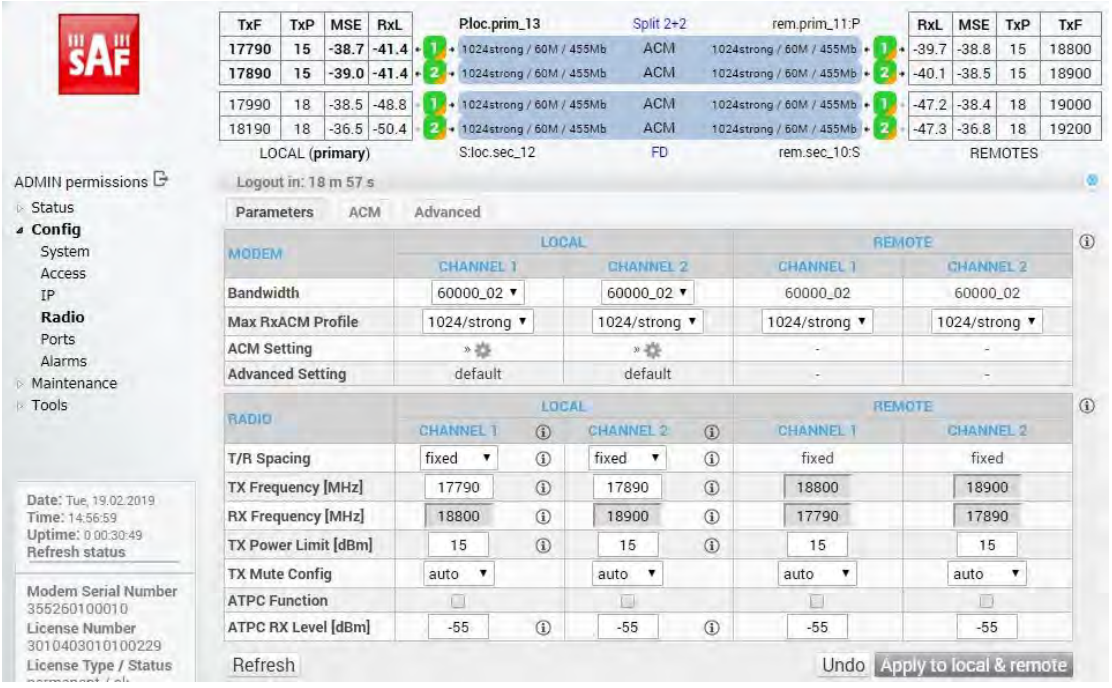


Figure 5.112 *Example of Primary IDU Radio configuration*

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

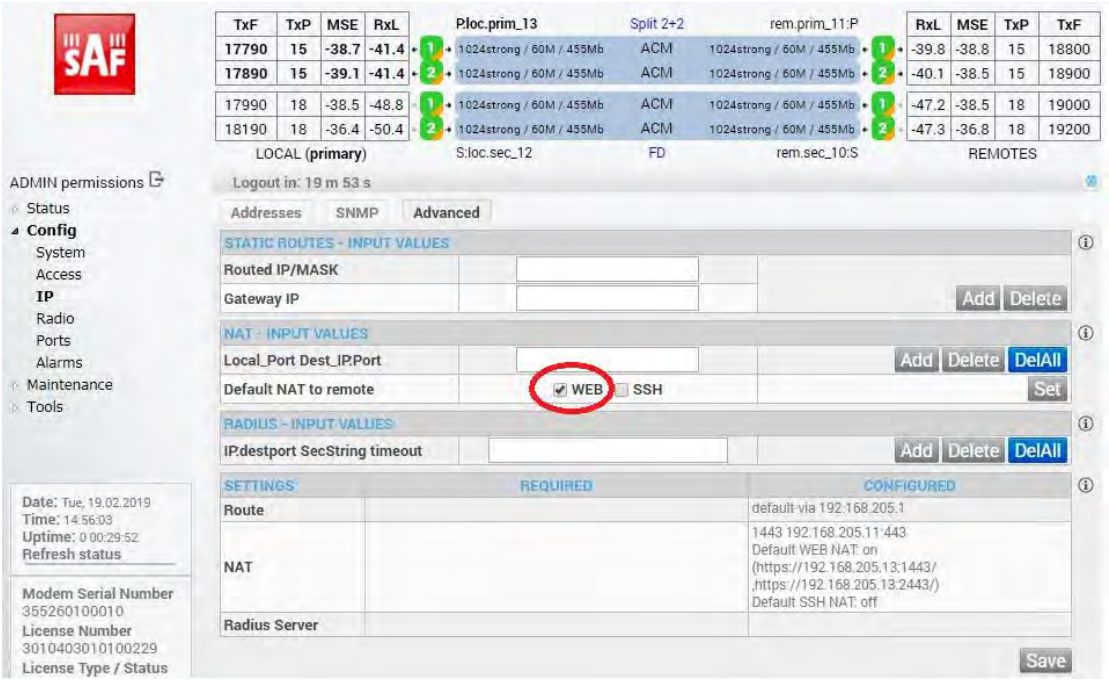


Figure 5.115 *Example of IP NAT configuration*

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

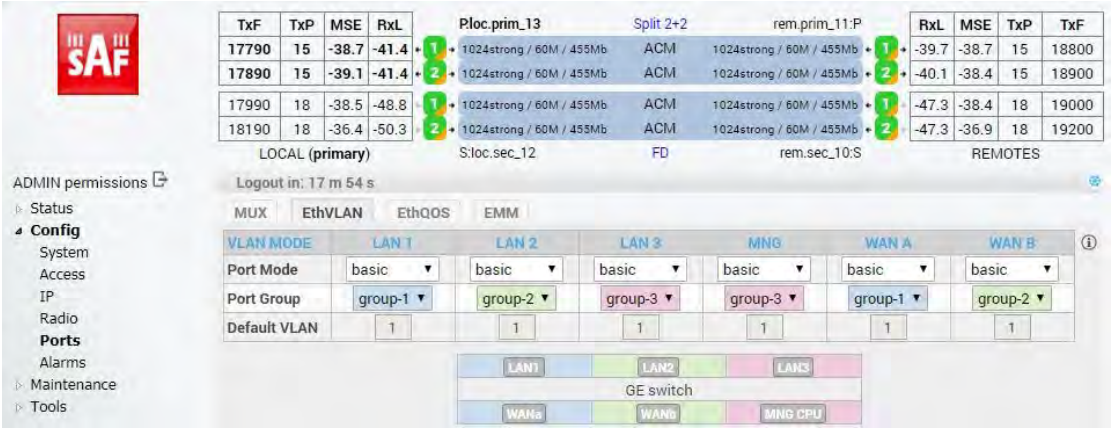


Figure 5.116 *Example of port grouping*

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'

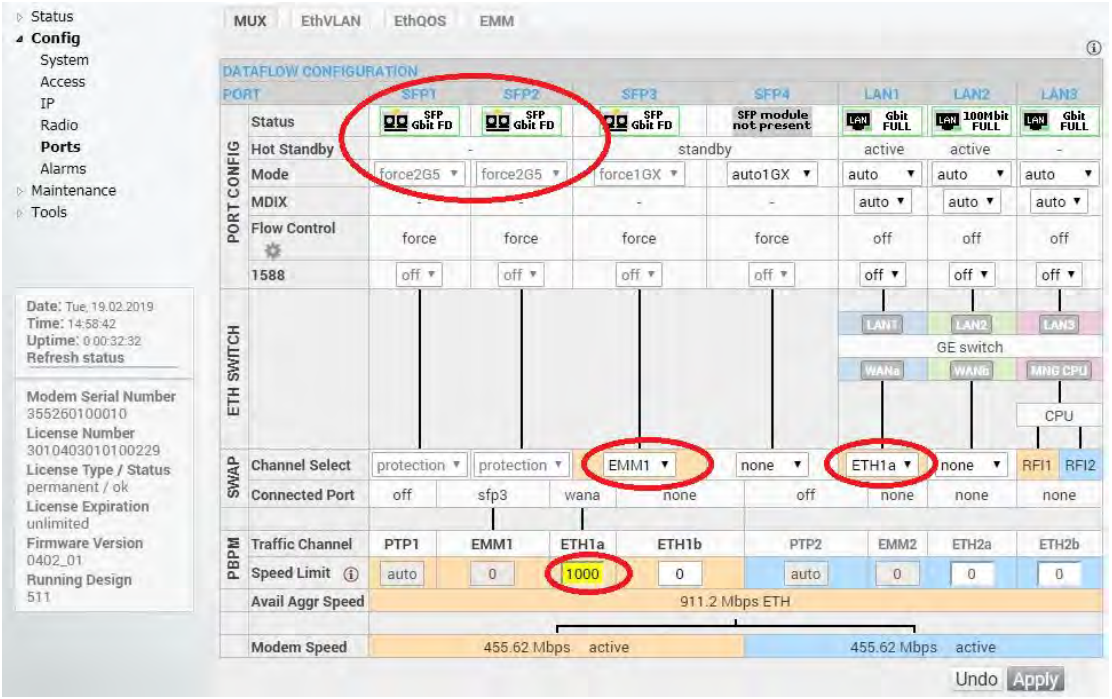


Figure 5.117 *Example of port configuration*

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->Minor](#)' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover in all Phoenix G2 IDUs. In the example LAN1, SFP1, SFP2, SFP3 and ASI Port 1 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

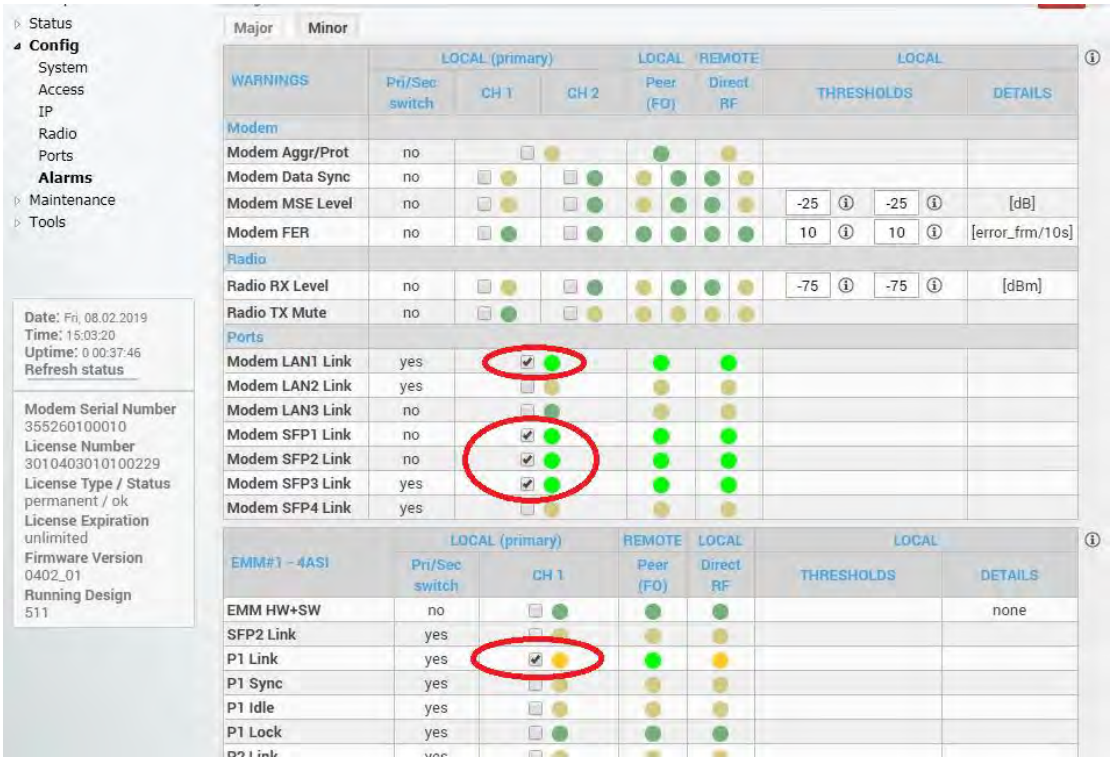


Figure 5.118 *Example of alarm configuration*

9) Save new settings by pressing Write button.
10) Reboot all 4 IDUs after successful reconfiguration
11) 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

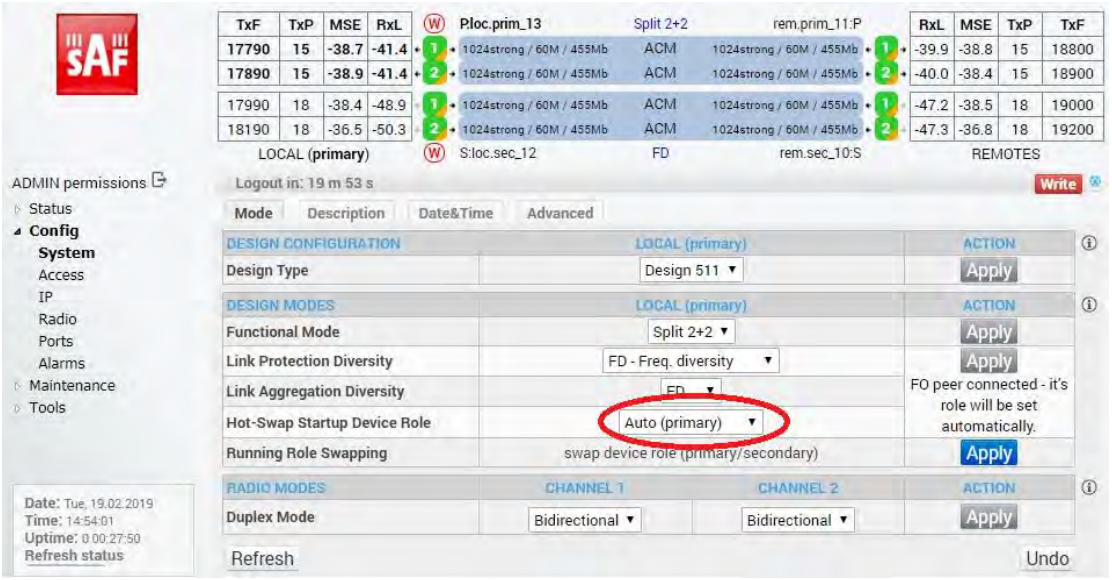


Figure 5.119 *Example of system configuration in Auto mode*

12) 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):

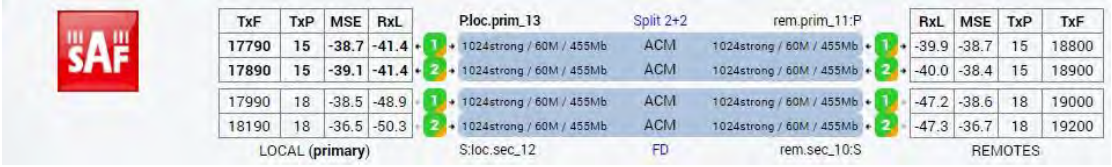


Figure 5.120 *Status of 2+2 FD aggregation FD protection mode*

Example 12 – 2+2 XPIC aggregation HSB/SD protection scheme

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.

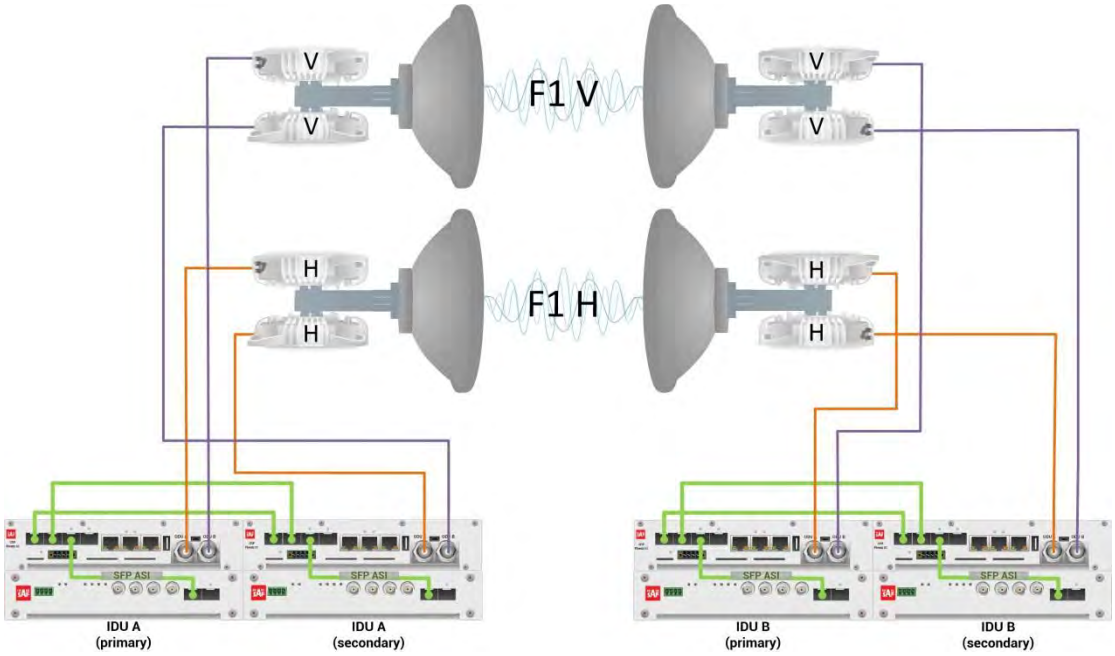


Figure 5.121a *Example of 2+2 XPIC aggregation HSB/SD protection scheme*

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.

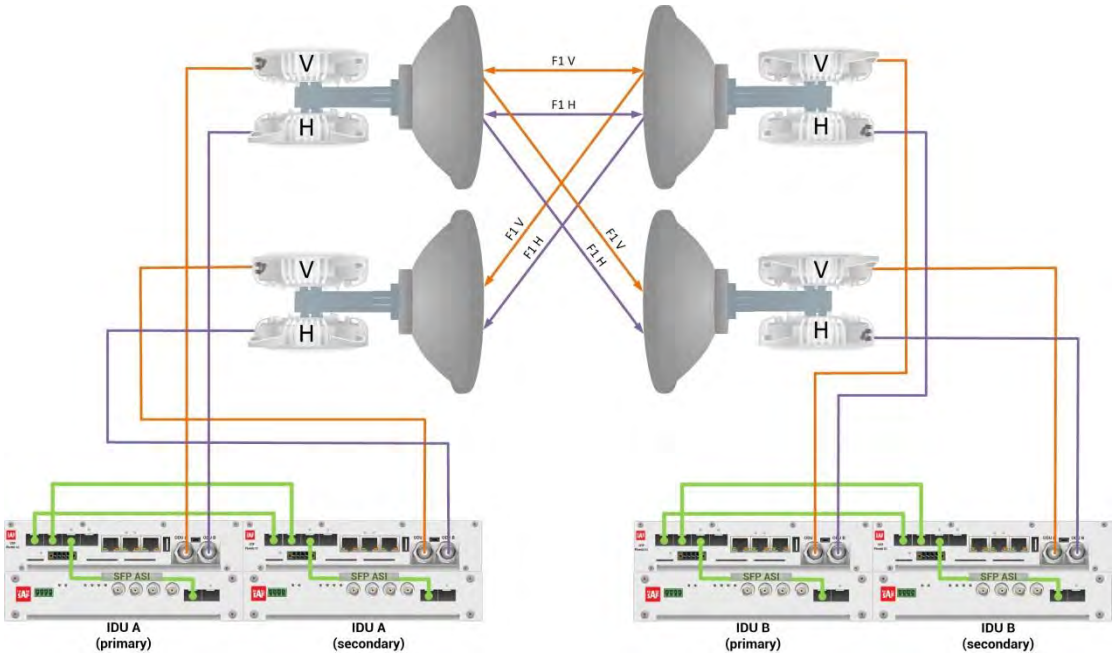


Figure 5.121b *Example of 2+2 XPIC aggregation HSB/SD protection scheme*

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 concrete 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

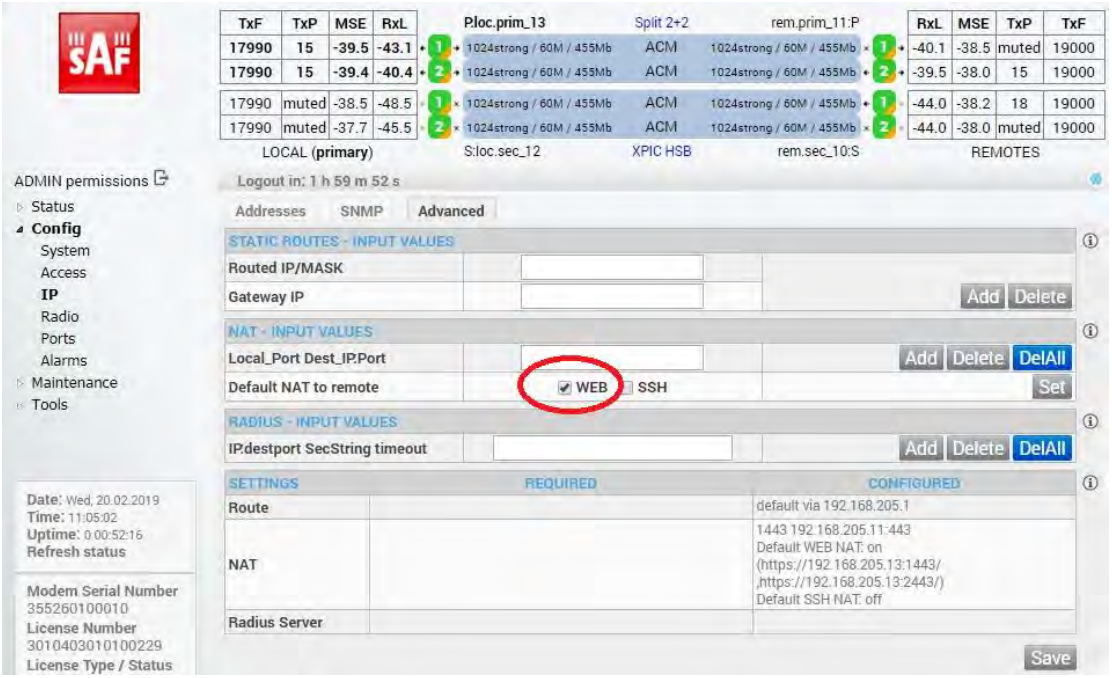


Figure 5.125 *Example of IP NAT configuration*

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

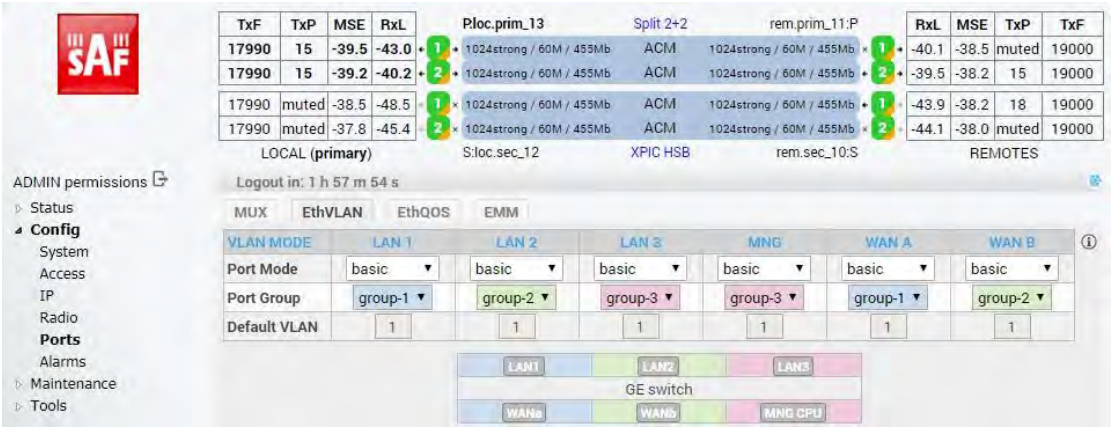


Figure 5.126 *Example of port grouping*

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'

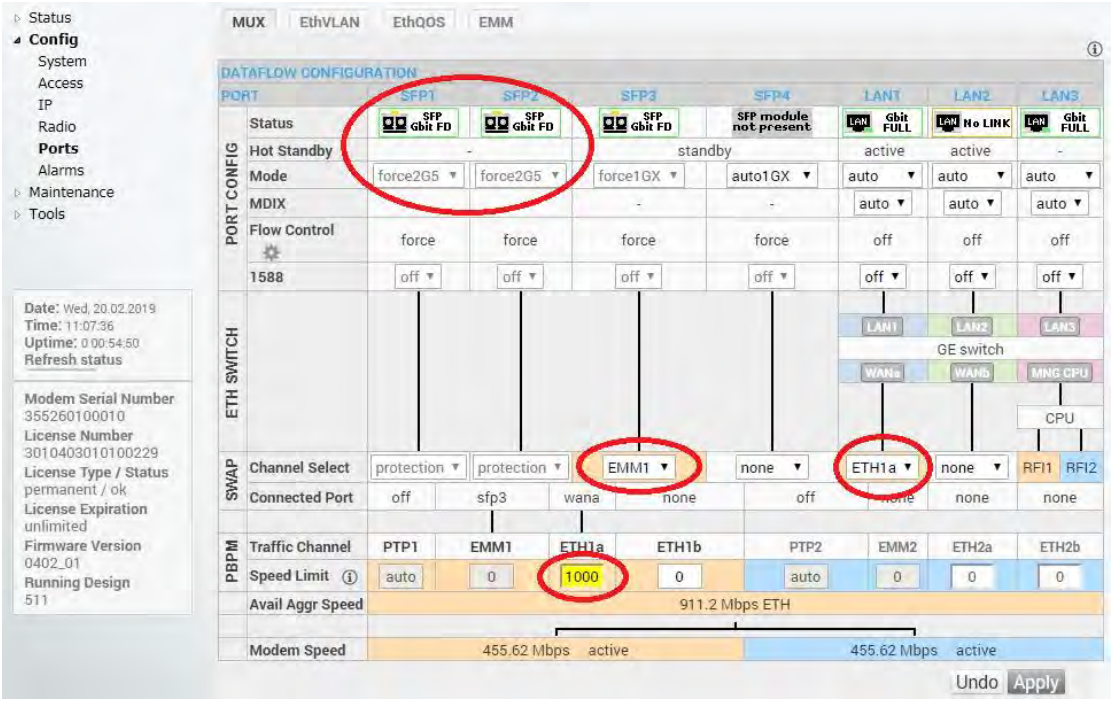


Figure 5.127 *Example of port configuration*

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->Minor](#)' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover in all Phoenix G2 IDUs. In the example LAN1, SFP1, SFP2, SFP3 and ASI Port 1 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

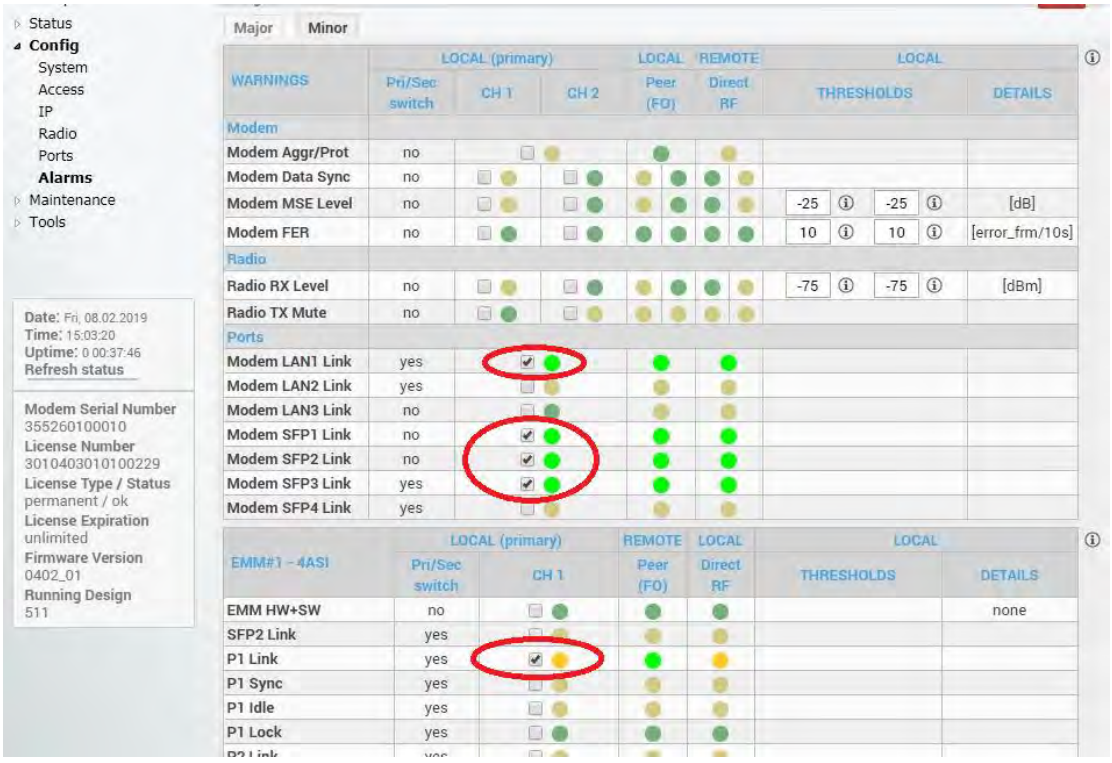


Figure 5.128 *Example of alarm configuration*

9) Save new settings by pressing Write button.
10) Reboot all 4 IDUs after successful reconfiguration
11) 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

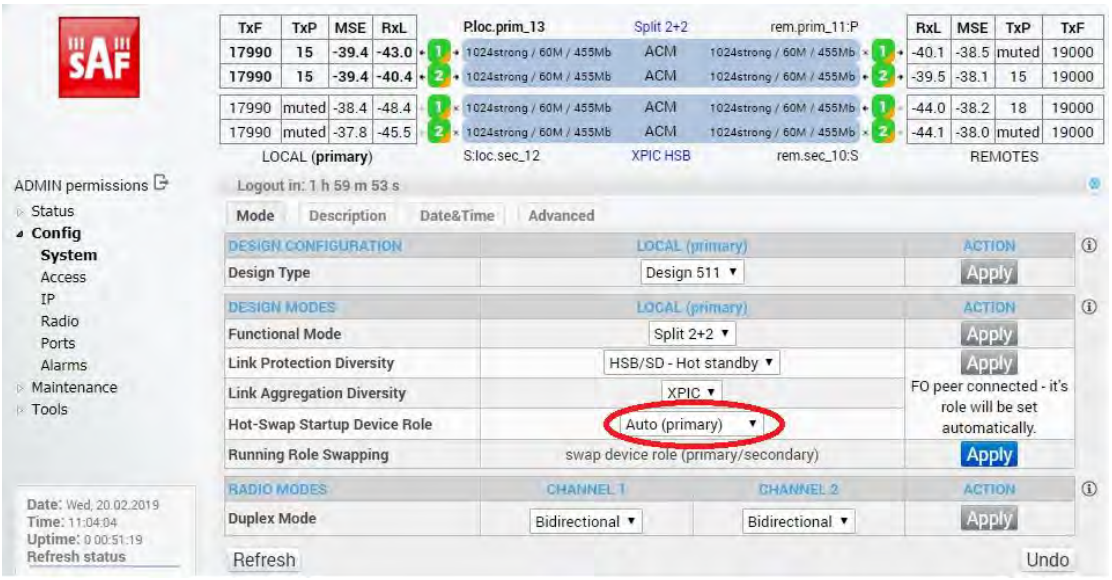


Figure 5.129 *Example of system configuration in Auto mode*

12) 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):

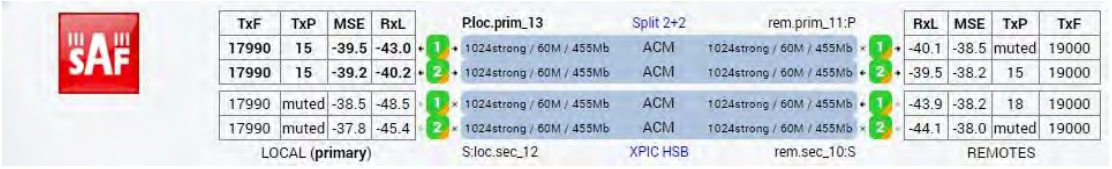


Figure 5.130 *Status of 2+2 XPIC aggregation HSB/SD protection mode*

Example 13 – 2+2 XPIC aggregation FD protection scheme

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.

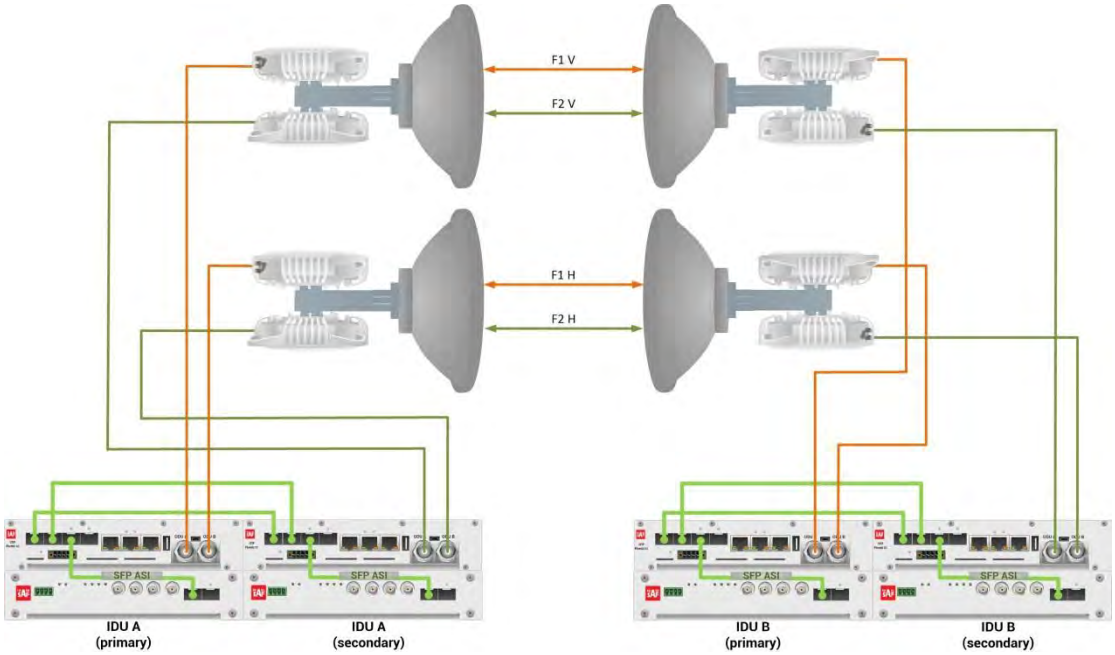


Figure 5.131a *Example of 2+2 XPIC aggregation FD protection scheme*

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.

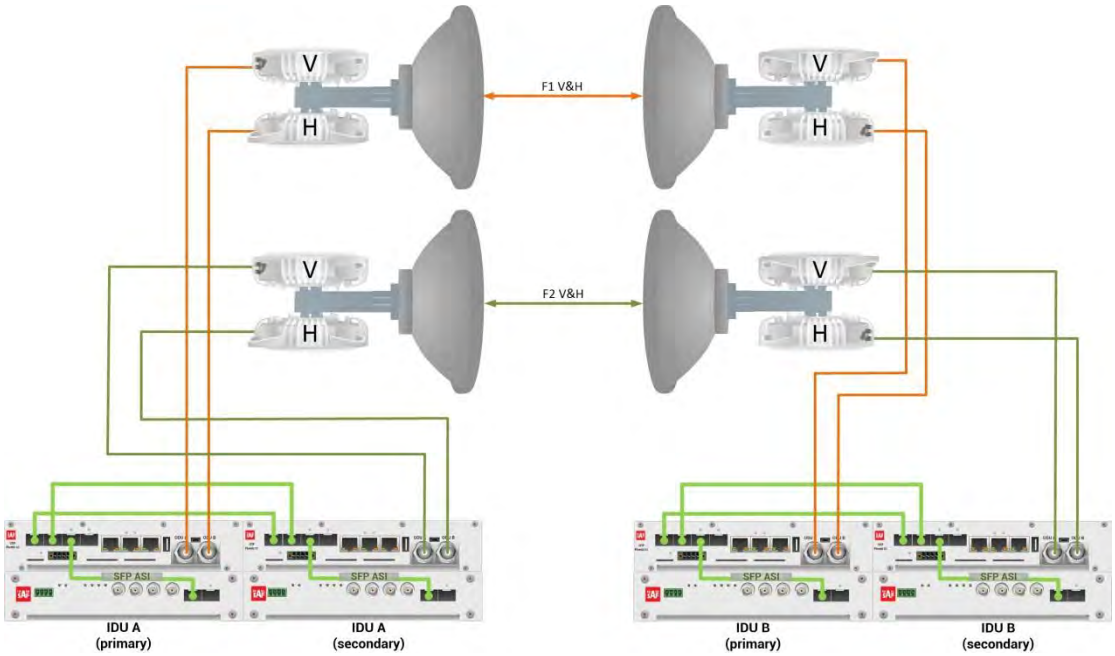


Figure 5.131b *Example of 2+2 XPIC aggregation FD protection scheme*

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 concrete 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 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 '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*

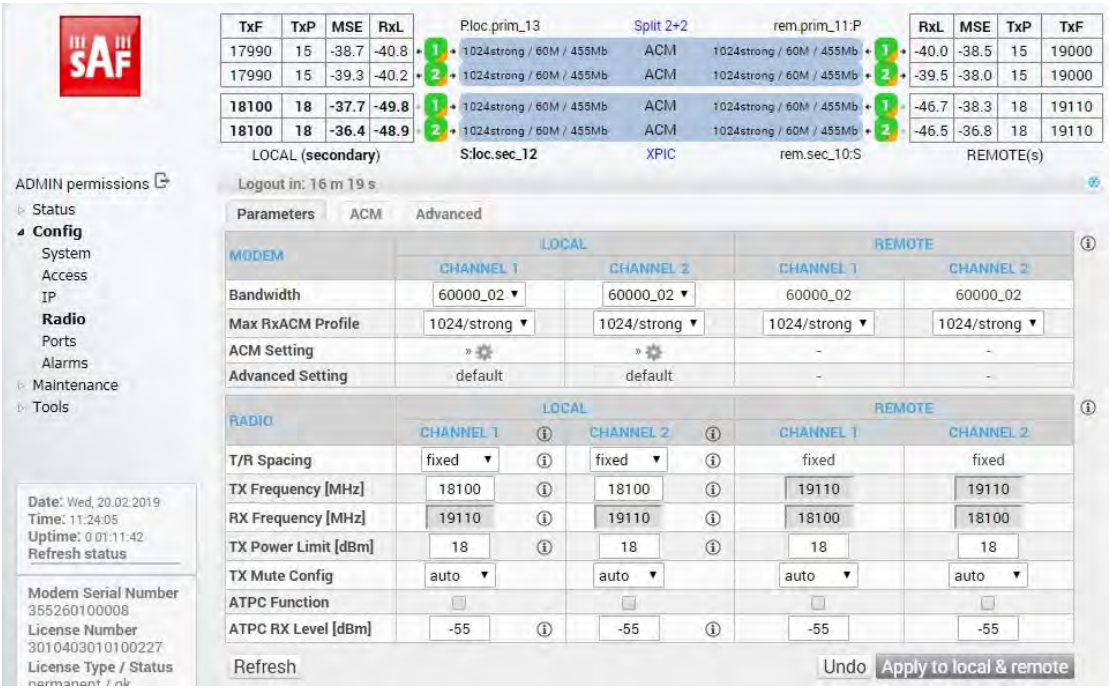


Figure 5.134 *Example of Secondary IDU Radio configuration*

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

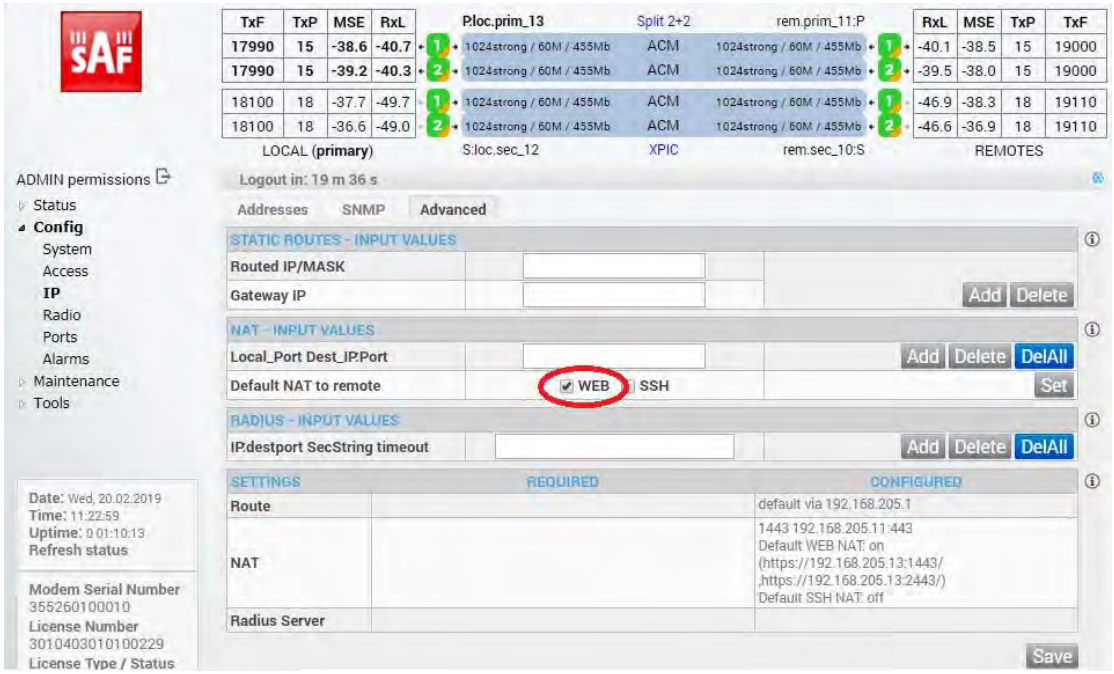


Figure 5.136 *Example of IP NAT configuration*

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

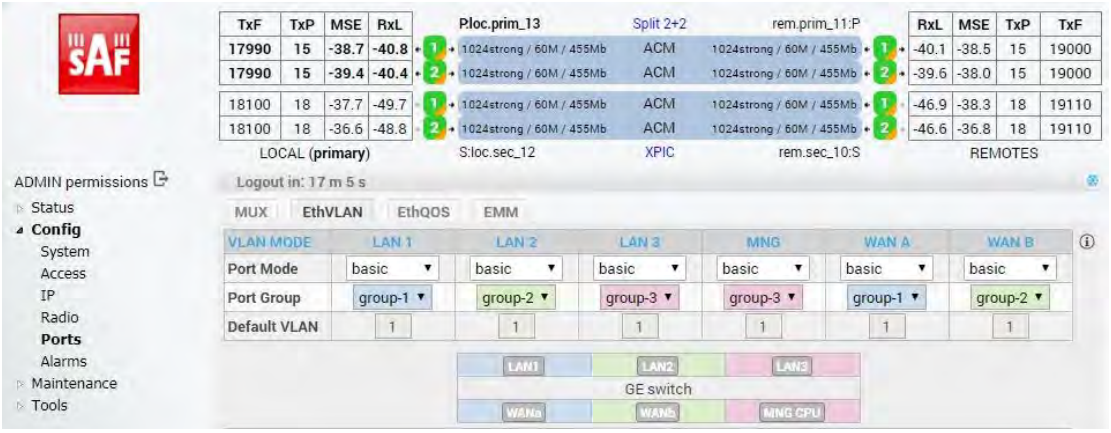


Figure 5.137 *Example of port grouping*

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'

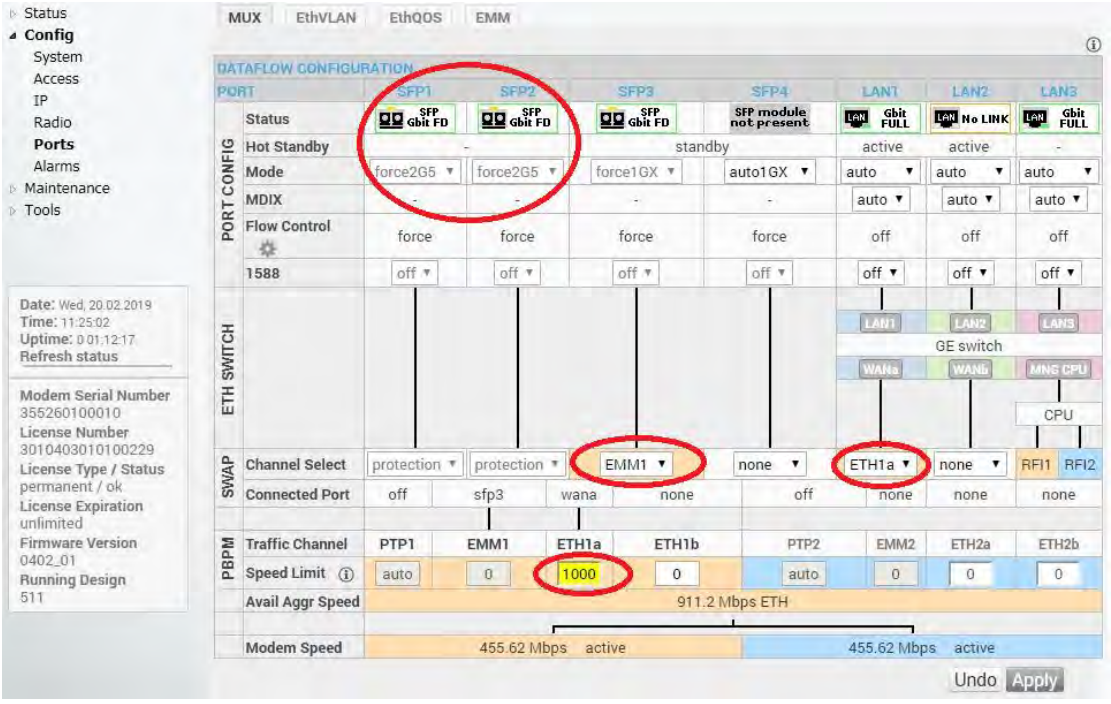


Figure 5.138 *Example of port configuration*

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->Minor' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover in all Phoenix G2 IDUs. In the example LAN1, SFP1, SFP2, SFP3 and ASI Port 1 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

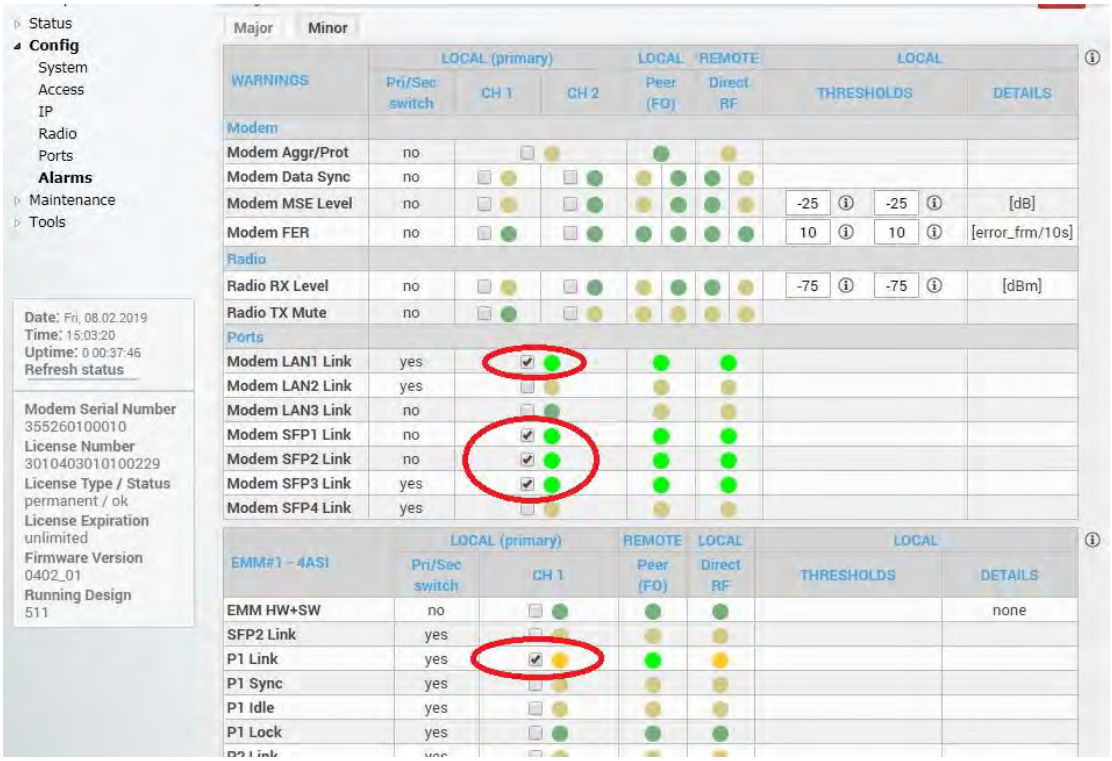


Figure 5.139 *Example of alarm configuration*

9) Save new settings by pressing  button.
10) Reboot all 4 IDUs after successful reconfiguration
11) 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

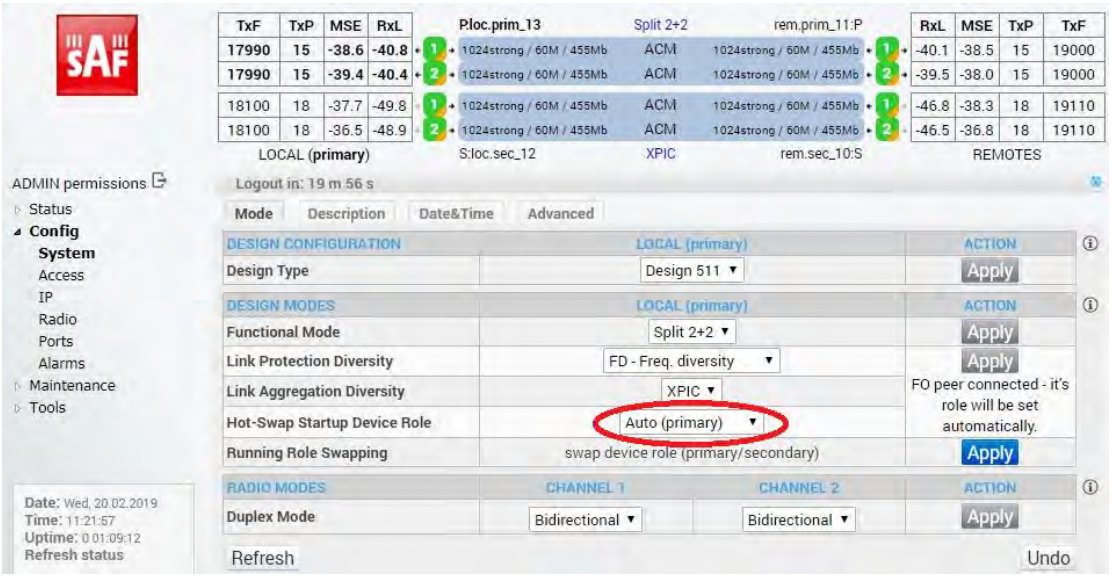


Figure 5.140 *Example of system configuration in Auto mode*

12) Save new settings by pressing  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):

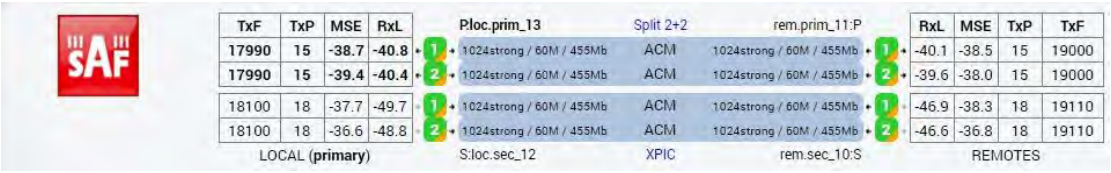


Figure 5.141 *Status of 2+2 XPIC aggregation FD protection mode*

Example 14 – 1+1 HSB/SD Full protection scheme

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

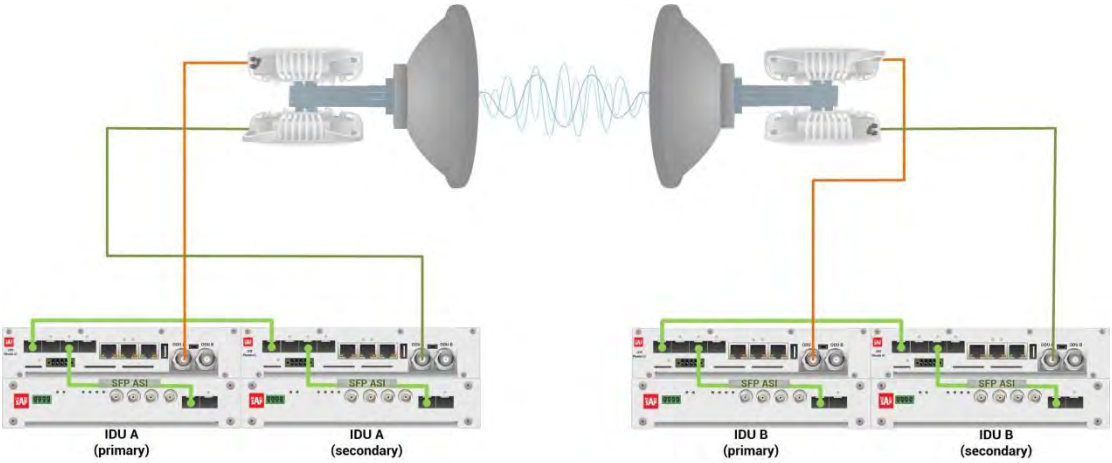


Figure 5.142a *Example of 1+1 HSB full protection scheme*

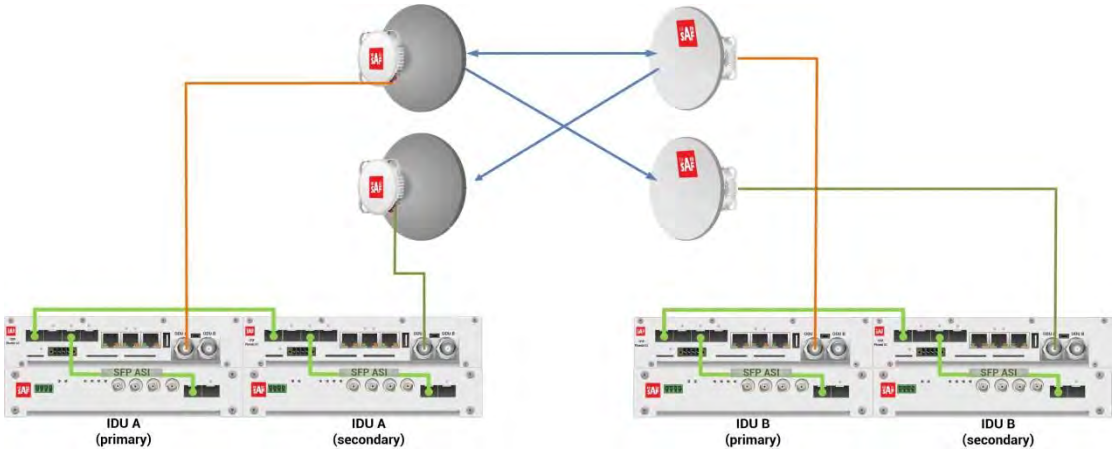


Figure 5.142b *Example of 1+1 SD full protection scheme*

This concrete example describes an application where the Design Type 'Design 511', 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', 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

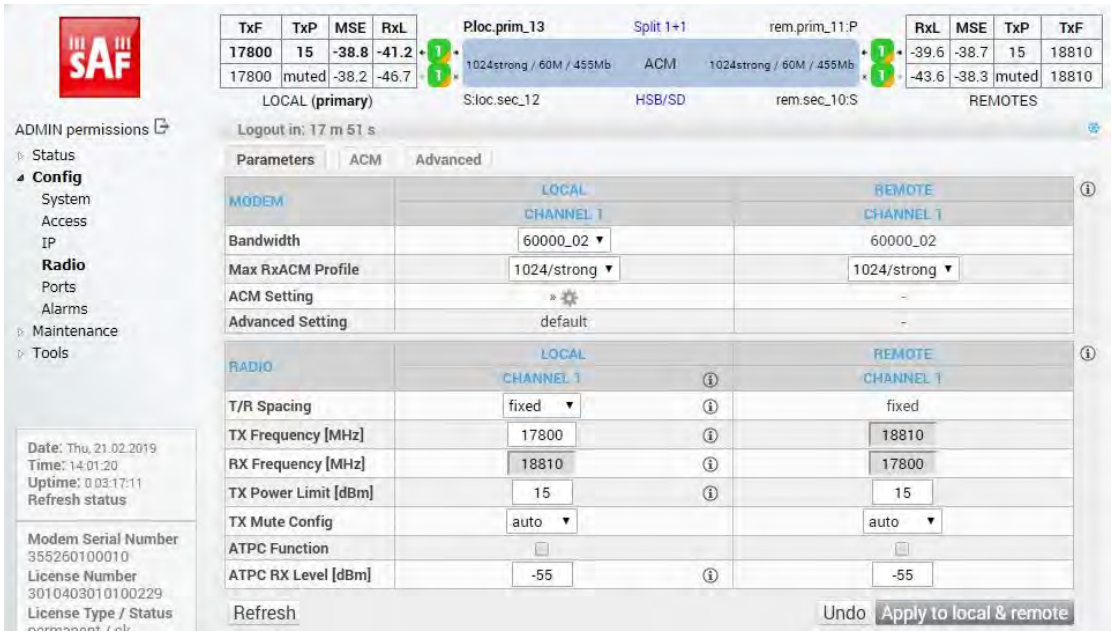


Figure 5.144 *Example of Radio configuration*

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

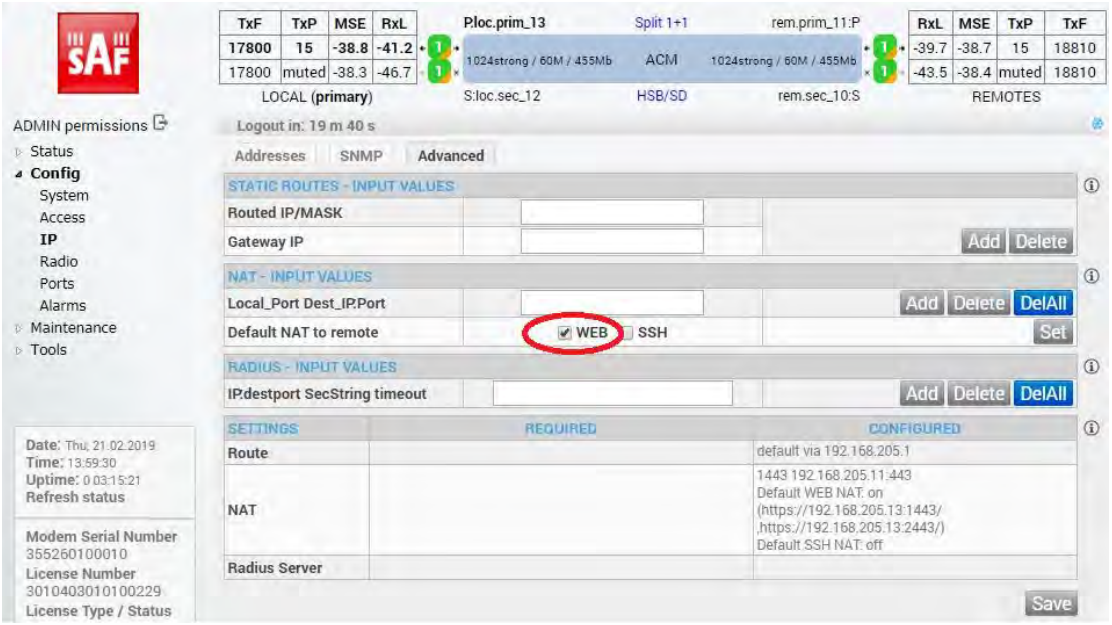


Figure 5.146 *Example of IP NAT configuration*

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'

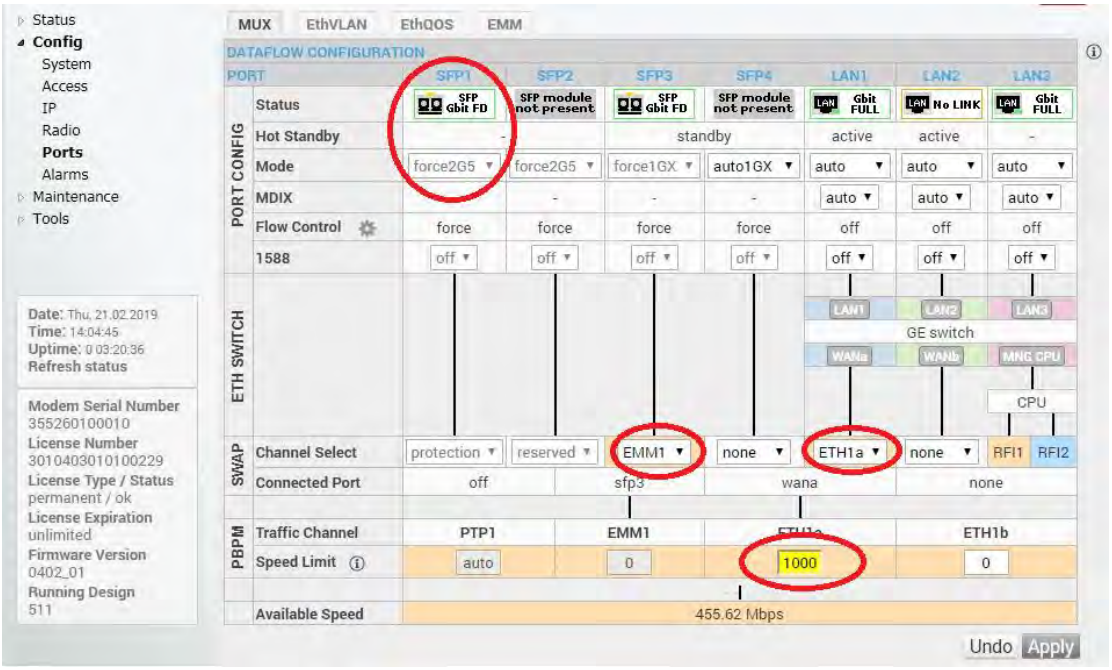


Figure 5.148 *Example of port configuration*

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->Minor' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover in all Phoenix G2 IDUs. In the example LAN1, SFP1, SFP3 and ASI Port 1 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

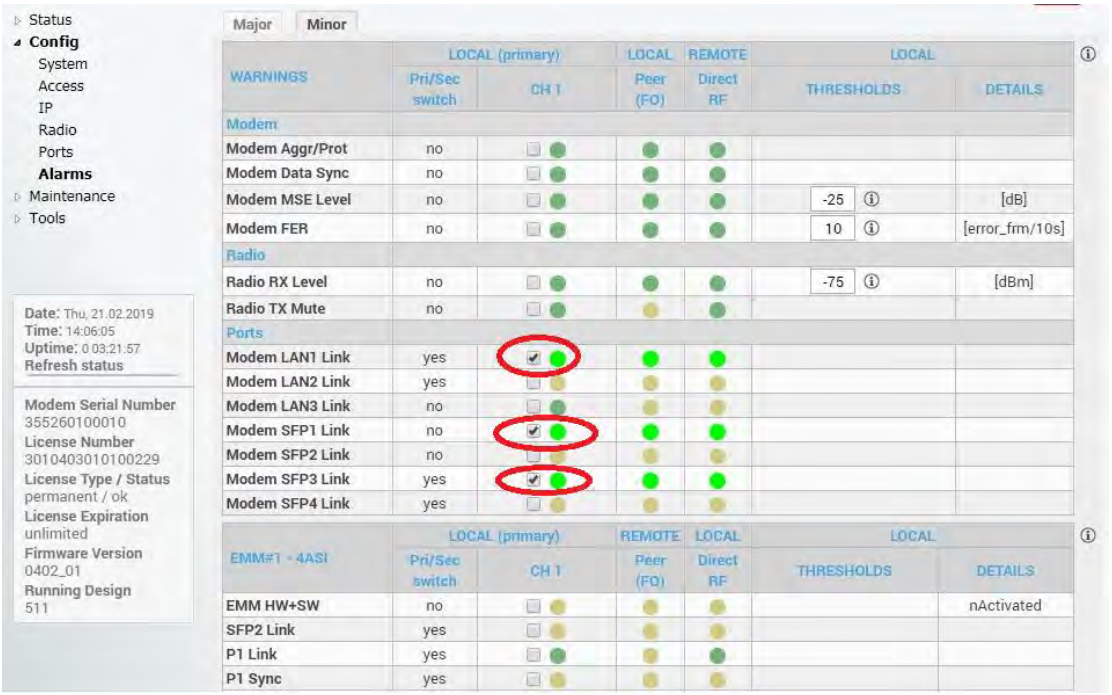


Figure 5.149 *Example of alarm configuration*

9) Save new settings by pressing 

button.
10) Reboot all 4 IDUs after successful reconfiguration

11) 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

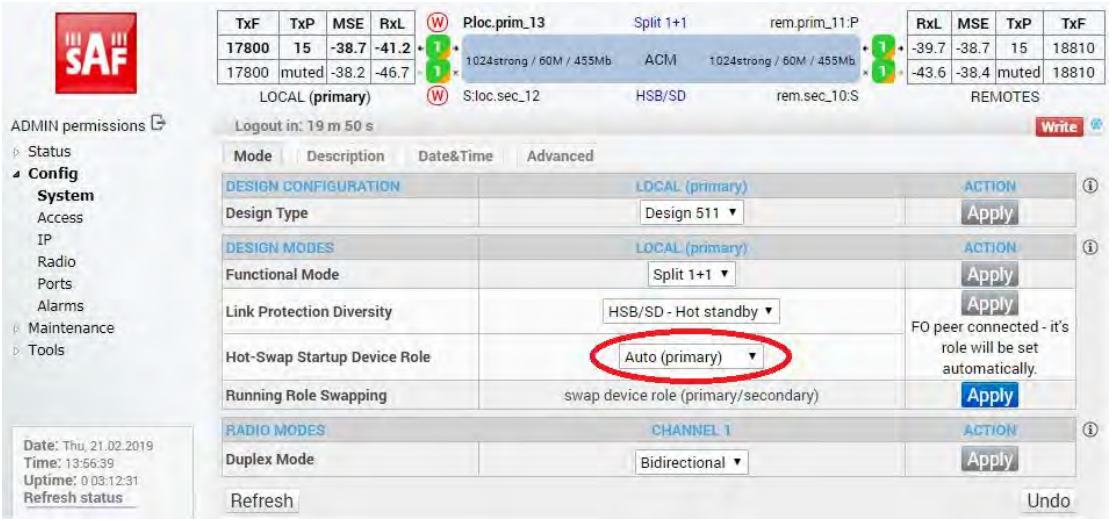


Figure 5.150 *Example of system configuration in Auto mode*

12) 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 scheme

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

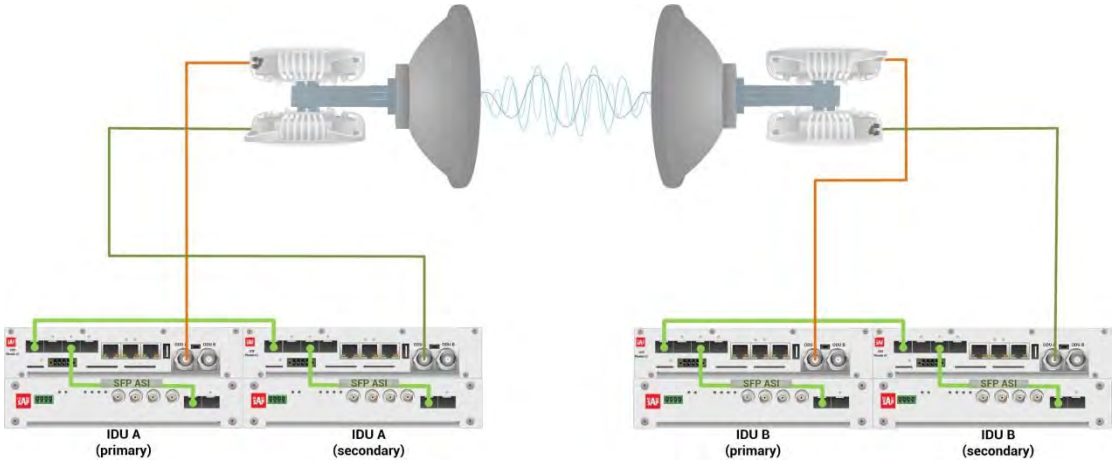


Figure 5.152 *Example of 1+1 FD full protection scheme*

This concrete example describes an application where the Design Type 'Design 511', 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', 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

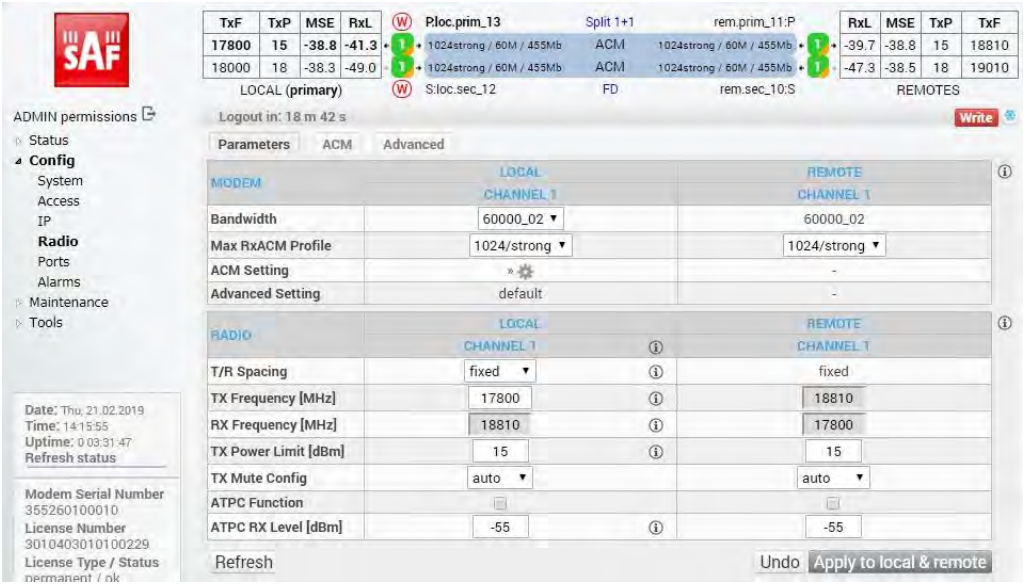


Figure 5.154 *Example of Primary Radio configuration*

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

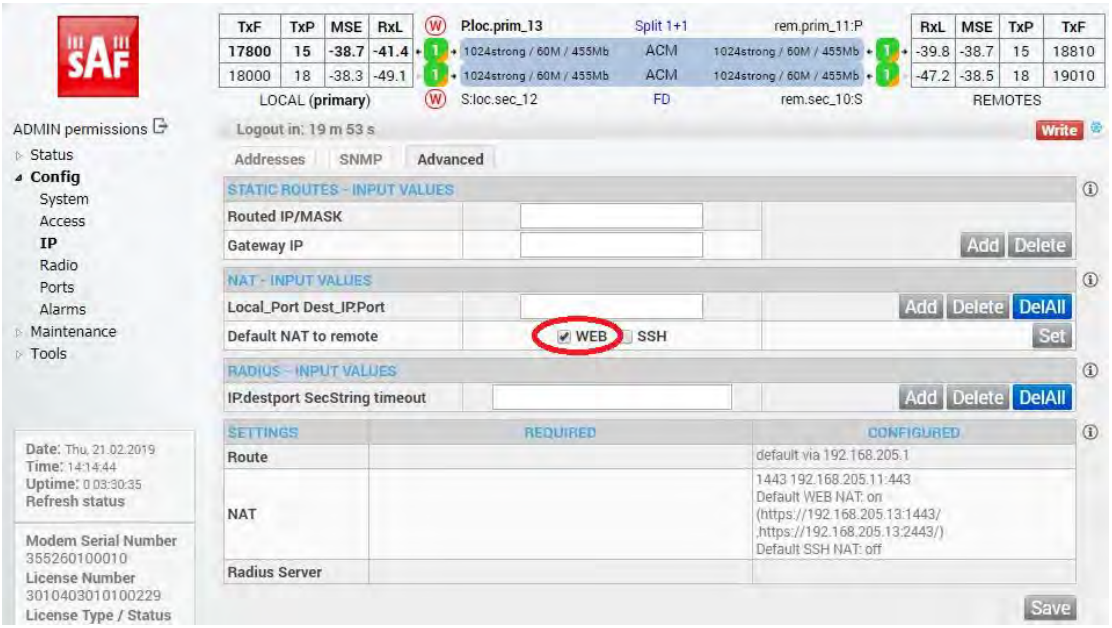


Figure 5.157 *Example of IP NAT configuration*

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'

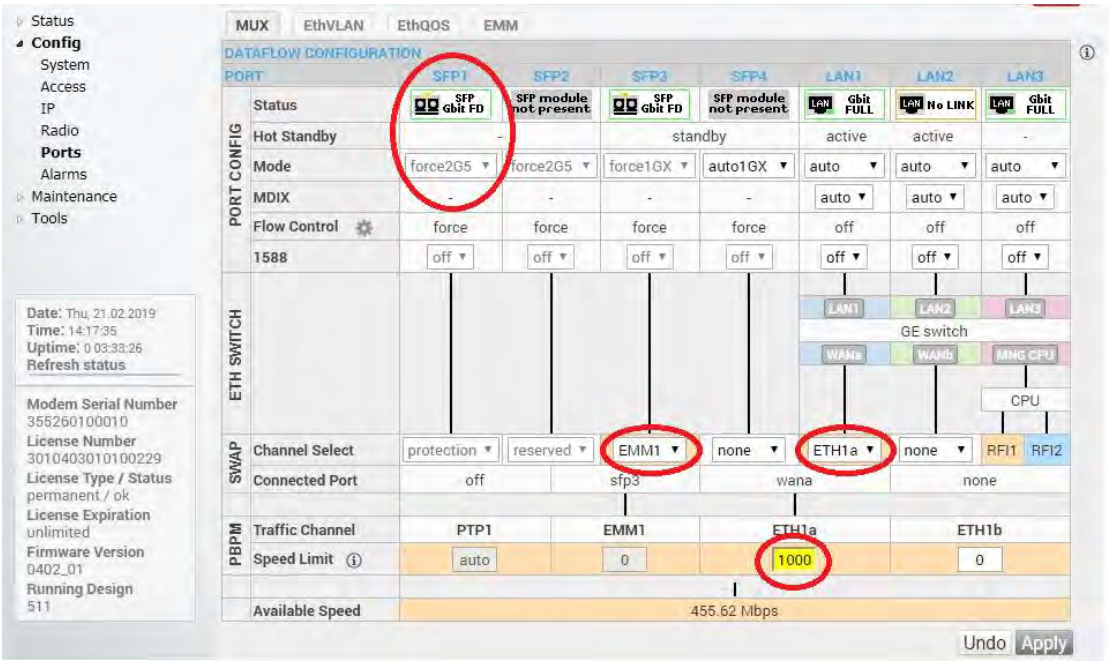


Figure 5.159 *Example of port configuration*

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->Minor' configure interface (LAN, SFP, ASI port) alarms which will be used for protection switchover in all Phoenix G2 IDUs. In the example LAN1, SFP1, SFP3 and ASI Port 1 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

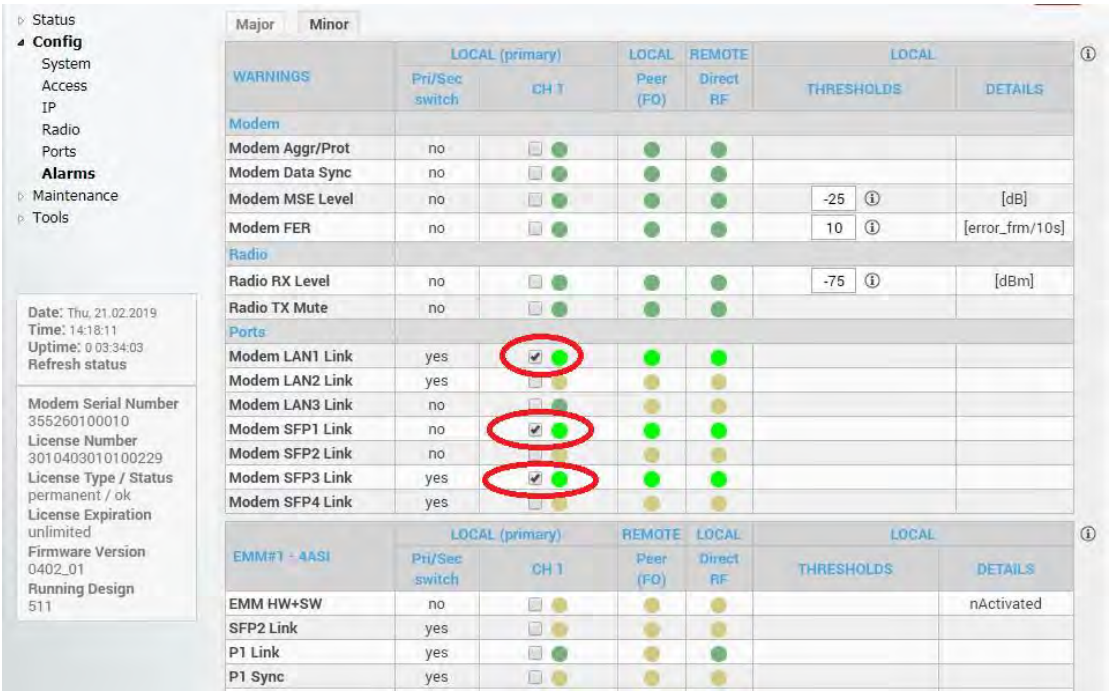


Figure 5.160 *Example of alarm configuration*

9) Save new settings by pressing Write button.
10) Reboot all 4 IDUs after successful reconfiguration
11) 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

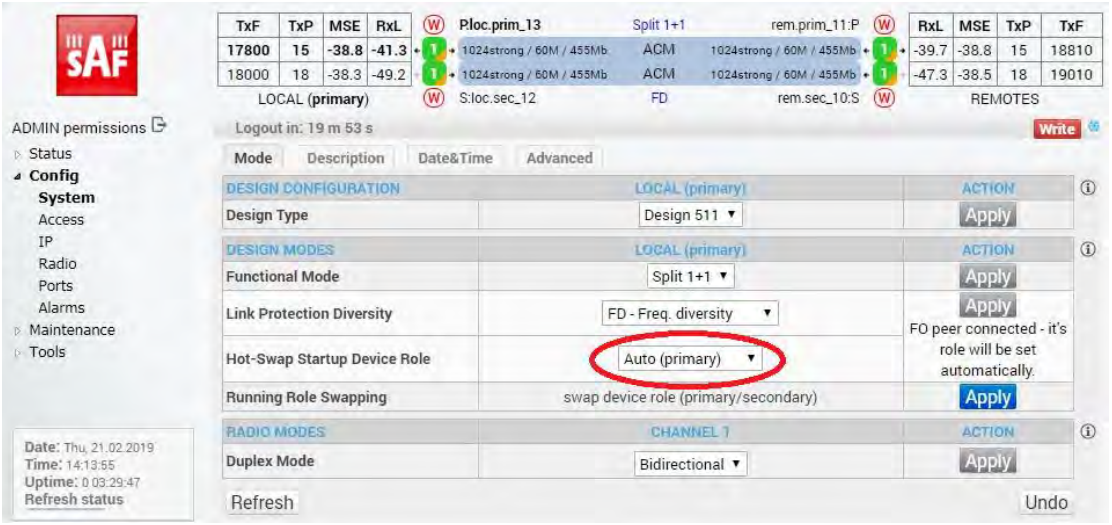


Figure 5.161 *Example of system configuration in Auto mode*

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 – 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:

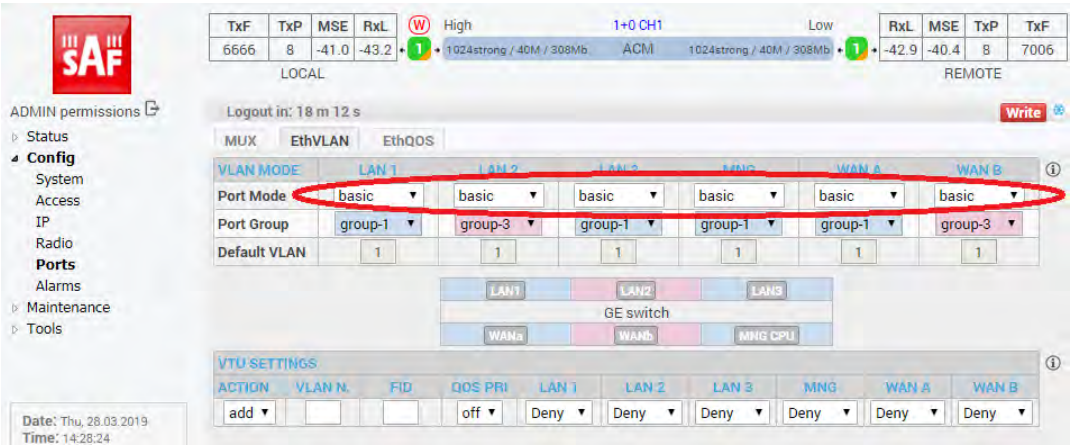


Figure 5.163 *Port mode configuration before VLAN ID configuration*

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:

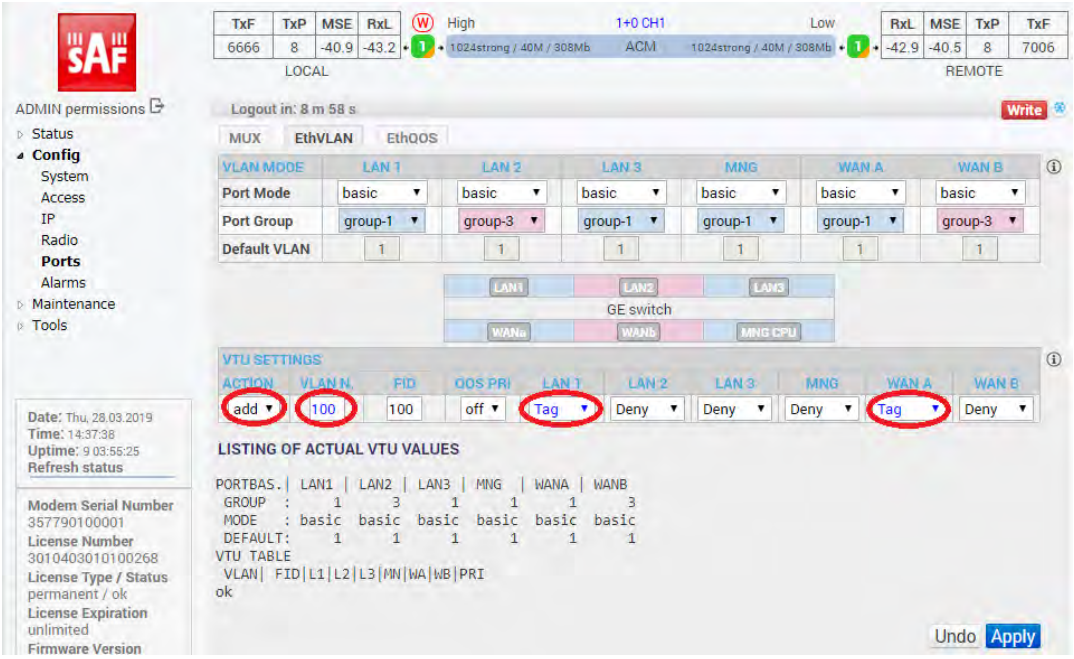


Figure 5.164 *Traffic VLAN configuration*

3) The new applied VLAN ID will be indicated in VTU table:

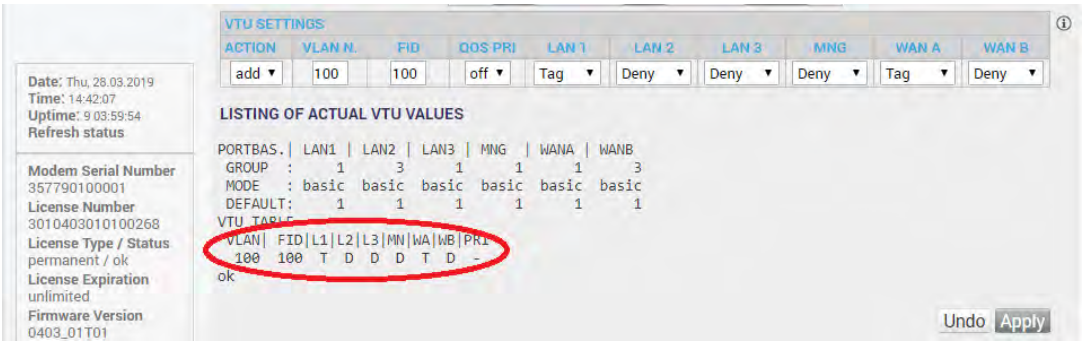
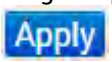


Figure 5.165 *Traffic VLAN configuration*

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 

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:

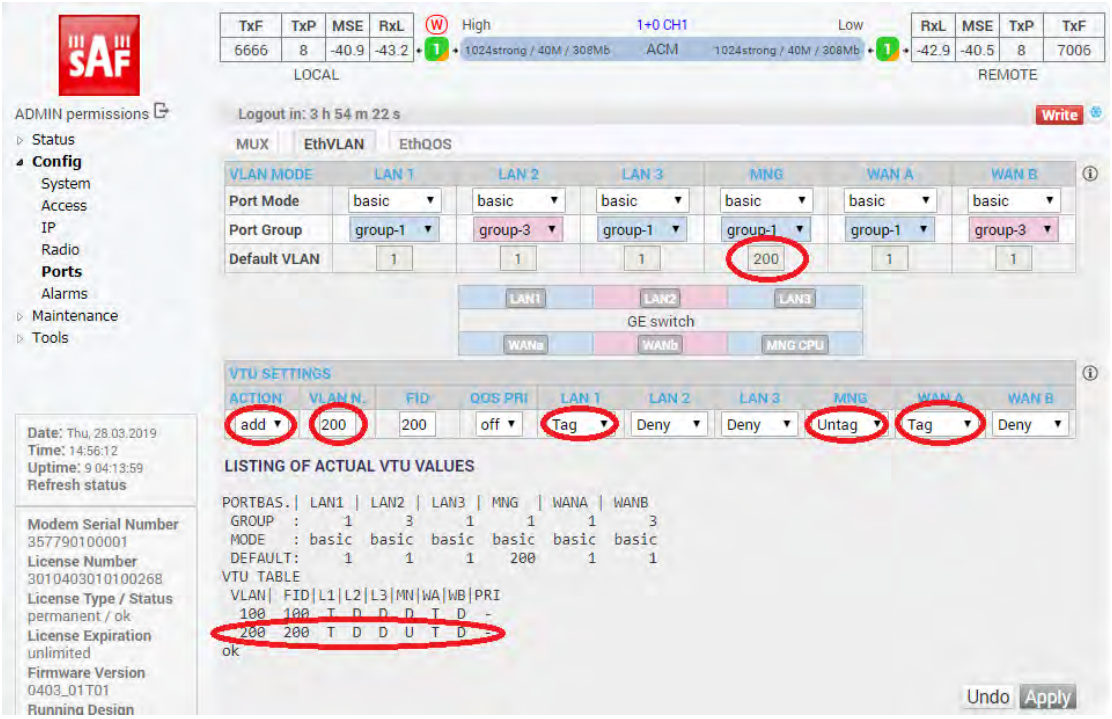


Figure 5.166 *Management VLAN configuration*

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 5.167 *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 successfull VLAN configuration save new settings by pressing Write button.

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
	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