User Manual

IPLink-SM Series

TDM/IP Split Mount System

for

IPL-IDU-E and IPL-IDU-EA Models

Rev 01 - March 2016

Document Disclaimer

The information contained in this manual remains the property of Vislink and may not be used, disclosed or reproduced in any other form whatsoever without the prior written permission of Vislink.

Vislink reserves the right to alter the equipment and specification appertaining to the equipment described in this manual without notification.

This document is supplied on the express terms that it is to be treated as confidential and that it may not be copied, used or disclosed to others for any purpose except as authorized by Vislink.

Trademark Information

Add any additional Trademark content from external companies from their websites trademark pages etc.

Conventions

NOTE: Notes are used to convey additional information.

⚠ Caution: Cautionary notes are given where potential equipment damage could occur.

⚠ Warning: Warnings are shown where there is potential for personal danger or death. This warning should be read and understood before attempting to carry out any work on any equipment attached or related to the equipment in use. The danger is real and not understanding the warning could lead to injury, harm or potential death.

VISLINK Contacts

Vislink A/S technical support can be reached using the following contact information:

Worldwide:

- UKsupport@vislink.com
- +44 (0) 1442 431410
- +44 (0) 1787 226227

Americas:

- USsupport@vislink.com
- +1 978 671 5929
- 888 777 9221

Document History

Revision	Date	Modification
1	March 2016	Initial prototype release of document.

TABLE OF CONTENTS

Table of Figures

Table of Tables

1. BASIC INFORMATION

1.1. Introduction

IPLink-SM is a universal IDU designed for split-architecture high-performance Point-to-Point (P2P) digital microwave links with adjustable data rate from 10 to 730 Mbps (2+0 mode).

It can be connected to VISLINK IPLink-SM ODUs.

The system is designed mainly for network operators interested in IP-based transports and backhaul infrastructures.

Ethernet plus broadcast ASI interface models are also available via an optional E1/T1 expansion chassis.

The IPLink-SM IDU, in combination with its ODU, supports both ETSI and ANSI licensed frequency bands. The IPLink-SM IDU boasts hitless Adaptive Code Modulation (ACM), excellent system-gain and bandwidths for both ETSI and ANSI standard channel plans.

1.2. Safety Information

IPLink-SM complies with the basic requirements of European R&TTE Directive 1999/5/EC Article 3 and meets the requirements contained in the harmonized standards R & TTE, in accordance with article 5 of the directive. IPLink-SM also complies with the basic requirements of FCC rules according to the table below.

Essential Requirements Under Article 3	Harmonized Standards Under Article 5
Article 3.1 (a): Protection of health and safety of users (contained requirements of Directive 73/23/EEC and council recommendation 1999/519/EC)	EN 60950-1 (2006) EN 60950-22 (2006) EN 50 385 (2002)
Article 3.1 (b): Electromagnetic compatibility (contained requirements of Directive 2004/108/EC)	ETSI EN 301 489-1 V 1.6.1(2008) ETSI EN 301 489-4 V1.3.1(2002)
Article 3.2: Requirements for effectively use the frequency spectrum	ETSI EN 302 217-1 V1.2.1 (2007)

Table 1-1 Requirements and Harmonized ETSI standards

Essential requirements	Standards
US FCC limits	System has been tested for compliance with FCC Part 101 and the General requirements of Part 2. The limits for digital devices pursuant to Parts 15.107 and 15.109 Class A have been applied

Table 1-2 Requirements and Harmonized FCC standards

The product complies with the basic requirements for this type of equipment and all of the above technical standards. Operation of equipment is safe under normal conditions of use as set out in this User Guide.

1.3. Warranty Information

Modifying or tampering with any internal components of the IPLink-SM product could cause a malfunction and/or invalidate warranty coverage.

This page is intentionally unused.

2. TECHNICAL DESCRIPTION

The digital IPLink-SM microwave system has a split-mount configuration design, with an architecture intended for use as a rack mounted indoor unit (IDU) and tower mounted RF outdoor unit (ODU).

A universal IDU hardware version is available with bandwidths up to 60 MHz at applicable maximum RF power outputs.

The indoor unit (IPLink-SM IDU) is universal with respect to ETSI and ANSI channel bandwidth standards and is universal for all available frequency bands, its configuration then depends on the loaded software license key. The outdoor units are unique for each frequency band and sub-band.

2.1. System Description

Signals received by the parabolic antenna are interconnected via a waveguide adapter to the receiving filter in the outdoor unit (ODU). The task of the ODU is to convert the frequency of the received/transmitted signals to/from the IF. The resulting converted signal, together with the management channel, is carried via the coaxial cable to the IPLink-SM indoor unit (IDU). The signal is demodulated inside the IDU, followed by the recovered user and management data intended for communication with the ODU.

User Ethernet data is either connected to/from the Gigabit Ethernet ports or to an optional expansion chassis by means of SFP modules. Data transmissions are processed in a similar manner, but in a reverse order.

The IPLink-SM system is technically characterized by the following basic features:

- Standard licensed ETSI and ANSI frequency bands
- Modulation schemes:
  - QPSK, 8 PSK, 16/32/64/128/256 QAM
- Channel bandwidth:
  - ETSI standards 7/14/27.5/28/40 and 56 MHz
  - ANSI standards 10/20/25/30/40/50 and 60 MHz
- LDPC based Forward Error Correction.
- Hitless Adaptive modulation (ACM)
- Four basic design modes (SW setting / License Key):
  - SINGLE – one data stream over air
  - MULTI – up to four independent data streams over air
  - AGGREGATE – 2+0 configuration with true capacity doubling
  - PROTECTED – 1+0 configuration in HSB/SD/FD modification
- Two functional options (SW setting / License Key):
  - AES128, AES256 – AES encryption for high system security
  - PTP1588 – option which ensure IEEE1588 support
- Integrated traffic ports:

  - 3x Gigabit Ethernet ports (10/100/1000Base-T) for user data traffic and/or management access
  - 2x SFP slots for additional GIGE port extension, EMM module connection or IDU interconnection (protection, aggregation)
- Integrated management ports:
  - USB-B – for separate IP management access
  - USB-A – configuration restoration and backup by means of USB Flash memory
- SyncE support in each design mode
- Integrated data verification system of received corrupted packets (CRC)
- Integrated BER tester and measurement of the nature of received signal (MSE, modulation diagram of received data)
- ATPC function support (Automatic Transmit Power Control)
- Integrated spectral analyzer for the detection of the free channel, or alternatively for detection of interference with the particular band
- Unified standard management IP access – TELNET, HTTP, SNMP v.2c
- Secure management IP access - SSH, HTTPS, SNMP v.3

2.2. Indoor Unit (IDU)

The IPLink-SM Indoor Unit (IDU) multiplexes data for wireless transmission over an RF carrier, utilizing a digital modem that controls the system. The IDU's functionality is simple to configure using software. The core of the unit is a DSP module that generates an intermediate frequency output for the outdoor unit and then processes a returned intermediate frequency generated by the outdoor unit.

The indoor unit is fitted with three 1000Base-T (RJ45) user ports, one port can be reserved for either an individual management connection or as a standard user port. Two SFP slots are intended for additional Gigabit Ethernet connections or for 1+1 or 2+0 configuration IDU to IDU interconnections or for EMM Expansion chassis port extensions.

The IDU USB-B port is available for independent connection management, a second USB port (USB-A) is reserved for flash memory sticks for items such as configuration backup, logs etc.

The management system is based on the IP protocol. The outdoor units (ODU) management is integrated directly into the command set of the indoor unit (IDU) and is an integral part of this unit's software.

The management system base is configurable to utilize one of the following:

- Character-oriented IP access (TELNET, SSH)
- Web based GUI (HTTP, HTTPs)
- SNMP based system management

The IDU unit takes power with a nominal voltage of -48 VDC and a GND must be connected to the positive pole.

2.3. Indoor Unit Front Panel Overview

2.3.1. Front Panel IDU Connectors

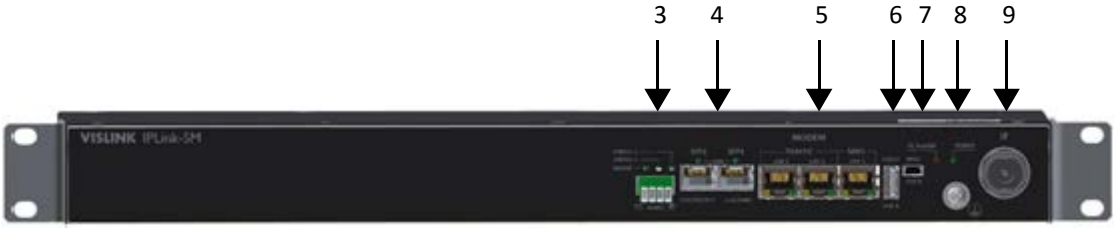

Figure 2-1 Indoor Unit Front Panel IPL-IDU-E Overview

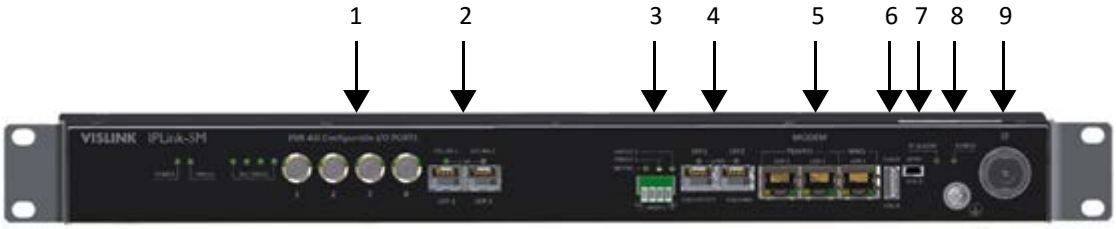

Figure 2-2 Indoor Unit Front Panel Overview IPL-IDU-EA Overview

No.	ID	Function
1	DVB ASI	Four configurable I/O DVB-ASI ports (75 Ohm).
2	SFP 1 UPLINK1	Master SFP port reserved for connection to IDU or to master Expansion module card in Expansion module chain. SFP 2 UPLINK2 – slave SFP port reserved for connection to slave EMM card in Expansion module chain or to relay IDU in add/drop configuration.
3	-48 VDC	Power supply connector, + pole is grounded inside the device.
4	SFP 1 GIGE/PROTECT	User port for alternative Gigabit Ethernet connection or IDU interconnection in case of protected or aggregate design selection. SFP 2 GIGE/EMM – user port for alternative Gigabit Ethernet connection or EMM module connection.
5	TRAFFIC LAN 1/2	Gigabit Ethernet user ports for Ethernet connection. MNG LAN 3 – by default it is reserved for management access (out of band management), but can be configured also for user data traffic.
6	FLASH USB A	USB interface for connecting USB memory.
7	MNG USB B	USB interface for an alternative IP access.
8	Ground Connector	Ground connector.
9	IF	ODU – N connector for connecting ODU over coaxial cable (IF connection).

Table 2-1 Front Panel Connector and LED Identifiers

2.3.2. Front Panel IDU LEDs

2.3.2.1. LED Indicators on the IDU Front Panel – System Status:

- SYNC – indication of modem synchronization (digital modem)
  - Lights – synchronization OK
  - No light – loss of synchronization
- LOCAL STATUS – indication of the LOCAL device status
  - Lights – status OK
  - Flashes – status WARNING
  - No light – status UNKNOWN
- REMOTE STATUS – indication of the REMOTE device status
  - Lights – status OK
  - Flashes – status WARNING
  - No light – no communication with remote device or UNKNOWN status
- ODU STATUS – indication of the ODU status
  - Lights – status OK
  - Flashes – communication problem (ODU is not responding)
- POWER – indication that IDU is under power
  - Lights – power ON
  - No light – power OFF

2.3.2.2. LED indicators on the IDU front panel – ports status:

- SFP 1/2 LINK – indication of presented signal at SFP port
  - Lights – signal detected and synchronized
  - Flashes – incorrect result from auto-detection process
  - No light – no correct signal detected
- LAN 1/2/3 GIGE DETECT – indication of Gigabit ETH mode on appropriate port
  - Lights – GIGE mode ON
  - No light – no GIGE mode detected
- LAN 1/2/3 LINK/ACT – indication of link and data activity on appropriate ETH port
  - Lights – Ethernet link detected
  - Flashes – data activity (Rx/Tx) at appropriate port
  - No light – no Ethernet link

2.4. Functional Block Diagram Examples

2.4.1. IPLink-SM Indoor Unit (IDU)

Figure 2-3 shows a functional block diagram for the IPL-IDU-E Indoor unit.

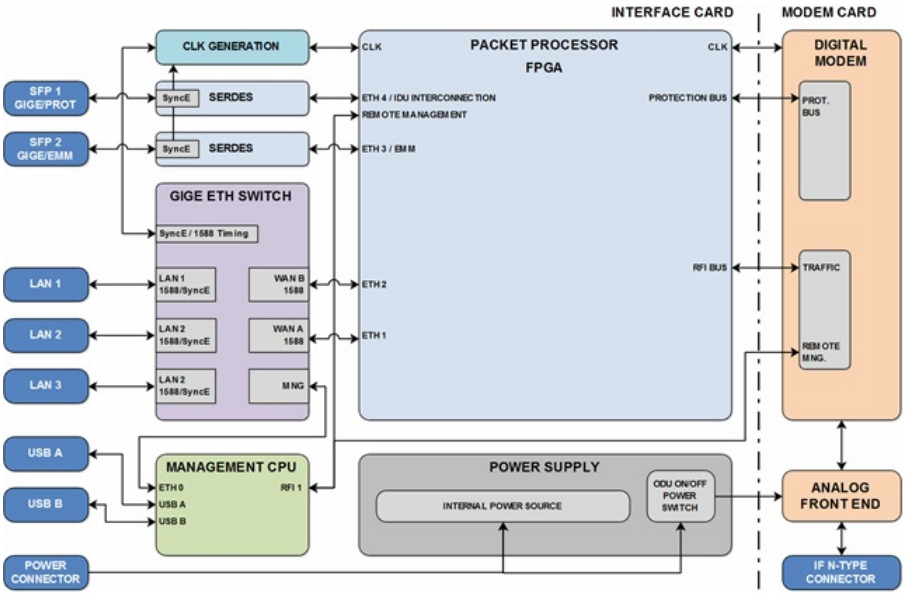

Figure 2-3 IPL-IDU-E Indoor Unit Block Diagram

The IPLink-SM IDU consists of two main boards:

- The Interface Card performs the function of a data interface, packet processor and management unit.
- The Modem Card performs the function of digital modem (DSP) and analogue modem (analogue front end with mixers and filters).

Data is first processed by an integrated six-port Gigabit Ethernet switch, two WAN ports of this switch are interfaced into a universal Packet Processor (PBPS – Priority Based Packet System). SFP interfaces are also directly interfaced into a universal Packet Processor. The function of the Packet Processor depends on the configuration selected. The digital modem then adds synchronization marks and FEC to the data stream creating a digitally modulated signal. The signal is passed to the analogue block for signal processing.

All internal connections are via a high-speed bus and controlled via the CPU. The CPU block is also accessible via management interfaces and allows you to perform all the settings both locally and remotely trough the IP interface in the IPLink-SM IDU.

The Packet Processor uses a priority scheme. The scheme prioritizes traffic processing on port ETH 4. This prioritization is reduced as you move towards port ETH 1. However, Packet Processor prioritization is design dependent and user configurable.

2.4.2. Single Transmission Configuration

Figure 2-4 shows the unit configured for a SINGLE transmission mode. This mode transmits a single transmission data stream over the air. IPLink-SM IDU is configured to this mode by means of IDU management. The Packet Processor function is also shown.

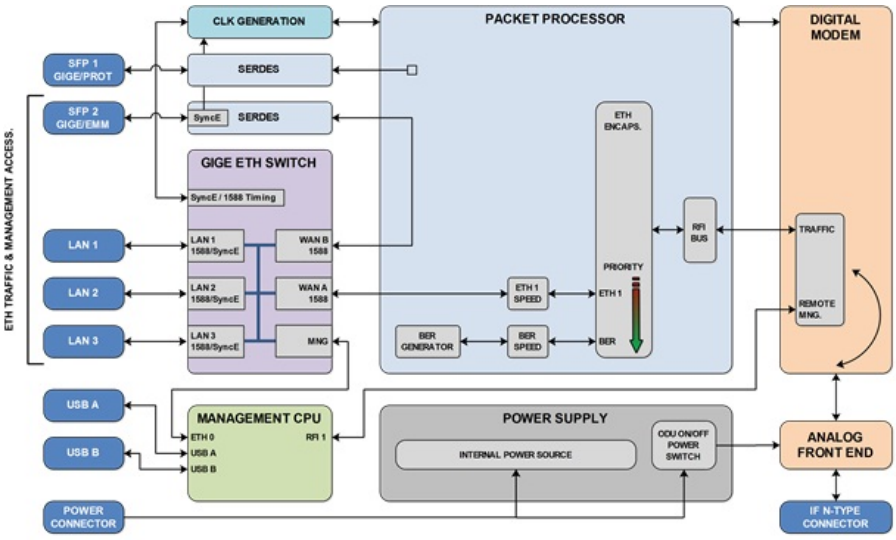

Figure 2-4 Single Transmission Mode Block Diagram

The Ethernet Switch is configured into a mode where the WAN port “WAN A” is connected to the Packet Processor and a second WAN port “WAN B” is connected to SFP 2 port. The SFP 1 port is not used in this mode. The Packet Processor uses basic Ethernet stream encapsulation in combination with a BER stream, which is transferred in time when Ethernet frames are not available.

Main Advantage:

- Highest data throughput, because Ethernet traffic is coded by basic encapsulation process with the lowest data overhead.

Disadvantage:

- The packet processor doesn't generate its own priority packets, so any data stream errors are only detected by means of an Ethernet Frame's CRC inside the Ethernet Switch. Due to the missing priority packet layer, you cannot use some options, such as AES.

2.4.3. Multi Transmission Configuration

Figure 2-5 shows the unit configured for MULTI transmissions. The configuration allows for up to four independent data streams over the air. IPLink-SM multi-mode is configured via IDU management. The Packet Processor function is also shown.

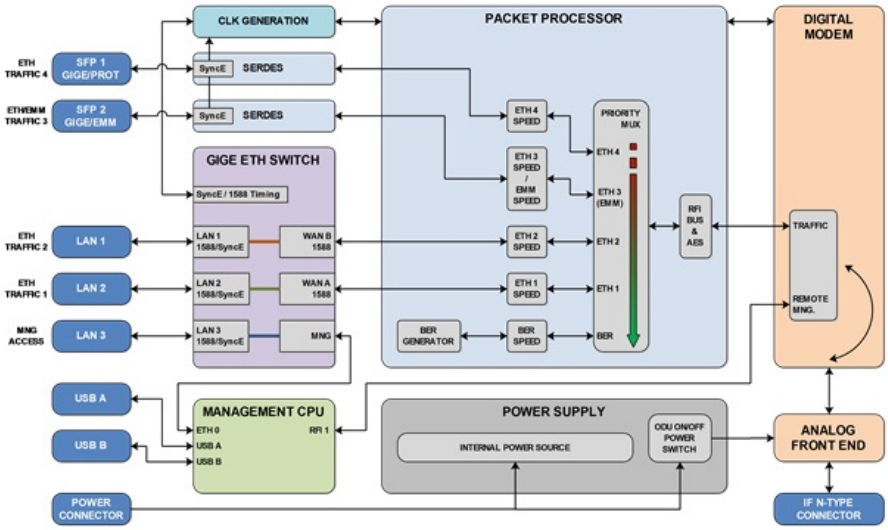

Figure 2-5 Multi-Transmission Block Diagram

The Ethernet Switch is configured into mode where both WAN ports WAN A/B are connected to Packet Processor. Ports SFP 1 and SFP 2 are connected directly to Packet Processor as well and are transparent for Ethernet traffic (Flow Control function must be activated on connected Ethernet equipment). Packet Processor uses Priority based process for independent streams transport over air. BER stream is additionally added, when throughput capacity over modem is higher than allocated throughput over Packet Processor. Additional AES encryption can be inserted in front of modem processing.

Main Advantages:

- Up to four independent data streams over air.

Disadvantages:

- Slightly lower throughput compared to the SINGLE configuration/design when just one traffic stream is configured at the IDU.

2.4.4. Protected Configuration

Figure 2-6 shows the unit configured in PROTECTED mode. The Protected configuration is a 1+1 system configuration when protection (hitless in specific conditions) is required.

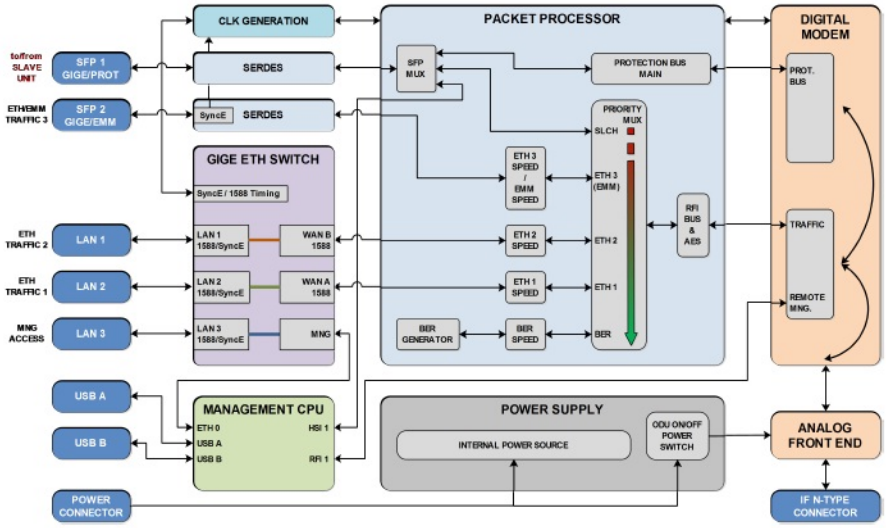

Figure 2-6 Protected Mode Block Diagram (Master Mode)

The Ethernet Switch is configured so both WAN ports WAN A/B are connected to the Packet Processor. WAN ports WAN A/B are grouped inside the Ethernet switch with the appropriate LAN ports (LAN 2/1). Port SFP 2 is also connected to the Packet Processor and is transparent to Ethernet traffic (the Flow Control function must be activated on any connected Ethernet equipment) or for the EMM module data stream from a connected external EMM. Port SFP 1 is reserved for a second IDU (Master – Slave) interconnection.

NOTE: It is highly recommended to use port LAN 3 as out-of-band management access port.

The Packet Processor uses a Priority based process for independent stream(s) transport over the air. The BER stream is added when the throughput capacity over the modem is higher than the allocated capacity for the user ports over the Packet Processor. Additional AES encryption can be inserted before modem processing. Protection is provided via the Modem Card.

Figure 2-7 shows the Packet Processor function for a Slave Unit.

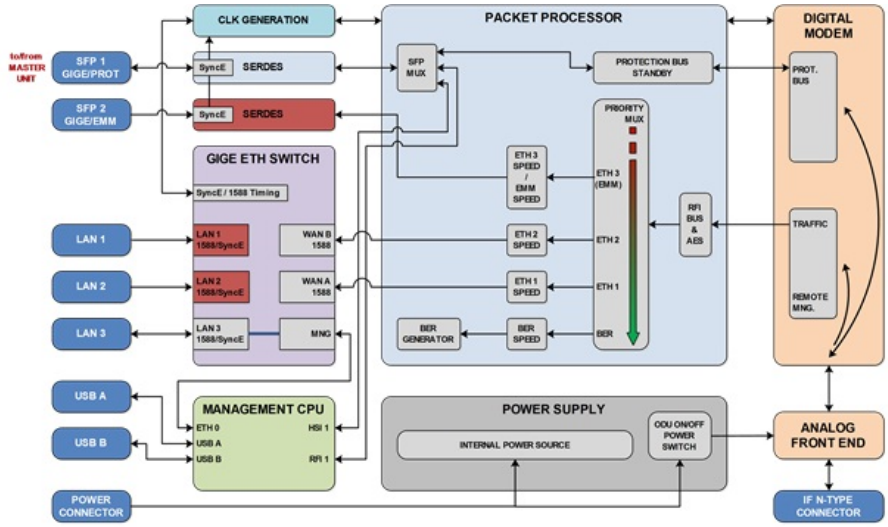

Figure 2-7 Protected Mode Block Diagram (Slave Mode)

The user data ports LAN 1/2, SFP 2 are deactivated (don't transmit data from IDU). Port SFP 1 is reserved for the first IDU (Master – Slave) interconnection.

NOTE: It is highly recommended to use port LAN 3 as out-of-band management access port.

The Packet Processor functionality is limited to receiving direction only, its function is not important for system functionality, because a complete data stream is copied from the protection bus (SFP 1) directly into the digital modem. The Packet Processor adds management channels into the Fiber Optic high speed stream. Protection is provided via the Modem Card.

Main Advantages:

- 1+1 protection in all modes HSB, SD, FD also with interface redundancy.

Disadvantages:

- Two units must be used for protection mode.

2.4.5. Aggregate Configuration

Figure 2-8 shows the AGGREGATE configuration which is a true 2+0 system configuration (capacity doubling) when ETH traffic aggregation is required.

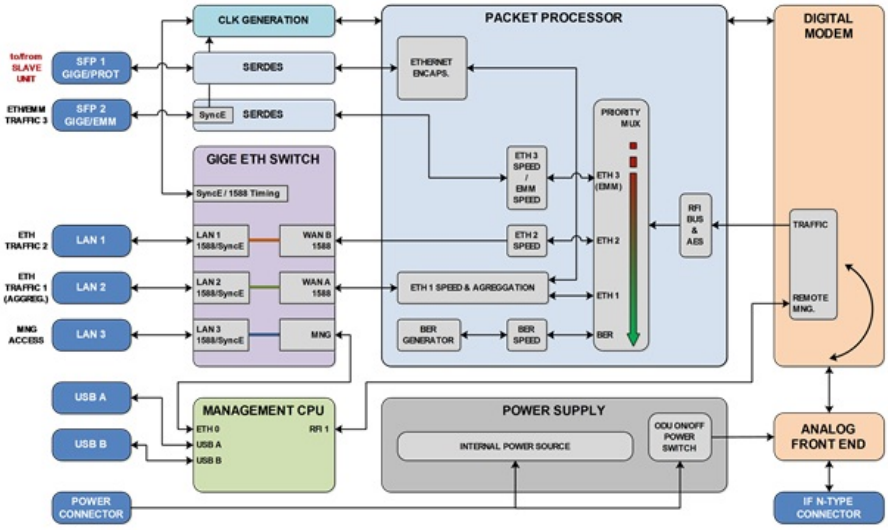

Figure 2-8 Aggregate Configuration Block Diagram (Master Mode)

The Ethernet Switch is configured into a mode where both WAN ports WAN A/B are connected to the Packet Processor. WAN ports WAN A/B are grouped inside the Ethernet switch with the appropriate LAN ports (LAN 2/1). Port SFP 2 is also connected to the Packet Processor and is transparent to Ethernet traffic (Flow Control function must be activated on connected Ethernet equipment) or for EMM module data stream from a connected external EMM. Port SFP 1 is reserved for the second IDU (Master – Slave) interconnection. Only Ethernet traffic connected to the internal channel ETH 1 can be aggregated with the traffic of the Slave Unit. This mode is still combined with any transmission of more traffic channels over the air.

NOTE: It is strictly recommended to use port LAN 3 as out-of-band management access port.

The Packet Processor uses a Priority based process for independent streams transport over the air. The BER stream is added when the throughput capacity over the modem is higher than the allocated capacity for the user ports over the Packet Processor. Additional AES encryption can be inserted before modem processing. Aggregation is provided by an Aggregation Block inside the Packet Processor.

Figure 2-9 shows the Packet Processor function for the Slave Unit.

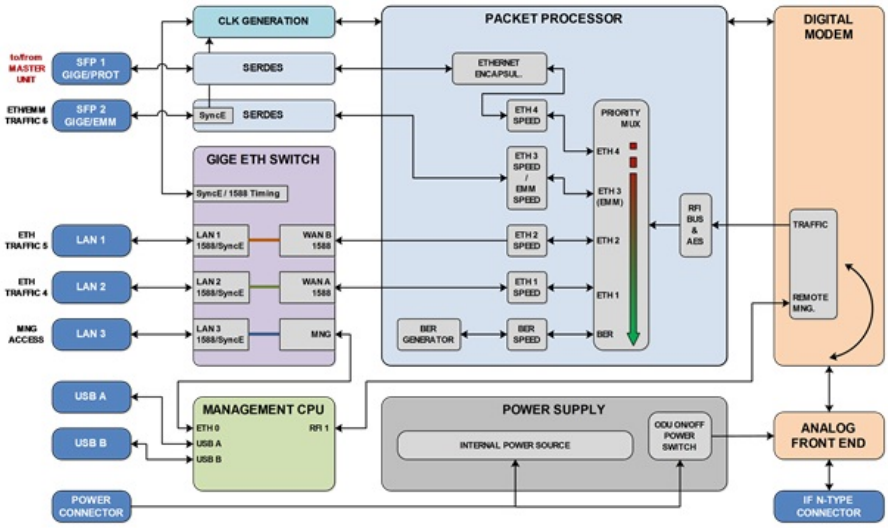

Figure 2-9 Aggregate Configuration Block Diagram (Slave Mode)

The Ethernet Switch is configured into a mode where both WAN ports WAN A/B are connected to the Packet Processor. WAN ports WAN A/B are grouped inside the Ethernet switch with the appropriate LAN ports (LAN 2/1). The Port SFP 2 is also connected to the Packet Processor and is transparent to Ethernet traffic (Flow Control function must be activated on the connected Ethernet equipment) or for EMM module data stream from the connected external EMM. The Port SFP 1 is reserved for the first IDU (Master – Slave) interconnection. Traffic connected to the internal port ETH 4 is an aggregate stream from the Master Unit and is transported with the highest priority.

Note: It is strictly recommended to use port LAN 3 as out-of-band management access port.

The Packet Processor still uses a Priority based process for independent streams transport over the air. The BER stream is added when throughput capacity over the modem is higher than the allocated capacity for user ports over the Packet Processor. Additional AES encryption can be inserted in before modem processing.

Main Advantages:

- True 2+0 aggregation, two links with different speeds can be used for Ethernet traffic capacity aggregation. This mode can be used as an alternative to protected mode, when one Ethernet channel is used (not hitless).

Disadvantages:

- Two units must be used for aggregate mode.

2.4.6. IDU Block Scheme in Terms of IP

Figure 2-10 depicts a simplified block diagram of the IPLink-SM IDU in terms of IP management.

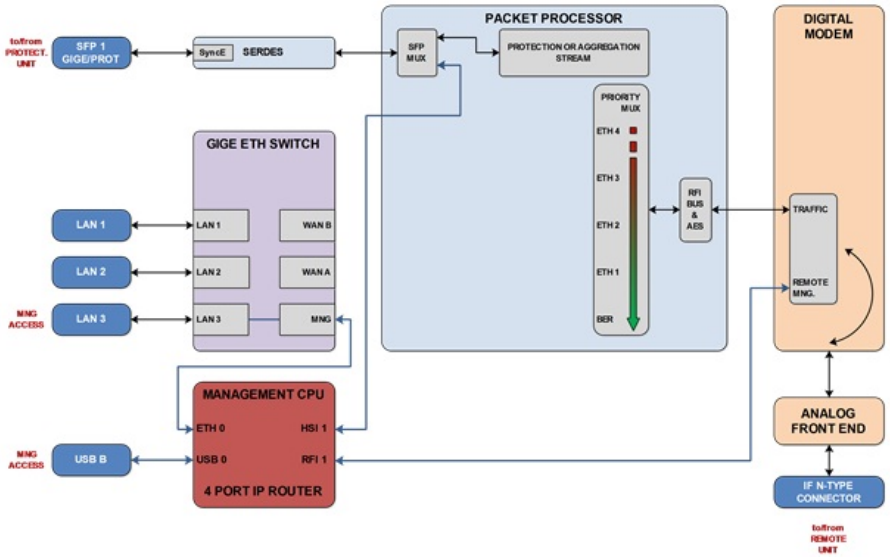

Figure 2-10 IP Management Scheme Block Diagram

The processor performs the function of an IP router. The individual IP frames routing is based on standard routing rules, in this case on static routing.

2.4.6.1. Four IP ports enter the processor (MANAGEMENT CPU)

- **ETH 0** – Ethernet port of the CPU with its own MAC address and all the standard features of an Ethernet interface. Primary / Secondary addresses and appropriate subnet masks are assigned to this interface.
- **RFI 1** – ppp (point-to-point) type of interface which interconnects local CPU with the remote side CPU accessible through the separate channel inside air-frame.
- **HSI 1** – ppp (point-to-point) type of interface which interconnects local CPU with the protection unit CPU or IPLink-SM EXP module accessible through the separate channel inside Fiber Optic-frame.
- **USB 0** – USB port which is reserved for local IP access.

Each device supports the following basic IP settings:

- **The primary IP address, including the mask** – In basic configuration, this address is identical to the ports ETH 0, RFI 1 and HSI 1 (ppp unnumbered mode), the mask indicates the range of addresses connected directly to the ETH 0 interface.
- **The address of the remote radio unit (rrfi1)** – This address is automatically assigned a static route of the remote device connected via port RFI 1 (microwave connection).
- **The address of protection unit (rhsi1)** –this address is automatically assigned together with a static route to the protection unit connected via port HSI 1 (Fiber Optic Connection).
- **Default gateway** – the address from the assigned subnet. This is used for routing frames with a different IP address than the range of IP addresses included in the routing table.

Each device supports also the following advanced IP settings

- **The secondary IP address, including the mask** – the address is assigned to the port ETH 0, the mask indicates the range of addresses connected directly to the ETH 0 interface. When no conflict with address range 10.10.10.0/24 exists, there is not necessary to change this address.
- **The USB IP address, including the mask** – this address is assigned to the port USB 0, the mask indicates the range of addresses connected directly to such interface. When no conflict with address range 10.10.11.0/24 exists, there is not necessary to change this address.
- **The RFI1 port IP address** – it is possible to set specific IP address for internal ppp port and change ppp mode from unnumbered to numbered one.
- **The HSI1 port IP address** – it is possible to set specific IP address for internal ppp port and change ppp mode from unnumbered to numbered one.
- **The File Transfer specification** – this setting specifies file transfer destination. Local USB A port can be selected (default) or FTP server by means of FTP IP specification can be used either for firmware update from CLI or for log files storage.
- **The Remote Time Server** – this setting selects whether remote time server is used for time synchronization. NTP or RDATE type can be selected for this function, appropriate IP address of selected server must be entered.
- **Static routes** – the user can define additional static routes as well.
- **NAT** – possibility of the address translation according to the rules in the NAT table.

All above explained parameters have an influence on the type of management access either directly on the managed unit or on the whole microwave network.

2.5. Outdoor Unit (ODU)

The Outdoor microwave unit part for the IPLink-SM system is available for a full range of standard licensed frequency bands and specific unlicensed bands.

Microwave link IPLink-SM point-to-point units (in the basic configuration 1+0) consists of two Outdoor Radio Units (ODU). The ODU performs the up-conversion of the IF frequency from the IDU (@ 350 MHz) to the desired transmission band.

The ODU also performs the down-conversion from the received frequency band to the IDU IF frequency (@ 140 MHz) for the receiving part of the IDU. The coaxial cables that connects the IDU and ODU supplies power to the ODU as well access to configure it. Configuration management is done via the software GUI from the Indoor Unit. Management of the ODU is integrated directly in the command set of the Indoor Unit and it is an integral part of the IDU software.

For an easy primary setting of the optimal received signal level, the ODU is fitted with a BNC connector where the measured DC voltage [mV] is kept directly proportional to the level of Received Signal Strength (RSSI).

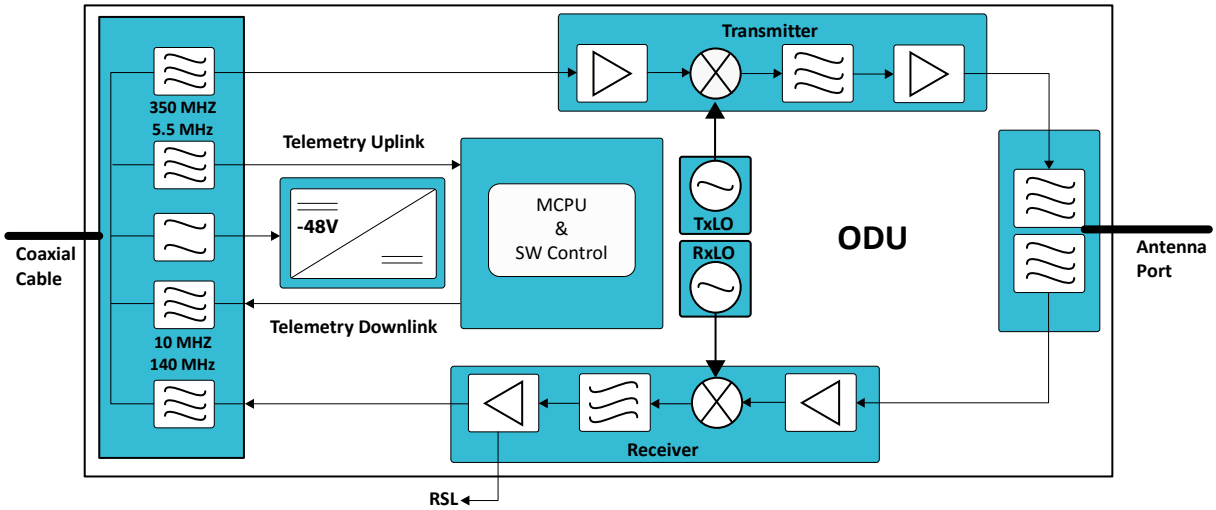

Figure 2-11 Outdoor Unit (ODU) Block diagram

The outdoor unit is an integral part of the antenna system. The ODU is mounted behind the parabolic antenna. Different antennas are available on request, with diameters of:

- 1ft. (30cm)
- 2ft. (60cm)
- 3ft. (90cm)
- 4ft. (120cm)
- 6ft. (180cm)

2.5.1. ODU for Licensed Frequency Bands

A licensed outdoor unit operates in frequency bands that meet the international standards and requirements for this type of equipment (especially ETSI EN 302 217). The modulation scheme is adjustable from QPSK to 256 QAM, with output power range between 0 to 30 dBm, depending on the selected frequency band and the type of modulation scheme. A maximum transmission date rate is 365 Mbps in 1+0 mode.

For technical reasons, each frequency band is covered by more (three or four) pairs of microwave units, where one pair is tunable in the low portion of the band (in low sub-band), the second/third pair in the middle portion of the band (in middle sub-band) and the last pair in the high portion of the band (in high sub-band). Each pair then consists of two radio units (ODU), where one unit transmits in the upper part and the second unit in the bottom part of the given sub-band, the frequency separation is then known as the duplex spacing (Tx/Rx).

The ODU operating in the lower part of a particular sub-band of a given frequency, can only work with an ODU tunable to the higher part of the same sub-band of the same frequency.

There are two connectors on the ODU in conjunction with a grounding terminal:

- N connector for connecting with the IDU via coaxial cable
- BNC connector for measurement of Received Signal Strength (RSSI)

Figure 2-12 Outdoor Unit Overview

The antenna is secured to the ODU using the integrated waveguide transition (Microwave adapter) using the four flexible clips.

2.6. External Multiplexer Modules

The basic functionality of the External Multiplexer Modules is multiplexing of specific data types (E1, T1, ASI) into one high speed data stream, which is then transported over the Fiber Optic interface (SFP2) to a connected IDU. The coded data stream is muxed with other data sources (ETH channels) inside IDU and transmitted to the remote IDU and any appropriate remote External Multiplexer Module(s). Up to four External Multiplexer Modules can be connected in series to one IDU.

The management of all External Multiplexer Modules is integrated inside the IDU management system, therefore the configuration of all External Multiplexer Module parameters is similar to IDU configuration.

The External Multiplexer Module unit must be connected to the power supply with a nominal voltage of -48 VDC and GND must be connected to the positive pole.

2.7. Expansion Module IPL-IDU-E1T1-EXP

The IPL-IDU-E1T1-EXP (External Multiplexer Module) provides E1/T1 extensions for Indoor Units. The IPL-IDU-E1T1-EXP module enables multiplexing for up to 16 E1/T1 circuits. The multiplexer features a basic unit with 16 x E1/T1 built-in ports and 2 x SFP 1000Base-SX ports. The compact, simple to configure and easily scalable design can provide a solution for up to 64 x E1/T1 circuits or enables cascading with other extension devices for the IPLink-SM (e.g. IPL-IDU-ASI-EXP, IPL-IDU-E1T1-EXP). The units are configured using the IDU software GUI (e.g. set-up of basic mode E1/T1, add/drop multiplexer, backup). The actual overall capacity for TDM is allocated in the Priority Base Packet System (PBPS), based on the selected E1/T1 ports configured in the software GUI for the IDU.

Priority Base Packet System (PBPS) is proprietary multiplexer system.

2.7.1. Expansion Module Connections

Figure 2-13 Expansion Module IPL-IDU-E1T1-EXP Overview

NOTE: shows the expansion module for “IPL-IDU-E” & “IPL-IDU-EA” models.

ID	Function
1	**E1/T1 PORTS –** RJ-45 connectors for G.703 signals connection (by default unbalanced)
2	**SFP 1 UPLINK1 –** master SFP port reserved for connection to IDU or to master Expansion module card in Expansion module chain
3	**SFP 2 UPLINK2 –** slave SFP port reserved for connection to slave Expansion module card in Expansion module chain or to relay IDU in add/drop configuration
4	Grounding connector

Table 2-2 Expansion Module

2.7.2. Connectors on the Expansion module IPL-IDU-E1T1-EXP front panel

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

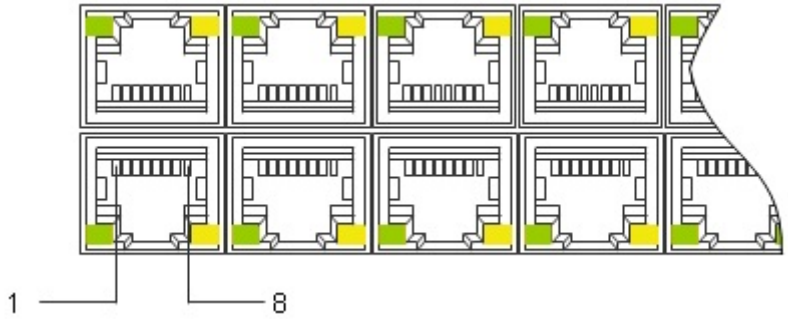

Figure 2-14 Expansion Module IPL-IDU-E1T1-EXP Overview

Pin	Signal
1	Rx-
2	Rx+
4	Tx-
5	Tx+

Table 2-3 RJ45 Pin Out Connector Detail

NOTE: All the ports are protected against ESD (electrostatic discharge), CDE (Cable Discharge Events), and lightning.

If connecting a 16E1 balanced RJ45 interface to an unbalanced BNC E1 interface, then the cable-in must be used:

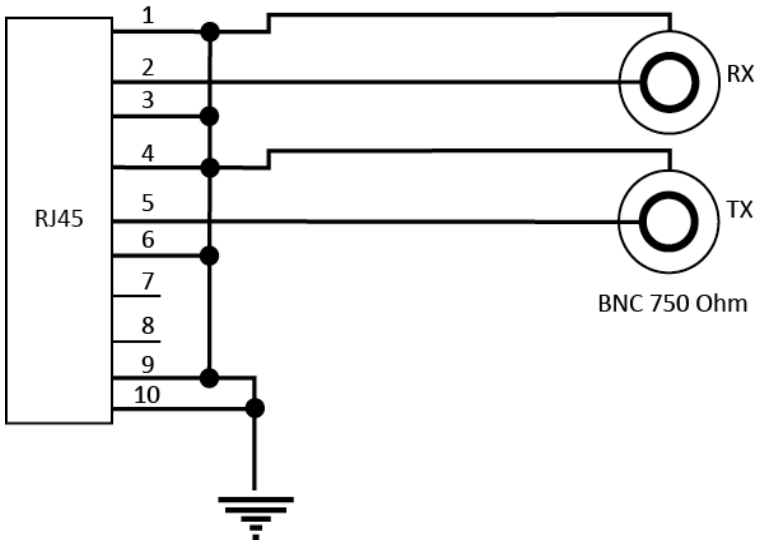

Figure 2-15 RJ45 to BNC E1 Connection Overview

Pinout for this cable is as follows:

Pin	Signal
1	Rx Ring
2	Rx Tip
3	GND (over 0805 0R resistor)
4	Tx Ring
5	Tx Tip
6	GND (over 0805 0R resistor)
7	NC
8	NC
9	GND (over 0805 0R resistor)
10	GND (over 0805 0R resistor)

Table 2-4 RJ45 to BNC E1 Connector Detail

2.7.3. LED indicators on the IPL-IDU-E1T1-EXP – System Status

- **STATUS** – indication of the LOCAL Expansion module status
  - Lights – status OK (card enabled, proper communication with IDU)
  - Flashes – status WARNING (card is not enabled in the system or no communication with IDU)
  - No light – status ERROR (a firmware is not loaded into Expansion module HW)
- **POWER** – indication that EMM is under power (green LED)
  - Lights – power ON
  - No light – power OFF

2.7.4. LED Indicators on the IPL-IDU-E1T1-EXP – Port Status

- **SFP 1/2 LINK** – indication of presented signal at SFP port
  - Flashes – signal detected and synchronized, valid communication with IDU
  - No light – no correct signal detected

- **LINK** – indication of G.703 link status on appropriate port (green LED)
  - Lights – signal detected at port
  - No light – no link at port
- **AIS** – indication of AIS signal at appropriate G.703 port
  - Lights – AIS signal detected
  - No light – no AIS at appropriate G.703 port

2.7.5. General Application with IPL-IDU-E1T1-EXP

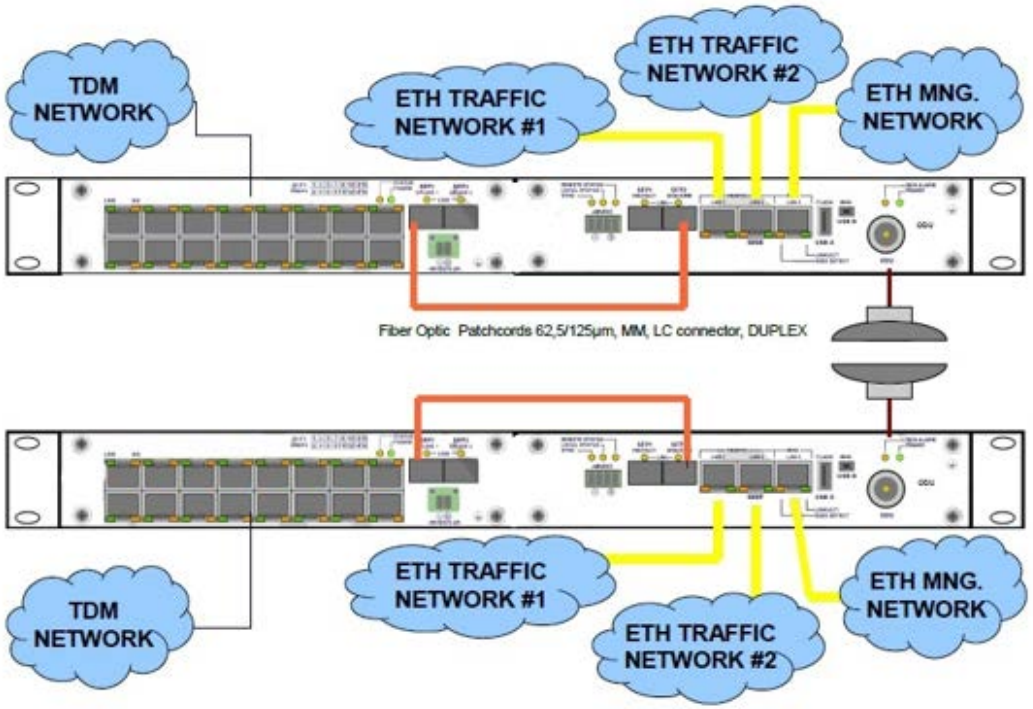

Figure 2-16 Connection Overview IPL-IDU-E1T1-EXP

The external multiplexer 16x E1 or 16x T1 application uses the Priority Base Packet System (PBPS is proprietary multiplexer system) for multiplexing from 1x up to 16x E1/T1 circuits. The PBPS data stream is first completed with the data channel for communication with the IDU and is subsequently packed into standard Ethernet frames for transmission over the network.

2.7.6. Up to 64 E1/T1 External Connections Multiplexed

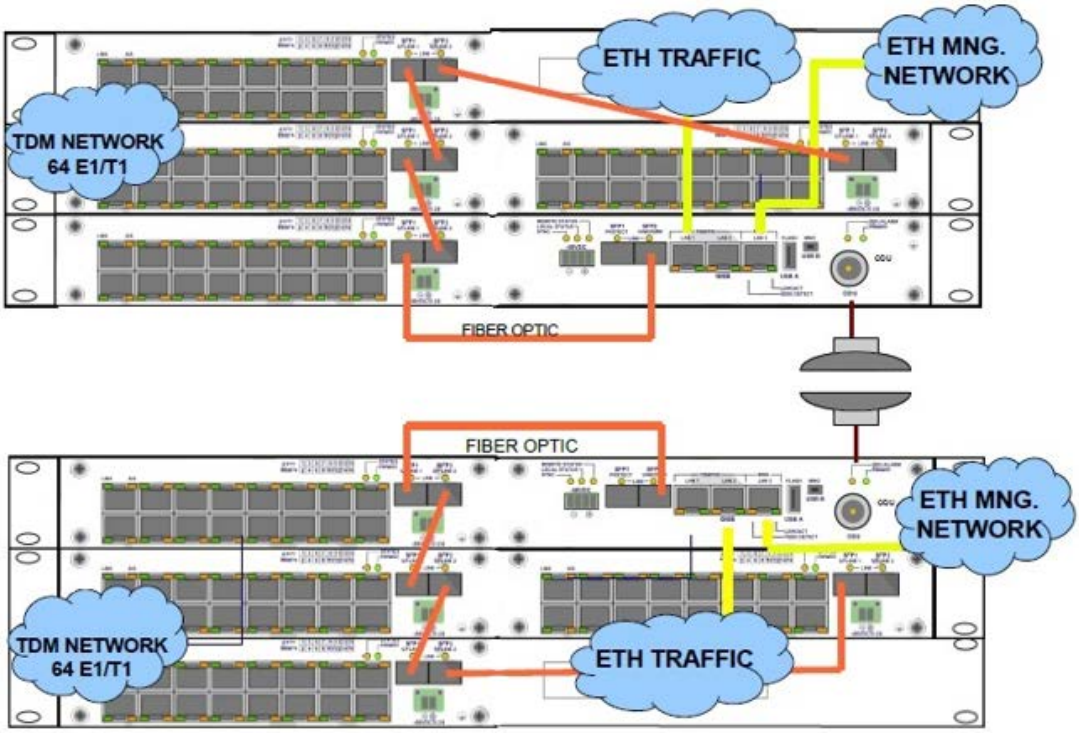

Figure 2-17 Connection Overview for up to 64 E1/T1 External Multiplexer

Up to 4 x IPL-IDU-E1T1-EXP modules can be connected in series to allow the maximum of 64x E1/T1 channels (ports). Port Nr. 2 SFP 1000Base-SX is dedicated for the modules interconnection in series. The configuration of all CFIP external modules is performed from the IDU GUI (set-up of basic configuration E1/T1, add/drop multiplexer, backup).

2.7.7. 1+1 Application with IPL-IDU-E1T1-EXP

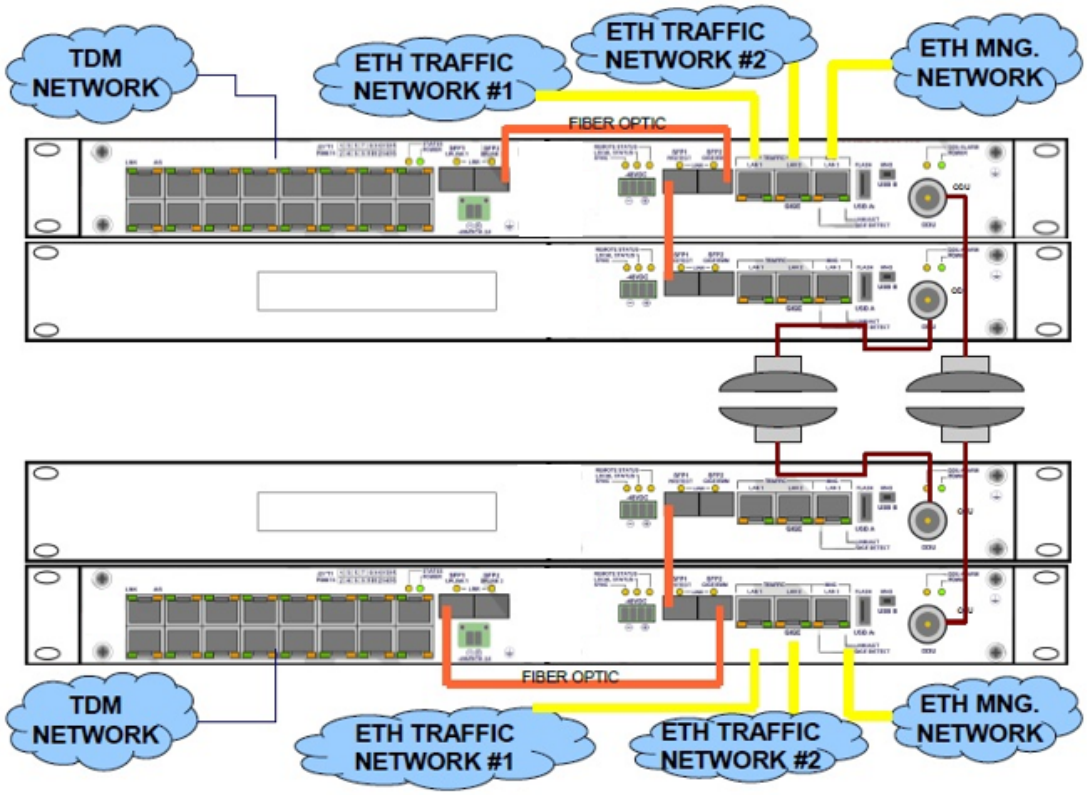

Figure 2-18 Connection Overview for up to 64x E1/T1 External Multiplexer

The combination of 1+1 protected configuration with extension module IPL-IDU-E1T1-EXP.

2.7.8. Add-drop Multiplexer Application

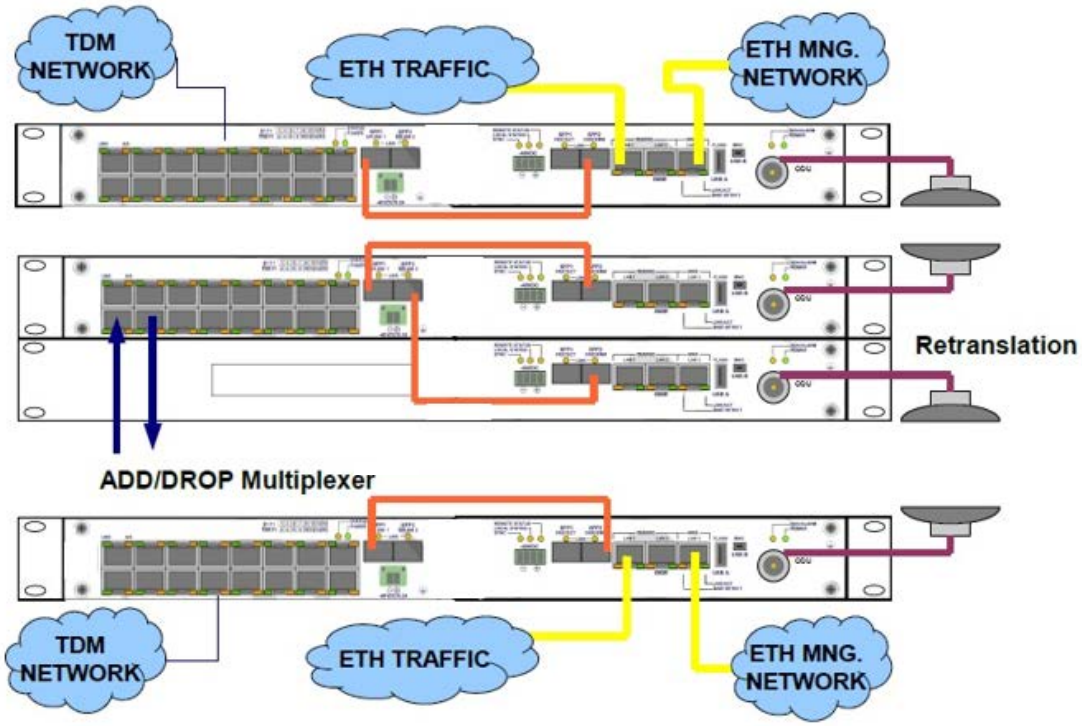

Figure 2-19 Connection Overview for Add-drop Multiplexer Application

2.8. Management and Configuration Examples for IPL-IDU-E1T1-EXP

The configuration and status of a module can be found in the web-based GUI on the Ports tab in the EMM management menu.

Figure 2-20 GUI – EMM Management Menu – Ports Tab

EMM SUPPORT:

- This check box changes the mode of the SFP2 port from standard Gigabit ETH to proprietary EMM (Expansion) mode. When EMM mode is enabled, the IDU starts communication with all connected EMM expansion modules.

EMM SETTING:

- ***EMM Type*** - displays the type of connected EMM (Expansion) card.
  - **N/A** - indicates that particular position is empty.
  - **RELAY-IDU** - indicates that the relay IDU is connected directly to IDU SFP port (relay application) or to EMM slave SFP port (add/drop configuration).
- ***EMM Mode*** – this function is related to the IPL-IDU-E1T1-EXP module only and allows you to choose the traffic interface mode between E1 and T1.
- ***EMM Enable*** – Choose to enable or disable generation/reception of data frames to/from the Fiber Optic stream. When enabled a particular EMM module occupies the appropriate range of traffic port channels.
- ***EMM Add/Drop ID*** – specifies EMM Add/Drop Range – channel range which is in use by the current EMM module. In auto mode the EMM module occupies the port channel range according to its position in EMM modules chain. If specific Add/Drop port channels are in range, then manual Add/Drop ID settings are available.
- ***EMM Add/Drop Range*** – This displays the appropriate port channel range according to the EMM modules position and EMM Add/Drop ID setting.

The configuration menu of a particular EMM (Expansion) module can be selected from the **EMM selection** dropdown box on the bottom of the EMM configuration page (see Figure 2-21).

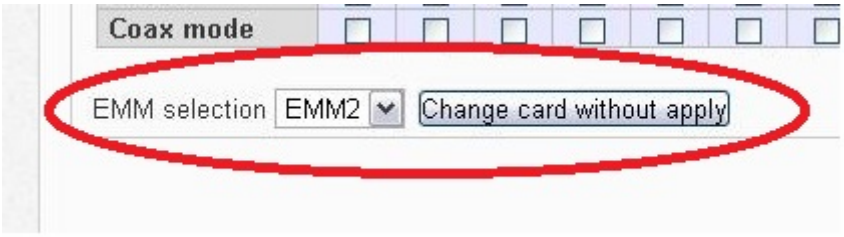

Figure 2-21 EMM Selection Configuration Selection

After selecting a particular EMM module and clicking “Change card without apply”, the appropriate EMM module’s configuration menu displays (see Figure 2-22).

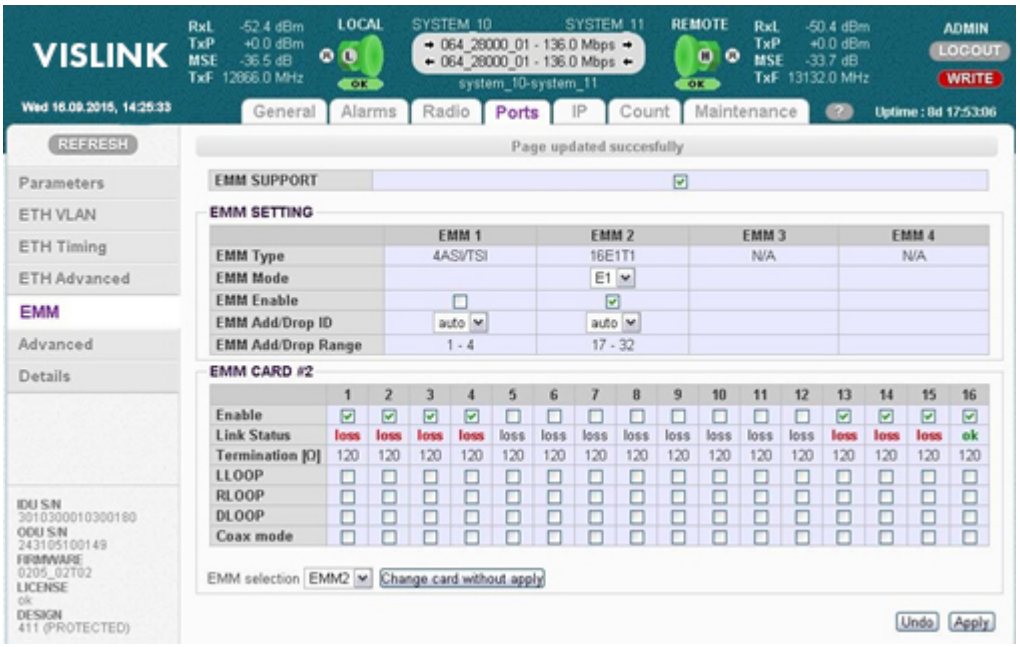

Figure 2-22 EMM Module’s Configuration Menu

EMM CARD #x settings for IPL-IDU-E1T1-EXP:

- ***Port/Channel Number*** - a number of E1/T1 ports (channels) the number in red indicates an alarm status for an appropriate internal channel (check alarm page for more details).
- ***Enable*** – selects which E1/T1 ports are enabled for customer traffic connection. Selecting/enabling ports reserves the appropriate capacity allocation from the IDU for this type of traffic.
- ***Link Status*** – displays the actual status of E1/T1 port or appropriate internal traffic channel.
- ***Termination*** – displays the actual impedance matching of E1/T1 port.
- ***LLOOP*** – local loopback configuration, incoming data stream from E1/T1 port is looped.
- ***RLOOP*** – remote loopback configuration, receiving data stream from Fiber Optics is looped.
- ***DLOOP*** – dual loopback configuration, both data stream directions are looped inside the IDU.
- ***Coax Mode*** – allows selecting E1/T1 interface mode (impedance) between 120 Ohm balanced and 75 Ohm unbalanced standards. When enabled – 75 Ohms is selected. Chosen interface mode is displayed in the “Termination” row.

2.9. Technical Specification of CFIP-E1/T1-EXT module

2.9.1. Traffic Interfaces

Item	Parameter	Value
IPL-IDU-E1T1-EXP	Number of Ports	16 (16xRJ-45)
	Interface	G.703-E1 balanced 120Ohm for E1 mode G.703-E1 unbalanced 75Ohm for E1 mode T1.102-T1/100 ohm for T1 mode
	Specification Compliance	T1.102, AT&T Pub 62411, T1.231, T1.403, ITU-T G.703, G.742, G.775, G.823, ETS 300 166, and ETS 300 233
	Coding	HDB3 for E1 mode, B8ZS for T1 mode
	Speed	2.048 Mbps for E1 mode, 1.554Mbps for T1 mode
	IDU direction interface	1x SFP 1000Base-SX (proprietary GIGE protocol) for connection with IPLink-SM IDU
	EXP module extension interface	1x SFP 1000Base-SX (proprietary GIGE protocol) for connection with additional EMM module
	EXP module scalability	Up to 64 E1 / T1 with combination of 4x EMM-16E1/T1 modules in series

Table 2-5 Traffic Interfaces Technical Specification

2.9.2. Network Management System

Item	Parameter	Value
Ports	Main NMS ports	2x SFP 1000Base-SX (proprietary GIGE protocol) from IDU
NMS form	Protocols	Proprietary
	Management Speed	1Mbps
GUI	Type	WEB based as additional function of IDU, folder PORTS
SNMP	Version	SNMP v1, SNMP v2c, SNMP v3 IDU support
	Read access	Complete MIB IDU support
	Write access	Sub-set of link parameter IDU support
Security	Licenses	Time limited/permanent IDU Support
	Access levels	guest/user/admin with password security IDU Support

Table 2-6 Network Management System Technical Specification

2.9.3. Miscellaneous

Item	Parameter	Value
Mechanical	Dimension [w x h x d]	19" EIA rack mount x 1RU (1.75 in./44mm)
	Weight	3 lbs. (1,36 kg)
	Protection	EN 60529 (IP31)
Input Voltage Level	EMM only	-20 VDC up to -60 VDC (standard version)
Power Consumption	IPL-IDU-E1T1-EXP	< 9 W
Environmental Operational Conditions	Temperature	23°F to 113°F (-5° to +45°C)
	Humidity	0 to 95%, Non condensing
	Altitude	14,500 Feet (4,420 Meters)
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
	EMC	EN 55022 class B, EN 61000-4-2,3,4,5,6,8,11 EN 61000-3-2,3
	Safety	IEC 60950-1/EN 60950-1

Table 2-7 Miscellaneous Technical Specification

2.10. Expansion Module IPL-IDU-ASI-EXP & IPL-ID-EA Indoor Units (IDUs)

The IPL-IDU-ASI-EXP (External Multiplexer Module) or IPL-IDU-EA Model expansion card provides ASI channels for IPLink-SM Indoor Units. The IPL-IDU-ASI-EXP Expansion Chassis enables multiplexing for up to four ASI channels into a compact stream, which is directed over a fiber optic connection to/from the IPLink-SM IDU. The multiplexer features a basic unit with 4x built-in ASI ports (one BNC per ASI channel) and 2x SFP 1000Base-SX ports.

The compact, simple to configure and easily scalable design enables cascading with other IPLink-SM extension devices (e.g. IPL-IDU-E1T1-EXP). The configuration is performed via the web-based GUI of the IDU.

The overall capacity for ASI is allocated in the PBPS and is based on the actual selected ASI ports in the software GUI of the IDU.

Priority Base Packet System (PBPS) is a proprietary multiplexer system.

Figure 2-23 IPL-IDU-ASI-EXP (ASI Expansion Chassis for “IPL-IDU-E” and “IPL-IDU-EA)

Figure 2-24 IPL-IDU-EA-xxxxx-A (Ethernet plus ASI; available for 1+0 and 1+1 configurations)

2.10.1. IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDUs User Ports

Each ASI channel can be independently configured into Tx or Rx mode. The following port combinations are available using this setting:

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

2.10.2. Connectors on the IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDU Front Panel

The following connectors are available on the front panel:

- DVB ASI – There are four configurable I/O DVB-ASI ports (75 Ohm).
- SFP 1 UPLINK1 – The master SFP port is reserved for connection to an IDU or to the master Expansion module card in the Expansion module chain.
- SFP 2 UPLINK2 – The slave SFP port is reserved for connection to the slave EMM card in an Expansion module chain or to relay the IDU in an add/drop configuration.
- -48 VDC – The power supply connectors positive-pole is grounded inside the device.
- Grounding connector.

2.10.3. LED Indicators on the IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDU – System Status

- **STATUS** – indication of the LOCAL EMM status
  - Lights – status OK (card enabled, proper communication with IDU)
  - Flashes – status WARNING (card is not enabled in the system or no communication with IDU or configuration was not finished yet)
  - No light – status ERROR (a firmware is not loaded into Expansion module HW)
- **POWER** – indication that Expansion module is under power (green LED)
  - Lights – power ON
  - No light – power OFF

2.10.4. LED indicators on the IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDU – Ports Status

- **SFP 1/2 LINK** – indication of presented signal at SFP port
  - Flashes – signal detected and synchronized, valid communication with IDU
  - No light – no correct signal detected
- **ASI STATUS** – indication of ASI status; depends on mode settings of appropriate ASI port (1-4):
  - Port in Tx Mode
  - Blink – ASI signal presented, sending data
  - No light – no data (IDLE status)
  - Port in Rx Mode
  - Lights – signal detected but in IDLE or *no sync* mode
  - Blink – incoming ASI signal
  - No light – no input signal detected

2.10.5. General Application with IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDUs

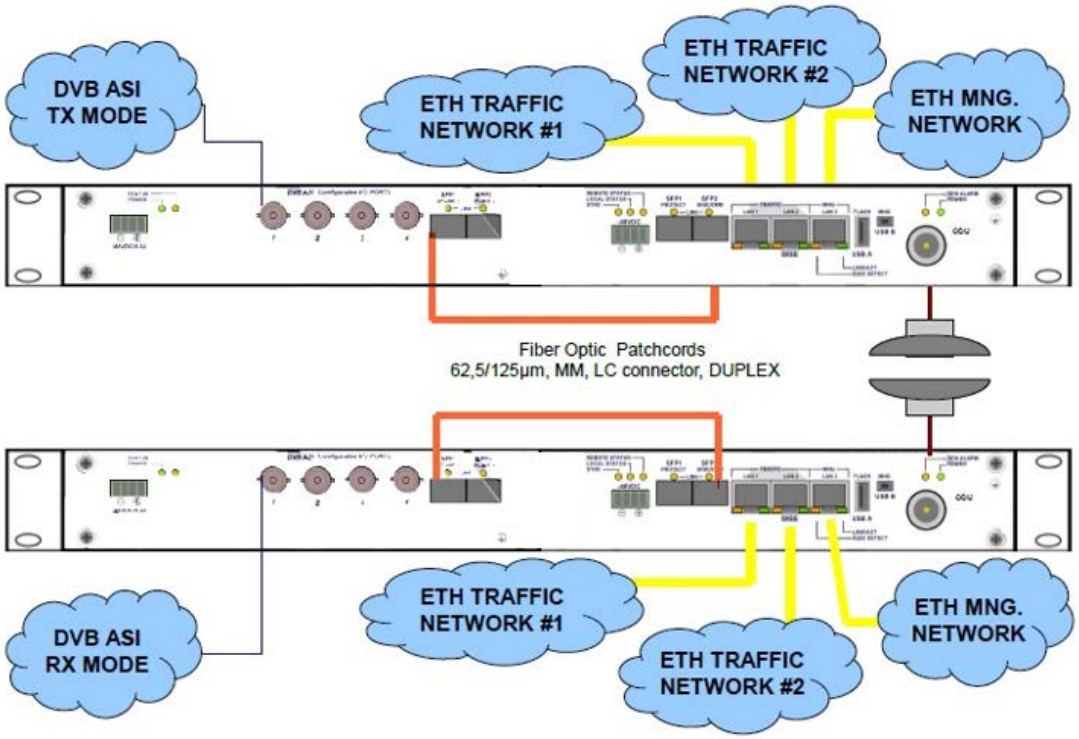

Figure 2-25 General Application with IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDUs

This application uses a combination of IPLink-SM IDUs with the MULTI configuration selected and one IPL-IDU-ASI-EXP card configured for unidirectional mode (Tx ports at one link side, Rx ports at opposite link side).

The Priority Base Packet System (PBPS - proprietary multiplexer system) is used for one up to four ASI channels multiplexing. The PBPS data stream is first completed with a management data channel to communicate with the connected IDU and is subsequently packed into the standard Ethernet frame for transmission over a Fiber Optic interconnection. The PBPS packets from the IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDU are then combined with another PBPS packets from an internal data source (Ethernet) then assembled on IDU according to the default priority scheme.

2.10.6. IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDU Cascading

Up to 4 x IPLink-SM EXP modules can be connected in series to give the maximum quantity of external ports (any combination of IPL-IDU-ASI-EXP, IPL-IDU-E1T1-EXP). Port Nr. 2 SFP 1000Base-SX is dedicated for interconnecting the modules in series. The configuration of all IPLink-SM EXP modules is performed from the GUI of Indoor Unit.

Ensure that the radio capacity is adequate for the required port capacity on the IPLink-SM EXPs.

2.10.7. 1+1 application with IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDUs

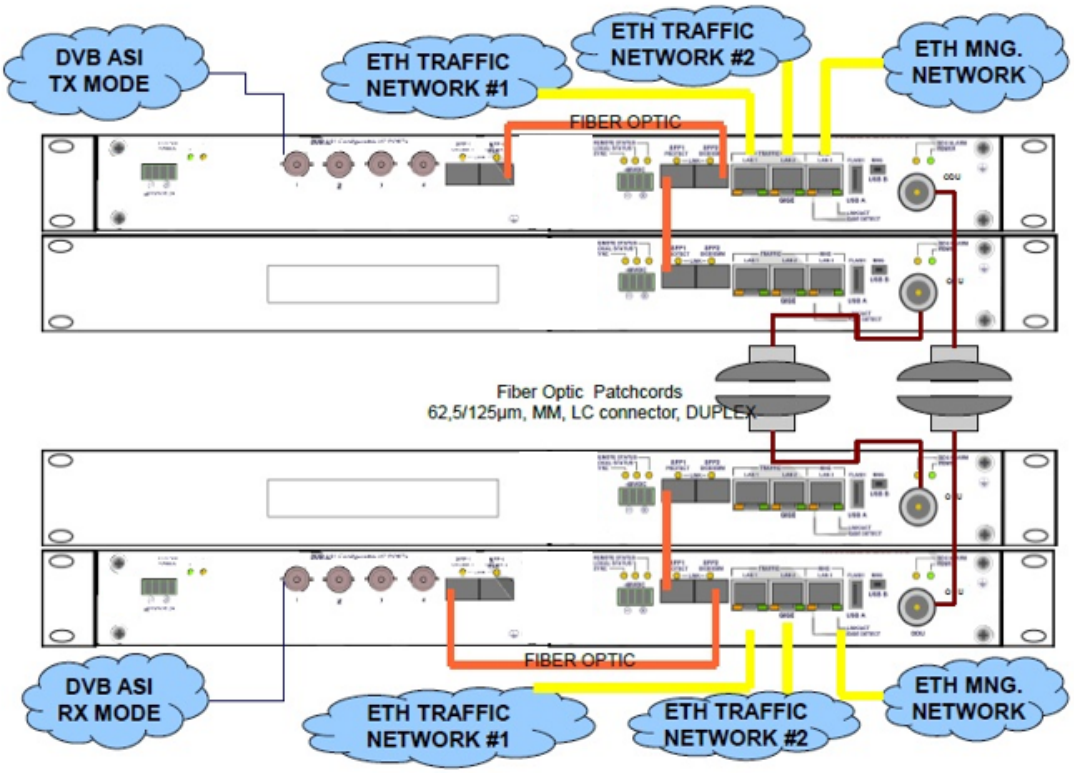

Figure 2-26 1+1 Application with IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDUs

This application uses combination of two IPLink-SM IDUs with selected PROTECTED design and one IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDU card in unidirectional mode (Tx ports at one link side, Rx ports at opposite link side).

The PBPS is used for 1 up to 4 ASI channels multiplexing. The data PBPS stream is first completed with management data channel for communication with the connected master IDU and subsequently is packed into standard Ethernet frame for transmission over FO interconnection. The PBPS packets from IPLink-SM EXP are then combined with another PBPS packets from internal data sources (Ethernet) assembled on IDU according to default priority scheme. The port SFP2 on IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDU can be optionally connected into slave IDU for possibility to change slave/master mode of IDUs.

2.10.8. 1+0 Retranslation Application with IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDU

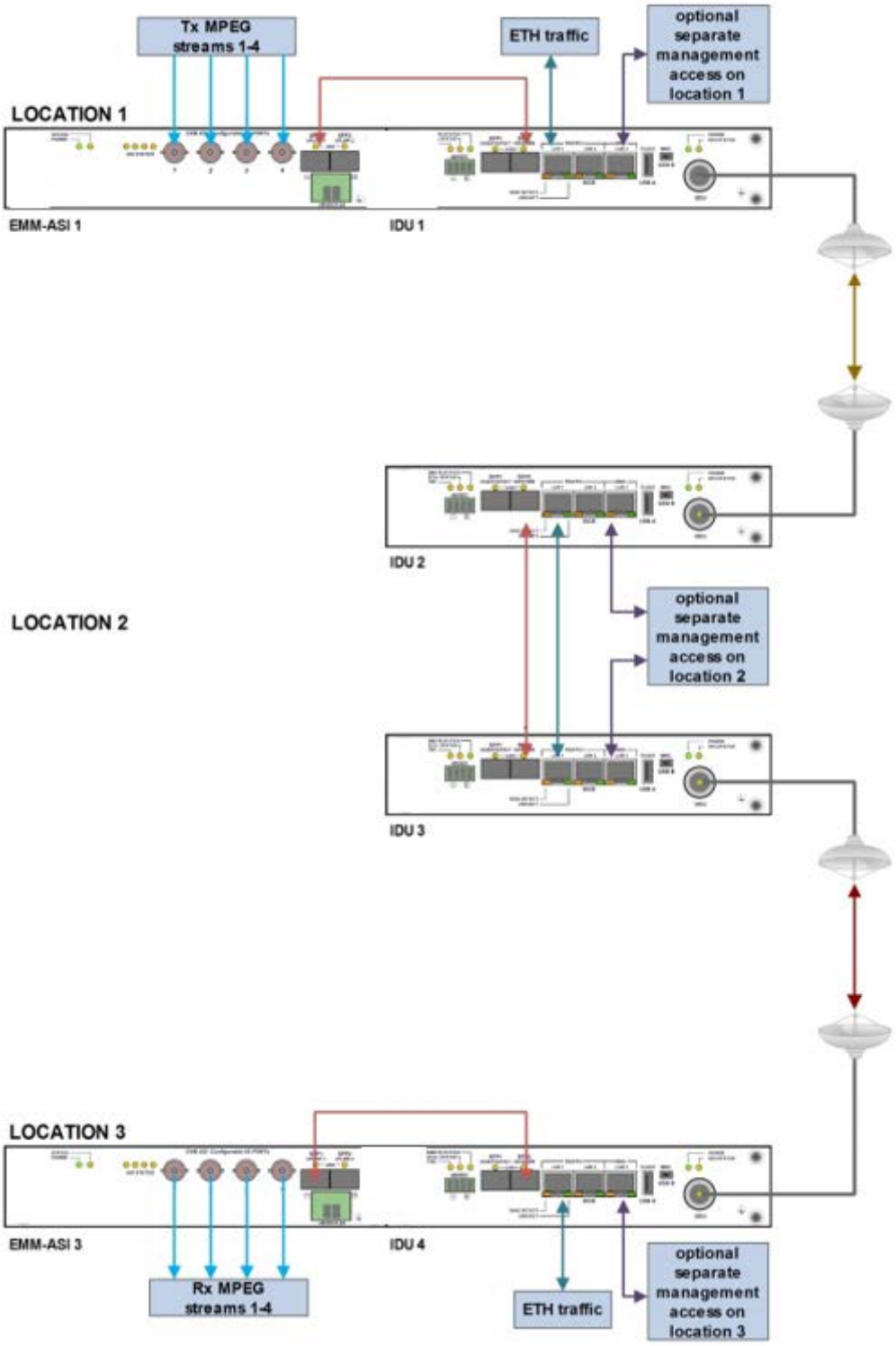

Figure 2-27 1+0 Retranslation Application

This application uses two links. All IPLink-SM IDUs are configured in MULTI design. Two IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDUs are connected to end-point IPLink-SM IDUs to send data over links. Both IPLink-SM IDUs in location 2

(midpoint) are interconnected via SFP2 interfaces, thus no need for additional IPL-IDU-ASI-EXP modules to retranslate the signal.

2.10.9. 1+0 Retranslation with Add/Drop application with IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDUs

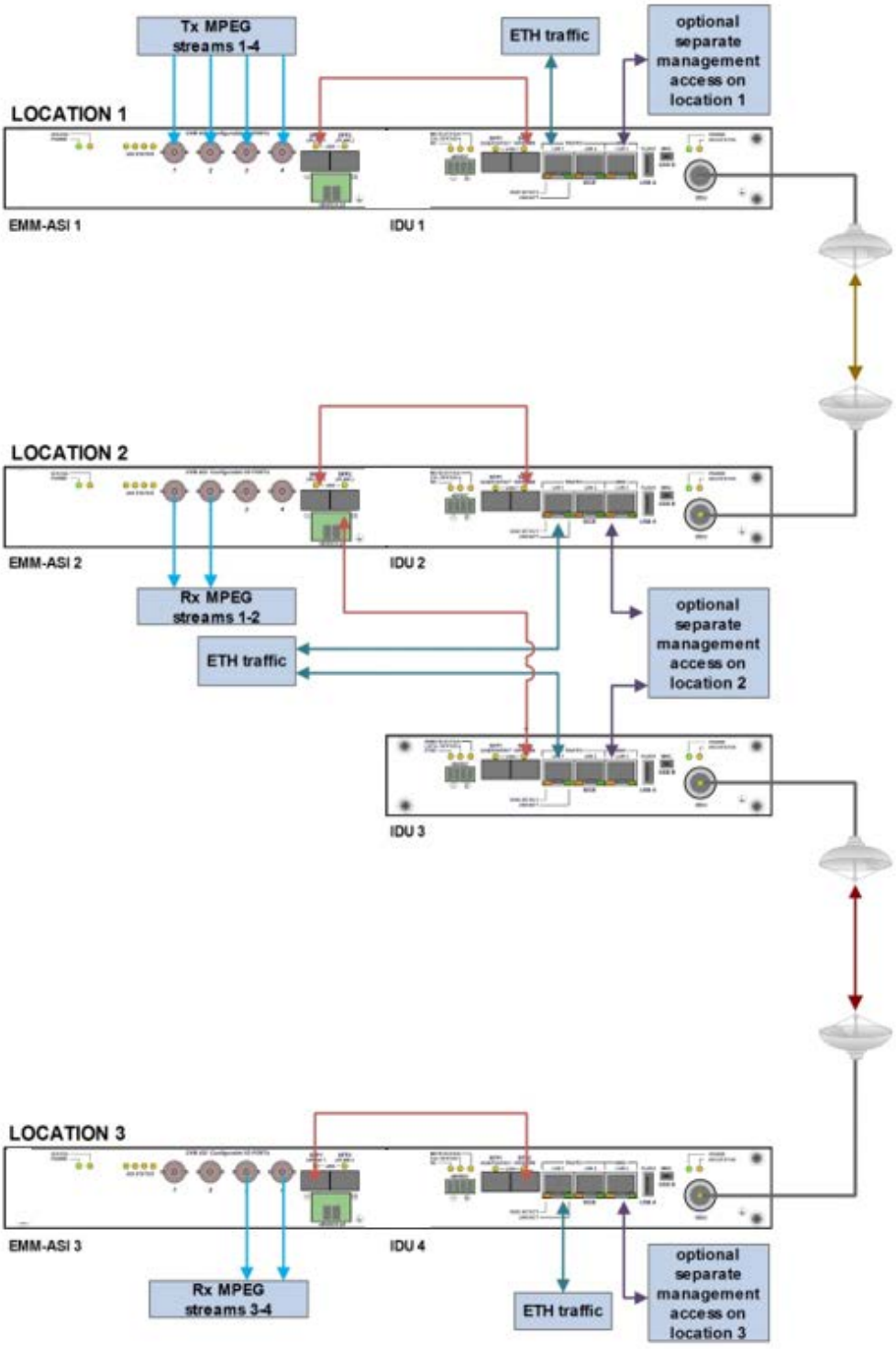

Figure 2-28 1+0 Retranslation with Add/Drop Application

This application uses two links. All IPLink-SM IDUs are configured in MULTI mode. Two IPL-IDU-ASI-EXP or IPL-IDU-EA Model IDUs are connected to end-point IPLink-

SM IDUs to send data over links. One IPL-IDU-ASI-EXP module is used in midpoint to Add/Drop part of an ASI stream.

Figure 2-29 shows an example of midpoint IPL-IDU-ASI-EXP module configuration.

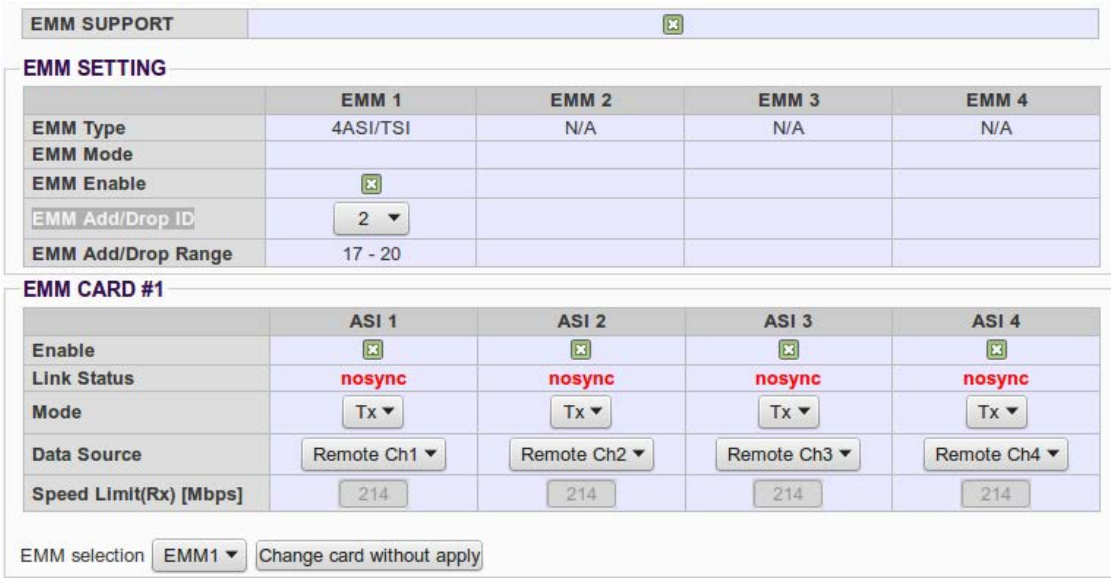

Figure 2-29 Midpoint IPL-IDU-ASI-EXP Module Configuration Example

- EMM Add/Drop ID
  - This must be selected depending on the sequence of external modules connected to the IDUs on endpoints. If the ASI module on the endpoint is the first (closest to the IDU) then the ID must be chosen as “1”. If the ASI module on the endpoint is installed as the second point/closest then “EMM Add/Drop ID” must be selected as “2”, and so on.
- EMM Add/Drop Range
  - Selection is automatic depending on the EMM Add/Drop ID selected and depending on any other external modules connected to endpoints on the IPL-IDU-E1T1-EXP or IPL-IDU-ASI-EXP module(s).

2.10.10. Management and Configuration Examples for IPL-IDU-ASI-EXP

Figure 2-30 shows the configuration and status menu on the web GUI in the Ports/EMM management menu.

Figure 2-30 Ports EMM Management Menu

- EMM SUPPORT:
  - This check box changes mode of SFP2 port from standard Gigabit ETH to proprietary EMM (Expansion) mode. When EMM mode is enabled by this checkbox, IDU starts communication with all connected EMM expansion modules.
- EMM SETTING:
  - ***EMM Type*** - displays the type of connected EMM (Expansion) card.
  - **N/A** - indicates that particular position is empty.
  - **RELAY-IDU** - indicates that the relay IDU is connected directly to IDU SFP port (relay application) or to EMM slave SFP port (add/drop configuration).
  - ***EMM Mode*** – this function is solely related to the IPL-IDU-E1T1-EXP module and allows you to choose the traffic interface mode between E1 and T1.
  - ***EMM Enable*** – enables or disables generation/reception of data frames to/from Fiber Optic stream. When enabled the particular EMM module occupies the appropriate range of traffic port channels
  - ***EMM Add/Drop ID*** – specifies EMM Add/Drop Range – channel range which is in use by the current EMM module. In “auto” mode the EMM module occupies the port channel range according to its position in the EMM modules chain. Manual Add/Drop ID settings are also available if a specific range of Add/Drop port channels is required.
  - ***EMM Add/Drop Range*** – displays appropriate port channel range according to the EMM module position and EMM Add/Drop ID setting.

The configuration menu for particular EMM (Expansion) modules is selected from the dropdown box “EMM selection” on the bottom of the EMM configuration page:

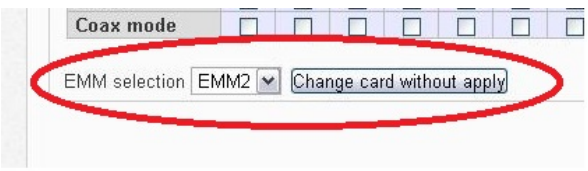

Figure 2-31 EMM Selection Box

After selecting a particular EMM module and clicking “Change card without apply”, the appropriate EMM module’s configuration menu is displayed as in Figure 2-32.

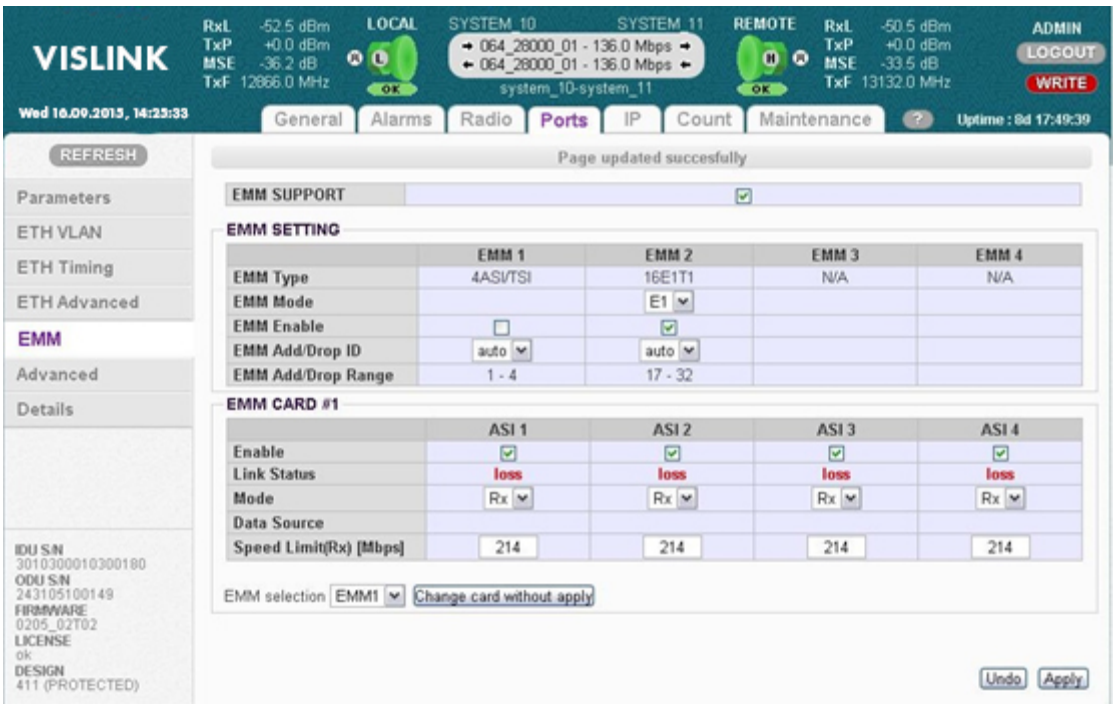

Figure 2-32 Change Card without Apply Option Screen

EMM CARD #x settings for IPL-IDU-ASI-EXP or IPL-IDU-EA Model

- ***Port/Channel Number*** - a number of ASI ports (channels).
- ***Enable*** – selects which ASI ports are enabled for DVB ASI connection. The necessary link capacity is automatically allocated according to the sum of all ASI Rx streams.
- ***Link Status*** – displays the actual status of an ASI port:
  - Status indications in case if ***Rx mode*** is set:
  - **ok** - a valid ASI signal is present at appropriate input port
  - **ok** - a valid ASI signal is present at appropriate input port, but the port is not enabled for traffic application
  - **Idle** - ASI signal detected and successfully synchronized, but the signal does not contain user data (MPEG stream is missing)
  - **Idle** - ASI signal detected and successfully synchronized but the signal does not contain user data (MPEG stream is missing) and the particular port is not enabled for traffic application
  - **nosync** - indicates that synchronization was not established for current received ASI signal
  - **nosync** - indicates that synchronization was not established for current received ASI signal and the port is not enabled for traffic application
  - **loss** - no signal detected at ASI input port
  - **loss** - no signal detected at ASI input port and the port is not enabled for traffic application
  - Status indications in case if ***Tx mode*** is set:
  - **ok** - a valid inbound signal is present and transmitted via appropriate ASI port

- **ok** - a valid inbound signal is present, but the port is not enabled for transmitting
- **Idle** - ASI signal detected and successfully synchronized but the signal does not contain user data (MPEG stream is missing)
- **Idle** - ASI signal detected and successfully synchronized but the signal does not contain user data (MPEG stream is missing), and the particular port is not enabled for traffic application

- ***Mode*** – specifies if the particular port operates in Rx (input from coaxial cable) or Tx (output to coaxial cable) mode
- ***Data Source*** – specifies source for Tx signal. Either remote ASI port (Remote CH1-4) or one of available local ASI Rx port (Local Ch1-4) can be chosen. This setting is available in Tx mode only
- ***Speed Limit(Rx) [Mbps]*** - maximal data rate for inbound traffic to avoid overload of overall link capacity. This setting is available in Rx mode only

2.10.11. IPL-IDU-ASI-EXP and IPL-IDU-EA Model Technical Specifications

Item	Parameter	Value
IPL-IDU-ASI-EXP and IPL-IDU-EA	Number of traffic Ports	4 (4xBNC)
	Interface	unbalanced 75 ohm
	Tx Output Voltage (p-p)	800 mV
	Min Rx. Sensitivity	200 mV (for D21.5 idle pattern)
	Specification Compliance	DVB-ASI, EN/ISO/IEC 13818-1, ETS 300 429
	Coding	8B/10B, MPEG-2 TS
	Port Speed	270Mbit/s at BNC port
	Max. speed for ASI channel	216 Mbps
	ASI channel shaping	8-216 Mbps
	Packet format	188 bytes / 204 bytes (with FEC)
	IDU interconnection interface	1x SFP 1000Base-SX (proprietary GIGE protocol) for connection with IPLink-SM IDU
	IPLink-SM EXP extension interface	1x SFP 1000Base-SX (proprietary GIGE protocol) for connection with additional IPLink-SM EXP module
	IPLink-SM EXP scalability	Up to four IPLink-SM EXP cards in cascade

Table 2-8 Technical Information - Traffic Interfaces

Item	Parameter	Value
Ports	Main NMS ports	2x SFP 1000Base-SX (proprietary GIGE protocol) from IDU
NMS form	Protocols	Proprietary
	Management Speed	1Mbps
GUI	Type	WEB based as additional function of IDU, folder PORTS
SNMP	Version	SNMP v1, SNMP v2c, SNMP v3 IDU support
	Read access	Complete MIB IDU support
	Write access	Sub-set of link parameter IDU support
Security	Licenses	Time limited/permanent IDU Support
	Access levels	guest/user/admin with password security IDU Support

Table 2-9 Technical Information - Network management system

Item	Parameter	Value
Mechanical	Dimension [w x h x d]	19" EIA rack mount x 1RU (1.75 in./44mm)
	Weight	3 lbs. (1,36 kg)
	Protection	EN 60529 (IP31)
Input Voltage Level	IPLink-SM EXP only	-20 VDC up to -60 VDC (standard version)
Power Consumption	IPL-IDU-ASI-EXP	< 9 W
Environmental Operational Conditions	Temperature	23 ° to 113 °F (-5 ° to +45 °C)
	Humidity	0 to 95%, Non condensing
	Altitude	14,500 Feet (4,420 Meters)
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
	EMC	EN 55022 class B, EN 61000-4-2,3,4,5,6,8,11 EN 61000-3-2,3
	Safety	IEC 60950-1/EN 60950-1

Table 2-10 Technical Information - Miscellaneous

2.11. Antenna

The ODU, Outdoor microwave unit, is designed for direct assembly to a microwave parabolic antenna to form a compact unit. The microwave adapter, which is part of the antenna kit, allows the transition between the flange of antenna and the microwave interface of the ODU. The parabolic antennas are available in different diameters:

- 1ft. (30cm)
- 2ft.(60cm)
- 3ft.(90cm)
- 4ft.(120cm)
- 6ft.(180cm)

Antennas can be used for horizontal and for vertical polarization, as well as right-side and left-side assembly.

The microwave unit and parabolic antenna can also be connected using a flexible waveguide. This alternative method of connection is suitable for installation of microwave link to antennas from a different manufacturer. The flexible waveguide is not included in the antenna shipment by default, it can be purchased separately.

NOTE: Always request information about the suitability of antennas from other suppliers with the manufacturer in advance.

Alternatively, use a directional coupler for 1+1 HSB protection configuration or an OMT (orthomode transducer) adapter for a cross polarization configuration (aggregate 2+0) for two ODUs using as single antenna.

Figure 2-33 Parabolic Antenna

2.12. Accessories

For correct installation of the microwave link and its proper function it is recommended to only use the following approved parts and accessories. The manufacturer takes no responsibility for any malfunction of the link when you use any alternative, non-approved part or accessories.

NOTE: The following parts are optional and ordered in addition to the standard delivery items, excluding IDU grounding kit.

2.12.1. IDU Grounding Kit

The Indoor Unit grounding kit comes as standard with the purchased unit.

- We recommend grounding the IDU to the rack cabinet using the enclosed Grounding kit.
- Similarly, we recommend grounding the ODU using the ground where the unit is mounted (mast mount, pole etc.).

2.12.2. Power Supply

The recommended power supply is a 90-Watt regulated switching power supply (PS-230/48) with 48 VDC and 1.9-Amp output. This is an additional, optional accessory.

To avoid overloading the PS-230/48 we recommend only powering a single IDU and a single ODU from each switching power supply PS-230/48 i.e. only power one side of the microwave link.

NOTE: If you connect more devices to the power supply, it may fail/overload.

2.12.3. IDU-ODU Cable

The IDU–ODU cable is a 50Ω coaxial cable intended to interconnect the Indoor Unit with the Outdoor Unit. Any type of good quality 50Ω cable can be used; the cable requires an N–type male connector on each end. There are two N–type male connectors included in each radio unit delivery that fit RG–213 cables or other cables with a surface diameter of 10mm. As the attenuation of the cable is essential, particularly at 350MHz frequency, its usage is restricted. The attenuation of the signal should not exceed 22dB at 350MHz. You can use up to 100m of RG-213 coaxial cable and LMR–400 cable can reach up to 300 m.

2.12.3.1. N-Connector

We recommend to use only brand-name N-connectors (male) e.g. Rosenberger, Telegartner, Amphenol.

2.12.4. Coaxial Cable Grounding Kit

To ensure sufficient lightning protection for the radio units using cables of 50m to 100m, we recommend installing grounding kits to the cable. For longer cables (>100m) we recommend installing a grounding kit every 50m and as well as on the cable at the point it enters the building.

2.12.5. Ethernet Cable with RJ-45 Connectors

We recommend a twisted-pair type CAT5e manufactured from Belden as a suitable Ethernet cable.

2.12.6. Surge Suppressors

To protect the IDU, an RF surge suppressor must be installed on the coaxial cable at the point it enters the building. A surge suppressor must also be installed on the coaxial cable near the ODU. The surge suppressor helps to reduce/eliminate the damages resulting from excess voltage.

2.12.7. N-plug to N-jack Right Angle Adaptor

The right angle adaptor is recommended to connect the coaxial cable to an IPLink-SM IDU unit where a 90° connection is required. We recommend to use only brand-name R/A adaptors e.g. Rosenberger, Telegartner, Amphenol.

3. INSTALLATION

3.1. Introduction

The installation and commissioning of the IPLink-SM microwave system should be carried out by an authorized engineer or partner. If an authorized partner is used, they are liable for trouble shooting any possible failures during the warranty period. All equipment and power supplies must be installed according to each country's national electrical codes and standards.

3.2. Installation Tools Required

Table 3-1 shows the necessary tools required for installation of the IDU/ODU. These tools are not included in the delivery.

Tool	Purpose
Cross screwdriver	for IDU rack cabinet installation
Engineer´s wrench	M7, M10, M13, M17
Vulcanized isolation tape	for N and BNC connector insulation
DC voltmeter	for RSSI measurement on ODU
BNC – DC voltmeter reduction	for RSSI measurement

Table 3-1 Installation Tools

3.3. Unpacking the Device

After unpacking the device, check that the delivery contains all the parts listed on the packing list, including any related accessories.

3.4. ODU Installation

3.4.1. Setting the Polarization

You can set the ODU polarization by fixing the antenna in the required position before attaching the ODU with the relevant adapter rotation position. An arrow symbol on the ODU case explicitly identifies its polarization. Vertical polarization is denoted by the arrow pointing upward or downward. Similarly, horizontal polarization is denoted by the arrow pointing 90° left or right relative to the vertical polarization. Table 3-2 shows the optional polarization positions available.

	ODU position		Adapter slot
Vertical polarization			
Horizontal polarization			

Table 3-2 ODU Polarizations

3.4.2. Mounting the Antenna to the ODU

Mounting the parabolic antenna to the ODU is a simple process. The installation is performed by fastening four latches to the antenna adapter, noting and matching the polarization (see Figure 3-1 and Figure 3-2).

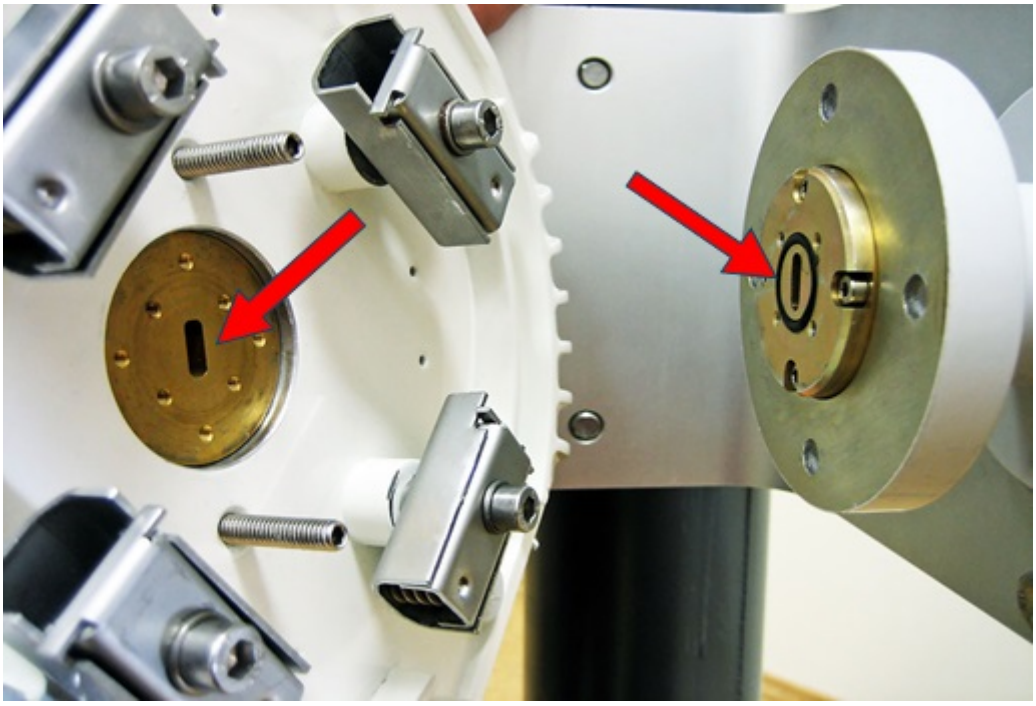

Figure 3-1 Fastening the ODU to the Antenna Noting Polarization

Figure 3-2 Final ODU and Antenna Installation

⚠ CAUTION: Always fasten the two opposite fixing latches at the same time. Make sure that the adapter slot and ODU waveguide slot match before attempting to install or while changing the polarization.

3.5. IDU Installation

The IPLink-SM IDU format was designed in accordance with the mounting requirements for a standard 19" rack cabinet, so it occupies the least possible height.

NOTE: Figure 3-3 is Ethernet Only, available for 1+0 and 1+1 configurations and Figure 3-4 is Ethernet plus ASI, available for 1+0 and 1+1 configurations.

Figure 3-3 IPL-IDU-E-xxxxx-A

Figure 3-4 IPL-IDU-EA-xxxxx-A

3.6. Cable Installation

3.6.1. IDU - ODU interconnection

To connect the IDU and OU use a low-loss coaxial cable with a specified impedance of 50Ohm terminated on both sides with N-connectors. Some examples of suitable coaxial cables are RG-213 and LMR-400. The assumed maximum length of cable between IDU and ODU is 100 m for RG-213 and 300 m for LMR-400. Section 3.7 lists the recommended IDU/ODU cables.

⚠ CAUTION: Check the cable impedance or cable impedance matching before connecting cables between the ODU and the IDU.

3.6.2. Connecting Management Interfaces

Use the management Ethernet cable (included in standard IDU delivery) or alternatively, use a management USB-B cable (not in standard IDU delivery).

After connecting the management interface cable (assumed to be Ethernet) into the port LAN 3 on IDU front panel. From here it is possible to perform the primary configuration for the microwave link and subsequently manage the entire system.

Alternatively, use a management USB cable (USB A – computer side / USB B – IDU side) into the port marked MNG / USB B.

3.6.3. Connecting Power Supply

The device is powered from a DC source -48 VDC where the positive pole is grounded. Before applying power to the system, do not forget to properly ground the ODU unit. Use the ODU units grounding screw to ground it to the antenna mast, which it is attached to. Also properly ground the IDU unit to the rack cabinet where it is installed.

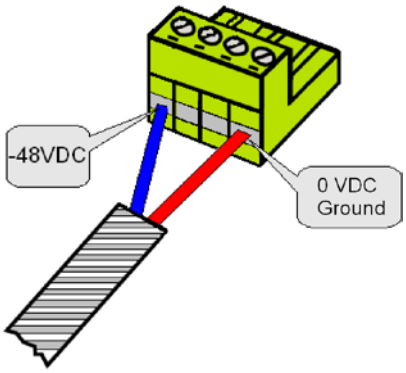

Figure 3-5 DC Connector Pinout for IDU

⚠ CAUTION: Pay close attention to the correct power supply pinout polarity. The power Supply pole 0 VDC is internally grounded, inside the IDU.

3.6.4. Grounding

For reliable and safe function of the whole system it is necessary to correctly ground the IDU and ODU units. The grounding cable for the IDU is a standard shipped accessory. Figure 3-5 shows the correct IDU wiring diagram. Figure 3-6 shows the ODU (M8) grounding screw.

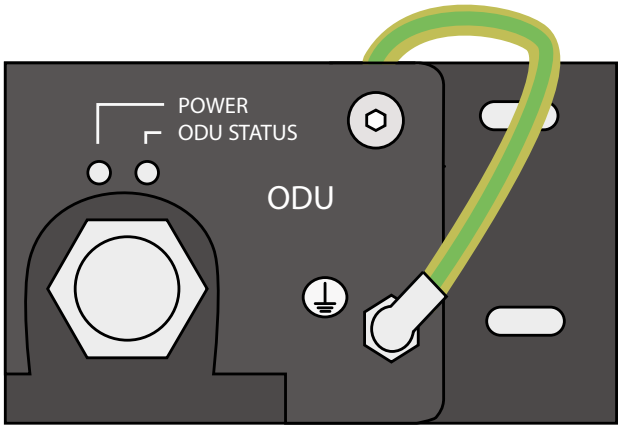

Figure 3-6 IDU Ground

3.7. Powering up the System

After carefully checking the coaxial cable installed between the IDU and ODU and each grounding point, proceed to applying power to the IDU. It will take around 20 seconds for the IDU to boot into its normal operating state. When the device boots up, watch the system status LEDs:

- POWER
- SYNC
- LOCAL STATUS
- REMOTE STATUS
- ODU STATUS

3.7.1.1. Standard System LED Behavior During Startup

1. The POWER LED should light after power up.
2. All system LEDs are off for approx. 10 seconds after power up.
3. All system LEDs illuminate for approx. four seconds after previous state.
4. All system LEDs flash for approx. three seconds after previous state.
5. Normal LED function then indicates current system state.

The following status of system LEDs indicates the correct initial start-up:

1. POWER lights.
2. SYNC is off.
3. LOCAL STATUS LED flashes-up.
4. REMOTE STATUS LED is off.
5. ODU STATUS LED lights.

Proceed to the initial link configuration and antenna alignment when the IDU has correctly started up.

3.8. Preparing for Link Configuration

Use a PC with a suitable Ethernet interface or USB port for the initial configuration.

3.8.1. PC Setup with LAN Adapter

If you are using the management Ethernet cable for the initial configuration, you must first set your computer IP address from the range which corresponds to the default IDU factory setup. Each unit has the same factory default IP address for its ETH port.

3.8.1.1. Default IDU ETH IP Settings

The factory default IDU IP address is 10.10.10.10, net-mask 255.255.255.0, therefore, it is necessary to set the PC address in the range of 10.10.10.1-254, you can use any address within this range, except for the IP address the device is using IP address 10.10.10.10.

3.8.1.2. Computer LAN Adapter Settings

We recommend that you set your PC IP address as follows:

- IP: 10.10.10.1
- Net mask: 255.255.255.0

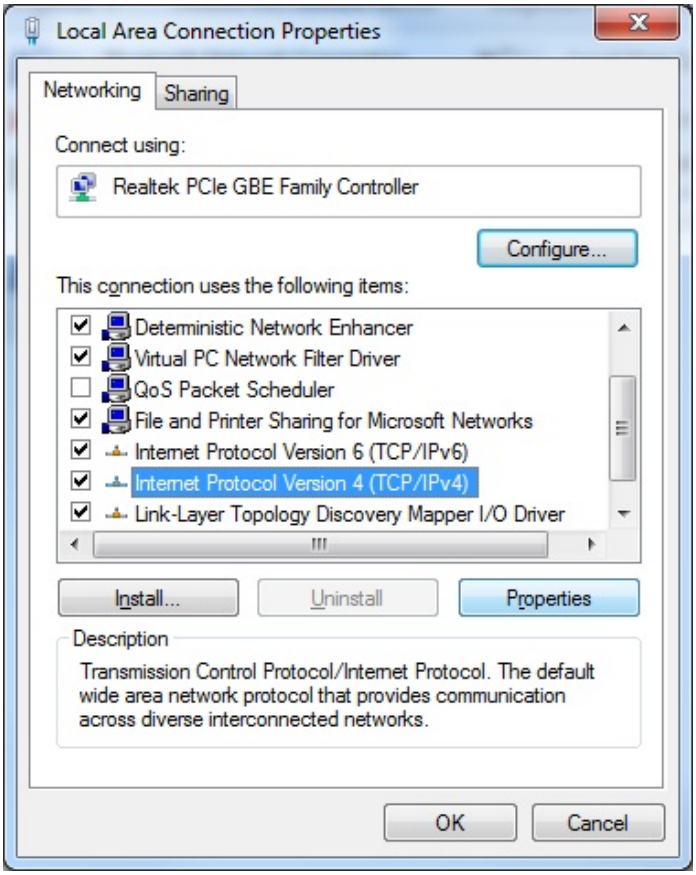

Figure 3-7 PC IP LAN Setup – Local Network Connection

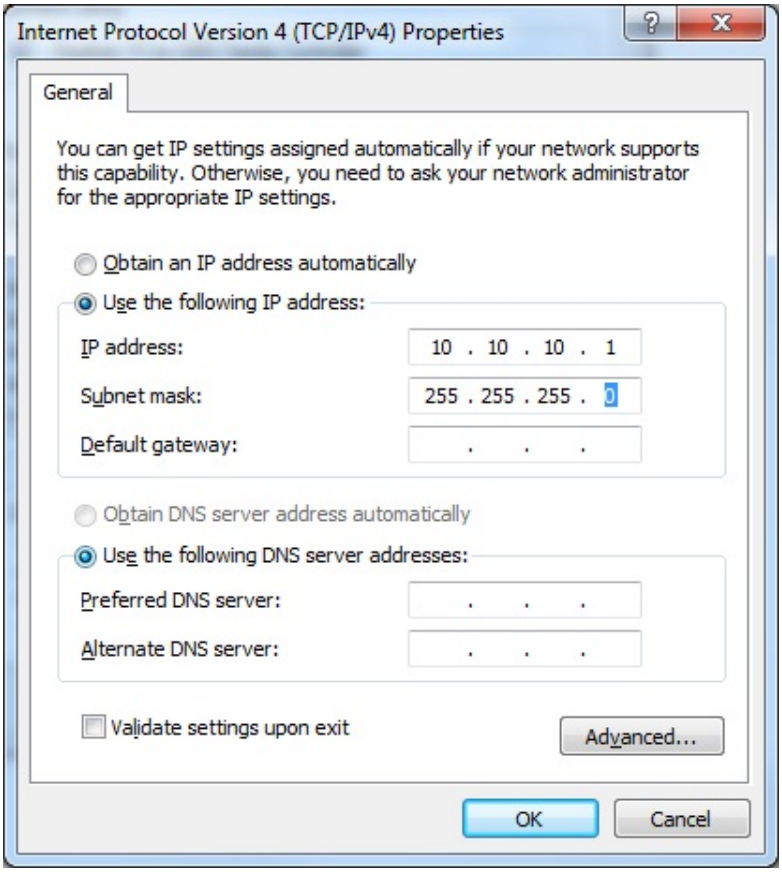

Figure 3-8 PC IP LAN Setup – Internet Protocol

3.8.2. PC setup with USB Adapter

If you use a USB cable for management and the initial configuration, you must first install the USB/IP driver on your computer with Microsoft® Windows® OS (a Linux based OS does not require an additional driver to be installed).

Follow the steps described in paragraphs below:

1. Connect the IDU to your computer (using a USB type A to USB type B cable).
2. Wait for Windows driver installer prompt and select the appropriate driver file (i.e. usb-gadget-eth.inf).

NOTE: If required, ask the manufacturuer's representative for the driver file before the installation process.

3. Follow the instructions for your OS.
4. After installation the USB connection is identified as an additional network adapter (see Figure 3-9).

Figure 3-9 PC IP USB Setup – USB Network Adapter

NOTE: You need to assign the correct IP address to your USB network adapter after installing the driver. Each IDU has the same default IP address for the USB port (USB IP address).

3.8.2.1. Default IDU USB IP Settings

The factory default IDU IP address is 10.10.11.10, net-mask 255.255.255.0, therefore, it is necessary to set the PC address in the range of 10.10.11.1-254, you can use any address within this range, except for the IP address the device is using i.e. IP address 10.10.11.10.

3.8.2.2. Computer USB Adapter Settings

Follow the steps described in Section 3.9.1.2 to configure the LAN adapter address.

NOTE: If using the USB cable options, ensure you select the USB adapter, not the LAN adapter.

3.9. Basic Link Setup

Once the mechanical link installation is complete, proceed with the basic link settings. This allows you to test the antenna alignment and test the connection functionality.

3.9.1. Login

To log in to your Local IDU, do the following:

1. Open your preferred web browser.
2. In the address bar type in the required IP address:

- For Ethernet connections use 10.10.10.10
- For USB connection use 10.10.11.10

NOTE: Mozilla Firefox version 3.xx and higher is recommended. However, connections with IE 5 and above or OPERA 9.xx and above are possible.

When the IDU login window appears as in Figure 3-10, type in the following:

- Login: admin
- Password: secret

Figure 3-10 LOGIN Window

NOTE: A warning message stating: Incorrect login name or password is displayed when an incorrect Login name or Password are entered.

3.9.2. GUI Basics

When you successfully log in to the IDU, the web management GUI interface shows. The web GUI is split into several sections and navigation is achieved using the tabs at the top of each page. Each tab has its own set of sub-menus, located at the left-hand side of each screen, see Figure 3-11. The following information shows the function for each section.

3.9.2.1. Header Section

Basic link parameters are displayed in this top bar section. Content in this section is common to all GUI pages.

3.9.2.2. Main Menu

Main menu tabs are accessible from the top of each GUI page.

3.9.2.3. Sub-menu

Specific sub-menu folders, via the side bar, display for each Main menu tab.

3.9.2.4. Auto-Refresh and Refresh Buttons

The auto-refresh **A** button is only available on specific GUI pages. Enabling this actions the page to periodically auto-refresh. The refresh interval is defined by the time elapsed between clicking the **REFRESH** button, followed by setting the interval by clicking the **A** button. The **REFRESH** button is used to update standard information for the GUI page.

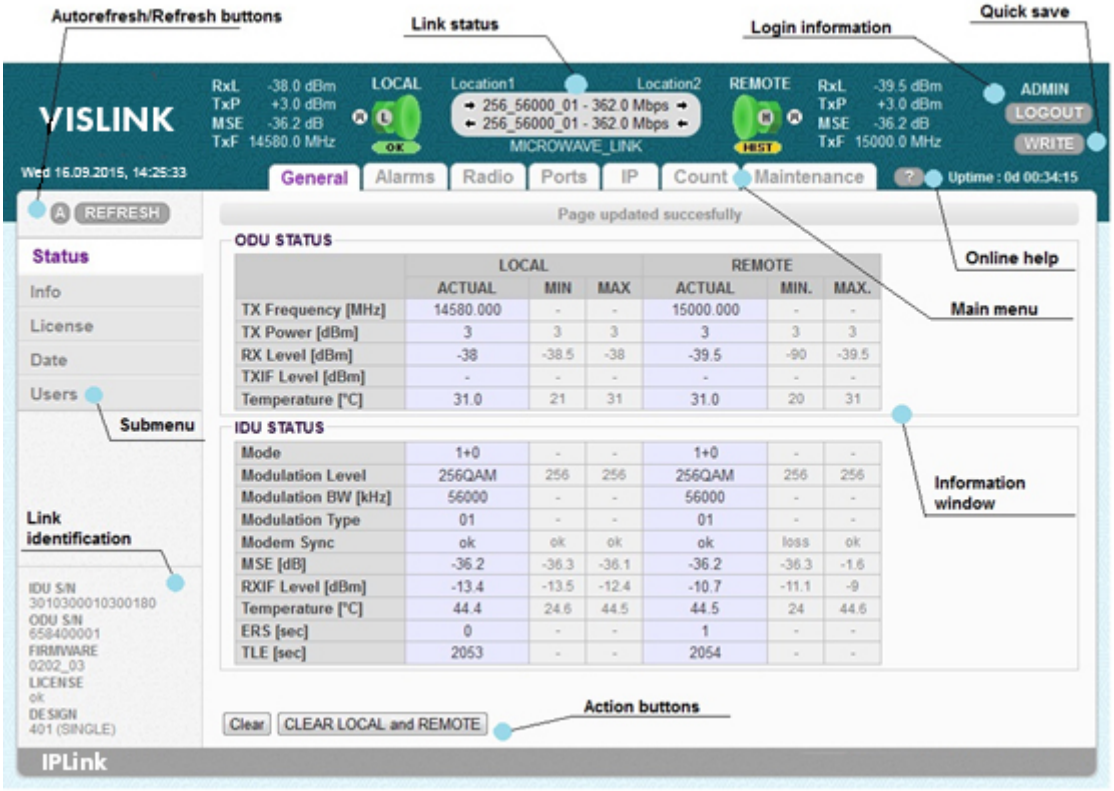

Figure 3-11 Overview of GUI Window

3.9.2.5. IP Setting

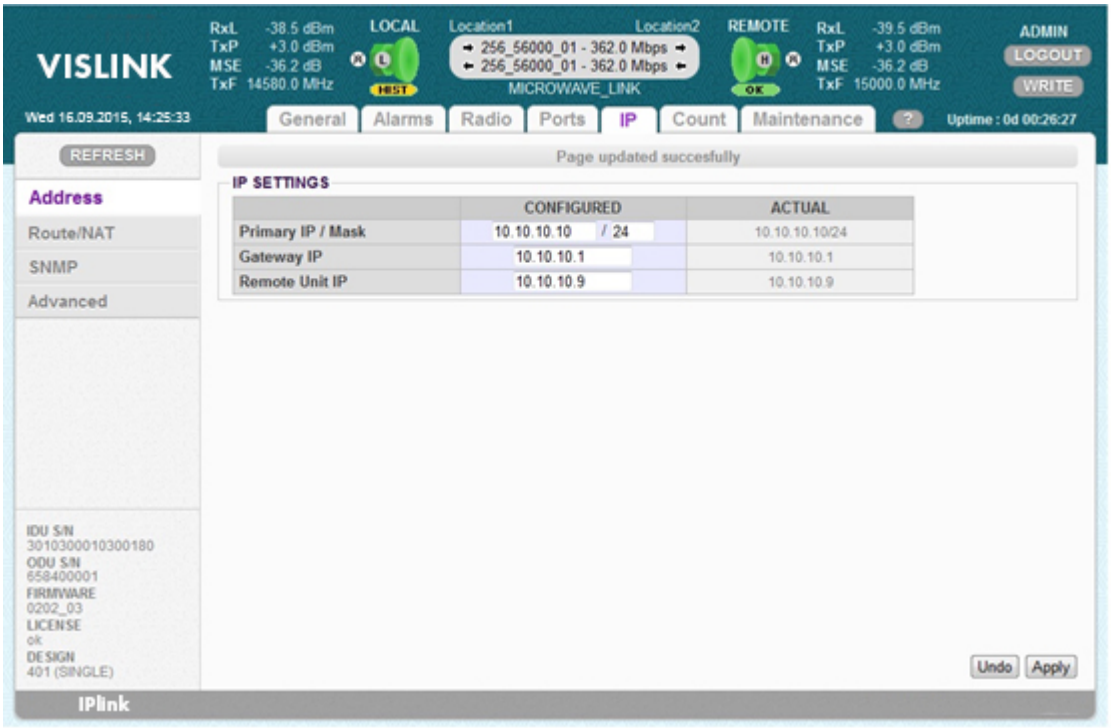

Figure 3-12 IP Address Configuration – GUI Page IP / Address

We recommend entering the basic IP configuration for local and remote IDU units at the very beginning of set up. This step is necessary for proper communication between the local and remote sites, optionally to ensure remote access to IDU devices situated externally from the customer´s network. In our following example, we use the factory default configuration, which is the basic type of out-of-band management access. Our following examples assume that remote IP access will be provided from the local link site: LOCATION1_M. For this configuration we have set the following IP addresses:

- Local link site named - LOCATION1_M:
  - Primary IP / Mask = 192.168.3.201/24
  - Default Gateway IP = 192.168.3.1
  - Remote Unit IP = 192.168.3.211
- Remote link site named - LOCATION2_M:
  - Primary IP / Mask = 192.168.3.211/24
  - Default Gateway IP = 192.168.3.201
  - Remote Unit IP = 192.168.3.201

NOTE: The remote device (IDU) must replicate the IP addresses entered for primary IP and remote IP in reverse, as the above example shows.

1. Using your preferred web browser, select the **IP** tab and **Address** side bar (see Figure 3-12).
2. Enter the above assigned primary IP address and net-mask, default gateway IP address and IP address for the remote IDU on both sites.
3. Click the **APPLY** button to confirm the entry values.

NOTE: It is necessary to assign the correct Primary IP and Remote Unit IP addresses at installation. Information from remote units cannot be displayed when this step is skipped. The next time that IP settings can be applied is during the complete link configuration.

To apply any IP configuration changes into an operating system, it is necessary to subsequently confirm all IP settings by clicking the **Write And Apply** button in the confirmation window (See Figure 3-13). Without this confirmation step, the temporary IP setting file is changed, but the IP changes are not applied into the running system.

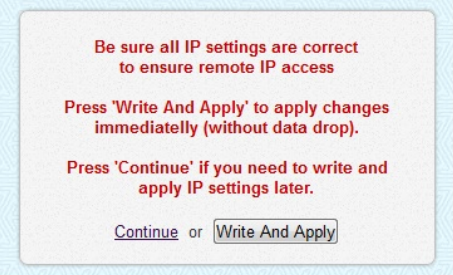

Figure 3-13 IP Setting Confirmation

3.9.3. Basic Radio Settings

It is also necessary to set the basic radio parameters at this early stage. These settings will be used for the final stage of link installation. According to the Telecommunication Authority allocated parameters (Tx frequency, Tx power) and requested data throughput, we set the microwave link into a functional configuration, as follows.

This example uses a local link site with a name of LOCATION1:

Setting	Value	Information
TX Frequency	14580 MHz	Set assigned Tx frequency for the Low Sub-band
Tx Power Limit	3dBm	Set the required maximum output power
ATPC	Off	Turn off the ATPC (must be off during the installation)
ODU TX Mute Config	auto	Unmuted output power
Modulation Limit	*256_56000_01*	Set the modulation to the most sensitive in assigned BW (56MHz in our case)
ACM	Off	Adaptive modulation function should be off

Table 3-3 Basic Radio Settings – Local (Site 1)

This example uses an opposite (remote) link site with name LOCATION2:

Setting	Value	Information
TX Frequency	15000 MHz	Set assigned Tx frequency for the High Sub band
Tx Power Limit	3dBm	Set the required maximum output power
ATPC	Off	Turn off the ATPC (must be off during the installation)
ODU TX Mute Config	auto	Unmuted output power
Modulation Limit	*256_56000_01*	Set the modulation to the most sensitive in assigned BW (56MHz in our case)
ACM	Off	Adaptive modulation function should be off

Table 3-4 Basic Radio Settings – Local (Site 2)

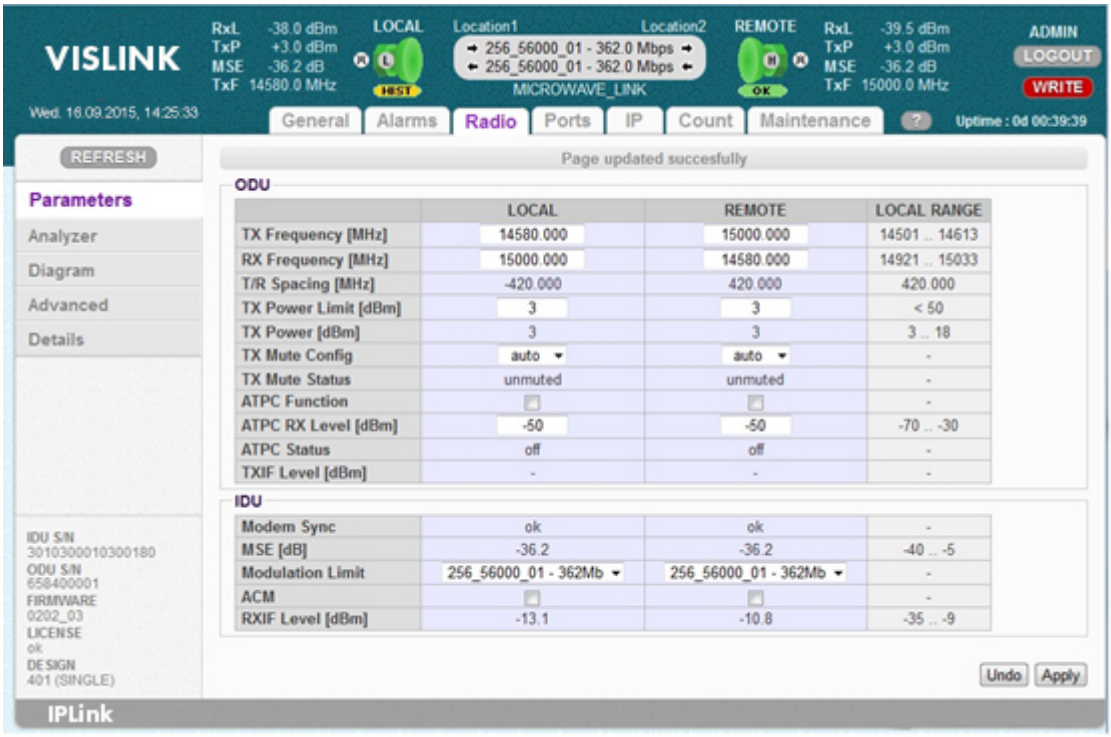

Figure 3-14 Radio Parameters Setting – GUI Page “Radio / Parameters

1. Set all the other parameters as depicted in Figure 3-14 and apply them by clicking the **APPLY** button.
2. Save this new configuration into start-up memory by clicking the **WRITE** button, located in the top bar of the GUI page.

NOTE: Configure the opposite side in the same way.

3.10. Antenna Alignment

Antenna alignment is performed with both terminals operating in normal weather conditions.

Aligning the antenna is performed in both horizontal and vertical direction using a DC voltmeter. The highest is the measured voltage, the highest is the received signal level. The voltage level is measured directly on the output BNC connector (see Figure 3-15) on the microwave ODU (RSSI – Received Signal Strength Indication). We recommend using an appropriate BNC reduction.

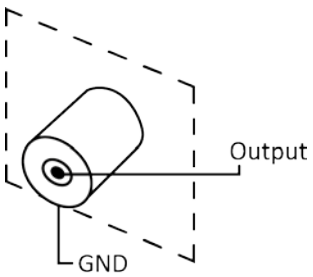

Figure 3-15 Pinout of RSSI connector on ODU

Figure 3-16 describes a typical Received Signal Level Voltage (RSL) for licensed bands.

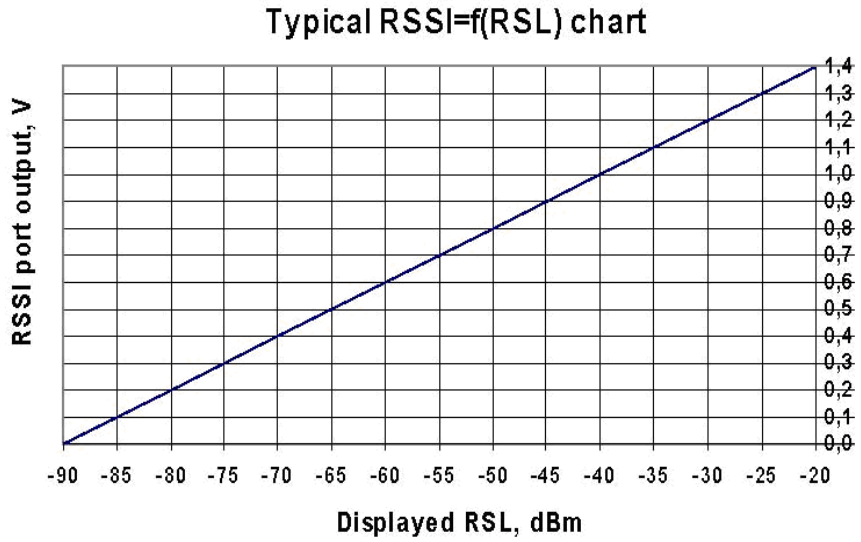

Figure 3-16 Graphed RSL [dBm] Verses RSSI Voltage [V]

Antenna alignment should only be performed in favorable weather conditions. Do not perform alignment during adverse weather when the value of the measured signal varies significantly giving inaccurate measurements.

NOTE: Adverse weather conditions are considered to be: rain, fog, snow, smog, etc.

NOTE: When aligning the antennas watch out for false alignment. This can occur when receiving side lobe signals from the remote antenna. It is important to identify the main antenna lobe. To do this, rotate the antenna to have the maximum RSL voltage. The value of RSL should always correspond to the expected calculated received signal strength value.

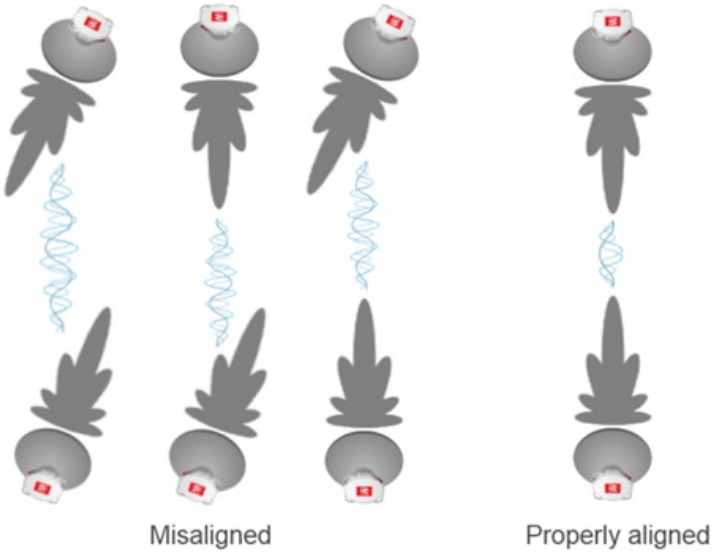

Figure 3-17 Alignment Principals

3.11. Functional Testing

Before connecting the user ports and the commissioned link, we recommend performing a quick test of the basic device functions to verify proper microwave

link installation. This step requires you to connect your PC and check the basic radio parameters.

3.11.1. Obtaining the Basic Link Information

Connect your PC according to the procedure described in Section 3.9 and use the **General** tab **Status** side bar for obtaining the required information (see Figure 3-18) and set the following parameters:

Setting	Information
TX Power	The figure should have a value corresponding to the assignment from Telecommunication Authority.
Rx Level	The figure should be in the range of -35 to -60 dBm and should correspond to the expected level resulting from preliminary link calculations (tolerance + / - 3 dBm). Approximately the same value (+/- 3 dBm) should also be measured on the opposite site.
MSE	Data should be in the range of -40 (better) to -30 dB (worse).
Modem Sync	The synchronization status of the modem part.

Table 3-5 Basic Link Information

The MSE parameter indicates the quality of the received signal. The MSE (Mean Square Error) parameter refers to the average of the squared difference between the actual received symbols and the ideal points. The closer together the points are in the state diagram, the better. The displayed MSE value is the normalized MSE parameter.

The values of MSE thresholds for each modulation is presented in the Technical Specification document.

You should also carry out the same evaluation on the opposing terminal as well.

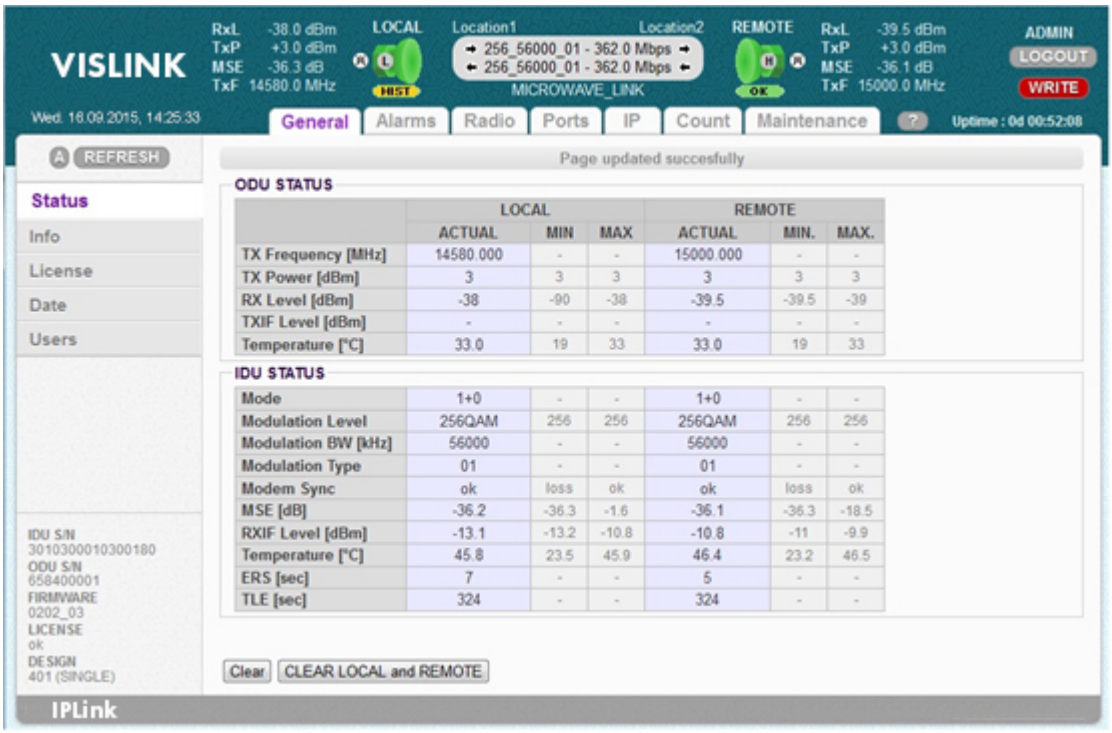

Figure 3-18 Main Microwave Link Parameters – GUI page General / Status

NOTE: If the measured values do not match the above stated ranges, you are required to complete a detailed link adjustment.

3.11.2. Five-Minute Link Quality Measurement (Optional)

The next step is a five-minute measurement test of the microwave link. The real required modulation scheme should be configured according to Figure 3-14. The MSE level must be checked again before this test.

1. When the updated configuration is complete and the MSE level is the expected level, click the **CLEAR LOCAL and REMOTE** button form the **General** tab using the **Status** side-bar.
2. Use the **Count** tab and **Basi**c side-bar to see the link statistics after a period of around 5 minutes.

The result is shown in Figure 3-19. There is no need to have any data connection into LAN ports to perform this test.

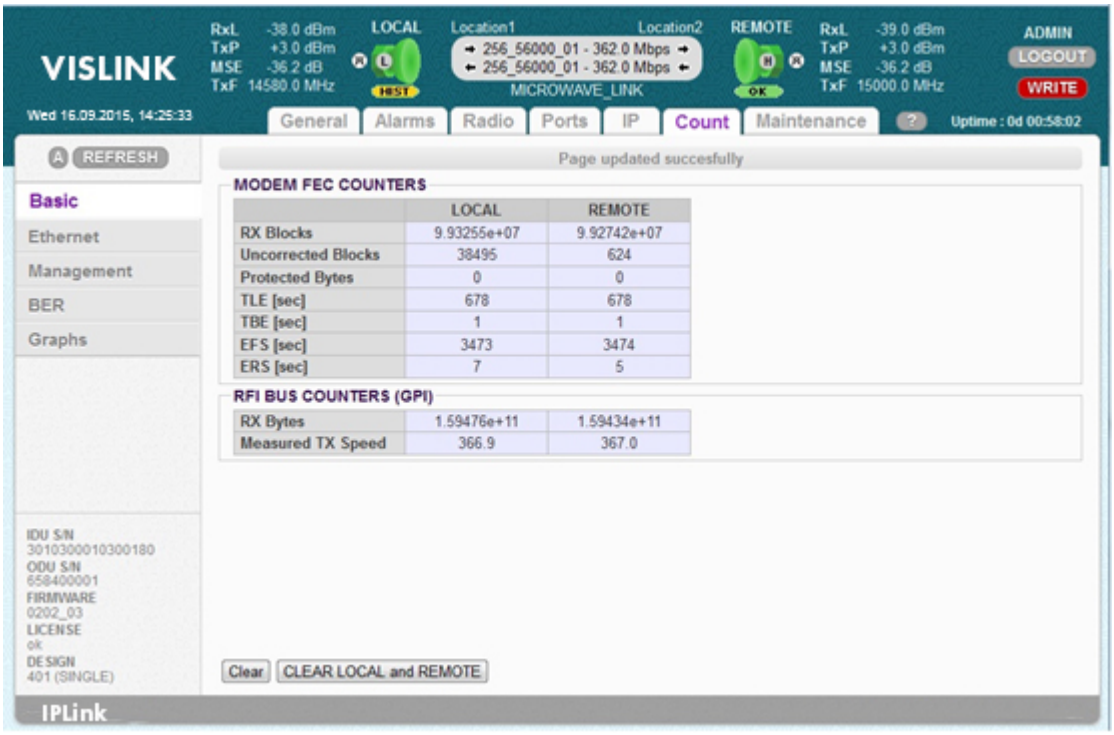

Figure 3-19 Basic Radio Link Statistics GUI Page - Count Tab/Basic Side-bar

Setting	Information
RX Blocks	The number of correctly received air frames, large number.
Uncorrected Blocks	The number of frames which couldn't be corrected by FEC; the figure should be “0”.
Protected Bytes	Important just for protection mode, the figure should be “0”
TLE	Time since last error; number of seconds from last recorded error. It should correspond to the time since last clicking the **CLEAR LOCAL and REMOTE** button on

	the main page General tab using the Status side-bar and it should be the same as EFS value.
TBE	Time between last two error events, the figure should be “0”
EFS	Error free seconds. This should correspond to the time since clicking the **CLEAR LOCAL and REMOTE** button from the main page **General** tab using the **Status** side-bar.
ERS	Error seconds. The number of seconds recorded during an error/ This figure should be “0”.

Table 3-6 Basic Tab/Count Side Bar Readings

If the test results are different compared to the expected values, you should perform a detailed check of the installation for the microwave link. The opposite terminal for the link should show similar results. The results can be read from the column marked REMOTE.

3.12. Connecting External Equipment

The IPLink-SM microwave system is equipped with Gigabit Ethernet ports to allow simultaneous connection of standard SFP modules into the free SFP slots. This allows you to connect external modules (EMM) or additional Gigabit Ethernet equipment.

3.12.1. Connecting Gigabit Ethernet Port

Figure 3-20 shows the Gigabit Ethernet 10/100/1000Mbps port pinout. Make sure that all four pairs of the cable are wired according to the pinout detailed in Table 3-7.

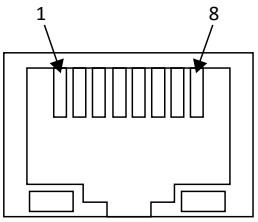

Figure 3-20 Gigabit Ethernet Port Pinout

Pin Number	Signal
Pin 1 to Pin 2	DA+ to DA-
Pin 3 to Pin 6	DB+ to DB-
Pin 4 tp Pin 5	DC+ to DC-
Pin 7 to Pin 8	DD+ to DD-

Table 3-7 Gigabit Ethernet Port Pin-out Twisted Pairs

NOTE: It is necessary to prevent possible Ethernet loops before connecting the Ethernet cable to the Gigabit Ethernet ports. Therefore, the correct Port settings must be carried out before more than one Ethernet cable is inserted into IDU.

3.12.3. Connecting an External EMM Module via Port SFP 2

Depending on the individual application, the number of IDU ports can be extended by means of a specific external multiplexer module (EMM). The EMM-16E1T1 connects via the SFP 2 port of the IDU and utilizes a Fiber Optic cable.

The IDU and EMM module must be then equipped with an SFP module to connect the Fiber Optic cable.

The SFP module should be inserted before the IDU is powered up, but can also be plugged in when the system is powered. Use an appropriate Fiber Optic patch cable using LC connectors between the IPLink-SM IDU and EMM.

NOTE: A 0.5 m long cable is usually adequate for rack mounted units.

4. LINK CONFIGURATION

4.1. Introduction

After the microwave link is installed, you then need to carry out the complete setup for all the required link parameters, including IP management settings. We recommend taking note of parameters, such as IP addresses, Tx frequency, Tx power etc. in advance in a well-arranged table.

Save the settings data list to make it easy to quickly replace a unit and restore the previous configuration settings.

The rest of this section describes setting up the link using the web GUI interface. Link set-up using text commands is possible, but beyond the remit of this manual.

NOTE: Do not use the browsers **Back** or **Refresh** functions during the set-up or to view the previous window(s). Use only the Main menu and submenu folders and GUI buttons of IPLink-SM IDU device.

4.2. Connection and Login

4.2.1. Local Access via the Ethernet LAN Interface

To setup the IDU via the management Ethernet LAN port (default LAN 3) you are required to connect the PC to the port LAN 3 on the IDU front panel using the proper Ethernet cable (see Section 3.9.1).

4.2.2. Local Access via the USB-B Interface

To setup the IDU via the management USB-B port, you are required to connect the PC and USB-B port on the IDU front panel using the proper USB-A to USB-B cable (See Section 3.9.2).

4.2.3. Login Using a Web Browser

You need to configure the computer's network connection before connecting the Ethernet management cable or USB management cable to the IDU.

Depending on the cable in use, the IPLink-SM IDU IP address is either of the following:

- The secondary IP address for access via LAN port, which is set to the default value:
  - IP address: 10.10.10.10/24
  - Network mas: 255.255.255.0
- The USB IP address for access via USB port, which is set to the default value:
  - IP address: 10.10.11.10/24
  - Network mask 255.255.255.0

You can access the IDU GUI via a web browser after you have correctly set the configuration of the computer's network connection. Enter the corresponding IP address in to the web browsers address bar for the type of cable in use to connect from the PC to the IPLink-SM IDU i.e. 10.10.10.10 if connecting using the LAN 3 port). This should then navigate to the login window (See Figure 3-10).

Your login remains active until you logout of the device. It is not possible to configure the IDU from two terminals at the same time (only one terminal is used in set-up mode at one time). Only one user with User or Administrator rights can be logged in.

For security, the device has an automatic timeout period of 10 minutes from the last action, after this time the user is automatically logged out.

For the standard configuration we recommend logging in with USER mode.

Only one user can be logged in in to the system at a time.

The administrator ADMIN-level is superior to the User-level. If an Administrator attempts to login to the system when a User account is active, a pop-up window alerts the Administrator to logout the User.

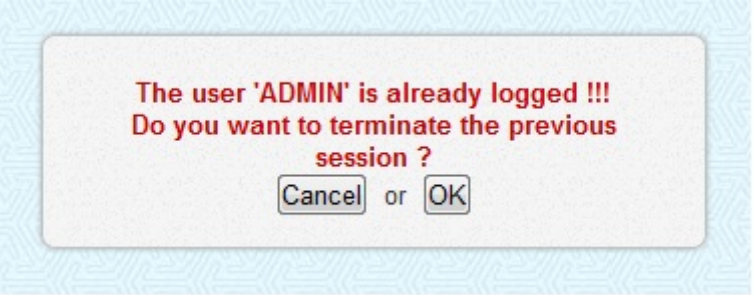

Figure 4-1 Alert window about already logged User

The rights and options for each access mode are described in more details in Section 4.3.6.

4.3. General System Configurations

4.3.1. Protection Configuration Settings

The availability of the **Protection** side-bar page on the **General** tab depends on the selected configuration type and the available license content (see Section 4.9.6). When using a Protected 1+1 configuration and the same design is supported in the license file the general protection settings can be managed in the GUI page as per Figure 4-2.

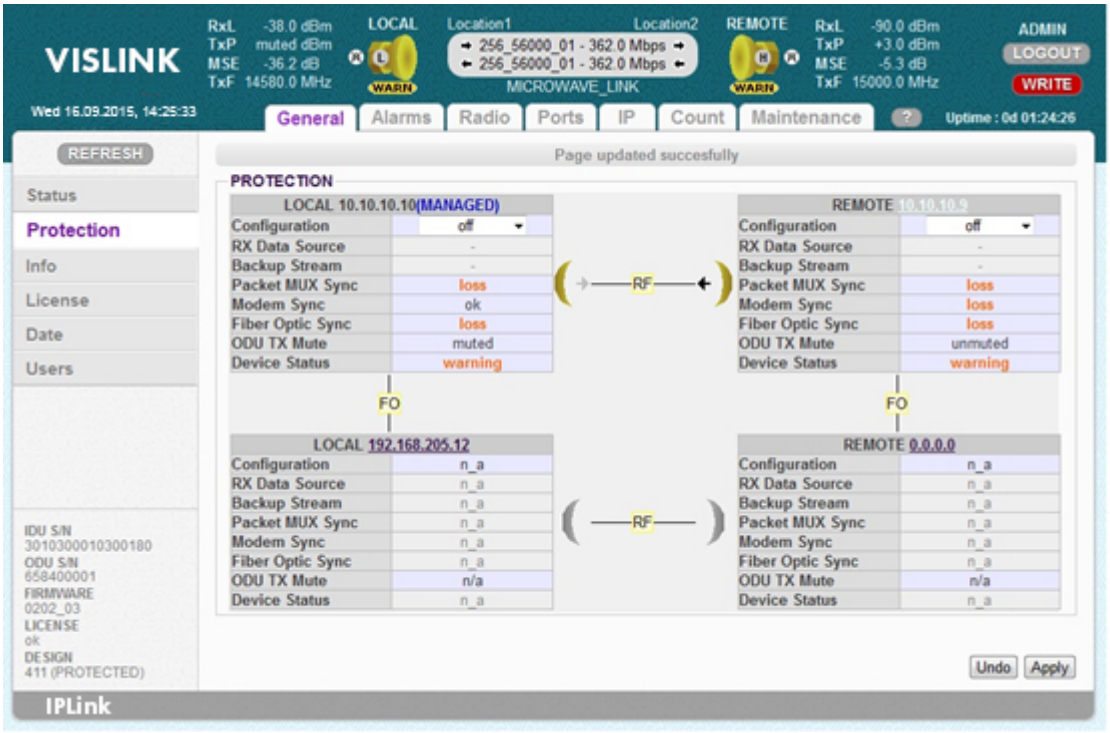

Figure 4-2 Initial Protection Configuration GUI Page

Protection mode defaults to **Off** once a change is made to this configuration. This is to prevent any possible settings mistakes, such as radio interference, port loopbacks etc. Tx Power is muted and all traffic ports are shut down in **Protection Off** mode.

NOTE: You should set all Radio, IP and Port parameters according to the prepared system configuration and configure protection mode as the last step in the system configuration procedure.

The GUI's graphical antenna icons (RF) are used as an aid to understand the actual state of the IDU. States include:

- The state of the whole protected link (green – no alarm)
- The mode of appropriate ODU transmitter:
  - A black arrow indicates that transmitter is unmuted.
  - A number of arrows indicates TX mode – FD/SD+HSB.

The Protection page GUI shows several drop-down boxes that describe particular settings and display boxes.

Configuration – This drop-down menu allows you to select between **actual** and **configured** protection mode. To ensure the correct system interconnection exists at both local, remote and neighboring units once the settings are entered, we recommend setting the required protection mode at the MASTER SIDE. The slave units then automatically inherit settings.

The possible modes are:

- **master/FD, slave/FD** – This mode configures the frequency diversity mode when two transmitters and two receivers operate on different carrier frequencies, but use identical corresponding transmitters at the far end. This protection mode protects against Multipath Fading and also against PtP system HW failure.
- **master/SD, slave/SD –** This mode configures the space diversity mode when one transmitter is used (you are able to manually select the transmitter at the master or slave unit) and two receivers operate on a single carrier frequency. Two antennas at each installation site are required. If both master and slave units do not receive signals or fall out of synchronization, the opposite transmitter settings remain as is. This protection mode usually protects against Multipath Fading.
- **master/HSB, slave/HSB –** This mode configures hot standby protection mode when one transmitter is used at a time (you can select a transmitter manually at the master or slave unit) and two receivers operate on a single carrier frequency. Use a single antenna with a directional coupler at each installation side. If both master and slave units do not receive a signal or fall out of synchronization, the system swaps the transmission sequence on the opposite transmitters (mutes one transmitter while the other one transmits) to ensure correct system function. This mode protects against PtP system HW failure. Protection is hitless for Rx failures, when transmitters are swapped there is a short data-drop.
- **RX Data Source** – This box shows the actual traffic stream from either the master link (main) or slave link (backup) currently running on the master unit.
- **Backup Stream** – This box is used to show that the main and backup streams are aligned at the master unit during normal system operation. The aligned status is shown when the master Modem is synced. This status loses relevancy if the master IDU drops out of sync with the Modem.
- **Packet MUX Sync** – This box displays actual Packet MUX synchronization at the master and slave unit. Packet MUX synchronization at the master side must report as OK for correct protection operation, even if the master IDU's drops out of sync with the modem.
- **Fiber Optic Sync** – This parameter shows the actual Fiber Optic connection status between the master and slave unit.
- **ODU TX Mute** – A muted or unmuted status indicates whether the appropriate ODU transmitter is active (unmuted) or in standby/non-functional mode (muted).
- **Device Status** – This value shows the alarm status for the appropriate units.

4.3.2. Aggregation Configuration Settings

Availability of the settings on the **Aggregation** configuration page primarily depends on the selected configuration type and the available license key (see Section 4.8.6). When the Aggregate 2+0 configuration is selected and the same design is supported in the license file, then the general aggregation configuration can be managed from the web GUI using the **General** tab **Aggregation** side-bar as shown in Figure 4-3.

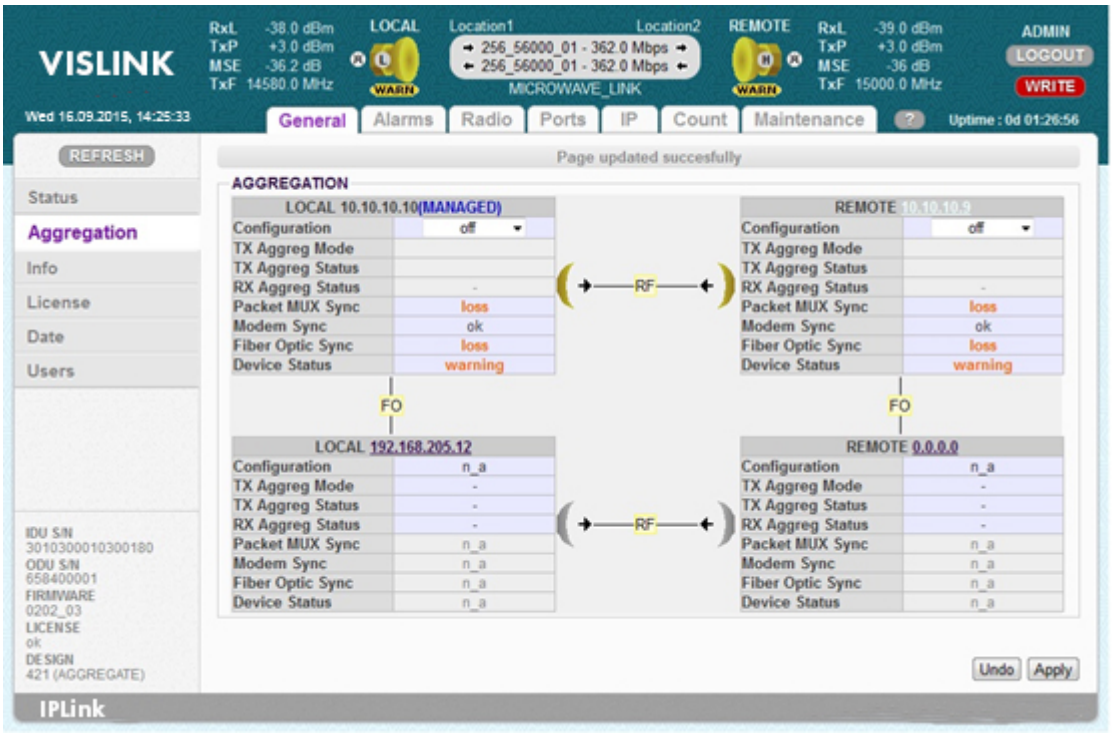

Figure 4-3 Initial Aggregation Configuration – GUI Page

The **Aggregation** configuration defaults to **off** if any change is made to the default settings. This default selection prevents any possible settings mistakes, such as radio interferences, port loopbacks etc.

NOTE: You should set all Radio, IP and Port parameters according to the prepared system configuration and configure **Aggregation** as the last step in the systems configuration procedure.

The GUI's graphical antenna icons (RF) are used as an aid helping you to understand the actual state of the IDU and whole link state (green = no alarm).

The following describes the particular setting and display boxes:

Configuration – This drop-down menu shows and selects actual / configured aggregation mode. To ensure correct system interconnection at both local, remote and neighboring units once the settings are entered, we recommend setting the required protection mode at the MASTER SIDE. The slave units will automatically inherit settings.

The possible modes are:

- ***master/2+0*** – This mode configures the master mode for the aggregation configuration, when two transmitters and two receivers operate on two different carrier frequencies. It also allows a cross-polar configuration in a specific case for the aggregation configuration scheme (contact your local representative for more details). This aggregation mode controls the aggregation process on both units.
- ***slave/2+0 –*** This mode configures the slave mode for the aggregation configuration. This aggregation mode uses the highest priority channel ETH 4 to transmit data over a slave link.
- ***off –*** This mode disables the Aggregation function. This mode functions similarly to the MULTI configuration, except it uses only three channels over air.
- **TX Aggreg Mode** – This drop-down menu sets the specific Tx Aggregation modes. The possible modes are:
  - ***auto*** – The TX data stream is automatically divided into two links according to the momentary available capacity of each link.
  - ***master only*** – Aggregation is disabled in this mode. The Tx data stream is manually directed to the master link only.
  - ***slave only*** – Aggregation is disabled in this mode. The Tx data stream is manually directed to the slave link only.
- **TX Aggreg Status –** This box shows the actual TX status; this is important for auto aggregation mode. In this mode the aggregation block automatically decides what direction to use for Tx data transmission:
  - ***aggregate –*** Data is transferred over both links (normal mode).
  - ***master only –*** Data is transferred over the master link (slave link is down or in an error mode or the mode is manually set to master only).
  - ***slave only –*** Data is transferred over a slave link (the master link is down or in an error mode or the mode is manually set to slave only).
- **RX Aggreg Mode** – This box displays the status for the receiver in an aggregation block:
  - ***ok –*** The receiving block operates properly, both traffic directions are aligned.
  - ***alignment drops –*** Incorrect order of packet is detected at the receiving side. This status indicates an abnormal packet delay at the master or slave link.
  - ***packet discards –*** This status indicates packet losses at the master or slave link.
- **Packet MUX Sync** – This box displays the actual Packet MUX synchronization status at the master and slave unit.
- **Fiber Optic Sync** – This parameter shows the actual Fiber Optic interconnection status between master and slave unit.
- **Device Status** – This value shows the alarm status for the relevant unit.

4.3.3. Basic Link Info

We recommend filling-in the table with the complete link identification. This information will be useful at the next step of the system description. This configuration is accessible from the Web GUI page **General** tab usign the **Info** side-bar as in Figure 4-4.

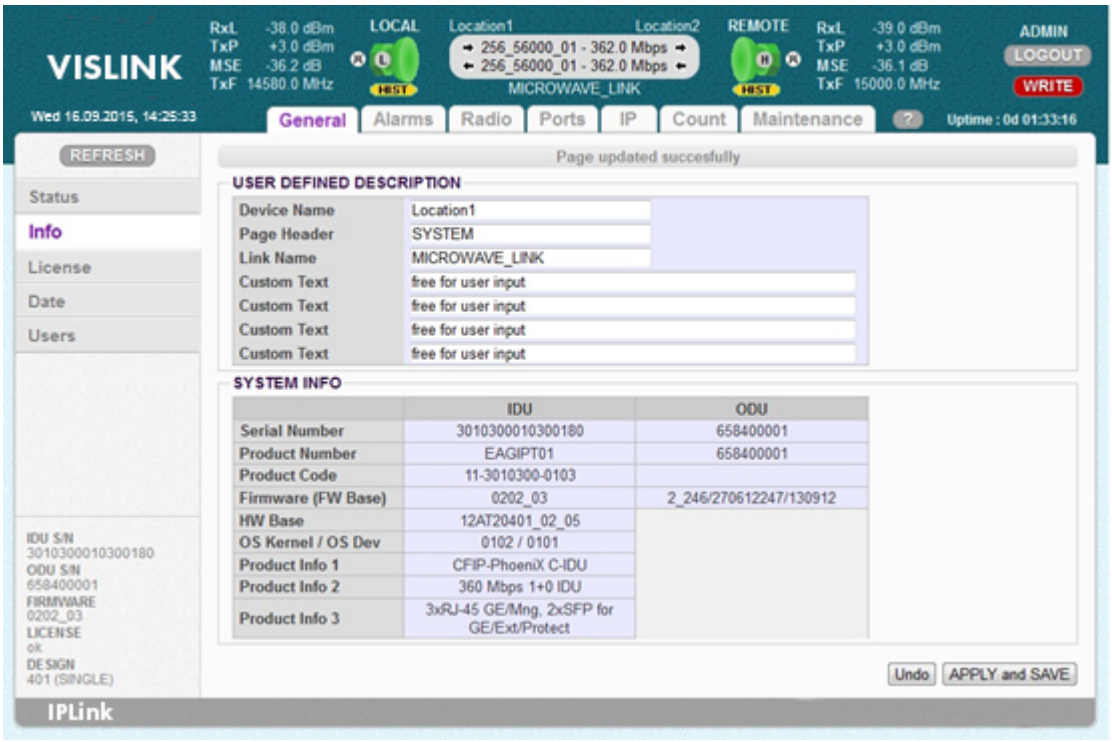

Figure 4-4 Wireless Link Info – GUI Page

The information available on the **Info** side-bar, via the **General** tab displays basic system identification information like IDU/ODU Serial Numbers, Product Numbers, Firmware Specification etc.

The description of the particular settings and display boxes are:

Device Name – This text is displayed in the GUI header for identification of the unit. The same name is used as a prompt in CLI. Maximal length is 13 characters.

Page Header – This text is used in the WEB browsers bookmarks for better identification for the unit currently being managed. The maximum length string is 25 characters.

Link Name – This text is displayed in the GUI header for accurate identification of the managed link. The same name should be entered at both sides of the microwave link. The maximum length string is 25 characters.

Custom Text – Up to four user specific descriptions can be entered. Maximum string length is 80 characters per row.

NOTE: All settings from this page are saved directly to the start-up memory, this is common for all alternative configurations W0-W3.

4.3.4. Date and Time

We recommend accurately setting the Date and Time information on all IDU units within the microwave network. This is especially helpful for alarm events and log analysis. This configuration is accessible from the web GUI page **General** tab using the **Date** side bar as in Figure 4-5.

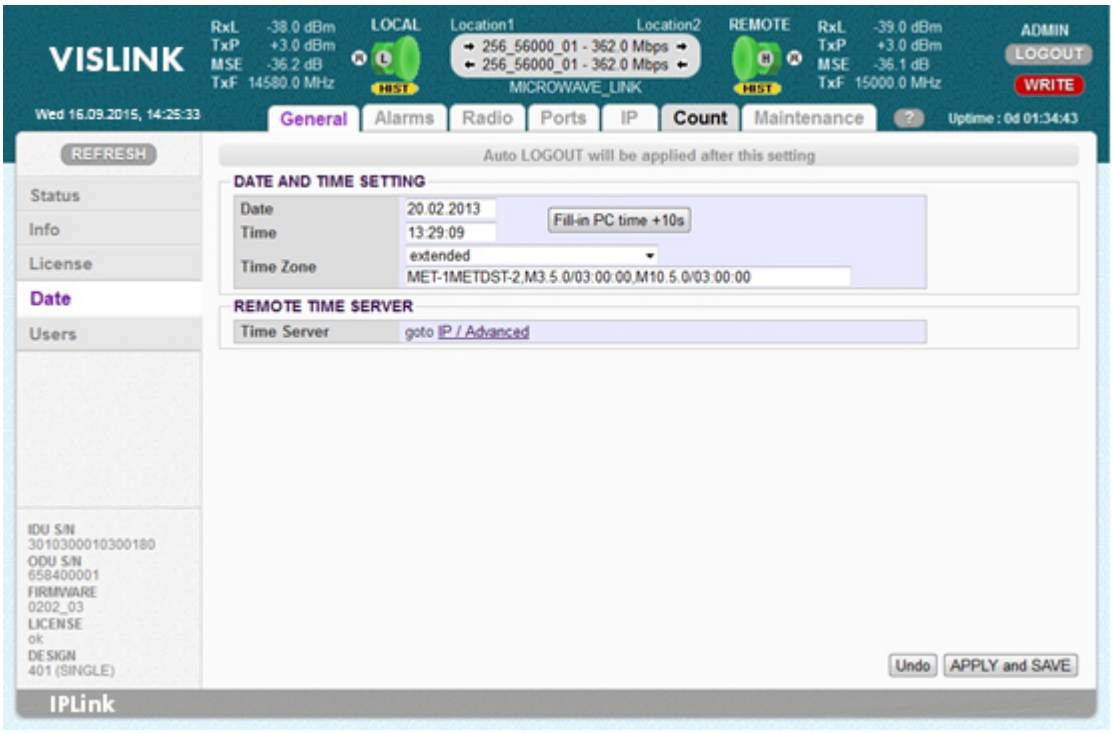

Figure 4-5 Date and Time Specification – GUI Page

Description for setting and display boxes:

- **Date** – Actual date.
- **Time –** Actual time.
- **Time Zone** – Selection of the local Time Zone from the drop-down menu.
- **Fill-in-PC Time +10s** – Click this button to increase the actual PC time by 10 seconds. This value is entered into Date and Time boxes. A 10 second offset is used, because the time setting is applied before the **APPLY and SAVE** button is clicked.
- **Time Server** – This setting is part of the IP configuration, this activates together with other IP parameters. When the Time server option is selected, the Date and Time are synchronized from an external source.

4.3.5. Access Rights

You are required to be logged in to the system to be able to locally and remotely monitor and manage the IPLink-SM microwave link. The relevant access rights are automatically granted to the user independently of your login level (after entering a Login and a Password). This affects the scope of the management capabilities for the microwave link. These login levels must be respected no matter if you access it from the web interface or from a Telnet, SSH or SNMP connection.

If you require access into managed networks, we recommend changing the default usernames and passwords to use your own secure usernames and password. These

configuration options are available via the web GUI page using the **General** tab and **Users** side-bar as in Figure 4-6.

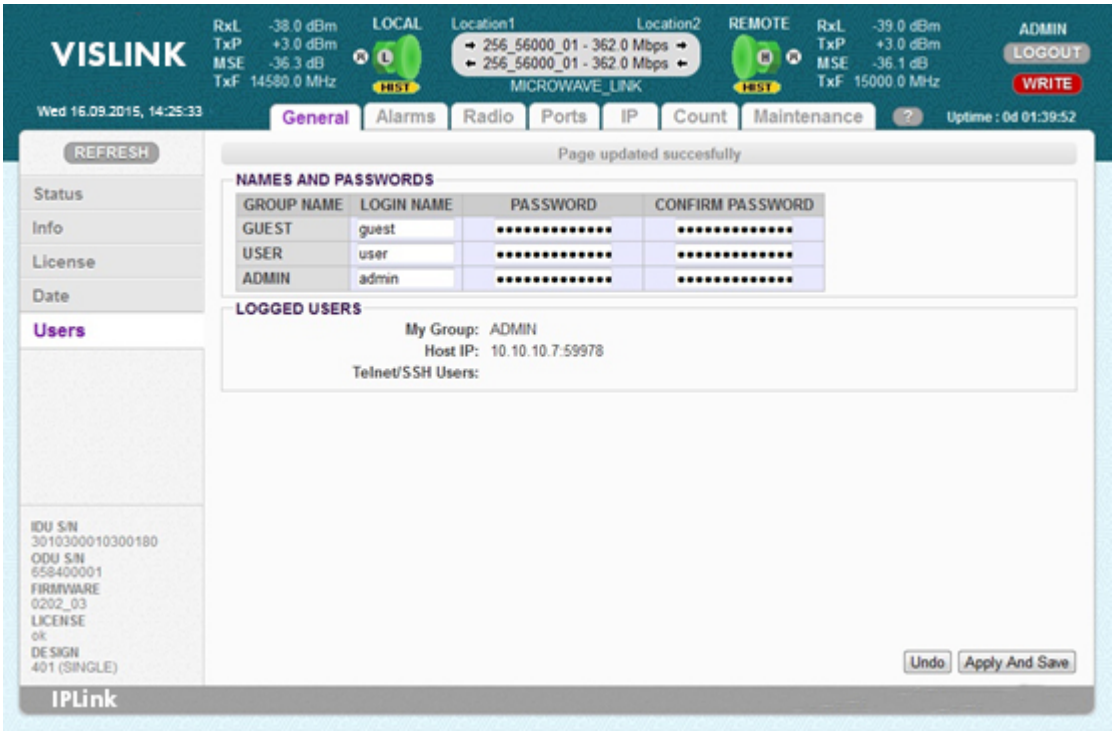

Figure 4-6 Access Level Settings

Each of the three possible login modes has different rights for system management.

The following Login and Password field details are factory defaults:

- GUEST: guest
- USER: user
- ADMIN: admin

Guest - Login with the user name "***guest***" and leave the password field blank (no password required).

In this basic user mode, you can monitor the traffic on the microwave link, monitor the quality of the frequency tuning, read out the values from the equipment (TxPower, etc.), clear some counters etc. Up to a maximum of three user-level users can be logged in to the system at a time.

User - Login with the following credentials:

- User name = ***user***
- Password = ***test***

The User-level user has the same rights as the Guest user with extended rights to configure and set the microwave link parameters. Only one user-level user can be logged in to the device at a time. However, up to three guest users can be logged in at the same time to monitor the system.

If a User-level user attempts to log on the system when an Administrator is already in the system, an alert window shows "***The user ADMIN is already logged in***" and the log aborted.

Administrator - Login with the following defaults:

- User name = ***admin***
- Password = ***secret***

An Administrator-level user has the same rights as a Guest- and User-level user. However, logging in as an Administrator provides additional rights to perform actions such as:

- Uploading new firmware to the equipment.
- Controlling the database of users.
- Manage/change user names and passwords.

An Administrator is classed as a super-user. When an Administrator tries to logon to the system and a standard user is already logged in the system, an alert window asks if the Administrator wants to log the User out. This because only one of the two types of user can be logged in at a time.

An Administrator-level user controls each group to manage/change the log on details from the default, factory-set values.

The following shows the allowed configuration for User names and passwords:

- **LOGIN NAME** – 1-12 characters
- **PASSWORD** – 1-15 characters

The valid characters are letters, numbers and special symbol "_".

Login names must be different for each access right group.

NOTE: All settings from this page are directly saved to a specific start-up memory which is common for all alternative configurations W0-W3.

4.4. Alarm Configuration

A proper alarm configuration helps to effectively solve potential troubleshooting events and/or disclose any system instability. From a configuration point of view, the most important alarm settings are available from the web GUI page from the **Alarms** tab **Config & Status** side bar.

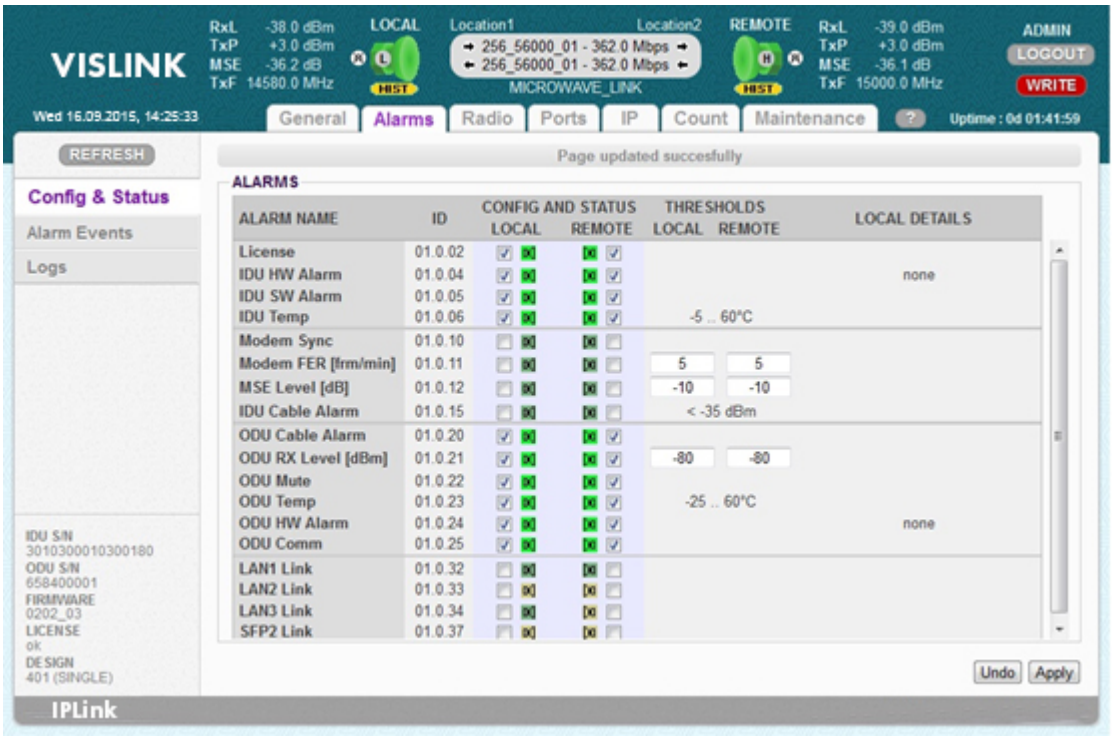

Figure 4-7 Alarms Setting – GUI page

4.4.1. Config and Status

This web GUI page stores the configuration table where it is possible to change the modes.

You can activate individual alarm IDs, which then influence the IDU status. If this feature is configured in IP settings, then when activated, the alarm ID generates an alarm event, this event is passed to the internal alarm log file and passes a trap message to the SNMP. When a single warning alarm ID is activated, the whole IDU reports a warning status. Alarms are highlighted by a yellow colored local unit icon, located at the top of each GUI page.

The alarm ID is activated on a system level (both to local and remote units) from the managed unit.

Setting up solid alarm threshold values for specific alarm IDs allows the system to compare the actual values to the alarm threshold level values, allowing it to monitor and alert you to any issues.

You can check the status of alarms from the GUI page, which monitors the alarm status for both active and inactive alarm IDs.

The system uses different colored icons for each alarm to help you to quickly understand the status for the appropriate alarm ID:

Icon	Description
	The Green icon indicates that the alarm ID is activated (monitored) without any alarm status detected.
	The Dark Green icon indicates that the alarm ID is inactivate and no alarm status is detected.
	The Yellow icon indicates that the alarm ID is activated (monitored) and a warning status is detected.
	The Dark Yellow icon indicates that the alarm ID is not activated but a potential warning status is detected.

Table 4-1 Alarm Icon ID Table

4.4.1.1. IDU System Alarms

The **Alarms** tab and **Config & Status** side-bar page stores the configuration table where it is possible to change the following modes:

License Alarm – ID 01.0.02 (critical). This alarm ID indicates actual license status:

- No alarm = License OK.
- Warning = License is in blocked or remote_violation status.

Protection Alarm – ID 01.0.03. This alarm ID indicates actual protection status:

- No alarm = Protection parameters (Rx Data Source and Backup Stream) are in normal status (Rx Data Source=Main, Backup Stream=aligned).
- Warning = One or more protection parameters are in abnormal state.

IDU HW Alarm – ID 01.0.04 (critical)

This alarm ID indicates the actual status of the IDU HW (hardware). The explicit reason for such a HW alarm event is then described in column **LOCAL DETAILS** in the GUI:

- No alarm = all internal HW blocks work properly.
- Warning = one or more internal HW blocks indicate abnormal function.

IDU SW Alarm – ID 01.0.05 (critical)

This alarm ID indicates actual status of IDU SW (software):

- No alarm = all internal SW blocks work properly.
- Warning = one or more internal SW blocks indicate abnormal function.

IDU Temp Alarm – ID 01.0.06

This alarm ID indicates the actual status of the IDU temperature:

- No alarm = Actual temp. is in the range of -5 up to +60°C.
- Warning = Actual temp. is out of range of -5 up to +60°C.

4.4.1.2. IDU Modem and MUX Alarms

Modem Sync Alarm – ID 01.0.10 (critical)

This alarm ID indicates the actual status of modem synchronization:

- No alarm = Modem synchronized.
- Warning = Modem sync loss.

Modem FER Alarm – ID 01.0.11

This alarm ID indicates the status of the modem frame (air-frame) error rate in the last 60 seconds, with respect to the configured threshold:

- No alarm = Actual modem FER value is lower than the FER threshold defined in the same alarm row.
- Warning = Actual modem FER value is higher or equal to the FER threshold defined in the same alarm row.

MSE Level Alarm – ID 01.0.12

This alarm ID indicates the actual modem MSE value in dB with respect to configured threshold:

- No alarm = Actual MSE value is lower than the MSE threshold defined in the same alarm row.
- Warning = Actual MSE value is higher or equal to the MSE threshold defined in the same alarm row.

MUX Sync Alarm– ID 01.0.13 (critical)

This alarm ID indicates actual status of packet processor (PBPS) synchronization:

- No alarm = PBPS synchronized.
- Warning = PBPS sync loss.

MUX FER Alarm – ID 01.0.14

This alarm ID indicates the status of the packet processor frame (PBPS frame) error rate in the last 60 seconds with respect to configured threshold:

- No alarm = Actual PBPS FER value is lower than the FER threshold defined in the same alarm row.
- Warning = Actual PBPS FER value is higher or equal to the FER threshold defined in the same alarm row.

IDU Cable Alarm – ID 01.0.15 (critical)

This alarm ID indicates actual status of IF level at the IDU input:

- No alarm = Actual IDU IF level (at 140MHz) is higher than -35dBm.
- Warning = Actual IDU IF level (at 140MHz) is lower or equal to -35dBm.

4.4.1.3. ODU Alarms

ODU Cable Alarm – ID 01.0.20 (critical)

This alarm ID indicates the actual status of IF level at the ODU input:

- No alarm = Actual ODU IF level (at 350MHz) is within the defined specified range.
- Warning = Actual ODU IF level (at 350MHz) is out of the defined specified range.

ODU RX Level Alarm – ID 01.0.21

This alarm ID indicates the status of the received RF level at the ODU receiver compared to the configured threshold:

- No alarm = Actual ODU Rx Level is higher than the Rx Level threshold defined in the alarm row.
- Warning = Actual ODU Rx Level is lower or equal to the Rx Level threshold defined in the alarm row.

ODU Mute Alarm – ID 01.0.22

This alarm ID indicates the actual ODU Mute status:

- No alarm = ODU is unmuted (auto unmute).
- Warning = ODU is muted (auto mute or manual mute).

ODU Temp Alarm – ID 01.0.23

This alarm ID indicates the actual status of the ODU temperature:

- No alarm = Actual temp. is in the range of -25 up to +60°C.
- Warning = Actual temp. is out of the range of -25 up to +60°C.

ODU HW Alarm – ID 01.0.24 (critical)

This alarm ID indicates the actual status of ODU HW (hardware). Explicit reason for such HW alarm event is then described in the column **LOCAL DETAILS** via the web GUI:

- No alarm = all internal HW blocks are working properly.
- Warning = one or more internal HW blocks are reporting abnormal function.

ODU Comm Alarm – ID 01.0.25 (critical)

This alarm ID indicates incorrect or missing communication between the local IDU and the local ODU:

- No alarm = IDU-ODU communication is ok.
- Warning = IDU-ODU communication failure.

4.4.1.4. Interface Alarms

LAN 1 Link Alarm – ID 01.0.32

This alarm ID indicates the actual status of the link at LAN 1 port:

- No alarm = Link OK at port LAN 1.
- Warning = NO Link at port LAN 1.

LAN 2 Link Alarm – ID 01.0.33

This alarm ID indicates the actual status of the link at LAN 2 port:

- No alarm = Link OK at port LAN 2.
- Warning = NO Link at port LAN 2.

LAN 3 Link Alarm – ID 01.0.34

This alarm ID indicates the actual status of the link at LAN 3 port:

- No alarm = Link OK at port LAN 3.
- Warning = NO Link at port LAN 3.

SFP 1 Link Alarm – ID 01.0.36

This alarm ID indicates the actual status of the link at SFP 1 port:

- No alarm = Link OK at port SFP 1
- Warning = NO Link at port SFP 1.

SFP 2 Link Alarm – ID 01.0.37

This alarm ID indicates the actual status of the link at SFP 2 port:

- No alarm = Link OK at port SFP 2.
- Warning = NO Link at port SFP 2.

4.5. Radio Configurations

4.5.1. Basic Radio Settings

The basic radio configuration is available via the web GUI using the **Radio** tab and **Parameters** side-bar. Parameters for both local and remote units can be set together in one configuration step when the appropriate boxes are edited for local and remote units (see Figure 4-8).

The configuration window is divided into three columns: LOCAL, REMOTE and LOCAL RANGE. The values in the LOCAL column are valid parameters for the local unit. Likewise, the values in the REMOTE column are for the remote side configuration (when communication with remote side is in operation). LOCAL RANGE column states the range of the applicable values, if such limitations exists for specific parameters.

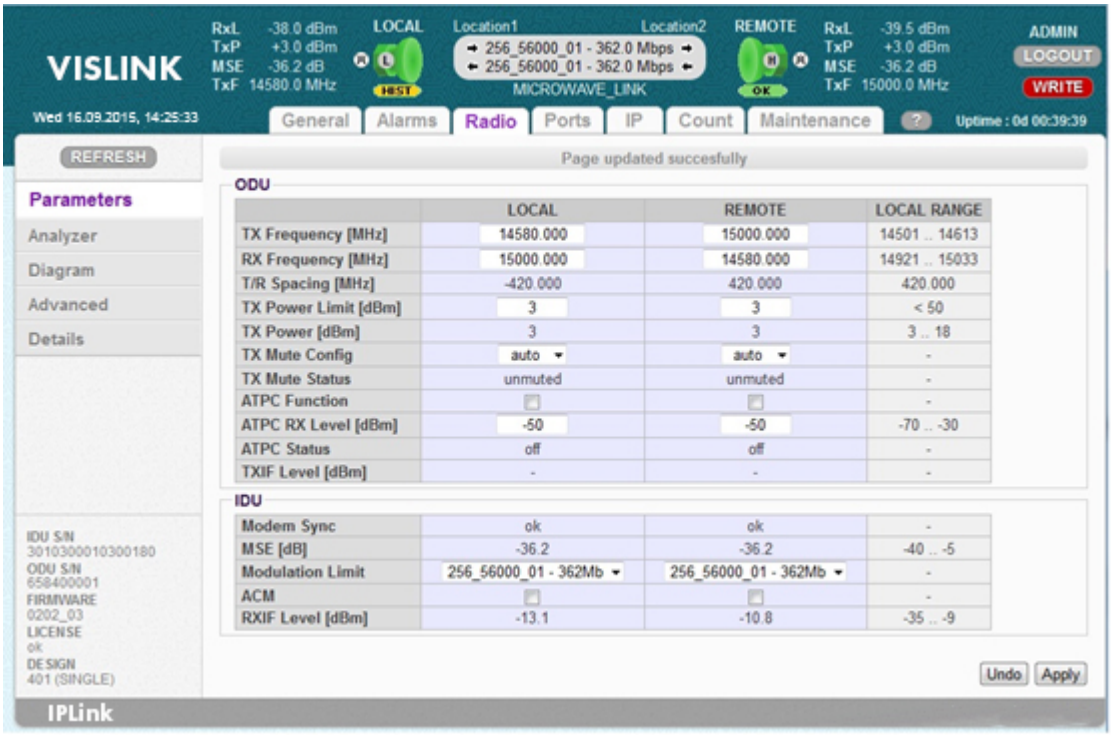

Figure 4-8 Radio Parameters Setting – GUI Page Radio / Parameters

Description for settings and display boxes:

- **TX Frequency –** The transmission frequency can be set within the displayed frequency range in accordance with concrete ODU sub band specification (read from the connected ODU). The displayed range is the edge to edge flat diplexer frequency scope and therefore respective Tx Frequency value within that scope must be increased or decreased by one half of the used modulation bandwidth, if that value is near these edges.
- **RX Frequency** – Receive frequency is usually set automatically because the majority of ODUs operate with the fixed T/R spacing. For specific ODUs, where the RX Frequency can be set independently, you can set this value.
- **T/R Spacing** – TX and RX frequency distance is a real calculated value of this parameter. There is a displayed standard ODU T/R spacing in the column **LOCAL RANGE**.
- **TX Power Limit** – The maximum transmission power parameter defines the maximum power level required for optimal transmission conditions. The operating TxPower then depends on the following:
  - Configured ATPC values
  - ODU limit which depends on the used RF band and selected modulation.
- **TX Power** – The output RF power level transmitted from the ODU. The **LOCAL RANGE** column displays the TX Power scope used by the ODU under actual conditions (band, modulation).
- **TX Mute Config** – Transmitter mute configuration. Two modes of this parameter can be selected. Mute mode is selected for fixed ODU mute configuration. Auto mute mode is the standard selection for this parameter. In that case an ODU is automatically muted when abnormal transmission conditions are detected by the IDU or ODU:

- Initial TX Frequency is outside the available range.
- ODU cable alarm.
- Specific protection mode.

- **TX Mute Status** – Actual transmitter mute status.
- **ATPC Function** – Automatic Transmit Power Control enables or disables the ATPC feature. The transmitted power is automatically adjusted to ensure that the optimum RxLevel (ATPC RxL) is received at the remote terminal (hitless regulation).

NOTE: The ATPC function should be always OFF during installation.

- **ATPC RX Level** – Required level for Automatic Transmit Power Control. Field specifies the optimal receive level used for ATPC function.
- **ATPC Status** – Status of ATPC loop:
  - ***off –*** indicates that ATPC function is disabled.
  - ***ok –*** indicates that ATPC loop has regulated required level.
  - ***out of range –*** indicates that ATPC loop cannot reach the required level.
- **TXIF Level** – Transmit IF level at ODU input (350 MHz) indicates the signal strength of the IF input in to the ODU. This level should be in the range of 0 dBm up to -30 dBm (low signal). By standard the output TXIF level from the IDU is 0 dBm. It is useful to check this value if it corresponds to the calculated cable attenuation.
- **Modem Sync** – Demodulator synchronization status is the basic indicator of proper function of IDU receiver.
  - ***ok*** – Indicates that demodulator is synchronized with received air-frame.
  - ***loss*** – Indicates that demodulator is not synchronized with received air-frame.
- **MSE** – Mean Square Error is a basic indicator of the quality of signal. The used MSE value is a normalized presentation of the MSE value. The absolute value can be presented as signal to noise ratio when the demodulated signal is close to the threshold level. The lower the value, the better the signal. The parameter is usually in the range of -10 dB to -40 dB. If **Modem Sync** is not displaying as ***ok***, then the MSE parameter may display some unpredictable values.
- **Modulation Limit** – Optimal modulation scheme selects either a fixed modulation scheme for **non-ACM** mode or defines the highest modulation scheme, which can be used in **ACM** mode.
- **ACM** – Automatic Change of Modulation. When this mode is selected then the hitless switch-over is permitted among several modulation schemes. This depends on actual MSE level. The IDU can automatically work in all modulation schemes lower than or equal to the modulation scheme defined in the **Modulation Limit** parameter.
- **RXIF Level** – Received IF level at IDU input (150 MHz) indicates the signal strength of the IF input into the IDU. This level should be in the range of -10 dBm up to -35 dBm (low signal). As standard, the output RXIF level from the ODU is -10 dBm. It is useful to check this value if it corresponds to the calculated cable attenuation.

The modulation scheme settings and the channel bandwidth can especially affect the final data rate (data throughput) and sensitivity (link distance) of the microwave link. Generally speaking, the narrower the bandwidth and the lower the modulation the lower the data rate, but greater the sensitivity (see the Technical Specification document).

Depending on the type of supplied license (limit for maximum data rate) the modulation type can be changed (type of modulation can be set / changed up to a maximum transmission capacity). The microwave link can be ordered with different licenses in accordance with actual price list and business policy. The transmission capacity can be changed in the range of 10 Mbps up to a maximum supplied license for data rates 365 Mbps for 1+0 mode.

A time-restricted license is available. This limits the microwave link for a limited period of time and allows it to be used with a higher data rate/type of modulation e.g. for temporary testing. After the expiration of this period the maximum type of modulation is automatically downgraded to the default modulation, depending on your license type. The user data transmission capacity is disabled (0 Mbps). It does not affect the out-of-band management channel.

The modulations are named according to the combination of the following parameters. The overall Capacity – real data throughput is written behind the modulation code. The modulation name code is described in the next example.

Example: 256_56000_01

- **256 –** code for 256 QAM**,** other possibilities are 4/8/16/32/64/128/256
- **56000** – code for 56 MHz BW, other possibilities are 07000, 10000, 14000, 20000, 27500, 28000, 30000, 40000, 50000, 56000, 60000
- **01** – it is code for modulation version

Any changes are confirmed by clicking the **APPLY** button. All the basic parameters can be configured for the local and remote terminal from this page when the proper connection is established. Save all changes and configurations by clicking the **WRITE** button.

4.5.2. Advanced Radio Settings

The Advanced Radio configuration window provides extended radio parameters settings which are usually required for maintenance and operation purposes. These settings are available via the web GUI page using the **Radio** tab and **Advanced** side-bar (see Figure 4-9).

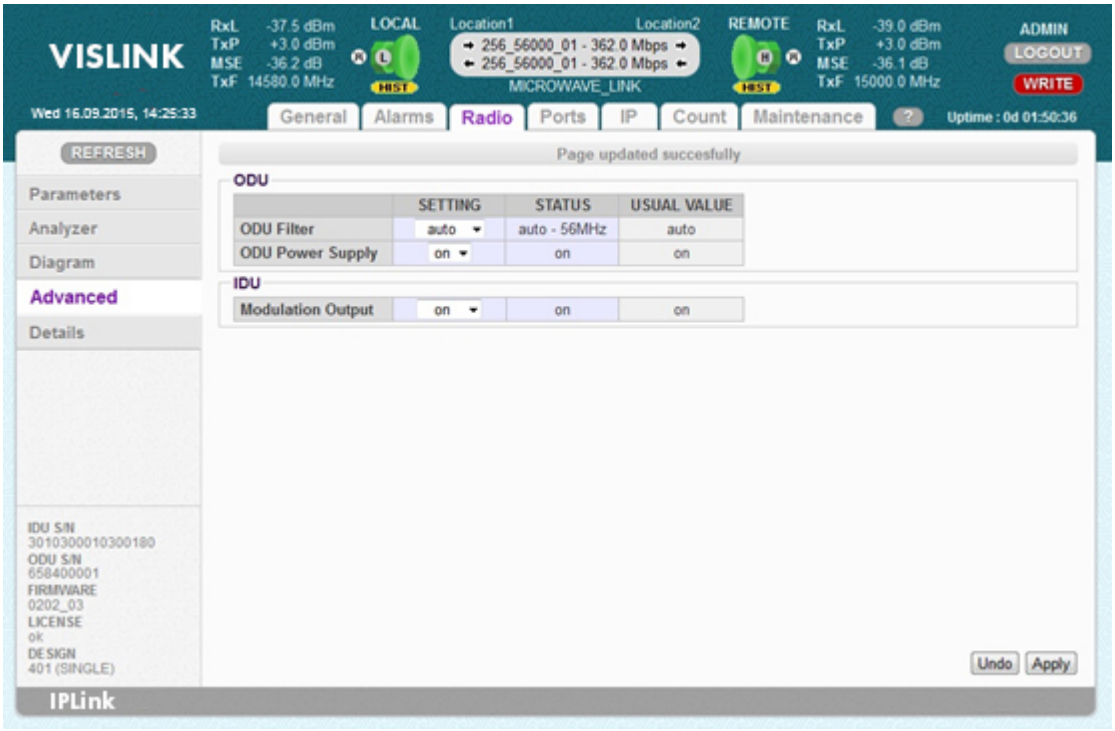

Figure 4-9 Radio Parameters Setting

Description of the setting and display boxes:

- **ODU Filter** – it is possible to change integrated filter inside IDU by means of this drop-down menu. The possible modes are as follows:
  - ***auto* –** Filter is selected automatically according to the modulation BW (default).
  - ***narrow*** – Manually selected the ODU narrow filter.
  - ***wide*** – Manually selected the ODU wide filter.

NOTE: A solid filter width for narrow or wide mode depends on the ODU type used. A wideband ODU uses 30 MHz / 60 MHz filters for narrow / wide modes. A narrowband ODU uses 10 MHz / 30(40) MHz filters for narrow / wide modes.

- **ODU Power Supply** – It is possible to turn-off the power supply for the ODU by means of this drop-down menu. The start-up configuration (RUN W0) is initiated after switching from OFF to ON mode. Therefore, a data drop will be evident after this switch.
  - **on** - ODU is powered (default)
  - **off** - ODU is turned-off).
- **Modulation output** – You can replace the standard modulated signal with a carrier signal (CW) in this drop-down menu. The possible modes are:
  - ***on*** – TxIF modulated signal is present at the IF output from the IDU (default).
  - ***off*** – Carrier signal with a frequency of 350 MHz is presented at the IF output.

4.6. Port Configurations

By selecting a relevant configuration, you can select the management access type, traffic modification (number of independent channels over the air) and the protection / aggregation function preference. See Section 4.10.6 before starting any port settings. Each configuration type uses a different port configuration scheme according to the description in Section 4.7. The following should be done individually for each configuration type.

The internal ETH switch is divided into three groups by default. This setting prevents potential loopbacks at the connected LAN ports for all configurations, even though this configuration is not usual for a solid configuration type selection.

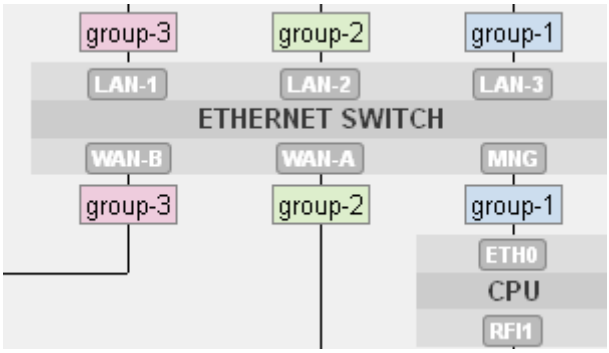

Figure 4-10 Default Configuration of Internal ETH Switch

4.6.1. Basic Port Settings –SINGLE Configuration

Port settings for the SINGLE configuration use the simplest configuration scheme, using the only independent traffic channel available for configuration. The internal ETH switch is divided into two separate groups:

- Group No.1 is reserved for management purposes (out of band type of management).
- Group No.2 is generally designated for traffic purposes (see Figure 4-10).

You can use up to three LAN ports (SFP 1, LAN 1, LAN 2) for traffic into the IDU with the maximum allocated speed for ETH traffic over the RF link.

Description of the setting and display boxes:

- **Status –** A graphical symbol describing the actual status of a particular LAN port (speed, duplex mode, link, administrative down status).
- **Mode** – This drop-down menu displays and defines the actual port mode (auto-negotiation on/off, speed/duplex, administrative down).
- **MDIX** – This allows you to set particular ETH cable crossing like auto / mdi /mdx by means of this configuration.
- **Flow control –** This setting manages the duplex flow control mechanism:
  - **off** – Flow control is disabled.
  - **on** – Flow control is enabled during auto-negotiation process.
  - **force** – Flow control is active, even if not supported.

- **Switch Settings** – This block illustrates the ETH switch fragmentation into groups and also their interconnection with the physical LAN ports and internal WAN ports. Group configuration is performed on the web GUI page **Ports** tab and **ETH VLAN** side-bar.
- **RFI Channels** – This describes the internal names for packet processor ports.
- **Speed Allocation** – This parameter can reduced the over-the-air speed for a particular packet processor channel. When the figure in this input box is higher than the value displayed in the row below (Available Speed) then the full capacity is reserved for this channel. The speed priority allocation goes from left to right.
- **Available Speed** – This parameter indicates the available speed for the appropriate channel. This value depends on the modulation scheme selected.
- **AES Encryption** – This line shows when the AES encryption block is enabled or disabled if supported with the running design and firmware.

NOTE: The AES Encryption option is not available for the SINGLE configuration.

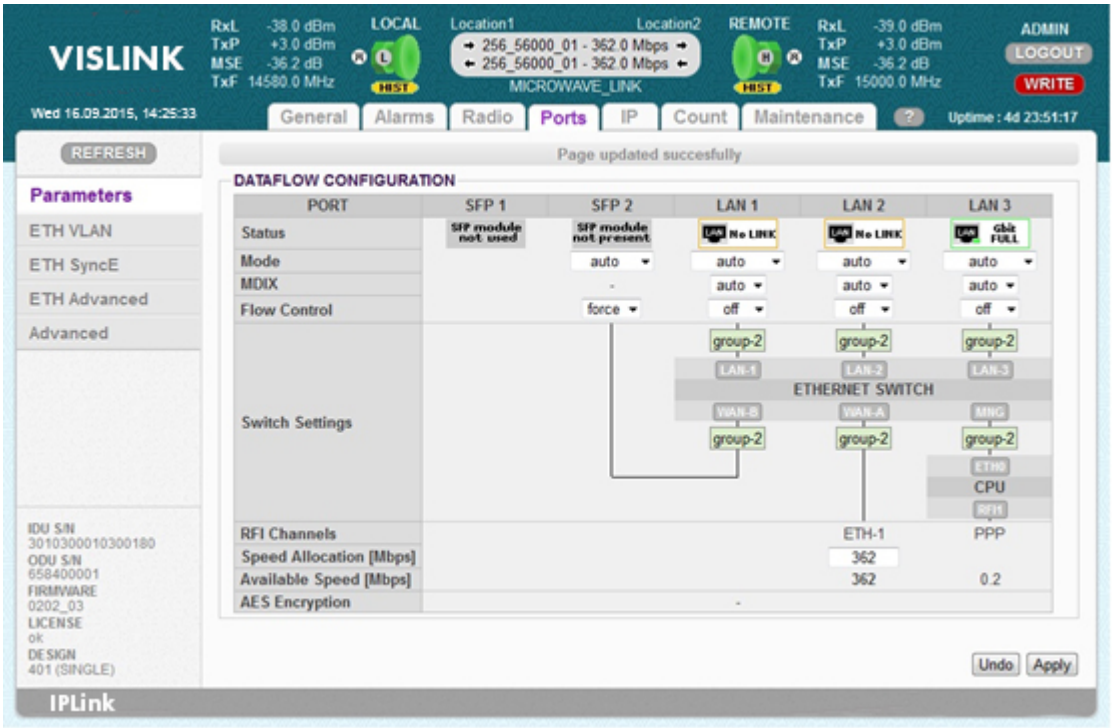

Figure 4-11 Port Settings - SINGLE Configuration

4.6.2. Basic Port Settings – MULT Configuration

Port settings for the MULTI configuration offer options to select up to four independent over-the-air traffic channels (Figure 4-12). The internal ETH switch is divided into three separate groups:

- Group No.1 is usually reserved for management purposes (out of band type of management).
- Group No.2 is designated for the first traffic channel (the lowest priority).
- Group No.3 is designated for the second traffic channel (higher priority).

The other two traffic channels are connected directly to the SFP PHYs, no ETH switch is part of the LAN interconnection. Traffic channel ETH 4 has the highest priority inside the packet processor structure.

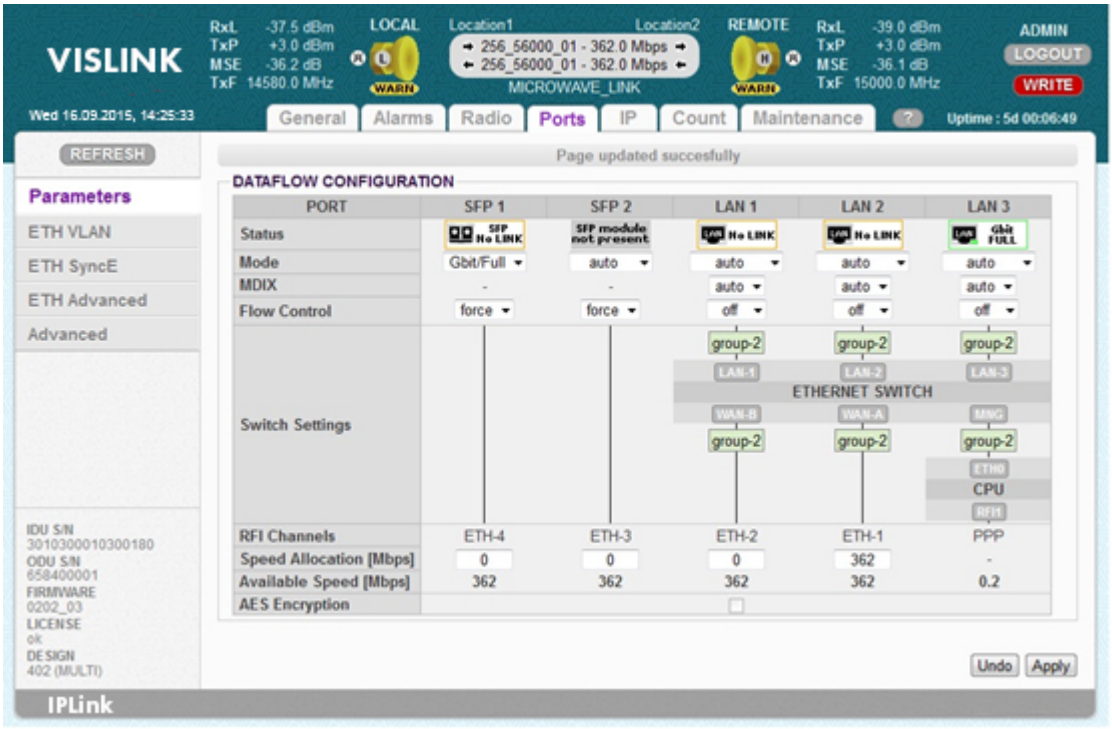

Figure 4-12 Ports Setting in MULTI Configuration

The Speed Allocation set-up is different in comparison with the SINGLE configuration. The overall allocated traffic capacity (the sum of all ports capacity) should be in the range for the speed available for the actual modulation scheme. When the adaptive modulation mode (ACM) is enabled, in order to switch to a lower level modulation scheme, you need to consider which lower priority channels do not need the free capacity allocation.

4.6.3. Basic Port Settings – PROTECTED Configuration

Port settings for the PROTECTED configuration are similar to the MULTI configuration function, except only three independent over-the-air traffic channels are available (see Figure 4-12). Port SFP 1 is reserved for the protection function (interconnection with a neighboring IDU).

There is also a difference between the master and slave units. All standard traffic ports (LAN 1, LAN 2, SFP 2) are automatically disabled (DOWN) at the slave unit (see Figure 4-13). This prevents multipath Ethernet loops. The same ports are also disabled when protection mode is configured into the **off** mode.

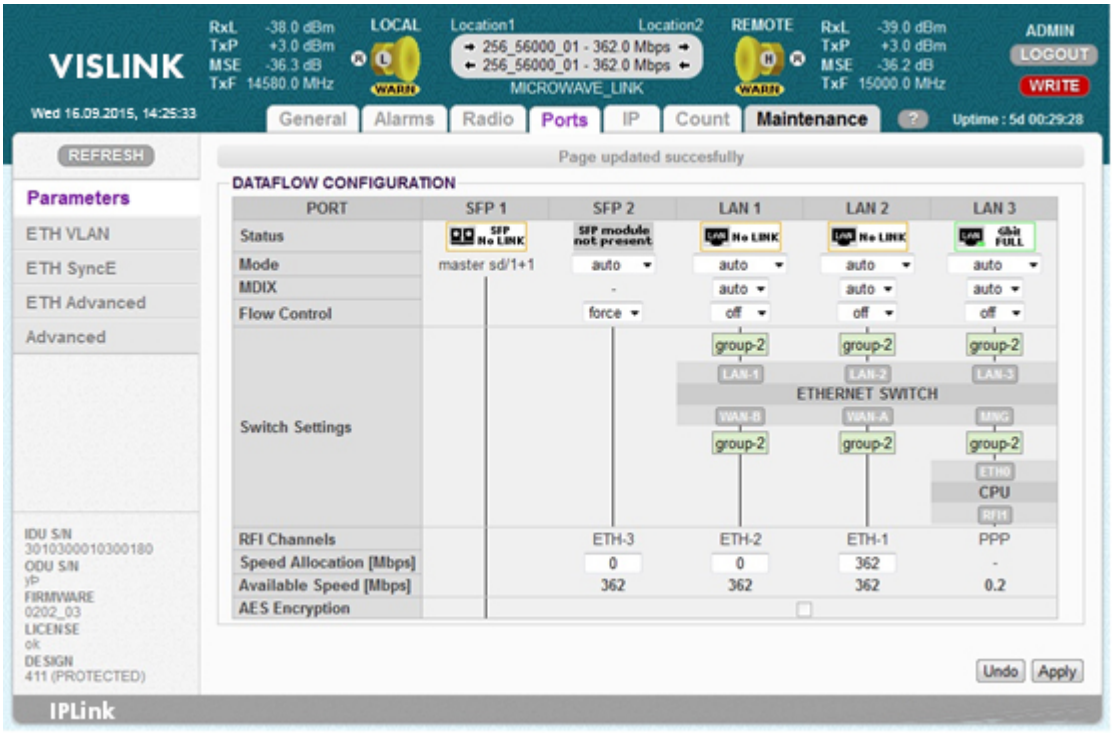

Figure 4-13 Ports Setting in PROTECTED Master Mode

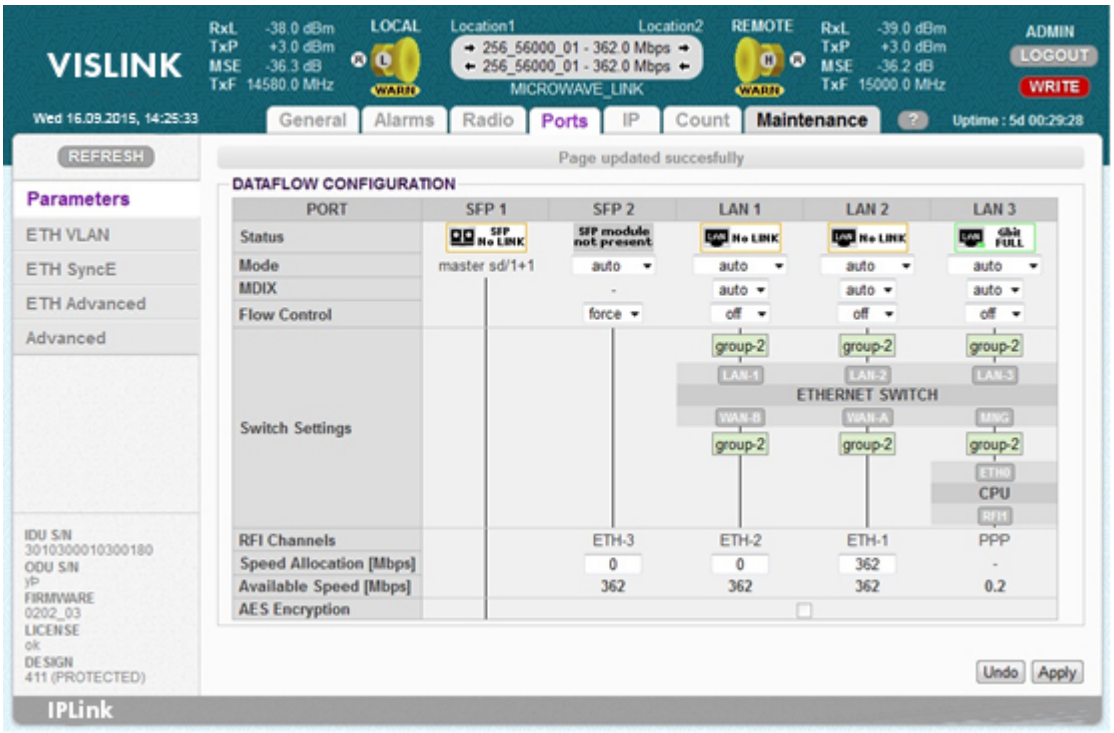

Figure 4-14 Ports Setting in PROTECTED Slave Mode

4.6.4. Basic Port Settings – AGGREGATE Configuration

Port settings for the AGGREGATE configuration are different for master and slave units. Traffic port SFP 1 and channel ETH-1 at the master unit are reserved for the aggregation function, the next two channels (ETH-2, 3) can be used for the next independent traffic stream (see Figure 4-15).

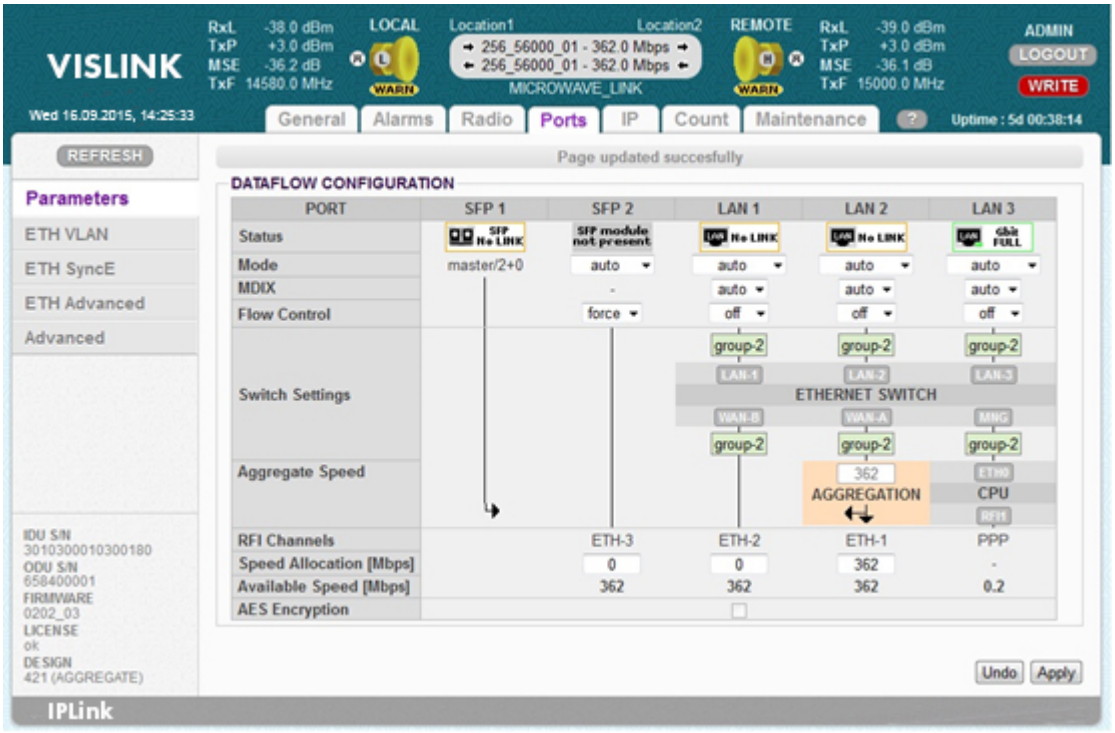

Figure 4-15 Ports Setting in AGGREGATE Master Mode

The channel ETH-4 at the slave unit is reserved for the slave aggregation stream (correct speed must be set), the rest of the ETH channels (ETH 1-3) are available for the next independent data sources.

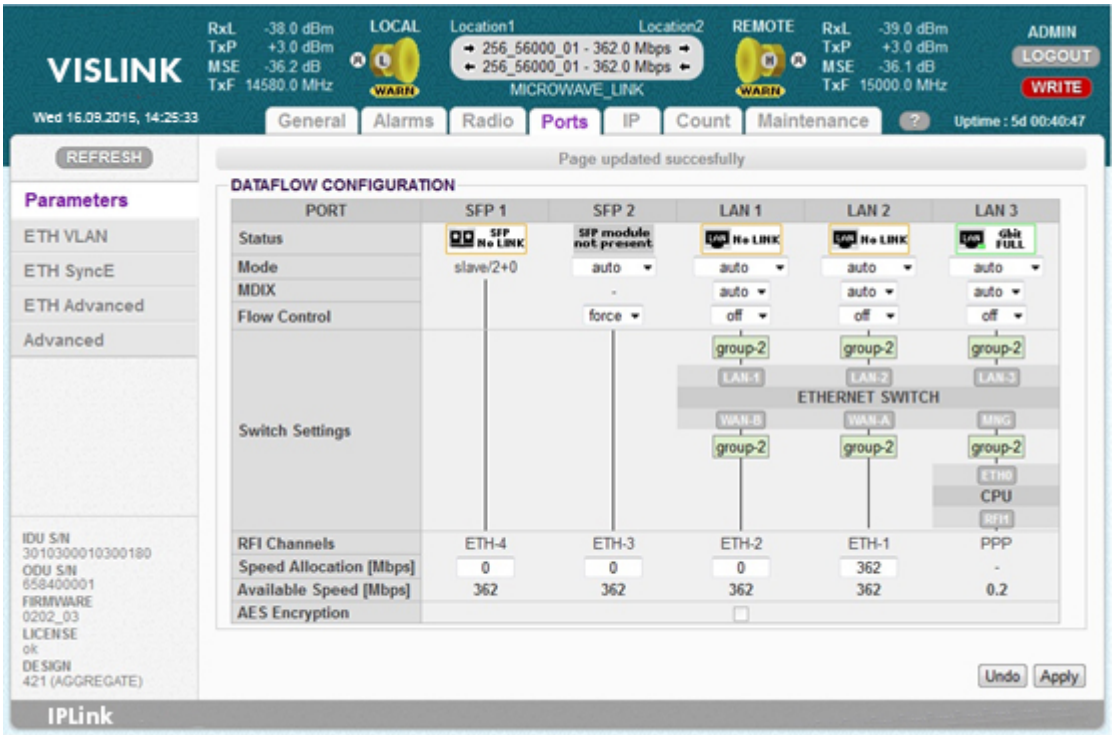

Figure 4-16 Ports Setting in AGGREGATE Slave Mode

4.6.5. ETH VLAN Settings

VLAN configuration is used to separate management traffic out from other customer data traffic. In some specific applications, it is useful to configure the ETH VLANs for customer traffic and filter input data traffic using this setting.

The VLAN configuration is available from the web GUI using the **Ports** tab **ETH VLAN** side-bar.

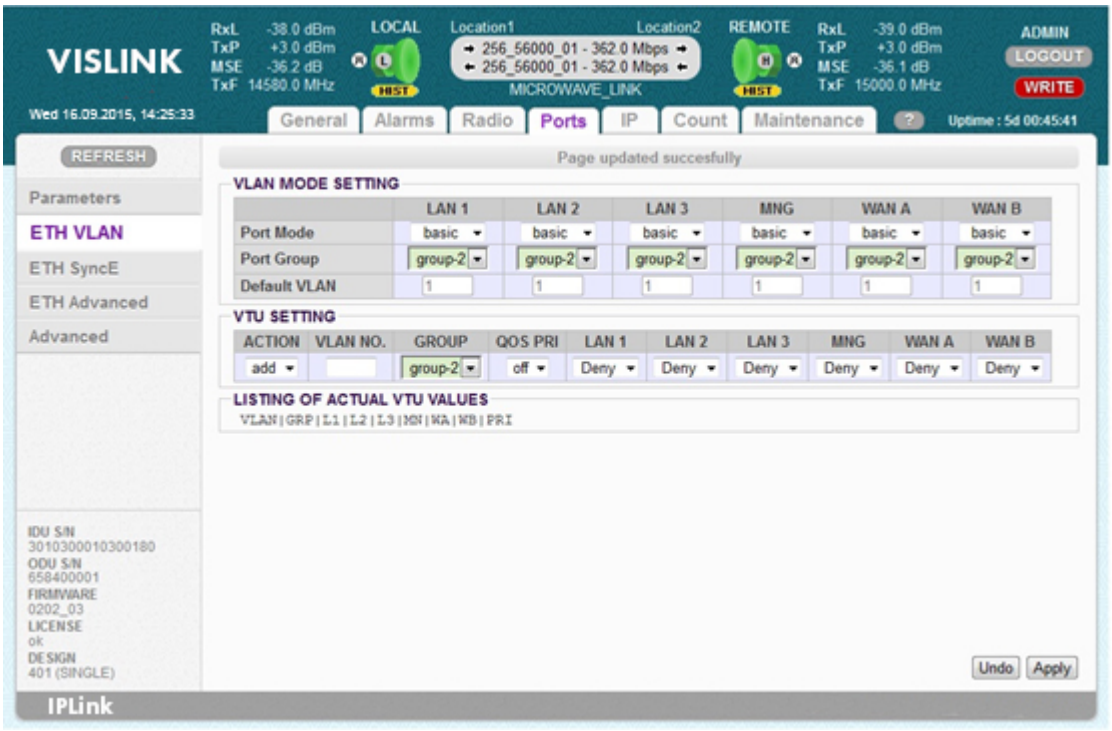

Figure 4-17 ETH VLAN Configuration Page

The following describes the setting and display boxes for VLAN MODE:

- **Port mode** – You can set-up the required VLAN mode separately for each ETH switch port. We recommend leaving all ports in basic mode, then edit VTU records first. You have to use the correct VLAN configuration and also have to set this network for identical VLAN support. VLAN Port modes are described below:
  - **basic** – Transparent mode where VLAN settings in the VTU table are ignored. Frames are transmitted unchanged, but only exit ports inside the same group.
  - **access** – The port is a member of just one untagged VLAN, the port is defined as “Default VLAN”. Only input untagged packets are accepted. The packets VLAN number (VID), assigned from port's Default VLAN, exist in VTU table. Frames are transmitted untagged and they are allowed to exit only via ports that are members of the frame's grouped VLAN.
  - **trunk** – The port can be a member of more tagged VLANs (VID extracted from VLAN tag) and one untagged VLAN defined as “Default VLAN” per port. Only frames with the same VLAN number are accepted (assigned from VLAN tag or port's Default VLAN). The VLAN tag exists in VTU table. The input port is a member of the VLAN. Frames are transmitted untagged or tagged according to the specification in the VTU record for each

port/VLAN, they are allowed to exit via ports that are members of the frame's VLAN from inside the same group.
  - **hybrid** – When the frame's VLAN number exists in the VTU table, the rules for trunk port are used, when the number does not exist, then the basic rules are applied.

- **Port Group** – This parameter defines a separate MAC address table domain inside the internal switch and defines the group of ports which can communicate to each other. Only the ports from the same group can communicate with each other. The other ports are completely isolated. It is possible that isolated networks (different groups) can use the same MAC addresses without collisions in the internal ETH switch ATU table.
- **Default VLAN** – This parameter is configured automatically with a new record into the VTU table. The default VLAN is updated for the port marked as untagged in the VTU record. VLAN No.1 cannot be added into VTU table and is seen as an emulated VLAN for internal purposes. When the default VLAN for this port is set as 1, the port cannot be configured into access mode. When the default VLAN value for the trunk port is 1, the port accepts only tagged frames.

Description for particular settings and display boxes – VTU SETTING

- **ACTION** – This adds or removes VTU records. The VTU record cannot be removed when it contains untagged ports configured for access mode. A simple VLAN NO. specification is required to erase a VTU record.
- **VLAN NO.** – The VLAN number for the edited VLAN (added or deleted). Every VLAN can only be defined for one Port Group. You can not name the same VLAN in multiple records or groups.
- **GROUP** – Defines the port Group for an individual VLAN.
- **QOS PRI** – When VTU override mode is selected, the QOS priority value of the original frame is overriden. This configuration influencees the internal frame processing by means of queue control (QPRI defined by OQPRI instead of IQPRI bits) frames are still output with the initial priority assignment (FPRI is not changed).
- **LAN 1-WAN B** – Defines the VLAN mode for each port in a configured VLAN.
- **Deny** – The port is not a member of the edited VLAN. Ports defined in different Groups should be set to this mode.
  - **Untag** – Port is a member of edited VLAN as untagged.
  - **Tag** – Port is a member of edited VLAN as tagged.

The description of particular setting and display boxes for VTU LISTING

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

4.6.6. ETH SyncE

Synchronous Ethernet mode is supported in SINGLE, MULTI and AGGREGATE configurations. This mode ensures the transmission of the timing reference, derived from a selected LAN port at the reference side of the link to the remote synchronized side of the same link. Figure 4-18 shows the configuration available on the GUI page.

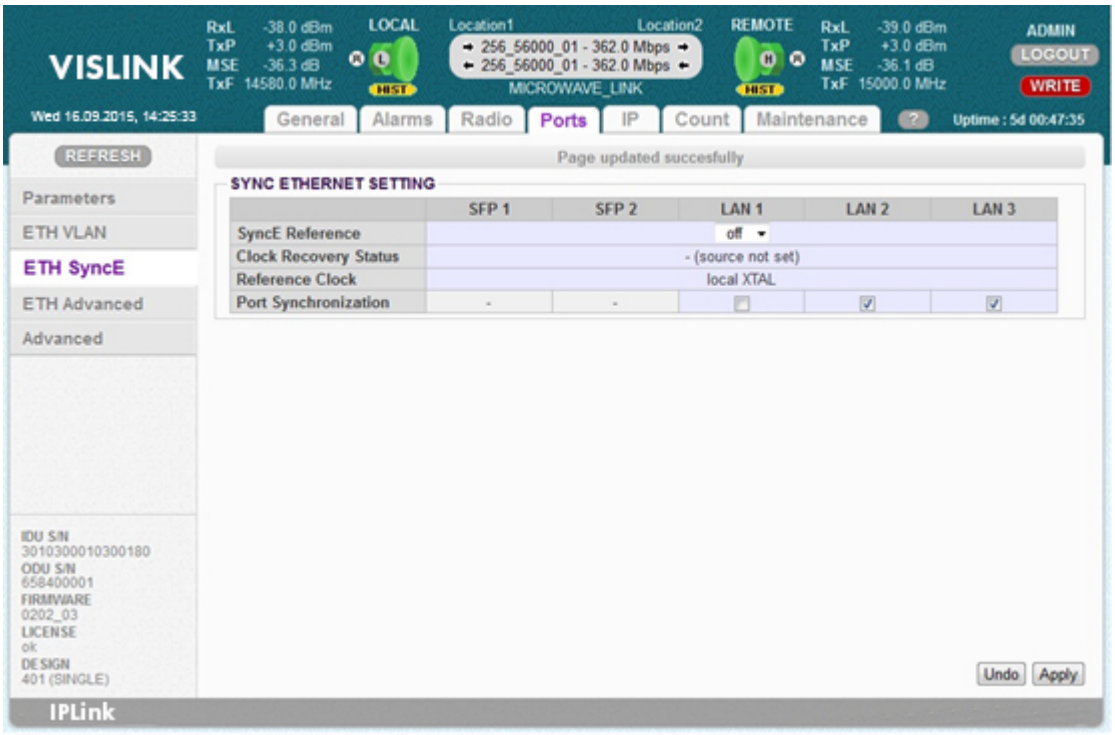

Figure 4-18 ETH SyncE GUI Page

The following describes the setting and display boxes for SyncE:

- **SyncE Reference** – This parameter defines the port selected for clock synchronization at the configured IDU. The available modes are:
  - **Off** – No settings configured
  - **lan1-3** – Clock reference is a specific PHY port LAN 1-3.
  - **sfp1-2** – Clock reference is a specific SFP port SFP 1-2.
  - **rf** – Clock reference is taken from a receiver RF timing (locking to remote IDU).
- **Clock Recovery Status** – Displays PLL lock status (locked / unlocked) and source reference signal status (***source ok***, ***source error***, ***source not set***).
- **Reference Clock** – Displays which internal clock reference is used for system timing. Local XTAL is displayed when no SyncE reference is selected or PLL is not locked. Recovered CLK is a status when system CLKs are locked to the external unit.
- **Port Synchronization** – It is possible to select which ports will be synchronized to the SyncE reference in these tick-boxes. The radio part (rf) is synchronized automatically when SyncE Reference is configured to LAN 1-3 / SFP 1-2 sources.

4.6.7. ETH Advanced Settings

The ETH Advanced web GUI page is dedicated to providing additional ETH configurations, which extend the basic functions of the internal ETH switch (Jumbo Frames, extended QOS, etc.).

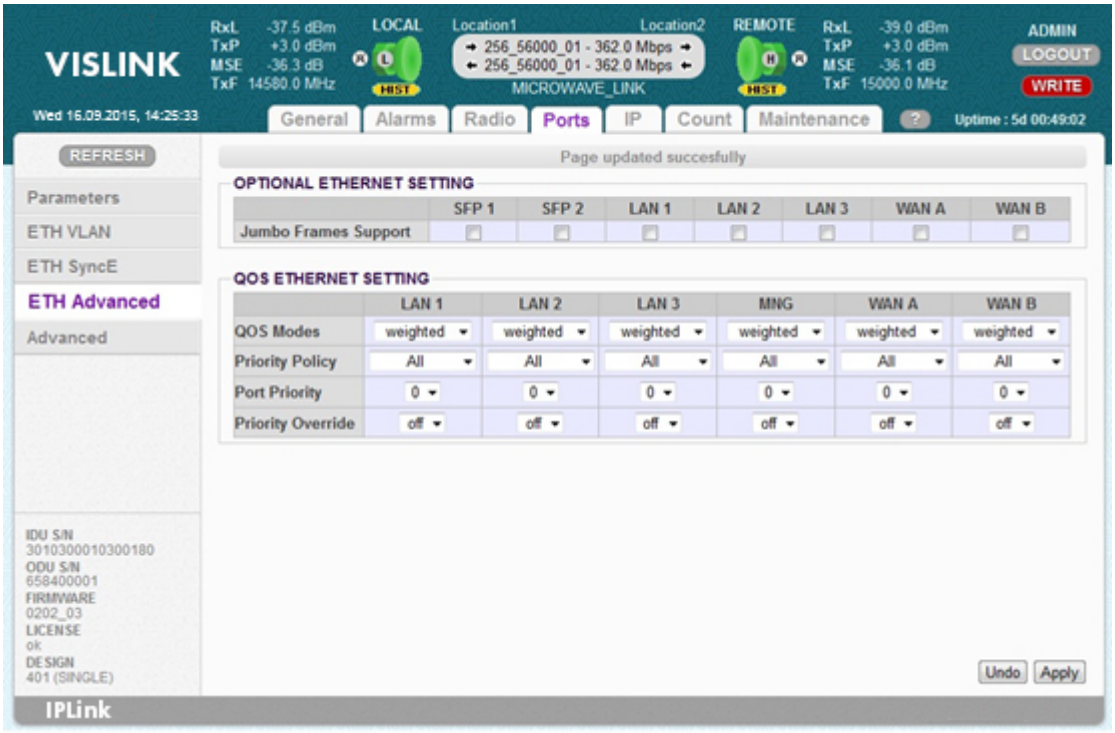

Figure 4-19 Advanced ETH Settings

The following describes the setting and display boxes for OPTIONAL ETHERNET SETTING:

- **Jumbo Frames Support** – these boxes make it possible to select the ports that support Jumbo Frames (length up to 10 kB). There are different Jumbo frames mode settings for the ETH switch ports (LAN1 -3, WAN A-B) and the SFP ports. Because SFP ports are not connected into the ETH switch directly and different designs use specific SFP modes, you need to decide the correct Jumbo frame configuration:
  - In the SINGLE configuration – Only Jumbo Frame settings for LAN and WAN ports are relevant. The setting of SFP boxes does not affect the proper ETH function.
  - In the MULTI configuration – All selection boxes have an influence on the function for Jumbo Frames function.
  - In the PROTECTED configuration – Jumbo frames setting for port SFP 1 (protection port) does not affect correct protection function.

NOTE: Jumbo Frames Support reserves more space in ETH switch FIFO and especially in packet processor FIFO. Therefore, number of buffered packets is limited in this mode.

The following describes the setting and display boxes for – QOS ETH.

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

Priority abbreviations:

- FPRI initial frame priority 0 up to 7 (bits [2:0])
- QPRI queue priority 0 up to 3 (bits [1:0])
- IQPRI initial queue priority 0 up to 3 (bits [1:0])
- OQPRI queue override priority 0 up to 3 (bits [2:1] from QOS PRI value)
- PRI_T PRI bits from 802.ac VLAN tag
- PRI_IP hex value of IP v4/6 frame's TOS/DiffServ/TC bits [7:2]

Port default priority:

- FPRI_D = port default frame priority, defined with Port Priority value
- QPRI_D = port default queue priority, defined with next mapping table
- QPRI_D = 0 when FPRI_D=0/1
- QPRI_D = 1 when FPRI_D=2/3
- QPRI_D = 2 when FPRI_D=4/5
- QPRI_D = 3 when FPRI_D=6/7

IEEE Tag priority:

- FPRI_T = IEEE Tag frame priority, defined with value of PRI bits from VLAN tag
- QPRI_T = IEEE Tag queue priority, defined with next mapping table
- QPRI_T = 0 when FPRI_T=0/1
- QPRI_T = 1 when FPRI_T=2/3
- QPRI_T = 2 when FPRI_T=4/5
- QPRI_T = 3 when FPRI_T=6/7

IP v4/6 priority:

- FPRI_IP = IPv4/6 frame priority, defined with following figure
- FPRI_IP = QPRI_IP*2 + FPRI_D[0]

or defined in another way:

- FPRI_IP[2:1] =QPRI_IP[1:0]
- FPRI_IP[0] = FPRI_D[0]
- QPRI_IP = IPv4/6 queue priority, defined with next mapping table (hex values)
- QPRI_IP = 0 when PRI_IP=00/04/08/0c/10/14/18/1c/20/24/28/2c/30/34/38/3c

- QPRI_IP = 1 when PRI_IP=40/44/48/4c/50/54/58/5c/60/64/68/6c/70/74/78/7c
- QPRI_IP = 2 when PRI_IP=80/84/88/8c/90/94/98/9c/a0/a4/a8/ac/b0/b4/b8/bc
- QPRI_IP = 3 when PRI_IP=c0/c4/c8/cc/d0/d4/d8/dc/e0/e4/e8/ec/f0/f4/f8/fc

The following explains all possible QOS modes:

QOS Modes – This drop-down menu defines output queue policy function. The function is independent of any other QOS configurations. Each output frame is assigned to the queue with the identical number of the frame's QPRI identifier:

- **weighted** – In the weighted scheme an 8, 4, 2, 1 round robin weighting is applied to the four priorities (8 frames from Q3, 4 frames from Q2, 2 frames from Q1 and 1 frame from Q0). This approach prevents the lower priority frames from being timed-out with only a slight delay to the higher priority frames.
- **strict 3xxx** – Strict priority for queue 3 and weighted round robin for queues 2,1 and 0. Queues 2, 1, 0 are served only when Q3 is empty.
- **strict 32xx** – Strict priority for queues 3, 2 and weighted round robin for queues 1 and 0. Queues 1, 0 are served only when Q3 and Q2 are empty.
- **strict 3210** – Strict priority for all queues. Lower priority queues are served only when higher priority queues are empty.

NOTE: QOS Mode configures the output policy (output from the switch) for each port, whereas other QOS setting modes configure the input port policies (input to switch). The priority assignment is done at the input to the switch, the function of the queue controller is defined at the output from the switch.

Priority policy – This drop-down menu defines the initial input queue policy. It defines the initial rules for which output queue will be assigned to every input frame:

- **All** – Next rules are used for priority assignment (from the top to the bottom order):
- **tagged IPv4/6 frames**
  - IQPRI = QPRI_T
  - FPRI = FPRI_T
- **tagged non IPv4/6 frames**
  - IQPRI = QPRI_T
    FPRI = FPRI_T
- **untagged IPv4/6 frames**
  - IQPRI = QPRI_IP
  - FPRI = FPRI_IP
- **untagged non IPv4/6 frames**
  - IQPRI = QPRI_D

- FPRI = FPRI_D

Port only – Next rule is used for priority assignment:

- **all frame types**
  - QPRI = QPRI_D
  - FPRI = FPRI_D

Tagged only – Next rules are used for priority assignment (from the top to the bottom order):

- **tagged frames**
  - IQPRI = QPRI_T
  - FPRI = FPRI_T
- **untagged frames**
  - QPRI = QPRI_D
  - FPRI = FPRI_D

IPv4/6 only – Next rules are used for priority assignment (from the top to the bottom order):

- **IPv4/6frames**
  - IQPRI = QPRI_IP
  - FPRI = FPRI_IP
- **non IPv4/6 frames**
  - IQPRI = QPRI_D
  - FPRI = FPRI_D

Port Priority – This allows you to configure the default port priority. Use values 0 to 7 (0 is the default value) to define FPRI_D and QPRI_D parameters according to the above described figures. The next possible function of this variable is to define and/or replace the QOS priority information, based on FPRI_D for the frames that are output with the VLAN tag. These updated frames can be input into the switch with QOS priority, this is different to the priority of the same frame at the output of the switch.

Priority Override – This allows you to replace the initial queue priority with a new priority. The new priority is assigned to each frame with the VLAN ID defined from the VTU table with properly configured QOS PRI value:

- **off** – QOS override is disabled.
- **vtu** – Queue priority override information (OQPRI) is derived from bits [2:1] of the QOS PRI parameter as defined in Section 4.7.5. When this parameter is set to the off state, the override process is not active for the appropriate VTU record, even though Priority override is enabled on the port.

4.6.8. Advanced Port Settings

The settings for the **Advanced** side bar is available from the **Ports** tab on the web GUI. The settings offer configuration options for extended modes, associated with packet processing. The available settings on this web GUI page allows you to define the AES encryption (Figure 4-20).

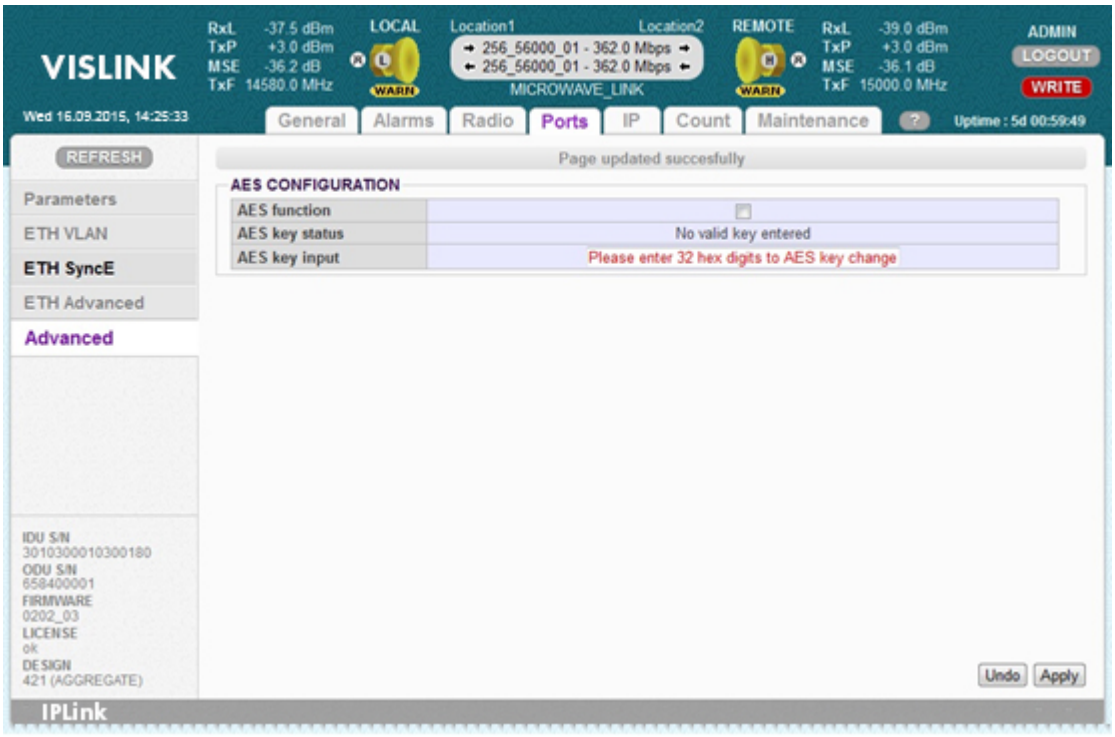

Figure 4-20 Advanced Port Setting GUI Page

Setting and Display Box Descriptions:

- **AES function** – This box enables or disables the AES encryption function. The function is subject to entering a valid license option and a valid AES key. When the checkbox is selected, the whole traffic stream from the packet processor is encrypted with the selected AES key. The opposite IDU must be defined in the same way with with an identical AES key. Out of band management channels are not encrypted in this mode, therefore remote access to the remote IDU is possible in any way.
- **AES key status** – This information line shows the status for the actual AES key and the last four digits of the valid key in use.
- **AES key input** – The AES key must be entered for the initial key definition, alternatively, it must be changed prior to initialization of the AES function.

NOTE: The AES option is not available to units configured for SINGLE mode.

4.7. IP Configurations

The management access type can use either the local connection via LAN 3 port, connected directly to the management CPU via Ethernet switch ETH 0 port or USB B port that connects directly to the management CPU via USB port 0.

Other IP ports on the management CPU are primarily used to interconnect with a remote IDU (RFI 1) or with a protection/aggregate unit (HSI1).

4.7.1. Basic IP Addresses Assignment

Every device in the local network has its own and unique primary IP address. This IP address allows each bit of network equipment access to your network. Pay attention to the configuration when setting-up the IP address, which needs to follow the general IP address rules (IP address, IP Netmask, IP gateway). Ensure that the correct IP addresses are assigned and configured for all units in the microwave network. We recommend preparing a short block diagram of the IDUs interconnections for the microwave network, also select the appropriate model for IP address setting, according to the required type of IP management access (in-band /out-of-band).

The basic IP setting should be done during installation and commissioning as described in Section 4.8.1. We recommend checking and updating all parameters on IP pages. These parameters must be entered for each IDU according to the management block scheme in use.

Description for settings and display boxes:

- **Primary IP / Mask** – The IP address is assigned to port ETH0 (local address) with the appropriate netmask specification. The netmask value is entered in the form of decimal numbers corresponding to the number of ones in the binary subnet mask presentation. i.e. The net-mask for subnet-mask 255.255.255.0 is presented as decimal number 24. The Local network has its own and unique primary IP address.
- **Default Gateway IP** – The default Gateway IP address is used for the CPU when the connection is outside the IP range as defined in the system routing table. This IP address must be a part of the system routing table. The routing table can be checked on via the web GUI page **IP** tab using the **Route/NAT** side-bar.
- **Remote Unit IP** – This address specifies the remote unit IP address that is connected over the RF link. This address is necessary for the automatic message exchange between these IDUs and for the correct out-of-band management functionality. The subnet mask is not required for this IP specification, because the ppp protocol is used.
- **Protection/Aggregate Unit IP** – This address specifies the neighbouring unit IP address (protection or aggregate) as connected over FO. This address is necessary for the automatic message exchange between these IDUs and for the correct out-of-band management functionality. The subnet mask is not required for this IP specification. This setting is only necessary for the Protected and Aggregate configurations.

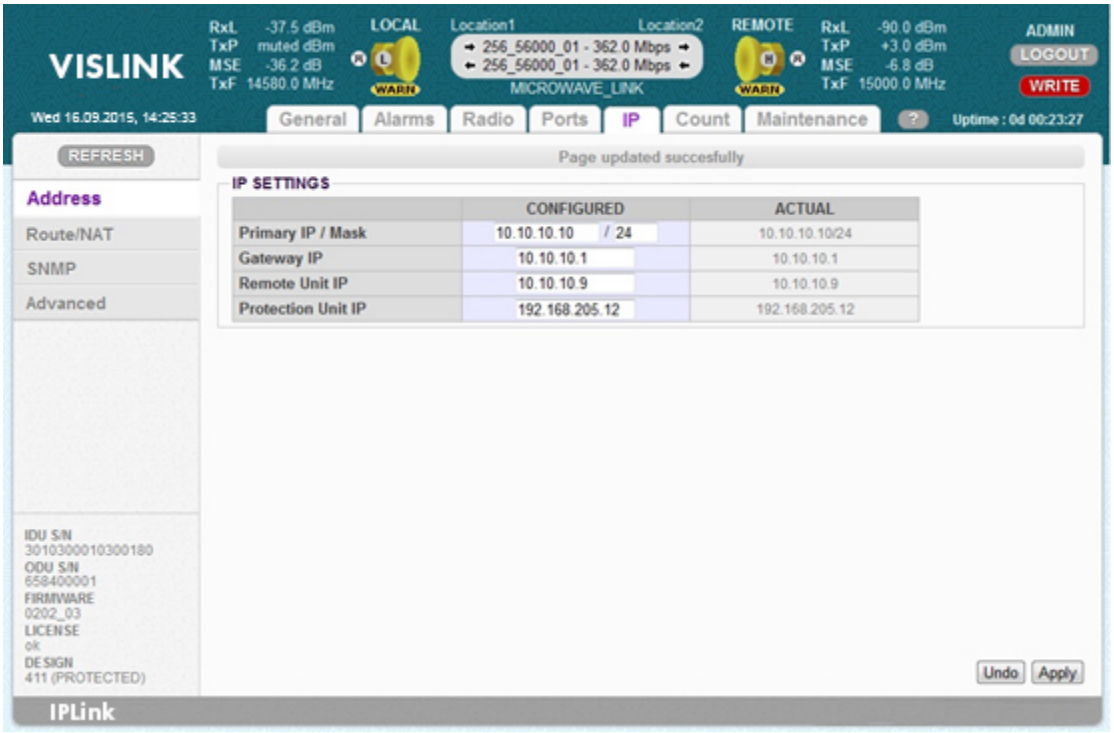

Figure 4-21 Basic IP Setting

The temporary configuration IP file is changed by clicking the **Apply** button, these changes are not immediately applied to the running system. After you click on **Apply**, an intermediate confirmation window appears. There are two possible ways to proceed:

1. Click the **Continue** button to continue with IP changes (static routes, NAT, advanced IP setting, SNMP, etc.). This is because we recommend applying all IP changes in one step. Any change in the temporary configuration IP file is indicated by a warning message in the status line at each IP page.
2. Click **Write and Apply** in the confirmation window to immediately apply the IP change to the running system.

NOTE: IP configuration changes should not cause user traffic data to drop.

4.7.2. Static Route and NAT Settings

To make specific configuration management access changes, it is sometimes necessary to add, change or delete static routes or NAT records. This is especially true for Out of band type management access. To edit these parameters use the **STATIC ROUTES – INPUT VALUES** and **NAT – INPUT VALUES** fields from the web GUI using the **IP** tab and **Route/NAT** side-bar (see Figure 4-22.)

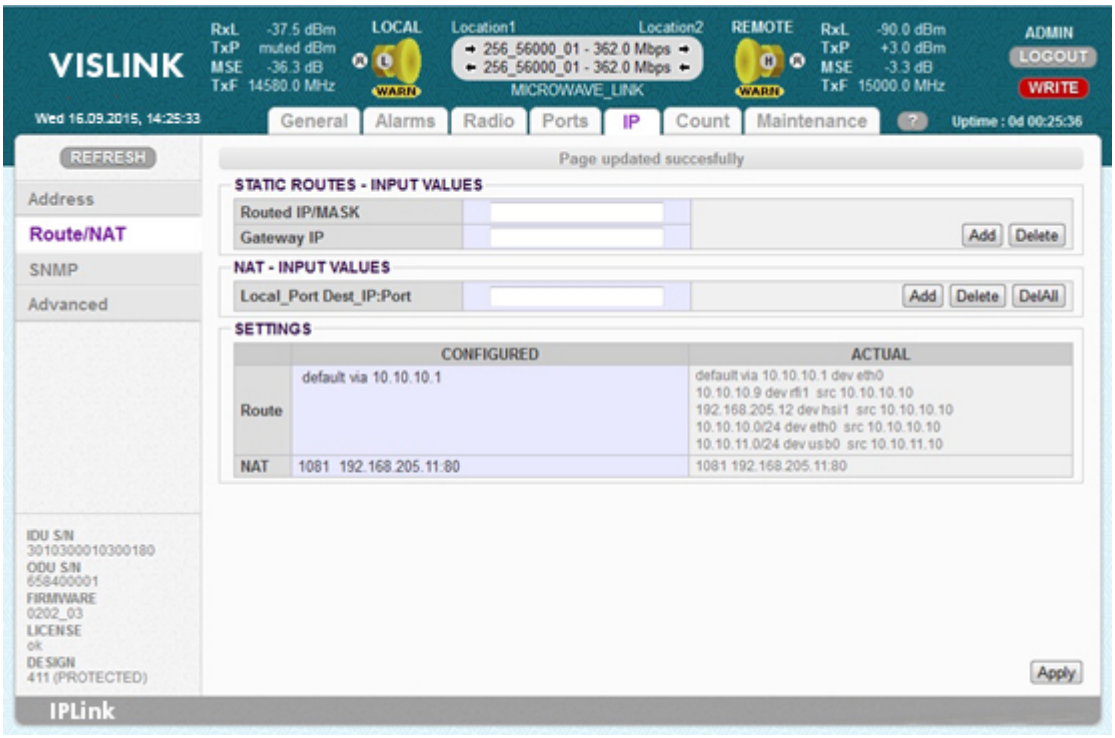

Figure 4-22 Static Route and NAT Setting

Each static route and/or NAT record must be entered separately. The same confirmation window as for the IP address configuration appears after erasing each record. Click the **Continue** button to proceeding with any other IP settings. Click the **Write And Apply** button to apply all IP settings to a running system after the last record is input (when no other IP configuration changes are not required).

Description for particular setting and display boxes for the Static Route – Input Values fields:

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

NOTE: The **ADD** button is used to enter new route information into the routing table. The **DELETE** button is used to delete a record from the routing table.

Description for particular setting and display boxes for the NAT changes field:

- **LocalPort DestIP:Port –** The NAT record must be entered as per the following command: ***local_port destination_ip: port***
  - ***local_port*** – The number of a port on the local IP used for address translation, it must be followed with space character.
  - ***destination_ip*** – IP address of destination/remote unit.
  - ***port*** – Port number of service at the destination/remote IP:
  - Example: ***1080 192.168.4.101:80***

Click the **ADD** button to enter a new NAT record into the NAT table. Click the **DELETE** button to delete a record from the NAT table. Click the **DELALL** button to delete all NAT records in one step.

4.7.2.1. Routing Table and NAT Table Checking

You can compare the Routing and NAT tables of a running system (ACTUAL) with records in temporary configuration file (CONFIGURED) in the SETTINGS section, see Figure 4-22.

NOTE: The **CONFIGURED** and **ACTUAL** setting fields are available in Figure 4-21.

The **ACTUAL** field only displays the added routes and NATs compared to the default settings in the **CONFIGURED** field. This section requires the default gateway record identifier as a minimum, as it is a member of the same definition file as other static routes.

Internally generated static routes are also displayed with the system core in the **ACTUAL** column. There is a small difference in the records for the **CONFIGURED** and **ACTUAL** columns.

Any difference between **CONFIGURED** and **ACTUAL** IP setting is indicated in the status line on all IP pages with an alert message ***"IP settings are not currently applied – press APPLY button".***

If detailed analysis is required, you can compare both sections visually.

4.7.3. SNMP Settings

SNMP management is configurable on the web GUI from the **IP** *tab and* **SNMP** *side-bar (*Figure 4-22*)*. Only SNMP traps are supported in the current firmware release.

Description for particular setting and display boxes for SNMP settings:

- **Trap Port** – This parameter specifies the port used for the SNMP trap message(s). The same configuration must be also be set at the SNMP agent station.
- **Trap Address 1-3** – Up to three IP addresses can be configured as a destination for the SNMP trap distribution. Trap message events are configured in the same way as the alarm settings.

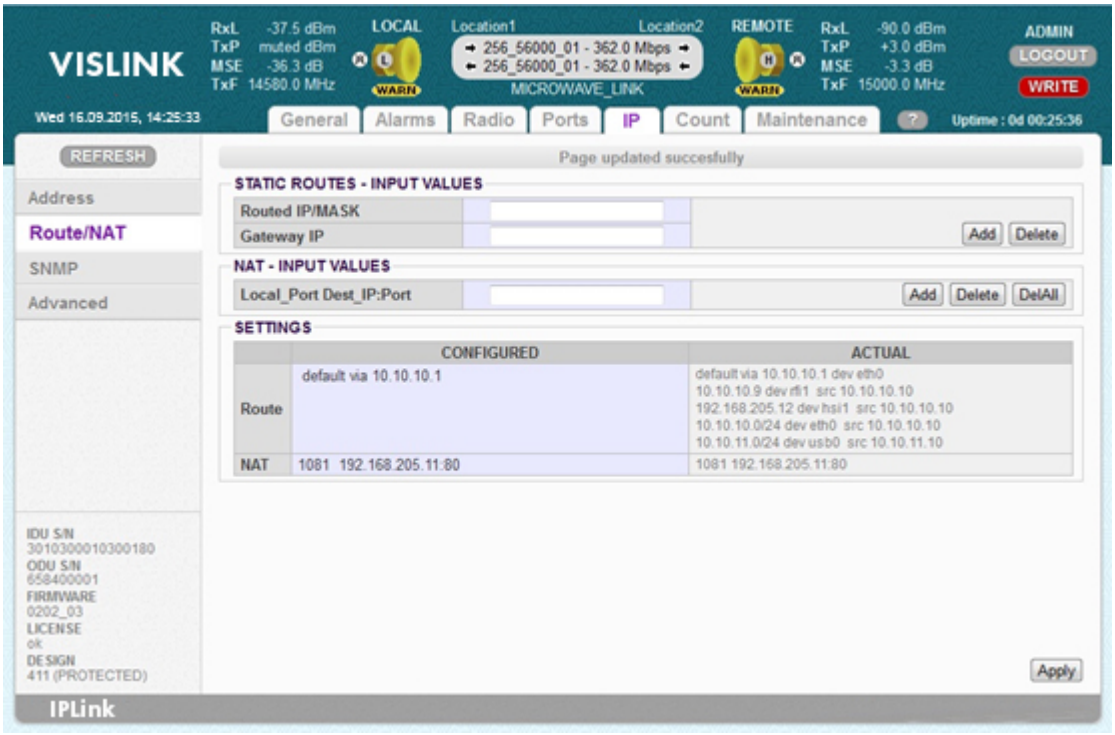

Figure 4-23 SNMP Setting

4.7.4. Advanced IP Settings

The advanced IP section makes it possible to change the extended IP configuration, which usually remains in the default state. This can sometimes be necessary to support specific management modes. The advanced management setting is accessible via the web GUI from the **IP** *tab and the* **Advanced** *side-bar (*Figure 4-23*)*.

Description for particular setting and display boxes for OPTIOPNAL ADDRESS SETTING:

- **USB IP/MASK** – Specifies the IP address for the USB management port. When the default IP address for this port conflicts with another network configuration, change the setting with this parameter.
- **Secondary IP/MASK** – Specifies the secondary IP address for the ETH 0 management port. When the default IP secondary address conflicts with another network configuration, change the settings with this parameter.
- **RFI1 port IP (PPP)** – Specifies the internal IP address for the RFI 1 port (which connects the remote unit(s)). The default RFI1 IP address uses the same value as the ETH 0 port (in unnumbered mode). It can be helpful to set the numbered ppp mode for a specific network configuration.
- **HSI1 port IP (PPP)** – Specifies the internal IP address for the HSI 1 port (which connects neighboring units). The default HSI 1 IP address uses the same value as the ETH 0 port (in unnumbered mode). It can be helpful to set the numbered ppp mode for a specific network configuration.

Description of particular setting and display boxes for FILE TRANSFER:

- **FTP/USB Server** – Specifiying the syntax "***usb"*** for this field uses the USB - A port as the destination/source interface to backup and/or restore the IDU configuration. Specifying the syntax "***ftp://IP/directory_structure/***" is used in this field an external FTP server is used as the destination/source address to backup and/or restore the IDU configuration.

Description of particular setting and display boxes for REMOTE TIME SERVER:

- **Server Type** – Three types of time server can be specified for time synchronization: "***ntp***", "***rdate***" or "***none***". The most useful setting is ntp mode. Select "**none**" if time synchronization is not required.
- **Server IP** – Specifies a remote time server IP when **ntp** or **rdate** mode are selected in the **Server Type** option.
- **Act as NTPD Server** – When this checkbox and ***ntp*** type of time server are selected then the CONFIGURED unit operates as the NTPD reference server. The time at the remote units can be synchronized from the CONFIGURED unit.

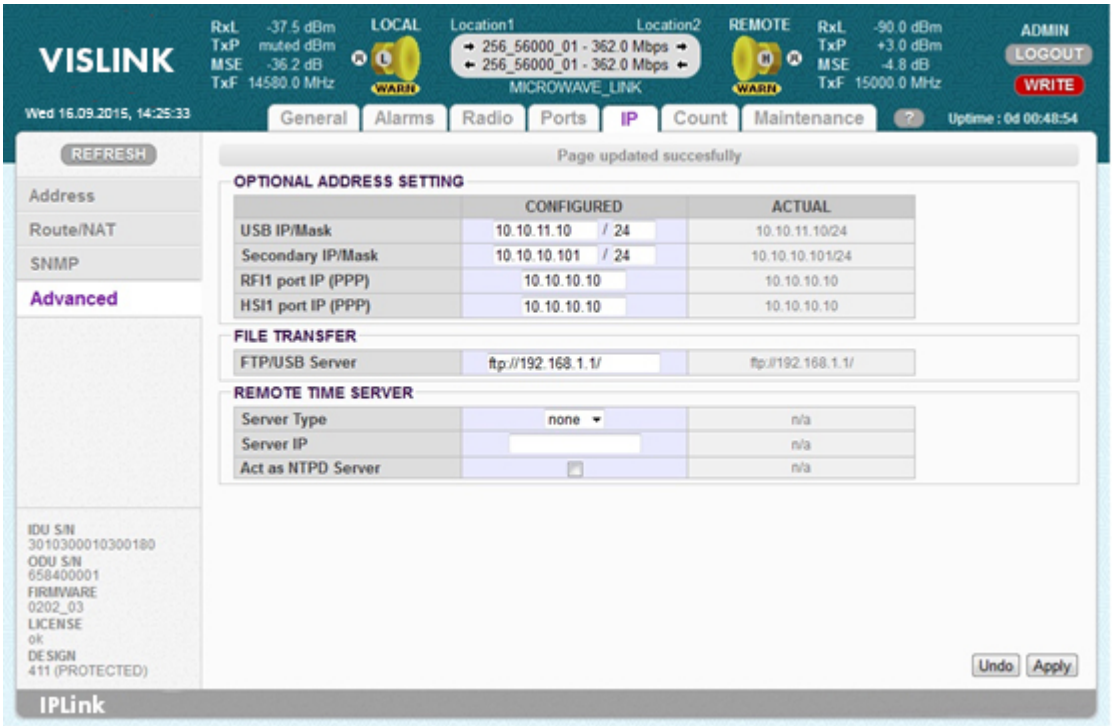

Figure 4-24 Advanced IP Setting

4.8. Maintenance and Advanced System Configuration

4.8.1. Saving the Configuration

To maintain the configured and modified link parameters after the equipment is power cycled (or after device restart) you must save the new configuration. To do this, use the **WRITE** button, available on each GUI page. The red background on the **WRITE** button indicates that the actual running configuration is not yet saved in the start-up memory. An intermediate window appears after clicking the write button (Figure 4-25). This confirmation window allows you to choose to write and store the configuration to the local unit or both local and remote units.

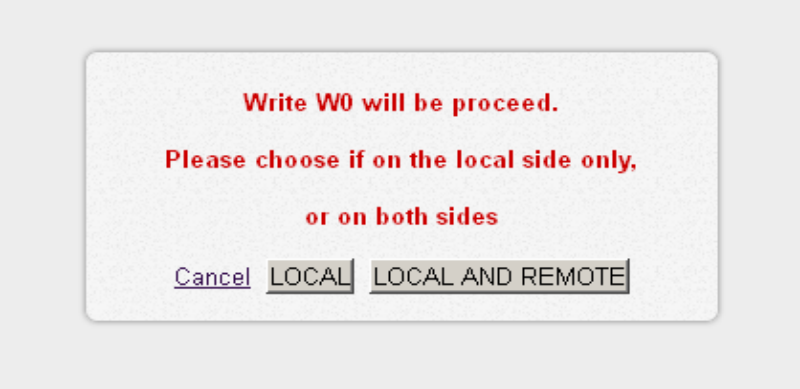

Figure 4-25 Write Confirmation

When the configuration is properly saved, it is possible to write the actual configuration into the optional memory positions (W1-W3). This operation saves the configuration settings as an alternative configuration for a future quick configuration scheme restoration. To do this, click on the relevant **RUN W0** to **RUN W3** buttons (Figure 4-26).

The **RETURN TO PREVIOUS PAGE** button in the bottom-right hand corner of the web GUI page helps you to quickly return to the previous active page.

NOTE: Before saving the start-up memory, make sure that all modes work properly and remote access to the IDU is possible. The automatic restore function cannot return to a previous status once you save the start-up memory.

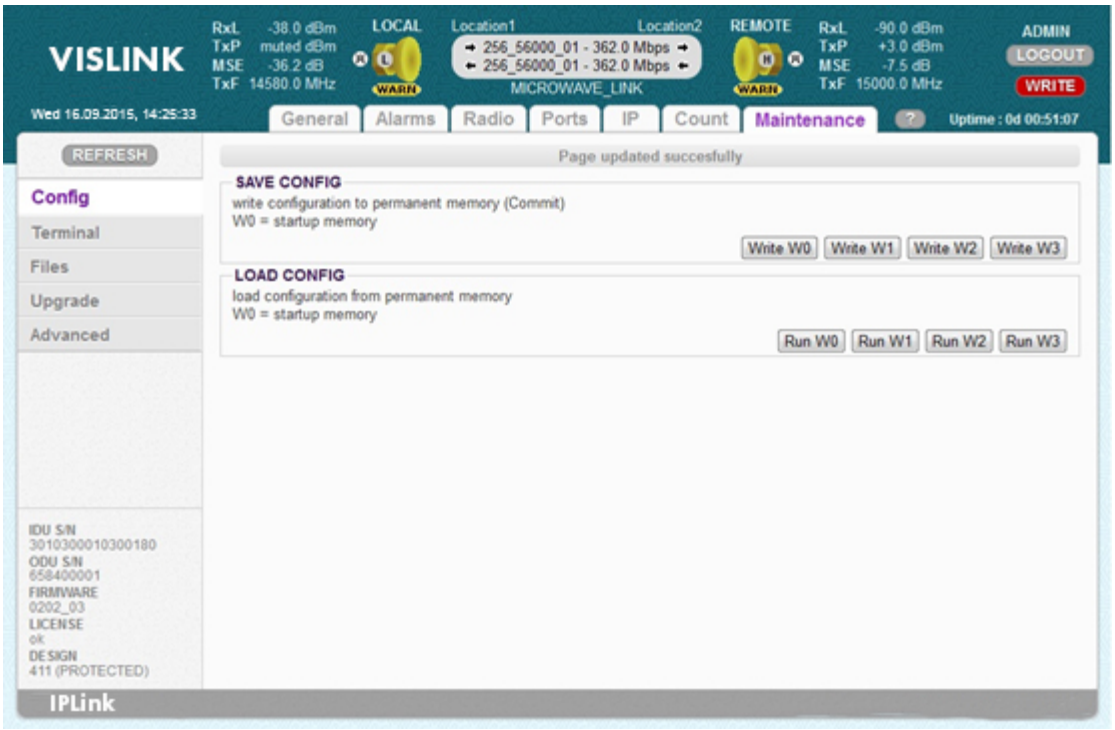

Figure 4-26 Write and Run Commands

4.8.2. Configuration Backup and Export

We recommend making a backup of the complete IDU configuration in case of a system fault. This will allow you to quickly repair the system or mirror the system

settings to any new replacement equipment. This backup configuration should be stored on a reliable medium.

The web GUI page **Maintenance** tab **Files** side-bar (Figure 4-27) provides access to the backup process.

4.8.2.1. Backup Procedure

Do the following to back-up your configuration:

1. Login using your preferred web browser using ADMIN rights.
2. Save the current configuration with the **WRITE** button, (available on each GUI page). This saves the running configuration to the start-up memory.
3. From the web GUI **Maintenance** tab on the **Files** side-bar, select the **Save Config** checkbox,
4. Click the **GENERATE** button.
5. Right-mouse click on the file "***fwconf_xxx_xxx.afw***", then select the destination location for the file and save it.

The configuration is now saved to your specified location.

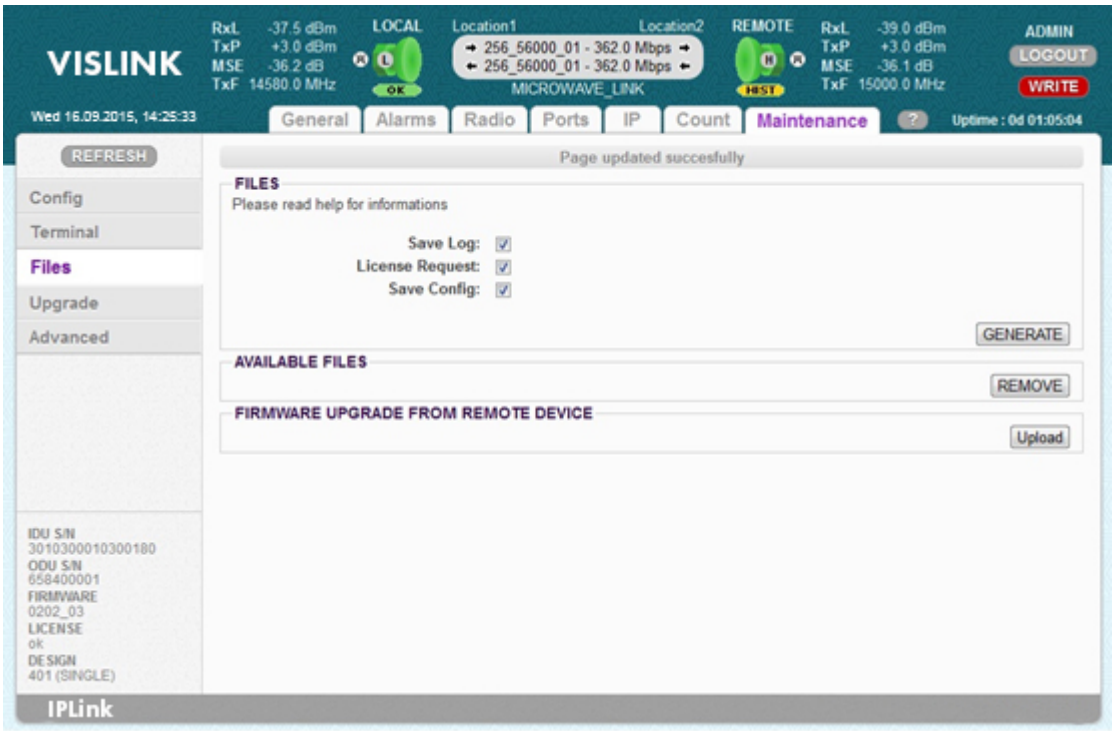

Figure 4-27 Configuration, Logs and License Request Backup

Description for particular setting and display boxes for FILES:

NOTE: It is possible to select what files are going to be generated for subsequent backup in the FILES section.

- **Save Log** – Compresses the log file as a tar gzip form. This can be used for troubleshooting purposes.
- **License Request** – A copy of the License File in an encoded form. This is used by your representative to generate any new licenses required. This file identifes the active license loaded on the IDU.

- **Save Config** – This encoded file contains the complete backup configuration of the IDU. When this file is uploaded into another IDU, then all original system settings and configurations are replaced with this backup configuration.

The required files are generated for processing after clicking **GENERATE**. When a USB memory stick is inserted in the USB A port and USB is defined as a destination for the file transfer, the files are saved to USB memory (see Section 4.8.5).

Description of particular setting and display boxes – **AVAILABLE FILES**:

Generated files are visible in this section. The save dialogue window appears after a right-mouse click. This allows you to select the required destination to save the individual files. The name for each file is the combination of a file identifier, IDU_SN and actual time mark.

Description of particular setting and display boxes for **FIRMWARE UPGRADE FROM REMOTE DEVICE**:

This selection makes it possible to upload any encoded *.afw file into a specific directory to the local IDU. This file can be subsequently downloaded and processed by a remote unit using the CLI command, entered on the remote unit. This is useful in case access to remote IDU is available only from the command line of the local IDU over TELNET / SSH. In some cases, this can be the only way to change the license or upgrade the firmware on a remote unit. The alternative and preferred method is to use an out-of-band connection to the remote unit by means of the NAT function (see Section 4.8.3).

4.8.3. Firmware and License Upgrade

Firmware and license upgrade is available to an ADMIN-level user only.

We recommend verifying the version of firmware loaded to the IDUs before upgrading or updating the license of a microwave link. It is possible that the IDU with older firmware may not recognize the new configurations, options or functions contained in new license key, hence may not operate properly or at all.

Both Firmware and License upgrade are available from the web GUI using the **Maintenance** tab and **Upgrade** side-bar using the identical update process. An intermediate window will appear after selection of this page (see Figure 4-28).

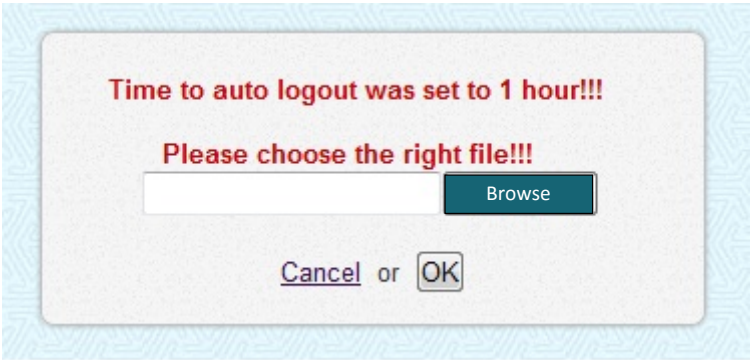

Figure 4-28 Firmware/License Upgrade

4.8.3.1. License Upgrade

A correct license file must be selected and confirmed by clicking the OK button. The upgrade process is then monitored in the processing window. A new license is active after one of the following events:

- New license is checked using the web GUI **General** tab and **License** side-bar.
- New modulation is selected when periodical license update loop is over (once every 6 hours).

4.8.3.2. Firmware Upgrade

IDU firmware is divided into four sections depending on their functions. It may not be necessary to update all part for every firmware release, only the following are different, compared to the newest version. The basic firmware parts are described in the following:

- **hwbase.afw** – software for internal HW parts
- **oskernel.afw** – operating system
- **dev.afw** – drivers for OS
- **fwbase.afw** – application software (WEB, SNMP, commands, etc.)

Assistance packages are also contained in every firmware release:

- **checkversions.afw** – This package compares the firmware version in the IDU with the newest version and prints the information on the parts that are necessary to upload.
- **fw_all.afw** – First of all, this package compares the current version of firmware in the IDU with the newest version and then automatically uploads the different parts.

4.8.3.3. Recommended Steps for Firmware Update

The following procedure outlines the recommended steps to upgrade the IDU firmware:

1. Login using your preferred web browser with ADMIN rights.
2. Save the current running configuration by clicking the **WRITE** button, which is available on each GUI page.
3. To compare the current running versions of each firmware section (o*s_kernel, os_dev, hw_base* and *fw_base*) against the newest version, do one of the following steps, selected from the web GUI:
    a. Manually compare the data shown on the **General** tab and **Info** side-bar with the new version of the file ***version.txt***.
    b. Open the **Maintenance** tab and **Upgrade** side-bar to select package ***checkversions.afw*** and use the on screen/print-out information for the parts that need to be upgraded.
4. Next choose one of the following steps:
    a. Select the file ***fw_all.afw*** from the provided SW package. The whole file will be uploaded into the device, the system compares the different versions and writes the different parts of the firmware into flash memory.

NOTE: This procedure isn't suitable for slow access to IDU management.

    b. Individually select the following files, in order: ***hwbase.afw, oskernel.afw, dev.afw*** and ***fwbase.afw*** (skip any particular file if you know it is not required and continue to the next required file in sequence) and wait for the process to complete.

5. After the last file uploads, restart the device from the web GUI ***Maintenance*** Tab ***Advanced*** *side-bar by clicking* **REBOOT**.

NOTE: During restart there is a data drop for about 20 seconds.

6. Login again with ADMIN rights and update the start-up memory configuration with the newest functional setting available in the newest firmware. Save the new configuration with the **WRITE** button, available on each page.
7. Make a new IDU initialization from the start-up memory. To do this, select **Run_W0** using the web GUI **Maintenance** tab and **Config** side-bar.

NOTE: During initialization there is data drop for about 5 seconds.

The new firmware should now be properly installed in the IDU. If not repeat the process.

4.8.4. Advanced System Configuration

The advanced system configuration is important for a correctly functioning system. The settings are accessible using the web GUI via the **Maintenance** tab and **Advanced** side-bar (see Figure 4-29).

All settings are applied separately by clicking the **APPLY** button.

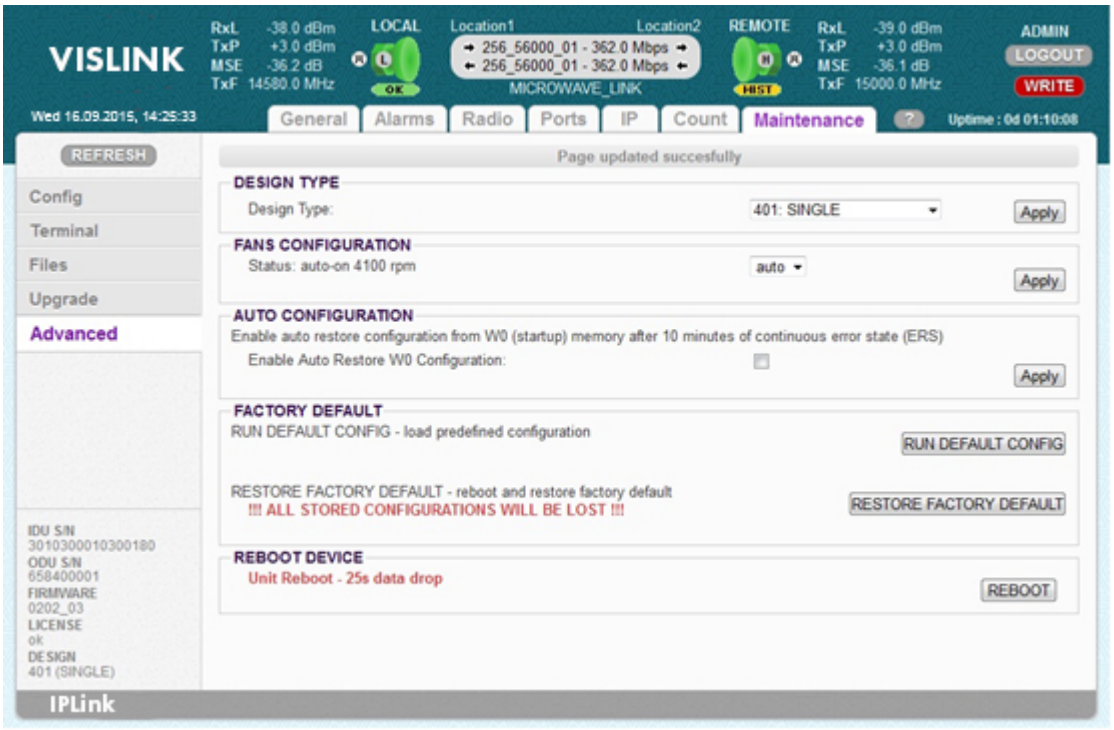

Figure 4-29 Web GUI Maintenance/Advanced

Description of particular setting and display boxes for Advanced:

- **DESIGN TYPE** – This drop-down allows you to choose the configuration in use according to the Design Type. This changes the complete system functionality. Design changes involve a reboot of the FPGA and correct hwbase software loading. This setting must be applied by clicking the **APPLY** button. The options available are:
  - **SINGLE** – One independent traffic channel over air.
  - **MULTI** – Up to four independent traffic channels over air.
  - **PROTECTED 1+1** – Link protection by means of two IDUs.
  - **AGGREGATE 2+0** – Speed aggregation by means of two IDUs.
- **FANS CONFIGURATION** – Three modes are available:
  - **auto** - the IDU temperature controls the fan speed (preferred/default option).
  - **on** - fan runs constantly.
  - **off** - fan is turned off.
- **AUTO CONFIGURATION** – If the checkbox is ticked, the start-up configuration is loaded after 10 minutes of continuous error. We recommend disabling this function during link configuration and installation.
- **FACTORY DEFAULT** – Two different factory settings are available:

- **RUN DEFAULT CONFIG –** This restores the default configuration of the major IDU components, some customer specific settings remain without change (design type, IP section, TX/RX frequencies, Tx Power, modulation type). This allows you to keep the remote connection with an IDU, but helps to return the default configuration of the extended configuration mode. The restored configuration must be stored into start-up memory using the **WRITE** button.
- **RESTORE FACTORY DEFAULT –** This restores the complete factory default configuration. All stored configurations will be lost. This selection should only be used when local management access to the IDU is ensured.

⚠ CAUTION: We recommend backing up (flash disk, PC) the actual configuration before clicking on **RESTORE FACTORY DEFAULT**.

- **REBOOT DEVICE** – IDU is restarted after clicking this button.

NOTE: The device reboot causes approx. 20 seconds of data drop.

This page is intentionally unused.

5. CONFIGURATION EXAMPLES

5.1. Example 1 – In-Band Management Separated by VLAN

In-Band management configuration manages traffic separation by means of a VLAN and is the preferred scheme when just one ETH connection (management & data traffic) into the microwave link is used. Communication with the remote side is ensured by sharing the common capacity for data and management traffic through the internal ETH switch. The management data, together with the user data, are broadcast via the common Gigabit cable from the external Ethernet switch to the IDU. Management traffic must be uniquely tagged by the VLAN. The same VLAN is then used across the whole management network to manage traffic separation.

The application example is shown in Figure 5-1. The configuration for the GUI pages at LOCATION 1 (provider side) is shown in Figure 5-2 and Figure 5-3.

This example describes an application using the Single configuration design on both link sides. Further settings include modulation set to QAM128 with 30 MHz bandwidth and the appropriate maximum data speed around 169 Mbps. The IP addresses of both IDUs are from the same IP subnet. This is because this scheme is similar to the switched Ethernet network. Slow separated management channels are also used in this configuration, but only for periodical message exchanges between both IDUs. The remote management connection is available from port LAN 1 or alternatively from ports LAN 2, SFP 2 (WAN B) and WAN A (over-air connection) in the form of tagged frames with VLAN #100. The alternative local management connection is available through the LAN 3 port on each IDU. This port accepts only untagged frames and the port is a member of the managed VLAN #100 (access mode). All data traffic is transparent between both IDUs excluding VLAN #100, which is reserved for management purposes. The CPU management port ETH 0 is accessible only from the management VLAN. The VLAN setting corresponds with the appropriate explanation in Section 4.7.5.

In-Band management configuration with VLAN is supported by all configuration designs (SINGLE, MULTI, AGGREGATE, PROTECTED).

Main Advantages:

- Fast management access to local and remote IDU.
- A single Ethernet cable is required to connected both data and management traffic.

Disadvantages:

- Management traffic shares capacity with data traffic.
- You need to know what type of customer traffic is in use, especially if a VLAN configuration is used at the provider and customer side.

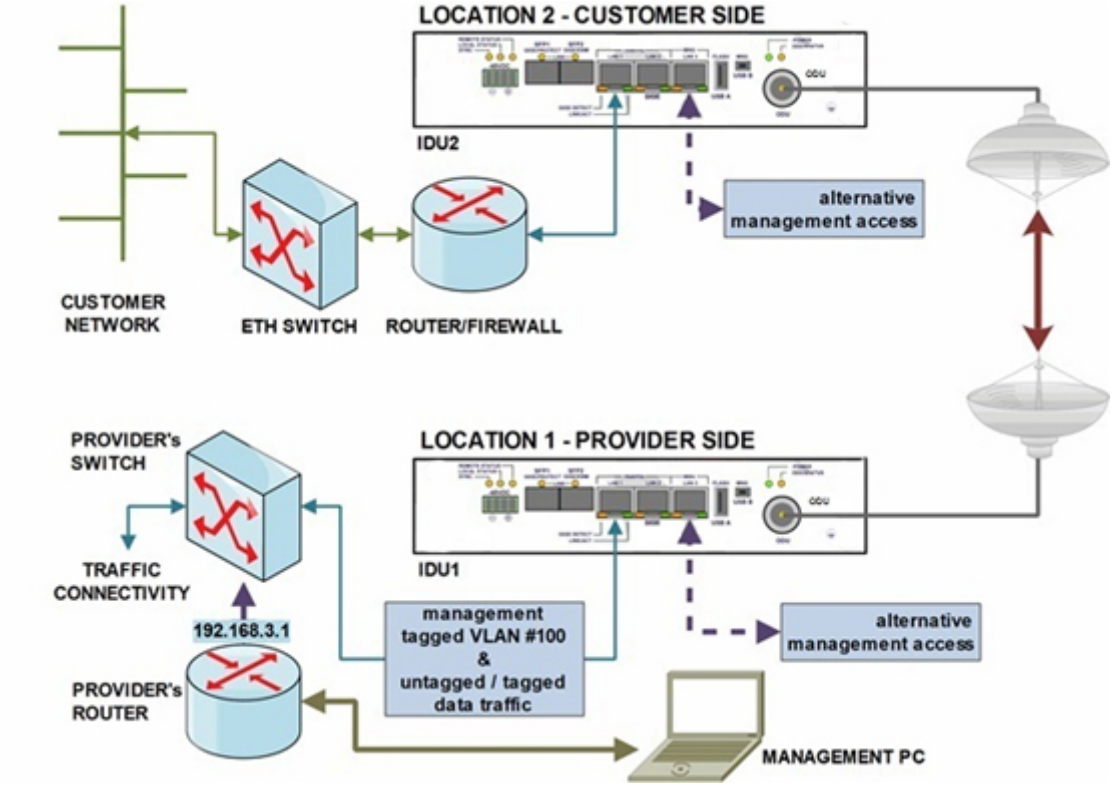

Figure 5-1 Example 1 – In-Band Management Separated by Means of VLAN

-	IDU1 (provider side)	IDU2 (customer side)
Maintenance | Advanced		
Configuration/Design	Single	Single
IP | Address		
Local IP	10.10.10.10/24	10.10.10.9/24
Remote IP	10.10.10.9	10.10.10.10
Gateway IP	10.10.10.1	10.10.10.1
Ports | Parameters		
Speed Allocation [Mbps]	ETH1 = 362	ETH1 = 362
Ports | ETH VLAN		
Port Mode	Hybrid = LAN1/2, WANA/B Access = LAN3, MNG	Hybrid = LAN1/2, WANA/B Access = LAN3, MNG
Port Groups	1 = all ports	1 = all ports
VTU Setting	Add 100 group1 off TTUUTT	Add 100 group1 off DDUUTD

Table 5-1 In-Band Management Separated by VLAN Settings

1. The SINGLE configuration must by selected as the first step in the configuration process on both IDUs.
2. Click **Apply**.

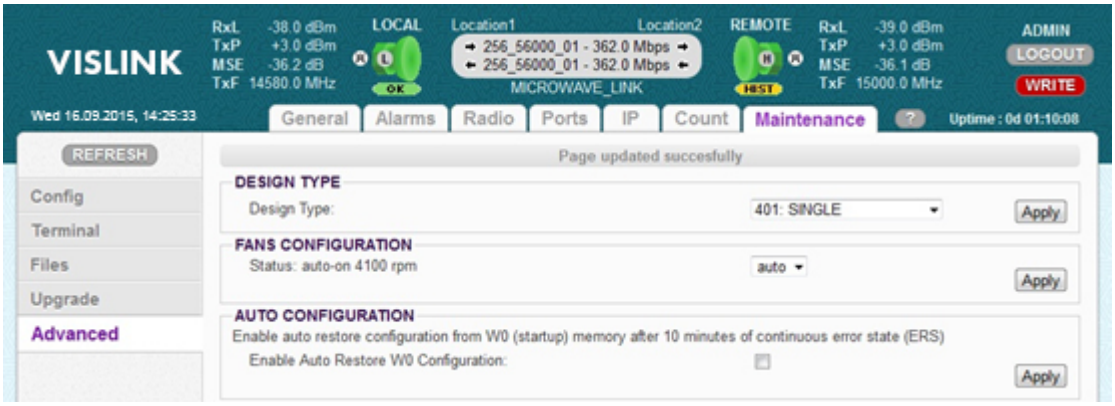

Figure 5-2 Example 1 – Selection of Design SINGLE at LOCATION 1

3. Enter and apply the correct IP address setting.
4. Click **Apply**.

NOTE: You are required to login back into the system after applying any IP change. IP configuration changes don't influence data traffic (no data drop during IP re-initialization).

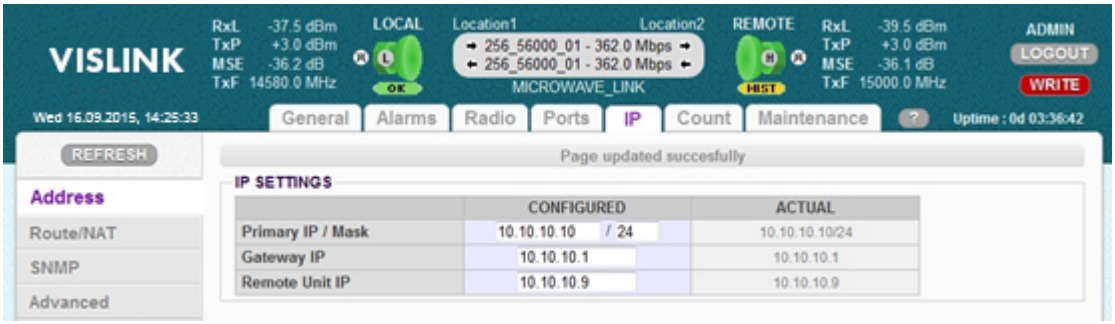

Figure 5-3 Example 1 – IP Address Setting at LOCATION 1

5. It is very important that you use the correct VLAN setting for the In-Band management configuration. To do this:
   a. Add the VTU record
   b. Change Port Modes and Port Groups.

NOTE: All changes should be applied together by clicking the **APPLY** button. Such change must be confirmed at the intermediate window by clicking the **Continue** button (remote access to the IDU must be ensured with a similar VLAN configuration in your network, otherwise the previous VLAN configuration is returned after 120 seconds).

The VTU record for IDU 2 ensures that management isn't accessible from the customer network side, it is only remotely available from the provider side or from local management ports LAN 3 at IDU 2.

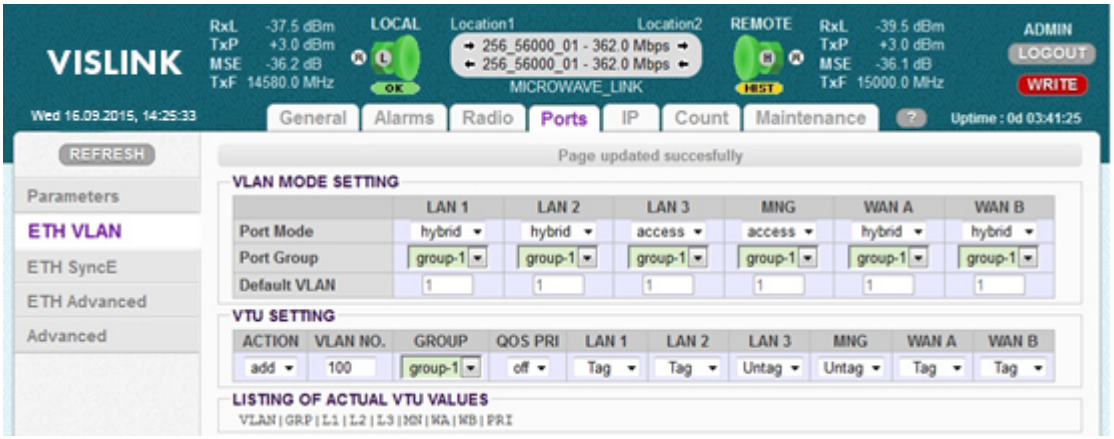

Figure 5-4 Example 1 – VLAN and Port Group Setting at LOCATION 1

6. Configure the basic port parameters, such as:

- Ethernet channel speed
- LAN port modes

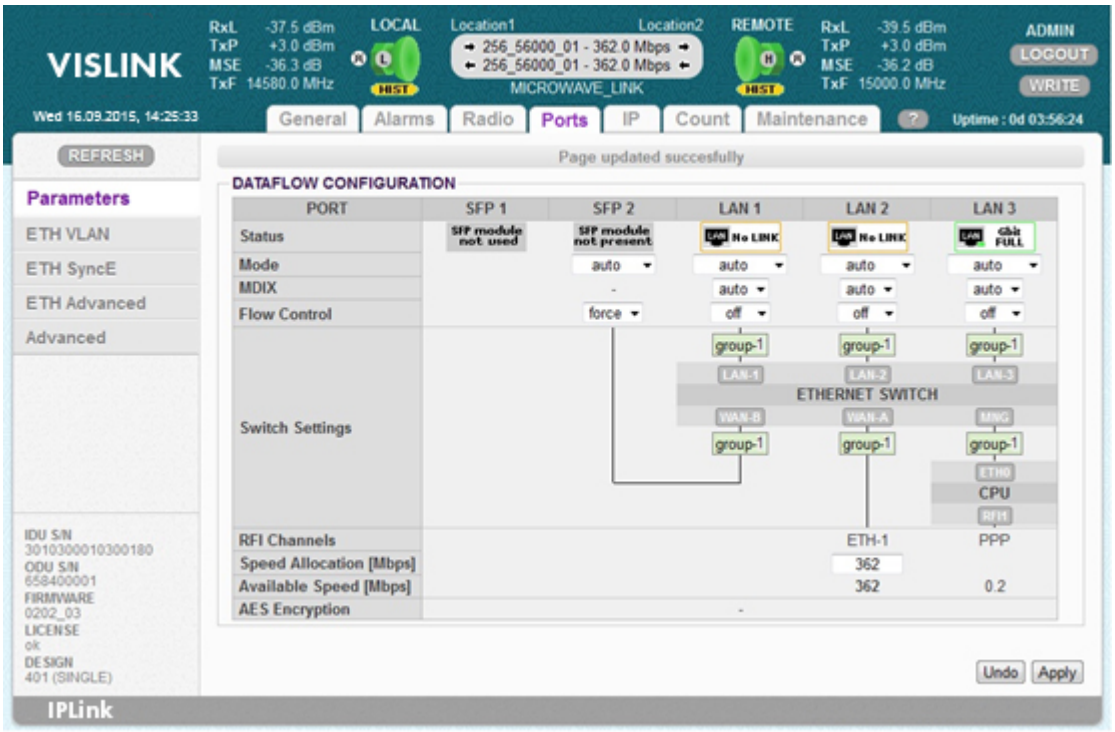

Figure 5-5 Example 1 – Ports Speed Setting at LOCATION 1

The configuration for IDU 2 at Location 2 is similar to the above GUI page examples, except the appropriate parameters are defined in Figure 5-1.

5.2. Example 2 – Out-of-Band MNG with NAT

Out-of-Band management configuration with NAT is a preferred scheme when just one link is supervised and management access is originated from provider side of the link. Management and data traffic must be separated at provider side in this mode. Communication with remote side is ensured by means of fixed internal low speed management channel (115 kbps), management traffic is routed through each management CPU inside IDU.

The application example is shown on the Figure 80. The configuration of the most important GUI pages at LOCATION 1 (provider side) is shown on Figure 4-2 to Figure 4-6.

This example describes an application where the SINGLE configuration/design is selected on both link sides and the modulation is set as QAM128 with 30 MHz bandwidth and the appropriate maximum data speed is about 169 Mbps. The IP address for both IDUs should be selected from different IP subnets. This is because the interconnection for both sides is routed using the IDU CPU. The slow separated management channel is used for periodical message exchanges between both IDUs and also for complete management traffic interconnection. The connection to the remote (customer) IDU is available by typing the following IP address, using an appropriate web browser:

- 192.168.3.201:1080

If alternative management access from this side (port LAN 3) is required, then the identical NAT record must be applied at the remote (customer) side (IDU 2).
In-band management can be combined with standard routed management access, when the customer side IP address range is added into the provider's static IP route table, this makes IDU 1 the gateway for this network. The NAT setting rules correspond with the explanation given in Section 4.8.3.

Out-of-Band management configuration with the NAT is supported by all configuration/designs (SINGLE, MULTI, AGGREGATE, PROTECTED).

Main Advantages:

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

Disadvantages:

- Management traffic uses slow channel (120 kbps).
- Management responses are slightly longer compared to In-Band management scheme.
- You need to understand NAT configuration techniques.

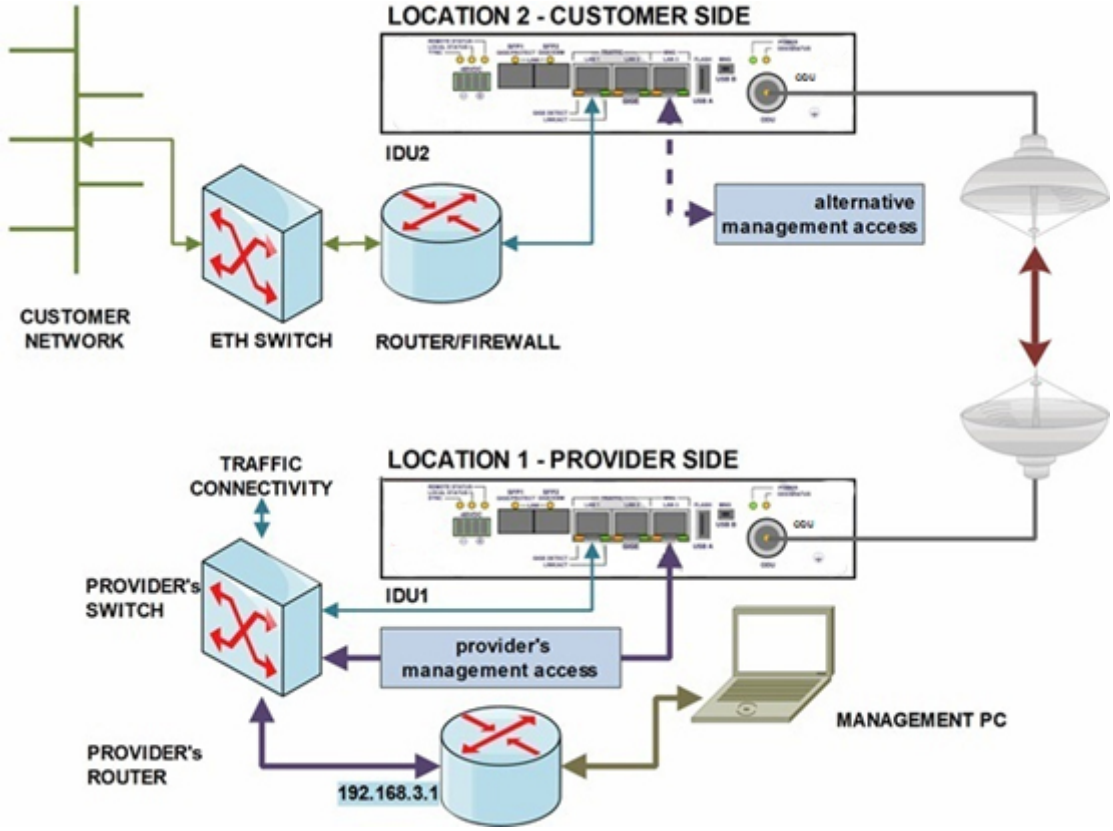

Figure 5-6 Example 2 – Out-of-Band Management Based on NAT

-	IDU1 (provider side)	IDU2 (customer side)
Maintenance | Advanced		
Design	Single	Single
IP | Address		
Local IP	10.10.10.10/24	10.10.9.9/24
Remote IP	10.10.9.9	10.10.10.10
Gateway IP	10.10.10.1	10.10.10.10
IP | Route/NAT		
NAT	Add 1080 10.10.9.9:80	Add 1080 10.10.10.10:80
Ports | Parameters	-	-
Speed Allocation [Mbps]	ETH1 = 362	ETH1 = 362
Ports | ETH VLAN		
Port Mode	Basic = all ports	Basic = all ports
Port Groups	1 = LAN3, MNG 2 = LAN1/2, WANA/B	1 = LANn3, MNG 2 = LAN1/2, WANA/B

Table 5-2 Out-of-Band MNG with NAT Settings

This example supposes that the SINGLE configuration/design is selected as the default type. The proper IP address setting must be entered, but applied later, together with IP NAT changes (chose **Continue** button at the intermediate IP window).

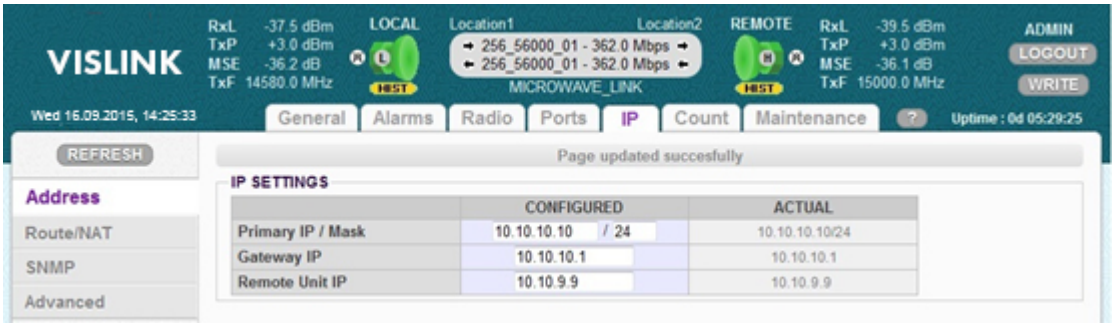

Figure 5-7 Example 2 – IP Address Setting at LOCATION 1

The most important step of configuring Out-of-Band management configuration is the proper configuration of the IP NAT setting. To do this:

1. Add the NAT record.
2. Apply all IP changes by clicking the **APPLY** button.

NOTE: This change must be confirmed on the pop-up window by clicking the **Write And Apply** button.

NOTE: You are required to login back into the system after applying any IP change. IP configuration changes don't influence data traffic (no data drop during IP re-initialization).

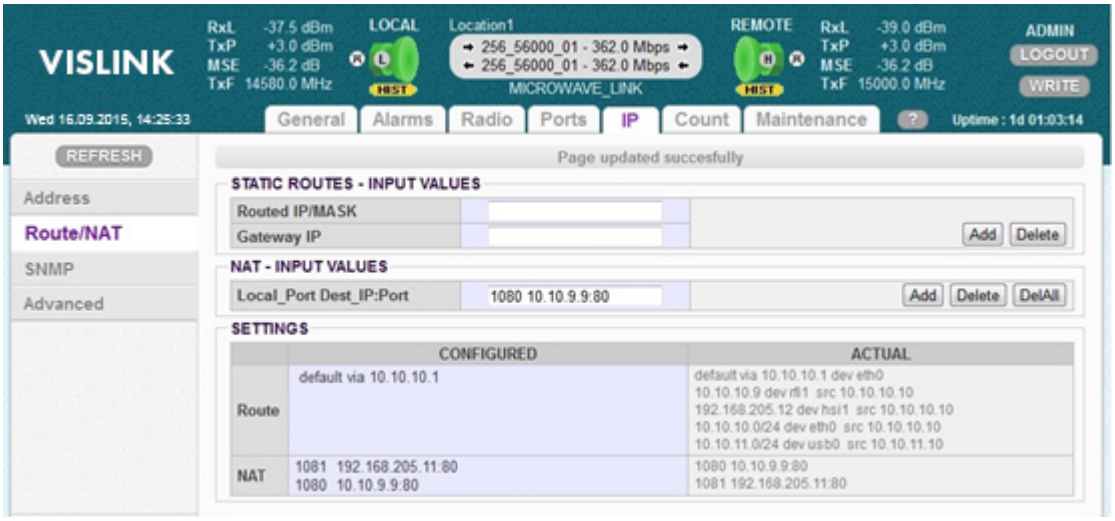

Figure 5-8 Example 2 – IP NAT Setting at LOCATION 1

3. Change the VLAN Port Mode and Port Group
4. Click APPLY.
5. Confirm the change by pressing **Continue** button

NOTE: Remote access to the IDU must be ensured with the same VLAN configuration on your network, otherwise the previous VLAN configuration will be returned after 120 seconds.

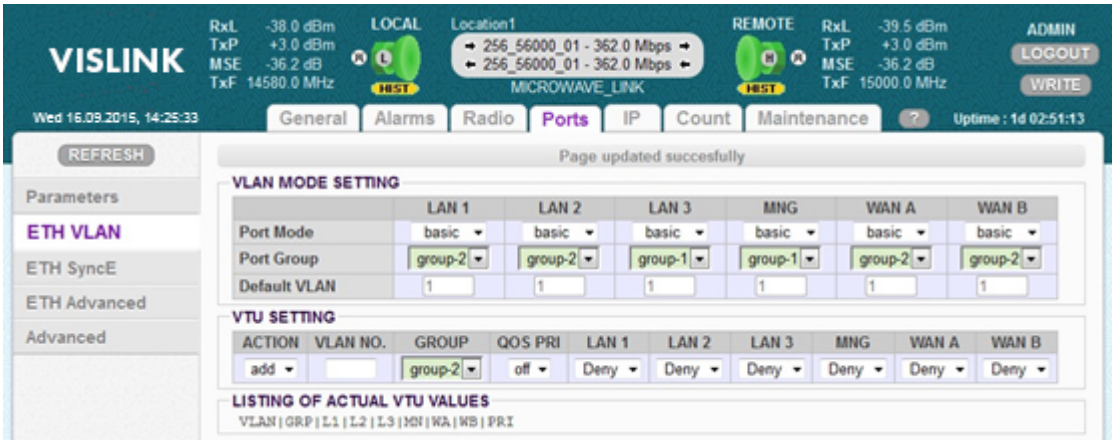

Figure 5-9 Example 2 – VLAN and Port Groups Setting at LOCATION 1

6. Configure the basic port parameters; Ethernet channel speed and LAN port modes.

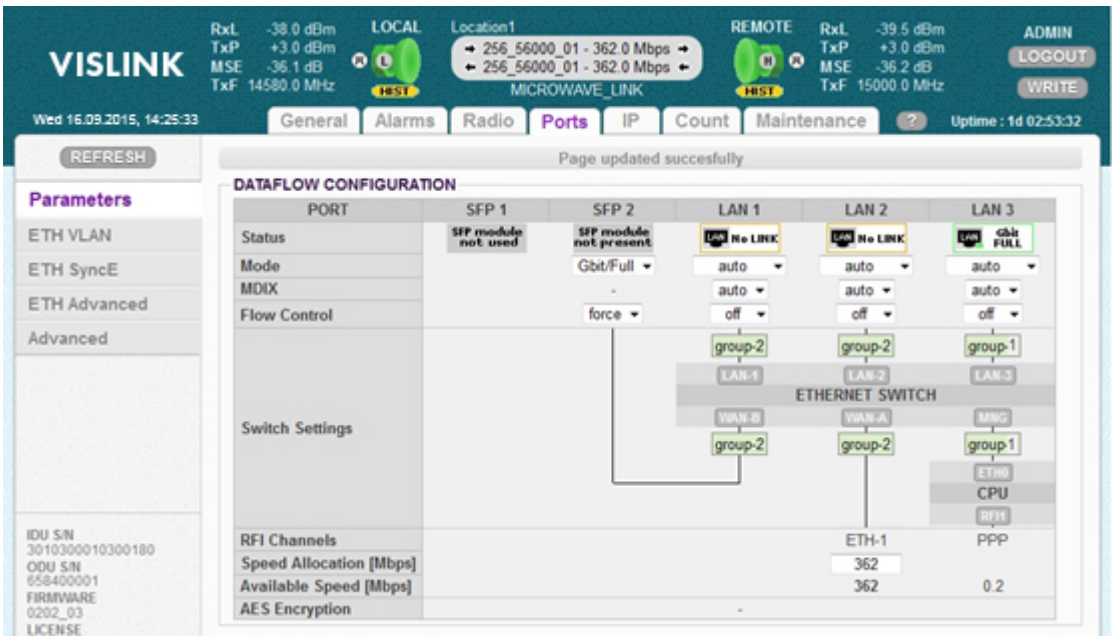

Figure 5-10 Example 2 – Ports Speed Setting at LOCATION 1

The configuration for IDU 2 at LOCATION 2 is similar to the above GUI pages, except with the parameters updated according to the definition in Figure 5-6 for IDU 2.

5.3. Example 3 – Out-of-Band MNG in Separated Channel

Out-of-Band management configuration in separated channel is a preferred scheme when more links in series are managed and management access is originated from any link location or from the provider's management node. Communication with the remote side is ensured by means of a configurable, separated, middle-speed traffic channel. Management traffic runs through the internal ETH switch inside each IDU. Management and data traffic are separated at the provider's side and they are then kept separate by a reserved standalone channel through radio links. Management access is also available from the opposite side (customer side) by a similar channel separation configuration.

The application example is shown in Figure 5-11. Configuration of the GUI pages at LOCATION 1 (provider side) is shown in Figure 5-12 to Figure 5-15.

This example describes the application where the MULTI configuration/design is selected on both link sides with the modulation set to QAM128 with 30 MHz bandwidth and the appropriate maximum data speed set to about 169 Mbps.

The IP addresses for both IDUs are from the same IP subnet, this is because this scheme is similar to the switched Ethernet network.

The slow separated management channel is also used in this configuration but only for periodical message exchanges between both IDUs. The alternative management connection is available through LAN 3 port on IDU 3. The capacity for the management channel should be configured in the range of about 1 Mbps to reserve the major capacity for data traffic.

The separate ETH management channel should be selected with a higher priority than is given to the data traffic channel. It prevents management access discontinuity in case the ACM is switched on and system speed reduces during bad receive conditions. The VLANs group setting is the general configuration which influences the correct function in this mode. It is explained in Section 4.7.5.

This mode isn't supported by the SINGLE configuration/design. All other configurations/designs (MULTI, AGGREGATE, PROTECTED) support this configuration mode.

Main Advantages:

- Separate management channel for local and remote IDU access, meaning that the whole system capacity is available for data traffic.

Disadvantages:

- Management traffic uses slow channel (120 kbps), management responses are longer in comparison to the In-Band management scheme.
- You are required to understand NAT configuration techniques.

	IDU1 (provider side)	IDU2 (customer side)	IDU3 (customer side)
Maintenance | Advanced			
Design	multi	multi	multi
IP | Address			
Local IP	10.10.10.10/24	10.10.10.9/24	10.10.10.8/24
Remote IP	10.10.10.9	10.10.10.10	10.10.10.7
Gateway IP	10.10.10.1	10.10.10.1	10.10.10.1
Ports | Parameters			
Speed Allocation [Mbps]	ETH1 = 362 ETH2 = 1	ETH1 = 362 ETH2 = 1	ETH1 = 362 ETH2 = 1
Ports | ETH VLAN			
Port Mode	basic = all ports	basic = all ports	basic = all ports
Port Groups	1 = lan3, mng, wanB 2 = lan1/2, wanA	1 = lan3, mng, wanB 2 = lan1/2, wanA	1 = lan2/3, mng, wanB 2 = lan1, wanA

Table 5-3 Out-of-Band Management Based on Separated Channel Settings

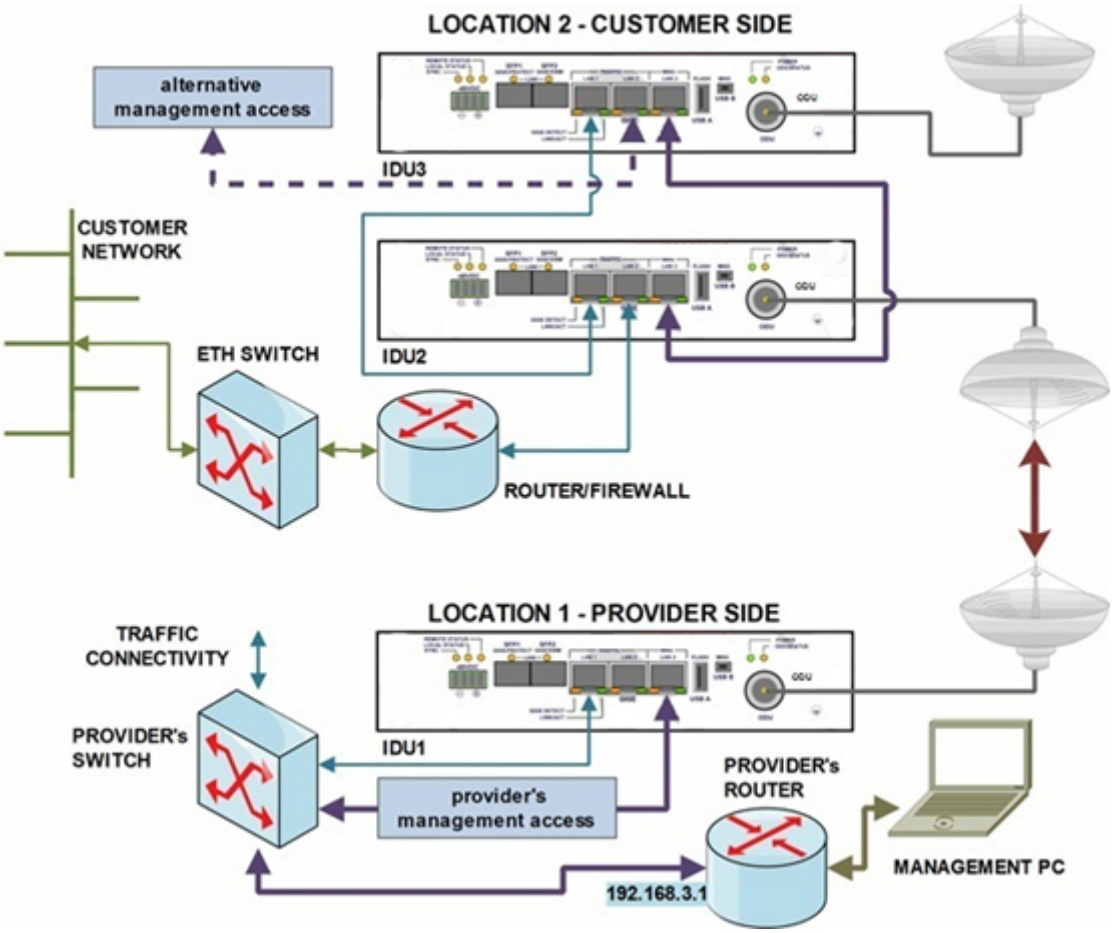

Figure 5-11 Example 3: Out-of-Band MNG in Separated Channel

1. The MULTI Configuration/design must by selected as the first step in the configuration process on both IDUs.

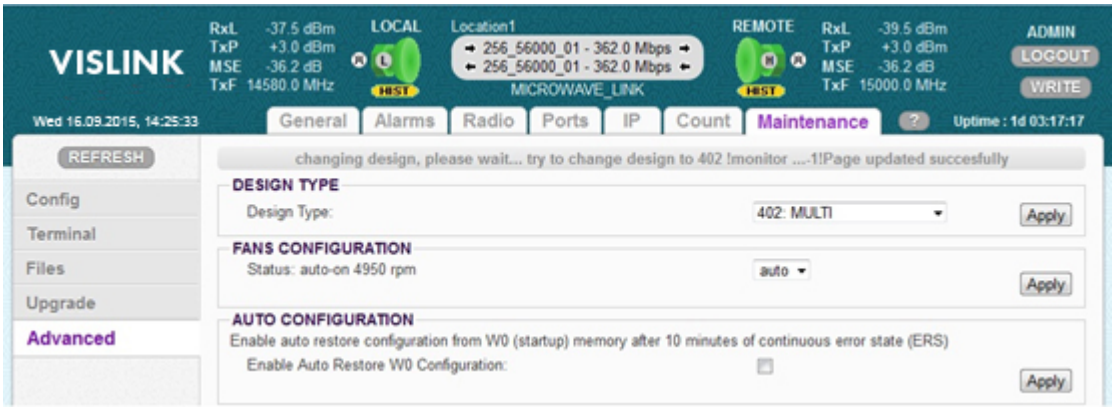

Figure 5-12 Example 3 – Selection MULTI Configurations at LOCATION 1

2. Enter the proper IP address setting.
3. Click **Apply**.

NOTE: You are required to login back into the system after applying any IP change. IP configuration changes don't influence data traffic (no data drop during IP re-initialization).

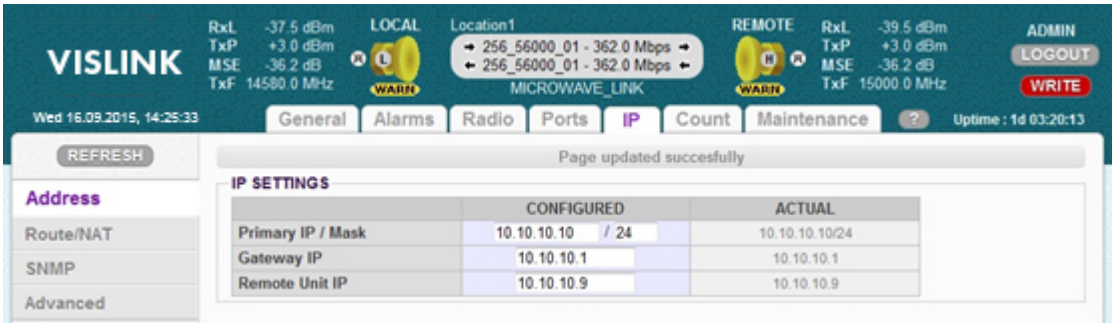

Figure 5-13 Example 3 – IP Address Setting at LOCATION 1

4. Appropriately change the VLAN Port Modes and Port Groups.
5. Save the changes by clicking the **APPLY** button.
6. Confirm this change in the pop-up window by clicking the **Continue** button

NOTE: Remote access to the IDU must be ensured with the same VLAN configuration on your network, otherwise the previous VLAN configuration will be returned after 120 seconds.

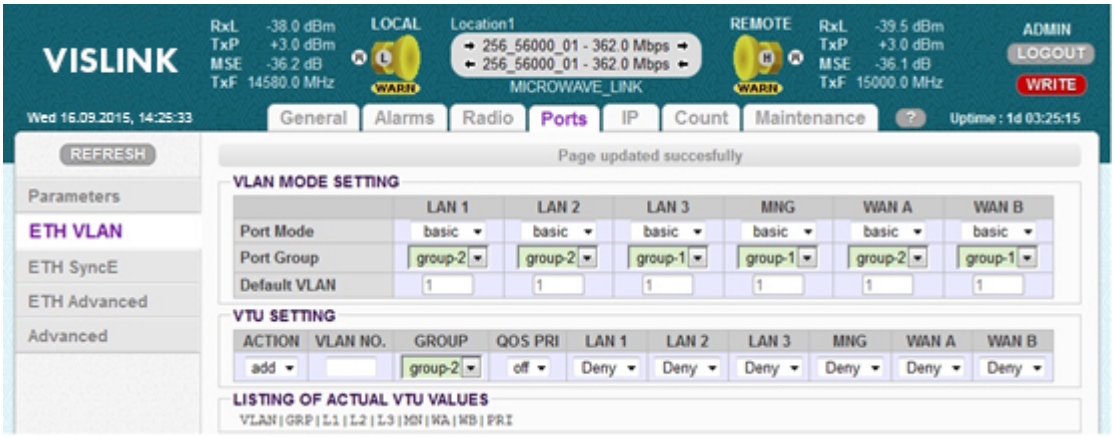

Figure 5-14 Example 3 – Port Modes and Port Groups Setting at LOCATION 1

The Ethernet channel ETH 2 is used as the separate management channel. Be sure there is enough free capacity for the management channel when channels ETH 4 and/or ETH 3 (with a higher priority) are also used, especially in ACM mode.

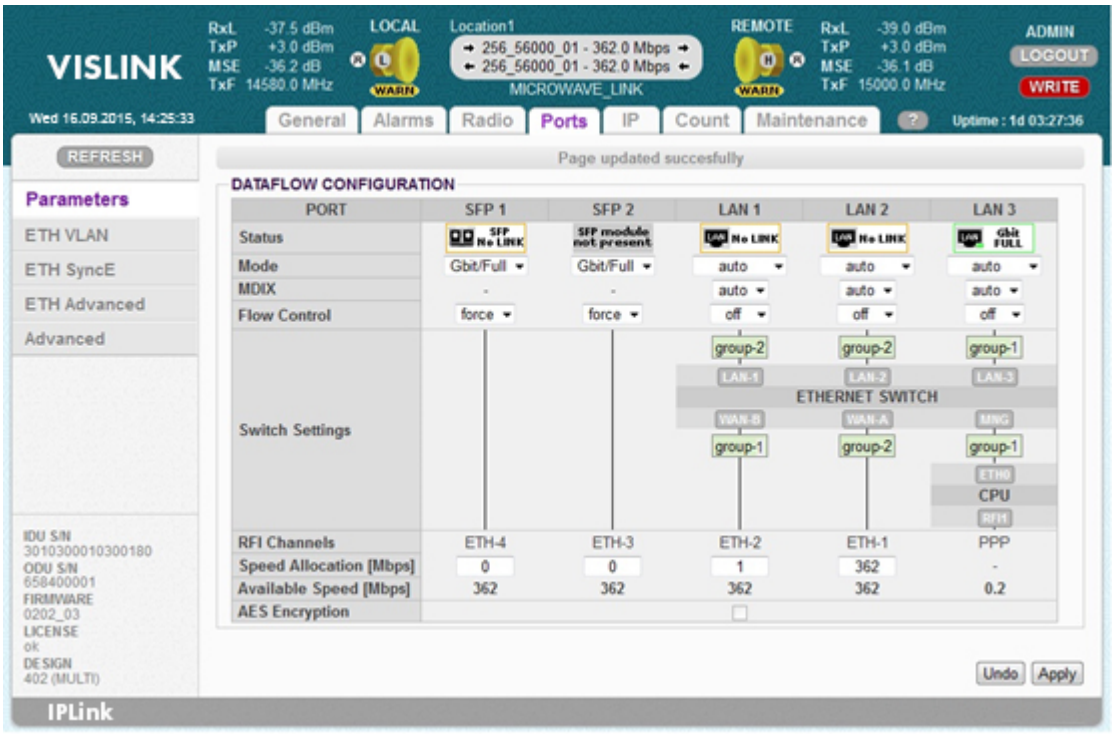

Figure 5-15 Example 3 – Ports Speed Setting at LOCATION 1

The configuration of other IDUs is similar to above explained GUI pages but with appropriate parameters defined in Figure 5-11.

5.4. Example 4 – VLAN Configuration

The main application for IDU VLAN functionality is the separation for different user data traffic in combination with the management of traffic separation by means of a VLAN. There are further VLAN modes that allow you to configure the same function with a different scheme.

The application example is shown in Figure 5-16. Configuration of the GUI pages at LOCATION 1 (provider side) and LOCATION 2 (customer side) are shown in Figure 5-17 to Figure 5-21.

This example describes an application using the SINGLE configuration/design on either side of the link. The modulation is QAM128, the bandwidth is set to 30 MHz and the maximum data speed is about 169 Mbps.

Four different data sources exist at the provider's side. Traffic 1-3 and management traffic must be marked in the provider's router or switch by a unique VLAN ID and the tagged frames then input via the provider's IDU. An appropriate VLAN configuration ensures that the specific ports are members of the specific VLANs. This is accomplished by combining VTU records and port VLAN modes. The VLAN setting corresponds with appropriate explanation in Section 4.7.5.

All VLAN configurations are supported by all configurations/designs (SINGLE, MULTI, AGGREGATE, PROTECTED).

Main Advantages

Simple separation of more data traffics.

- Common configuration for data and management traffic separation.

Disadvantages

- The VLAN configuration must be replicated at the provider's router or switch.
- All data sources share the same capacity.

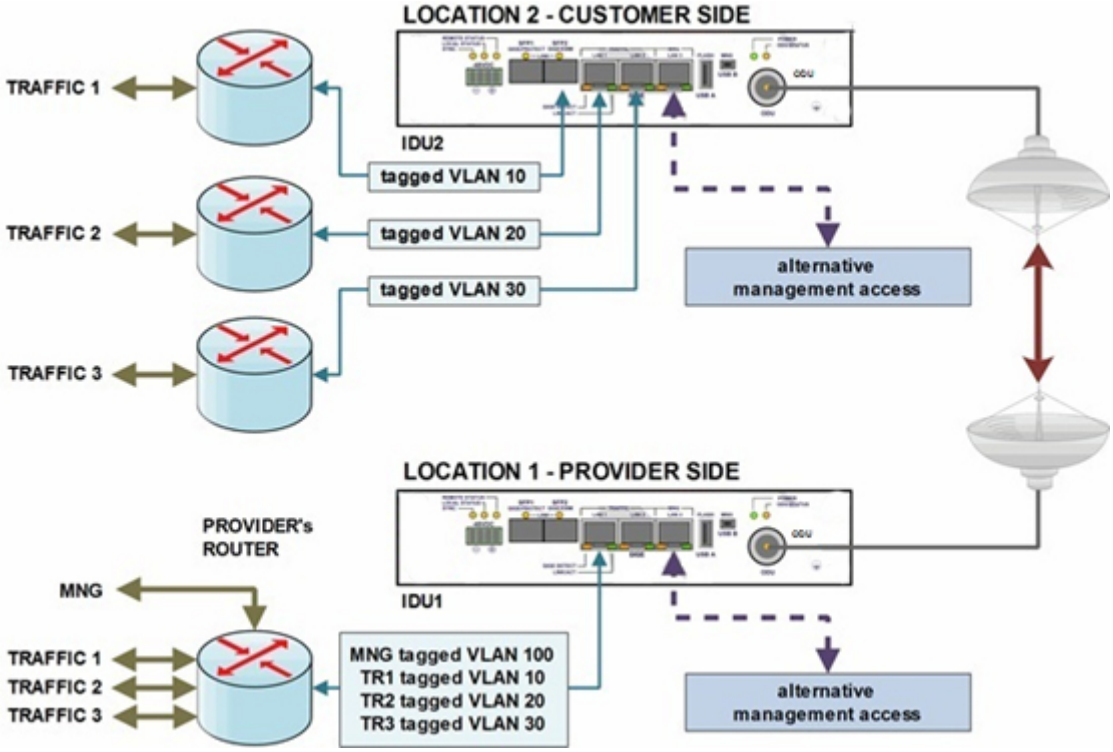

Figure 5-16 Example 4 – Application with VLANs

-	IDU1 (provider side)	IDU2 (customer side)
Maintenance | Advanced		
Design	Single	Single
IP | Address		
Local IP	10.10.10.10/24	10.10.10.9/24
Remote IP	10.10.10.9	10.10.10.10
Gateway IP	10.10.10.1	10.10.10.1
Ports | Parameters	-	-
Speed Allocation [Mbps]	ETH1 = 362	ETH1 = 362
Ports | ETH VLAN		
Port Mode	Basic = LAN2, WANB Access = LAN3, MNG Trunk = LAN1, WANA	Access = LAN3, MAN Trunk = LAN1/2, WANA/B
Port Groups	1 = LAN1/3, MNG. WANA 2 = LAN2, WANB	1 = all ports
VTU Setting	Add 100 group1 off TDUUTD Add 10 group1 off TDDDTD Add 20 group1 off TDDDTD Add 30 group1 off TDDDTD	Add 100 group1 off DDUUTD Add 10 group1 off DDDDTT Add 20 group1 off TDDDTD Add 30 group1 off DTDDTD

Table 5-4 VLAN Configuration Settings

1. The SINGLE configuration/design must by selected as the first step in the configuration process on both IDUs.

NOTE: The IP configuration is identical to the settings in Figure 5-1.

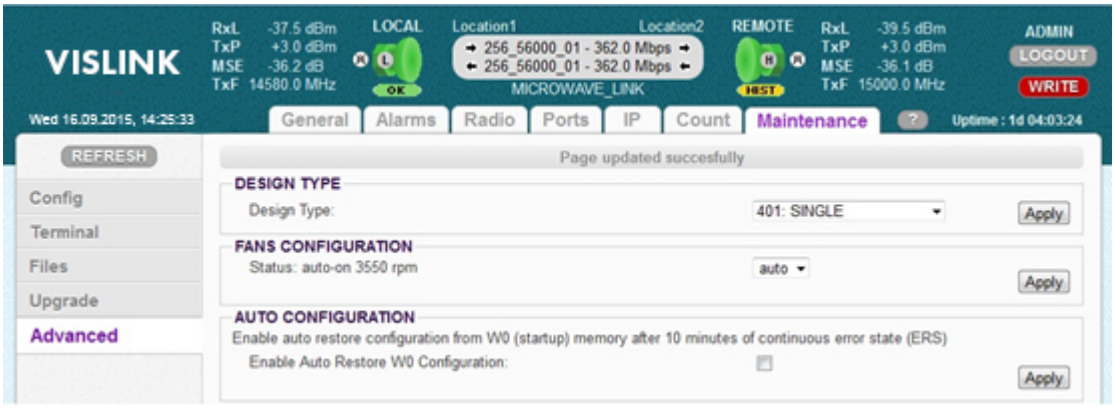

Figure 5-17 Example 4 – Select SINGLE Configuration at LOCATION 1

2. Add all VTU records, then change Port Modes and Port Groups.

NOTE: Trunk ports only accept tagged frames, which are contained in the VTU table and untagged frames which are internally assigned by the default VLAN ID (valid for this port). Access ports only accept untagged frames, which are internally assigned by the default VLAN ID (valid for this port). Switching rules for Trunk and Access ports are limited by Port Group rules and by the VTU records rules together. Ports in basic mode don't support any VTU records, only Port Group rules limit frame switching.

NOTE: All VLAN changes should be applied together by clicking the **APPLY** button. This change must be confirmed at the pop-up window by clicking the **Continue** button (remote access to the IDU must be ensured with a similar VLAN configuration in your network, otherwise the previous VLAN configuration will be returned after 120 seconds.

3. Configure the basic port parameters; Ethernet channel speed and LAN port modes.

Same configuration settings must be set on the customer side IDU. The VTU records in IDU 2 ensure that different LAN ports and internal the MNG port are assigned with just one VLAN, allowing for whole data traffic to be divided into ETH traffic, separated by channel.

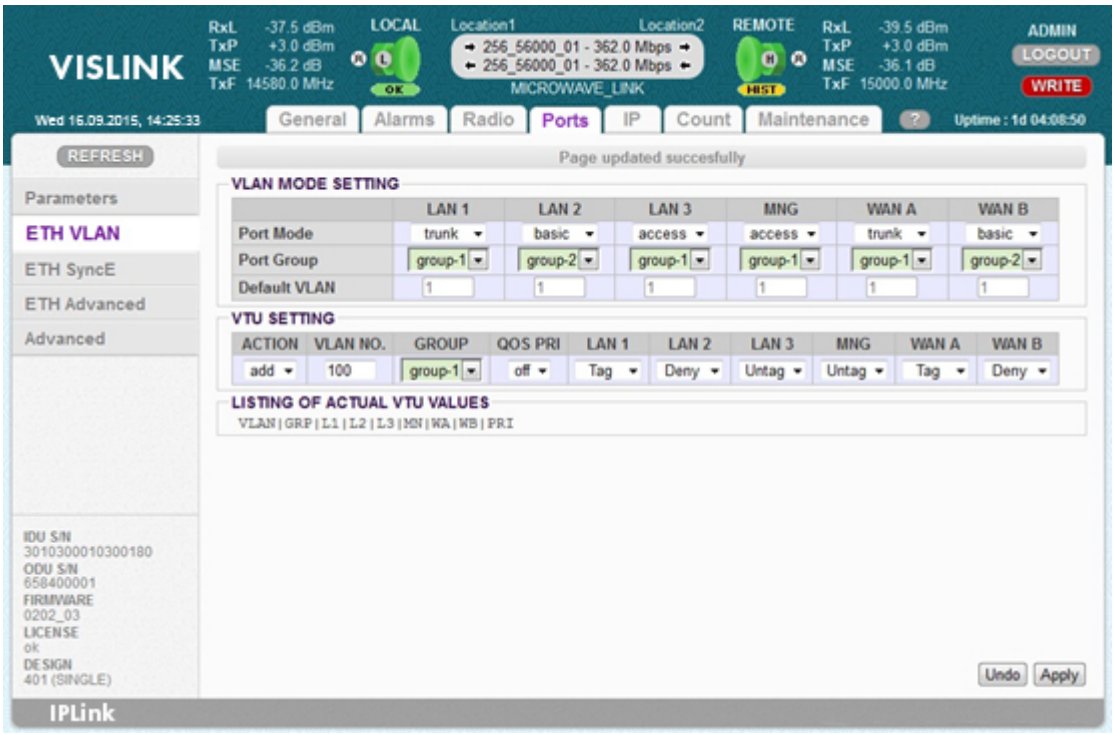

Figure 5-18 Example 4 – VLAN and Port Groups Setting at LOCATION 1

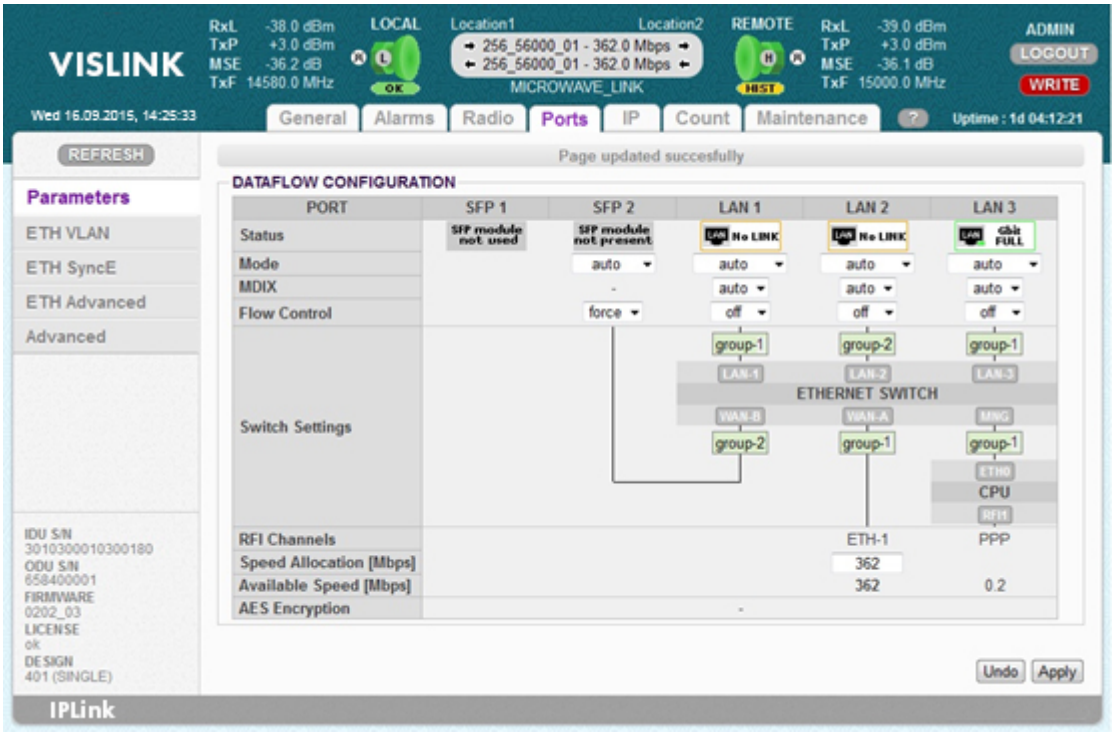

Figure 5-19 Example 4 – Ports Speed Setting at LOCATION 1

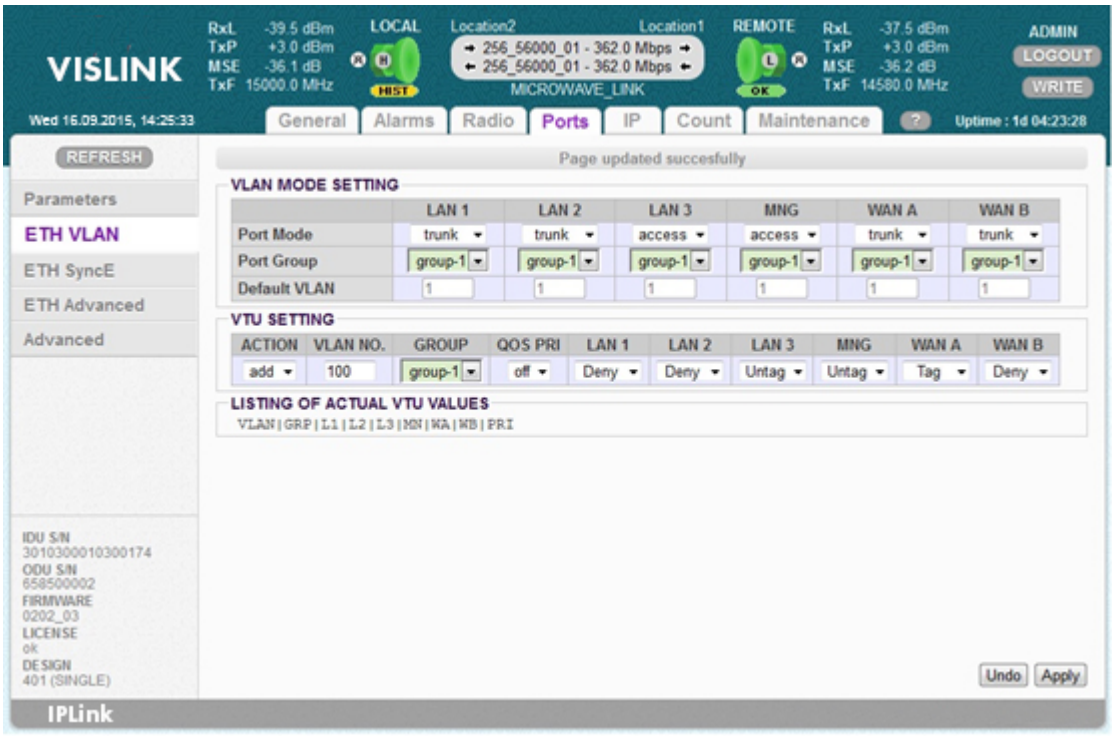

Figure 5-20 Example 4 – VLAN and Port Groups Setting at LOCATION 2

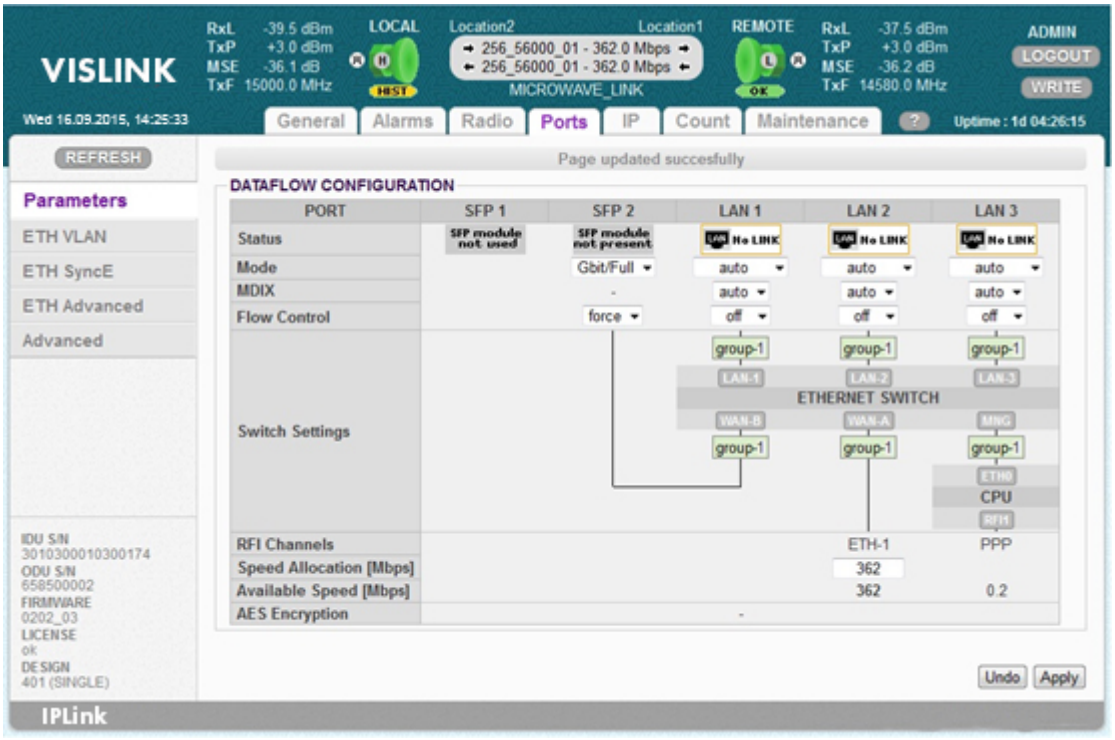

Figure 5-21 Example 4 – Ports Speed Setting at LOCATION 2

5.5. Example 5 – Advanced QOS Configuration

Prioritizing different data traffic streams by means of QOS is a major application for the IDU advanced QOS functionality. Further QOS modes exist to allow you to configure the same function with different QOS schemes.

The application example is shown in Figure 5-22. The configuration of the most important GUI pages at LOCATION 1 (provider side) and LOCATION 2 (customer side) is shown in Figure 5-23 to Figure 5-26.

This example describes an application using the SINGLE configuration/design on both link sides. The modulation is using QAM128 with a bandwidth of 30 MHz and the maximum data speed is about 169 Mbps. There are two different data sources and traffic is management with different function priorities at the provider's side. Traffic #1 is the stream with the highest priority (e.g. IPTV) traffic #2 is a stream with medium priority (e.g. Internet connection) and management traffic has the lowest priority in our example. We suppose that no traffic contains any priority declaration in the VLAN tag, but are tagged at the provider's side (when traffic contains a priority tag, it isn't necessary to use the following configuration. Frame priority is automatically assigned from PRI bits in the VLAN tag). The Strict 3xxx configuration ensures that frames with priority 6/7 will be unconditionally progressed with just one such packet in the buffer. No other frame (priority 0-5) will be progressed during this condition. The QOS setting corresponds with the appropriate explanation in Section 4.7.8.

All configurations/designs support QOS settings (SINGLE, MULTI, AGGREGATE, PROTECTED).

Main Advantages

- You can decide your own frame priorities independently to the original frame priority (from VLAN tag or from *IP v4/6 frame's TOS/DiffServ/TC)*
- Original frame priority can be changed and frames can progress with new priority settings.

Disadvantages

- All data sources in the same group share the same capacity.

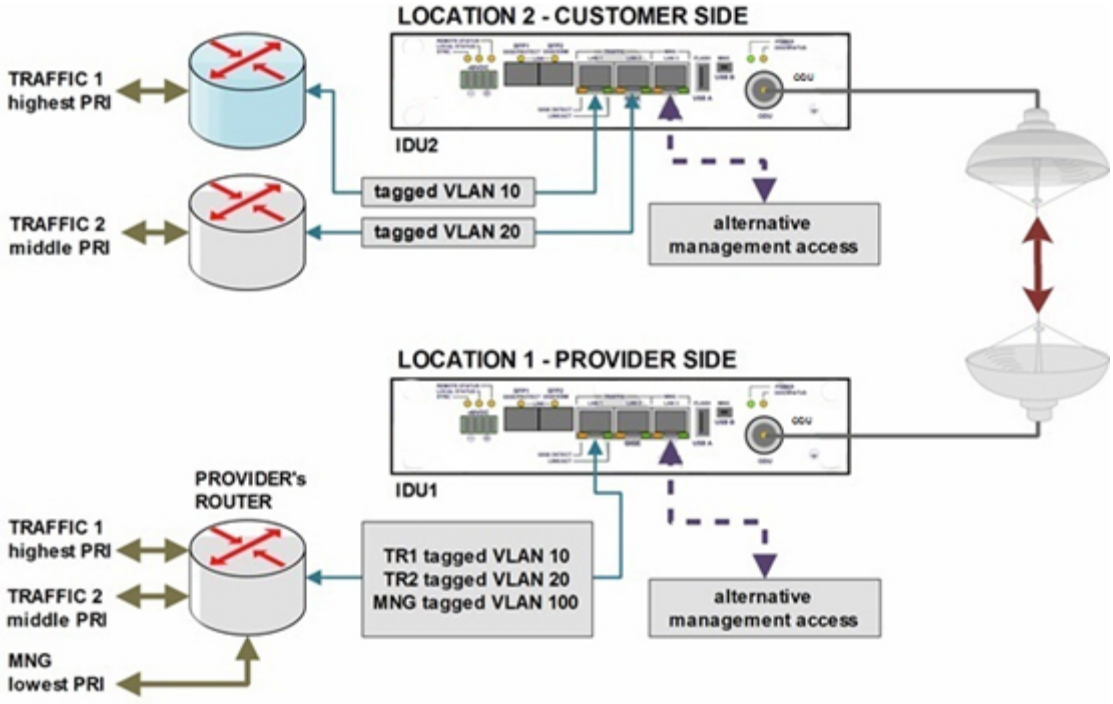

Figure 5-22 Example 5 – Application with Advanced QOS

-	IDU1 (provider side)	IDU2 (customer side)
Maintenance | Advanced		
Design	Single	Single
IP | Address		
Local IP	10.10.10.10/24	10.10.10.9/24
Remote IP	10.10.10.9	10.10.10.10
Gateway IP	10.10.10.1	10.10.10.1
Ports | Parameters		
Speed Allocation [Mbps]	ETH1 = 362	ETH1 = 362
Ports | ETH VLAN		
Port Mode	Access = LAN3, MNG Trunk = LAN1/2, WANA/B	Access = LAN3, MNG Trunk = LAN1/2, WANA/B
Port Groups	1 = all ports	1 = all ports
VTU Setting	Add 100 group1 0 TDUUTD Add 10 group1 7 TDDDTD Add 20 group1 5 TDDDTD	Add 100 group1 off DDUUTD Add 10 group1 off TDDDTD Add 20 group1 off DTDDTD

Ports | ETH Advanced		
QOS Modes	Weighted = LAN1/2/3, MNG, WANB Strict 3xxx = WANA	Weighted = LAN1/2/3, MNG, WANB Strict 3xxx = WANA
Priority Policy	All = all ports	All = WANA/B Port only = LAN1/2/3, MNG
Port Priority	0 = all ports	7 = LAN1 5 = LAN2 0 = LAN3, MNG, WANA/B
Priority Override	VTU = LAN1/3, MNG Off = LAN2, WANA/B	Off = all ports

Table 5-5 Advanced QOS Configuration Settings

This example assumes the SINGLE configuration/design is selected as the default design type.

The QOS PRI value is used for QOS priority definition for each specific VLAN frame.

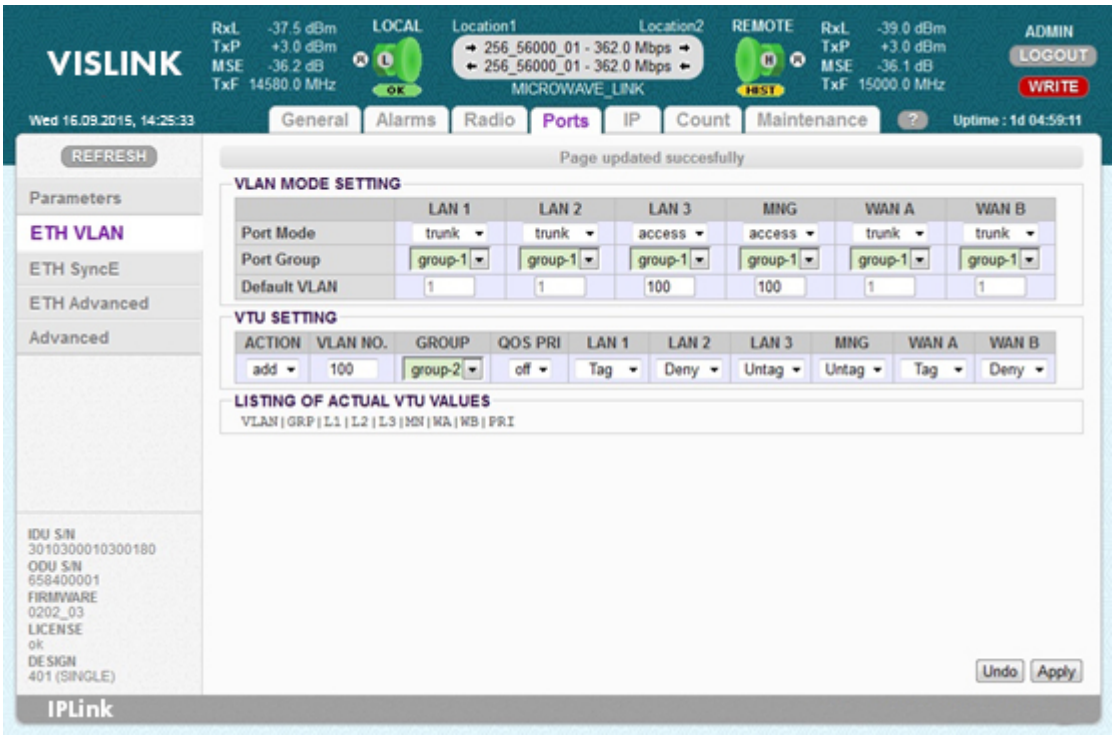

Figure 5-23 Example 5 – VLAN with QOS PRI Setting at LOCATION 1

The QOS modes and parameters are defined in ETH advanced section. The VTU priority override option is used for QOS discrimination at this side.

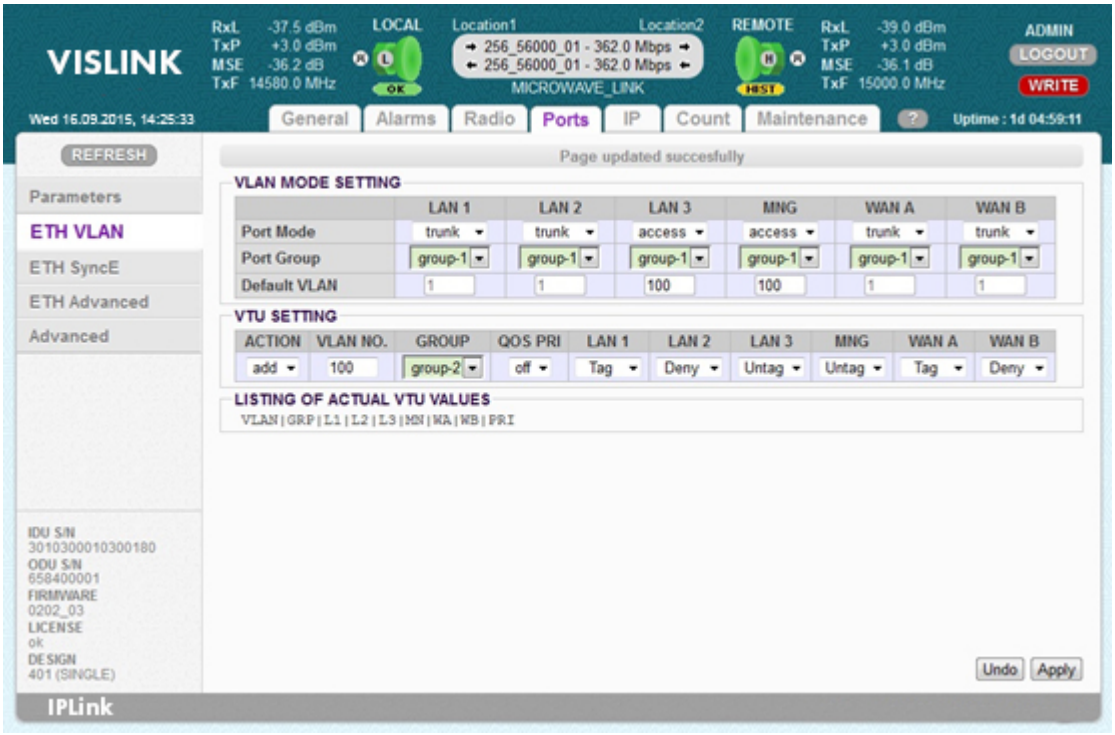

Figure 5-24 Example 5 – Advanced QOS Setting at LOCATION 1

The same configuration is done at the opposite side of the link. The Port Priority policy option is used for QOS discrimination at the local side.

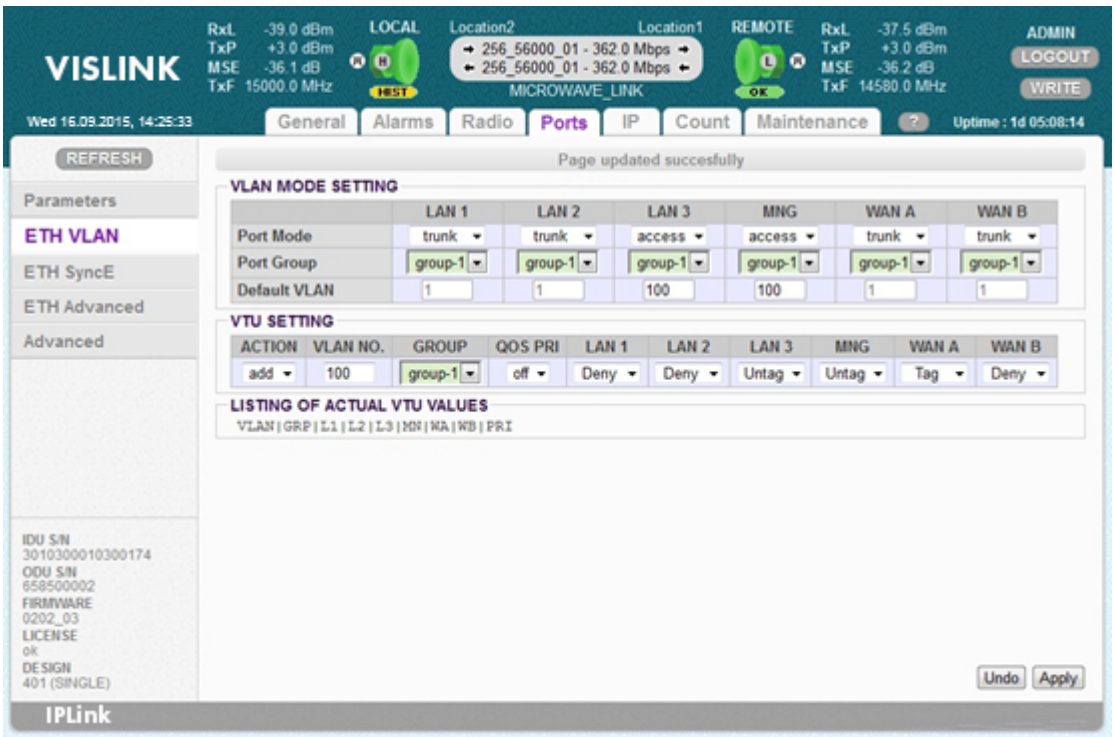

Figure 5-25 Example 5 – VLAN with QOS PRI Setting at LOCATION 2

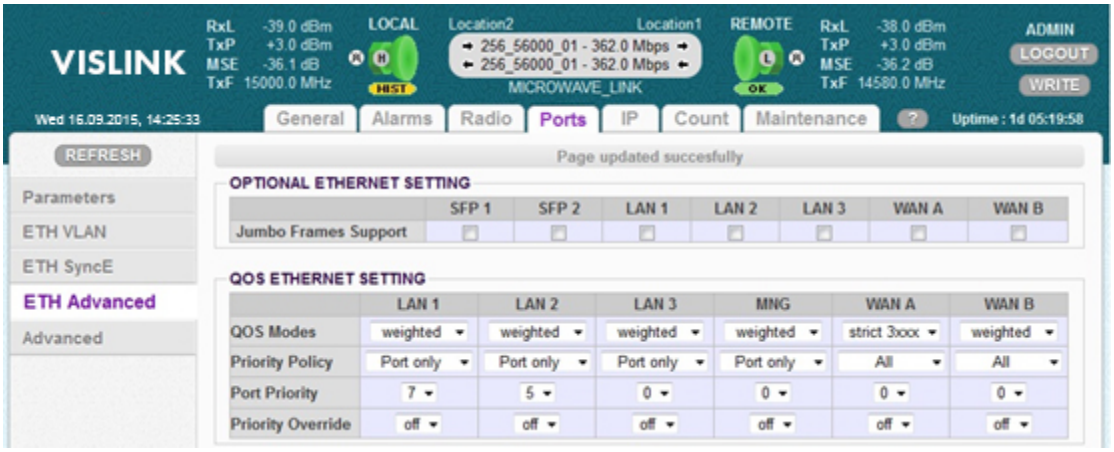

Figure 5-26 Example 5 – Advanced QOS Setting at LOCATION 2

5.6. Example 6 – Sync ETH Configuration

The configuration of the Sync ETH function is the main application for the synchronous clock transfer over a packet-based system. The remote synchronization of ETH traffic to a referenced source-signal must be properly configured according to the required clock transfer scheme.

The application example is shown in Figure 5-27. The configuration of the GUI pages at LOCATION 1 (provider side) and LOCATION 2 (customer side) are shown in Figure 5-28 to Figure 5-31.

This example describes the application using the MULTI configuration/design on all link sides with the modulation set to QAM128 with a bandwidth of 30 MHz, the maximum data speed is about 169 Mbps.

There are two sets of different data and management traffic at the provider side. Traffic #1 is the stream which is synced to the global reference signal (e.g. GPS timing) this must be configured at the provider IDU as the reference source for SyncETH distribution, traffic #2 is a standard stream and doesn't require SyncETH support (e.g. Internet connection). The same is valid for management traffic. Ports LAN 1-2 at the remote side IDU work in SyncETH mode and they are synced to the remote reference time (port LAN 1 at IDU1). SyncETH is also distributed to the next IDU and then on to the next base station.

The SyncETH setting corresponds with appropriate explanation in Section 4.7.7.

All SyncETH configurations are supported by the SINGLE, MULTI and AGGREGATE configurations/designs.

NOTE: The PROTECTED configuration/design doesn't support this mode.

Main Advantages:

- Synchronous clock transfers over a packet based system.
- SyncETH chaining over more links.

Disadvantages:

- Not supported in Protection mode.

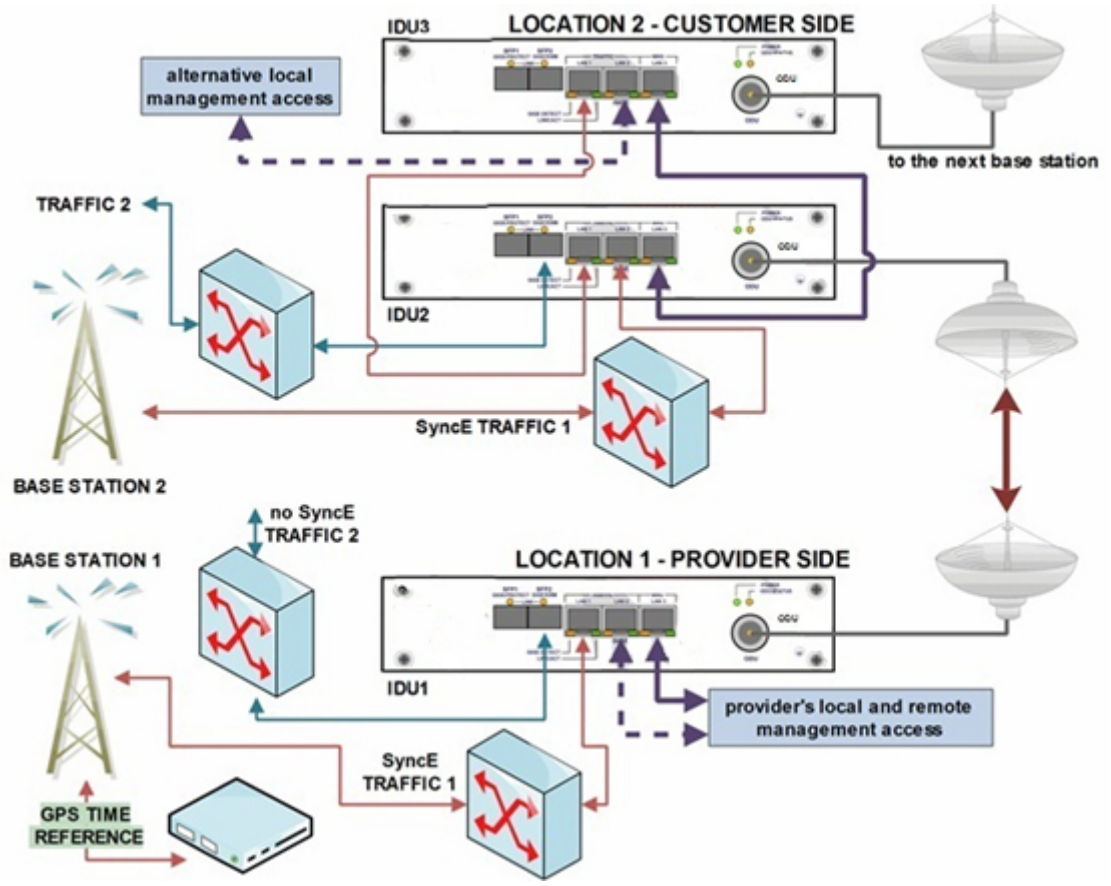

Figure 5-27 Example 6 – Application with Synchronous Ethernet

-	IDU1 (provider side)	IDU2 (customer side)	IDU3 (customer side)
Maintenance | Advanced			
Design	Multi	Multi	Multi
IP | Address			
Local IP	10.10.10.10/24	10.10.10.9/24	10.10.10.8/24
Remote IP	10.10.10.9	10.10.10.10	10.10.10.7
Gateway IP	10.10.10.1	10.10.10.1	10.10.10.1
Ports | Parameters			
Speed Allocation [Mbps]	ETH1 = 100 ETH2 = 1 ETH3 = 70	ETH1 = 100 ETH2 = 1 ETH3 = 70	ETH1 = 50 ETH2 = 1 ETH3 = 70
Ports | ETH VLAN			
Port Mode	Basic = all ports	Basic = all ports	Basic = all ports
Port Groups	1 = LAN2/3, MNG, WANB 2 = LAN1, WANA	1 = LAN3, MNG, WANB 2 = LAN1/2, WANA	1 = LAN2/3, MNG, WANB 2 = LAN1, WANA
Ports | Sync ETH			
SyncE Reference	LAN1	RF	LAN1
Port Synchronization	-	LAN1, LAN2	-

Table 5-6 Sync ETH Configuration Settings

This example assumes that the MULTI configuration/design is selected as the default.

1. Configure the correct speed assignment. This example combines SyncE functionality with Out-of-Band management mode in a separate ETH channel.

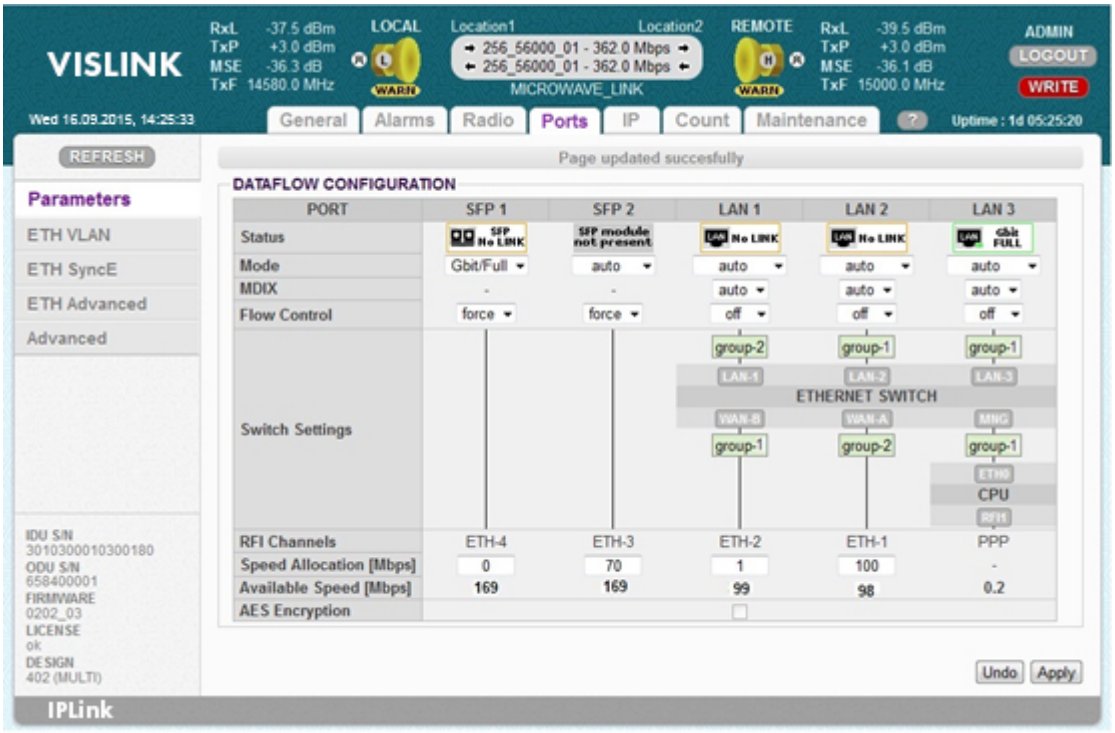

Figure 5-28 Example 6 – Ports Speed Setting at LOCATION 1

2. The SyncE parameters are defined in ETH SyncE section (see Section 4.7.7). Port LAN 1 is selected as the reference source, the RF stream is automatically synced to the reference when the clock recovery status is locked. The IDU uses the recovered CLK from LAN 1 as the main clock reference for both modem and LAN parts.

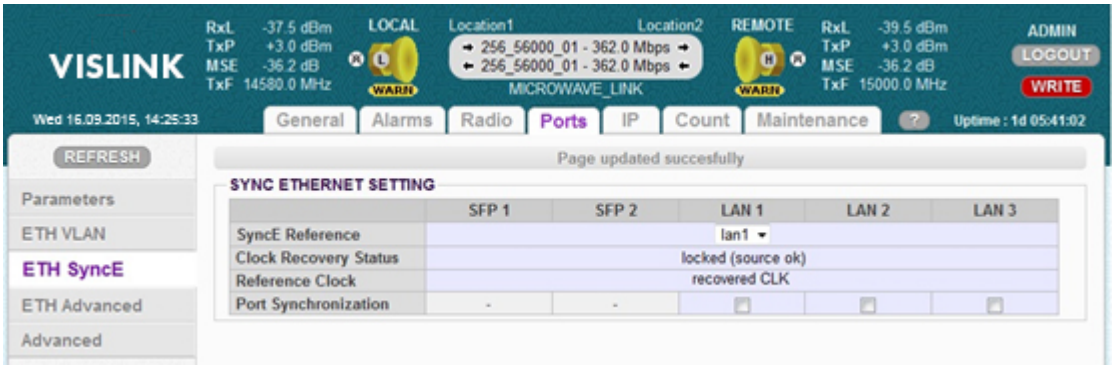

Figure 5-29 Example 6 – SyncETH Setting at LOCATION 1

NOTE: The same configuration settings are applied at the opposite side of the link. The receive RF stream is selected as the reference source. Selected LAN ports are automatically synced to this reference when the clock recovery status is locked. The IDU uses recovered CLK from an RF block as the main clock reference for both modem and LAN parts.

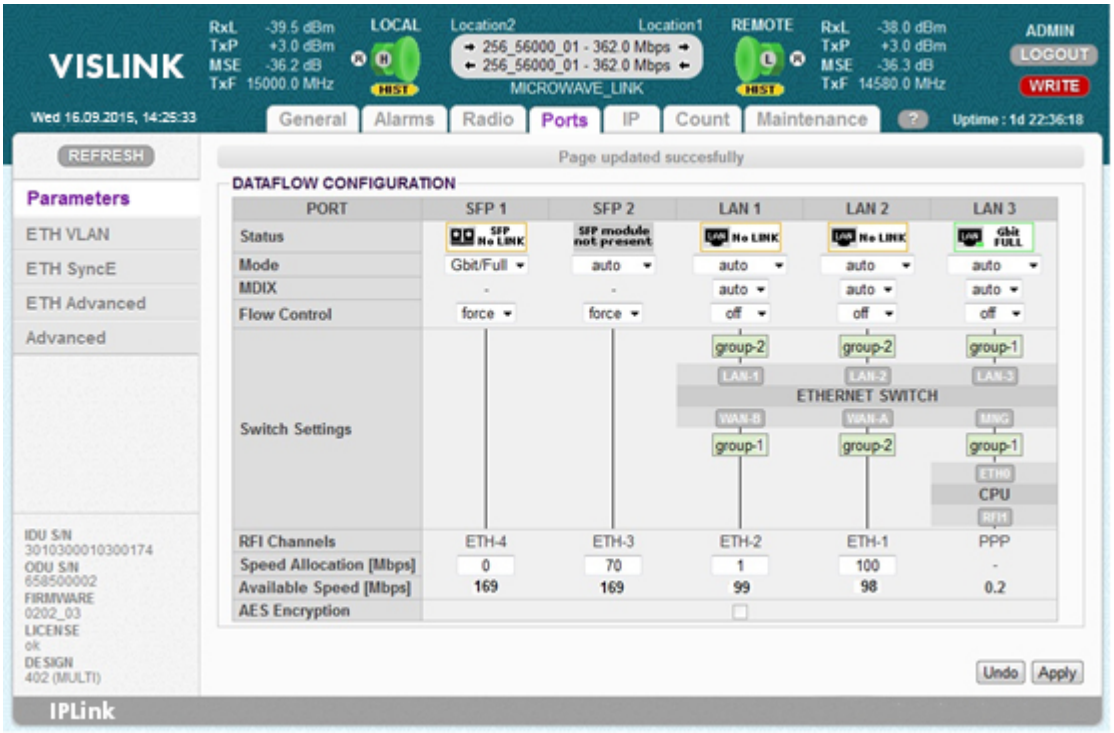

Figure 5-30 Example 6 – Ports Speed Setting at LOCATION 2

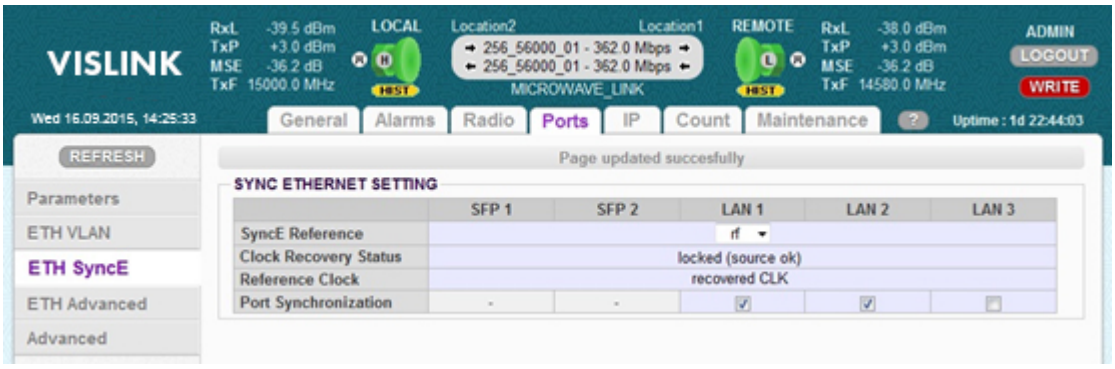

Figure 5-31 Example 6 – SyncETH Setting at LOCATION 2

IDU 3 is configured in a similar way to the above GUI pages but with appropriate parameters defined in Figure 5-27.

5.7. Example 7 – Basic 1+1 HSB/SD Protection Scheme

The basic 1+1 protection schemes ensure the correct data transmission over the microwave link if a specific HW block failure occurs or receive conditions degrade (multipath fading, …). The 1+1 / HSB (hot-standby) protection mode protects against system HW failures (hitless protects against ODU_Rx, IDU_RxAFE, with short data-drop protects against ODU_Tx, IDU_TxAFE).

The 1+1 / SD (space diversity) protects moreover against multipath fading. 1+1 / HSB mode uses one antenna via a directional coupler, two ODUs are connected into this coupler. The 1+1 / SD mode uses two antennas separated by a specific distance with just one ODU connected into each antenna. Just one transmitter is active in protection schemes (second one is automatically muted). Two receivers accept an identical signal and the master IDU decides which stream is used for final data de-multiplexing. The basic software difference between HSB and SD mode is; in SD mode, with transmitter failure detection, there is no switch-over between active and muted transmitter.

The application example for 1+1 / HSB mode is shown in Figure 5-32.The configuration of the GUI pages at LOCATION 1 (provider side) are shown in Figure 5-33 to Figure 5-39.

This example describes the application using the PROTECTED configuration/design on both sides of the link. The modulation is QAM128 with the bandwidth set to 30 MHz and the maximum data speed is about 169 Mbps.

Management access is similar to that shown in Section 5.1. All data sources are connected into the master unit (IDU 1, IDU 3) the slave and master IDUs are interconnected by fiber optic cable via ports SFP 1. The protection setting rules correspond with the appropriate explanation in Section 4.7.3.

Main Advantages

- One frequency pair is used.
- Just one cable between the master and slave IDU.
- Simple SW reconfiguration from master to slave IDU mode.
- Possible management access from master or slave units.

Disadvantages

- No hitless protection against transmitter failure.
- No protection against multipath fading in HSB mode.
- No protection against data interface part failure at master IDU.
- You are required to understand NAT configuration techniques.

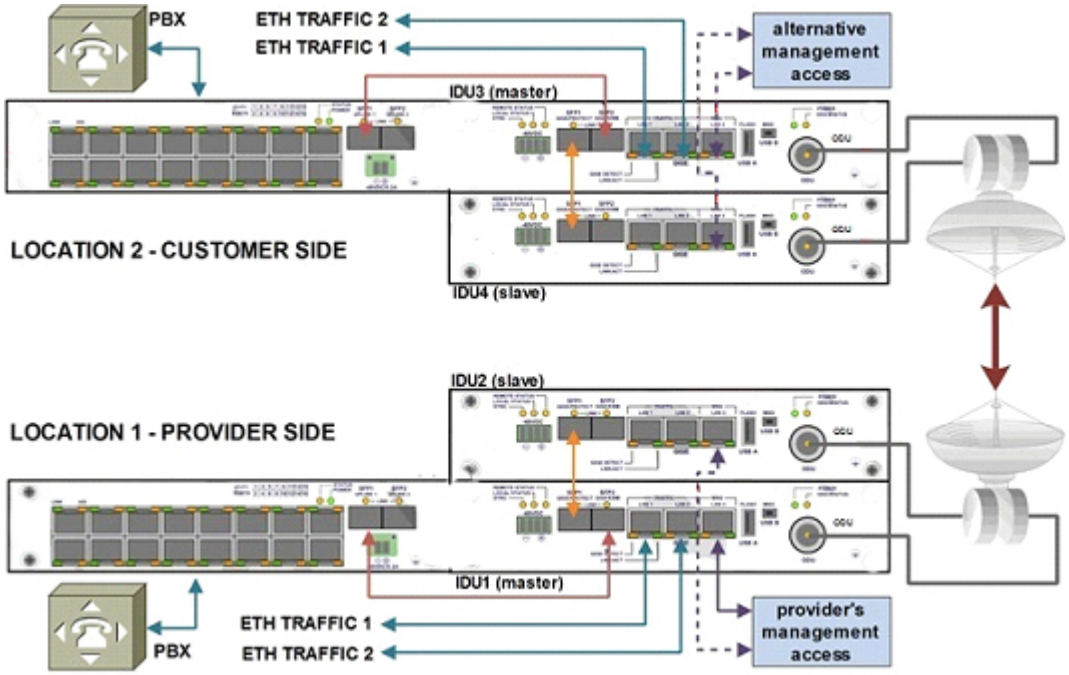

Figure 5-32 Example 7 – 1+1 HSB Protection Scheme with NAT Management

-	IDU1	IDU2	IDU3	IDU4
General | Protection				
Configuration	Master/HSB	Slave/HSB	Master/HSB	Slave/HSB
IP | Address				
Local IP	10.10.10.10/24	10.10.10.11/24	10.10.9.10/24	10.10.9.11/24
Remote IP	10.10.9.10	10.10.9.11	10.10.10.10	10.10.10.11
Protection IP	10.10.10.11	10.10.10.10	10.10.9.11	10.10.9.10
Gateway IP	10.10.10.1	10.10.10.1	10.10.9.1	10.10.9.1
IP | Route/NAT				
Static Routes (for diagonal unit)	10.10.9.11/32 via 10.10.10.11	10.10.9.10/32 via 10.10.10.10	10.10.10.11/32 via 10.10.9.11	10.10.10.10/32 via 10.10.9.10
NAT	1080 10.10.10.11:80 1180 10.10.9.10:80 1280 10.10.9.11:80	1080 10.10.10.10:80 1180 10.10.9.11:80 1280 10.10.9.10:80	1080 10.10.9.11:80 1180 10.10.10.10:80 1280 10.10.10.11:80	1080 10.10.9.11:80 1180 10.10.10.11:80 1280 10.10.10.10:80
Radio | Parameters				
Tx Frequency	14580 MHz	14580 MHz	15000 MHz	15000 MHz
Tx Power	3 dBm	3 dBm	3 dBm	3 dBm
Ports | Parameters				
Speed Allocation [Mbps]	ETH1 = 60 ETH2 = 60 ETH3 = 34	ETH1 = 60 ETH2 = 60 ETH3 = 34	ETH1 = 60 ETH2 = 60 ETH3 = 34	ETH1 = 60 ETH2 = 60 ETH3 = 34
Ports | ETH VLAN				
Port Mode	Basic = all ports	Basic = all ports	Basic = all ports	Basic = all ports
Port Groups	1 = LAN3, MNG 2 = LAN 2, WANA 3 = LAN 1, WANB	1 = LAN 3, MNG 2 = LAN 2, WANA 3 = LAN 1, WANB	1 = LAN 3, MNG 2 = LAN 2, WANA 3 = LAN 1, WANB	1 = LAN 3, MNG 2 = LAN 2, WANA 3 = LAN 1, WANB

Table 5-7 Basic 1+1 HSB/SD Protection Scheme Settings

1. Set the Protection mode configuration setting to **OFF** (this should be activated by default on both IDUs after changing to the PROTECTED configuration/design).

NOTE: In this mode only port LAN 3 (and USB B) are used to manage the connection, the ODU transmitter is automatically muted. This prevents any Ethernet loops or radio interferences during the configuration process.

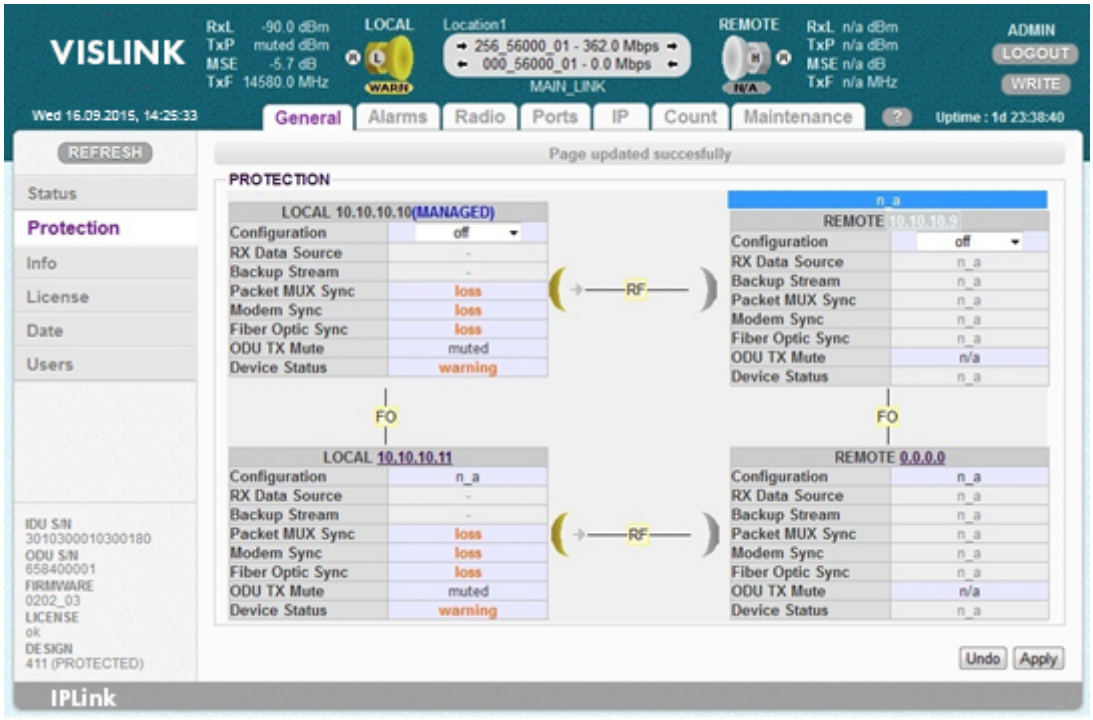

Figure 5-33 Example 7 – Default Protection Off

2. Enter the correct IP setting
3. Click the **Continue** button when the pop-up window shows.

NOTE: Apply the IP settings later, together with IP NAT changes.

4. Enter the required NATs and one static route.

NOTE: Add all NAT records, then add the necessary static route to the diagonal IDU and

5. Apply all IP changes by clicking the **APPLY** button.
6. Confirm at the pop-up window by clicking the **Write And Apply** button.

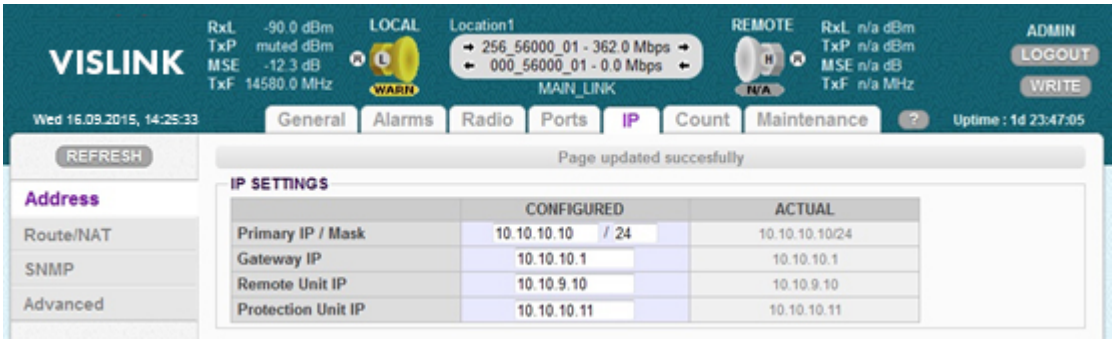

Figure 5-34 Example 7 – IP Address Setting at IDU1 – LOCATION 1

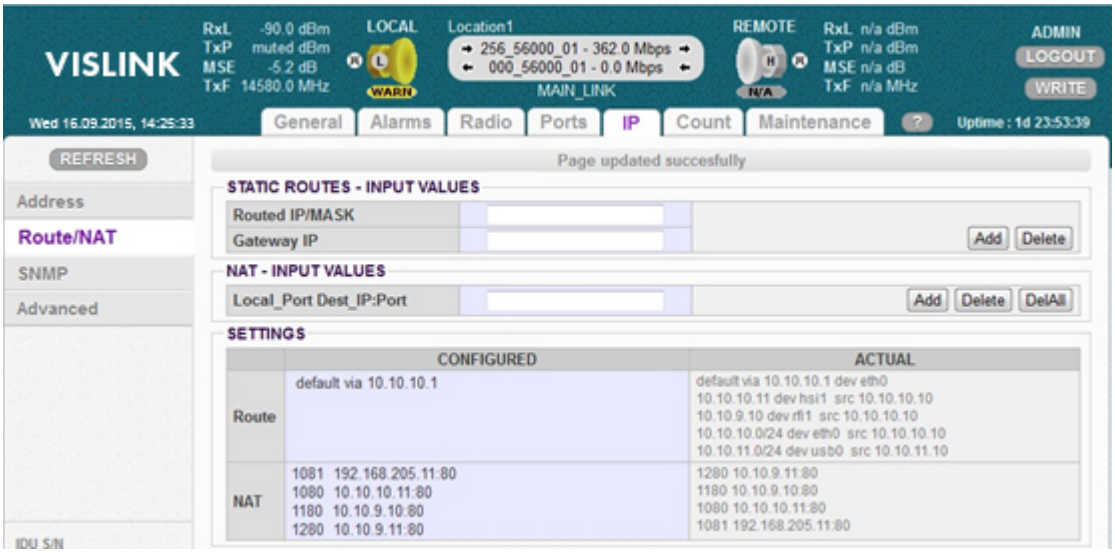

Figure 5-35 Example 7 – IP NAT and Static Route Setting at IDU1 – LOCATION 1

7. Configure the basic radio parameters.

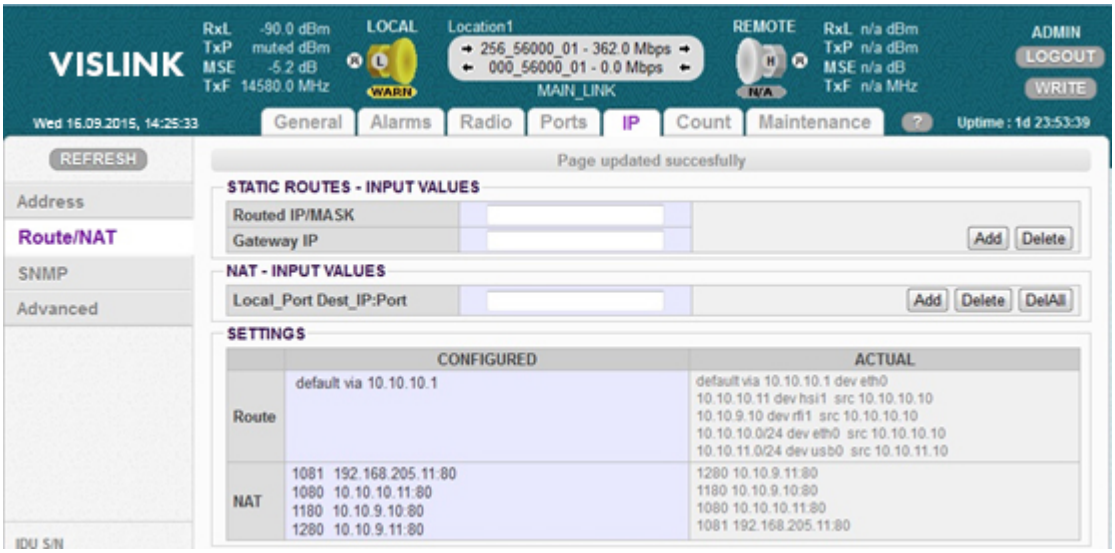

Figure 5-36 Example 7 – Basic Radio Parameters at IDU1 – LOCATION 1

8. Configure the Port Groups and Basic Port parameters according to the defined connection block scheme.

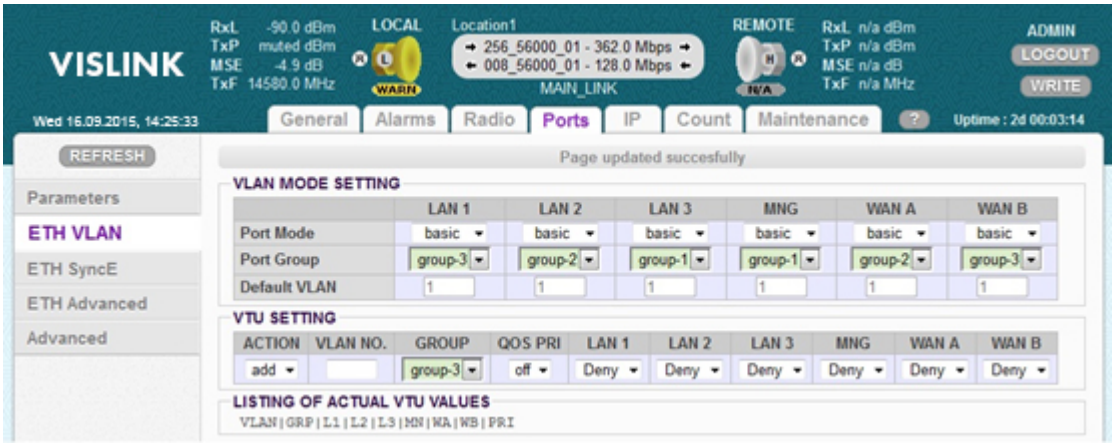

Figure 5-37 Example 7 – Port Groups Setting at IDU1 – LOCATION 1

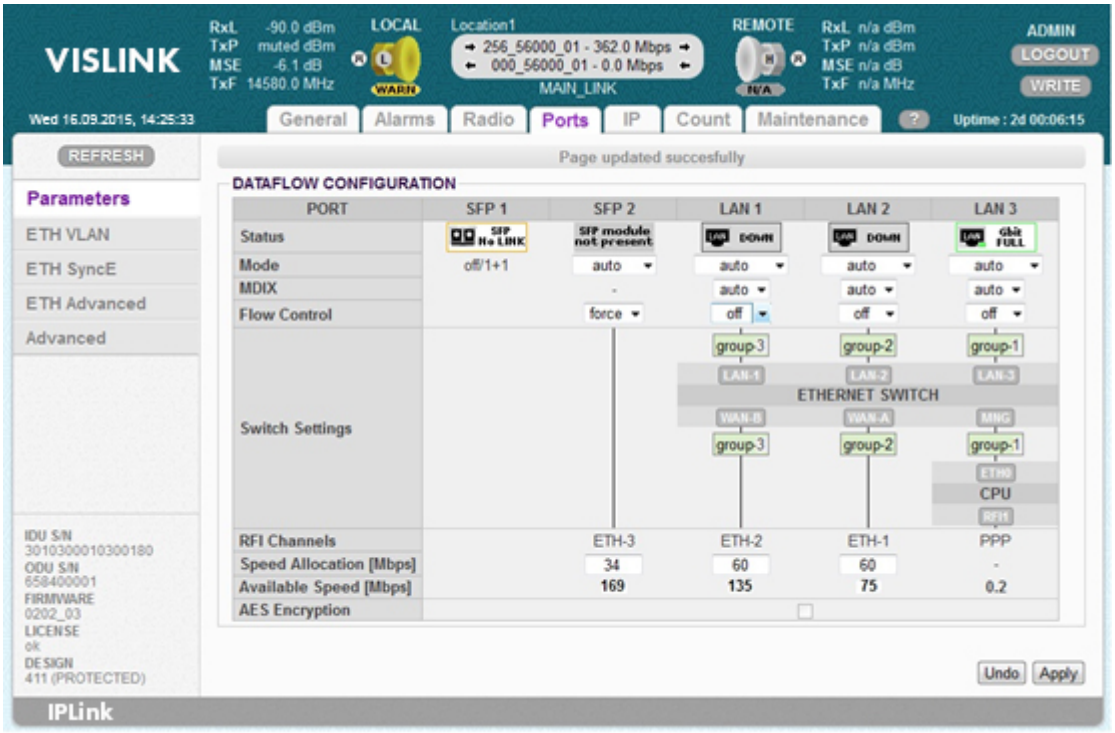

Figure 5-38 Example 7 – Basic Ports Setting at IDU1 – LOCATION 1

The same configuration needs to be applied on all IDUs using the protection scheme. The local USB port (IP address 10.10.11.10) or LAN 3 port (secondary IP address 10.10.10.10) can be used for local connection and configuration.

NOTE: Use an appropriate web browser to log on the appropriate port using the defined IP address.

When all the defined configurations are prepared on all IDUs, the required protection scheme must be selected at the master IDU (IDU 1/IDU 3). The slave IDUs will be configured automatically (you must ensure that all connections are made via the correct fiber optic cable).

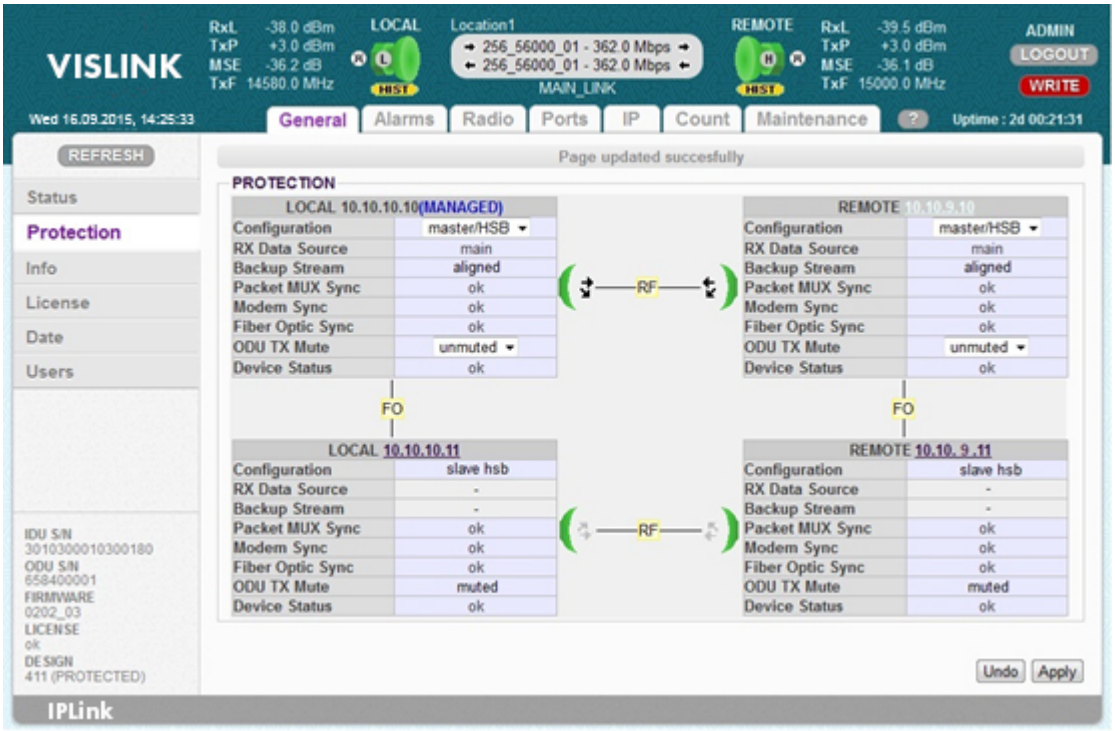

Figure 5-39 Example 7 – Protection Mode Selection at IDU1 – LOCATION 1

The Protection scheme should now be properly configured. IP management access uses NAT functionality:

- Master unit at provider side is accessible directly using IP 192.168.3.201
- Slave unit at provider side is accessible using IP 192.168.3.201:1080
- Master unit at customer side is accessible using IP 192.168.3.201:1180
- Slave unit at customer side is accessible using IP 192.168.3.201:1280

The LAN 3 port on any other IDU is alternatively used for management access, with similar NAT functionality:

- port 1080 for neighboring units over FO
- port 1180 for remote over air unit
- port 1280 for remote diagonal over air unit

The identical slave unit port configuration (port speed, port groups) and NAT configuration (NAT records, static route) at the master unit can be useful for quick reconfiguration from slave-to-master mode, but isn't required for normal protection function.

5.8. Example 8 – Basic 1+1 FD Protection Scheme

The 1+1 / FD (frequency diversity) protection mode protects against system HW failures (hitless protects against ODU_Rx, ODU_Tx, IDU_RxAFE, IDU_TxAFE) this is done in the same way that it protects against multipath fading. 1+1 / FD mode usually uses one antenna with OMT adapter with two ODUs connected into this adapter. Two transmitters are active in this protection schemes, two receivers receive the same signal which is up-converted to a different frequency. The master IDU decides which stream to use for final data de-multiplexing.

The application example for 1+1 / FD mode is shown in Figure 5-40. The configuration of the GUI pages at LOCATION 1 (provider side) is shown in Figure 5-41 to Figure 5-46.

This example describes the application using the PROTECTED configuration/design selected on both link sides. The modulation is set to QAM128 with a bandwidth of 30 MHz and the maximum data speed of about 169 Mbps. Management access is similar to Section 5.4.

All data sources are connected into the master unit (IDU 1, IDU 3) slave and master IDUs are interconnected using a fiber optic cable, connected into ports SFP 1. Management is also interconnected, using an Ethernet cable.

The protection setting rules correspond with appropriate explanation in Section 4.7.3.

Main Advantages:

- A universal protection scheme.
- Simple software reconfiguration from master to slave IDU mode.

Disadvantages:

- Two frequencies must be used.
- No protection against data interface part failure at the master IDU.

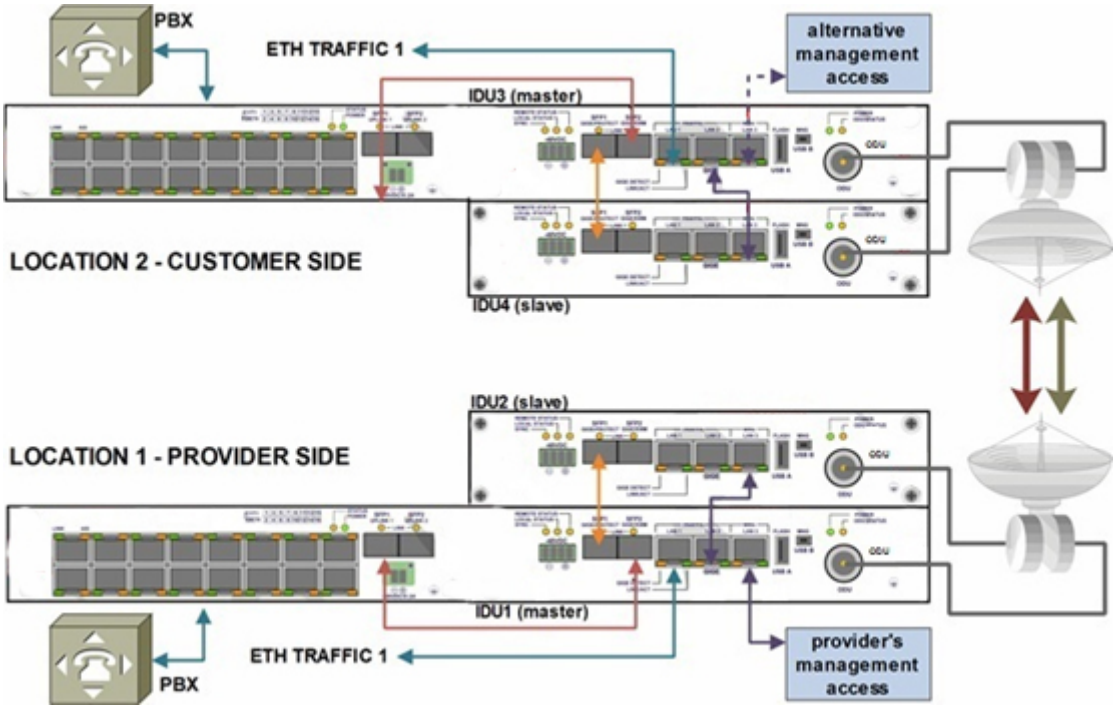

Figure 5-40 Example 8 – 1+1 FD Protection Scheme

	IDU1	IDU2	IDU3	IDU4
General | Protection				
Configuration	Master/FD	Slave/FD	Master/FD	Slave/FD
IP | Address				
Local IP	10.10.10.10/24	10.10.10.11/24	10.10.10.9/24	10.10.10.8/24
Remote IP	10.10.10.9	10.10.10.8	10.10.10.10	10.10.10.11
Protection IP	10.10.10.11	10.10.10.10	10.10.10.8	10.10.10.9
Gateway IP	10.10.10.1	10.10.10.1	10.10.10.1	10.10.10.1
Radio | Parameters				
Tx Frequency	14580 MHz	14680 MHz	15000 MHz	15100MHz
Tx Power	3 dBm	3 dBm	3 dBm	3 dBm
Ports | Parameters				
Speed Allocation [Mbps]	ETH1 = 140 ETH2 = 1 ETH3 = 34	ETH1 = 140 ETH2 = 1 ETH3 = 34	ETH1 = 140 ETH2 = 1 ETH3 = 34	ETH1 = 140 ETH2 = 1 ETH3 = 34
Ports | ETH VLAN				
Port Mode	Basic = all ports	Basic = all ports	Basic = all ports	Basic = all ports
Port Groups	1 = LAN 2/3, MNG, WANB 2 = LAN 1, WANA	1 = LAN 2/3, MNG, WANB 2 = LAN 1, WANA	1 = LAN 2/3, MNG, WANB 2 = LAN 1, WANA	1 = LAN2/3, MNG, WANB 2 = LAN 1, WANA

Table 5-8 Basic 1+1 FD protection scheme Settings

1. After changing to the PROTECTED configuration/design, the protection mode is set to **OFF** by default on both IDUs.

NOTE: In this mode just port LAN 3 (and USB B) can be used for management connections, the ODU transmitter is automatically muted. This prevents any Ethernet loops or radio interferences during the configuration process.

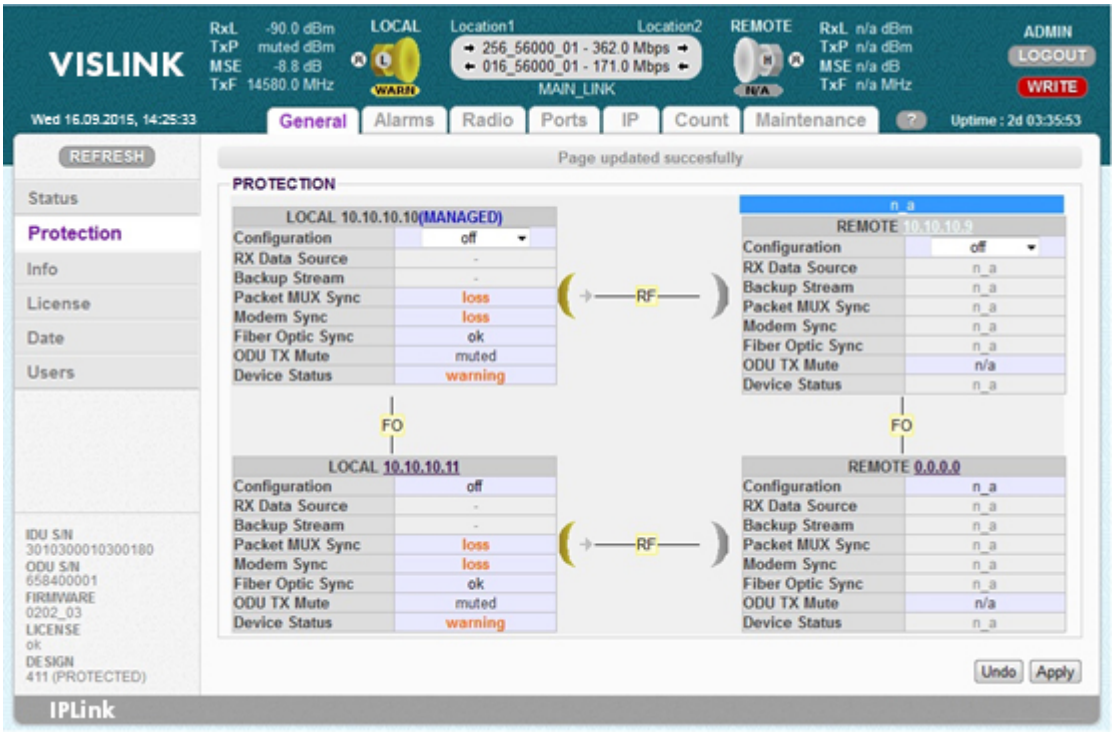

Figure 5-41 Example 8 – Default Protection off Mode at LOCATION 1

2. The proper IP address setting must be entered and applied by clicking the **APPLY** button. This change must be confirmed at the pop-up window by clicking the **Write And Apply** button.

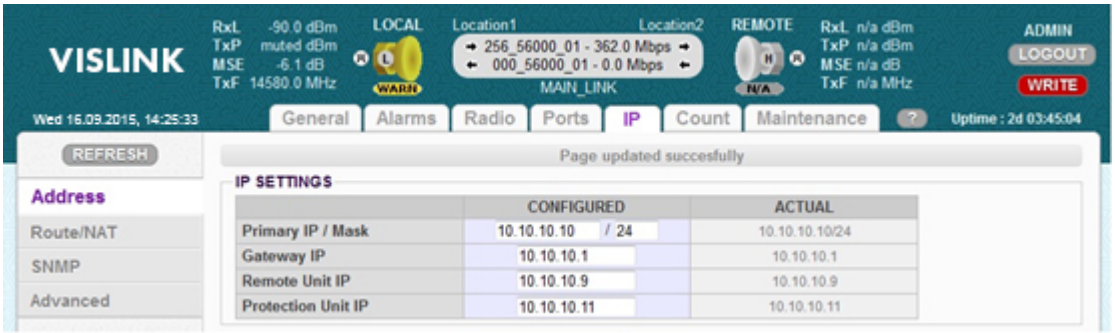

Figure 5-42 Example 8 – IP Address Setting at IDU1 – LOCATION 1

3. The basic radio parameters should now be configured.

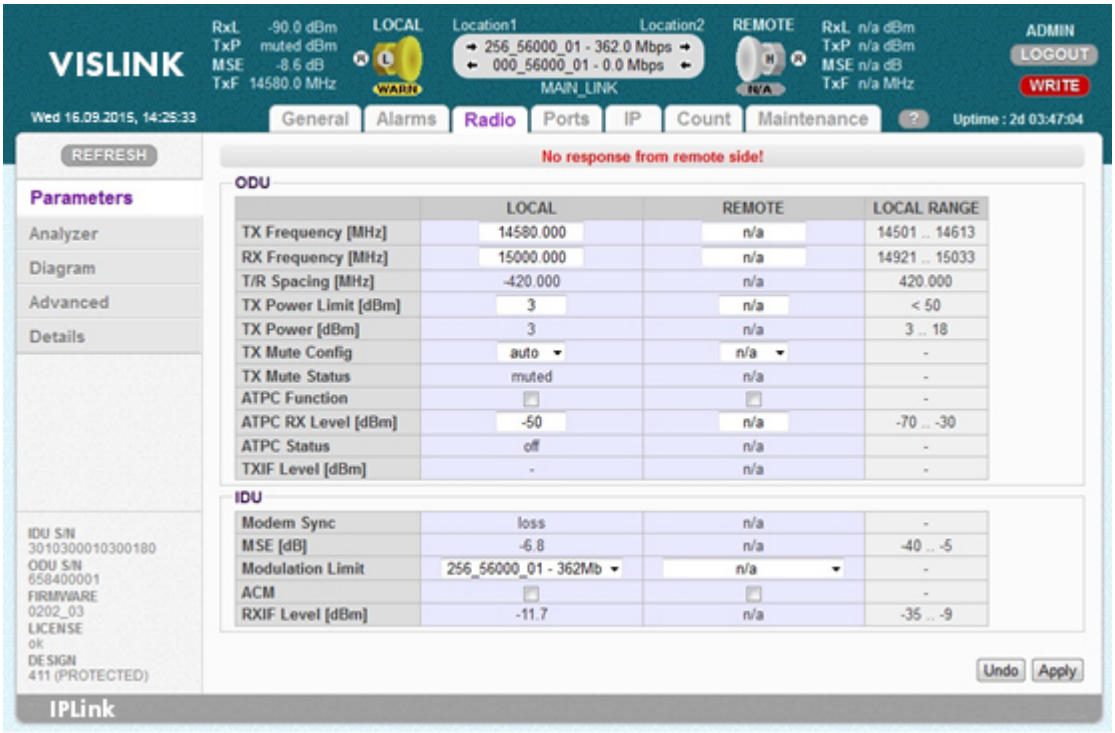

Figure 5-43 Example 8 – Basic Radio Parameters at IDU1 – LOCATION 1

4. The Port Groups and Basic Port parameters must be properly configured according to the defined connection block scheme.

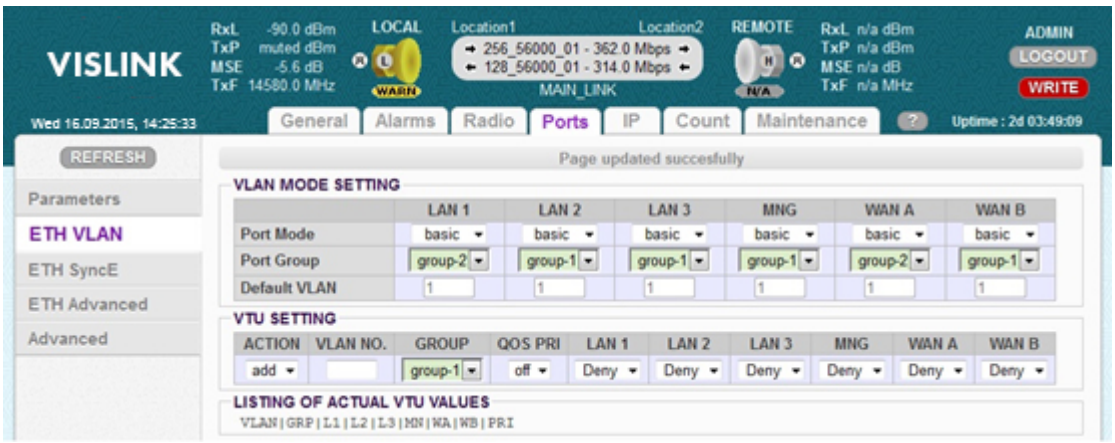

Figure 5-44 Example 8 – Port Groups Setting at IDU1 – LOCATION 1

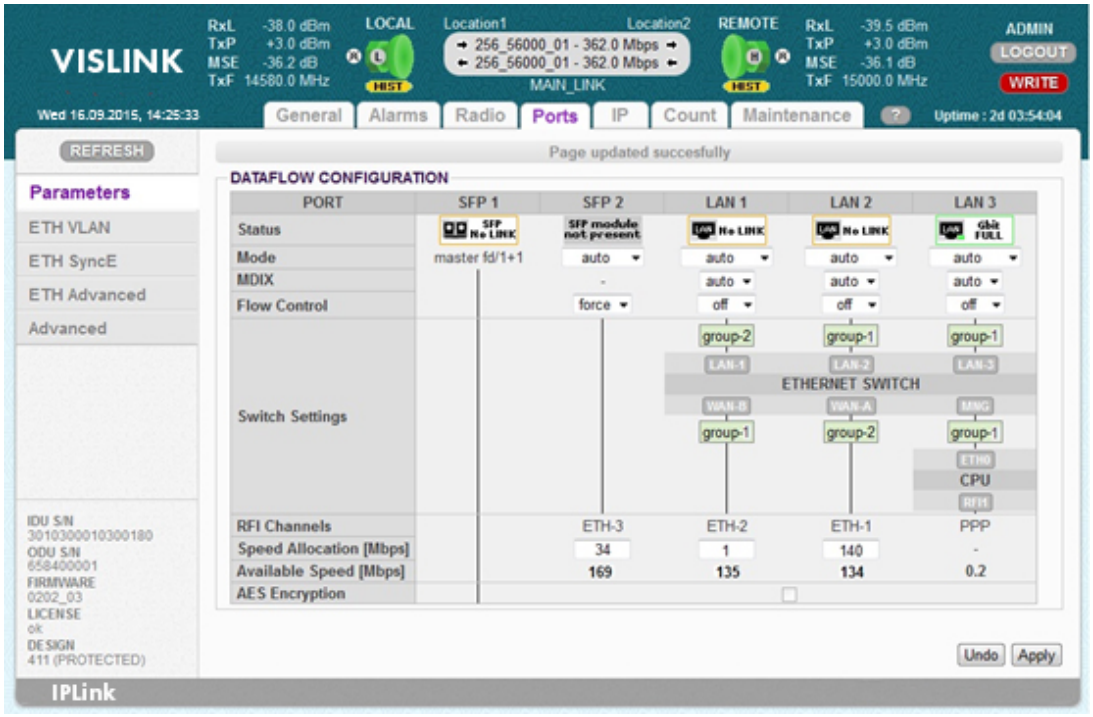

Figure 5-45 Example 8 – Basic Ports Setting at IDU1 – LOCATION 1

The same configuration should be applied on all IDUs in the protection scheme. The local USB port (IP address 10.10.11.10) or LAN 3 port (secondary IP address 10.10.10.10) can be used for local connection and configuration. The frequency at the backup link must be configured according to assigned frequency plan.

When all the previously described configurations are prepared on all IDUs, the required protection scheme must be selected at the master IDUs (IDU 1/IDU 3). The slave IDUs are configured automatically (using a fiber optic cable).

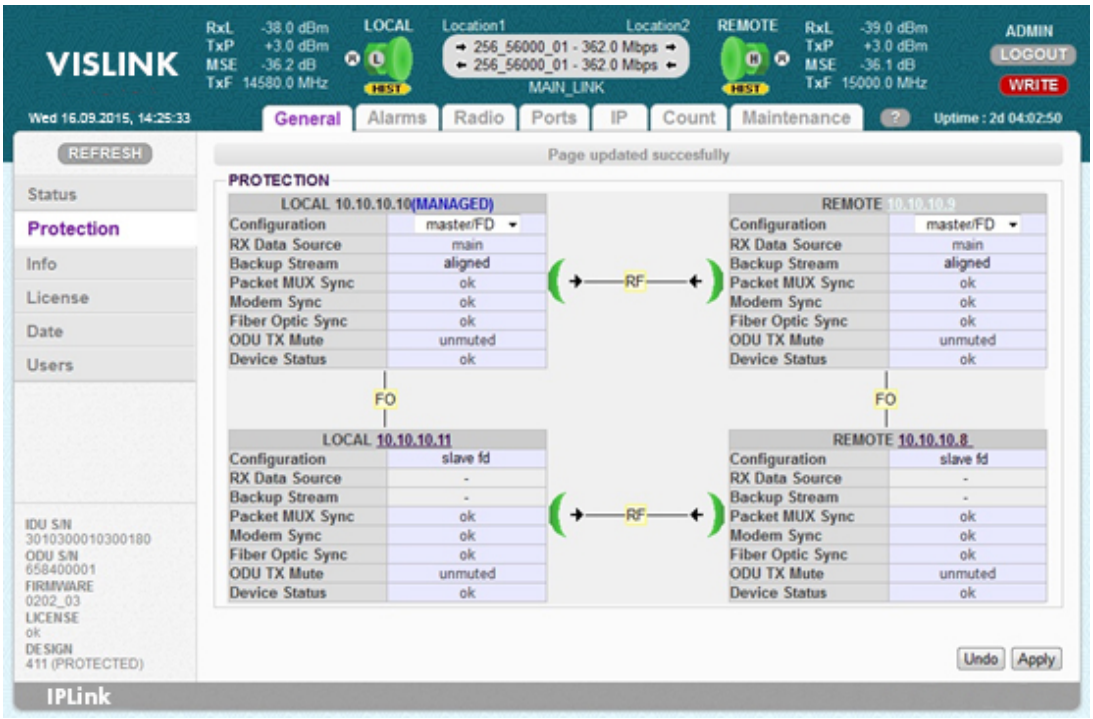

Figure 5-46 Example 8 – Protection Mode Selection at IDU1 – LOCATION 1

The Protection scheme should now be properly configured. The LAN 3 port on both master IDUs can be used for management access.

A similar slave unit port configuration (port speed, port groups) at the master unit can be helpful for quick reconfiguration from slave to master mode, but it isn't generally required for normal protection function.

5.9. Example 9 – Advanced 1+1 Protection Scheme

The advanced 1+1 protection configuration allows you to extend system protection against essential failures of the master unit (especially an interface card fault). This advanced protection configuration copies the function of basic 1+1 protection schemes, but, in parallel, doubles all data interface connections into the master and slave IDUs to provide redundancy.

The application example for 1+1 / FD mode with advanced interface connections is shown in Figure 5-47. Because the configuration of the whole system is similar to the previously described 1+1 / FD mode, only the application block diagram is discussed.

This example describes the application using the PROTECTED configuration/design on both link sides. The modulation is set to QAM128 with a bandwidth of 30 MHz and the maximum data speed is about 169 Mbps. Management access is similar to Section 5.13 with one difference that external switch at the customer side is used for management port interconnection. The Slave and master IDUs are interconnected using a fiber optic cable, connected into ports SFP 1. All data sources are connected into both master and slave units. The slave unit has all interfaces set to disabled as default (except LAN 3 port which is reserved for management purposes), this eliminates the risk of any ETH loops or IPLink-SM EXP loops. The separate management connection is also doubled using an independent Ethernet cable for the master and slave unit. It ensures access to the slave unit during a master unit fault.

The protection setting rules correspond with appropriate explanation in Section 4.7.3.

Main Advantages

- The most universal protection scheme.
- Simple software reconfiguration from master to slave IDU mode.

Disadvantages

- Two frequencies must be used.

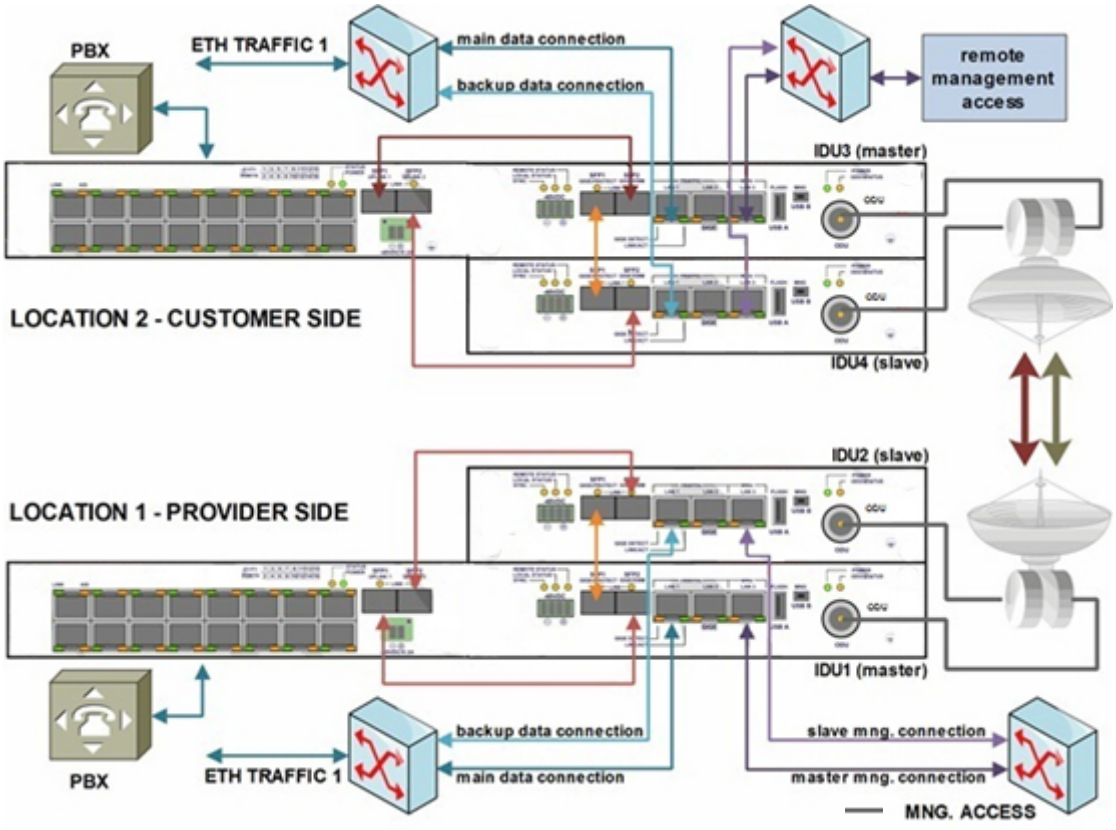

Figure 5-47 Example 9 – 1+1 FD with Advanced Interfaces Protection

	IDU1	IDU2	IDU3	IDU4
General | Protection				
Configuration	Master/FD	Slave/FD	Master/FD	Slave/FD
IP | Address				
Local IP	10.10.10.10/24	10.10.10.11/24	10.10.10.9/24	10.10.10.8/24
Remote IP	10.10.10.9	10.10.10.8	10.10.10.10	10.10.10.11
Protection IP	10.10.10.11	10.10.10.10	10.1010.8	10.10.10.9
Gateway IP	10.10.10.1	10.10.10.1	10.10.10.1	10.10.10.1
Radio | Parameters				
Tx Frequency	14580 MHz	14680 MHz	15000 MHz	15100 MHz
Tx Power	3 dBm	3 dBm	3 dBm	3 dBm
Ports | Parameters				
Speed Allocation [Mbps]	ETH1 = 140 ETH2 = 1 ETH3 = 34	ETH1 = 140 ETH2 = 1 ETH3 = 34	ETH1 = 140 ETH2 = 1 ETH3 = 34	ETH1 = 140 ETH2 = 1 ETH3 = 34
Ports | ETH VLAN				
Port Mode	Basic = all ports	Basic = all ports	Basic = all ports	Basic = all ports
Port Groups	1 = LAN3, MNG, WANB 2 = LAN1/2, WAN	1 = LAN3, MNG, WANB 2 = LAN1/2, WAN	1 = LAN3, MNG, WANB 2 = LAN1/2, WANA	1 = LAN3, MNG, WANB 2 = LAN1/2, WANA

Table 5-9 IDU - Advanced 1+1 Protection Scheme Settings

5.10. Example 10 – Ethernet Traffic Aggregation

The 2+0 aggregation mode adds a feature to increase the ETH traffic capacity by using two microwave links. The 2+0 aggregation configuration functions in a similar way to the two parallel links used with the MULTI configuration/design where the capacity of the traffic channel ETH 1 at the master unit is aggregated with the capacity of the traffic with channel ETH 4 at the slave unit. The proprietary aggregation algorithm divides the traffic two-ways, based on the available free space on the transmit FIFOs. The traffic division doesn't depend on the MAC address of the aggregated frames.

Figure 5-48 shows an application example for 2+0 aggregation mode. The configuration of the web GUI pages at LOCATION 1 (provider side) are shown in Figure 5-49 to Figure 5-54.

This example describes the application where the AGGREGATE configuration/design is selected on both link sides. The modulation is set to QAM128 with a bandwidth of 30 MHz, the maximum data speed is about 169 Mbps. Management access is similar to that shown in Section 5.13. Slave and master IDUs are interconnected using a fiber optic cable, connected into ports SFP 1. Aggregated data traffic is connected via port LAN 1 at the master unit. The first portion of aggregation is directed over channel ETH 1 at the master unit with a

capacity of about 170 Mbps. The second portion is directed over fiber optic (together with the low speed management channel) into the slave unit and then through channel ETH 4 with a configured capacity of 170 Mbps. The total bandwidth capacity is the sum of both capacities added together, in this example 340 Mbps. Other traffic channels on the master and also on the slave unit can be used in parallel for the next independent data transmission.

The aggregation setting rules correspond with the explanation given in Section 4.7.4.

Main Advantages:

- Simple to increase capacity.
- Aggregation algorithm not MAC address dependent.
- The next independent traffic channels are still available.
- Automatic protection (not hitless) for aggregated traffic.

Disadvantages:

- Two frequencies must be used or RF signal separation with high quality OMT.

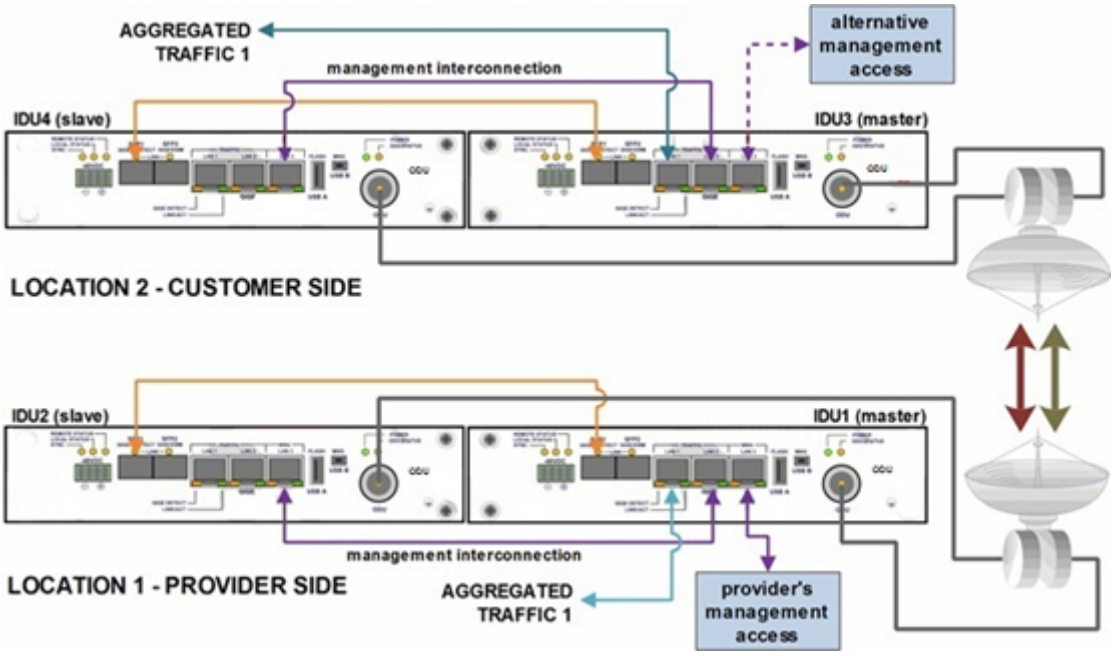

Figure 5-48 Example 10 – 2+0 Aggregation With out-of-Band Management

	IDU1	IDU2	IDU3	IDU4
General | Aggregation				
Configuration	Master	Slave	Master	Slave
IP | Address				
Local IP	10.10.10.10/24	10.10.10.11/24	10.10.10.9/24	10.10.10.8/24
Remote IP	10.10.10.9	10.10.10.8	10.10.10.10	10.10.10.11
Protection IP	10.10.10.11	10.10.10.10	10.10.10.8	10.10.10.9
Gateway IP	10.10.10.1	10.10.10.1	10.10.10.1	10.10.10.1
Radio | Parameters				
Tx Frequency	14580 MHz	14680 MHz	15000 MHz	15100 MHz
Tx Power	3 dBm	3 dBm	3 dBm	3 dBm
Ports | Parameters				
Speed Allocation [Mbps]	ETH1 = 170 ETH2 = 1 ETH3 = 0	ETH1 = 0 ETH2 = 0 ETH3 = 0 ETH4 = 170	ETH1 = 170 ETH2 = 1 ETH3 = 0	ETH1 = 0 ETH2 = 0 ETH3 = 0 ETH4 = 170
Ports | ETH VLAN				
Port Mode	Basic = all ports	Basic = all ports	Basic = all ports	Basic = all ports
Port Groups	1 = LAN2/3, MNG, WANB 2 = LAN1, WANA	1 = LAN 3, MNG 2 = LAN 1, WANA 3 = LAN 2, WANB	1 = LAN2/3, MNG, WANB 2 = LAN1, WANA	1 = LAN3, MNG 2 = LAN1, WANA 3 = LAN2, WANB

Table 5-10 Ethernet traffic Aggregation Settings

1. To configure the basic radio parameters, an accurate IP address setting must be entered and applied by clicking the **APPLY** button.

NOTE: Any changes must be confirmed in the pop-up window by clicking the **Write and Apply** button.

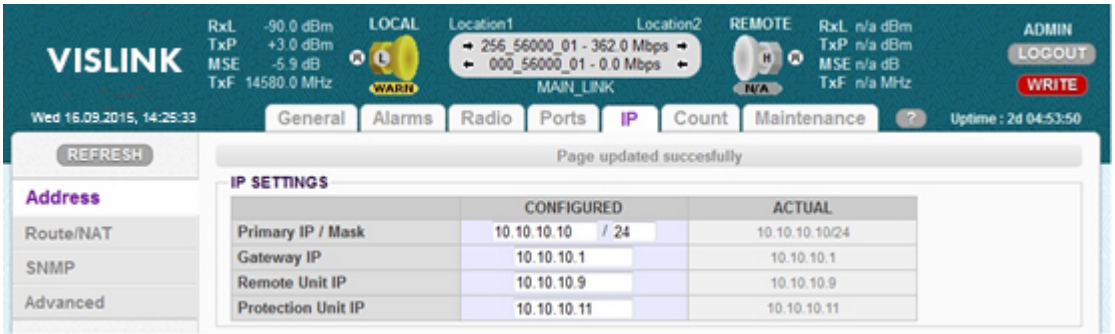

Figure 5-49 Example 10 – IP Address Setting at IDU1 – LOCATION 1

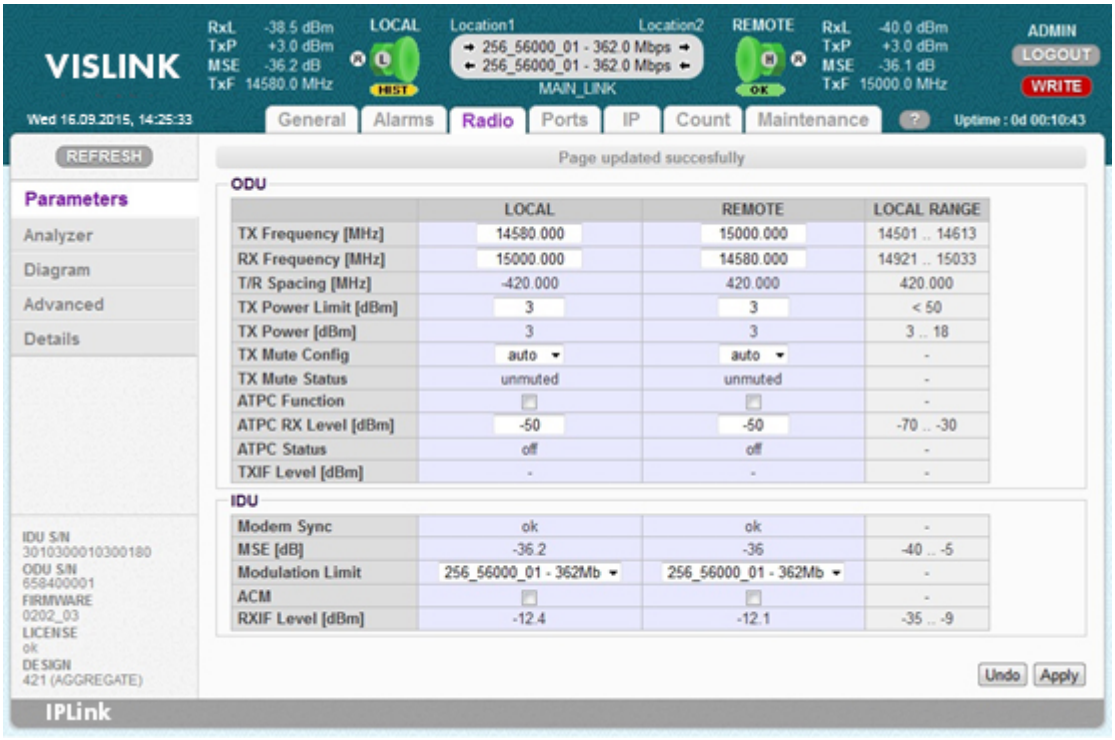

Figure 5-50 Example 10 – Basic Radio Parameters at IDU1 – LOCATION 1

2. The Port Groups must be properly configured according to the defined connection block scheme on each connected IDU.

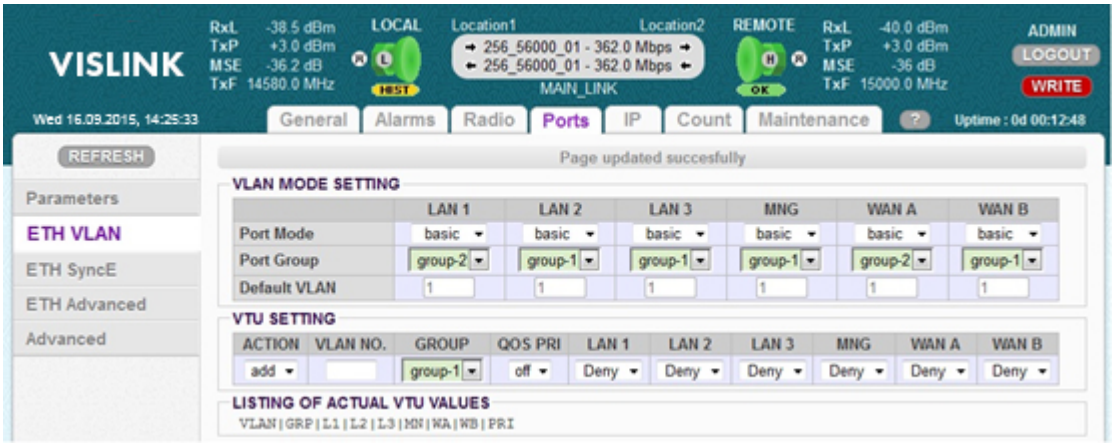

Figure 5-51 Example 10 – Port Groups Setting at IDU1 – LOCATION 1

3. Select the required aggregation scheme on the master IDUs (IDU 1/IDU 3). The slave IDUs are configured automatically

NOTE: The correct interconnection for this configuration is via an appropriate fiber optic cable.

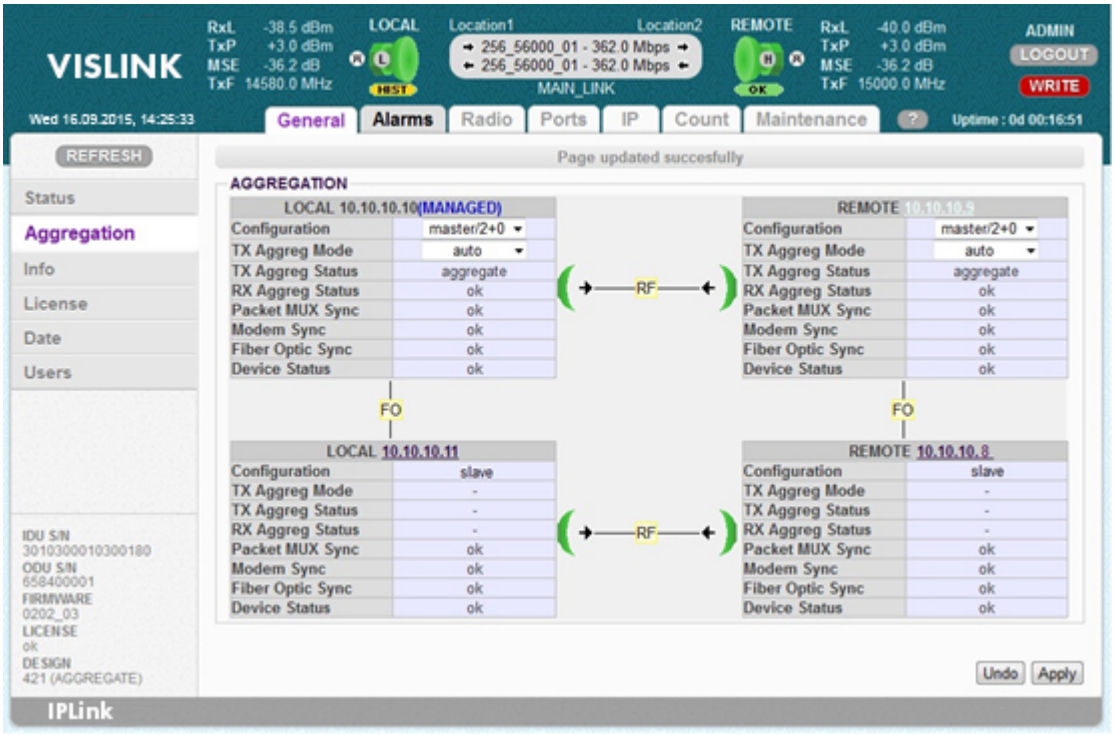

Figure 5-52 Example 10 – Aggregation Mode Selection at IDU1 – LOCATION 1

4. Finally, correctly configure the ETH channels on all master and slave units.

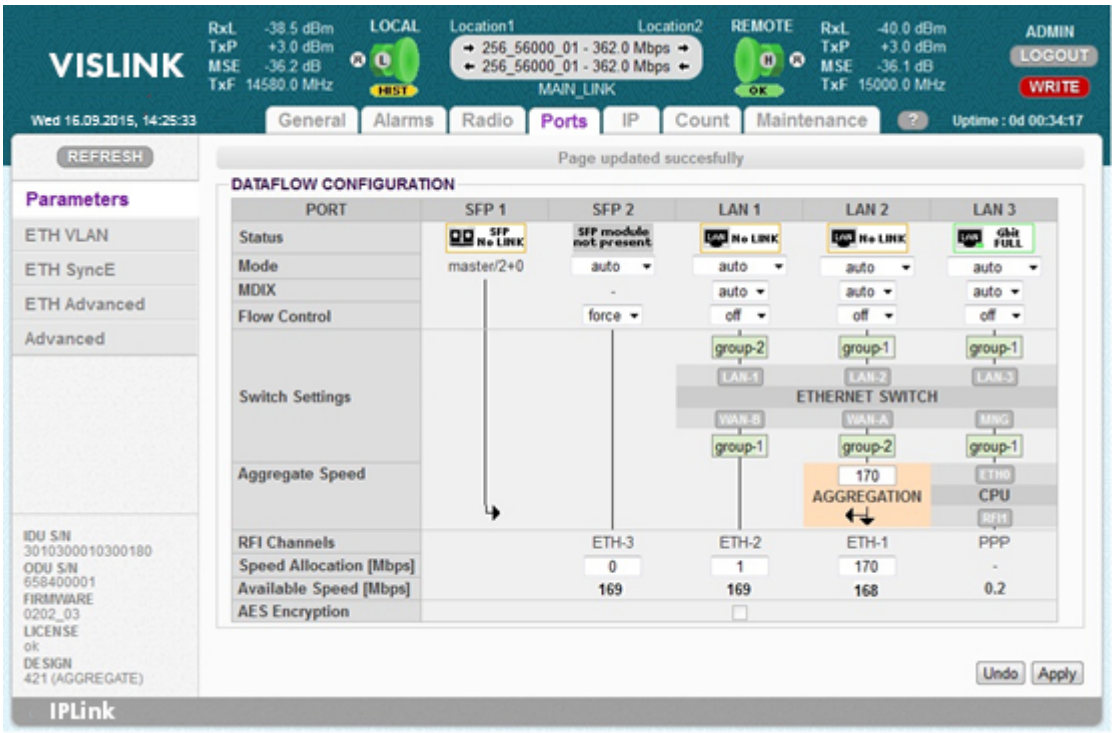

Figure 5-53 Example 10 – Port Setting at Master IDU1 – LOCATION 1

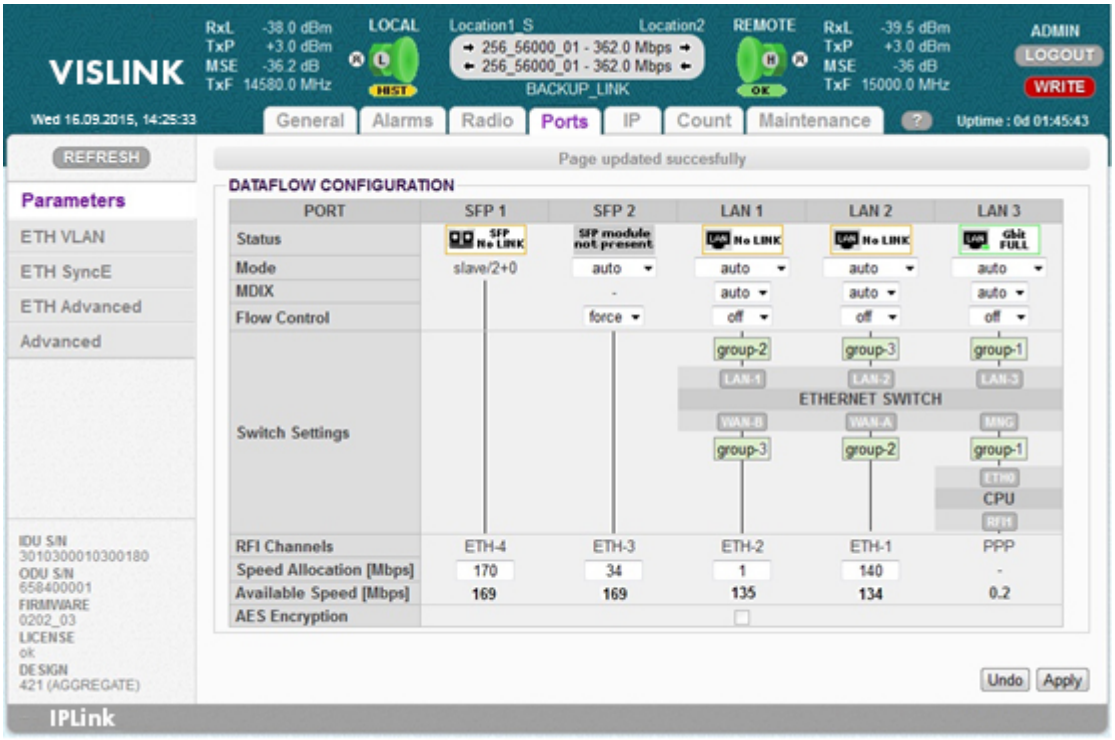

Figure 5-54 Example 10 – Port Setting at Slave IDU2 - LOCATION 1

The Aggregation scheme is properly configured now.

Appendix A Technical Parameters

A.1. General

Item	Parameter	Value
Frequency	Operating frequency range	6 to 42 GHz
	Frequency plans	According to CEPT/ITU-R recommendations
	T/R spacing	According to CEPT/ITU-R recommendations
Modulation	Modulation schemes	QPSK, 8PSK, 16QAM, 32QAM, 64QAM, 128QAM, 256QAM
	ACM	Hitless adaptive modulation
	ETSI Bandwidths	7/14/27.5/28/56 MHz
	ANSI Bandwidths	10/20/30/40/50/60 MHz
Data transmission	Capacity allocation	Packet transport (priority based packet system)
	Path configuration	1+0, 2+0, 1+1 (FD/SD/HSB)
	Forward error correction	LDPC
	Compression function	Online Ethernet header compression
	Data encryption	AES-128, AES-256
	Max. Real Data Throughput	up to 365 Mbps in 1+0 mode up to 730 Mbps in 2+0 mode

Table 5-11 System Parameters

A.2. IDU Specification

Item	Parameter	Value
1000Base-T	Number of Ports	3x (RJ-45) 2x SFP (1000BaseSX/LX)
	Basic function	user traffic interface/management
	VLAN	up to 4096 VLANs
	QoS	Source Port, 802.1p, IPv4 TOS/DSCP, IPv6 TC, VLAN VID,
	MAC table	up to 8192 addresses
	Maximum Frame Size	10K
EMM-16E1/T1	Number of Ports	16 (16xRJ-45)
	Interface	G.703-E1 120/75 ohm for E1 mode T1.102-T1/100 ohm for T1 mode
	Coding	HDB3 for E1mode, B8ZS for T1 mode
	Speed	2.048 Mbps for E1 mode, 1.554Mbps for T1 mode
	IDU interface	2x SFP 1000Base-SX (proprietary GIGE protocol)
EMM-ASI	Number of Ports	4xTx / 3xTx&1Rx / 2xTx&2xRx / 1xTx&3xRx / 4xRx
	Interface	4x BNC (DVB-ASI)

Item	Parameter	Value
	Coding	8B/10B, MPEG-2 TS
	Speed for ASI channel	8-216 Mbps
	IDU interface	2x SFP 1000Base-SX (proprietary GIGE protocol)

Table 5-12 IDU Traffic Interfaces

Item	Parameter	Value
ETH Compression efficiency (L1)	64Byte Frames	Max. 25% from available ETH speed
	512Byte Frames	Max. 3% from available ETH speed
	1518Byte Frames	Max. 1% from available ETH speed
ETH Throughput (L1) 256QAM_56MHz	64Byte Frames	461 Mbps
	512Byte Frames	375 Mbps
	1518Byte Frames	367 Mbps
ETH CT Latency (L1) 256QAM_56MHz	64Byte Frames	130 usec
	512Byte Frames	137 usec
	1518Byte Frames	145 usec

Table 5-13 Ethernet Traffic Parameters

A.3. Network Management System

Item	Parameter	Value
Ports	Main NMS ports	ETH port LAN-3
	Additional NMS ports	1000Base-T (LAN-1/2/3/SFP 2, USB-B (alternative IP port)
NMS form	Protocols	HTTP, HTTPS, SNMP v1/v2c./v.3, TELNET, SSH
	In-Band management	via VLAN
	Out-of-Band management	128 kbps
IP addresses	Addresses type	primary / secondary IP (IPv4/IPv6)
	Additional function	NAT, Ping, Telnet, rdate, ntp
GUI	Type	WEB based
SNMP	Version	SNMP v1, SNMP v2c, SNMP v3
	Read access	Complete MIB
	Write access	Subset of link parameter
Security	Licenses	Time limited / permanent
	Access levels	guest/user/admin with password security

Table 5-14 Management Parameters

A.4. Miscellaneous

Item	Parameter	Value
IDU Mechanical	Dimension [w x h x d]	210 mm x 44 mm x 250 mm
	Weight	2 kg
	Protection	IP31 (EN 60529)
ODU Mechanical	Dimension	Ø 295.2 mm; H: 92.5 mm
	Weight	3.9 kg
	Protection	IPx6 (EN 60529)
Input Voltage Level	IDU	-20 VDC up to -60 VDC
	ODU	-30 VDC up to -60 VDC
Power Consumption	IDU only	< 22 W (full port connection)
	ODU only	< 38 Watts
	IDU+ODU	< 60 Watts
	Maximum ODU current	up to 1.9 A DC
Environmental Operational Conditions	IDU Temperature	-5° to +45°C
	IDU Humidity	0 to 95%, Non condensing
	ODU Temperature	-33° to +55°C
	ODU Cold Start	Operational at -45°C, not guaranteed all specification
	ODU Humidity	0 to 100%

Table 5-15 Miscellaneous

A.5. Accessories

Power supply	85 VAC - 240 VAC
Input power	48 VDC ± 5%
Input frequency	47 Hz – 63 Hz
Operation temperature	0°C – 40°C
Protection	Surge and power guard, short-circuit protection
EMI	EN55022, EN55024
Dimensions H x W x D (cm)	3,7 x 6,5 x 16,7

Table 5-16 External Power Supply Parameters

This page is intentionally unused.

Appendix B Abbreviation list

- **AGC** - automatic gain control on RF cable
- **AIS** - continual sequence of ones on E1 data according to norm
- **ANEG** – auto-negotiation - automatic speed and duplex set-up on LAN ports
- **ATPC** - automatic control of output power at ODU on the basis of Rx level at remote unit
- **ATU** - table of MAC addresses
- **BER** - bit error rate (from last clearing)
- **EFS** - error free seconds
- **ERS** - error seconds
- **FER** - Frame Error Rate (per minute)
- **HWADDR** - MAC address of eth interface
- **IDU** – IPLink-SM Indoor Unit
- **MDIX** - configuration for wires crossover on LAN ports
- **MSE** - dispersion of dots from ideal location in I/Q diagram after demodulation. The sharpest the dots of status diagram are – the better (value should be in interval -40 to -32dB). MSE thresholds for each modulation with BW 28MHz are:
  - 128QAM = -24 dB
  - 64QAM = -21 dB
  - 32QAM = -18 dB
  - 16QAM = -15 dB
  - 8PSK = -13 dB
  - QPSK = - 9 dB
- **MUX** - data multiplexer (aggregating of several parallel streams into one serial stream and back)
- **NAT** - network address translation – translation of IP addresses (and ports)
- **ODU** - Outdoor Unit
- **PBPS** - packet multiplexer
- **RFI** - RF interface – interface towards PBPS
- **RSL** - received signal level in dBm
- **RSSI** - received Signal Strength Indication – received signal strength in mV, measured on BNC outdoor unit connector
- **SNMP** - Simple Network Management Protocol – protocol for remote system management
- **TBE** - time between errors
- **TLE** - time since last error occurrence
- **VLAN ID** - VLAN number
- **VLAN** - virtual LAN – the possibility to create more logical networks on one physical medium
- **VTU** - table of rules for VLANs
- **W0-3** - names of memories in device (W0 is boot memory)

This page is intentionally unused.

Appendix C ODU Technical Specification

C.1. ODU Technical Specifications

IPLink-SM ODU RSL at 10^{-6} (dBm) and Total Payload Capacity (Mbps)														
BW***, MHz	Modulation	FEC****	6 GHz	7 GHz	8 GHz	10 GHz	11 GHz	13 GHz	15 GHz	18 GHz	23 GHz	26 GHz	38* GHz	Bit rate, Mbps
3.5	QPSK	Strong	-97	-95	-95	-97	-96	-95	-93,5	-95	-97	-96,5	-93,5	3
	16APSK	Strong	-90,5	-88	-88	-90	-89	-88	-88	-88,5	-90	-89,5	-86,5	7
	32APSK	Strong	-87	-85	-85,5	-87	-86	-85	-85	-85,5	-87	-86,5	-83,5	9
	64QAM	Strong	-84	-81,5	-82	-84	-83	-82	-82	-82	-83,5	-83	-80	13
		Weak	-81,5	-79	-79,5	-81	-80	-79,5	-79	-79,5	-81	-81	-78	14
7	QPSK	Strong	-93	-92	-92	-94	-93	-92,5	-91	-92	-94	-93,5	-90,5	8
	16APSK	Strong	-86,5	-85	-85,5	-87,5	-86,5	-85,5	-85	-85,5	-87,5	-87	-84	17
	32APSK	Strong	-83,5	-82,5	-83	-84,5	-83,5	-83	-82,5	-83	-84,5	-84	-81	21
	64QAM	Strong	-80	-79	-80	-81,5	-80,5	-79,5	-79,5	-79,5	-81,5	-80,5	-77,5	28
	128QAM	Strong	-77	-76	-76,5	-78	-77	-76	-76,5	-76	-78	-77,5	-74,5	34
		Weak	-75	-73,5	-75	-76	-75	-74,5	-74	-74	-75,5	-75,5	-72,5	36
14	QPSK	Strong	-90	-90,5	-90	-91	-90	-90	-89	-90,5	-91	-90,5	-87,5	17
	16APSK	Strong	-83,5	-83,5	-83,5	-84,5	-83,5	-83,5	-83	-84	-84	-83,5	-80,5	34
	32APSK	Strong	-80	-80	-80,5	-81,5	-80,5	-80	-80	-80,5	-80,5	-80,5	-77,5	45
	64QAM	Strong	-77,5	-77,5	-78	-79	-78	-77,5	-77,5	-78	-78,5	-78	-75	57
	128QAM	Strong	-74,5	-74,5	-75	-75,5	-74,5	-74,5	-74	-75	-75	-75	-72	68
	256QAM	Strong	-71	-71	-71,5	-72	-71	-70,5	-70,5	-72	-71,5	-71,5	-68,5	79
		Weak	-67,5	-67,5	-68	-69	-68	-67,5	-67	-68	-65,5	-68	-65	86
28	QPSK	Strong	-90.5	-89.5	-89	-88.5	-89.5	-89.5	-89	-90	-89	-91.5	-85	35
	16APSK	Strong	-84.5	-83	-83	-82.5	-83.5	-83.5	-83	-84	-83	-85	-79	69

	32APSK	Strong	-81.5	-80	-80	-80	-80.5	-80.5	-80.5	-80.5	-80	-82	-76	88
	64QAM	Strong	-79	-77.5	-77.5	-77	-78	-77.5	-77	-78	-77.5	-79.5	-73.5	115
	128QAM	Strong	-75.5	-74.5	-74	-73.5	-74.5	-74.5	-74	-75.5	-74	-76.5	-70	138
	256QAM	Strong	-72.5	-71	-70.5	-70.5	-71	-71	-70.5	-72	-71	-73	-67	161
		Weak	-69	-67	-66	-66	-67	-67	-66.5	-69	-67.5	-70	-63.5	174
IPLink-SM ODU RSL at 10^{-6} (dBm) and Total Payload Capacity (Mbps)														
BW***, MHz	Modulation	FEC****	6 GHz	7 GHz	8 GHz	10 GHz	11 GHz	13 GHz	15 GHz	18 GHz	23 GHz	26 GHz	38* GHz	Bit rate, Mbps
40	QPSK	Strong	-89	-87.5	-88	-87.5	-88	-88	-88	-88	-87.5	-89.5	-83.5	49
	16APSK	Strong	-82.5	-81.5	-81.5	-81	-82	-82	-81.5	-82.5	-81	-83.5	-77	98
	32APSK	Strong	-80	-78.5	-79	-78.5	-79.5	-79.5	-79	-79.5	-78.5	-80.5	-74.5	127
	64QAM	Strong	-77	-76	-75.5	-75.5	-76.5	-76	-76	-77	-75.5	-78	-71.5	163
	128QAM	Strong	-74	-73	-72.5	-72.5	-73.5	-73	-72.5	-73.5	-72.5	-74.5	-68.5	196
	256QAM	Strong	-70.5	-69.5	-69	-68.5	-69.5	-69.5	-69	-70.5	-69	-71	-65	229
		Weak	-68	-67	-64.5	-64.5	-65.5	-65	-65	-67.5	-66.5	-68.5	-62.5	245
56	QPSK	Strong	-87	-85.5	-86	-85.5	-87	-86.5	-86	-87	-85.5	-88	-81.5	72/67**
	16APSK	Strong	-81	-80	-79.5	-79.5	-80.5	-80	-79.5	-80.5	-79.5	-82	-75.5	145/135**
	32APSK	Strong	-78	-77	-77.5	-77	-78	-77.5	-77	-77.5	-76.5	-79	-72.5	182
	64QAM	Strong	-75.5	-74.5	-74	-73.5	-74.5	-74.5	-74	-75.5	-74	-76	-70	240
	128QAM	Strong	-72	-71	-71	-70.5	-71.5	-71.5	-71	-72	-70.5	-73	-66.5	287
	256QAM	Strong	-68.5	-67.5	-67	-66.5	-68	-67.5	-67	-68.5	-67	-69.5	-63	335
		Weak	-64	-63	-63	-62.5	-63.5	-63	-62.5	-64.5	-62.5	-65	-58.5	363

Table 5-17 ODU Technical Specifications

Modulation	Standard/High Tx Power, dBm			
	6, 7, 8 GHz	10, 11, 13, 15 GHz	18, 23, 26* GHz	38* GHz
4QAM	+19/+27	+19/+25	19	17
16QAM	+18/+26	+18/+24	18	16
32QAM	+17/+25	+17/+23	17	15
64QAM	+15/+23	+15/+21	15	13
128QAM	+15/+23	+15/+21	15	13
256QAM	+12/+20	+12/+18	12	10

Table 5-18 IPLink-SM ODU Tx Power Table

6 GHz	7, 8 GHz	10, 11 GHz	13, 15 GHz	18, 23 GHz	26 GHz	38 GHz
N-type	UBR84	UBR100	UBR140	UBR220	UBR260	UBR320

Table 5-19 IPLink-SM ODU waveguide flange sizes

Max. Power consumption
SP: 13-27W
HP: 21-39W

Table 5-20 Max Power Consumption

This page is intentionally unused.