



CFIP Phoenix Series

TDM/IP Split Mount System

Technical Description & Configuration Guide

Product code: S0DRFMD1

Table of Contents

1	Overview	5
1.1	CFIP Phoenix TDM/IP split mount system	5
1.2	CFIP Phoenix feature Summary	6
1.2.1	Main Features	6
1.2.2	IDU mechanical features	6
1.2.3	ODU mechanical features	6
1.2.4	IRFU mechanical features	7
1.2.5	Interfaces/Management	7
1.3	CFIP Phoenix ODU Parameters	8
1.4	Application Examples	8
1.4.1	CFIP Phoenix 1+0 configuration	8
1.4.2	CFIP Phoenix 1+1 Frequency Diversity (FD)	8
1.4.3	CFIP Phoenix 1+1 Hot Stand-by (HSB)	9
1.4.4	CFIP Phoenix 1+1 Space Diversity (SD)	9
1.4.5	CFIP Phoenix Ring Topology	10
1.5	Technical specification	11
1.6	Cable Requirements	16
1.7	Labelling	17
2	Configuration and Management	19
2.1	Connecting CFIP Phoenix IDU to power source	19
2.1.1	Power protection port	20
2.1.2	Connecting CFIP Phoenix IRFU to power source	20
2.2	Resetting the CFIP Phoenix	20
2.3	Web Interface	21
2.3.1	10/100/1000Base-T Ports	21
2.3.2	Ethernet Management Connection Configuration	21
2.3.3	Connecting to Web Interface	21
2.3.4	Interface Description	23
2.3.5	Command Execution	24
2.3.6	Initial Configuration with Web GUI	25
2.4	Command Prompt Interface	28
2.4.1	RS-232 Serial Management Port	29
2.4.2	Telnet connection	31
2.4.3	Initial Configuration with Command Prompt	32
2.5	LED indications	32
2.5.1	CFIP Phoenix IDU alarm LED indications	32
2.5.2	Ethernet RJ-45 connector LED indications	33
2.5.3	E1 RJ-45 connector LED indications	33
3	Status Window	34
3.1.1	Radial MSE	36
3.1.2	LDPC	36
3.2	Alarm status	37
3.3	Ethernet aggregation status	37
3.4	Diagnostics data	38
4	Detailed Configuration in Web Graphic User Interface	40
4.1	ODU Configuration	40
4.1.1	Radio Configuration	40
4.1.2	ATPC Configuration	41
	ATPC Algorithm	42
4.2	IDU Configuration	43
4.2.1	Modem Configuration	43
4.2.2	Loopback Configuration	45
4.3	Protection configuration	47
4.3.1	Frequency Diversity (FD) protection mode	47
4.3.2	Hot Standby (HSB) and Space Diversity (SD) protection modes	49
4.3.3	Protection Status	52
4.3.4	Protection Configuration	53

4.3.5	Advanced Protection Configuration	53
4.4	<i>System Configuration</i>	54
4.4.1	User Configuration	55
4.4.2	Name configuration	56
4.4.3	Other configuration.....	56
4.4.4	NTP configuration	56
4.4.5	Upgrade Software	57
4.4.6	Service information	57
4.5	<i>IP Configuration Window</i>	58
4.5.1	Ethernet management port IP configuration	59
4.5.2	IP Services	59
4.5.3	Static Route Configuration	59
4.6	<i>Ethernet Configuration</i>	62
4.6.1	Link state propagation configuration	63
4.6.2	Protocol transparency	64
4.6.3	Ethernet ingress/egress rate configuration.....	64
4.7	<i>Aggregation configuration</i>	65
4.8	<i>VLAN Configuration</i>	67
4.8.1	Ethernet Switch Port Status and Settings.....	69
4.8.2	Ethernet Switch VLAN Status and Settings.....	69
4.9	<i>QoS</i>	72
4.9.1	General Configuration	72
4.9.2	QoS 802.1p Configuration	74
4.9.3	DSCP Configuration	74
4.10	<i>Spanning Tree Configuration</i>	76
4.10.1	Spanning Tree Configuration.....	76
4.10.2	Region, mapping configuration for MSTP	77
4.10.3	Spanning Tree Protocol statistics	78
4.11	<i>SNMP v1/v2 configuration</i>	79
4.11.1	SNMP community configuration	79
4.11.2	SNMP Allowed Hosts Configuration	79
5	Performance and Alarm Management	81
5.1	<i>Alarm Management</i>	81
5.1.1	Alarms and Events Structure	81
5.1.2	Alarms-Events and Groups Tables.....	81
5.1.3	Alarm Status Window	83
5.1.4	Alarm Log	84
5.1.5	Alarm and Alarm Threshold Configuration.....	84
5.1.6	Alarm Management Commands	86
5.2	<i>Performance Management</i>	87
5.2.1	Performance Management Data Collection.....	87
5.2.2	Performance Values	88
	Threshold Seconds (TS)	88
	Tide Mark (TM)	88
5.2.3	Performance Management in Web GUI.....	88
5.2.4	Adaptive Equalizer	91
5.2.5	Performance Management Commands	92
5.3	<i>Ethernet modem statistics</i>	93
5.4	<i>Ethernet switch statistics</i>	95
6	Miscellaneous Controls in Web Graphic User Interface	99
6.1	<i>Ethernet/Configuration files</i>	99
6.2	<i>License Management</i>	102
6.3	<i>Command Line</i>	104
6.4	<i>File System</i>	104
6.5	<i>Security commands</i>	106
7	Software Update	107
7.1	<i>Uploading File via Ethernet Management Port (FTP)</i>	107
7.2	<i>Uploading File via Serial Port (Xmodem)</i>	108

8	CFIP Discovery Protocol	110
8.1	CFIP Unit Discovery Procedure	110
8.2	Discovery Protocol Performance Examples	110
8.2.1	Discovery of IP Address and Firmware Version in Case The Subnet of CFIP Unit is Unknown	110
8.2.2	Discovery of IP Address and Firmware Version in Case The Subnet of CFIP Unit is Known	111
8.2.3	Discovery of IP Address and Firmware Version of Remote CFIP Unit Connected to Router In Case one IP address of Remote Units is Known.....	112
9	RSSI Port.....	113
10	Pinouts	114
10.1	Ethernet RJ-45 port	114
10.2	E1 port.....	114
10.3	Alarm port (26-pin D-SUB).....	114
10.4	RS232 (DB9 female connector).....	115
10.5	1+1 protection port (RJ-45)	115
10.6	1+1 protection cable.....	116
10.7	Power protection port	117
11	Available Accessories.....	118
11.1	Other Available Accessories	119
12	List of Abbreviations	121
13	SAF Tehnika JSC Contacts	123

Proprietary notice

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

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

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

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

Note: FODU/ODU does not contain serviceable parts. Warranty will not be applicable in the event FODU/ODU has been hermetically unsealed.

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

Copyright Notice

Copyright © 2015 SAF Tehnika, JSC. All rights reserved.

1 Overview

This document briefly describes the **CFIP Phoenix series TDM/IP split mount system (IDU+ODU)** covering the built-in management system, configuration functionality, hardware features, etc.

1.1 CFIP Phoenix TDM/IP split mount system

CFIP product family is the new next generation product line which is targeting growing demands for data transmission over microwave radio.

As a result the primary traffic interface for CFIP split mount system is Gigabit Ethernet. As CFIP is capable of providing bit rate of **up to 363Mbps**, it is a great addition to SAF portfolio. CFIP radio and modem performance allows achieving high system capacity by employing 256-decision states modulation scheme by user's choice. Apart from the **full system capacity of 363Mbps**, it is possible to configure the radio to any of 3.5, 7, 14, 28, 40 and 56 MHz channels as well as to any of **4QAM, 16QAM, 32QAM, 64QAM, 128QAM and 256QAM modulations**, thus providing various capacities to suit particular needs.

SAF Tehnika has employed most modern design solutions and components to create high performance split mount system with **low power consumption** – 33-69W per system.

CFIP is a perfect building block for any modern future proof wireless network, including mobile service providers, fixed data service operators, enterprise customers, municipal and governmental networks among others.

1.2 CFIP Phoenix feature Summary

1.2.1 Main Features

- Split mount system solution
- Capacity: up to **363 Mbps**
- Channel Bandwidth: **3.5 / 7 / 14 / 28 / 40 / 56 MHz**
- Modulations: **4QAM / 16QAM / 32QAM / 64QAM / 128QAM / 256QAM**
- Interfaces: **10 / 100 / 1000 Eth + 20E1/T1**
- Traffic: Ethernet only, Eth+1E1/T1 to Eth+20E1/T1
- Frequency bands: **6 / 7 / 8 / 10 / 11 / 13 / 15 / 18 / 23 / 26 / 38 GHz**
- **ACM** and **ATPC** with **QoS** four priority queues
- **802.1Q VLAN** support

1.2.2 IDU mechanical features

- 1U high
- Power consumption: **20-30W**
- Dimensions 45x430x240 mm, weight 3 kg.



Figure 1.1 CFIP Phoenix IDU

1.2.3 ODU mechanical features

- Compact unit, **285x285x80mm**, **3.9kg**, antenna adaption backwards compatible with all **CFM** and **CFQ** series units
- **3 handles** for user convenience
- Safe and easy to use **4 side locking** arrangement
- All connectors on the side of the unit, always at **45°** regarding vertical axis for both V and H polarization
- Power consumption: **13-39W**



Figure 1.2 CFIP Phoenix ODU

1.2.4 IRFU mechanical features

- Indoor radio unit (IDU+IRFU)
- 2U high
- Power consumption: **13-39W**
- Dimensions 90x430x260 mm, weight 5.8 kg.



Figure 1.3 CFIP Phoenix IRFU

1.2.5 Interfaces/Management

- CFIP Phoenix IDU unit provides **Ethernet, E1, power, EOW, alarm, serial, 1+1, ODU connectors** and a grounding screw
- **4 Gigabit Ethernet** ports for user and management traffic
- Ethernet traffic supports **QoS** and **4 priority queues**, essential for ACM use
- **User** and **NMS traffic** could be treated as a single data stream or separated by tagging with different **VLAN** tags
- **DB-9 connector** of the unit enables serial access into the unit
- **1+1 RJ-45** connector allows to interconnect 2 CFIP Phoenix IDUs for 1+1 configuration
- Web, Telnet and SNMP are available as **NMS** interfaces into the unit

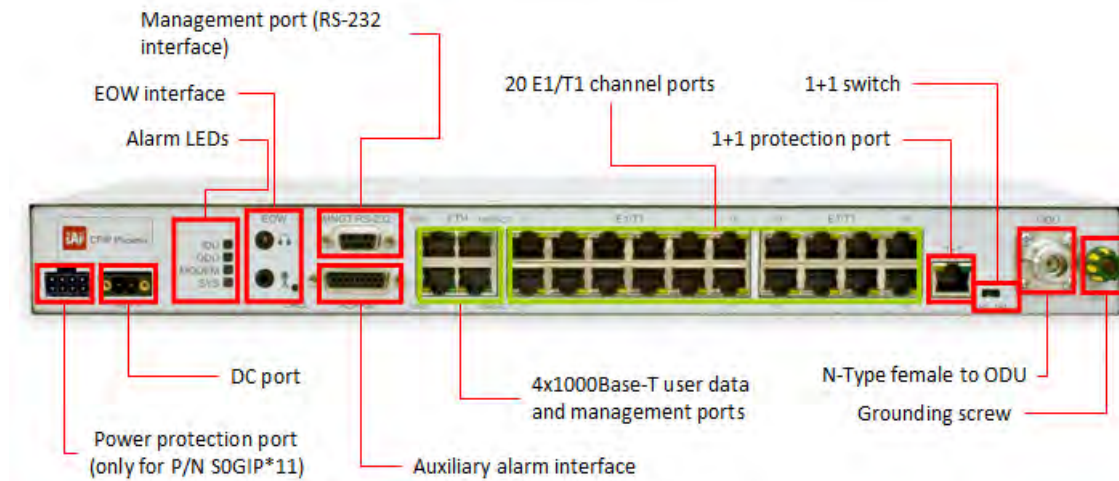


Figure 1.4 CFIP Phoenix IDU connectors

1.3 CFIP Phoenix ODU Parameters

- CFIP Phoenix is a good example of latest achievements in modem and transceiver development, providing both excellent radio parameters (System Gain), due to use of **QAM modulations** and efficient despite it consumes small amount of power Tx/Rx part of the system.
- RSL Threshold at for 6GHz ODU BER 10^{-6} , 56MHz, 256QAM, 363Mbps: **-64 dBm**.
- System Gain with guaranteed max Tx power and Rx sensitivity is **76 dB (SP)** and **84 dB (HP)**
- **ACM** (Adaptive Coding and Modulation), hitless ACM opens new possibilities depending on network designers strategy
- **ATPC**, Automatic Transmitter Power Control, for increased deployment density capability.
- **Very high flexibility** allows configuring the system to various channel bandwidths, modulation schemes and capacity settings

1.4 Application Examples

1.4.1 CFIP Phoenix 1+0 configuration

- Basic split-mount 1+0 system with up to 20E1/T1 or up to 363 Mbps Ethernet

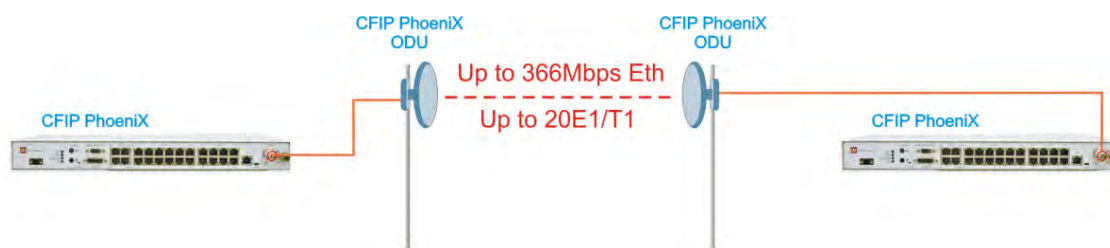


Figure 1.5 CFIP Phoenix 1+0 configuration

1.4.2 CFIP Phoenix 1+1 Frequency Diversity (FD)

- FD protected (1+1) configuration is used with single antenna and OMT (orthomode transducer) or a coupler at each side of the link;
- Each pair of ODUs utilizes its own frequency channel (f_{low} , f_{high} , f'_{low} , f'_{high});

- The outgoing (Tx) traffic at each site is passed to both ODUs, and both are always transmitting;
- The incoming (Rx) traffic is picked from one of the ODUs;
- 1+1 configuration provides hardware redundancy and mitigates multipath fading;
- Both Tx and Rx switching is hitless.

1.4.3 CFIP Phoenix 1+1 Hot Stand-by (HSB)

- HSB protected (1+1) configuration is used with single antenna and a coupler at each side of the link;
- Both the incoming (Rx) and outgoing (Tx) traffic is switched to either one link or other, only single ODU at each side is transmitting;
- Protects modem and radio from failure;
- Rx switching is hitless, Tx switching <50ms.

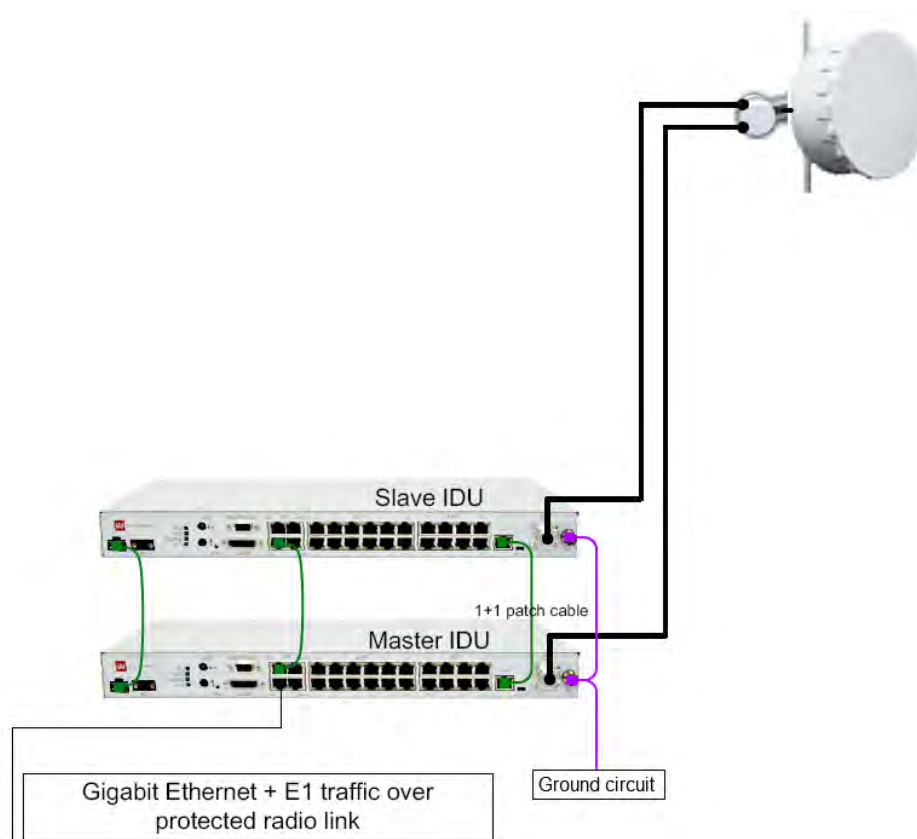


Figure 1.6 CFIP Phoenix FD and HSB 1+1 configuration

1.4.4 CFIP Phoenix 1+1 Space Diversity (SD)

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

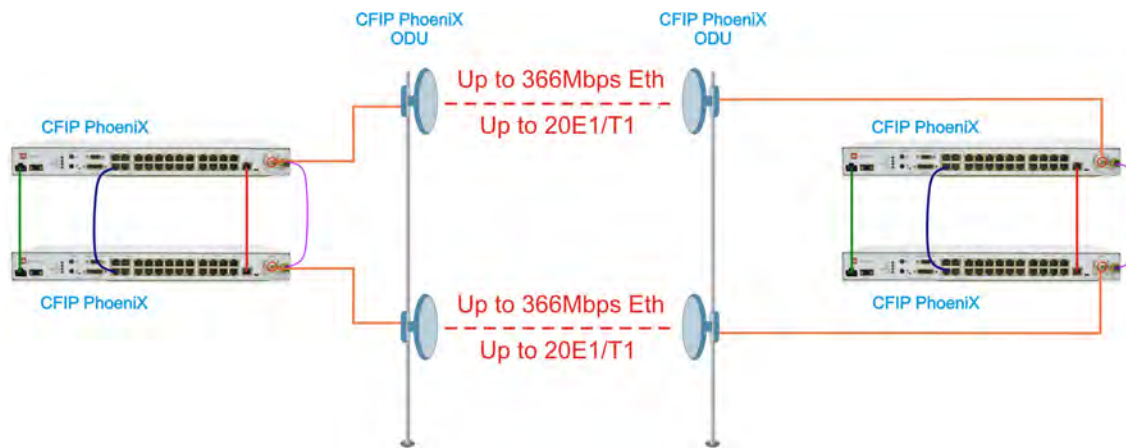


Figure 1.7 CFIP Phoenix 1+1 SD configuration

1.4.5 CFIP Phoenix Ring Topology

- Utilization of STP protocol allows CFIP Phoenix operation in ring topology (for Ethernet traffic only)

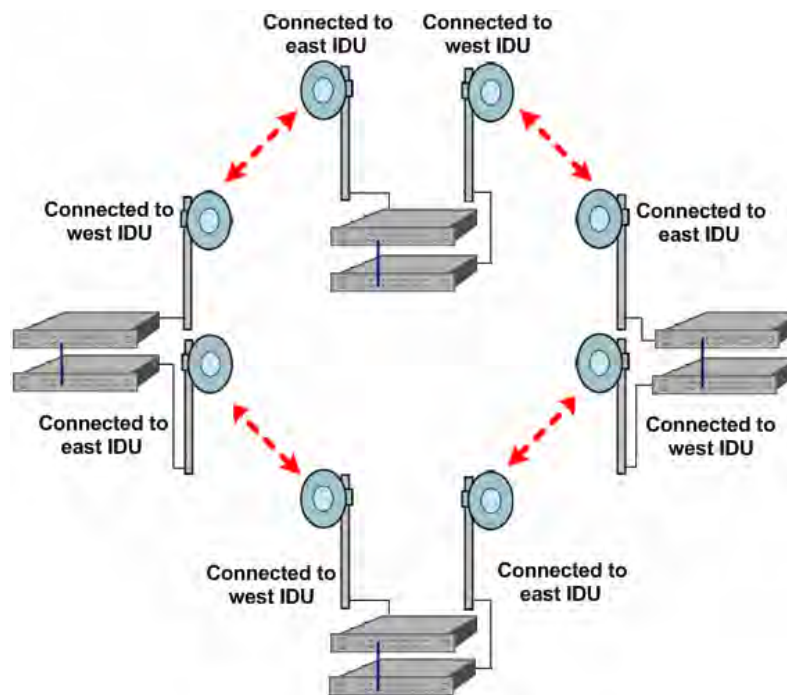


Figure 1.8 CFIP Phoenix ring topology configuration

1.5 Technical specification

CFIP Phoenix IDU

Modem	
Channel Bandwidths	3.5, 7, 14, 28, 40, 56 MHz
Modulations	4QAM, 16QAM, 32QAM, 64QAM, 128QAM, 256QAM
Capacity	9 - 363 Mbps
Supported ODUs	CFIP ODU
Applications	
Configuration	1+0, 1+1 (HSB, SD, FD), Ring/Mesh (with RSTP), 2+0, 3+0, 4+0 (built-in Ethernet aggregation)
Protection switching	Hot Stand-by (<50ms), Space/Frequency diversity (hitless, errorless)
Ports	
Ethernet	4x1000Base-T, RJ-45
E1 / T1	20 E1/T1, RJ-45
Serial port for configuration	RS-232, DB-9 connector
Alarm port	4 digital inputs, 4 relay outputs (26 pin hi-density D-SUB)
ODU port	N-Type Female
EOW port	3.5mm headset and mic, 64 Kbps
Extension/protection port	RJ-45
DC power connector	2ESDV-02 with screw locks
Management features	
Management port	Ethernet with VLAN support or serial (RS-232)
Monitoring	via Telnet, WEB GUI, NMS, SNMP Manager, Serial interface
SNMP	Yes, SNMP traps, MIB, SNMP v1/v2c, RMON
EMS	Uptime, Rx level, Tx level, System temperature, Radial MSE, LDPC decoder stress, constellation diagram, equalizer graph
ATPC feature	Web based, HTTP
ACM feature	Yes
Ethernet	
Switch type	Managed Gigabit Ethernet Layer 2
Max frame size	9728 bytes
MAC table	4K entries; automatic learning and aging
Packet buffer	128KB; non-blocking store & forward
Flow Control	IEEE 802.3x
VLAN support	IEEE 802.1Q (up to 4K VLAN entries)
QinQ (Double Tagging)	Yes, IEEE 802.1ad (Providing Bridging Technique)
QoS	64 level DiffServ (DSCP) or 8 level 802.1p mapped in 4 prioritization queues with VLAN support
QoS queuing	Fixed or weighted (configurable ratio)
Spanning Tree Protocol	IEEE 802.1D-2004 RSTP, IEEE 802.1Q-2005 MSTP
MEF	MEF 9, MEF 14
Mechanical & Electrical	
Operational use	Conforms to ETSI EN 300 019 Class 3.1E, IP20, NEMA 1
Temperature Range / Humidity	-5°C to +55°C / 5% to 95%
Dimensions: HxWxD / weight	1U (45x430x240 mm) / 3.1 kg
Max. power consumption	20-30 W
IDU-ODU connection	Belden 9914/RG-8 cable (300 m), RG213 cable (200 m), N-Type connectors
DC port	-40.5V to -57V DC (conforms to ETSI EN 300 132-2)
Built-in DC and IF port surge protection	Conforms to ETSI EN 301 489-1; EN 61000-4-5; IEC 61000-4-5



Ports	CFIP Phoenix ODU	CFIP Phoenix IRFU
Antenna	N-Type or flange	A) N-Type or flange B) Tx and Rx ports ¹
IF to IDU	N-Type	SMA
RSSI	BNC	2-port for multi-meter
Power	--- (over IF port)	2-pin power port (alternative to IF port)
Mechanical & Electrical		
Operational use	Conforms to ETSI EN 300 019 Class 4.1, IP65, NEMA 4X	Conforms to ETSI EN 300 019 Class 3.1E, IP20, NEMA 1
Temperature Range	-33°C to +55°C	-33°C to +55°C
Dimensions: HxWxD / weight	288x288x80 mm / 3.5 kg	19" 2U rack 90x430x260 / 5.8 kg
IF port surge protection	Conforms to ETSI EN 301 489-1; EN 61000-4-5; IEC 61000-4-5	
Input DC voltage	-40.5V to -57V DC (conforms to ETSI EN 300 132-2)	
Max. power consumption	SP: 13-27 W; HP: 21-39 W	

Max Tx Power					
Modulation	Standard / High Tx Power ¹ , dBm				
	4, U4 GHz	L6, U6, 7, 8 GHz	10, 11, 13, 15 GHz	18, 23, 26 GHz	38 GHz
4QAM	+33	+19/+27	+19/+25	+19	+17
16QAM	+32	+18/+26	+18/+24	+18	+16
32QAM	+31	+17/+25	+17/+23	+17	+15
64QAM	+29	+15/+23	+15/+21	+15	+13
128QAM	+29	+15/+23	+15/+21	+15	+13
256QAM	+26	+12/+20	+12/+18	+12	+10

Band	Frequency range	Duplex offset
4 GHz	3.6 – 4.2 GHz	213 MHz, 320 MHz
U4 GHz	4.4 – 5.0 GHz	100 MHz, 300 MHz, 312 MHz
L6 GHz	5.925 – 6.425 GHz	252.04 MHz, 266 MHz
U6 GHz	6.425 – 7.125 GHz	160 MHz, 170 MHz, 200 MHz, 340 MHz
7 GHz	7.110 – 7.900 GHz	154 MHz, 161 MHz, 168 MHz, 196 MHz, 245 MHz
8 GHz	7.725 – 8.5 GHz	119 MHz, 126 MHz, 151.614 MHz, 154 MHz, 160 MHz, 208 MHz, 266 MHz, 300 MHz, 310 MHz, 311.32 MHz, 525 MHz, 550 MHz

Band	Frequency range	Duplex offset
10 GHz	10.15 – 10.68 GHz	65 MHz, 91 MHz, 300 MHz, 350 MHz
11 GHz	10.7 – 11.7 GHz	490 MHz, 500 MHz, 530 MHz
13 GHz	12.75 – 13.25 GHz	225 MHz, 266 MHz
15 GHz	14.4 – 15.35 GHz	315 MHz, 322 MHz, 420 MHz, 475 MHz, 490 MHz, 644 MHz, 728 MHz
18 GHz	17.7 – 19.7 GHz	1008 MHz, 1010 MHz, 1560 MHz
23 GHz	21.2 – 23.6 GHz	1008 MHz, 1036 MHz, 1200 MHz, 1232 MHz
26 GHz	24.25 – 27.5 GHz	800 MHz, 1008 MHz
38 GHz	38.6 – 40 GHz	700 MHz, 1260 MHz

CFIP ODU waveguide flange sizes						
4, U4, L6, U6 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

Notes:

¹ For CFIP Phoenix IRFU with Tx and Rx ports (without diplexer), Tx Power and RSL figures for improve by up to 2 dB

CFIP Phoenix ODU

CFIP 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	4QAM	Strong	-97	-95	-95	-97	-96	-95	-93,5	-95	-97	-96,5	-93,5	3
	16QAM	Strong	-90,5	-88	-88	-90	-89	-88	-88	-88,5	-90	-89,5	-86,5	7
	32QAM	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	4QAM	Strong	-93	-92	-92	-94	-93	-92,5	-91	-92	-94	-93,5	-90,5	8
	16QAM	Strong	-86,5	-85	-85,5	-87,5	-86,5	-85,5	-85	-85,5	-87,5	-87	-84	17
	32QAM	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	4QAM	Strong	-90	-90,5	-90	-91	-90	-90	-89	-90,5	-91	-90,5	-87,5	17
	16QAM	Strong	-83,5	-83,5	-83,5	-84,5	-83,5	-83,5	-83	-84	-84	-83,5	-80,5	34
	32QAM	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
		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	4QAM	Strong	-90,5	-89,5	-89	-88,5	-89,5	-89,5	-89	-90	-89	-91,5	-85	35
	16QAM	Strong	-84,5	-83	-83	-82,5	-83,5	-83,5	-83	-84	-83	-85	-79	69
	32QAM	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
		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

CFIP 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	4QAM	Strong	-89	-87.5	-88	-87.5	-88	-88	-88	-88	-87.5	-89.5	-83.5	49
	16QAM	Strong	-82.5	-81.5	-81.5	-81	-82	-82	-81.5	-82.5	-81	-83.5	-77	98
	32QAM	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	4QAM	Strong	-87	-85.5	-86	-85.5	-87	-86.5	-86	-87	-85.5	-88	-81.5	72/67*
	16QAM	Strong	-81	-80	-79.5	-79.5	-80.5	-80	-79.5	-80.5	-79.5	-82	-75.5	145/135*
	32QAM	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

* Higher capacity is available in 16QAM and 4QAM if using 32QAM-256QAM with ACM enabled

** According to ETSI channel plan

*** Forward Error Correction (FEC) can be optimized either for sensitivity (Strong FEC) or for capacity (Weak FEC)

1.6 Cable Requirements

IDU-ODU cable

IDU-ODU cable is a 50 Ω coaxial cable intended to interconnect the Indoor Unit with the Outdoor Unit. Any type of 50 Ω cable of good quality can be used; the cable should be equipped with N-type male connectors on each end. There are two N-type male connectors included in each radio unit delivery that fit RG-213 cables or other cables with a surface diameter of 10 mm. As the attenuation of the cable is essential particularly at 350 MHz frequency, its usage is restricted, - the attenuation of the signal should not exceed 20 dB at 350 MHz. Commonly employing RG-213 type coaxial cable, its length may reach 100 m, LMR-400 type cable may usually reach up to 300 m in length.



Figure 1.9 CFIP Phoenix IDU-ODU cable

DC power cable

Due to low power consumption of the CFIP Phoenix split mount system, there are no special requirements for the cable used to connect the IDU to the DC power source. Any 2 wire power cable of good quality which fits well in SAF Tehnika's supplied 2 pole "screw on" power connector could be used. The power connector is 2 pole, type 2ESDV-02.

1+1 protection cable

Cable used should be rated Cat6 STP or better and length of the cable should not exceed meters. For pinouts and further details please refer to Chapter 10.6.

RS-232 Serial Connection

The ASCII console must be connected to the RS-232 serial port. This requires a twisted pair (TP) cable with common shield (foil and plaited shield); the cable must be suitable for DB-9 connector.

Using a proper cable, the operation is guaranteed for up to 10 m of cable.

RSSI BNC

To connect the digital multimeter to the CFIP Phoenix ODU RSSI port in order to adjust the antenna alignment, a coaxial cable with BNC connector on one end and appropriate termination on other end can be used (see example in *Figure 1.10*).



Figure 1.10 Cable for connecting the voltmeter to the CFIP Phoenix ODU RSSI port

1.7 Labelling

The label can be found on the front side of the unit.

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

- Model name. The model name example is:
CFIP-IDU-Phoenix for CFIP Phoenix Indoor Unit (IDU),
CFIP-18-Phoenix for 18GHz Outdoor Unit (ODU), etc
- Product Number (S0GIPT01, S18RFU05LA): product number contains information of product version (01), in case of ODU - in which frequency band (18) and band side (L, H) the ODU operates. Letters A, B, C or D indicate specific subband.
- Unit Serial Number (3221901 00024); the serial number uniquely identifies the unit.

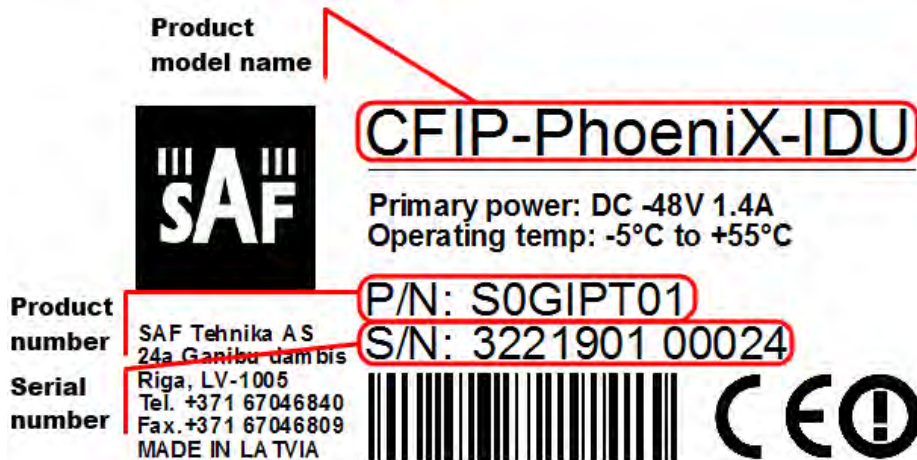


Figure 1.11 Label of the CFIP Phoenix Indoor Unit

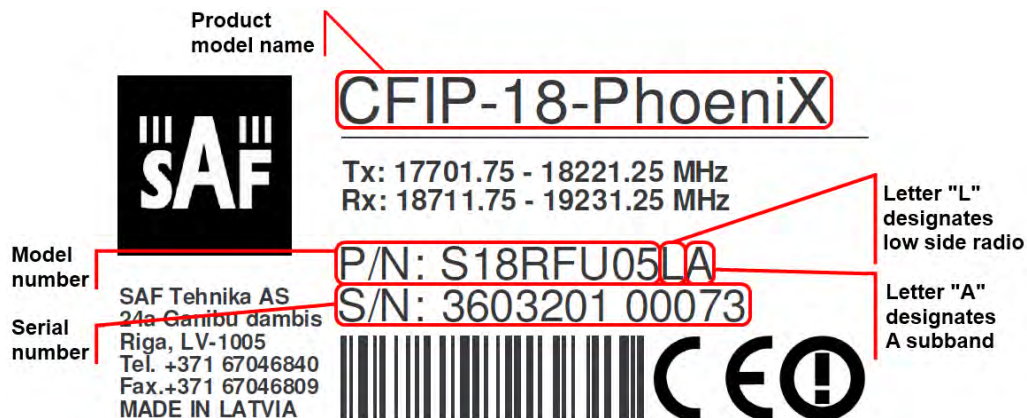


Figure 1.12 Label of the CFIP Phoenix ODU Low band side, operating in 18 GHz band



Figure 1.13 Label of the CFIP Phoenix IRFU Low band side, operating in 6 GHz band

P/N Translation for CFIP Phoenix ODU:

- "S" designates CFIP split mount series product;
- "18" designates Frequency range (18 GHz) of the Unit;
- "RF" designates standard power radio;
- "U" designates unified band ODU operating 3.5 - 56MHz;
- "05" designates the version number of the Unit;
- "L" designates the band side in which ODU operates (H, L);
- "A" designates the subband in which ODU operates (A, B, C).

Please note that frequency range is set from the central frequency of the first 14 MHz channel to the central frequency of the last 14 MHz channel (see the **Figure 1.14**).

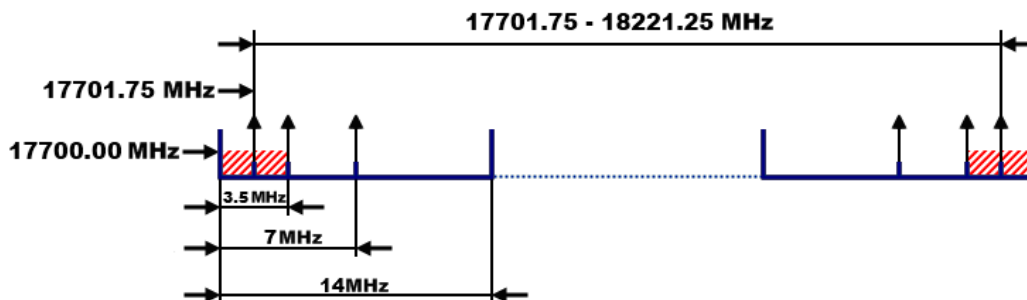


Figure 1.14 Frequency range of the low side CFIP Phoenix 18 GHz ODU

Figure 1.14 explains Tx frequency range of low side CFIP Phoenix 18 GHz radio.

2 Configuration and Management

2.1 Connecting CFIP Phoenix IDU to power source

In case AC/DC Power supply, 48VDC, 80W (EU - P/N IOAB4810, US – P/N IOAB4811, AUS - IOAB4818) provided by SAF Tehnika JSC is used to power up CFIP Phoenix IDU, interconnect IDU and power source through appropriate connectors. Otherwise perform the following steps to ensure that CFIP Phoenix IDU is powered up correctly:

1. It is necessary to interconnect CFIP Phoenix IDU DC power connector (located on left side of front panel) with power source. For this purpose power cable is required. Any 2 wire power cable of good quality which fits well in SAF Tehnika's supplied 2 pole "screw on" power connector could be used. The power cable connector is 2 pole, type 2ESDV-02. This connector has screw clamp terminals that accommodate 24 AWG to 12 AWG wire. The recommended wire size for construction of power cables under 3 meters in length, supplying -48 V DC, is 18 AWG. The opposite end of the power cable should have a termination appropriate for the power supply being used. The power cable should be of sufficient length to avoid tension in the cable and provide a service loop for connection, but not be of excessive length. Using the power cable connector of type 2ESDV-02, pin 1 (labelled '-') should be connected to the power supply terminal supplying -48 V DC, while pin 2 (labelled '+') should be grounded. Refer to **Figure 2.1**.

(!) Note that pin 2 ('+') of the CFIP Phoenix IDU DC Power connector (**Figure 2.1**) is connected to the IDU chassis ground internal to the IDU. Use of a power supply with an inappropriate ground reference may cause damage to CFIP Phoenix IDU and/or the power supply.

2. Connect the power cable to the -48 V DC power supply, and place the voltmeter probes at the unconnected ends of the power cable, with the positive voltmeter probe on pin 1 ('-') of the cable connector and the negative probe on pin 2 ('+'). The connector screw terminal screw heads may be used as convenient monitor points. Refer to **Figure 2.1**.
3. Turn on the -48 V DC supply. Verify that the digital voltmeter reads between -36 V DC and -57 V DC when monitoring the cable points specified above. Adjust the power supply output voltage and/or change the connections of the power supply to achieve this reading.
4. With the negative voltmeter probe still on pin 2 ('+') of the power cable connector (and the power supply still on), put the positive voltmeter probe to the CFIP Phoenix IDU chassis and verify a potential of zero volts between the IDU chassis and cable pin 2 ('+'). If the measured potential is not zero, the power supply may be grounded incorrectly and should not be used for CFIP Phoenix IDU powering. Note that this measurement assumes that CFIP Phoenix IDU is installed and properly grounded. If that is not the case, the same measurement can be made between cable pin 2 ('+') and a convenient ground (such as an ac outlet third-wire ground).
5. Turn the -48 V DC supply off.
6. Plug the power cable into CFIP Phoenix IDU front panel DC Power connector (**DC Input**). Place the voltmeter probes on the cable connector screw terminal screw heads as described in step 2 above. Refer to **Figure 2.1**. Note that CFIP Phoenix IDU does not have a power on/off switch. When DC power is connected, the digital radio powers up and is operational. There can be up to 500 mW of RF power present at the antenna port. The antenna should be directed safely when power is applied.
7. Turn on the -48 V DC power supply, and verify that the reading on the digital voltmeter is as specified in step 3 above.

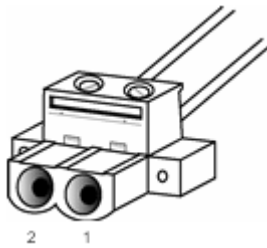


Figure 2.1 CFIP Phoenix IDU DC Power Cable Connector of type 2ESDV-02

After successful powering of Phoenix IDU there are four ways to adjust and read settings and operation parameters of the CFIP Phoenix equipment:

- 1. using Web terminal connected to the 10/100/1000Base-T Port,
- 2. using Telnet terminal connected to the 10/100/1000Base-T Port,
- 3. using NMS or SNMP terminal, connected to the 10/100/1000Base-T Port, or
- 4. using ASCII console connected to the serial port.

2.1.1 Power protection port

Optionally CFIP Phoenix IDU can be equipped with power protection port, which allows you to interconnect 2 CFIP Phoenix IDUs in 1+1 configuration for power interface redundancy functionality. Interconnection between power protection ports is done with optional power protection cable (P/N SOACPR11).

(!) Power protection port is available for CFIP Phoenix IDU with P/N SOGIP*11



Figure 2.2 CFIP Phoenix power protection port and cable (for IDU SOGIP*11)

2.1.2 Connecting CFIP Phoenix IRFU to power source

CFIP Phoenix IRFU can be powered via coaxial IF cable or using separate power supply, providing at least 60W load power.

(!) Note that pin 2 ('+') of the CFIP Phoenix IRFU DC Power connector (Figure 2.1) is connected to the IDU chassis ground internal to the IDU. Use of a power supply with an inappropriate ground reference may cause damage to CFIP Phoenix IRFU and/or the power supply.

2.2 Resetting the CFIP Phoenix

Depending on the method used, the user may reset the whole terminal or the management controller individually, see table below for details.

Reset action unplugging power source.	Restarts both the multiplexer module and the management module. Resets all management counters.
Resetting with  button in Web GUI 'Configuration → System configuration' window or using command	Restarts CPU of the management controller. Resets all management counters.

prompt command "system reset"	
Resetting with command prompt command "system reset cold"	Restarts modem and CPU of the management controller. Resets all management counters.

2.3 Web Interface

This section describes operation of Web interface.

2.3.1 10/100/1000Base-T Ports

10/100/1000Base-T port is used to connect CFIP Phoenix to a PC or Ethernet network for Web, SNMP and Telnet management.

(!) The length of 10/100/1000Base-T Port cable should not exceed 100m.

2.3.2 Ethernet Management Connection Configuration

Before proceeding with initial link setup in Web GUI, you must adjust IPv4 settings of your LAN adapter to 192.168.205.0 subnet. IP address should be other than default low/high side IP addresses (192.168.205.10/192.168.205.11).

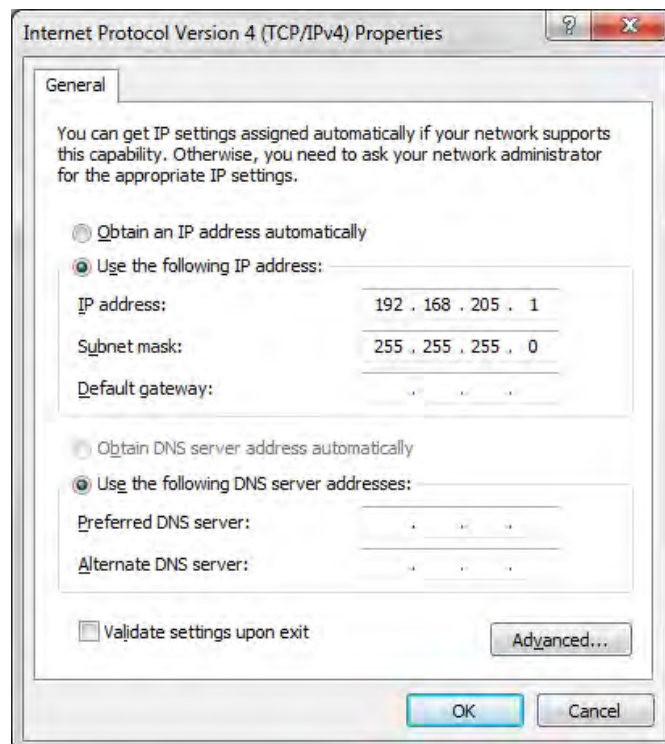


Figure 2.3 Internet Protocol Version 4 (TCP/IPv4) Properties

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

2.3.3 Connecting to Web Interface

It is recommended to use the following web-browsers (and all later versions):

- IE v. 6.0
- Mozilla Firefox v. 2.0.0.11
- Google Chrome



Figure 2.4 Supported browsers: “Internet Explorer”, “Mozilla Firefox” and “Google Chrome”

After web browsers selection, open it and enter address of the CFIP Phoenix IDU (**Figure 2.5**).

(!) The IP address of CFIP Phoenix IDU is **192.168.205.10**

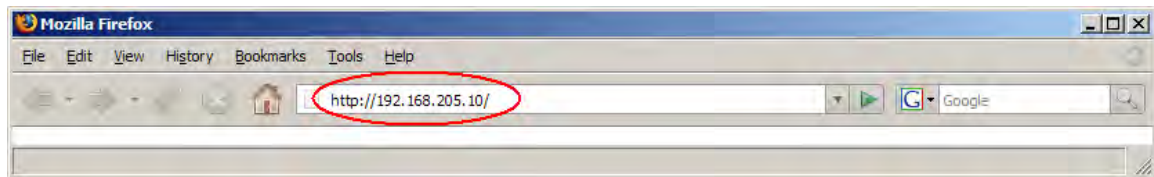


Figure 2.5 CFIP Phoenix IP address

(!) The default username and password for Web access are:

- username: *admin*
- password: *changeme*

If the IP address is correct and you have suitable browser version, you will see confirmation text. After confirmation you will be redirected to Web interface page. In case of not valid IP address you will not obtain the configuration interface. In case your browser is not accepted, you will see the text informing about that. You can push the button “Continue Anyway” to be redirected to Web interface page.

At first “Configuration→Configuration wizard” should be run in order to perform basic link configuration (by default Tx power is disabled and parameters of remote side will not be seen).

If configuration was made correctly, you will see the main window of the WEB Interface. If in the field displaying Local and/or Remote system values there are problems (configured values are not the same for Local and Remote, or there is a problem with parameter value), the appropriate cell will be highlighted in red colour.

(!) If you are not obtaining the correct Web page, try to clear browser cookies, cache and offline data and restart the browser.

(!) All the commands executed from Web GUI will be interpreted CLI commands and will be executed as in CLI.



Figure 2.6 Web Interface - main window

2.3.4 Interface Description

WEB interface consists of four parts, they are:

1. Top panel, that allows to log out and gives information about device type, software version, device name, IP, serial number and uptime;
2. Menu panel that is used to open links to other pages;
3. Status summary for local and remote devices: this section is available while browsing other pages.
4. The main panel where the new pages selected from the menu panel are displayed;

Also, special marks are used:

- Entries highlighted in red indicate that specific parameters do not comply with the norms of standard operation. For example: value is out of range; local value is not equal to the remote value and vice versa (only in some places); no value data (N/D).
- Entry highlighted in yellow indicates warning.
- 'N/D' in value place corresponds to 'No Data'.
- 'N/A' in value place corresponds to 'Not Available'.



Figure 2.7 Web Interface - main window with section numbering

2.3.5 Command Execution

There is "IP configuration" page shown in **Figure 2.8**. The entire page is divided into smaller fragments:

1. The header of page;
2. Sub-header of single type configuration parameters;
3. Execution controls related to a single type configuration parameters.
4. „Execute configuration“ button executes configuration changes only on the local side CFIP Phoenix, but "Execute for both" executes configuration changes on both remote and local side of CFIP Phoenix link. Enabling rollback feature allows going back to previous configuration in case of management connectivity loss.
5. Write to config file button, which generates "cfg write" CLI command, which saves changed configuration;
6. Configuration parameter name;
7. Configuration parameter **current** value;
8. Comments (not on every page).

“Execute for both” is available in “Main configuration” section during configuration of modem or ATPC parameters for local and remote radio sides simultaneously. Connection between both management CPUs must be established in order to complete successfully configuration execution for both sides.

“Rollback on” feature is intended to maintain connectivity of the CFIP link by cancelling last erroneous configuration changes and reverting to previous successful configuration used. Rollback will activate only if you lose connection to WEB interface of CFIP Phoenix after configuration changes applied, and reverting process will take approx. 3 minutes.

After parameter value editing, when the focus from this object is removed, this parameter value edit box may be highlighted in red, meaning that entered value is not valid.

If “Execute configuration” or “Execute for both” buttons are pressed, and one or several configuration values edit boxes is/are highlighted in red, the user will see error message with the explanation text.

The screenshot displays the CFIP Phoenix IDU web interface. At the top, a header bar shows the SAF logo, system name (SAF), IP (192.168.205.10), SN (323130101669), and uptime (02:23:09). The main content area is divided into a sidebar and a main panel. The sidebar contains links for Status, Configuration, Performance, Tools, and Help. The main panel features several configuration sections: 'Ethernet management port IP configuration' (with fields for IP address, mask, gateway, MAC address, and remote IP address), 'IP services' (with fields for FTP and TFTP services), and 'Static route configuration' (with fields for network address, mask, gateway, and flags). Red numbers 1 through 8 are overlaid on the interface to highlight specific elements: 1 points to the 'Ethernet management port IP configuration' section header; 2 points to the 'IP services' section header; 3 points to the 'Execute configuration' button; 4 points to the 'Execute & write configuration' button; 5 points to the 'Write to config file' button; 6 points to the IP address input field; 7 points to the IP mask input field; and 8 points to the 'System returned!' status message at the bottom.

Figure 2.8 Web Interface - IP configuration page with numbering

2.3.6 Initial Configuration with Web GUI

IP settings of connected laptop should be in the same subnet as manageable CFIP in order to observe it. Refer to Chapter 2.3.2 for further details. The next step is to connect to CFIP Phoenix by entering IP in the browser address line – which is by default 192.168.205.10. In case you are not sure which side you are managing at the moment, you can try both default IP addresses.

When you are connected to the CFIP Phoenix, you will see the window similar to the one shown in **Figure 2.6**.

To start simple configuration process, you must proceed with the configuration wizard which will set up the main parameters of the link to make it work. So, the first step is to go to ‘Configuration → Configuration wizard’ as shown below in the **Figure 2.9**.

Local system summary	
Rx level	-50 dBm
Rx modulation	256QAM
Radial MSE	-31.3 dB
LDPC stress	5.9e-05

Remote system summary	
Rx level	-50 dBm
Rx modulation	256QAM
Radial MSE	-30.2 dB
LDPC stress	4.0e-04

Figure 2.9 Starting configuration wizard

Initially, you can specify preferable system name, location name, passwords for guest and admin accounts.

(!) Default password for “admin” account is *changeme*.
“guest” account is disabled by default!

The next time you will try to access the Web GUI management, you will be asked to enter the user name (guest or admin) and user password.

(!) It is highly recommended to name the system after its geographical location.

By default, system name is ‘SAF’, but location name is not specified.

It is possible to perform configuration for local and remote ends of the link simultaneously. Please note that it requires modem synchronization between both sides of the link.

Local system summary	
Rx level	-50 dBm
Rx modulation	256QAM
Radial MSE	-31.3 dB
LDPC stress	5.9e-05

Remote system summary	
Rx level	-50 dBm
Rx modulation	256QAM
Radial MSE	-30.2 dB
LDPC stress	4.0e-04

Figure 2.10 STEP 1. Defining system name, location name and passwords for “guest” and “admin” accounts

After accepting and pressing ‘Next step >>’ button, you will be redirected to the second configuration wizard screen, where you will be asked to define the network IP settings by entering IP address, IP mask, default gateway and remote link side IP address.

Configuration wizard	
STEP 2: IP address configuration	
Please enter system IP address and network mask	
IP address	192.168.205.10
IP mask	255.255.255.0
IP default gateway	255.255.255.255
Remote IP Address	192.168.205.11
Previous step <<	Next step >>

Figure 2.11 STEP 2. Defining IP address, mask, default gateway and remote IP address

The third screen of the wizard is devoted to the modem and radio configuration and requires specifying utilized bandwidth (from 3.5 to 56 MHz), modulation type (4QAM, 16QAM, 32QAM, 64QAM, 128QAM or 256QAM), E1 channel port numbers, Tx power (range depends on modulation chosen) and Tx frequency; besides, the modem and radio data status is being shown. These configuration parameters will determine overall link capacity.

Configuration wizard	
STEP 3: Modem and radio configuration	
Please enter system modem and ODU parts parameters	
Modem configuration	
Modem data status	Ok
Modem standard	ETSI ▼
Bandwidth	56000 ▼ kHz
Modulation	256QAM WeakFEC ACM ▼
E1 channels	☐ 01 ☐ 02 ☐ 03 ☐ 04 ☐ 05 ☐ 06 ☐ 07 ☐ 08 ☐ 09 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ Select/Deselect
Radio configuration	
Radio data status	Ok
Tx power (0 .. 12 dBm for 256QAM modulation with ACM)	12 dBm
Tx frequency (17728000 .. 18195000 kHz)	17728000 kHz
Previous step <<	Next step >>

Figure 2.12 STEP 3. Defining modem bandwidth and modulation

The final screen allows checking the selected settings and applying them. The optional settings are as follows:

- *Clear cfg file before the new settings will take place* – resetting or keeping all the other parameters, not mentioned here, after configuration execution
- *Set local machine time* – uses the time of your laptop
- *Write this configuration into cfg file* – configuration is automatically written in configuration file

If „Rollback on“ is selected, configuration will be reverted in case erroneous configuration changes are applied

Configuration wizard

STEP 4: Check parameters

Please verify the parameters set.

guest	
Password	
admin	
Password	
System name	SAF
Location name	1
IP address	192.168.205.10
IP mask	255.255.255.0
IP default gateway	255.255.255.255
Remote IP address	192.168.205.11
Modem standard	ETSI
Bandwidth	56000 kHz
Modulation	256QAM WeakFEC ACM
E1 channels	0 ()
Tx power	12 dBm
Tx frequency	17728000 kHz
Clear cfg file before the new settings will take place	☒
Set local machine time	☒
Write this configuration into cfg file	☒
Previous step <	Rollback on ☒ Execute configuration

Figure 2.13 STEP 4 Checking settings and executing configuration

To verify the settings, we can go to 'Status' or the main screen, which is the first option in the navigation panel. If there are no 'red fields', everything is set correctly and the link is up.

2.4 Command Prompt Interface

CFIP equipment can be monitored and configured by using command interface described in this chapter.

This process is performed by connecting to Telnet terminal via Ethernet management port; Telnet management supports only one client.

Command line management interface offers the wider configuration and monitoring functionality. The available commands for Telnet management are found in detailed explanation of Web GUI windows, as well as in tables of additional commands.

(!) – To end Telnet session press Ctrl+D. Opening the session again, the prompt will appear to enter username and password.

– Default username is *admin* and password - *changeme*

(!) Syntactic notes for command prompt commands

- Commands are in **bold** font.
- All arguments (variables) are in *italic* font.
- Subcommands and keywords are in regular font.
- Arguments in square brackets ([]) are optional but required arguments are in angle brackets (< >).
- Alternative keywords are grouped in braces ({ }) and separated by vertical bars (|).
- The purpose of each command will be displayed if command is typed with “?” at the end (or any unrecognizable string) is entered, e.g., *radio ?*

The management system is automatically restarted if it freezes. This is performed by the watchdog timer. Restart of the management system is not affecting (interrupting) the Ethernet traffic.

2.4.1 RS-232 Serial Management Port

RS-232 serial management port provides terminal management via a connected PC or another terminal device or modem.

The terminal connected to serial management port provides the same management functionality as Telnet interfaces (refer to Chapter 2.3.2). In order to interconnect the CFIP Phoenix and the management terminal directly through serial ports, a “straight through” modem cable is required.



Figure 2.14 Serial connection to CFIP Phoenix

To connect the PC to the RS232 management port, using serial terminal-emulation software (e.g. [PuTTY](#)), use the following parameters:

- Baud rate: 19200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Data flow control: None

Below are connection steps with [PuTTY](#) - Windows freeware software.

- 1) Open *PuTTY* and go to “Serial” category. Specify your COM port number you will be using, change “Speed (baud)” to “19200” and “Flow control” to “None”:

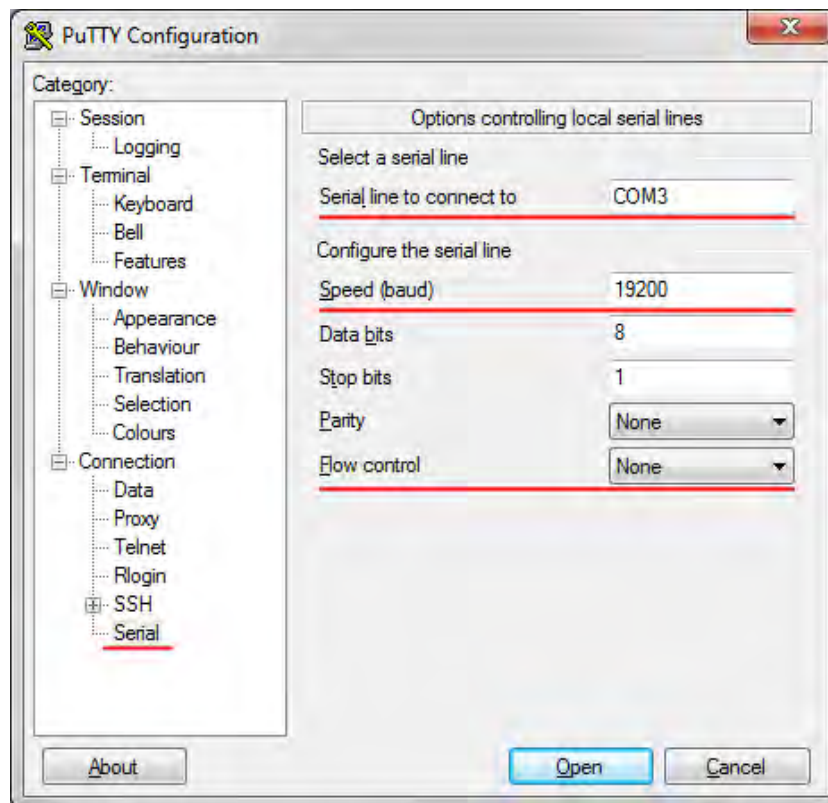


Figure 2.15 PuTTY configuration - 1

- 2) Go to "Keyboard" category and change "The Backspace Key" to "Control-H":

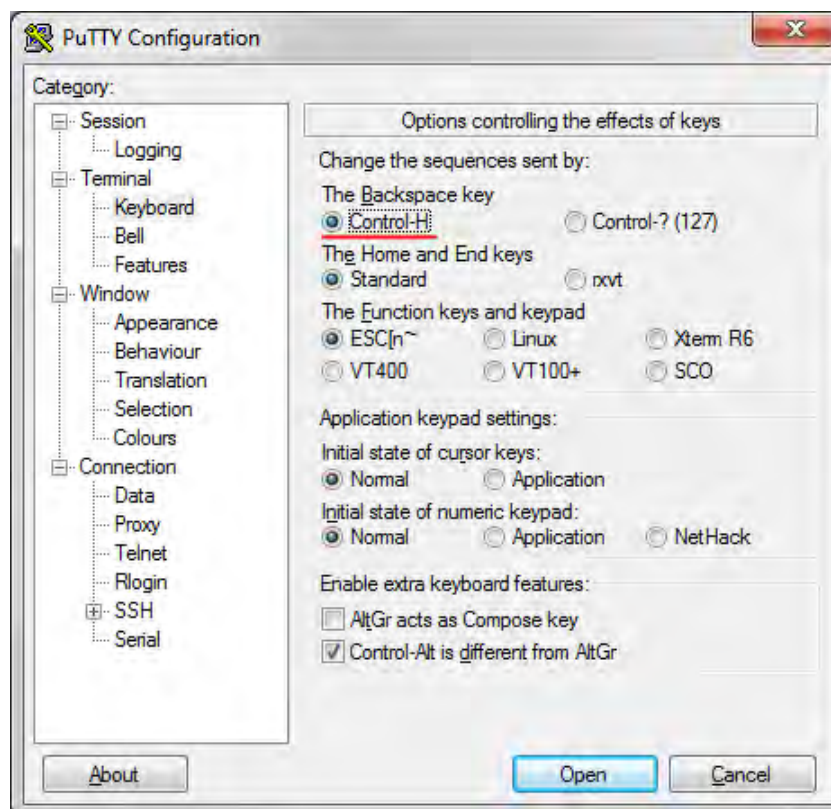


Figure 2.16 PuTTY configuration - 2

- 3) Press "Open" and after pressing "Enter" key following prompt should appear:



Figure 2.17 PuTTY serial prompt

Password is disabled by default. See Chapters 3...7 for available commands.

2.4.2 Telnet connection

The Telnet connection to the CFIP Phoenix is carried out using the Ethernet management connection. Please refer to Chapter 2.3.2 for Ethernet management port connection details.

You can use any Telnet client. Below are connection steps with [PuTTY](#) - Windows freeware software.

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

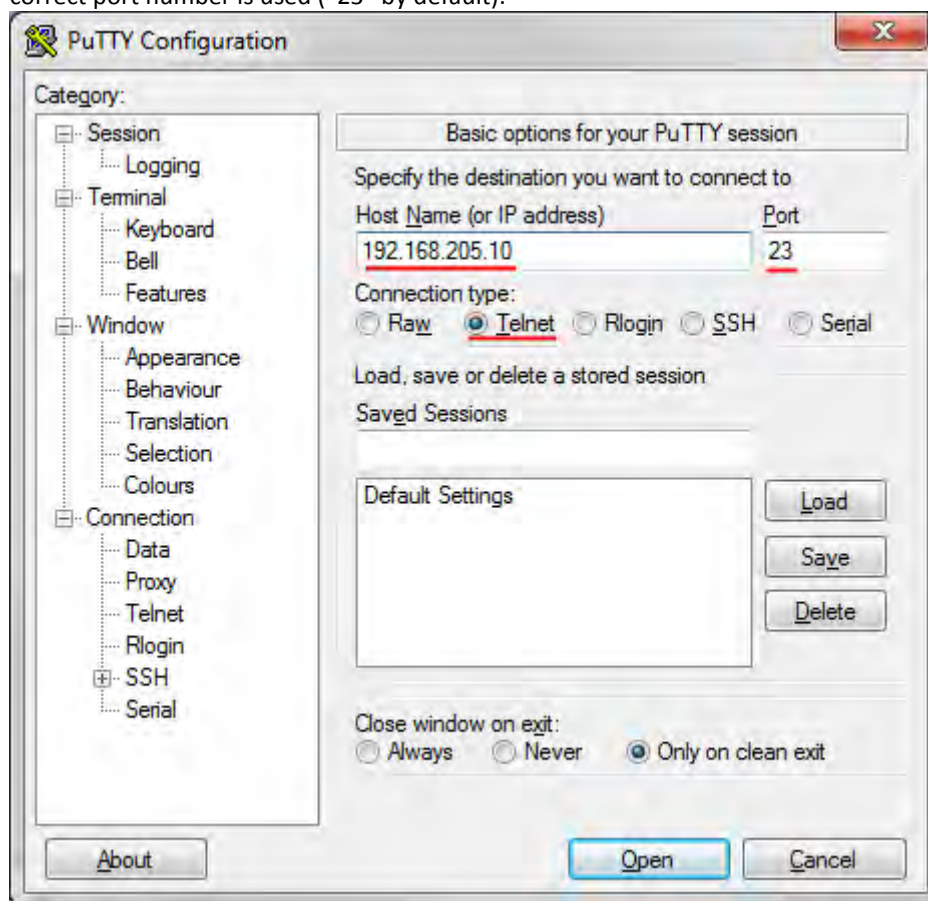


Figure 2.18 PuTTY configuration - 3

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

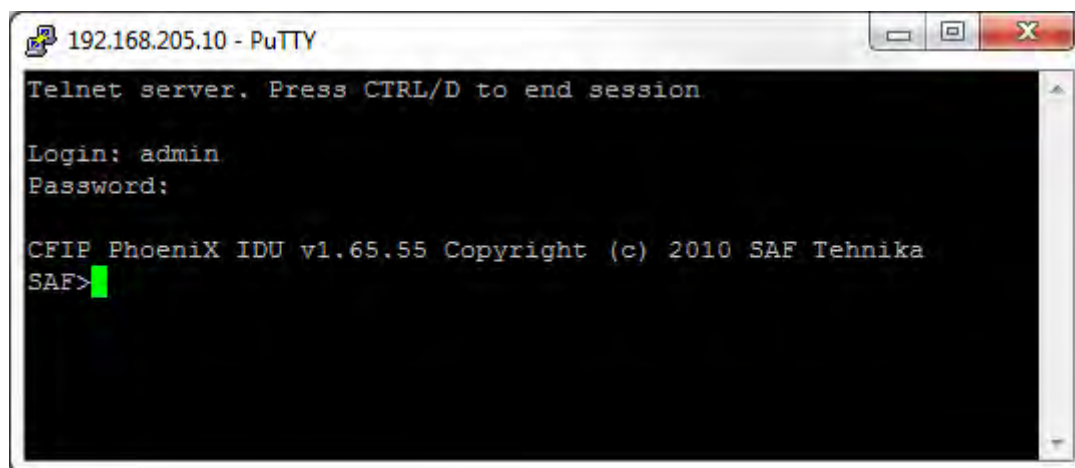


Figure 2.19 PuTTY Telnet prompt

See Chapters 3...7 for available commands.

2.4.3 Initial Configuration with Command Prompt

Configuration steps using command prompt are as follows:

1. Check the system settings with command '**status**'
2. Configuration required parameters:

(!) Before you set the parameters listed below, you must know what frequency and bandwidth you are allowed to use and at what power you are allowed to transmit.

- Tx power with the command '**radio txpower** [<power dBm>]';
 - Tx frequency with the command '**radio freq** [<freq KHz>]';
 - Channel bandwidth, modulation, FEC mode and channel mask with the command '**modem set** <bandwidth> <min modulation> <max modulation> <WeakFEC|StrongFEC> <channel mask>', where you can choose among 3.5-56 MHz values and modulations 4QAM – 256QAM;
 - Name of CFIP Phoenix with the command '**system name** <name>'. Default name is 'SAF';
 - IP address with the command '**net ip addr** <addr>', if it is necessary;
 - IP mask with the command '**net ip mask** <mask>', if it is necessary;
 - IP default gateway with the command '**net ip gw** <gw>', if it is necessary;
3. Save settings with the command '**cfg write**'; restarting with the command '**system reset**';
 4. Check the settings made, modem and radio status with the commands '**status**', '**modem status**' and '**radio status**' respectively.

2.5 LED indications

2.5.1 CFIP Phoenix IDU alarm LED indications

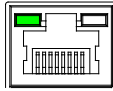
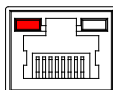
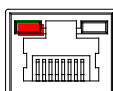
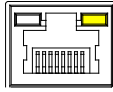
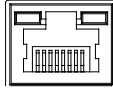
Below you can see table summarizing which alarms each of CFIP Phoenix IDU LEDs represents.

LED name	Description
ODU	Green – OK Yellow blinks – ODU Tx mute. Yellow – Rx level alarm; ODU Temperature failure; IDU PSU to ODU state alarm. Red – Tx PLL error alarm; Rx PLL error alarm; ODU RX LOS; ODU TX LOS; ODU RX failure; ODU TX failure; ODU Frequency failure. Red blinks – No data from ODU.
IDU	Green – OK Yellow – IDU temperature fault; Main supply 48V failure; IDU PSU state alarm; PSU temperature fault; Power supply voltage failure. Red blinks – No data from IDU temperature sensor; No data from main PSU IDU ADC; No data from main PSU ODU ADC; No data from PSU temperature sensor; No data from power supply ADC.
Modem	Green – OK Yellow – Radial MSE; LDPC decoder stress; RX carrier offset. Red – Acquire status alarm; Last acquire error status. Red blinks – No data from MODEM.
System	Green – OK after successful boot. Green blinks – System booting. Yellow - License expired. Yellow blinks - Invalid device license. Red – Boot failure or selftest failure.

2.5.2 Ethernet RJ-45 connector LED indications

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

2.5.3 E1 RJ-45 connector LED indications

E1 port LED (highlighted)	Color	Description
	 	Green (loop-back LED yellow or off) Indicates normal operation of the channel, no problems with signal reception.
	 	Red (loop-back LED yellow or off) Constant red indicates that E1 signal is lost. If red flashes momentarily, the bipolar violation (line code error) was received from user equipment.
	 	Blinking green and red (loop-back LED yellow or off) AIS signal is being received from user equipment.
	 	Yellow loop-back LED (loop-back switched on) When loopback LED is switched on, analog, digital or remote loop-back mode is active for that channel.
	 	No LED is lit Channel is switched off.

3 Status Window

The main window in the Web GUI is status window that shows all main system parameters, and, in case of failure or any other problems, it tints a specific parameter in red.

To have a better understanding on status window, we will go through every field.



SAF Name: SAF
IP: 192.168.205.10
SN: 323130101669
Uptime: 01:15:22
CFIP Phoenix IDU - v1.65.38
Logout

Status
Main status
Alarm status
Ethernet aggregation status
Diagnostics data
Configuration
Performance
Tools
Help

Local system summary
Rx level: -50 dBm
Rx modulation: 256QAM
Radial MSE: -31.3 dB
LDPC stress: 7.0e-05

Remote system summary
Rx level: -50 dBm
Rx modulation: 256QAM
Radial MSE: -31.4 dB
LDPC stress: 4.3e-05

Main status	Local	Remote
ODU status		
ODU data status	Ok	Ok
ODU side	Low	High
Tx mute	Off	Off
Tx power	0 dBm	0 dBm
ATPC	Disabled	Disabled
Rx level	-50 dBm	-50 dBm
Duplex shift	1010000 kHz	1010000 kHz
Tx frequency	17728000 kHz	17728000 kHz
Rx frequency	17728000 kHz	17728000 kHz
IDU configuration		
Configuration file	embedded->56_X_NWB_EIPv4d.bin	embedded->56_X_NWB_EIPv4d.bin
Bandwidth	56000 kHz ETSI	56000 kHz ETSI
Modulation	256QAM WeakFEC with ACM	256QAM WeakFEC with ACM
Total capacity / rate	362.860 Mbps with max ACM / Unlimited	362.860 Mbps with max ACM / Unlimited
Ethernet capacity / rate	362.860 Mbps with max ACM / Unlimited	362.860 Mbps with max ACM / Unlimited
E1 channels	0	0
IDU status		
IDU data status	Ok	Ok
IDU status	ACQUIRE_LOCKED	ACQUIRE_LOCKED
Radial MSE	-31.3 dB	-31.4 dB
LDPC decoder stress	6.4e-05	4.8e-05
ACM engine	On	On
Current modulation Rx / Tx	256QAM WeakFEC / 256QAM WeakFEC	256QAM WeakFEC / 256QAM WeakFEC
Current link capacity Rx / Tx	362.860 / 362.860 Mbps	362.860 / 362.860 Mbps
E1 status *	Ok	Ok
Diagnostics		
Diagnostics data status	Ok	Ok
IDU temperature	+56.5 °C / +133.7 °F	+57.5 °C / +135.5 °F
ODU temperature	+49.0 °C / +120.2 °F	+48.0 °C / +118.4 °F
Modem temperature	+70.0 °C / +158.0 °F	+66.0 °C / +150.8 °F
IDU input voltage	47.00 V	47.20 V
IDU input current	0.446 A	0.443 A
IDU power consumption	20.951 W	20.893 W
ODU PSU state	Ok	Ok
IDU output voltage to ODU	46.80 V	47.10 V
IDU output current to ODU	0.360 A	0.347 A
ODU power consumption	16.836 W	16.355 W
ODU cable attenuation	-2 dB	-2 dB
AUX alarm input	0000	0000
AUX alarm output	0000	0000
Tx polarization	N/A	N/A
Name (serial number)	SAF (323130101669)	SAF (383611101716)
License remaining time	N/A	N/A
Firmware version	v1.65.38	v1.65.38

Note: Fields marked with * are clickable.

Figure 3.1 "Main status" page

- Shows the name of this CFIP Phoenix, its IP address, serial number and uptime since the last restart. If uptime is displayed in red, the connection to CFIP management port was lost;
- Shows the firmware version this CFIP Phoenix is currently using;
- Logout button allows ending the current Web GUI management session and logging in as a different user if necessary. After pressing the button, you are automatically redirected to the login page;
- The tree of Web GUI sections;
- Shows short summary of the main operational parameters of local and remote system.

- Rx level (or RSL) at both ends must not differ significantly from the previously calculated value.
 - Modulation indicates which modulation mode is used. For better operation the same modulation must be set at both ends.
 - Radial MSE is explained below in the Chapter 3.1.1.
 - LDPC is explained below in the Chapter 3.1.2.
6. *ODU data status* – shows if management CPU was able to read data from radio;
 7. *ODU side* – shows the radio side of local and remote CFIP (command line – **radio side**);
 8. *Tx mute* – shows if transmitter is currently muted;
 9. *Tx power* – shows current transmitter power in dBm. Factory default setting is “Off” (command line - **radio status** or **status**);
 10. *ATPC* – shows if ATPC is enabled or disabled (command line – **atpc status**);
 11. *Rx level* – shows current level of received signal. It must not differ significantly from the previously calculated value (command line - **radio status** or **status**);
 12. *Duplex shift* – shows the margin between the transmitting and receiving frequencies (command line - **radio status**);
 13. *Tx frequency* – shows the transmitting frequency (command line - **radio status**);
 14. *Rx frequency* – shows the receiving frequency (command line - **radio status**);
 15. *Configuration file* – shows which configuration the modem is currently using. It should match on both sides of the link (command line – **modem configuration**);
 16. *Bandwidth* – shows width of currently utilized bandwidth in MHz (command line – **modem status** or **status**);
 17. *Modulation* – shows modulation mode set (command line – **modem status** or **status**);
 18. *Total capacity* – shows total capacity set (command line – **modem status**);
 19. *Ethernet capacity / rate* – shows Ethernet capacity set and rate limitation of Ethernet switch. If Ethernet rate is not limited “Unlimited” will be displayed after “/” symbol (command line – **modem status** or **status**);
 20. *E1 channels* – shows number of E1 channels set. The number must be equal at both ends (command line – **modem status** or **status**);
 21. *IDU data status* – shows if management CPU was able to read data from modem;
 22. *IDU status* – indicates the acquire status of the modem. ‘ACQUIRE_IN_PROGRESS’ will appear during start-up, when modem acquires required parameters, but in normal operation mode ‘ACQUIRE_LOCKED’ will be seen. Any other options designate failure (command line – **modem status** or **status**);
 23. *Radial MSE* – shows radial mean square error value. Refer to Chapter 3.1.1. for detailed description (command line - **modem status** or **status**);
 24. *LDPC decoder stress* – shows the load of LDPC (low-density parity-check code) decoder. Refer to Chapter 3.1.2. for detailed description (command line – **modem status** or **status**);
 25. *ACM engine* – shows if ACM (Adaptive Coding and Modulation) engine is enabled (command line – **modem status** or **status**);
 26. *Current modulation Rx / Tx* – shows the modulation modes currently utilized (command line – **modem status**);
 27. *Current link capacity Rx / Tx* – shows the current capacities in both directions (command line – **modem status**);
 28. *E1 status* – shows if the E1 channel is connected or not and shows status of LOS and AIS indications. To see the status, click on the text (command line – **e1 status**);
 29. *Diagnostics data status* – shows if system parameters are in acceptable margins (command line - **diagnostics**);

30. *IDU temperature* – shows the IDU internal temperature in degrees by Celsius and Fahrenheit (command line - **diagnostics** or **status**);
31. *ODU temperature* – shows the ODU internal temperature in degrees by Celsius and Fahrenheit (command line - **odu status**);
32. *Modem temperature* – shows the temperature on modem chip in degrees by Celsius and Fahrenheit (command line - **diagnostics**);
33. *IDU input voltage* – shows the input voltage of IDU PSU in volts (command line – **diagnostics psu status**);
34. *IDU input current* – shows the current of IDU PSU in amperes (command line – **diagnostics psu status**);
35. *IDU power consumption* – shows the amount of power consumed by IDU PSU in watts (command line – **diagnostics psu status**);
36. *ODU PSU state* – shows whether ODU PSU is operating (command line – **diagnostics psu status**);
37. *IDU output voltage to ODU* – shows the input voltage of ODU PSU in volts (command line – **diagnostics psu status**);
38. *IDU output current to ODU* – shows the current of ODU PSU in amperes (command line – **diagnostics psu status**);
39. *ODU power consumption* – shows the amount of power consumed by ODU PSU in watts (command line – **diagnostics psu status**);
40. *ODU cable attenuation* – shows attenuation on IDU-ODU cable (command line – **odu status**);
41. *AUX alarm input* – shows which inputs from four available are active (command line - **diagnostics**);
42. *AUX alarm output* – shows which outputs from four available are active (command line - **diagnostics**);
43. *Tx polarization* – shows transmission polarization and position of connectors and cables (command line - **diagnostics**);
44. *Name (serial number)* – shows system name and serial number (command line – **system name** and **system inventory**);
45. *License remaining time* – shows amount of time (in seconds) remaining for active time limited license (if applicable); in case of no license “N/A” is being shown; in case of unlimited time license “Unlimited” is being shown (command line – **license status**);
46. *Firmware version* – shows current firmware version. Make sure it is the same on both ends of the link (command line – **ver**).

3.1.1 Radial MSE

Radial MSE is a method for estimating the signal to noise ratio. ACM engine uses normalized MSE, which is the inverse of SNR. It is calculated by dividing the estimated MSE level with the energy of the received constellation. Radial MSE peak value threshold is dependent on modulation used and LDPC code rate.

If the Radial MSE value trespasses following thresholds, BER at the output of LDPC decoder will reach the value of $1.0 \cdot 10^{-6}$:

4QAM StrongFEC	16QAM StrongFEC	32QAM StrongFEC	64QAM StrongFEC	128QAM StrongFEC	256QAM StrongFEC	256QAM WeakFEC
- 8.5 dB	-13.8 dB	-16.0 dB	- 19.3 dB	-22.3 dB	-25.1 dB	-27.6 dB

3.1.2 LDPC

The **LDPC** is monitored for the number of errors being corrected on the input of LDPC decoder (see **Figure 3.2**).

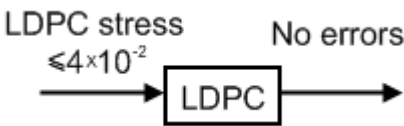


Figure 3.2 LDPC decoder structure

LDPC stress value thresholds @ BER $1.0 \cdot 10^{-6}$:

- for Strong FEC mode $\sim 4.0 \cdot 10^{-2}$;
- for Weak FEC mode $\sim 1.0 \cdot 10^{-2}$

As long as LDPC stress value is under the specified thresholds, the amount of errors (and BER itself) on the output of LDPC remains at zero level.

3.2 Alarm status

Table on “Alarm status” page summarizes current alarms by showing alarm group number, date and time the alarm occurred and its name.

Alarm status			
Alarm gr.	Date	Time	Alarm
51	2014-06-18	10:21:20	Ethernet interface - Ports[P1(LAN)P3(LAN)P4(LAN)] Link[Off]

Figure 3.3 Alarm status

Full list of alarms is available in “Alarm configuration” page where it is possible to disable alarm if necessary. For further details please refer to Chapter 5.1.

3.3 Ethernet aggregation status

Ethernet aggregation status page shows summary of current n+0 aggregation status if such is enabled. In case of no configuration “Ethernet aggregation is disabled” will be shown.

Ethernet aggregation status	
1 Clear max N/D time	
Local Master device Nr. 1 Aggregation status	
ID	#010
Status	2+0
Mode	Aggregation
Role	Master
State	2 Active
Previous state	3 Start
Max N/D time	4 0.00 of 0.60 sec
	5 Alarms
None	
Local Slave device Nr. 2 Aggregation status	
ID	#020
Mode	Aggregation
Role	Slave
State	Active
Previous state	Active Slave
Max N/D time	0.17 of 0.60 sec
	Alarms
None	
Remote Master device Nr. 1 Aggregation status	
ID	#010
Status	2+0
Mode	Aggregation
Role	Master
State	Active
Previous state	Start
Max N/D time	0.70 of 0.60 sec
	Alarms
None	

Figure 3.4 Ethernet aggregation/protection status

1. Clear max N/D time – clear maximum no data time;
2. State – displays current device state status – Active or Standby;
3. Previous state – displays previous device state status;
4. Max N/D time: - displays maximum disconnection time between devices;
5. Alarms - displays alarm notifications:
 - Local modem Airloss – there is no radio connection between local and remote device
 - LAN1-4 link down – media is disconnected;
 - No data from device Nr.1-4 – media is connected but not receiving aggregation information from aggregated device;
 - No data from remote device – local device is not receiving aggregation information from remote device.

3.4 Diagnostics data

“Diagnostics data” page summarizes system inventory and troubleshooting information.

Diagnostics data	
Inventory information	1
ODU Product Code: S18RFU05LA	
ODU Serial Nr: 360320100183	
ODU RFVER: RMBVER: 5 SWVER: 2.18	
IDU Product Code: S0GIPN01	
IDU Serial Nr: 323130101669	
IDU Detected PCB: SOBMB001_R06	
MAIN ID: 1.4 HWVER: 6.0 SWVER: 1.65 SN: 142341401735 Name: SOMMB001 Features: 0.0	
PSU ID: 2.2 HWVER: 1.0 SWVER: 0.0 SN: 242441601182 Name: SOMPSB01 Features: 0.0	
Download of diagnostics files	
Download system information	2
Download alarm log file	3
Download pm log 1 minute interval	4
Download pm log 15 minute interval	5
Download pm log 60 minute interval	6

Figure 3.5 Diagnostics data

1. *Inventory information* - displays the CFIP Phoenix IDU and ODU product code, serial number and additional hardware information;
2. *Download system information* - allows saving system information (output from “full system information page”) in separate txt file on your hard disk drive. Same functionality is available in “Configuration→System configuration→Service information→Download system information” (Chapter 4.4.6);
3. *Download alarm log file* - allows saving alarm log file in separate txt file on your hard disk drive. Same functionality is available in “Performance→Alarm log→>Alarm-event log file<” (Chapter 5.1.4);
4. *Download pm log 1 minute interval* - allows saving performance log file for 1 minute intervals in separate txt file on your hard disk drive. Same functionality is available in “Performance→Performance log→Performance log file download: 1 min interval” (Chapter 5.2.3);
5. *Download pm log 15 minute interval* - allows saving performance log file for 15 minutes intervals in separate txt file on your hard disk drive. Same functionality is available in “Performance→Performance log→Performance log file download: 15 min interval” (Chapter 5.2.3);
6. *Download pm log 60 minute interval* - allows saving performance log file for 60 minutes intervals in separate txt file on your hard disk drive. Same functionality is available in “Performance→Performance log→Performance log file download: 60 min interval” (Chapter 5.2.3).

4 Detailed Configuration in Web Graphic User Interface

Configuration section in Web interface allows customizing your system to suit your specific needs.

4.1 ODU Configuration

The ODU configuration window provides the configuration of CFIP Phoenix radio part parameters. Below is a short explanation of provided customization fields.

4.1.1 Radio Configuration

ODU configuration	
Radio configuration	
ODU data status	1 Ok
Radio side	2 Low
Tx power (0 .. 12 dBm)	3 0 dBm
Tx frequency (17728000 .. 18195000 kHz)	4 17728000 kHz
Rx frequency	5 18738000 kHz
Duplex shift	6 1010000 kHz
Tx mute	7 off sec
8 Rollback on ☐ Execute configuration	
9 Execute for both	

Figure 4.1 Radio configuration

1. *ODU data status* – shows if management CPU was able to read data from the radio;
2. *Radio side* – shows if radio side you are currently viewing is low or high (command line – **radio side**);
3. *Tx power* – allows you to define transmitter power. If the RSL is too high (much higher than normal -50dBm), you might want to lower transmitter power. Too high Rx level (> -20 dBm) may even result in synchronization loss. The minimum and maximal values you can choose are dependent on modulation type and CFIP model. Maximal and minimal Tx power values are shown in the brackets. (command line - **radio txpower** [<power dBm>]);
4. *Tx frequency* – allows you to enter preferable transmitter frequency, hence defining utilized channel (command line - **radio txfreq** [<freq KHz>]);
5. *Rx frequency* – shows the current receiver utilized frequency (command line - **radio freq**);
6. *Duplex shift* – shows the duplex shift between the transmitter frequency and receiver frequency (command line - **radio duplexshift**);
7. *Tx mute* – allows turning transmitter power off. It may be effective when diagnosing on interference existence – when transmitter power of one side is off, you should not experience significant RSL on the other side (command line - **radio txmute** [on/off]);
8. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.
9. Pressing “Execute for both” applies changes made to the corresponding section both for local and remote side CFIP Phoenix.

4.1.2 ATPC Configuration

To configure ATPC, it is necessary to set Rx (remote) “min” and “max” values and enable the ATPC feature.

ATPC update period and ATPC delta are recommended to be left unchanged.

It is also possible to change the limit of Tx power correction.

(!) Note, that ATPC is mechanism for reducing Tx power, that's why to make proper use of ATPC, transmitter power (Tx power) must be set to the maximum value.

ATPC configuration	
ATPC function	1 ☐ Enabled ☒ Disabled
ATPC update period (1..5)	2 1 sec
Tx power correction	3 0 dB
Tx power correction limit (-12..0 dB)	4 0 dB
Remote device status	5 Ok
Rx (remote) level (-90..-20 dBm)	6 -55 dBm -50 dBm
Difference between Rx min and Rx max must be at least 3 dBm	
Rx (remote) level	7 -39 dBm
8	Rollback on ☐ Execute configuration
9	Execute for both
10	Write to config file
11	Write to config file for both
System returned:	12 Ok

Figure 4.2 ATPC configuration

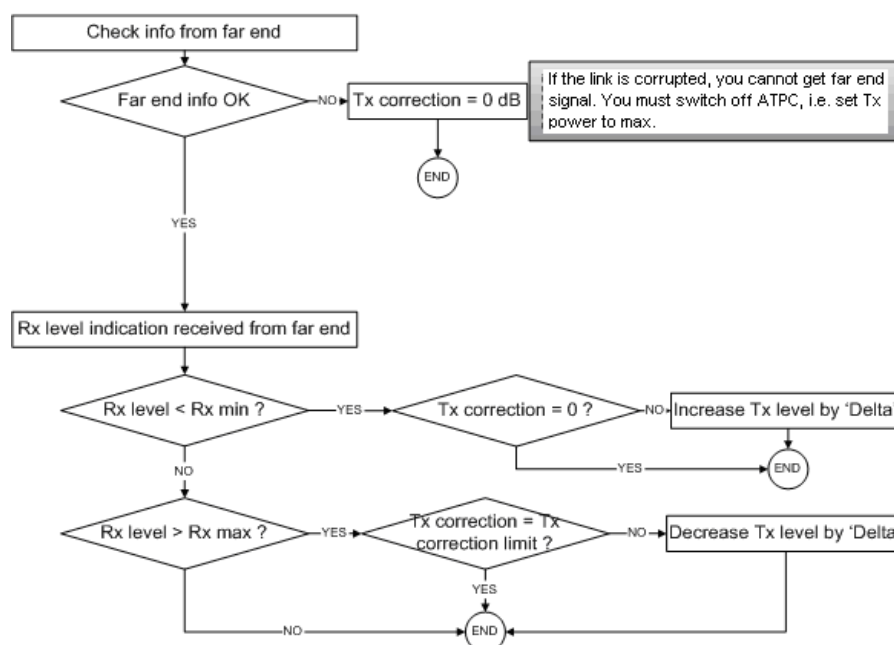
1. *ATPC function* – allows enabling or disabling ATPC (Automatic Transmit Power Control). By default this feature is disabled (command line – **atpc [enable/disable]**);
2. *ATPC update period (1..5)* – allows defining the period in seconds in which ATPC parameters are being updated. By default the update period is 1 second (command line – **atpc delay <power change delay time 1..5 sec>**);
3. *Tx power correction* – displays the amount of transmitter power in decibels ATPC has currently corrected (command line – **atpc status**);
4. *Tx power correction limit* – allows defining the amount of dB ATPC will be able to correct regarding initial Tx power value (command line – **atpc limit <tx power correction limit>**);
5. *Remote device status* – shows if management CPU was able to read data from remote management CPU;
6. *Rx (remote) level (-90..-20 dBm)* – allows defining the maximum and minimum Rx level. ATPC Tx power correction will be performed only in case of exceeding these defined thresholds Rx level (command line – **atpc rxminmax <rxmin> <rxmax>**);
7. *Rx (remote) level* – shows current Rx level of remote end (command line – **atpc status**);
8. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If “Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.
9. Pressing “Execute for both” applies changes made to the corresponding section both for local and remote side CFIP Phoenix.
10. Pressing “Write to config file” saves all the changes made on the whole page (command line – **cfg write**);
11. Pressing “Write to config file for both” saves all the changes made on the whole page for both ends of the link simultaneously (command line – **cfg write**);
12. *System returned* - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says “Ok”.

ATPC Algorithm

ACM can be implemented together with **automatic transmit power control (ATPC)**, complimentary features that enhance overall system performance. ATPC reduces the average transmitted power as well as CCI and adjacent-channel interference (ACI), which is caused by extraneous power from a signal in an adjacent channel. It also enables a more efficient and cost-effective network frequency plan and deployment, as well as eliminating some of the receivers' "upfade" problems by changing the transmitted power according to the link momentary conditions. The lower average Tx power also extends the equipment's mean time between failures.

ATPC can be used together with ACM to control the transmitted power in any given ACM profile. Different algorithms can be implemented to achieve maximal spectral efficiency or minimal transmitted power using both features in combination. One implementation could target maximal spectral efficacy by trying to reach the highest ACM profile, while the other is willing to compromise on some of the spectral efficiency enabling CCI and ACI reduction. In any chosen algorithm, ATPC reduces the average transmitted power, benefiting each ACM profile and any link condition.

The local CFIP Phoenix receives information (each second) about Rx level from the far-end CFIP Phoenix through the service channel; depending on the received Rx level parameter, the local CFIP Phoenix adjusts the transmitter power in accordance with the algorithm shown below.



Rx level - the Rx level figure received from the far-end
 Rx max - maximum permissible Rx level at the far-end
 Rx min - minimum permissible Rx level at the far-end
 Tx correction
 Tx correction limit
 Delta - the value by which the Tx power is increased or decreased
 according to far-end Rx level indication (1 dBm by default)

Figure 4.3 ATPC algorithm

4.2 IDU Configuration

4.2.1 Modem Configuration

Modem configuration	
Modem data status	1 Ok
Modem standard	2 ETSI ▼
Bandwidth	3 56000 ▼ kHz
Modulation	4 256QAM WeakFEC ▼
E1 channels	5 ☐ 01 ☐ 02 ☐ 03 ☐ 04 ☐ 05 ☐ 06 ☐ 07 ☐ 08 ☐ 09 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16 ☐ 17 ☐ 18 ☐ 19 ☐ 20 ☐ Select/Deselect
6 Rollback on ☐ Execute configuration	
7 Execute for both	

Figure 4.4 Modem configuration

1. *Modem data status* – shows if management CPU was able to read data from modem;
2. *Modem standard* – allows switching between ETSI and ANSI (FCC) standards, changing available bandwidths to 3.5/7/14/28/40/56 MHz and 5/10/20/30/40/50 MHz and changing between E1 and T1 channels respectively (command line – **modem standard** <ETSI/ANSI>);
3. *Bandwidth* – allows choosing between 3.5 and 56 MHz bandwidths available. The default value is 3.5 MHz. The wider bandwidth you have, the higher will be the overall link bitrate. The maximum bitrate of 363 Mbps is available using 56 MHz bandwidth (command line – **modem set** <bandwidth> <min_modulation> <max_modulation> <strongFEC/weakFEC> <channel mask>);
4. *Modulation* – allows choosing between 256QAM, 128QAM, 64QAM, 32QAM, 16QAM and 4QAM modulations. The default value is 4QAM. The higher is the modulation order, the higher is the overall link bitrate, but worse RSL threshold. The maximum bitrate of 363 Mbps is available using 256QAM modulation (command line – **modem set** <bandwidth> <min_modulation> <max_modulation> <strongFEC/weakFEC> <channel mask>). See below the explanation for **Adaptive Coding** and **Modulation** and **FEC** modes;
5. *E1 channels* – allows to choose preferable E1 channels to be used. Each E1 channel activated detracts 2.048Mbps from Ethernet capacity. By default E1 channels are turned off (command line – **modem set** <bandwidth> <min_modulation> <max_modulation> <strongFEC/weakFEC> <channel mask>). In order to switch to T1 channels, modem standard needs to be changed to ANSI (FCC);
6. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.
7. Pressing “Execute for both” applies changes made to the corresponding section both for local and remote side CFIP Phoenix link.

Adaptive code and modulation (ACM) technology allows operators to achieve high-capacity data transmission over microwave links and improve the link utilization. This reduces both operational and capital expenditures for maintaining high-capacity links. ACM can maintain the highest link spectral efficiency possible at any given time in any link condition.

In traditional voice-dominated wireless backhaul transmission networks, service availability levels of 99.995% are the norm.

However, newer services such as Internet browsing, video streaming and video conferencing can operate at more relaxed availability levels. With use of QoS prioritizing ACM can allocate the required

availability based on the priority. As a result, high-priority services such as voice enjoy 99.995% availability, while low-priority services like video streaming are allocated lower priorities.

Use of QoS prioritizing defines which services should be transmitted under any link condition and which services should be adapted whenever the link condition is degraded and the link payload is decreased.

For example, when bad weather has decreased the channel capacity of a link, ACM maintains high-priority services – such as voice data – with full bandwidth capacity while adapting the bandwidth capacity of low- and mid-priority services such as Internet browsing (see **Figure 4.5**).

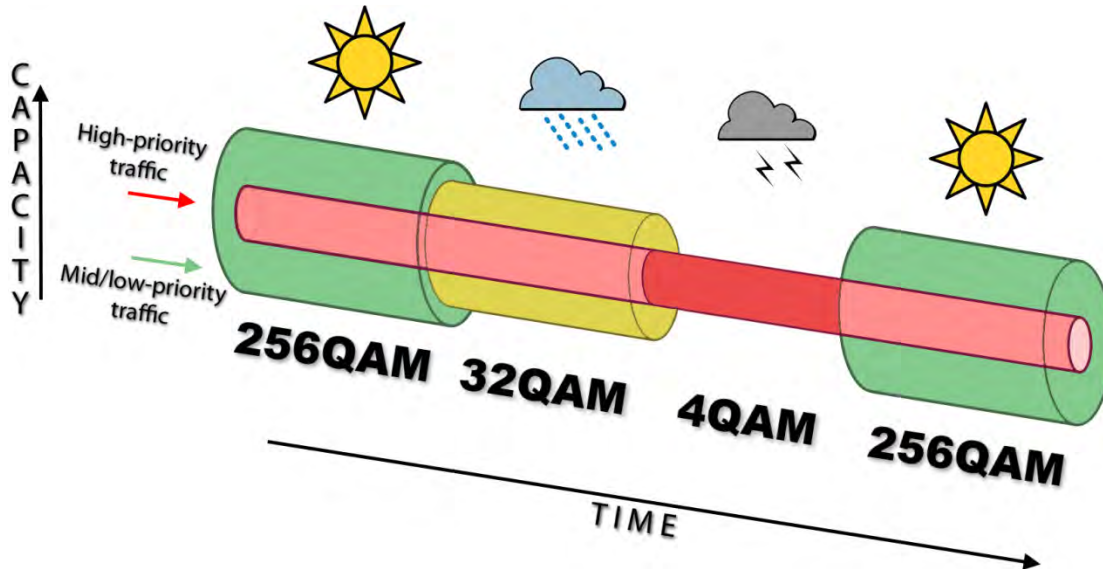


Figure 4.5 ACM bandwidth capacity adaptation

Full modulation range: 256QAM, 128QAM, 64QAM, 32QAM, 16QAM, 4QAM

Traffic can be mapped into different priorities, which define the level of service for each application. **Figure 4.6** illustrates how different services – such as rich voice and video – are mapped into different classes of availability (CoA) such as 99.995% or 99.687%.

The implementation of multiple priorities increases the available capacity up to 10 times that of standard links. When conditions are clear, the wireless link operates at maximum capacity and provides all services with the full data rate. When link conditions are poor – during harsh rain, for example – predefined high-availability services such as voice are not affected. However, the capacity of low-priority services is adapted dynamically to the changing link conditions. This is done by provisioning bandwidth according to the link conditions and traffic priority.

An ACM profile defines the link parameters (modulation) for a given range of the Radial MSE. The Radial MSE range of each profile defines the threshold for switching from one ACM profile to another. Each ACM profile has a different spectral efficiency, derived from its modulation.

The receiver continuously monitors the link condition based on Radial MSE value.

Once the estimators at the receiver side show that the link performance is not suitable for the current ACM profile, an ACM switching process will be initiated. In case of degradation in the link performance, the new ACM profile will include lower modulation, decreasing the link bitrate. The ACM switching rate is measured in dB/s and is a key feature of ACM systems.

In general, the higher the switching rate, the better the system's immunity to rapid Radial MSE changes. When the switching is being executed, the payload rate is being modified to fit the aggregated data rate to the new available link data rate.

Alternatively, ACM can also be used to increase the link distance, resulting in added link spectral efficiency. The same concept is implemented as previously, with the margins that were kept for 99.995-percent bandwidth availability now used to increase the link distance. Whenever the link conditions are degraded, the system will switch to an ACM profile with lower spectral efficiency to enable maintaining the link.

The following real-world example illustrates the benefits of ACM. Consider a CFIP link operating at 23 GHz with 56 MHz channel spacing and 45.9 dBi (120 cm) antenna gain. The link is operating in a moderate rain region similar to central Europe with a distance of 15 kilometers.

The system operation is set to a minimal payload of 69 Mbps Ethernet for 99.995% availability.

Most of the time system would support 363Mbps Ethernet connection instead of a 69 Mbps connection. The system automatically monitors the link conditions and changes the capacity without interrupting the data transmission (hitless changes), as shown in **Figure 4.6**.



Figure 4.6 Link availability and classes of services

In comparison similar system using 256QAM and providing similar capacity would provide only 99,687% of availability. Besides, lack of ACM would not provide higher availability. You would have to decrease the distance, decrease modulation or increase antenna sizes to achieve 99,995% availability for the given link.

This example demonstrates how the new technology, based on an ACM mechanism, can play a key role in the development of cost-effective next-generation wireless access networks, by taking advantage of traffic evolution from synchronous TDM traffic to packet IP-based traffic.

The **FEC** mode (Weak or Strong) allows increasing overall capacity of the link in terms of deteriorating RSL sensitivity threshold.

For more details refer to table in Chapter 1.5.

4.2.2 Loopback Configuration

Loopback tests are accessible using local or remote management methods.

For safety purposes all loopbacks (local and remote) can be set on a fixed time interval only. If no time interval is specified, the default value is 60 seconds (1 minute).

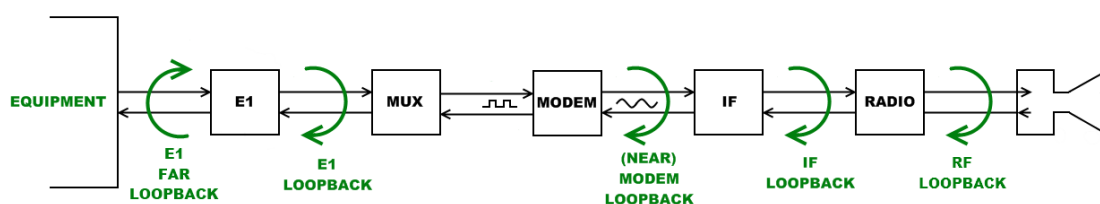


Figure 4.7 Loopback modes

- **E1** and **E1 FAR** loopback modes loop signal back to local end and to remote end respectively in bounds of E1 interface. E1 loopback mode must be set on the particular channel you need to test. If no E1 channels are selected, E1 loopback mode is not available. E1 loopbacks are named “interface” and “interface far” in “Loopback name” dropdown menu.
- **MODEM** loopback mode loops signal back to local end after the modem.
- **IF** loopback mode loops signal back to local end by linking intermediate frequencies.

Figure 4.8 Loopback configuration

1. *Loopback name* – allows choosing loopback mode (command line – **loopback** {status | none | if | modem | e1 <num> [far] | e1 mask <mask> [far]} [<time>]);
2. *Loopback timeout* – allows specifying activity time of chosen loopback mode in seconds (command line – **loopback** {status | none | if | modem | e1 <num> [far] | e1 mask <mask> [far]} [<time>]);
3. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.
4. Pressing “Write to config file” saves all changes made in the whole page (command line – **cfg write**);
5. Pressing “Write to config file for both” saves all changes made in the whole page for both sides of the link simultaneously (command line – **cfg write**);
6. *System returned* - in case of error or incorrectly entered parameter value, or other problems in the whole page – info message will be displayed here. Otherwise it says “Ok”.

Additional radio and modem configuration commands in Telnet/serial interface	
Command	Description
modem status	Shows all the modem parameters.
modem configuration show	Displays current configuration file.
modem configuration <file>	Uses separate configuration file.
modem configuration embedded	Switches back to the embedded configuration last used.
modem factory [max]	Resets modem settings to factory defaults (minimum bandwidth, minimum modulation). ‘max’ option will set maximum configuration (maximum bandwidth, maximum modulation + ACM).
modem ipremote [on off]	Allows enabling manual remote IP specifying (<i>modem ipremote off</i>). By default remote IP is being obtained automatically (<i>modem ipremote on</i>).
modem standard [etsi ansi]	Allows switching between ETSI and ANSI (FCC) standards, allowing to utilize E1 channels or T1 channels respectively.
modem counters [show clear]	Shows modem performance counters according to G.826 standard.
radio factory [max]	Resets radio settings to factory defaults. By default Tx power will be turned off. ‘max’ option will switch Tx power to the maximum value after restart.
radio duplexshift [<DS KHz>]	Allows switching to different duplexshift if supported.
radio side [L H]	Allows switching radio side if supported.

4.3 Protection configuration

This section describes 1+1 protection implementation for Phoenix IDU. The possible 1+1 configuration modes are Frequency diversity (FD), Hot Standby (HSB) and Space diversity (SD).

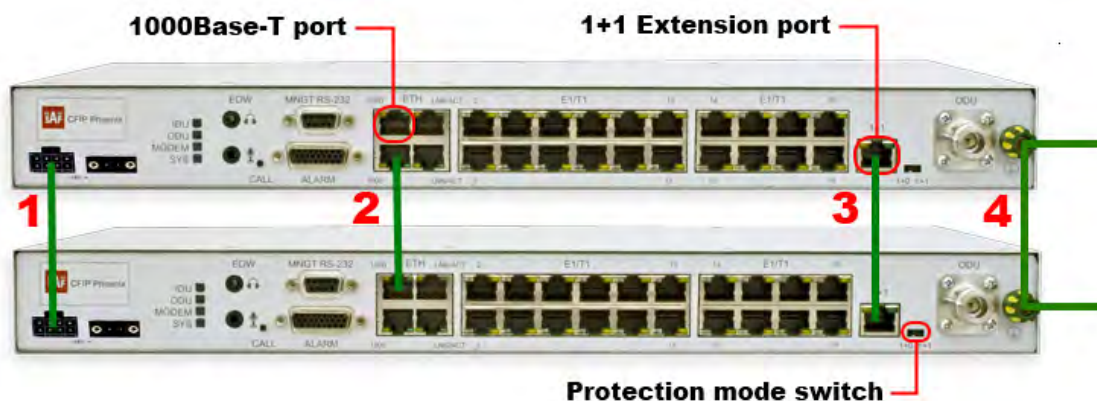


Figure 4.9 1+1 interconnection of two CFIP Phoenix IDUs (with power protection ports – P/N SOGIPT11)

For 1+1 operation two CFIP Phoenix IDUs (“working” and “protection”) **before power is supplied** should be interconnected as shown in **Figure 4.9** - via one of the 1000Base-T user data and management Ethernet switch ports with Ethernet cable (IOACPP02); modems should be interconnected via special extension port for 1+1 protection with protection cable CAT6 (P/N SOACPP1); grounding screws should be interconnected with grounding cable and connected to ground circuit; power protection ports (if available) should be interconnected with power protection cable (P/N SOACPR11).

(!) Power protection connector for power redundancy is optional and is available only for CFIP Phoenix IDU P/N SOGIP*11.

(!) For proper 1+1 operation 2 IDU's are required on each side of the link.

4.3.1 Frequency Diversity (FD) protection mode

For FD mode performance two links differentiated by frequencies are working in parallel. Each link uses different frequency pair. One of the links is marked as ‘working’ and the other one as ‘protection’ link. At transmitter side the data is duplicated and transmitted in both links. At receiver side data is received from both transmitters. The decoder of working link then selects the preferred received data.

Setup for 1+1 Frequency Diversity (FD) mode

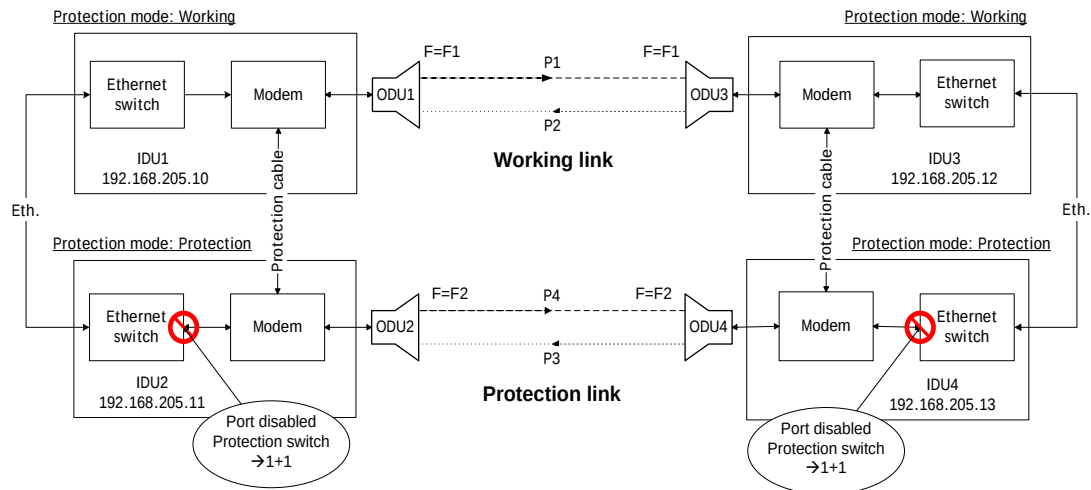


Figure 4.10 CFIP Phoenix FD mode

1. Connect each IDU to appropriate ODU. Note that High ODUs should be at one site and Low ODUs at remote site.
2. IDU pairs must be interconnected as shown in **Figure 4.9**.
3. **Before power is supplied to equipment:**
 - both IDUs on each side of the link should be grounded;
 - switches of IDUs must be set to correct state. For working link protection mode switch on CFIP Phoenix IDU front panel should be set to "1+0" position and for protection link protection switch should be to "1+1" position as shown in **Figure 4.10**.
4. Choose different frequencies for 'working' and 'protection' links as shown in **Figure 4.10**: F1 and F2.
5. Supply the IDUs with power and proceed with configuration.

Configuration of 1+1 Frequency Diversity (FD) mode

It is possible to perform configuration in Web GUI or through CLI (serial or telnet connection). For detailed description of commands necessary for 1+1 configuration refer to Chapter 4.3.5.

For 1+1 FD mode it is necessary to:

- Assign different IP addresses for each IDU. Note that IP addresses should be within the same subnet;
- Set different frequency pairs for working and protection links as shown in **Figure 4.10**: F1 and F2;
- Set appropriate state (working/protection) for each IDU;
- Disable automatic remote IP address identification (set by default) in "Tools→Command line" with command "modem ipremote off" and set appropriate remote site IP address for each IDU in "Configuration→IP configuration": "Remote IP address" for local working IDU is "IP address" of remote working IDU and "Remote IP address" for local protection IDU is "IP address" of remote protection IDU.

Example of configuration for FD mode:

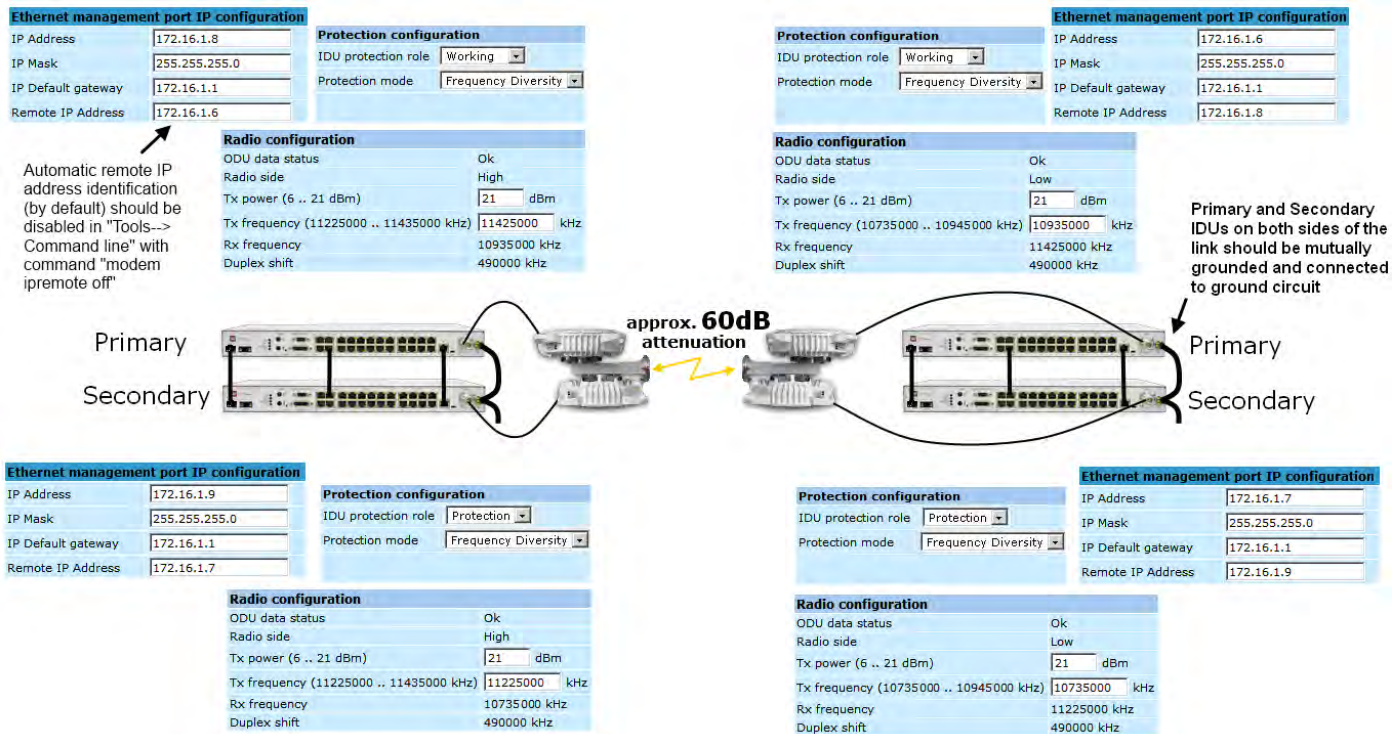


Figure 4.11 CFIP Phoenix configuration for 1+1 FD mode

Please refer to Chapter 4.3.5 for details of 1+1 configuration parameters and configuration possibilities via CLI. After successful 1+1 FD configuration, the screen of 'Protection configuration' in Web GUI should look as follows:

Protection configuration				
Protection status				
Value	Local	Local alternate	Remote	Remote alternate
Status	Working	Protection	Working	Protection
Mode	Frequency Diversity	Frequency Diversity	Frequency Diversity	Frequency Diversity

Figure 4.12 Protection configuration window after successful FD configuration

4.3.2 Hot Standby (HSB) and Space Diversity (SD) protection modes

For HSB and SD mode two transmitters are operating at the same frequency. One of the transmitters is in operation 'Active' while the other one is in 'Standby' mode (Tx power is muted). The data is duplicated at the transmitter side of the working link and sent towards receivers of both links (working and protection). The decoder of working unit selects the preferred link.

Setup for 1+1 Hot Standby (HSB) and Space Diversity (SD) protection modes

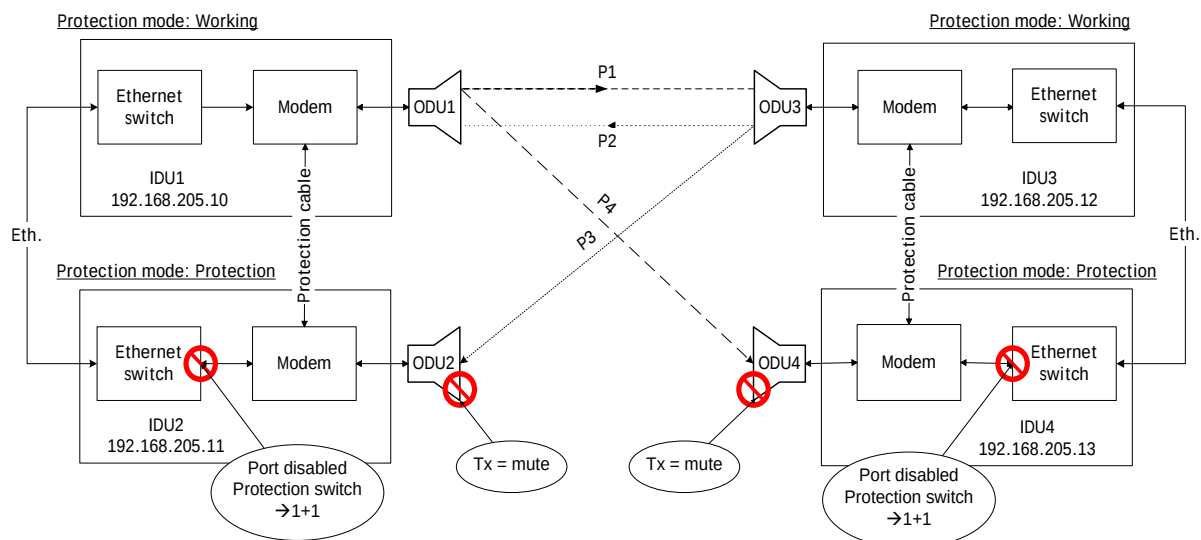


Figure 4.13 CFIP Phoenix HSB mode

1. Connect each IDU to appropriate ODU. Note that High ODUs should be at one side and Low ODUs at remote side. Note that for HSB mode ODUs should be interconnected through coupler at each site.
2. IDU pairs must be connected as shown in **Figure 4.9**. Note that switches of IDU pair ('working' and 'protection') are connected through one of the 1000Base-T user data and management ports via Ethernet cable, and modems are connected through special extension port for 1+1 protection via protection cable CAT6 (available from SAF Tehnika P/N S0ACPP1).
3. Choose same frequencies for 'working' and 'protection' links.
4. **Before power is supplied to equipment:**
 - both IDUs on each side of the link should be grounded;
 - switches of IDUs must be set to correct state. For working link protection mode switch on CFIP Phoenix IDU front panel should be set to "1+0" position and for protection link protection switch should be to "1+1" position as shown in **Figure 4.13**;
 - power protection ports of appropriate units should be interconnected (if available).
5. Supply the IDUs with power and proceed with configuration.

Configuration for 1+1 Hot Standby Mode

It is possible to perform configuration in Web GUI or through CLI (serial or telnet connection). For detailed description of commands necessary for 1+1 configuration refer to Chapter 4.3.5.

For 1+1 HSB mode it is necessary to:

- Assign different IP addresses for each IDU. Note that IP addresses should be within the same subnet;
- Set the same frequency pair for working and protection links;
- Set appropriate state (working/protection) for each IDU;
- Disable automatic remote IP address identification (set by default) in "Tools→Command line" with command "modem ipremote off" and set appropriate remote site IP address for each IDU in "Configuration→IP configuration": "Remote IP address" for local working IDU is "IP address" of remote working IDU and "Remote IP address" for local protection IDU is "IP address" of remote protection IDU;
- It is recommended that 'Standby' and 'Activetry' times remain default. IDU will remain in appropriate state during forcing it to another state for this specified time.

Example of configuration for HSB mode:

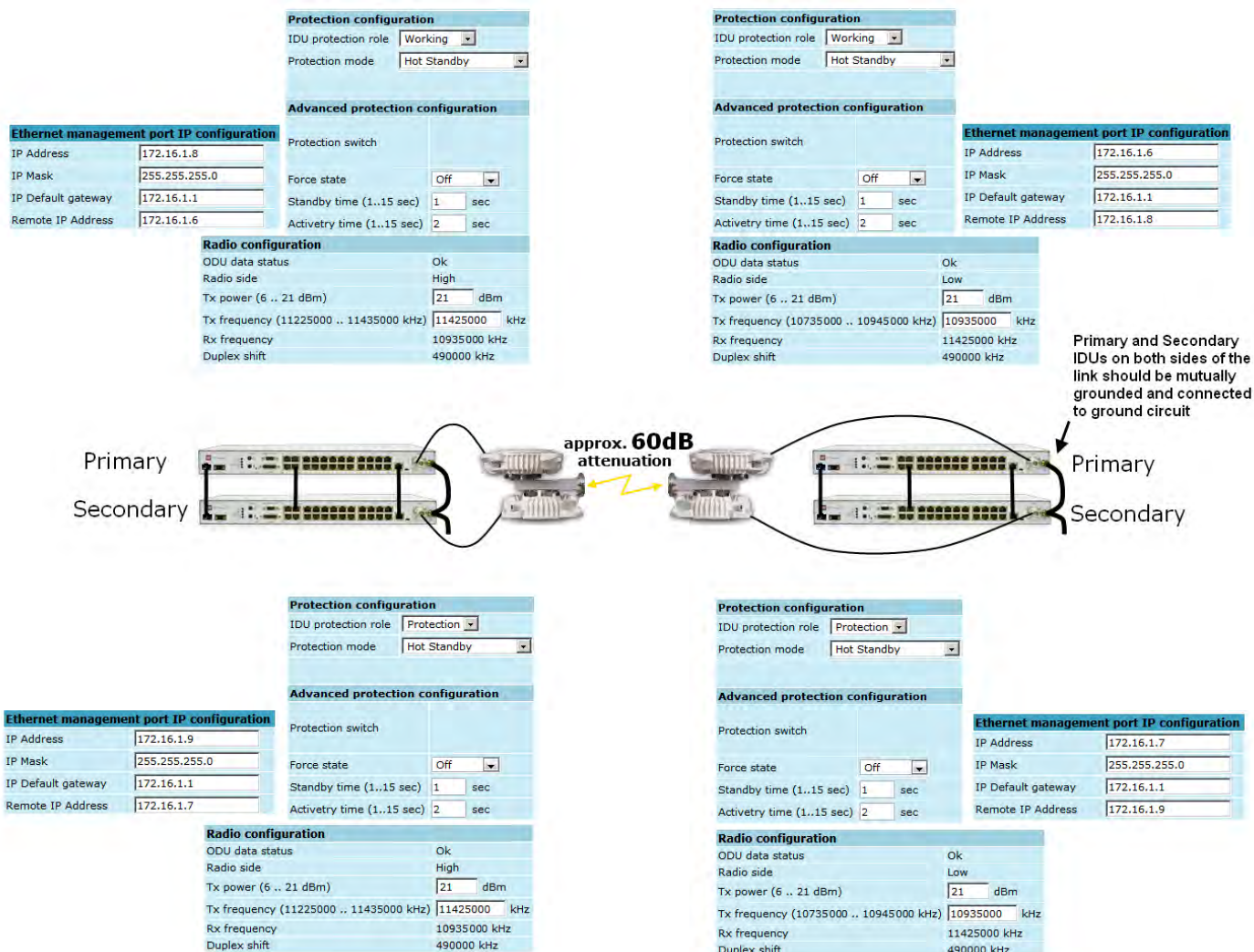


Figure 4.14 CFIP Phoenix configuration for 1+1 HSB mode

After successful 1+1 HSB configuration, the screen of 'Protection configuration' in Web GUI should look as follows:

Protection status				
Value	Local	Local alternate	Remote	Remote alternate
Status	Working	Protection	Working	Protection
Mode	Hot Standby	Hot Standby	Hot Standby	Hot Standby
State	Standby	Active	Active	Standby
Previous state	Active	Active Try	Active Try	Active

Figure 4.15 Protection configuration window after successful HSB configuration

Configuration for 1+1 Space Diversity Mode

For 1+1 SD mode it is necessary to:

- Assign different IP addresses for each IDU. Note that IP addresses should have the same subnet;
- Set the same Tx frequency pair for working and protection link;
- Set appropriate state (working/protection) for each IDU;
- Disable automatic remote IP address identification (set by default) in "Tools→Command line" with command "modem ipremote off" and set appropriate remote site IP address for each IDU in "Configuration→IP configuration": "Remote IP address" for local working IDU is "IP address" of remote working IDU and "Remote IP address" for local protection IDU is "IP address" of remote protection IDU;

- It is recommended that 'Standby' and 'Activetry' times remain default. IDU will remain in appropriate state during forcing it to another state for this specified time.

Example of configuration for SD mode:

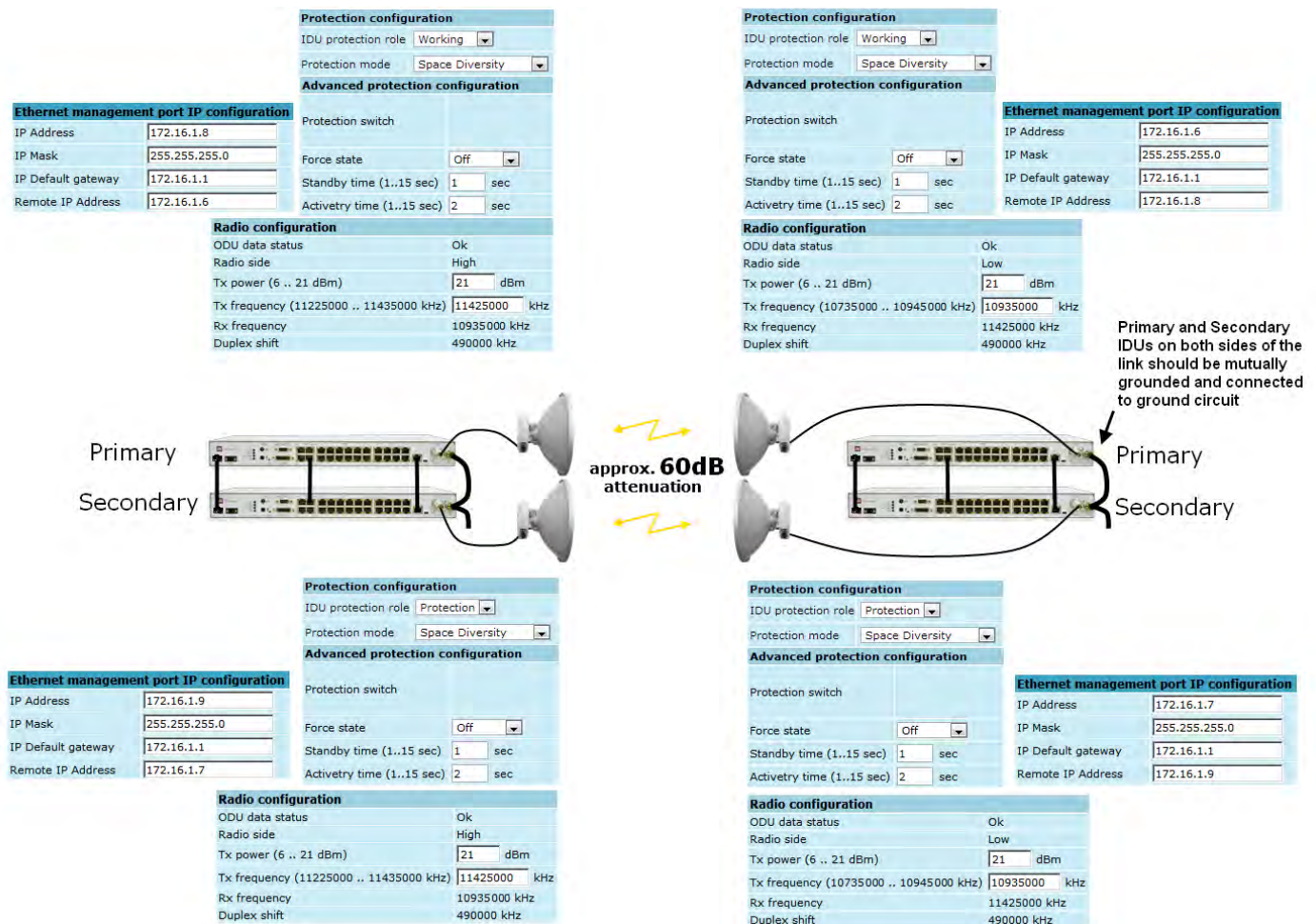


Figure 4.16 CFIP Phoenix configuration for 1+1 SD mode

The same commands can be executed using Web GUI. Please refer to Chapter 4.3.5 for details. After successful 1+1 SD configuration, the screen of 'Protection configuration' in Web GUI should look as follows:

Protection status				
Value	Local	Local alternate	Remote	Remote alternate
Status	Working	Protection	Working	Protection
Mode	Space Diversity	Space Diversity	Space Diversity	Space Diversity
State	Active	Standby	Active	Standby
Previous state	Start	Start	Start	Start

Figure 4.17 Protection configuration window after successful SD configuration

The following subsections are giving detailed description of Web GUI Protection configuration window.

4.3.3 Protection Status

You will see the following Protection Status window when 1+1 mode is disabled:

Protection status				
Value	1 Local	Local alternate	Remote	Remote alternate
Protection status	2 Protection disabled	N/A	N/A	N/A

Figure 4.18 Protection status while 1+1 is disabled

1. *Value* – denotes the names of CFIP Phoenix units in 1+1 configuration. ‘Local’ and ‘Local alternate’ designates both units (working and protection) at the local side and ‘Remote’ and ‘Remote alternate’ designates both units of remote side.
2. *Protection status* – denotes that CFIP Phoenix 1+1 protection is disabled.

In case 1+1 Hot Standby mode is enabled the Protection Status window might look as follows:

Protection status					
Value		Local	Local alternate	Remote	Remote alternate
Status	1	Working	Protection	Working	Protection
Mode	2	Hot Standby	Hot Standby	Hot Standby	Hot Standby
State	3	Standby	Active	Active	Standby
Previous state	4	Active	Active Try	Active Try	Active

Figure 4.19 Protection status while 1+1 is enabled

1. *Status* – for enabled 1+1 protection mode designates the status of each CFIP Phoenix unit in 1+1 protection mode. ‘Working’ denotes that particular unit is used for main working link and ‘Protection’ designates that particular unit is used for protection purpose.
2. *Mode* – specifies the 1+1 protection mode. Possible modes are ‘Hot Standby’ or ‘Frequency Standby’
3. *State* – designates the state of each unit specifically for Hot Standby mode. ‘Active’ designates that CFIP Phoenix unit is active part of 1+1 Hot Standby mode and ‘Standby’ state denotes that unit is on standby.
4. *Previous state* – denotes the previous state of each CFIP Phoenix unit in 1+1 protection mode

4.3.4 Protection Configuration

Protection configuration		
IDU protection role	1	Working
Protection mode	2	Hot Standby
	3	Rollback on ☐ Execute configuration

Figure 4.20 Protection configuration

1. *IDU protection role* – allows specifying the protection role of CFIP Phoenix IDU from drop-down menu. Available roles are ‘Working’, ‘Protection’ or ‘Disable’ that allows disable the protection role of IDU (command line – **prot set {hsb/fd} {working/protection/disable} [independent]**);
2. *Protection mode* – gives the possibility to choose ‘Hot Standby’ or ‘Frequency Diversity’ protection mode from the drop-down menu (command line – **prot set {hsb/fd} {working/protection/disable} [independent]**);
3. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.

4.3.5 Advanced Protection Configuration

The following section will appear in Web GUI only if protection is enabled for 1+1 Hot Standby mode.

Advanced protection configuration	
Protection switch	1 Active Standby
Force state	2 Off
Standby time (1..15 sec)	3 1 sec
Activetry time (1..15 sec)	4 2 sec
5 Rollback on ☐ Execute configuration	
6 Write to config file	
System returned:	7 Ok

Figure 4.21 Advanced protection configuration

1. **Protection switch** – temporarily switches IDU to active or standby state (command line – **prot {active|standby}**);
2. **Force state** – permanently switches IDU to active or standby state until force state is disabled by selecting 'Off' (command line – **prot force {active|standby|off}**);
3. **Standby time** – allows specifying Standby time (in range 1 – 15sec) for Standby state. IDU will remain for this time slot in Standby state during forcing it to another state (command line – **prot time standby [<0...15 sec.>]**);
4. **Activetry time** – allows specifying Active try time (in range 1-15sec) for Activetry state. IDU will remain for this time slot in Activetry state during forcing it to another state (command line – **prot time activetry [<0...15 sec.>]**);
5. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.
6. Writes to configuration file all the changes made on the whole page (command line – **cfg write**);
7. **System returned** - in case of error or incorrectly entered parameter value, or other problems on the whole page – info message will be displayed here. Otherwise it says “Ok”.

Additional user management commands in Telnet/serial interface	
Command	Description
prot status [remote alternate altrem all]	Shows protection status of particular IDU, as well as of any or all units involved in 1+1 configuration
prot alarms	Shows protection alarm status
prot trace	Traces protection state changes by printouts on terminal
prot ext statistics	Shows protection information exchange quality statistics between local and alternate IDU
prot ext statistics clear	Clears all previous exchange quality statistics

4.4 System Configuration

The system configuration window provides the configuration of web access, telnet and FTP interfaces; allows changing system name, web data refresh time and system time.

4.4.1 User Configuration

Figure 4.22 User configuration

1. **guest** – Enter new password (length: 4..30 characters) – allows entering preferable ‘guest’ account password and enabling the account. By default guest account is disabled. Maximal length of the password cannot exceed 30 symbols. Guest account has only monitoring privileges. The following Web GUI sections are available:

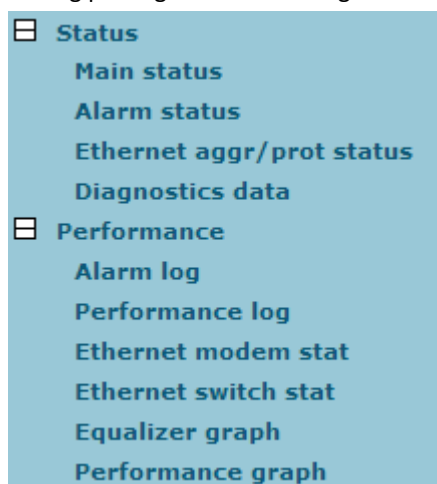


Figure 4.23 Menu for “guest” user

2. **admin** – Enter new password (length: 4..30 characters) – allows to enter preferable ‘admin’ account password. Maximal length of user name cannot exceed 30 symbols. By default password for ‘admin’ account is ‘changeme’. Admin account has full control of the CFIP configuration process.
3. **Hide password(-s)** – Hides typed in password. This option unchecked will display typed in password in plaintext.
4. By pressing “Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If “Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.

More detailed status controls are available in command prompt, which include:

Additional user management commands in Telnet/serial interface	
Command	Description
access login <name> <password>	Logs on as a user specified by <name> and <password>.
access logout	Logs current user out.
access set <guest/admin> <password> [plaintext]	Allows specifying a new password for a specific account (admin or guest). ‘plaintext’ option will save the password in plaintext in configuration script without encrypting it (by default saved passwords in configuration file are encrypted).
access show	Shows user name and password of a user currently logged on.
access list	Shows the list of usernames and passwords the current account is able to manage (if logged on as admin, ‘guest’ and ‘admin’ account passwords will be seen).

4.4.2 Name configuration

Name configuration		
System name (<= 16 characters)	1	SAF
Location name (<= 16 characters)	2	
System hostname (<= 16 characters)	3	
4		Rollback on ☐ Execute configuration

Figure 4.24 Name configuration

1. *System name (Max length: 16 characters)* – allows entering preferable system name. Maximum length of the system name cannot exceed 16 symbols. Default name is 'SAF' (command line – **system name** <name>);
2. *Location name (Max length: 16 characters)* – allows entering preferable system location name. Maximum length of the location name cannot exceed 16 symbols. By default system location is not specified (command line – **system location** <name>);
3. *System hostname (Max length: 16 characters)* – allows entering preferable system hostname. Maximum length of the hostname cannot exceed 16 symbols. By default system location is not specified (command line – **system location** <name>);
4. Pressing „Execute configuration” applies changes made to the corresponding section only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case of erroneous configuration changes applied.

4.4.3 Other configuration

Other configuration		
Web refresh (2 .. 60 sec)	1	5
Time (Usage: YY-MM-DD HH:mm:ss)	2	13-07-31 10:38:28 Set local machine time
3		Rollback on ☐ Execute configuration

Figure 4.25 Other configuration

1. *Web refresh (2 .. 600 sec)* – allows specifying time interval of Web data refreshing. The default value is 5 seconds. You can choose between 2 and 600 seconds (10 minutes) (command line – **web refresh** <web refresh time>);
2. *Time (Usage: YY-MM-DD HH:mm:ss)* – allows changing system date and time manually by entering date and time in specific syntax. “Set local machine time” button forces system to use the time set on your PC or laptop, from which you are connected to the Web interface (command line – **system time** [yyyy-mm-dd hh:mm:ss]);
3. By pressing “Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If “Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.

4.4.4 NTP configuration

Starting from firmware version 1.64.xx CFIP Phoenix features NTP (Network Time protocol) implementation – SNTP (Simple Network Time Protocol).

NTP configuration	
NTP Status	1 NTP disabled
NTP enable	2 ☐ Enable ☒ Disable
NTP server IP address	3 92.240.64.22
NTP time zone (-12..12)	4 3
5 Rollback on ☐	
6 Execute configuration	
Write to config file	
Immediate CPU restart	7 Restart CPU

Figure 4.26 NTP configuration

1. *NTP Status* – shows if NTP is enabled or disabled (command line – **system ntp status**);
2. *NTP enable* – allows enabling or disabling NTP. By default this feature is disabled (command line – **system ntp [enable/disable]**);
3. *NTP server IP address* – allows to specify NTP server IP address (command line – **system ntp server <IP address>**);
4. *NTP time zone (-12..12)* – allows to specify UTC (Coordinated Universal Time) offset (command line – **system ntp timezone <UTC offset>**);
5. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied;
6. Writes to configuration file all the changes made on the whole page (command line – **cfg write**);
4. Restarts CFIP Phoenix you are connected to (command line – **system reset**).

(!) Note that after restarting the CFIP will use only those settings, which are written to the configuration script. Other settings will be set to default values.

4.4.5 Upgrade Software

Upgrade software	
Choose file:	1 Browse... Upgrade

Figure 4.27 Upgrade software

1. *Choose file* – allows choosing location of software upgrade file (e.g. cfipidu165.elf.ezip) stored on your hard disk. Software upgrade file must have *.elf.ezip extension.

4.4.6 Service information

Service information	
Open full system information page	1 Download system information
Open advanced ethernet information page	2 Download ethernet statistics
System returned:	3 Ok

Figure 4.28 Service information

1. *Open full system information page / Download system information* – allows to open/save full system information page. Links on the top of the page allow you to save full system information page and alarm log in separate txt files on your hard disk drive;

2. *Open advanced ethernet information page / Download ethernet statistics* – allows to open/save advanced Ethernet statistics. Link on the top of the page allow you to save advanced Ethernet statistics page in separate txt file on your hard disk drive;
3. *System returned* - in case of error or incorrectly entered parameter value, or other problems in the whole page – the info message will be displayed here. Otherwise it says “Ok”.

(!) Note that Advanced Ethernet information page resets all counters and gathers Ethernet information. Please wait until information is gathered and displayed.

<i>Additional system commands in Telnet/serial interface</i>	
Command	Description
System status	Displays the name of the device and its uptime.
System inventory [show]	Displays the CFIP Phoenix product code, serial number and additional information.
System aliases [list all basic off add remove clear]	list – shows the alias list and whether the aliases are going to be used. The user can choose whether to see all the aliases (adding the argument “all”), built-in aliases (“built-in”), or optional aliases (“optional”), or user aliases (“user”); all – all the aliases will be used; basic – only basic (built-in, hidden and user) aliases will be used; off – no aliases will be used; add – if two arguments are given, creates an alias of the second argument, named as the first argument. If one argument given, alias command tries and loads the aliases from a file specified by the argument; remove – removes the alias specified by the argument; clear – removes all the user aliases.
System commands [show help]	show – displays all available commands; help – displays available help messages for all commands.
System reset [cold]	Restarts CPU of the management controller. Resets all management counters. cold – Restarts modem as well.
Ver	Displays hardware and software version of CFIP-IDU-Phoenix, as well as built date.

4.5 IP Configuration Window

The IP configuration window provides configuration of the Ethernet management port addressing, IP services and routes. Settings listed here are essential for building a network or other specific traffic purposes.

4.5.1 Ethernet management port IP configuration

Ethernet management port IP configuration		
IP address	1	192.168.205.10
IP mask	2	255.255.255.0
IP default gateway	3	255.255.255.255
Ethernet MAC address	4	00.04.A6.81.19.11 (17)
Remote IP address	5	192.168.205.11 ☒ Auto
For proper service channel operation IP address of remote side management CPU should be specified in the same subnet!		
	6	Rollback on ☐ Execute configuration
	7	Execute & write configuration

Figure 4.29 Ethernet management port IP configuration

1. *IP Address* – allows specifying IP address of CFIP Phoenix you are currently logged in. Default IP address is 192.168.205.10. (command line – **net ip addr <addr>**);
- (!) Note that CFIP Phoenix IP addresses have to have the same subnet.
2. *IP Mask* – allows specifying IP mask of CFIP Phoenix you are currently logged in. Default IP mask is 255.255.255.0, and it should not be changed unless you are owning network with huge amount of hops (command line – **net ip mask <mask>**);
 3. *IP Default gateway* – allows specifying gateway of CFIP Phoenix you are currently logged in. Default gateway is 255.255.255.255 which means that there is no gateway specified (command line – **net ip gw <gw>**);
 4. *Ethernet MAC address* – shows the MAC address of CFIP Phoenix you are currently logged in (command line – **net mac**);
 5. *Remote IP Address* – shows IP address of remote (far-end) CFIP Phoenix if the link is up (even in case of wrong IP configuration) (command line – **net ip remaddr <remaddr>**);
 6. By pressing “Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If “Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.
 7. By pressing “Execute configuration & write configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix and saved to configuration file.

4.5.2 IP Services

IP services	
FTP service	1 Start FTP
TFTP service	2 Start TFTP

Figure 4.30 IP services

1. *FTP service* – starts FTP service for file access and software update of your CFIP Phoenix. By default FTP service is not running (command line – **net start ftp**);
2. *TFTP service* – starts TFTP service for file transfer between both CFIP Phoenix link sides. By default TFTP service is not running (command line – **net start tftp**).

4.5.3 Static Route Configuration

(!) Do not make any changes to default route; otherwise, management connection to CFIP will be lost.

Figure 4.31 Static route configuration

1. *Static routes* – shows the list of existing static routes, as well as allows you to choose specific route you are willing to change or delete. By default there is one route which depends on earlier entered IP settings (command line – **net route**);
2. *Network address* – allows specifying network address for the route changing/adding (command line – **net route add/delete** <dest addr> [MASK <mask>] <gateway>);
3. *Network mask* - allows specifying network mask for changing/adding the route (command line – **net route add/delete** <dest addr> [MASK <mask>] <gateway>);
4. *Gateway* - allows specifying gateway for the route changing/adding (command line – **net route add/delete** <dest addr> [MASK <mask>] <gateway>);
5. After entering addresses or selecting a specific route, buttons “Add”, “Change” and “Delete” allow you to modify CFIP Phoenix routes. If „Rollback on” is selected, configuration will be reverted in case of erroneous configuration changes applied.
6. Writes to configuration file all the changes made on the whole page (command line – **cfg write**);
7. *System returned* - in case of error or incorrectly entered parameter value, or other problems on the whole page – info message will be displayed here. Otherwise it says “Ok”.

Additional network configuration commands in Telnet/serial interface	
Command	Description
Net ping <ip>	This command is for troubleshooting purposes to verify the service channel connectivity, - it sends a special packet to the specified address and then waits for a reply.
Net telnet <host> [<port>]	Opens Telnet session with the CFIP Phoenix IDU, <i>host</i> – IP address of the IDU unit management Ethernet port.
Net tftp <host> {get put} <source> [<destination>]	Uploads or downloads (put/get) file (<source>) to or from the host IDU unit (<host>).
Web trace {show on off}	Web trace allows you to see commands being executed through Web interface when you're using serial or telnet connection. <i>Show</i> – shows web trace status (on or off), <i>on</i> – turns web trace on, <i>off</i> – turns web trace off.
Web timeout <time in minutes>	Allows setting the time, after which the Web GUI presumes no connectivity state. By default the value is set to 15 minutes.
Web alert <on off>	Allows to enable or disable Web connectivity alert when Web GUI becomes unreachable

Below is the explanation of the procedure of network IP configuration in case of network IP Class area change.

For the purpose of illustration, we use B class IP network address 10.0.10.11 for the remote side CFIP and 10.0.10.10 for the local side CFIP, while the IP address of our management PC LAN adapter will be 10.0.0.1.

The steps of the configuration procedure are as follows:

1) Enter the remote side (far-end) Web GUI first (in the following case it is 192.168.205.10) and go to **"IP configuration"**. The configuration in this particular example will look in the following way:

Ethernet management port IP configuration	
IP Address	10.0.10.10
IP Mask	255.255.0.0
IP Default gateway	255.255.255.255
Ethernet MAC address	00.04.A6.80.B2.08 (8)
Remote IP Address	192.168.205.11
Rollback on ☐ Execute configuration	

Figure 4.32 Changing subnet for remote side

(!) "Rollback on" should not be selected!

Press **"Execute configuration"**.

2) Enter the local side (close-end) Web GUI and go to **"IP configuration"**. The configuration will look in the following way:

Ethernet management port IP configuration	
IP Address	10.0.10.11
IP Mask	255.255.0.0
IP Default gateway	255.255.255.255
Ethernet MAC address	00.04.A6.80.B2.07 (7)
Remote IP Address	10.0.10.10
Rollback on ☐ Execute configuration	

Figure 4.33 Changing subnet for local side

(!) "Rollback on" should not be selected!

Press **"Execute configuration"**.

3) In "MS Windows" go to "Control panel → Network Connections". In LAN "Properties" find "Internet Protocol TCP/IP" and click on its "Properties" (detailed description is in Chapter 2.3.2. Configuration of LAN Ethernet port must be as follows:

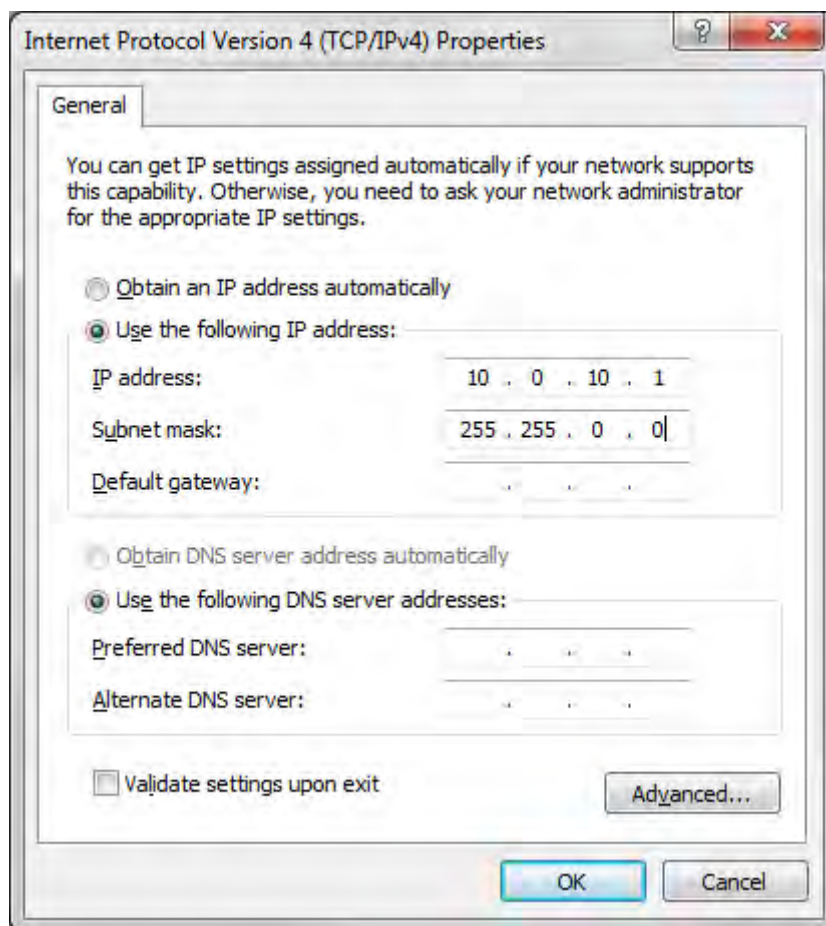


Figure 4.34 Internet Protocol (TCP/IP) Properties

- 4) Go to the remote side Web GUI, choose “Tools → Configuration file” and press “Cfg write”.
- 5) Repeat step 4) for the local side Web GUI.

4.6 Ethernet Configuration

The Ethernet configuration window provides the speed settings for all four LAN ports of Ethernet switch as well as shows the current status of all four LAN ports (command line – **ethernet stat**).

Explanation of customization fields:

Ethernet configuration					
Ethernet status and configuration					
	1 P1 (LAN)	P2 (LAN)	P3 (LAN)	P4 (LAN)	P5 (WAN)
Port state	2 Ok	Ok	Ok	Ok	Ok
Link	3 Off	1000 Mbps	Off	Off	1000 Mbps
Duplex (actual)	4 Full	Full	Full	Full	Full
Rx flow	5 Off	On	Off	Off	On
Tx flow	6 Off	On	Off	Off	Off
Rx state	7 On	On	On	On	On
Tx state	8 On	On	On	On	On
Speed (set)	9 auto	auto	auto	auto	
Ethernet flowcontrol	10 ☒ On ☐ Off	☒ On ☐ Off	☒ On ☐ Off	☒ On ☐ Off	Auto ☒ Auto
11	Rollback on ☐				Execute configuration

Figure 4.35 Ethernet status and configuration

1. Represents four LAN (Local Area Network) ports of the CFIP Phoenix switch, as well as WAN (Wide Area Port) connected to modem Ethernet interface;
2. *Port state* – shows operation status of each port;

3. *Link* – shows whether link with appropriate port is established. If link is off, according field will be shown in red;
4. *Duplex (actual)* – shows if port is currently operating in full or half duplex mode;
5. *Rx flow* – shows if 'flow control' is enabled or disabled for ingress traffic;
6. *Tx flow* – shows if 'flow control' is enabled or disabled for egress traffic;
7. *Rx state* – shows if ingress activity is allowed;
8. *Tx state* – shows if egress activity is allowed;
9. *Speed (set)* – shows current operation mode of each port and allows to set manual speed setting (10hdx/10fdx/100hdx/100fdx/1000fdx) (command line – **ethernet set** <1 | 2 | 3 | 4> *connection* <auto | 10hdx | 10fdx | 100hdx | 100fdx | 1000fdx>);
10. *Ethernet flowcontrol* – allows manually disabling or enabling flow control for specific port. Default option is auto (from autonegotiation). Uncheck "auto" in order to enable manual force mode (command line – **ethernet flowcntrl** {forced <Ports> | auto});
11. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.
12. configuration will be reverted in case erroneous configuration changes are applied.

4.6.1 Link state propagation configuration

Link state propagation (LSP) functionality allows shutting down specified LAN ports if synchronization loss events occur so that customer-premises equipment (CPE) is able to apply necessary changes promptly.

Link state propagation configuration		
LAN ports	1	☐ 1 ☐ 2 ☐ 3 ☐ 4
LSP timings		
LAN auto recovery* (0..600) sec	2	0 sec
SyncLoss keepalive timeout (0..10) sec	3	3 sec
LSP startup timeout (0..3600) sec	4	60 sec
SNMP traps	5	☐ Enabled ☒ Disabled
*LAN port will recover after synchronization reestablishment, if 0 sec. has been set!		
6		Rollback on ☐ Execute configuration

Figure 4.36 Link state propagation configuration

1. *LSP ports* – enables LSP (Link State Propagation) on selected LAN ports (command line – **ethernet rps ports** <ports>);
2. *LAN auto recovery* (0..600) sec* – synchronization loss timeout after which port is reenabled even if link synchronization is still lost, otherwise timeout is ignored. If parameter is set to "0", port will not be reenabled until link synchronization is recovered (command line – **ethernet rps time** <tm1> <tm2> <tm3>);
3. *SyncLoss keepalive timeout (0..10) sec* – LAN port shutdown timeout after synchronization loss and synchronization recovery events (command line – **ethernet rps time** <tm1> <tm2> <tm3>);
4. *LSP startup timeout (0..3600) sec* – LSP activity timeout after management CPU start up and configuration script execution. During this period synchronization events are ignored (command line – **ethernet rps time** <tm1> <tm2> <tm3>);
5. *SNMP traps* – SNMP trap will be sent if enabled. Note that SNMP trap address should be configured in SNMP configuration page (command line – **ethernet rps trap** <on/off>);
6. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.

4.6.2 Protocol transparency

Protocol transparency						
	1	P1 (LAN)	P2 (LAN)	P3 (LAN)	P4 (LAN)	P5 (WAN)
STP	2	☒	☒	☒	☒	☒
LACP	3	☐	☐	☐	☐	☐
OAM	4	☐	☐	☐	☐	☐
	5	Rollback on ☐				Execute configuration

Figure 4.37 Protocol Transparency

1. Represents four LAN (Local Area Network) ports of the CFIP Phoenix switch, as well as WAN (Wide Area Port) connected to modem Ethernet interface;
2. STP – allows enabling/disabling Spanning Tree Protocol (STP) transparency by passing through/filtering BPDU (Bridge Protocol Data Unit) frames on specified ports (command line – **ethernet transparency STP {enable | disable} {<port list> | All}**);
3. LACP – allows enabling/disabling Link Aggregation Control Protocol (LACP) transparency by passing through/filtering LACP frames on specified ports (command line – **ethernet transparency LACP {enable | disable} {<port list> | All}**);
4. OAM – allows enabling/disabling Operations, Administration and Management (OAM) transparency by passing through/filtering OAM frames on specified ports (command line – **ethernet transparency OAM {enable | disable} {<port list> | All}**);
5. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.

4.6.3 Ethernet ingress/egress rate configuration

Ethernet ingress/egress rate configuration		
Port	Ingress rate	Egress rate
LAN 1 (0.0625 .. 1000 Mbit/s)	Disabled Mbit/s	Disabled Mbit/s
LAN 2 (0.0625 .. 1000 Mbit/s)	Disabled Mbit/s	Disabled Mbit/s
LAN 3 (0.0625 .. 1000 Mbit/s)	Disabled Mbit/s	Disabled Mbit/s
LAN 4 (0.0625 .. 1000 Mbit/s)	Disabled Mbit/s	Disabled Mbit/s
WAN (0.0625 .. 1000 Mbit/s)	Disabled Mbit/s	Disabled Mbit/s
MNG (0.0625 .. 1000 Mbit/s)	Disabled Mbit/s	Disabled Mbit/s
	2	Rollback on ☐ Execute configuration
	3	Write to config file
System returned:	4	Ok

Figure 4.38 Ethernet ingress/egress rate configuration

1. Following section allows configuring ingress and egress rates on available Ethernet switch ports. In case ver.2 license with Ethernet rate limitation is applied, according Ethernet limitation will be indicated as ingress rate for WAN port;
2. Pressing „Execute configuration” applies changes made to the corresponding section only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case of erroneous configuration changes applied;
3. Writes to configuration file all the changes made on the whole page (command line – **cfg write**);
4. System returned - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says “Ok”.

4.7 Aggregation configuration

Link aggregation in n+0 mode allows utilizing up to 1000 Mbps Ethernet Layer 2 throughput by using independent frequency pair for each link. Traffic is being balanced (n+0) by internal switches of Master link. In case of link aggregation n+0 traffic distribution between n links is based upon the source and destination MAC addresses of Ethernet packets. Link aggregation (n+0) requires multiple MAC to MAC address pair connections as path for each connection is chosen based upon Ethernet frame's source and destination MAC addresses.

In case of link aggregation n+0 OMT, dual-polarized antenna or coupler can be used.

When active link is down, in n+0 mode all connections are being switched to active links. Average switchover time is 100ms.

Necessary equipment for CFIP Phoenix link aggregation n+0

2, 3 or 4 CFIP Phoenix links

1. 2 Gigabit Ethernet switches with at least n+2 ports (e.g. 4 ports for 2+0 configuration). There are no special requirements for external switch (SOHO switches can be used).

General configuration guide

Do not interconnect CFIP Phoenix IDUs with each other and do not plug CFIP Phoenix IDUs into switches before you have finished the configuration.

1. Choose one link which will operate as "Master". Other link will operate as "Slave"
2. Configure each link separately in mode you would like to operate. All CFIP Phoenix links should operate in the same operational mode (bandwidth, modulation, Ethernet capacity)
3. In case of link aggregation n+0 different frequencies should be set for master and slave links.
4. Choose different IP addresses for each CFIP Phoenix unit. Please see example given in **Figure 4.39**.
5. Remote IP address for all units should be entered manually. In order to do that in "Tools→Command line" should be entered "*modem ipremote off*" command and afterwards appropriate remote IP address entered in "Configuration→IP configuration"
6. When you have configured both links proceed with n+0 configuration

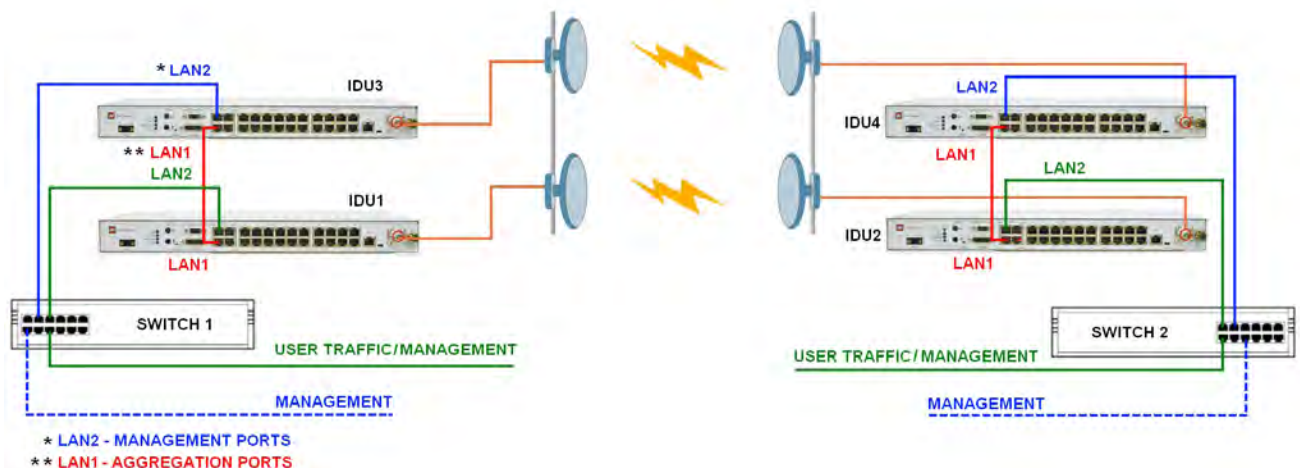


Figure 4.39 Link aggregation 2+0 setup

IDU1 IP address - 192.168.205.10 – Master local unit

IDU2 IP address - 192.168.205.11 – Master remote unit

IDU3 IP address - 192.168.205.12 – Slave local unit

IDU4 IP address - 192.168.205.13 – Slave remote unit

Configuration for master unit:

Ethernet aggregation configuration					
Aggregation status					
Link ID	#020				
State	Active				
Previous state	Start				
Aggregation configuration					
Role	1	Master ▼			
Mode	2	Aggregation ▼			
Revertive mode	3	Enabled ▼			
Master aggregation table					
Master unit IP address: a	192.168.205.013	Link ID: c	020	Port state: On	Traffic/MNG port: e 1 ▼
Slave unit IP address: b	192.168.205.011	Link ID: d	010	Port state: On	Aggregation port: f 2 ▼
Add entry 5					
6 Rollback on ☐ Execute configuration					
7 Write to config file					
System returned: 8 Ok					
*ASP - Aggregation Status on Port 9					

Figure 4.40 Ethernet aggregation configuration for Master

1. *Role* – choose “Master”;
2. *Mode* – choose “Aggregation” for link aggregation 2+0;
3. *Revertive mode* – in case of “enabled” setting link will automatically reconfigure back to 2+0 operation when unit/cable/link failure is resolved. In case of “disabled” setting link will continue to operate in 1+0 mode; In order to activate 2+0 manually, it is necessary to press “Change state: Active” button on any of two Slave units.
4. In “Master aggregation/protection table” set the following:
 - a. IP address of Master unit (you are configuring)
 - b. IP address of Slave unit (directly connected to Master unit *a*)
 - c. Link ID for Master link (same Link ID should be set on second Master unit)
 - d. Link ID for Slave link (same Link ID should be set on second Slave unit)
 - e. LAN port number which will be used as Traffic port (connection to external switch)
 - f. LAN port number which will be used as Aggregation/Protection port (connection with Slave unit)
5. *Add entry* – use to add additional Slave units (in case of 3+0 or 4+0 configurations);
6. Pressing „*Execute configuration*” applies changes made to the corresponding section only for the local side CFIP Phoenix. If „*Rollback on*” is selected, configuration will be reverted in case of erroneous configuration changes applied;
7. Writes to configuration file all the changes made on the whole page (command line – **cfg write**);
8. *System returned* - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says “Ok”.

Configuration for local slave unit:

Ethernet aggregation configuration			
Aggregation status			
Link ID	#010		
State	Active		
Previous state	Start		
Aggregation configuration			
Role	1	Slave ▼	
Mode	2	Aggregation ▼	
Revertive mode	3	Enabled ▼	
Master aggregation table			
Master unit IP address: a	192.168.205.013	Link ID: c	020
Slave unit IP address: b	192.168.205.011	Link ID: d	010
		Port state:	On
		Management port: e	1 ▼
		Aggregation port: f	2 ▼
Add entry 5			
6 Rollback on ☐ Execute configuration			
7 Write to config file			
System returned: 8 Ok			
*ASP - Aggregation Status on Port 9			

Figure 4.41 Ethernet aggregation configuration for Slave

1. Role – choose “Slave”;
2. Mode – choose “Aggregation” for link aggregation 2+0 or “Protection” for link protection 1+1;
3. Revertive mode – in case of “enabled” setting link will automatically reconfigure back to 2+0 operation when unit/cable/link failure is resolved. In case of “disabled” setting link will continue to operate in 1+0 mode; In order to activate 2+0 manually, it is necessary to press “Change state: Active” button (7) on any of two Slave units.
4. In “Slave aggregation/protection table” set the following:
 - a. IP address of Master unit (directly connected to Slave unit b)
 - b. IP address of Slave unit (you are configuring)
 - c. Link ID for Master link (same Link ID should be set on second Master unit)
 - d. Link ID for Slave link (same Link ID should be set on second Slave unit)
 - e. LAN port number which will be used as Management port (connection to external switch)
 - f. LAN port number which will be used as Aggregation/Protection port (connection with Master unit)
5. Pressing „Execute configuration” applies changes made to the corresponding section only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case of erroneous configuration changes applied;
6. Writes to configuration file all the changes made on the whole page (command line – **cfg write**);
7. Change state: Active – can be used to manually reactivate 2+0 aggregation mode if Revertive mode was disabled and for some reason link reconfigured to 1+0
8. System returned - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says “Ok”.

4.8 VLAN Configuration

The VLAN configuration window provides configuration of port-based Ethernet Virtual Local Area Networks (VLANs), allowing using up to 4095 different VLAN IDs. It is possible to assign 2 modes to your VLANs – Trunk (VLAN tagged packets are passed through on egress and ingress directions) and Access (VLAN tagged packets are untagged on egress direction).

In order to add VLAN tag to untagged packets on ingress direction, according “Default VLAN” (5) should be specified. By default “Default VLAN” value on all ports is VLAN ID 1.

When upgrading from any firmware prior to 1.63.xx, “Default VLAN” VID 0 will be changed to VID 1, but if “Default VLAN” VID was other than “0”, it will remain the same.

Additionally starting from 1.63.xx firmware all ports (except WAN) by default are configured as Access VLAN ID 1.

(!) When upgrading from any firmware prior to 1.63.xx you had VLAN configuration applied, management access will be available with previously specified management VLAN ID (as Default VLAN ID will remain the same), but it will be required to delete VLAN ID 1 from VLAN configuration table in order to make any further changes to VLAN configuration table.

VLAN configuration

802.1Q VLAN **1** ☒ Enabled ☐ Disabled

802.1Q Double Tagging **2** ☐ Enabled ☒ Disabled

VLAN configuration table

VLAN Nr.\Port 3	LAN 1	LAN 2	LAN 3	LAN 4	WAN	MNG	
Default VLAN 4	1	1	1	1	1	100	
1 - 99	☒ Trunk	☐ Trunk	☐ Trunk	☐ Trunk	☒ Trunk	☐ Access	Del
100 5	☒ Trunk	☐ Trunk	☐ Trunk	☐ Trunk	☒ Trunk	☒ Access	Del
101 - 4095	☒ Trunk	☐ Trunk	☐ Trunk	☐ Trunk	☒ Trunk	☐ Access	Del
Select/Deselect all VLAN(-s) 6	☐	☐	☐	☐	☐	☐	
Delete VLAN(-s) 7	From -						Del
8	Rollback on ☐					Execute configuration	

Add new VLAN

Nr.: - **9**

☐ Trunk ☐ Trunk ☐ Trunk ☐ Trunk ☐ Trunk ☐ Access

10 Reset VLAN(-s)

11 Write to config file

System returned: **12** Ok

Figure 4.42 VLAN configuration

1. 802.1Q VLAN – enables support of 802.1Q VLAN (command line – **ethernet vlan** [enable | disable]);
2. 802.1Q Double Tagging – enables double tagging feature, which is useful for ISP applications. When the ISP aggregates incoming traffic from each individual customer, the extra tag (double tag) can provide an additional layer of tagging to the existing IEEE 802.1Q VLAN. The ISP tag (extra tag) is a way of separating individual customers from other customers. Using the IEEE 802.1Q VLAN tag, a user can separate the individual customer's traffic. If P1-P4 (LAN1-LAN4) is being used in Access mode, it is required to enable this option (command line – **ethernet vlan doubletag** [enable | disable]); With enabled QinQ feature, client VLAN (C-tag) stays with default Ether type 0x8100 and Service tag (S-tag) is added with Ether type 0x9100.
3. VLAN Nr.\Port – displays all 6 ports of CFIP Phoenix switch;
4. Default VLAN – specifies default VID for untagged frames; Must match VLAN ID if port is set to Access mode – example for Management port is seen on **Figure 4.42** (command line – **ethernet vlan <N> default <port list>**);
5. VLAN table displays the list of set VLAN IDs and appropriate VLAN types on all available switch ports (command line – **ethernet vlan status**);
6. Select/Deselect all VLAN(-s) – Allows selecting or deselecting all VLANs of the corresponding column;
7. You can delete single VLANs or VLAN ranges by entering preferable VID range and pressing "Del" button;
8. By pressing "Execute configuration" changes made to the corresponding section apply only for the local side CFIP Phoenix. If "Rollback on" is selected, configuration will be reverted in case erroneous configuration changes are applied.

9. You can add VLANs by entering preferable VID, enabling appropriate port, choosing VLAN type and pressing "Add" button (command line – **ethernet vlan** <N[- N]> {Delete} | {Port <port list [1[u]] [2[u]] [3[u]] [4[u]] [5[u]] [6[u]]>};
10. **Reset VLAN(-s)** – resets the whole VLAN configuration (command line – **ethernet vlan reset**);
11. Writes to configuration file all the changes made on the whole page (command line – **cfg write**);
12. **System returned** - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says "Ok".

4.8.1 Ethernet Switch Port Status and Settings

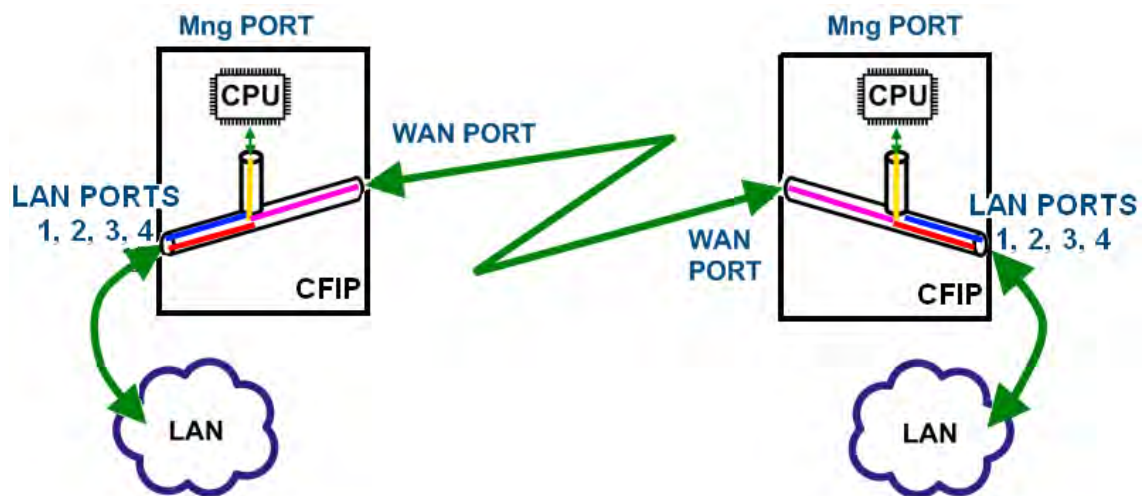


Figure 4.43 Ethernet switch ports

Switch LAN ports 1, 2, 3 and 4 are connected to LAN interface.

Switch WAN port is connected to WAN interface, modem and radio part.

Switch Mng port is connected to LAN Management CPU.

4.8.2 Ethernet Switch VLAN Status and Settings

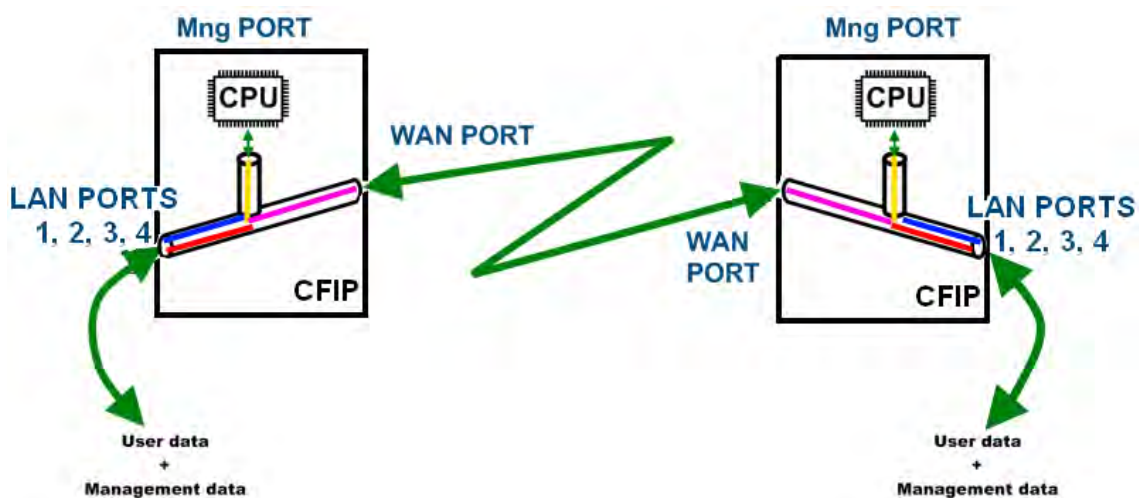


Figure 4.44 System without VLANs

When VLANs are not used (**Figure 4.44**), user data and management data are not separated either logically, or physically.

When using VLANs (**Figure 4.45**), it is necessary to use external switches (Switch 3 and Switch 4). These switches add/remove VLAN tags per port basis. Thus, management data and user data have different VLAN tags and are logically separated.

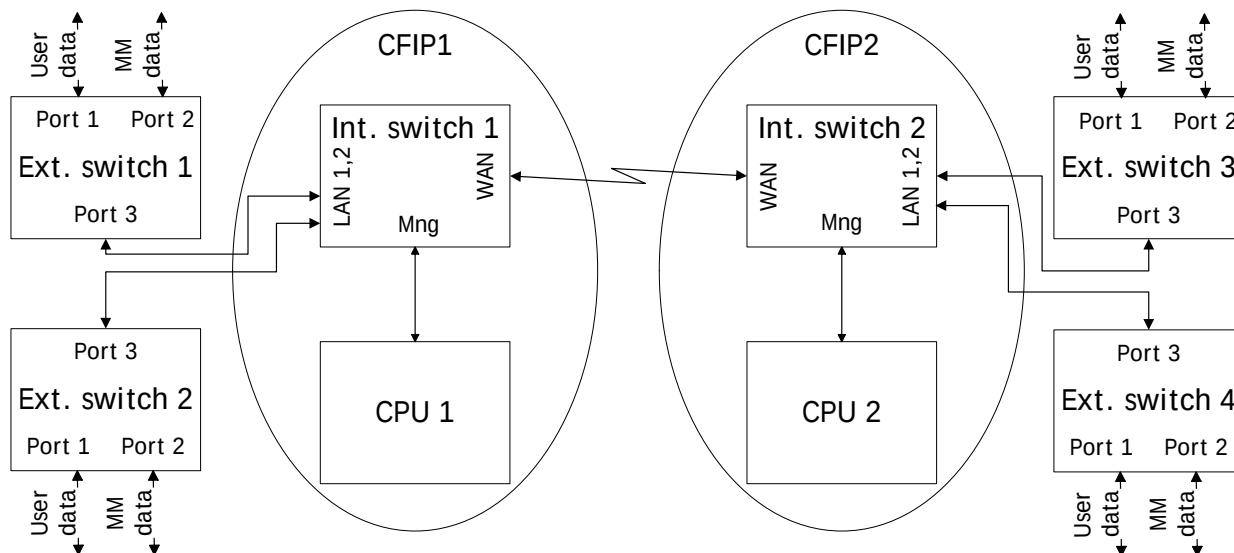


Figure 4.45 System with VLANs

System with two separate VLANs – A and B. **Figure 4.46.** represents ports membership to VLANs.

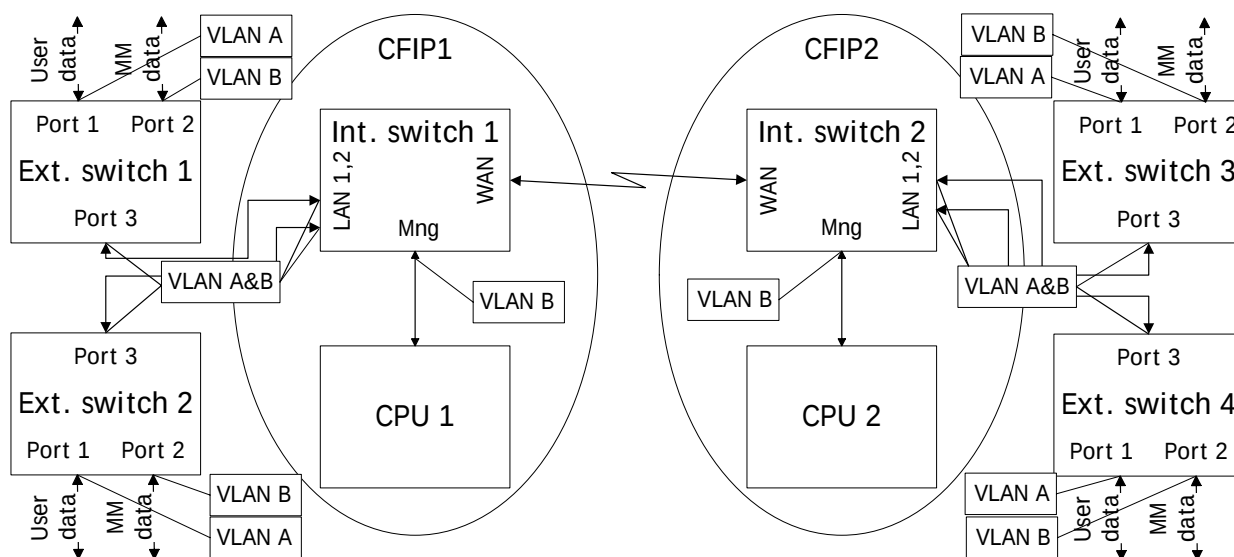


Figure 4.46 VLANs and ports membership

LAN and WAN ports of Int. switch 1 and switch 2 are sending data according to VLAN ID and destination address, and adding VLAN tags for packets outgoing from Mng port. Additionally, VLAN tag is removed at Mng port of Switch 1 and Switch 2.

VLAN A is the Trunk type VLAN with LAN & WAN port membership.

VLAN B is the Management type VLAN with LAN & WAN & Mng membership.

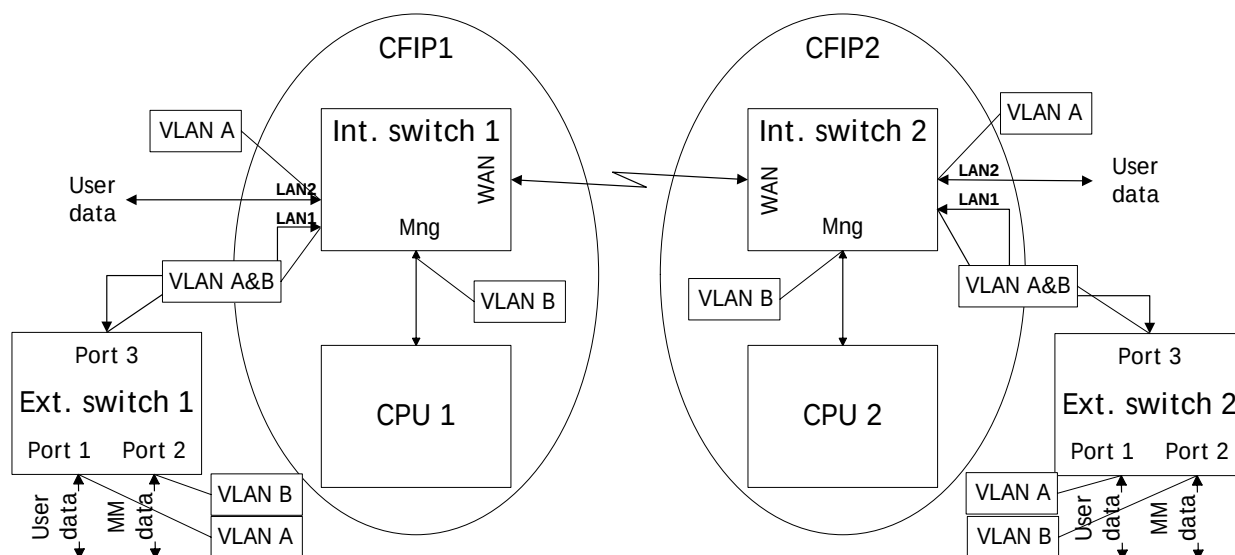


Figure 4.47 Configuration with management and user VLANs on separate LAN ports

For both switches:

VLAN A is configured as:

- Trunk type VLAN with LAN1 & WAN membership;
- Access type VLAN with LAN2 & WAN membership with removing and inserting VLAN tags while packet is being transmitted to LAN2 and WAN, respectively.

VLAN B is configured as:

- Management type VLAN with LAN1, WAN and Mng ports membership when removing VLAN tags while packet is being sent to Mng port and inserting tag while packet is transmitting to LAN&WAN ports.

Limitations and rules on using VLAN:

- Supports up to 4096 full range VLAN IDs.
- Only one VLAN with unique IDs is allowed. When adding a different VLAN with the same IDs, the old VLAN is deleted (also the other types of VLANs).
- Simultaneous use of Access and Trunk type VLANs on one LAN port is not allowed.
- After the VLAN table initialization is completed, 802.1Q VLAN mode must be enabled.
- WAN (P5) allows using only Trunk VLAN Type and Management (P6) – only Access VLAN Type
- In order to pass untagged packets through the link, VLAN ID "0" should be added as Trunk VLAN Type on LAN (P1-4) and WAN (P5).

Steps required for VLAN configuration:

- 1) Add preferable VLAN IDs in "Configuration→VLAN Configuration" in Web GUI on both sides of the link;
- 2) Enable "802.1Q VLAN" for remote unit first, then for the local unit;
- 3) Configure switches for VLAN tag encapsulation on both ends of the link;
- 4) Reconnect to Web GUI via configured Management VLAN ID.

Examples of VLAN usage:

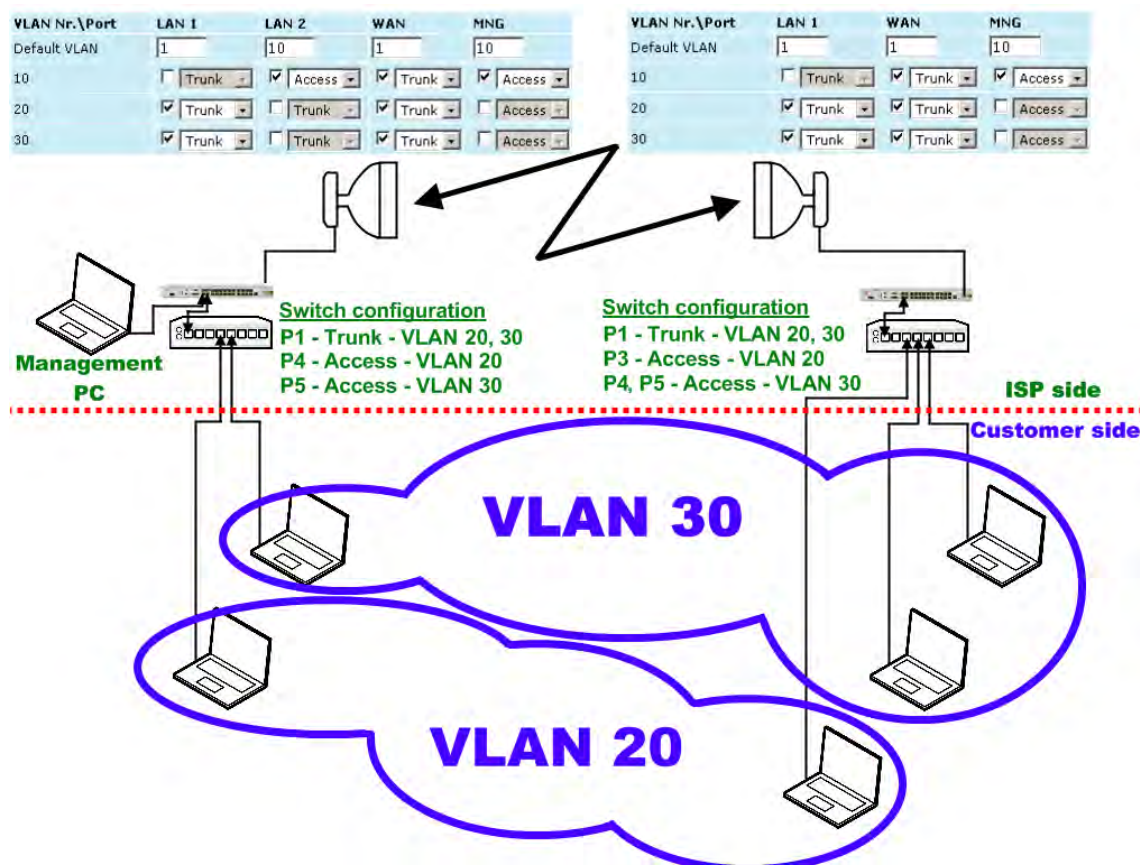


Figure 4.48 VLAN configuration of CFIP Phoenix link

4.9 QoS

4.9.1 General Configuration

QoS status provides control over main QoS parameters, accordingly allowing enabling or disabling QoS 802.1p, DiffServ or port based priorities and change priority queuing mode.

QoS general configuration							
QoS general status							
Name	LAN 1	LAN 2	LAN 3	LAN 4	WAN	MNG	
QoS 802.1p	1 ☐	☐	☐	☐	☐	☐	Enable/Disable all
DiffServ	2 ☐	☐	☐	☐	☐	☐	Enable/Disable all
Port based priority	3 1	1	1	1	1	1	
Rollback on ☐							Execute configuration
QoS general queuing							
Queuing priority selection	4	802.1p					
Queuing type	5	☐ Fixed ☒ Weighted					
Name		Q1	Q2	Q3	Q4		
Weights (0 < Q1 < Q2 < Q3 < Q4 < 50)	6	1	2	4	8		
7	Rollback on ☐						
							Execute configuration
							Write to config file
System returned:	9	Ok					

Figure 4.49 QoS general configuration

1. QoS 802.1p – enables or disables 802.1p priorities for any available switch port – LAN1/2/3/4, WAN or Mng (command line – **ethernet QoS 802.1p** {[enable | disable <Port>] | [map]});

2. *DiffServ* – enables or disables DiffServ (DSCP) priorities for any available switch port – LAN1/2/3/4, WAN or Mng (command line – **ethernet QoS DSCP** [enable | disable <port>] | map);
3. *Port based priority* – implies ingress packets on specified ports directly to priority queue set. By default port based priority queuing passes packets from all ports to lowest (1) priority queue (command line – **ethernet QoS port** <port> <priority>);
4. *Queuing priority selection* – allows to select primary QoS method, upon which queueing decision shall be made;
5. *Queuing type* – allows choosing fixed priority queuing mode or weighted queuing mode;
6. *Weights* ($0 < Q1 < Q2 < Q3 < Q4 < 50$) – allows specifying correlation of all four queues. Queue values should correspond to limitations. Default correlation is 1:2:4:8.
7. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.
8. Writes to configuration file all the changes made on the whole page (command line – **cfg write**);
9. *Execution status* - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says “Ok”.

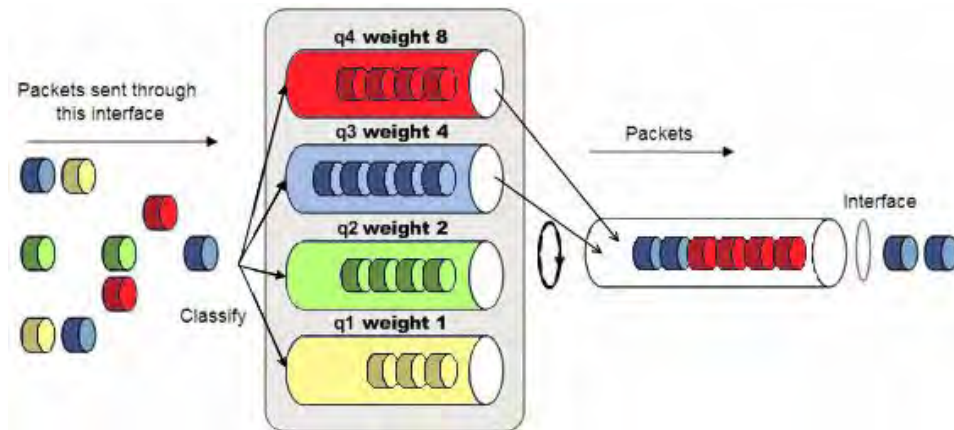


Figure 4.50 Weighted priority queuing mode

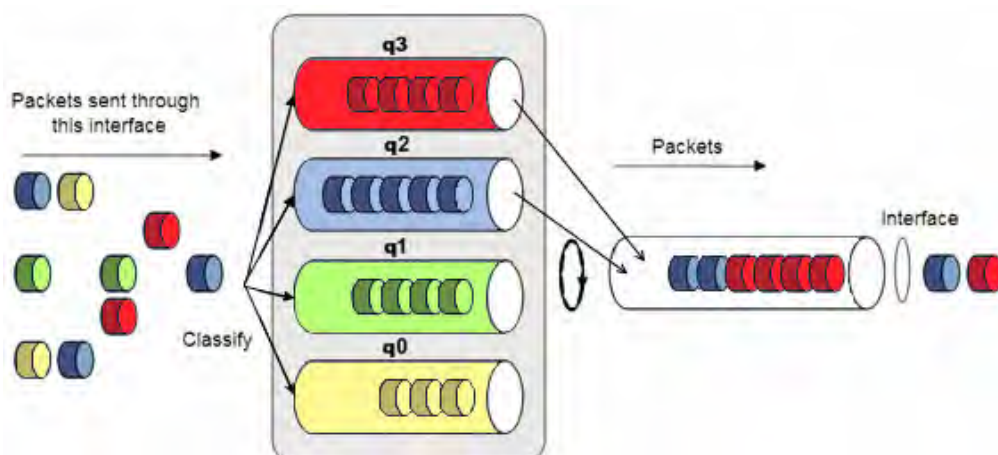


Figure 4.51 Fixed priority queuing mode

In case of weighted priority queuing mode, highest (q3) priority buffer may pass up to 8 consecutive packets subsequently proceeding to lower priority buffer (q2), which may pass up to 4 consecutive packets. This means that highest priority after passing 8 consecutive packets will wait no longer than until 7 packets of lower priorities pass ($4(q2)+2(q1)+1(q0)$).

If any queues are empty, the highest non-empty queue gets one more weighting. For example, if q2 is empty, q3:q2:q1:q0 becomes (8+1):0:2:1.

In case of fixed queuing mode, highest priority buffer (q3) will pass packets as long as its buffer is full.

By default weighted priority queuing mode is enabled.

4.9.2 QoS 802.1p Configuration

QoS 802.1p provides configuration of QoS 802.1p priority mapping. You are able to map 8 different traffic 802.1p values (0 – 7) into 4 priority queues (1 – 4).

802.1p value	Queue value
0	1
1	1
2	2
3	2
4	3
5	3
6	4
7	4

Rollback on ☐ Execute configuration

Write to config file

System returned: Ok

Figure 4.52 QoS 802.1p priority mapping

1. *QoS 802.1p priority mapping* – allows assigning queue values to specific 802.1p values.
2. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.
3. Writes to configuration file all the changes made on the whole page (command line – **cfg write**);
4. *System returned* - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says “Ok”.

4.9.3 DSCP Configuration

QoS DSCP provides mapping of different traffic DSCP classes to priority queues.

QoS DSCP configuration

DSCP mapping **1**

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0	1 ▼	16	2 ▼	32	3 ▼	48	4 ▼
1	1 ▼	17	2 ▼	33	3 ▼	49	4 ▼
2	1 ▼	18	2 ▼	34	3 ▼	50	4 ▼
3	1 ▼	19	2 ▼	35	3 ▼	51	4 ▼
4	1 ▼	20	2 ▼	36	3 ▼	52	4 ▼
5	1 ▼	21	2 ▼	37	3 ▼	53	4 ▼
6	1 ▼	22	2 ▼	38	3 ▼	54	4 ▼
7	1 ▼	23	2 ▼	39	3 ▼	55	4 ▼
8	1 ▼	24	2 ▼	40	3 ▼	56	4 ▼
9	1 ▼	25	2 ▼	41	3 ▼	57	4 ▼
10	1 ▼	26	2 ▼	42	3 ▼	58	4 ▼
11	1 ▼	27	2 ▼	43	3 ▼	59	4 ▼
12	1 ▼	28	2 ▼	44	3 ▼	60	4 ▼
13	1 ▼	29	2 ▼	45	3 ▼	61	4 ▼
14	1 ▼	30	2 ▼	46	3 ▼	62	4 ▼
15	1 ▼	31	2 ▼	47	3 ▼	63	4 ▼

2 Rollback on ☐ **Execute configuration**

3 **Write to config file**

System returned: **4** Ok

Figure 4.53 DSCP mapping

1. *DSCP mapping* – allows assigning queues for different DSCP classes. You may have up to 64 different traffic DSCP classes;
2. By pressing „*Execute configuration*” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „*Rollback on*” is selected, configuration will be reverted in case erroneous configuration changes are applied.
3. Writes to configuration file all the changes made on the whole page (command line – *cfg write*);
4. *System returned* - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says “Ok”.

4.10 Spanning Tree Configuration

4.10.1 Spanning Tree Configuration

Spanning Tree Protocol 7 Instance 0 / main config						
Bridge Configuration				Root Information		
Bridge ID	32768 .00.04.A6.80.D6.85		1	Regional Root ID	32768.00.04.A6.80.D6.85 8	
				Regional Root Port	N/A 9	
				Regional Root Path Cost	0 10	
Hello Time (1 – 100 sec)	2		2	Hello Time	2 11	
Max Age (6 – 40 sec)	20		3	Max Age	20 12	
Forward Delay (4 – 30 sec)	15		4	Forward Delay	15 13	
				Root ID	32768.00.04.A6.80.D6.85 14	
Version	RSTP		5	Root Port	N/A 15	
STP operation	Enabled		6	Root Path Cost	0 16	
Port	Priority	Path Cost/ auto	State	Role	Edge	Point-to-Point
P1 (LAN)	128	20000 ☒	Discarding	Disabled	Yes	Yes
P2 (LAN) 17	128	20000 ☒	Forwarding	Designated	Yes	Yes
P3 (LAN)	128	20000 ☒	Discarding	Disabled	Yes	Yes
P4 (LAN)	128	20000 ☒	Discarding	Disabled	Yes	Yes
P5 (WAN) 18	128	200000 ☐	Forwarding	Designated	Yes	Yes
19						Execute configuration
20						Write to config file
System returned: Ok				21		

Figure 4.54 Spanning Tree Protocol – Bridge configuration

Bridge configuration - Values 2-4 take effect only if a given Bridge is Root:

1. *Bridge ID* – value from (0..61440); this parameter and MAC address determine whether a given Bridge is Root Bridge. Advantage is given to the combination of *Priority* and *Address*, which is numerically smaller;
2. *Hello Time (1..100)* – time gap, between which the BPDU packets are being sent;
3. *Max Age (6..40)* – this parameter determines time period, during which the received BPDU packets' information is stored for a separate port;
4. *Forward Delay (4..30)* – time period that determines time a separate port stays in *Listening* and *Learning* conditions;
5. *Version* – allows to switch STP versions between STP, RSTP or MSTP;
6. *STP operation* – Enable or Disable STP operation;
7. Change between MST instances configuration when MSTP operation mode is enabled;

Root information – displays the data only when STP/RSTP/MSTP is enabled:

8. *Regional Root ID* – displays the Bridge ID for *instance 0** of current Root bridge;
9. *Regional Root Port* – currently selected root port for *instance 0** is being shown;
10. *Root Path Cost* – displays the path cost port for *instance 0** from current bridge to root bridge;
11. *Hello Time* – displays the current hello time;
12. *Max Age* – displays the current max age;
13. *Forward Delay* – displays the current forward delay;

14. *Bridge ID* – displays the Bridge ID of current Root bridge;
15. *Root Port* – currently elected root port is being shown;
16. *Root Path Cost* – displays the path cost from current bridge to root bridge;
17. *Port 1 LAN* – STP parameters of LAN port;
18. *Port 2 WAN* – STP parameters of WAN port:
 - *Priority (0..240)* – Port Priority. Combination of Priority, Port number and Path Cost determines whether the port will be selected as Root port or will be blocked on the occasion of loop, etc;
 - *Path cost (1..200000000)* – this parameter setting depends on the capacity of a separate port;
 - *State* – port condition. Can be one of the following: *Disabled*, *Blocking*, *Listening*, *Learning* or *Forwarding*;
 - *Role* – role of the particular port. Can be one of the following: *Root*, *Designated*, *Alternate*, *Backup* or *Disabled*;
 - *Edge* – specifies whether this particular port is Edge port or not;
 - *Point-to-point* – specifies whether there is point-to-point connection from particular port or not;
19. By pressing „*Execute configuration*” changes made to the corresponding section apply only for the local side;
20. *Write to config file* - saves to configuration file all the changes made on the whole page (command line – **cfg write**);
21. *System returned* - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says “Ok”.

* Instance 0 carries all STP-related information and refers only when MSTP is enabled

4.10.2 Region, mapping configuration for MSTP

The screenshot shows the 'Spanning Tree Protocol' configuration page. The 'Region Configuration' section includes fields for 'Region name (1 - 32 characters)' (highlighted with a red 1, containing '00:04:a6:80:c7:f7'), 'Region revision (0 - 65535)' (highlighted with a red 2, containing '0'), and 'Region digest' (highlighted with a red 3, containing '0xAC36177F50283CD4B83821D8AB26DE62'). A red 4 points to the 'Execute configuration' button. The 'VLAN mapping' section has a 'VLAN (1 - 4094)' field (highlighted with a red 5) and an 'Instance' dropdown (highlighted with a red 6, set to 'Instance 1'). Below these is a large empty table area. At the bottom, a 'Write to config file' button is highlighted with a red 6, and a 'System returned: Ok' status bar is highlighted with a red 7.

Figure 4.55 Spanning Tree Protocol – Redion configuration

1. *Region name (0 - 32 characters)* – displays region name. By default device’s MAC address;
2. *Region revision (0- 65545)* – displays region revision;
3. *Region digest* – hash value calculated over VLANs to Multiple Spanning Tree Instance mapping table contents and region revision;

4. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side;
5. *VLAN (1 – 4094)* – map VLAN ID or VLAN IDs range for each instance. Up to seven instances;
6. *Write to config file* - saves to configuration file all the changes made on the whole page (command line – **cfg write**);
7. *System returned* - in case of error or incorrectly entered parameter value, or other problems on the whole page – the info message is being shown here. Otherwise it says “Ok”.

4.10.3 Spanning Tree Protocol statistics

Spanning tree protocol statistics summarizes STP statistics on all available switch ports.

Spanning Tree Protocol Statistics						
Instance 0 (CST)	LAN 1	LAN 2	LAN 3	LAN 4	WAN	
Rx MSTP BPDUs 1	0	0	0	0	0	0
Rx RSTP BPDUs 2	0	0	0	0	0	0
Rx Conf. BPDUs 3	0	0	0	0	0	0
Rx TCN BPDUs 4	0	0	0	0	0	0
Bad MSTP BPDUs 5	0	0	0	0	0	0
Bad RSTP BPDUs 6	0	0	0	0	0	0
Bad Conf. BPDUs 7	0	0	0	0	0	0
Bad TCN BPDUs 8	0	0	0	0	0	0
Tx MSTP BPDUs 9	0	0	21	0	0	0
Tx RSTP BPDUs 10	0	0	0	0	0	0
Tx Conf. BPDUs 11	0	0	0	0	0	0
Tx TCN BPDUs 12	0	0	0	0	0	0
Fwd Transitions 13	0	0	1	0	0	0
Time Since Top Chg 14						00:00:00
Top Change Count 15						0

Figure 4.56 Spanning Tree Protocol Statistics

1. *Rx MSTP BPDUs* – displays how many MSTP BPDUs packets received;
2. *Rx RSTP BPDUs* – displays how many RSTP BPDUs packets received;
3. *Rx Conf BPDUs* – displays how many STP BPDUs packets received;
4. *Rx TCN BPDUs* – displays how many topology changing notification BPDUs packets received;
5. *Bad MSTP BPDUs* – displays how many bad MSTP BPDUs packets received;
6. *Bad RSTP BPDUs* – displays how many bad RSTP BPDUs packets received;
7. *Bad Conf BPDUs* – displays how many bad STP BPDUs packets received;
8. *Bad TCN BPDUs* – displays how many bad topology changing notifications BPDUs packets received;
9. *Tx MSTP BPDUs* – displays how many MSTP BPDUs packets send;
10. *Tx RSTP BPDUs* – displays how many RSTP BPDUs packets send;
11. *Tx Conf BPDUs* - displays how many STP BPDUs packets send;
12. *Tx TCN BPDUs* – displays how many topology changing notification BPDUs packets send;
13. *Fwd Transitions* – displays how many times port has been changed to forward status;
14. *Times Since Top Chg* – displays time since last topology change in HH:MM:SS;
15. *Top Change Count* - displays total change count for all port;

4.11 SNMP v1/v2 configuration

The SNMP v1/v2 configuration pages provide configuration of SNMP communities, host and trap addresses. SAF NMS system will work only when SNMP is properly configured.

Explanation of customization fields:

4.11.1 SNMP community configuration

The screenshot shows the 'SNMP community configuration' web interface. It includes input fields for 'Read (<= 31 characters)', 'Write (<= 31 characters)', and 'Trap (<= 31 characters)'. The 'Trap' field contains 'saf-trap'. Below these is a 'List of trap managers' section with a list box and an 'Add or Delete IP address of trap receiver to list of trap managers' section with an input field and 'Add'/'Delete' buttons. At the bottom, there is a 'Rollback on' checkbox and an 'Execute configuration' button. Red numbers 1 through 6 are overlaid on the interface to indicate specific fields and actions.

Figure 4.57 SNMP community configuration

1. *Read* - Specifies the SNMP v1/v2 community name of the agent to enable parameters to be read (not configured) (command line – ***snmp community read*** <communityname> and ***snmp2 community read*** <communityname>);
2. *Write* – specifies the community name of the agent to enable parameters to be written (configured) (command line – ***snmp community write*** <communityname> and ***snmp2 community write*** <communityname>);
3. *Trap* – specifies SNMP v1/v2 trap community name for trap authentication in monitoring applications (command line – ***snmp community trap*** <communityname> and ***snmp2 community trap*** <communityname>);
4. *SNMP trap host list* – shows the list of IP addresses of the management terminal with the installed Trap Manager software, based on SNMP v1/v2 platform. The CFIP Phoenix management controller sends SNMP traps to the Trap Manager with IP address specified here. The SNMP Trap Manager is a PC with installed SNMP trap management software. The default Trap Manager IP address is 255.255.255.255 meaning that no trap packets are sent by the management controller;
5. Allows to add or delete SNMP v1/v2 trap host IP addresses from the list (command line – ***snmp trap*** <IP addresses of trap receivers> and ***snmp2 trap*** <IP addresses of trap receivers>);
6. By pressing „Execute configuration” changes made to the corresponding section apply only for the local side CFIP Phoenix. If „Rollback on” is selected, configuration will be reverted in case erroneous configuration changes are applied.

4.11.2 SNMP Allowed Hosts Configuration

The screenshot shows the 'SNMP allowed hosts configuration' web interface. It includes a 'List of SNMP managers' section with a list box. Below it is an 'Add or Delete IP address to list of SNMP managers' section with an input field and 'Add'/'Delete' buttons. At the bottom, there is a 'Reset SNMP host(-s)' button and a 'Write to config file' button. A 'System returned:' status bar at the very bottom shows 'Ok'. Red numbers 1 through 5 are overlaid on the interface to indicate specific fields and actions.

Figure 4.58 SNMP allowed hosts configuration

1. *SNMP host list* – shows the list of available v1/v2 SNMP hosts; adds or deletes the host IP address to the CFIP SNMP v1/v2 host table. If the SNMP host connected to the CFIP is not added to the CFIP SNMP v1/v2 host table, the CFIP will not respond to the SNMP requests from that host. If „Rollback on” is selected, configuration will be reverted in case of erroneous configuration changes applied.
2. Allows to add or delete SNMP host IP addresses from the list (command line – ***snmp host {add | delete | list | reset} <ipaddr>*** and ***snmp2 host {add | delete | list | reset} <ipaddr>***);
3. Reset SNMP host(-s) – deletes all SNMP managers’ IP addresses from the list;
4. Writes to configuration file all the changes made on the whole page (command line – ***cfg write***);
5. *System returned* - in case of error or incorrectly entered parameter value, or other problems in the whole page – info message will be displayed here. Otherwise it says “Ok”.

5 Performance and Alarm Management

5.1 Alarm Management

5.1.1 Alarms and Events Structure

All alarms and events are placed in indexed table. Low level raw alarms and events are placed in the first table. Raw alarms and events are merged in groups, which are placed in the second indexed group table. Raw alarm table and group table are related one to many, or one to one if each alarm has a separate group (see **Figure 5.1**). Group is in *SET* state if one or more group members are in *SET* state. If there is no info about any group member alarm or event state, then there is no info about group state too.

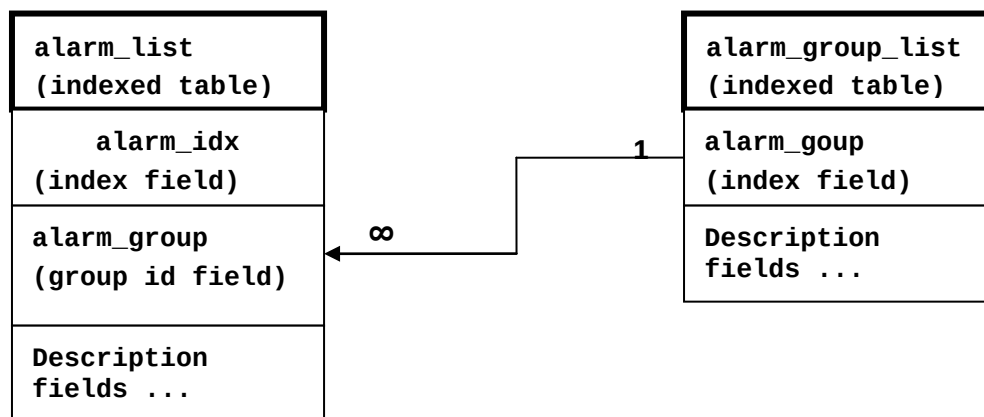


Figure 5.1 Alarm and group table relation

5.1.2 Alarms-Events and Groups Tables

Most groups write log when group state changes (Set/Reset), but some groups are only rising.

Alarms events and event groups:

Alarm ID	Group ID	Alarm-Event name	Description
1	1	==> System Start	Software started [Only rising]
2	2	Invalid device license	License is not valid
3	3	License expired	License validity has expired
4	4	License will soon expire	License validity will soon expire
5	5	Log was Cleared	Entered when 'Log Clear' command was called [Only rising]
6	6	Log ERROR	Log data structure missing
7	7	Log TEST	Log test was made
8	8	Counters was Cleared	System performance counters were cleared [Only rising]
9	9	Config was Written	Configuration was written [Only rising]
10	10	System CPU restart ==>	Entered when system restart was called [Only rising]
11	11	No data from IDU temperature sensor	No data from temperature sensor connected via I2C interface

12	12	IDU temperature fault	Temperature is out of defined range
13	13	No data from main PSU IDU ADC	No data from IDU ADC connected via I2C interface
14	14	Main supply 48V failure	Main supply voltage is out of defined range
15	15	IDU PSU state	One of the possible PSU state "OFF", "IDLE", "Ok", "OVERLOAD", "SHORT", "FAULT" state was changed for IDU
16	16	No data from main PSU ODU ADC	No data from ODU ADC connected via I2C interface
17	17	IDU PSU to ODU state	One of the possible PSU state "OFF", "IDLE", "Ok", "OVERLOAD", "SHORT", "FAULT" state was changed for ODU
18	18	No data from PSU temperature sensor	No data from PSU temperature sensor via I2C interface
19	19	PSU temperature fault	PSU temperature is out of defined range
20	20	Main 3,3V PSU failure	Main supply 3,3V voltage is out of defined range
21	21	No data from power supply ADC	No data from ADC connected via I2C interface
22	22	1,0V failure	Power supply voltage out of defined range
23	22	1,2V failure	Power supply voltage out of defined range
24	22	1,5V failure	Power supply voltage out of defined range
25	22	2,5V failure	Power supply voltage out of defined range
26	22	3,3V failure	Power supply voltage out of defined range
27	22	Main 3,3V failure	Power supply voltage out of defined range
28	22	5,0V failure	Power supply voltage out of defined range
29	23	No data from RADIO	No data from ODU
30	24	Rx level alarm	Rx alarm level is out of defined range
31	25	Tx PLL error alarm	Tx PLL failure
32	26	Rx PLL error alarm	Rx PLL failure
33	29	ODU TX LOS	Tx IF AGC error is greater than 2 dB
34	31	ODU TX failure	Tx RF AGC error is greater than 2 dB
35	28	ODU RX LOS	RxPow < RslMinPower
36	30	ODU RX failure	Rx AGC error is greater than 2 dB
37	32	ODU TX Frequency failure	Tx synthesizer could not synchronize
38	32	ODU RX Frequency failure	Rx synthesizer could not synchronize
39	32	ODU IF Frequency failure	IF synthesizer could not synchronize
40	27	ODU Temperature alarm	ODU sends temperature alarm
41	27	ODU Temperature fault	ODU temperature is out of defined range U temperature is out of defined range
42	33	ODU Tx mute on	ODU transmitter was muted
43	34	ODU RF loopback on	ODU radio frequency loopback was enabled

44	35	No data from MODEM	No data from MODEM connected via UART interface
45	36	Acquire status alarm	Modem acquire failure status
46	37	Last acquire error status	Modem last acquire failure status
47	38	Radial MSE	Radial MSE is out of defined range
48	39	LDPC decoder stress	LDPC decoder stress is out of defined range
49	40	Tx ACM profile was changed	ACM profile was changed
50	41	RX carrier offset	Error in Rx carrier offset
51	42	No data from modem temperature sensor	No data from modem temperature sensor via I2C interface
52	43	Modem temperature fault	Modem temperature is out of defined range
53	44	ATPC Tx power correction was changed	ATPC Tx power correction was changed
54	45	Rollback initiate system CPU restart ==>	System restart was called by rollback [Only rising]
55	46	System CPU reset was WDT initiated ==>	System restart was called by watchdog [Only rising]
56	47	PM log flash write error	Error while writing pm log to flash
57	48	Command from interface	Message about command execution from particular interface
58	49	Message of event	Informative message
59	50	E1/T1 interface	E1/T1 interface state was changed
60	51	Eth interface	No connection to Ethernet LAN port
61	52	AUX alarm in 1	AUX alarm 1 was enabled
62	53	AUX alarm in 2	AUX alarm 2 was enabled
63	54	AUX alarm in 3	AUX alarm 3 was enabled
64	55	AUX alarm in 4	AUX alarm 4 was enabled
65	56	No protection data from alternate	If 1+1 protection is enabled and no data from alternate (paired) device
66	57	Protection state was changed	Protection state was changed
67	58	Aggregation state was changed	Event of aggregation state change in aggregation 2+0 configuration
68	59	Aggregation events	Event of aggregation 2+0 configuration
69	60	Keepalive ethernet switch reset	Ethernet switch does not respond and thus is reset

5.1.3 Alarm Status Window

‘Status → Alarm status’ in navigation bar shows you all the current alarms.

Date and time represents the time the alarm appeared, so you can easily evaluate for how long the alarm has been active. ‘Alarm gr.’ is the number of alarm group in which the specific alarm is

grouped. Complete list of alarm individual IDs and group IDs can be seen in the table above or using the command **'alarm list'** in the command prompt.

To configure representation of alarms, refer to **Chapter 5.2.5**.

Alarm status			
Alarm gr.	Date	Time	Alarm
51	2014-06-18	10:21:20	Ethernet interface - Ports[P1(LAN)P3(LAN)P4(LAN)] Link[Off]

Figure 5.2 Alarm status window

5.1.4 Alarm Log

To view alarms history, go to 'Performance → Alarm log'.

Alarm log shows 21 latest alarm entries per page and about 2000 latest alarm entries in total.

Alarm entries are mostly distributed in two groups – 'Set' when alarm appears and 'Reset' when alarm disappears.

To view earlier log entries, please enter the number of log entry and press 'Previous 21' or 'Next 21' to view 21 entries before or after entered entry number.

Note that the alarm ID (for example, '057' in the **Figure 5.3**) here is an individual ID, not a group ID.

You also have fast access to alarm filtering, where it is possible to choose which alarm ID you are willing to search among all log entries. To configure detailed and permanent alarm representation, refer to the next chapter.

Alarm log

0366: 2014-06-18 10:31:26 - 057 - Command from interface - TASK> modem set 56000 4QAM 256QAM WeakFEC 0

0367: 2014-06-18 10:31:28 - 033 - ODU TX LOS - Set

0368: 2014-06-18 10:31:29 - 049 - Tx ACM profile was changed - [256QAM]

0369: 2014-06-18 10:31:29 - 033 - ODU TX LOS - Reset

0370: 2014-06-18 10:31:31 - 049 - Tx ACM profile was changed - [256QAM]

0371: 2014-06-18 10:31:37 - 057 - Command from interface - TASK> net ping 192.168.205.11

0372: 2014-06-18 10:31:59 - 057 - Command from interface - TASK> modem standard etsi

0373: 2014-06-18 10:31:59 - 057 - Command from interface - TASK> modem set 56000 256QAM 256QAM WeakFEC 0

0374: 2014-06-18 10:32:01 - 033 - ODU TX LOS - Set

0375: 2014-06-18 10:32:02 - 033 - ODU TX LOS - Reset

0376: 2014-06-18 10:32:10 - 057 - Command from interface - TASK> net ping 192.168.205.11

0377: 2014-06-18 10:32:20 - 057 - Command from interface - WEB> odu txmute off

0378: 2014-06-18 10:32:21 - 057 - Command from interface - TASK> odu txsp 0

0379: 2014-06-18 10:32:21 - 057 - Command from interface - TASK> odu txfreq 17728000

0380: 2014-06-18 10:32:29 - 057 - Command from interface - TASK> net ping 192.168.205.11

0381: 2014-06-18 10:33:20 - 057 - Command from interface - TASK> modem standard etsi

0382: 2014-06-18 10:33:20 - 057 - Command from interface - TASK> modem set 56000 4QAM 256QAM WeakFEC 0

0383: 2014-06-18 10:33:22 - 031 - Acquire status alarm - [ACQUIRE_LOCKED]-> Reset

0384: 2014-06-18 10:33:23 - 032 - Last acquire error status - [ACQUIRE_SUCCESS]-> Reset

0385: 2014-06-18 10:33:23 - 043 - Command from interface - WEB> modem set 30000 256QAM 256QAM WeakFEC 0

0386: 2014-06-18 10:33:26 - 035 - ACM profile was changed - [256QAM]

End

|<

Previous 21

386

Next 21

>|

Filter: none

> Alarm-event log file <

Clear alarm log

Figure 5.3 Alarm log window

5.1.5 Alarm and Alarm Threshold Configuration

The alarm configuration screen allows you to configure alarm representation. You have a choice to see specific alarm groups globally in alarm status (**Global**), in alarm log (**Log**) or in NMS system (**SNMP**). AUX allows choosing one of four available alarm outputs.

Alarm & log configuration	Global	Log	SNMP	AUX
[1] ==> System Start	☒	☒	☐	None ▾
[2] Invalid device license	☒	☒	☒	None ▾
[3] License expired	☒	☒	☒	None ▾
[4] License will soon expire	☒	☒	☒	None ▾
[5] Log was Cleared	☒	☒	☒	None ▾
[6] Log ERROR	☒	☒	☒	None ▾
[7] Log TEST	☒	☒	☒	None ▾
[8] Counters was Cleared	☒	☒	☐	None ▾
[9] Config was Written	☒	☒	☒	None ▾
[10] System CPU restart ==>	☒	☒	☒	None ▾
[11] No data from IDU temperature sensor	☒	☒	☒	None ▾
[12] IDU temperature fault	☒	☒	☒	None ▾
[13] No data from main PSU IDU ADC	☒	☒	☒	None ▾
[14] Main supply 48V failure	☒	☒	☒	None ▾
[15] IDU PSU state	☒	☒	☒	None ▾
[16] No data from main PSU ODU ADC	☒	☒	☒	None ▾
[17] IDU PSU to ODU state	☒	☒	☒	None ▾
[18] No data from PSU temperature sensor	☒	☒	☒	None ▾
[19] PSU temperature fault	☒	☒	☒	None ▾
[20] Main 3,3V PSU failure	☒	☒	☒	None ▾
[21] No data from power supply ADC	☒	☒	☒	None ▾
[22] Power supply voltage failure	☒	☒	☒	None ▾
[23] No data from RADIO	☒	☒	☒	1 ▾
[24] Rx level alarm	☒	☒	☒	None ▾
[25] Tx PLL error alarm	☒	☒	☒	None ▾
[26] Rx PLL error alarm	☒	☒	☒	None ▾
[27] ODU Temperature failure	☒	☒	☒	None ▾
[28] ODU RX LOS	☒	☒	☒	None ▾
[29] ODU TX LOS	☒	☒	☒	None ▾
[30] ODU RX failure	☒	☒	☒	None ▾
[31] ODU TX failure	☒	☒	☒	None ▾
[32] ODU Frequency failure	☒	☒	☒	None ▾
[33] ODU Tx mute	☒	☒	☒	None ▾
[34] ODU RF loopback	☒	☒	☒	None ▾
[35] No data from MODEM	☒	☒	☒	2 ▾
[36] Acquire status alarm	☒	☒	☒	2 ▾
[37] Last acquire error status	☒	☒	☒	2 ▾
[38] Radial MSE	☒	☒	☒	None ▾
[39] LDPC decoder stress	☒	☒	☒	None ▾
[40] Tx ACM profile was changed	☒	☒	☒	None ▾
[41] RX carrier offset	☒	☒	☒	None ▾
[42] No data from modem temperature sensor	☒	☒	☒	None ▾
[43] Modem temperature fault	☒	☒	☒	None ▾
[44] ATPC Tx power correction was changed	☒	☒	☒	None ▾
[45] Rollback initiate system CPU restart ==>	☒	☒	☒	None ▾
[46] System CPU reset was WDT initiated ==>	☒	☒	☒	None ▾
[47] PM log flash write error	☒	☒	☒	None ▾
[48] Event of command execution starting	☒	☒	☐	None ▾
[49] Message of event	☒	☒	☐	None ▾
[50] E1 interface	☒	☒	☒	None ▾
[51] Ethernet interface *	☒	☒	☒	None ▾
[52] AUX alarm in 1	☒	☒	☒	None ▾
[53] AUX alarm in 2	☒	☒	☒	None ▾
[54] AUX alarm in 3	☒	☒	☒	None ▾
[55] AUX alarm in 4	☒	☒	☒	None ▾
[56] No protection data from alternate	☒	☒	☒	None ▾
[57] Protection state was changed	☒	☒	☒	None ▾
[58] Aggregation state was changed	☒	☒	☒	None ▾
[59] Aggregation events	☐	☒	☒	None ▾
[60] Keepalive ethernet switch reset	☒	☒	☒	None ▾

System returned: Ok

Figure 5.4 Alarm configuration window

Alarm threshold configuration screen allows you to define specific threshold levels to bound alarms to desirable values, so that you are able to adapt alarm system to your individual needs.

Alarms in bold font represent group alarms and alarms in normal font – individual alarms.

Alarm threshold configuration						
Set all fields to default				Set all to default		
Alarm ID	Alarm name	Low value	High value	Delta value	Current value	Default value
12	IDU temperature fault	-5.0 C	85.0 C	1.0 C	44.5 C	☒
14	Main supply voltage failure	36.00 V	57.00 V	1.00 V	47.00 V	☒
19	PSU temperature fault	-5.0 C	85.0 C	1.0 C	46.0 C	☒
22	1,0V failure	0.85 V	1.15 V	0.03 V	0.98 V	☒
23	1,2V failure	1.15 V	1.32 V	0.03 V	1.20 V	☒
24	1,5V failure	1.43 V	1.57 V	0.03 V	1.49 V	☒
25	2,5V failure	2.40 V	2.70 V	0.03 V	2.50 V	☒
26	3,3V failure	3.15 V	3.60 V	0.03 V	3.31 V	☒
27	Main 3,3V failure	3.15 V	3.60 V	0.03 V	3.42 V	☒
28	5,0V failure	4.50 V	5.50 V	0.03 V	5.25 V	☒
30	Rx level alarm	-80.0 dBm	-30.0 dBm	1.0 dB	-50.3 dBm	☒
41	ODU Temperature fault	-33.0 C	85.0 C	1.0 C	44.0 C	☒
47	Radial MSE		-9.6 dB	1.0 dB	-31.3 dB	☒
48	LDPC decoder stress		1.0e-03		7.3e-05	☒
50	RX carrier offset	-700 kHz	700 kHz	10 kHz	4 kHz	☒
52	Modem temperature fault	-5.0 C	95.0 C	1.0 C	60.0 C	☒
Execute configuration						
Write to config file						
System returned:				Ok		

Figure 5.5 Alarm threshold configuration window

5.1.6 Alarm Management Commands

To manage alarms in command prompt, the commands are as follows:

Alarm management commands	
Command	Description
Log show [<start line>]	The management controller maintains event log, - events include configuration changes, management controller restarts, and local site alarm changes. The “log show” or “log” commands display the latest 20 log entries, the log entries are numbered, - entry with the largest number is the latest event. The “log show” command can be followed up with an entry number to display the latest 20 entries beginning from the entry specified by the number, e.g., “log show 100” will display entries 100...120.

Alarm management commands	
Command	Description
Log filter <alarm ID> [<num>]	Filters event list by specific alarm ID. <start line> ; works similarly to 'log show' command.
Log file <file name>	Makes event log file with specified filename.
Alarm stat	Lists alarm groups currently set.
Alarm list	Displays the list of all alarms, their group IDs and alarm IDs.
Alarm groups	Displays the list of all alarms and their group IDs.
Alarm cfg <group ID> [<global> <led> <aux> <log> <snmp>]	Allows defining detailed alarm representation settings. [<global> <led> <aux> <log> <snmp>] must be defined in a row of '1's or '0's of 5 values for specified group ID with <group ID>. '1' means the values are 'on' and '0' – 'off'.
Alarm threshold {stat} {<Alarm ID> lo hi delta <value>}	Sets threshold values outside which alarm status will be shown.

5.2 Performance Management

The main aim of the *performance management* is to register mostly critical device performance event values in predefined time intervals.

5.2.1 Performance Management Data Collection

The performance parameters are collected within time intervals of 1 min., 15 min. and 1 hour. List reserved space for every time interval is 1440 records (see **Figure 5.6**).

Second-by-second the input performance event values are stored by updating previous second values. The register is called *current register*. The *current register* contains the performance values collected second-by-second from the reset instant to the present second.

At the end of period the contents of current registers are transferred to the history registers (records), with a time-date stamp to identify the period, after which the current register must be reset.

Some current register values are passed to the threshold crossing control unit for triggering threshold crossing notification.

Optionally, the same values are output to the Message Communication Function (MCF) to be forwarded to the managing system.

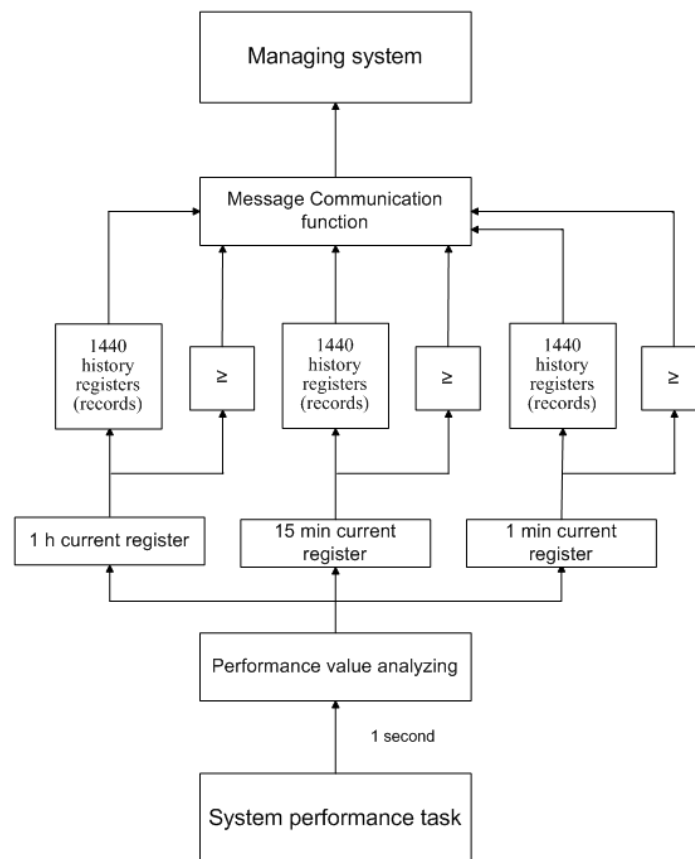


Figure 5.6 Functional architecture for data collection, history and thresholding treatment

5.2.2 Performance Values

Threshold Seconds (TS)

The TS is defined as one second period during which the detected value is outside of predefined thresholds. The current value of the counter associated with TS should be readable by the managing system on request. In case a threshold associated to TS counter is changed, the current value of the counter should be reset to zero.

Tide Mark (TM)

The TM is a mechanism that records the maximum and the minimum value reached during measurement period. The tide mark values are automatically reset to the current value assumed at the beginning of each measurement period. The TM is therefore composed of two values: the minimum and the maximum value. Comparison between the current value and the minimum and maximum values is performed on a second basis.

5.2.3 Performance Management in Web GUI

The main performance management tool in the CFIP Phoenix is Web interface, allowing user to review performance measurements in a very convenient and visualized way.

Going to 'Performance → Performance log' in navigation panel on the left side of the Web GUI window will lead you to the log parameters' selection screen, where you will be able to choose between 10 different parameters to display in summarizing performance log or pick 'ALL' to display all 10 parameters in conjoint log which is shown in **Figure 5.7**.

Performance log field selection

Select objects to display

- ☒ ALL
- ☒ Uptime
- ☒ Rx level
- ☒ Tx level
- ☒ IDU temperature
- ☒ ODU temperature
- ☒ Modem temperature
- ☒ Radial MSE
- ☒ LDPC decoder stress
- ☒ PSU input voltage
- ☒ PSU consumed power

Save&Proceed

Performance log file download: **1 min interval / 15 min interval / 60 min interval**

Figure 5.7 Selecting performance log parameters

Performance log																														
Nr	Date	Time	Radio						IDU/System						Modem						Power supply unit									
			Rx level			Tx level			Temperature, C			Uptime	Temperature, C			Radial MSE	LDPC decoder stress			Temperature, C			Input voltage, V			Consumed power, W				
			Min	Max	TS	Min	Max	TS	Min	Max	TS		Min	Max	TS		Min	Max	TS	Min	Max	TS	Min	Max	TS	Min	Max	TS		
1419	11-08-01	15:53	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:24:08	48.5	49.0	0	-31.6	-31.5	0	1.4e-05	2.6e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1420	11-08-01	15:54	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:25:08	48.5	48.5	0	-31.6	-31.5	0	1.2e-05	2.9e-05	0	61.0	61.0	0	47.00	47.00	0	33.69	33.99	0
1421	11-08-01	15:55	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:26:08	48.5	48.5	0	-31.6	-31.5	0	1.2e-05	2.5e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1422	11-08-01	15:56	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:27:08	48.5	49.0	0	-31.6	-31.5	0	1.1e-05	2.4e-05	0	61.0	61.0	0	47.00	47.00	0	33.62	33.99	0
1423	11-08-01	15:57	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:28:08	48.5	49.0	0	-31.6	-31.5	0	1.4e-05	2.6e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1424	11-08-01	15:58	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:29:08	48.5	49.0	0	-31.6	-31.5	0	1.2e-05	2.4e-05	0	61.0	61.0	0	47.00	47.00	0	33.62	33.99	0
1425	11-08-01	15:59	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:30:08	48.5	49.0	0	-31.6	-31.5	0	1.3e-05	2.5e-05	0	61.0	61.0	0	47.00	47.00	0	33.69	33.99	0
1426	11-08-01	16:00	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:31:08	48.5	49.0	0	-31.6	-31.5	0	1.2e-05	2.7e-05	0	61.0	61.0	0	47.00	47.00	0	33.69	33.99	0
1427	11-08-01	16:01	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:32:08	48.0	48.5	0	-31.6	-31.5	0	1.2e-05	2.7e-05	0	61.0	61.0	0	47.00	47.00	0	33.69	33.99	0
1428	11-08-01	16:02	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:33:08	48.0	48.5	0	-31.6	-31.5	0	1.2e-05	2.6e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1429	11-08-01	16:03	-43	-43	0	0	0	0	36.0	37.0	0	2 days 23:34:08	48.0	48.5	0	-31.6	-31.5	0	1.3e-05	2.8e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1430	11-08-01	16:04	-43	-43	0	0	0	0	36.0	37.0	0	2 days 23:35:08	47.5	48.0	0	-31.6	-31.5	0	1.2e-05	2.5e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1431	11-08-01	16:05	-43	-43	0	0	0	0	36.0	37.0	0	2 days 23:36:08	47.5	48.0	0	-31.6	-31.5	0	1.0e-05	2.9e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1432	11-08-01	16:06	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:37:08	48.0	48.0	0	-31.6	-31.5	0	1.1e-05	3.1e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1433	11-08-01	16:07	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:38:08	48.0	48.5	0	-31.6	-31.5	0	1.3e-05	2.5e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	34.06	0
1434	11-08-01	16:08	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:39:08	48.5	48.5	0	-31.6	-31.5	0	1.1e-05	2.6e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1435	11-08-01	16:09	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:40:08	48.5	48.5	0	-31.6	-31.5	0	1.1e-05	2.7e-05	0	61.0	61.0	0	47.00	47.00	0	33.69	33.99	0
1436	11-08-01	16:10	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:41:08	48.5	48.5	0	-31.6	-31.5	0	1.4e-05	2.9e-05	0	61.0	61.0	0	47.00	47.00	0	33.69	33.99	0
1437	11-08-01	16:11	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:42:08	48.5	48.5	0	-31.6	-31.5	0	1.2e-05	2.7e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1438	11-08-01	16:12	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:43:08	48.5	48.5	0	-31.6	-31.5	0	1.2e-05	2.3e-05	0	61.0	61.0	0	47.00	47.00	0	33.77	33.99	0
1439	11-08-01	16:13	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:44:08	48.5	49.0	0	-31.6	-31.5	0	1.2e-05	2.6e-05	0	61.0	61.0	0	47.00	47.00	0	33.69	33.99	0
1440	11-08-01	16:14	-43	-43	0	0	0	0	37.0	37.0	0	2 days 23:45:08	48.5	49.0	0	-31.6	-31.5	0	1.4e-05	2.3e-05	0	61.0	61.0	0	47.00	47.00	0	33.62	33.99	0
Select time interval: 1 Min Start date: Start time: End date: End time: Show																														
< Previous Next >																														
Clear performance log																														

Figure 5.8 Performance log window

Time interval can be chosen between 1 min, 15 min or 1 hr. You can also define the start time and the start date. When start values are defined, it is also possible to define the end time and the end date.

TS (threshold seconds) show the amount of seconds in a chosen period (1min, 15min or 1h) when the parameter has been out of bounds set by performance thresholds in 'Configuration → Performance log configuration'.

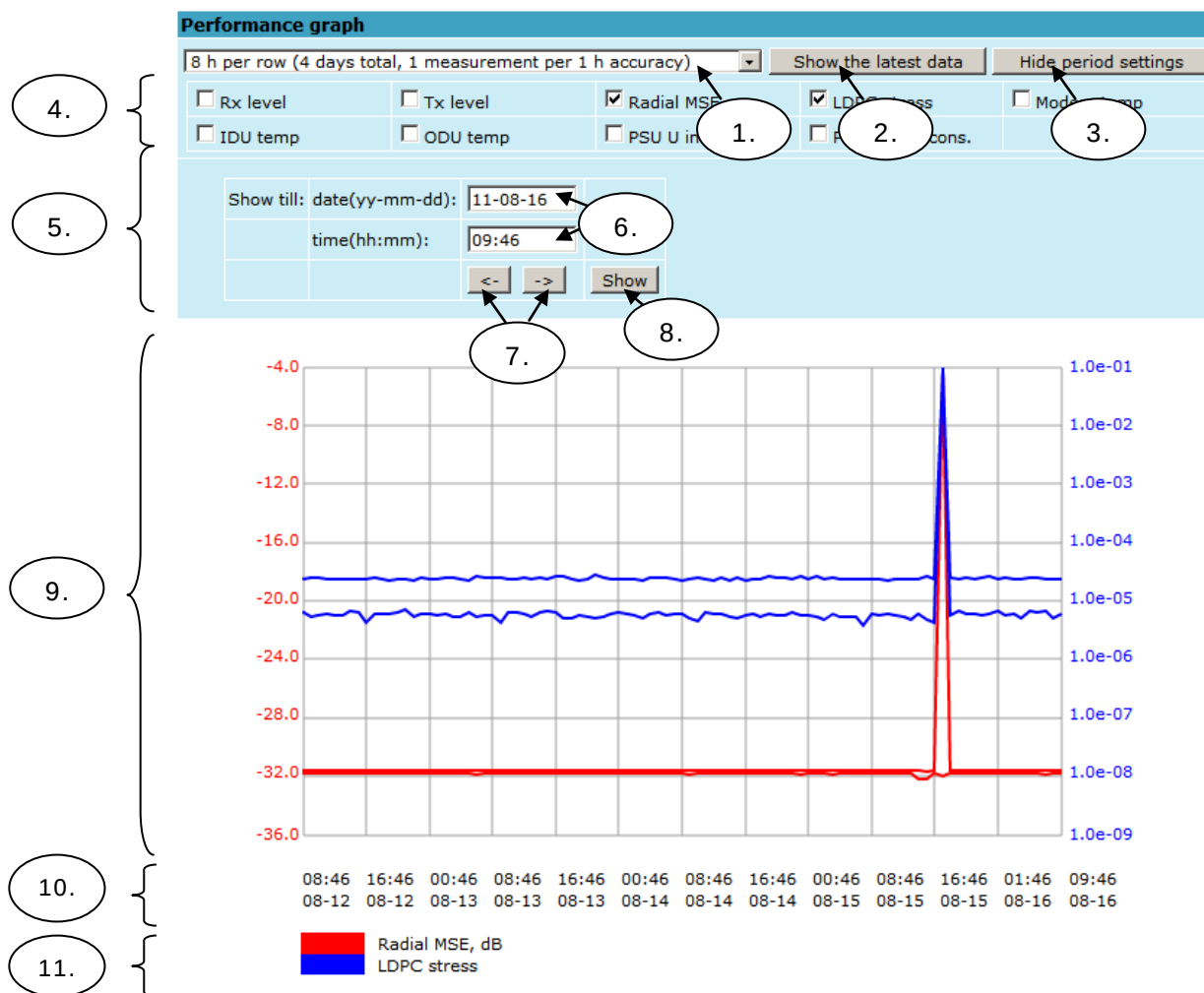
To define thresholds from where TS (threshold seconds) will be counted, you must go to 'Configuration → Performance log configuration' and enter preferable threshold values. Refer to Chapters 5.2.1 and 5.2.2 for further details on threshold seconds.

Performance log configuration					
☐ All to default					
Rx level	min (-120)	-90 dBm	max (-20)	-30 dBm	☐ auto
Tx level	min (-30)	-30 dBm	max (40)	35 dBm	☐ auto
IDU temperature	min (-10)	-5.0 C	max (70)	+55.0 C	☐ auto
ODU temperature	min (-50)	-33.0 C	max (90)	+85.0 C	☐ auto
Modem temperature	min (-50)	-33.0 C	max (90)	+85.0 C	☐ auto
Radial MSE			max (-10)	-12.0 dB	☐ auto
LDPC decoder stress			max (1)	5.0e-03	☐ auto
PSU input voltage	min (35)	40.00 V	max (60)	50.00 V	☐ auto
PSU consumed power	min (1)	5.00 W	max (55)	40.00 W	☐ auto
					Execute configuration
					Write to config file
System returned:		Ok			

Figure 5.9 Performance log configuration window

The main advantage in terms of demonstration means is obtained from 'Performance graphs', which are found in 'Performance → Performance graph' section.

You are able to choose between 9 parameters – Rx level; Tx level; Radial MSE; LDPC stress; Modem temperature; IDU temperature; ODU temperature; PSU input voltage and PSU power consumption – and to view their graphs. It is possible to choose between 8 scales – from 12 last minutes to the maximum of 6 last days to be displayed in the graph. It is also possible to choose time period to be displayed, defining date and time till which the graph will be shown.



If you cannot see the graph, click here to install an SVG viewer from <http://www.adobe.com/svg/viewer/install/>

Figure 5.10 Performance graph showing system temperature and Rx level in period of last 6 hours

1. Time scale selector. User can select the scale and accuracy (1 / 15 / 60 minutes). The lower accuracy, the longer the period available for data (mechanism of the performance management system)
2. Updates the performance graph; the latest data is shown
3. Shows / hides period settings (point 5)
4. Performance data selector. Only two performance parameters can be selected at a time
5. Period settings. Allows the user to specify time period for the graph
6. Date and time fields. The date format is "yy-mm-dd", the time format is "hh:mm"
7. Sets date and time fields (point 6) one screen back / forth
8. Shows / updates the performance graph using the period settings (point 5)
9. Performance graph. Displays two performance parameters. Each parameter is shown with the minimum and maximum curves, which are in the same color. The curves in red have the scale on the left, while the curves in blue have the scale on the right
10. Time scale. Shows the time scale chosen from the time scale selector (point 1) for the performance data available. If no data is available for the according moment, "___:___" is shown
11. Legend for the curves of the performance graph. Contains the color, the name and the unit of measurement, if available.

In case no performance data has been recorded, or the period specified has no data, "No data" is shown (instead of points 9, 10, 11).

5.2.4 Adaptive Equalizer

CFIP Phoenix features adaptive equalizer, which is a filter that automatically adapts to time-varying properties of a communication channel with selective fading, having a target to compensate the inequalities in frequency response, mitigating the effects of multipath propagation. In wireless telecommunications, using QAM modulation this filter equalizes not only a separate quadrature channel, but provides a cancellation of cross-interference between them.

In current CFIP device an adaptive equalizer is realized as complex-arithmetic 24-taps digital FIR (Finite Impulse Response) filter. In other words, equalizer is a selective frequency amplifier and attenuator, a device, which application to IF (Intermediate Frequency) band-limited signal is schematically shown in the picture below:

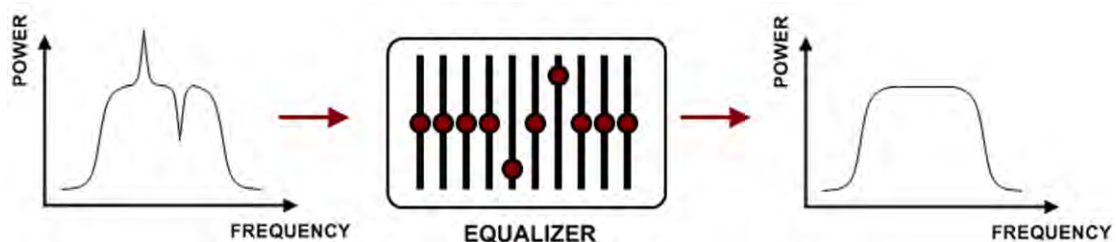


Figure 5.11 Equalizer operation

Equalizer graph window shows adaptive equalizer taps' coefficients, which at a set time moment minimize multipath fading effect in channel.

Example of equalizer taps' coefficients and its frequency response in case of a normal operation is shown below:

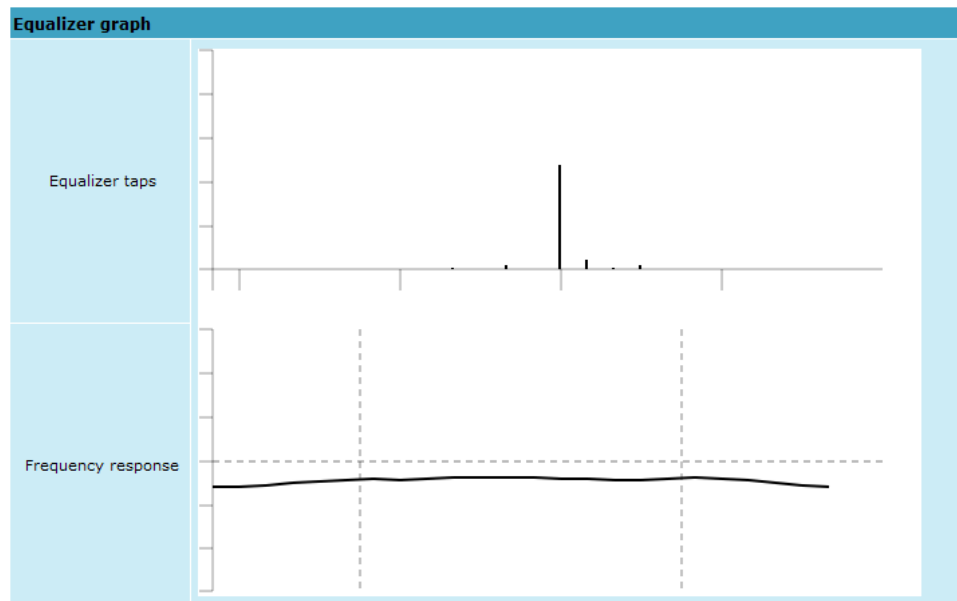


Figure 5.12 Equalizer graph – normal operation

During normal operation frequency response curve is smooth and the only equalizer tap towers are in the centre of equalizer taps graph, otherwise frequency response curve will appear jagged and many equalizer taps will become visible. The latter case most probably will indicate to multipath issue, which must be inspected with use of precise and accurate path profiling. An example of multipath caused equalization is shown on the picture below. Taps mainly on the right side designate a weaker reflected signal in comparison with the main signal.

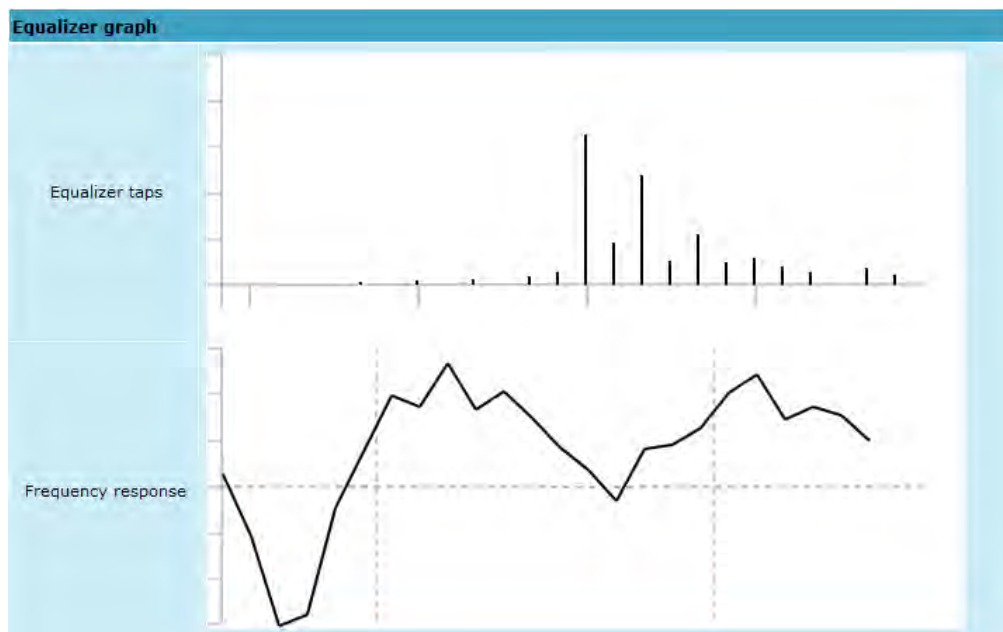


Figure 5.13 Equalizer graph – multipath

5.2.5 Performance Management Commands

It is also possible to view performance log in command prompt.

The list of available commands is the following:

Additional performance management commands in Telnet/serial interface	
Command	Description
pm log <interval> <last rec count> <start date> <start time> <end date> <end time>}}	Lists performance management log with selected <interval> of 1min, 15min or 1hr. Allows choosing the number of last records to be shown (<last rec count>) or to define start and end time and date. Note that end time and date values must be entered after entering start time or date respectively.
pm select {Up_TIME . Rx_LEVEL . Tx_LEVEL . RADIAL_MSE . LDPC_STRES . MOD_TEMPER . IDU_TEMPER . ODU_TEMPER . PSU_U_IN . PSU_POW.} {ALL NOT}	Allows selecting the system parameters to be monitored and shown in the performance management log.
pm logclear	Clears performance log.
pm threshold stat auto {{/Rx_LEVEL Tx_LEVEL RADIAL_MSE LDPC_STRES MOD_TEMPER IDU_TEMPER ODU_TEMPER PSU_U_IN PSU_POW} {min max <value>} auto }	Sets threshold levels for parameters from where TS (Threshold Seconds) are counted and shown in the performance log.

5.3 Ethernet modem statistics

Ethernet modem statistics window shows the full Ethernet and framing statistics of CFIP modem since unit start or statistics reset. All statistics are also accessible using command prompt command **ethernet statistics all**.

Explanation of fields:

Ethernet modem statistics			
Statistics for 1 day 22:40:03		1	
Modem state		Ok	2
		3	Clear statistics
Name	Rx	Name	Tx
Truncated frames	4 0	Vlan tags	26 0
Log events	5 0	Backpres. events	27 0
Vlan tags detected	6 0	Pause frames	28 0
Unsup. opcodes	7 0	Control frames	29 0
Pause frames	8 0	Wire byte counter	30 3357985167
Control frames	9 0	Underruns	31 0
Dribble nibbles	10 0	Giants	32 0
Broadcasts	11 11036	Late collisions	33 0
Multicasts	12 11054	Max collisions	34 0
Dones	13 21245712	Excessive defers	35 0
Jumbo frames	14 0	Non-exc. defers	36 0
Length check errors	15 0	Broadcasts	37 21383
CRC errors	16 0	Multicasts	38 21437
Code errors	17 0	Dones	39 21282030
False carrier errors	18 0	Length check errors	40 0
Rx Dv event	19 0	CRC errors	41 0
Prev. pkt dropped	20 0	Collisions	42 0
Byte counter	21 3364556166	Byte counter	43 3357985167
Name	GFP	Name	QoS
FCS errors	22 0	Rx Q1 frames	44 21245712
CHEC errors	23 0	Rx Q1 dropped	45 0
Dropped frames	24 0	Rx Q2 frames	46 0
Delineation errors	25 0	Rx Q2 dropped	47 0
		Tx frames	48 21282031
		Tx dropped	49 0

Figure 5.14 Ethernet modem statistics

- Shows the time during which statistics have been gathered;

2. *Modem state* – shows if the modem is operating correctly;
3. *Clear statistics* – resets all statistics counters (not available for “guest” account);
4. *Truncated frames* – number of truncated received frames;
5. *Long events* – frames having byte count greater than MAXIMUM FRAME SIZE parameter (1518, 1536 or 1916 bytes);
6. *Vlan tags detected* – VLAN tagged frames;
7. *Unsup. opcodes* – frames recognized as control frames but contained an Unknown Opcode;
8. *Pause frames* – frames received are control frames with valid PAUSE opcodes;
9. *Control frames* – frames received as control frames;
10. *Dribble nibbles* – indicates that following the end of the packet additional 1 to 7 bits are received. A single nibble, named the dribble nibble, is formed but not sent to the system;
11. *Broadcasts* – packets, which destination address contained broadcast address;
12. *Multicasts* – packets, which destination address contains multicast address;
13. *Dones* – reception of packets successfully completed;
14. *Jumbo frames* – frame Type/Length field larger than 1518 (Type Field) bytes;
15. *Length check errors* – frame length field in the packet does not match the actual data byte length and is not a Type Field;
16. *CRC errors* – frame CRC do not match the internally generated CRC;
17. *Code errors* – one or more nibbles are signalled as errors during reception of the packet;
18. *False carrier errors* – indicates that following the last received statistics vector, a false carrier was detected, noted and reported with next received statistics. The false carrier is not associated with this packet. False carrier is activated on the receiving channel that does not result in a packet receive attempt being made;
19. *Rx Dv event* – indicates that the last receiving event seen is too short to be a valid packet;
20. *Prev. pkt dropped* – indicates that since the last RSV, a packet is dropped (i.e. interframe gap too small);
21. *Byte counter* – total number of bytes received on the wire, not counting collided bytes;
22. *FCS errors* – number of generic framing procedure (GFP) frames with CRC errors received by the de-encapsulation block;
23. *CHEC errors* – number of generic framing procedure (GFP) frames with CHEC errors received by the de-encapsulation block;
24. *Dropped frames* – number of generic framing procedure (GFP) frames that were dropped in the de-encapsulation block;
25. *Delineation errors* – number of ‘loss of synchronization’ events;
26. *Vlan tags* – number of VLAN tagged packets, 32-bit counter;
27. *Backpres. events* – carrier-sense-method backpressure was previously applied;
28. *Pause frames* – frames transmitted are control frames with a valid PAUSE opcodes;
29. *Control frames* – frames transmitted are control frames;
30. *Wire byte counter* – total number of bytes transmitted on the wire, including all bytes from collided attempts;
31. *Underruns* – underruns occur during frame transmission;
32. *Giants* – frames having byte count greater than the MAXIMUM FRAME SIZE parameter (1516, 1536 or 1916 bytes);
33. *Late collisions* – Collisions occurred beyond the collision window (512 bit times);
34. *Max collisions* – packets aborted after number of collisions exceeded the RETRANSMISSION MAXIMUM parameter;

- 35. *Excessive defers* – packets deferred in excess of 6,071 nibble times in 100 Mbps mode, or 24,287 bit-times in 10 Mbps mode;
- 36. *Non-exc. defers* – packets deferred for at least one attempt, but less than an excessive defer;
- 37. *Broadcasts* – packets, which destination address contained broadcast address;
- 38. *Multicasts* – packets, which destination address contained multicast address;
- 39. *Dones* – transmission of packets successfully completed;
- 40. *Length check errors* – frame length field in the packet does not match the actual data byte length and is not a Type Field;
- 41. *CRC errors* – frame CRC do not match the internally generated CRC;
- 42. *Collisions* – number of collisions the current packet incurred during transmission attempts;
- 43. *Byte counter* – total count of bytes transmitted on the wire not including collided bytes;
- 44. *Rx Q1 frames* – number of frames received on Q1;
- 45. *Rx Q1 dropped* – number of frames dropped on Q1;
- 46. *Rx Q2 frames* – number of frames received on Q2;
- 47. *Rx Q2 dropped* – number of frames dropped on Q2;
- 48. *Tx frames* – number of frames passed through TX FIFO;
- 49. *Tx dropped* – number of frames dropped in TX FIFO.

5.4 Ethernet switch statistics

Ethernet switch statistics window shows the full Ethernet statistics of CFIP switch since unit start or statistics reset. All statistics are also accessible using command prompt command ***ethernet counters*** <1|2|3|4|5|6|All|Clear>.

Explanation of fields:

Ethernet switch statistics

Statistics for 2 days 20:14:49

Clear statistics

Value	LAN 1	LAN 2	LAN 3	LAN 4	WAN	MNG
TxOctets	0	43777391	0	0	583372487	553022860
TxDropPkts	0	0	0	0	0	0
TxQ0PKT	0	195071	0	0	3660037	3467434
TxBroadcastPkts	0	1295	0	0	4604	4782
TxMulticastPkts	0	0	0	0	50	0
TxUnicastPkts	0	193776	0	0	3655383	3462652
TxCollisions	0	0	0	0	0	0
TxSingleCollision	0	0	0	0	0	0
TxMultiCollision	0	0	0	0	0	0
Transmit	0	0	0	0	0	0
TxLateCollision	0	0	0	0	0	0
TxExcessiveCollision	0	0	0	0	0	0
TxFrameInDiscards	0	0	0	0	0	0
TxPausePkts	0	0	0	0	0	0
TxQ1PKT	0	0	0	0	0	0
TxQ2PKT	0	0	0	0	0	0
TxQ3PKT	0	0	0	0	0	0
RxOctets	0	42115998	0	0	587213552	550289572
RxUndersizePkts(runts)	0	0	0	0	0	0
RxPausePkts	0	0	0	0	0	0
RxPkts64Octets	0	128455	0	0	57930	821
RxPkts64to127Octets	0	68571	0	0	1766003	1719640
RxPkts128to255Octets	0	349	0	0	1776370	1726998
RxPkts256to511Octets	0	381	0	0	0	7342
RxPkts512to1023Octets	0	45293	0	0	0	10
RxPkts1024to1522Octets	0	6	0	0	18903	253
RxOversizePkts	0	0	0	0	0	0
RxJabbers	0	0	0	0	0	0
RxAlignmentErrors	0	0	0	0	0	0
RxFCSErrors	0	0	0	0	0	0
RxGoodOctets	0	42115998	0	0	587213552	550289572
RxDropPkts	0	0	0	0	0	0
RxUnicastPkts	0	238967	0	0	3618462	3454498
RxMulticastPkts	0	50	0	0	0	0
RxBroadcastPkts	0	4038	0	0	744	566
RxSACChanges	0	0	0	0	0	0
RxFragments	0	0	0	0	0	0
RxExcessSizeDisc	0	0	0	0	0	0
RxSymbolError	0	0	0	0	0	0
RxPkts1523to2047Octets	0	0	0	0	0	0
RxPkts2048to4095Octets	0	0	0	0	0	0
RxPkts4096to8191Octets	0	0	0	0	0	0
RxPkts8192to9728Octets	0	0	0	0	0	0
RxDiscard	0	0	0	0	0	0

Figure 5.15 Ethernet switch statistics

1. Shows the time during which statistics have been gathered;
2. *Clear statistics* – resets all statistics counters (not available for “guest” account);
3. *TxOctets* - The total number of good bytes of data transmitted by a port (excluding preamble but including FCS);
4. *TxDropPkts* - This counter is incremented every time a transmit packet is dropped due to lack of resources (e.g., transmit FIFO underflow), or an internal MAC sublayer transmit error not counted by either the TxLateCollision or the TxExcessiveCollision counters;
5. *TxQOPKT* - The total number of good packets transmitted on COS0, which is specified in MIB queue select register when QoS is enabled;
6. *TxBroadcastPkts* - The number of good packets transmitted by a port that are directed to a broadcast address. This counter does not include errored broadcast packets or valid multicast packets;
7. *TxMulticastPkts* - The number of good packets transmitted by a port that are directed to a multicast address. This counter does not include errored multicast packets or valid broadcast packets;

8. *TxUnicastPkts* - The number of good packets transmitted by a port that are addressed to a unicast address;
9. *TxCollisions* - The number of collisions experienced by a port during packet transmissions;
10. *TxSingleCollision* - The number of packets successfully transmitted by a port that have experienced exactly one collision;
11. *TxMultiCollision* - The number of packets successfully transmitted by a port that have experienced more than one collision;
12. *TxDeferred Transmit* - The number of packets transmitted by a port for which the first transmission attempt is delayed because the medium is busy. This only applies to the Half Duplex mode, while the Carrier Sensor Busy;
13. *TxLateCollision* - The number of times that a collision is detected later than 512 bit-times into the transmission of a packet;
14. *TxExcessiveCollision* - The number of packets that are not transmitted from a port because the packet experienced 16 transmission attempts;
15. *TxFramelnDiscards* – The number of valid packets received which are discarded by the forwarding process due to lack of space on an output queue (not maintained or reported in the MIB counters). This attribute only increments if a network device is not acting in compliance with a flow control request, or the sum of the drop count when the packet is dropped on the flow control;
16. *TxPausePkts* - The number of PAUSE events at each port;
17. *TxQ1PKT* – The total number of good packets transmitted on COS1, which is specified in MIB queue select register when QoS is enabled;
18. *TxQ2PKT* – The total number of good packets transmitted on COS2, which is specified in MIB queue select register when QoS is enabled;
19. *TxQ3PKT* - The total number of good packets transmitted on COS3, which is specified in MIB queue select register when QoS is enabled;
20. *RxOctets* - The number of data bytes received by a port (excluding preamble, but including FCS), including bad packets;
21. *RxUndersizePkts(runts)* - The number of good packets received by a port that are less than 64 bytes long (excluding framing bits, but including the FCS);
22. *RxPausePkts* - The number of PAUSE frames received by a port;
23. *RxPkts64Octets* - The number of received packets (including error packets) that are 64 bytes long;
24. *RxPkts65to127Octets* - The number of received packets (including error packets) that are between 65 and 127 bytes long;
25. *RxPkts128to255Octets* - The number of received packets (including error packets) that are between 128 and 255 bytes long;
26. *RxPkts256to511Octets* - The number of received packets (including error packets) that are between 256 and 511 bytes long;
27. *RxPkts512to1023Octets* - The number of received packets (including error packets) that are between 512 and 1023 bytes long;
28. *RxPkts1024to1522Octets* - The number of received packets (including error packets) that are between 1024 and 1522 bytes long;
29. *RxOversizePkts* - The number of good packets received by a port that are greater than 1522 bytes (tagged) and 1518 bytes (untagged). This counter alone is incremented for packets in the range 1523–1536 bytes inclusive, whereas both this counter and the *RxExcessSizeDisc* counter are incremented for packets of 1537 bytes and higher;
30. *RxJabbers* – The number of packets received by a port that are longer than 1522 bytes and have either an FCS error or an alignment error;
31. *RxAlignmentErrors* - The number of packets received by a port that have a length (excluding framing bits, but including FCS) between 64 and 1522 bytes, inclusive, and have a bad FCS with a nonintegral number of bytes;

- 32. *RxFCSErrors* – The number of packets received by a port that have a length (excluding framing bits, but including FCS) between 64 and 1522 bytes inclusive, and have a bad FCS with an integral number of bytes;
- 33. *RxGoodOctets* – The total number of bytes in all good packets received by a port (excluding framing bits, but including FCS);
- 34. *RxDropPkts* - The number of good packets received by a port that were dropped due to a lack of resources (e.g., lack of input buffers) or were dropped due to a lack of resources before a determination of the validity of the packet was able to be made (e.g., receive FIFO overflow). The counter is only incremented if the receive error was not counted by the *RxExcessSizeDisc*, the *RxAlignmentErrors*, or the *RxFCSErrors* counters;
- 35. *RxUnicastPkts* – The number of good packets received by a port that are addressed to a unicast address;
- 36. *RxMulticastPkts* – The number of good packets received by a port that are directed to a multicast address. This counter does not include errored multicast packets or valid broadcast packets;
- 37. *RxBroadcastPkts* – The number of good packets received by a port that are directed to the broadcast address. This counter does not include errored broadcast packets or valid multicast packets;
- 38. *RxSACHanges* – The number of times the SA of good receive packets has changed from the previous value. A count greater than 1 generally indicates the port is connected to a repeater-based network.
- 39. *RxFragments* – The number of packets received by a port that are less than 64 bytes (excluding framing bits) and have either an FCS error or an alignment error;
- 40. *RxExcessSizeDisc* – The number of good packets received by a port that are greater than 1536 bytes (excluding framing bits but including the FCS) and were discarded due to excessive length. The *RxOversizePkts* counter alone is incremented for packets in the range 1523–1536 bytes inclusive, whereas both this counter and the *RxOversizePkts* counter are incremented for packets of 1537 bytes and higher;
- 41. *RxSymbolError* – The total number of times a valid-length packet was received at a port and at least one invalid data symbol was detected. The counter only increments once per carrier event and does not increment on detection of a collision during the carrier event;
- 42. *RxPkts1523to2047Octets* – The number of received packets (including error packets) that are between 1523 and 2047 bytes long;
- 43. *RxPkts2048to4095Octets* – The number of received packets (including error packets) that are between 2048 and 4095 bytes long;
- 44. *RxPkts4096to8191Octets* – The number of received packets (including error packets) that are between 4096 and 8191bytes long;
- 45. *RxPkts8192to9728Octets* - The number of received packets (including error packets) that are between 8192 and 9728bytes long;
- 46. *RxDiscard* - The number of good packets received by a port that were discarded by the Forwarding Process.

6 Miscellaneous Controls in Web Graphic User Interface

These controls are located in the Navigation Panel under the “Tools” item.

6.1 Ethernet/Configuration files

This section allows working with CFIP configuration script.

The management module has RAM and EEPROM chips on-board. When CFIP is booted up, bootstrap is loaded from the EEPROM into RAM. The bootstrap contains the parameters that were previously stored in EEPROM using **write** and/or **cfg write** commands. These parameters are stored in EEPROM in the form of script and during boot up, the script parameters are loaded into RAM. These parameters can be freely changed in run-time, - changing the data in RAM. If the CFIP is shut down without saving the current configuration (script) in EEPROM, the original configuration will be restored from EEPROM during next boot-up.

Example of script can be observed on the screenshot below.

The script can be edited:

- string can be added by simply entering required string (see Nr. 7 on the screenshot below) or by executing command in CLI or in the appropriate Web GUI section (the script will be supplemented with the new string or the instant string entry will be updated);
- string can be deleted by entering appropriate line number (see Nr. 2 on the screenshot below) or by using “**cfg delete** <string#>” in CLI.

The changes can be saved in EEPROM by pressing “Cfg write” button (see Nr. 3 on the screenshot below) or by entering “**cfg write**” command in CLI.

(!) Note! The parameters that are not specified in the configuration script will have their default values when the CFIP is restarted.

Explanation of customization fields:

Configuration (cfg & Ethernet) files																																																
CFG file																																																
Download configuration file	1		Download cfg file																																													
Upload configuration file	2	Choose File No file chosen	Upload cfg file																																													
3 Saved configuration file		4 Running configuration file																																														
<pre>01: net ip remaddr 192.168.205.11 02: net ip addr 192.168.205.10 03: net ip mask 255.255.255.0 04: net ip gw 255.255.255.255 05: modem ipremote off 06: modem set 56000 4QAM 256QAM WeakFEC 0 07: odu txsp 0 08: odu txfreq 17728000 09: atpc disable 10: system language RU 11: system language EN 12: web trace off 13: system name "SAF" 14: system location "1"</pre>		<pre>01: net ip remaddr 192.168.205.11 02: net ip addr 192.168.205.10 03: net ip mask 255.255.255.0 04: net ip gw 255.255.255.255 05: modem ipremote off 06: atpc disable 07: system language RU 08: system language EN 09: web trace off 10: system name "SAF" 11: system location "1" 12: odu txsp 0 13: odu txfreq 17728000 14: modem set 56000 4QAM 256QAM WeakFEC 0</pre>																																														
Delete entry number from running configuration file	5		Delete																																													
Advanced cfg file features																																																
Execute current configuration	6		Cfg run																																													
Input file name to backup cfg in system memory	7	cfg_backup	Cfg backup																																													
Input file name to restore cfg from system memory	8		Cfg restore																																													
Enter string, which you want to save in cfg	9		Cfg add																																													
Load factory configuration file	10		Cfg factory																																													
Ethernet configuration file																																																
Backup Ethernet configuration file	11	ethernet.bak	Backup Ethernet config file																																													
Download current Ethernet configuration to PC	12		Download Ethernet configuration																																													
Upload Ethernet configuration file	13	Choose File No file chosen	Upload Ethernet configuration																																													
Run/restore Ethernet configuration from file	14	ethernet.bak	Run Ethernet config file																																													
15 Saved configuration file		16 Running configuration file																																														
<pre>### Ethernet Configuration ### VLANs Ethernet VLAN 1 Port 1u 2u 3u 4u 5 6u ### VLAN configuration Ethernet VLAN Disable Ethernet VLAN doubletag Disable Ethernet VLAN doubletag tpid 9100 ### QoS configuration Ethernet QoS Queuing Weighted Ethernet QoS Queuing Weights 1 2 4 8 Ethernet QoS Queuing Selection 802.1p ### Ethernet QoS 802.1p map ### Ethernet QoS DSCP map ### Ethernet Rate limiting ### Ethernet Port Trunking Ethernet Trunking disable ### Ethernet Flowctrl Ethernet Flowctrl auto ### Spanning Tree Configuration Ethernet STP Port Disable 5 ### Instance 0 Ethernet STP Port PathCost 0 5 200000 ### Region Configuration ### STP Mode Configuration ### Link state propagation configuration ### Ethernet set connection speed</pre>		<pre>### VLANs Ethernet VLAN 1 Port 1u 2u 3u 4u 5 6u ### VLAN configuration Ethernet VLAN Disable Ethernet VLAN doubletag Disable Ethernet VLAN doubletag tpid 9100 ### QoS configuration Ethernet QoS Queuing Weighted Ethernet QoS Queuing Weights 1 2 4 8 Ethernet QoS Queuing Selection 802.1p ### Ethernet QoS 802.1p map ### Ethernet QoS DSCP map ### Ethernet Rate limiting ### Ethernet Port Trunking Ethernet Trunking disable ### Ethernet Flowctrl Ethernet Flowctrl auto ### Spanning Tree Configuration Ethernet STP Port Disable 5 ### Instance 0 Ethernet STP Port PathCost 0 5 200000 ### Region Configuration ### STP Mode Configuration ### Link state propagation configuration ### Ethernet set connection speed</pre>																																														
File system content																																																
<table border="1"> <thead> <tr> <th>Name</th> <th>Date</th> <th>Time</th> <th>Size</th> <th>Flags</th> </tr> </thead> <tbody> <tr> <td>28_32_NWB_2IPv4d.bin</td> <td>2014-05-06</td> <td>10:59:44</td> <td>7506 bytes</td> <td></td> </tr> <tr> <td>cfipidul63.elf.ezip</td> <td>2014-05-06</td> <td>11:00:16</td> <td>1209492 bytes</td> <td>Ec</td> </tr> <tr> <td>cfipidul65.elf.ezip</td> <td>2014-06-11</td> <td>13:36:34</td> <td>1297168 bytes</td> <td>Ec</td> </tr> <tr> <td>ethernet.bak</td> <td>2014-06-11</td> <td>13:38:30</td> <td>855 bytes</td> <td></td> </tr> <tr> <td>boot.ini</td> <td>2014-06-11</td> <td>15:03:00</td> <td>23 bytes</td> <td>Be</td> </tr> <tr> <td>PhoenixX_ODU_v2_18.h86</td> <td>2014-06-11</td> <td>17:11:08</td> <td>221528 bytes</td> <td></td> </tr> <tr> <td>lang.dat</td> <td>2014-06-13</td> <td>14:56:17</td> <td>139716 bytes</td> <td></td> </tr> <tr> <td>ethernet.cfg</td> <td>2014-06-13</td> <td>15:21:59</td> <td>789 bytes</td> <td></td> </tr> </tbody> </table>				Name	Date	Time	Size	Flags	28_32_NWB_2IPv4d.bin	2014-05-06	10:59:44	7506 bytes		cfipidul63.elf.ezip	2014-05-06	11:00:16	1209492 bytes	Ec	cfipidul65.elf.ezip	2014-06-11	13:36:34	1297168 bytes	Ec	ethernet.bak	2014-06-11	13:38:30	855 bytes		boot.ini	2014-06-11	15:03:00	23 bytes	Be	PhoenixX_ODU_v2_18.h86	2014-06-11	17:11:08	221528 bytes		lang.dat	2014-06-13	14:56:17	139716 bytes		ethernet.cfg	2014-06-13	15:21:59	789 bytes	
Name	Date	Time	Size	Flags																																												
28_32_NWB_2IPv4d.bin	2014-05-06	10:59:44	7506 bytes																																													
cfipidul63.elf.ezip	2014-05-06	11:00:16	1209492 bytes	Ec																																												
cfipidul65.elf.ezip	2014-06-11	13:36:34	1297168 bytes	Ec																																												
ethernet.bak	2014-06-11	13:38:30	855 bytes																																													
boot.ini	2014-06-11	15:03:00	23 bytes	Be																																												
PhoenixX_ODU_v2_18.h86	2014-06-11	17:11:08	221528 bytes																																													
lang.dat	2014-06-13	14:56:17	139716 bytes																																													
ethernet.cfg	2014-06-13	15:21:59	789 bytes																																													
There are currently 2877077 Bytes in 8 files in TFS																																																
Disk free space = 3667911 Bytes																																																
Current time 2014-06-18 13:33:17																																																
Flags: E=exec_binary, e=exec_script, c=compressed, l=symlink																																																
b=run_at_boot, B=qry_run_at_boot																																																
18			Write to config file																																													
19			Write to config file for both																																													
System returned:			20 Ok																																													

Figure 6.1 Configuration (cfg & Ethernet) files

1. *Download cfg file* – allows downloading system configuration file and saving it on your hard drive.
2. *Upload configuration file* - allows uploading system configuration file to CFIP Phoenix flash memory. In order to load configuration file from system memory, **cfg restore** should be used (refer to number 9);
3. *Saved configuration file* - shows contents of system configuration file saved in EEPROM memory. Commands contained in this configuration file are executed at every system start-up;
4. *Running configuration file* - shows currently running system configuration file (command line – **cfg show**). In order to save current configuration use command **cfg write**;
5. *Delete entry number from running configuration file* – allows deleting a specific line from currently running system configuration (refer to number 4); (command line – **cfg delete <line>**);
6. *Execute current configuration* – executes commands present in currently running system configuration file (command line – **cfg run**);
7. *Input file name to backup cfg in system memory* – allows choosing file name under which currently running system configuration file will be saved in the CFIP flash memory (command line – **cfg backup <file>**);
8. *Input file name to restore cfg from system memory* – allows loading system configuration file from backup file located in flash memory (command line – **cfg restore <file>**). To view the contents of flash memory refer to number 18;
9. *Enter string, which you want to save in cfg* – allows you to enter desirable command, which will be added to running system configuration file as the last line (command line – **cfg add <cmdline>**);
10. *Load factory configuration file* – Resets system configuration by loading in EEPROM the script with default settings. This command performs the following actions (in the following order):
 1. clears the currently saved system configuration file from EEPROM,
 2. creates and stores new system script in EEPROM the with the following settings:
 - net ip addr 192.168.205.10 or 192.168.205.11 (as marked on the label)
 - net ip remaddr 192.168.205.11 or 192.168.205.10
 - net ip mask 255.255.255.0
 - net ip gw – 255.255.255.255 (default gateway - none)
 - SNMP trap 255.255.255.255 (none)
 3. restarts the management controller.
(command line – **cfg factory**);
11. *Backup Ethernet configuration file* – allows choosing file name under which currently running Ethernet configuration file will be saved in the CFIP flash memory (command line – **ethernet config <file>**);
12. *Download current Ethernet configuration to PC* – allows downloading Ethernet configuration file and saving it on your hard drive.
13. *Upload Ethernet configuration file* – allows uploading Ethernet configuration file to CFIP Phoenix flash memory. In order to load Ethernet configuration file from system memory, appropriate dialog should be used - refer to number 15;
14. *Run/restore Ethernet configuration from file* – allows loading Ethernet configuration file from backup file located in flash memory. To view the contents of flash memory refer to number 18;

15. Saved configuration file - shows contents of system configuration file saved in EEPROM memory. Commands contained in this configuration file are executed at every system start-up;
16. Running configuration file - shows currently running system configuration file (command line – **eth config**). In order to save current configuration use command **cfg write**;
17. *File system content* – shows contents of internal flash memory (command line – **tfs ls**);
18. *Write to config file* – saves all changes made (command line – **cfg write**);
19. *Write to config file for both* – saves all changes made for local and remote side (command line – **cfg write**);
20. *System returned* - in case of error or incorrectly entered parameter value, or other problems in the whole page – the info message will be displayed here. Otherwise it says “Ok”.

<i>Additional commands for script editing in Telnet/serial interface</i>	
Command	Description
Cfg load	Loads the configuration script from EEPROM into RAM.
Cfg clear	Clears the script stored in RAM.
Cfg insert <line> <cmdline>	Inserts typed command line with specified line number into configuration script stored in RAM.
Cfg cmd <file with commands>	Restarts CPU of management controller and loads configuration script from the specified file.
Cfg group	Groups commands in configuration script.

6.2 License Management

License management allows specifying data transmit parameters and functionality for specific time period or for unlimited time.

CFIP without licensing option will operate with full functionality, but CFIP with licensing option but without activated licenses will operate with minimum functionality (Limited 4QAM modulation). Functionality may be expanded using appropriate license key.

Explanation of fields:

License management																																						
Active license status																																						
	1	Show active license																																				
License status	2	Ok																																				
Version	3	2																																				
Left time	4	Unlimited																																				
Key	5	SSSS-SSSSS-SSSSS-SSSSS																																				
Time	6	Unlimited																																				
		<table border="1"> <thead> <tr> <th>Bandwidth</th> <th></th> <th>Maximal modulation</th> </tr> </thead> <tbody> <tr> <td>3500 KHz</td> <td>7</td> <td>256QAM</td> </tr> <tr> <td>5000 KHz</td> <td>8</td> <td>256QAM</td> </tr> <tr> <td>7000 KHz</td> <td>9</td> <td>256QAM</td> </tr> <tr> <td>10000 KHz</td> <td>10</td> <td>256QAM</td> </tr> <tr> <td>14000 KHz</td> <td>11</td> <td>256QAM</td> </tr> <tr> <td>20000 KHz</td> <td>12</td> <td>256QAM</td> </tr> <tr> <td>28000 KHz</td> <td>13</td> <td>256QAM</td> </tr> <tr> <td>30000 KHz</td> <td>14</td> <td>256QAM</td> </tr> <tr> <td>40000 KHz</td> <td>15</td> <td>256QAM</td> </tr> <tr> <td>50000 KHz</td> <td>16</td> <td>256QAM</td> </tr> <tr> <td>56000 KHz</td> <td>17</td> <td>256QAM</td> </tr> </tbody> </table>	Bandwidth		Maximal modulation	3500 KHz	7	256QAM	5000 KHz	8	256QAM	7000 KHz	9	256QAM	10000 KHz	10	256QAM	14000 KHz	11	256QAM	20000 KHz	12	256QAM	28000 KHz	13	256QAM	30000 KHz	14	256QAM	40000 KHz	15	256QAM	50000 KHz	16	256QAM	56000 KHz	17	256QAM
Bandwidth		Maximal modulation																																				
3500 KHz	7	256QAM																																				
5000 KHz	8	256QAM																																				
7000 KHz	9	256QAM																																				
10000 KHz	10	256QAM																																				
14000 KHz	11	256QAM																																				
20000 KHz	12	256QAM																																				
28000 KHz	13	256QAM																																				
30000 KHz	14	256QAM																																				
40000 KHz	15	256QAM																																				
50000 KHz	16	256QAM																																				
56000 KHz	17	256QAM																																				
ACM	18	Enabled																																				
E1 channels	19	4																																				
Ethernet	20	8.0000 of 8.0000 Mbps																																				
License selection																																						
Available licenses	21	SSSSS-SSSSS-SSSSS-SSSSS / Unlimited time Activate																																				
License key	22	SSSSS-SSSSS-SSSSS-SSSSS Activate																																				
System returned:	23	Ok																																				

Figure 6.2 License management

1. *Show active license* – if non-active license is selected, pressing this button will switch selection back to currently active license (command line – ***license status***);
2. *License status* – shows if management CPU was able to read license data (command line – ***license status***);
3. *Version* – shows version of active or currently selected license; Version 2 licenses feature Ethernet rate limitation, for version 1 licenses Ethernet rate is always 'Unlimited' (command line – ***license status***);
4. *Left time* – shows the amount of time left for active or currently selected license (command line – ***license status***);
5. *Key* – displays active or currently selected license key (command line – ***license status***);
6. *Time* – shows time limitation for active or currently selected license (command line – ***license status***);
7. *3500 KHz* – shows the maximum modulation that can be used together with 3.5 MHz channel bandwidth (command line – ***license status***);
8. *5000 KHz* – shows the maximum modulation that can be used together with 5 MHz channel bandwidth (command line – ***license status***);
9. *7000 KHz* – shows the maximum modulation that can be used together with 7 MHz channel bandwidth (command line – ***license status***);
10. *10000 KHz* – shows the maximum modulation that can be used together with 10 MHz channel bandwidth (command line – ***license status***);
11. *14000 KHz* – shows the maximum modulation that can be used together with 14 MHz channel bandwidth (command line – ***license status***);
12. *20000 KHz* – shows the maximum modulation that can be used together with 20 MHz channel bandwidth (command line – ***license status***);

13. *28000 KHz* – shows the maximum modulation that can be used together with 28 MHz channel bandwidth (command line – **license status**);
14. *30000 KHz* – shows the maximum modulation that can be used together with 30 MHz channel bandwidth (command line – **license status**);
15. *40000 KHz* – shows the maximum modulation that can be used together with 40 MHz channel bandwidth (command line – **license status**);
16. *50000 KHz* – shows the maximum modulation that can be used together with 50 MHz channel bandwidth (command line – **license status**);
17. *56000 KHz* – shows the maximum modulation that can be used together with 56 MHz channel bandwidth (command line – **license status**);
18. *ACM* – shows if adaptive coding and modulation (ACM) is allowed for the active license (command line – **license status**);
19. *E1 channels* – shows how many E1 channels are allowed by the license (command line – **license status**);
20. *Ethernet* – shows Ethernet rate limitation for active or currently selected license. Ethernet rate of version 1 licenses will always be “Unlimited” (command line – **license status**);
21. *Available licenses* – shows the list of entered licenses. To activate any license, select it. “Add” button will transform into “Activate”, which should be pressed (command line – **license list**);
22. *License key* – allows entering a license key. Entering a license key twice, activates it (command line – **license key <key>**);
23. *System returned* – in case of error or incorrectly entered parameter value, or other problems on the whole page – info message will be displayed here. Otherwise it says “Ok”.

6.3 Command Line

In the command line you are able to execute all the commands to manage CFIP Phoenix which are available through serial/telnet interface. This dialog box translates commands to Telnet commands and sends them to the device. The initial screen shows you the available commands. To view help on a command, type in “<command> ?”, where <command> stands for the specific command.

Command management

Valid commands:

status odu prot aggr atpc modem loopback ethernet t1 eow system diagnostics

cfg tfs net license alarm log pm web snmp access cls ver help

Enter Command

Figure 6.3 Command management

Additional command prompt commands	
Command	Description
Cls	Clears the screen.
Help <command>	Provides help messages for commands.

6.4 File System

The software used by CFIP management controller is organized in files, which are stored on Flash disk.

The following files are required for the CFIP to start:

- ‘boot.ini’ file, - device boot configuration file. This file is a text file and contains the name of the firmware file which must be executed on start-up. The file name can be freely changed, but its default name is ‘boot.ini’; hereinafter, it is assumed that this file has default filename. The most important factor concerning this file is that it must be uploaded with ‘B’ and ‘e’ attribute flags (flags are case sensitive!), only then it will be treated as executive script.

Attribute flags for ‘boot.ini’ file:

B – query run at boot; **e** – executive script

For information how to upload files in the Flash disk, please refer to **Chapter 7**.

- Firmware file, - this file is the main firmware executable for the appropriate CFIP model. The file name can be freely changed, but its default name will contain the version and CFIP model, e.g., ‘cfipf000.elf.ezip’. The most important factor concerning this file is that it must be uploaded with ‘E’ and ‘c’ attribute flags, otherwise this file will not be used as the firmware.

Attribute flags for firmware file:

E – executable binary; **c** - compressed

Notes:

- The files are uploaded from PC to Flash disk using TFTP/FTP (via Ethernet management port), or using Xmodem protocol (via RS232 serial port), for more information about file upload please refer to **Chapter 7**; configuration backup files are created by CFIP management system.
- The flash disk may store other files as well, for example - previous firmware versions, configuration backup files, - up to 6.5 Mb (about 5 firmware files).
- The attribute flags for files are case sensitive.
- The file names can be changed, but it is very important that the file has the necessary attribute flags; otherwise, the file will not be used either as firmware, or as ‘boot.ini’ type file.
- There are no file extensions in the file system; either file, when edited, is treated as ASCII text file.
- When uploading the file, if the Flash disk stores the file with the same filename as for the file being uploaded, it will be overwritten with the new file.

Configuration backup files

Using ‘*cfg backup <filename>*’ command, the user can create the backup file of the current CFIP configuration. The configuration backup file is a text file and, when created, contains the current configuration script, - the same configuration script that is stored in EEPROM. Please refer to **Chapter 7** for more information on configuration script.

The configuration backup files are stored on Flash disk, where they can be edited or downloaded to PC. The backup configuration file can be applied in run-time, by consecutively entering ‘*cfg restore <filename>*’ and ‘*cfg run*’ commands. Note: the configuration restored from file is not stored in EEPROM and, therefore it will be lost during CFIP restart. To save it in EEPROM use ‘*write*’ command.

The user can create and store several configuration files to quickly revert to other CFIP site configurations.

Working with files

The following commands are intended to operate with files stored in Flash disk in the management controller.

tfs edit <file>	Edits the specified file. This command is applied for editing configuration backup files and boot configuration file (boot.ini). For example, <i>edit boot.ini,Be</i> – file ‘boot.ini’ will be opened for editing. ‘Be’ specifies that this file will be saved with attributes ‘B’ and ‘e’. If boot.ini file is intended to be modified, it should always be opened specifying ‘B’ and ‘e’ flags as in the example above, this will ensure that file is saved with these attributes (flags). To close the file and save changes press Ctrl+Z, to close the file without saving changes press Ctrl+Q. The configuration backup files do not require specific attributes.
tfs ls	Displays the list of files stored on the Flash disk and the number of bytes, both free and used by these files. ‘tfs dir’ can also be used.
tfs cat <filename>	Displays the contents of the text file. ‘tfs type’ can also be used.
tfs del <filename>	Deletes the specified file from Flash disk. ‘tfs rm’ can also be used.

6.5 Security commands

General tips

Telnet server supports one user only, web server supports up to 32 users simultaneously. By default the username and password for Web server, FTP server and Telnet terminal is:

- Username (login): *admin*
- Password: *changeme*

The username and password can be changed in Web GUI “System configuration → User configuration”

‘**access set** <username> <password> [plaintext]’ command.

Take note of upper case and lower case type: it should be taken into account for the password!

The passwords may contain spaces; if using space(s), the password should be entered in quotation marks.

For Telnet, FTP and Web GUI the password can be changed by simply entering the security command ‘**access set** <guest / admin> <password> [plaintext]’ while logged on and then saving the configuration in EEPROM by using ‘**write**’ command.

To terminate Telnet session press Ctrl+D.

(!) “guest” account is unable to change its access password.

(!) Specification of the password should always be followed by saving the configuration script (using “**cfg write**” command); otherwise, the password request will be ignored after the restart of CFIP.

7 Software Update

To simplify the firmware update process, SAF Tehnika JSC provides special update package, as a new version is available. This update pack is available as archive (e.g. zip), which includes firmware file (with *.elf.ezip,Ec extension), upgrade instructions, release notes and MIB files for SNMP protocol. The latest CFIP series firmwares are available in the following URL:

<https://saftehnika.com/en/downloads> (registration required)

The main method for firmware upgrade is being done via Web GUI, which automates the whole firmware upgrade process. To perform software upgrade from Web GUI, please go to “Configuration → System configuration” and in “Upgrade software” section press “Browse...” button and locate firmware upgrade file (e.g. cfipf000.elf.ezip,Ec) on your hard disk.

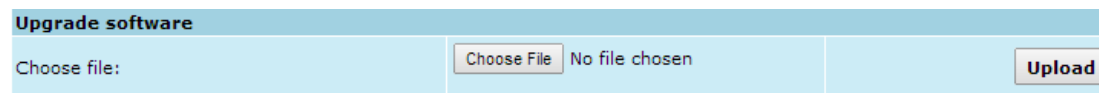


Figure 7.1 Upgrade software

Although upgrade procedure usually takes less than 1 min., Management CPU might initiate defragmentation of flash memory and upgrade process may take up to 3-5 minutes. Please do not unplug power until firmware upgrade procedure is finished - Web GUI will automatically reconnect and login page will appear.

Besides there are other various ways how the user can update the CFIP management software by uploading the appropriate firmware file to the CFIP Phoenix flash disk and further editing boot configuration file if necessary. The file upload can be performed:

- via Ethernet management port using update package,
- via Ethernet management port using FTP,
- via Ethernet management port using TFTP, or
- via RS232 serial port using Xmodem protocol.

Following chapters describe other methods how to update the software,

7.1 Uploading File via Ethernet Management Port (FTP)

Before uploading file via FTP, make sure the CFIP FTP server is running. To start it, go to ‘Configuration → IP configuration’ in Web GUI and press ‘Start FTP’:

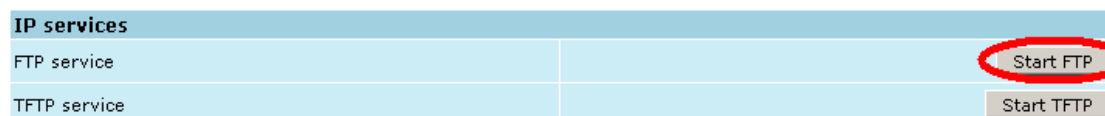


Figure 7.2 IP services

1. Open command window.
2. Start FTP client by entering “**ftp**” command (“ftp>” prompt will appear).
3. Connect to CFIP FTP server using command “**open** <CFIP_IP_address>”. Type in username and password when prompted (by default username is *admin* and password is *changeme*).
4. Enter the command “**type binary**” to make sure the binary transfer mode is selected.
5. Use command “**send** <local file> <remote file>, <flags>” to upload files to CFIP Flash disk. For example:

```
send c:\boot.ini boot.ini,Be
```

Use flags ‘E’ and ‘c’ if the file is a firmware file; if the file is a boot configuration file (boot.ini), the flags must be ‘B’ and ‘e’ (‘Be’); the flags for configuration backup files may not be specified.

Use command "**ls**" to list files on CFIP flash disk.

Use command "**delete <filename>**" to delete the file from the CFIP Flash disk.

6. Proceed with steps 5. and 6. in **Chapter 7.1**.

You can also use any preferable FTP client if you wish.

7.2 Uploading File via Serial Port (Xmodem)

File upload via serial port takes much longer time compared to use of TFTP and should be used only in case Ethernet connection with the CFIP management system is not available, or does not start normally.

1. Connect the ASCII console to the CFIP serial port, make connection with the following properties: Bits per second: 19200; Data bits: 8; Parity: none; Stop bits: 1; Flow control: none; if using 'Hyper Terminal' program, please refer to **Chapter 2.3.1** for information how to make a connection.
2. Type 'restartcpu' and, while CFIP is booting, press any key when 'boot.ini?' prompt appears. This will stop executing script in 'boot.ini' file and the CFIP will remain in MicroMonitor mode. This is the system start-up mode which loads the management system firmware;

Note: When you are in MicroMonitor mode, the 'uMON>' prompt will be displayed, instead of normal prompt with CFIP name (default 'SAF>').

3. In MicroMonitor mode enter the following command:

```
xmodem -cd -F <file_path-no_flags> -f Ec
```

where

<file_path-no_flags> - file name with no flags specified

'Ec' – file flags, in case the file is firmware file - 'E' and 'c' flags must be used; if the file is boot configuration file (boot.ini), the flags must be 'Be' ('B' and 'e'); the flags for configuration backup files may not be specified, in that case the command will be

```
xmodem -cd -F <file_path-no_flags>
```

After xmodem command execution, proceed to the next step.

4. Use terminal emulation software with file upload function, such as *Hyper Terminal* (in Windows) to upload the firmware file to CFIP as binary image (use binary transfer mode), using *Xmodem* protocol.

If you are using *Hyper Terminal*, proceed as follows: from menu select 'Transfer→Send File...', then select file and in 'protocol' box select *Xmodem* protocol and press 'Send' button. The following box should appear:

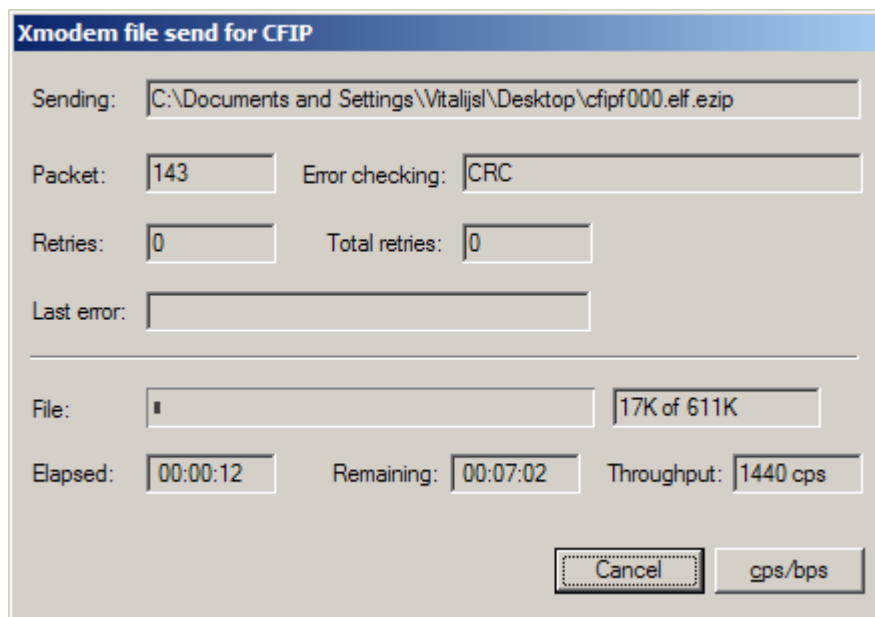


Figure 7.3 Xmodem file send for CFIP

When upload is complete, the following information will be displayed (**Figure 7.4**):

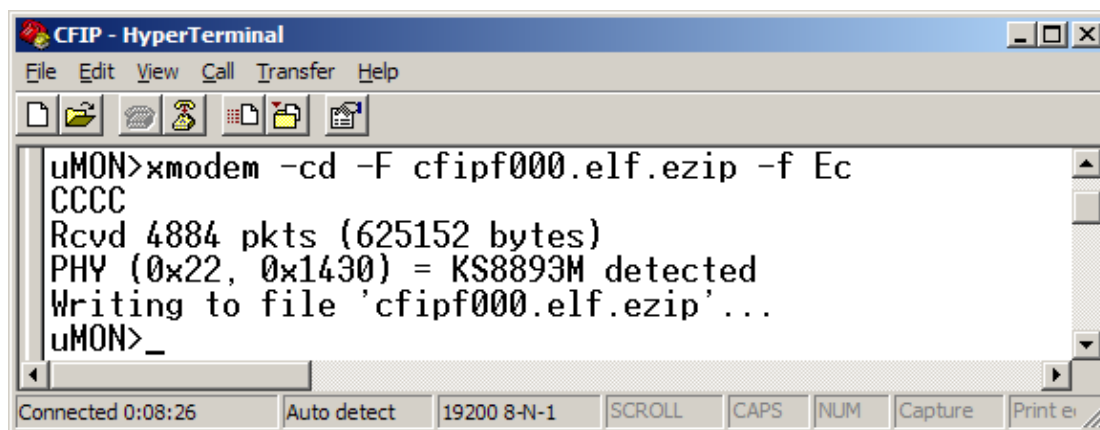


Figure 7.4 HyperTerminal

5. Enter 'reset' command to exit from MicroMonitor mode and restart the CFIP.
6. Proceed with steps 5. and 6. in **Chapter 7.1**.

8 CFIP Discovery Protocol

Discovery Protocol is Layer 3 Network protocol. This feature allows gathering information from connected CFIP devices. The protocol discovers the IP address and software version of connected CFIP unit. Discovery protocol uses UDP packets sent on port 78.

Discovery Protocol feature may be useful, when the IP address of connected device is unknown and there is no possibility to establish connection through serial management port in order to find out the IP address.

8.1 CFIP Unit Discovery Procedure

In order to discover the IP address and software version of CFIP unit proceed with the following steps:

- Connect your PC to CFIP unit through PoE injector
- Download Discovery Protocol (available from saftehnika.com webpage „[link](#)“)
- Open the cmd window on your PC (Go to "Start->Run.." and enter "cmd")
- Check for the IP address of your PC Ethernet adapter connected to CFIP unit by executing the command "ipconfig"
- Navigate to the folder containing previously downloaded and unzipped Discovery Protocol using "cd" command
- Now the necessary Discovery Protocol command can be executed (e.g. "dp sight <scan_addr>", where <scan_addr> should be substituted by Ethernet adapter IP address of your PC.)

Discovery Protocol Commands:

Discovery protocol commands	
Command	Description
dp sight <local_addr>	Allows to find out the IP address and firmware version of CFIP unit without knowing the IP subnet.
dp scan <local_addr> <scan_addr>	This command gathers the information in the specified subnet. It sends discovery packets to the broadcast address <scan_addr> and returns the IP address and firmware version of CFIP unit.
dp remote <local_addr> <remote_addr> <scan_addr>	Allows to find out the IP address and firmware version of CFIP remote unit. This procedure allows bypassing routers as the response packets are unicast packets.

8.2 Discovery Protocol Performance Examples

8.2.1 Discovery of IP Address and Firmware Version in Case The Subnet of CFIP Unit is Unknown

For this purpose the command "dp sight <local_addr>" should be executed in 'cmd'. Instead of <local_addr> place the IP address of your PC Ethernet adapter that is connected to CFIP unit. Refer to **Figure 8.1** for example.

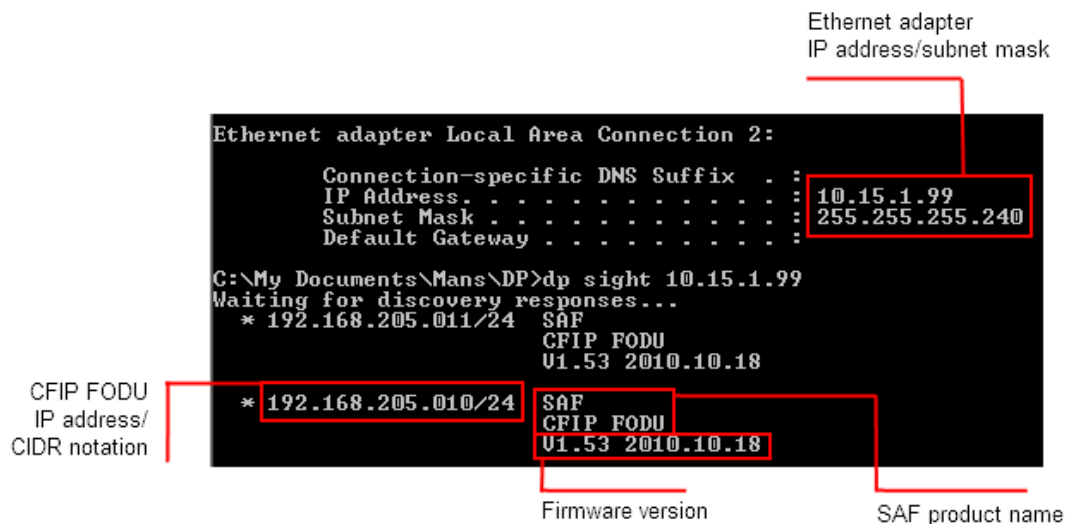


Figure 8.1

(!) Note that IP addresses of Ethernet adapter and CFIP units may belong to different subnets. This command sends discovery messages on broadcast address 255.255.255.255 to all devices in network. All CFIP devices connected to this network are responding with its own IP address/CIDR notation and firmware version.

CIDR notation (routing prefix) is related to network mask that is also necessary in order to manage CFIP unit. The IP address of your PC Ethernet adapter and CFIP unit should be from the same subnet in order to manage the CFIP unit. In the table below some examples are given for CIDR notation and subnet mask relation.

CIDR notation	Network mask
/24	255.255.255.0
/25	255.255.255.128
/26	255.255.255.192
/27	255.255.255.224
/28	255.255.255.240
/29	255.255.255.248
/30	255.255.255.252

8.2.2 Discovery of IP Address and Firmware Version in Case The Subnet of CFIP Unit is Known

For this purpose the command “dp scan <local_addr> <scan_addr>” should be executed in ‘cmd’. Instead of <local_addr> place the IP address of your PC Ethernet adapter that is connected to CFIP unit and instead of <scan_addr> place the broadcast address of specified subnet. Refer to **Figure 8.2** for example.

```

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.205.1
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 

C:\My Documents\Mans\DP>dp scan 192.168.205.1 192.168.205.255
Waiting for discovery responses...
* 192.168.205.010/24 SAF
    CFIP FODU
    01.53 2010.10.18

* 192.168.205.011/24 SAF
    CFIP FODU
    01.53 2010.10.18
  
```

Ethernet adapter
IP address/subnet mask

CFIP FODU
IP address/
CIDR notation

Firmware version

SAF product name

Figure 8.2

(!) Note that IP address of Ethernet adapter should belong to the same subnet as CFIP units, i.e. the subnet of CFIP units should be known. The subnet mask of Ethernet adapter and CFIP units may differ. This command sends discovery messages on specified broadcast address to all devices in the specified subnet. All CFIP devices from specified subnet are responding with its own IP address/CIDR notation and firmware version

8.2.3 Discovery of IP Address and Firmware Version of Remote CFIP Unit Connected to Router In Case one IP address of Remote Units is Known

For this purpose the command “dp remote <local_addr> <remote_addr> <scan_addr>” should be executed in ‘cmd’. Instead of <local_addr> place the IP address of your PC Ethernet adapter that is connected to router/CFIP unit. Instead of <remote_addr> place the IP address of one of the remote CFIP units known to you. Instead of <scan_addr> place the broadcast address. Refer to **Figure 8.3** for example.

```

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.205.99
    Subnet Mask . . . . . : 255.0.0.0
    Default Gateway . . . . . : 

C:\My Documents\Mans\DP>dp remote 192.168.205.99 192.168.205.11 255.255.255.255
Waiting for discovery responses...
* 192.168.205.010/24 SAF
    CFIP FODU
    01.53 2010.10.18
  
```

Ethernet adapter
IP address/subnet mask

CFIP FODU
IP address/
CIDR notation

Firmware version

SAF product name

Figure 8.3

(!) Note that one IP address of remote CFIP units should be known. The remote host sends discovery packets to specified broadcast address and the responses are delivered to the local host. This allows to find out the IP address and firmware version of neighbouring devices of a known remote device. The bypassing of a router is possible as the response packets are unicast.

9 RSSI Port

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

The following chart and table shows typical relationship of the received signal level (Rx level) displayed by CFIP vs. RSSI port output voltage (RSSI – Received Signal Strength Indicator). The RSSI port is located on ODU. The evaluated Rx level has the error ± 2 dB.

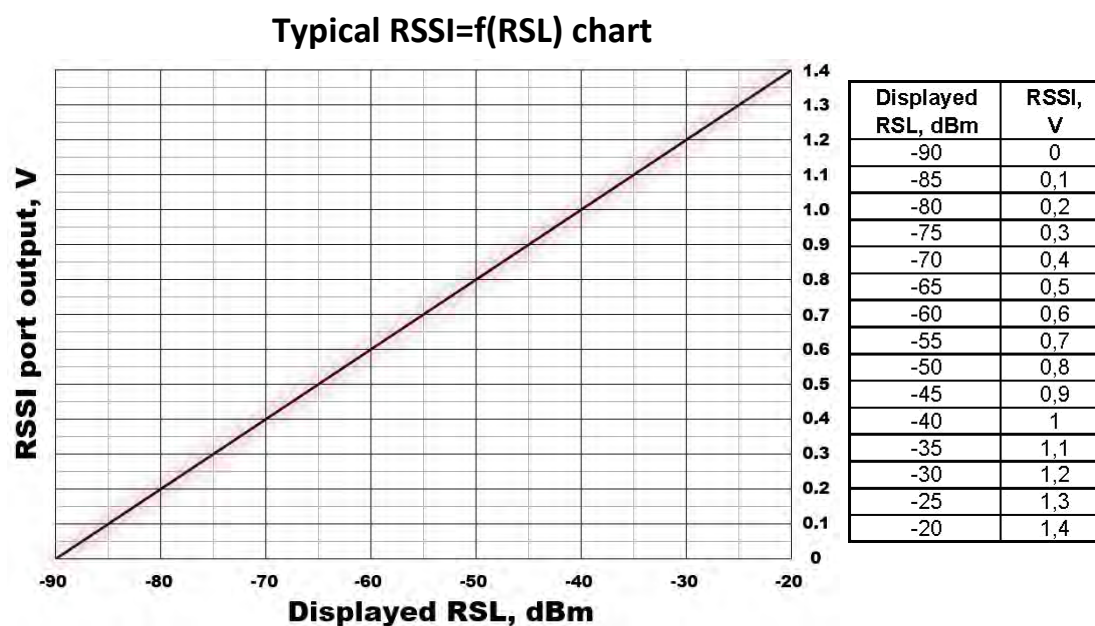


Figure 9.1 RSSI chart

10 Pinouts

10.1 Ethernet RJ-45 port

The pinouts of RJ45 socket are as follows:

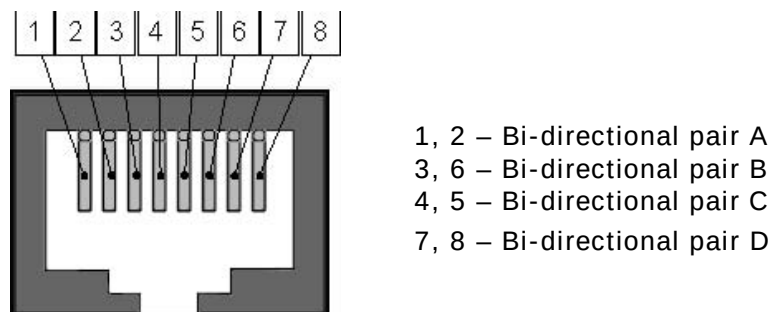


Figure 10.1 Ethernet RJ-45 port pinouts

10.2 E1 port

RJ-45 pinouts

The pinouts of CFIP Phoenix IDU RJ-45 sockets for E1 channels are shown in **Figure 10.2**.

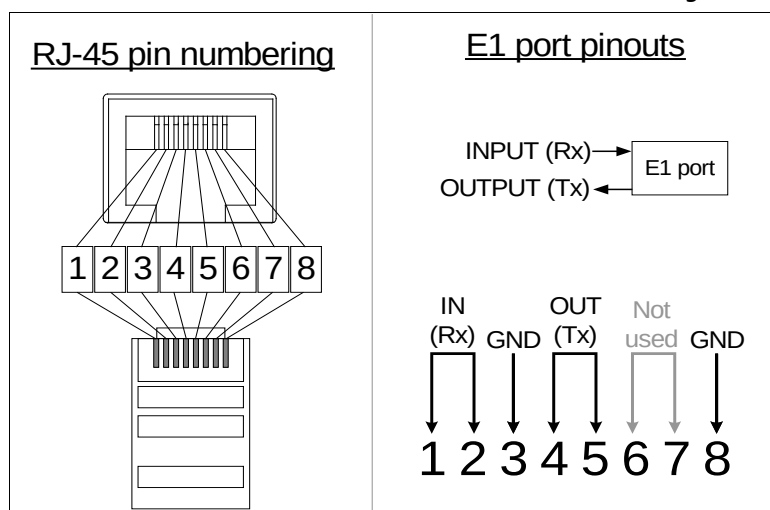


Figure 10.2 E1 traffic port pinouts

10.3 Alarm port (26-pin D-SUB)

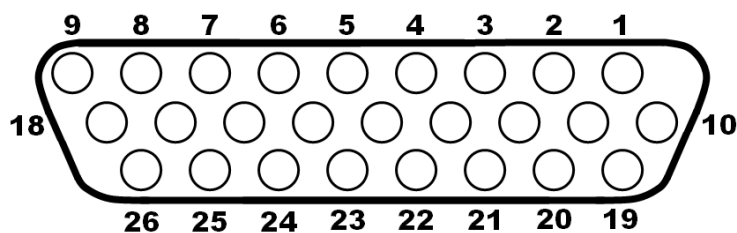


Figure 10.3 Alarm 26-pin D-SUB port pinouts

The pin assignments for relay outputs are the following:

Pin type	Pin number	Pin type	Pin number
Alarm input 1	1	Ground	12
Alarm input 2	2	Ground	13
Alarm input 3	3	Alarm output 4 NC	15
Alarm input 4	4	Alarm output 3 NC	16
Alarm output 4 NO	6	Alarm output 2 NC	17
Alarm output 3 NO	7	Alarm output 1 NC	18
Alarm output 2 NO	8	Alarm output 4 COM	23
Alarm output 1 NO	9	Alarm output 3 COM	24
Ground	10	Alarm output 2 COM	25
Ground	11	Alarm output 1 COM	26

Electrical specifications of auxiliary alarm inputs

- Nominal open output voltage: 5V;
- Nominal closed contact current: 1 mA;
- Maximum closed contact resistance: 800 Ω ;
- Minimum open contact resistance: 10 k Ω .

Electrical specifications of auxiliary alarm outputs

- Max. switching voltage: 68 VDC;
- Max. switching current (steady state): 2 A;
- Max. contact resistance: 75 m Ω .

10.4 RS232 (DB9 female connector)

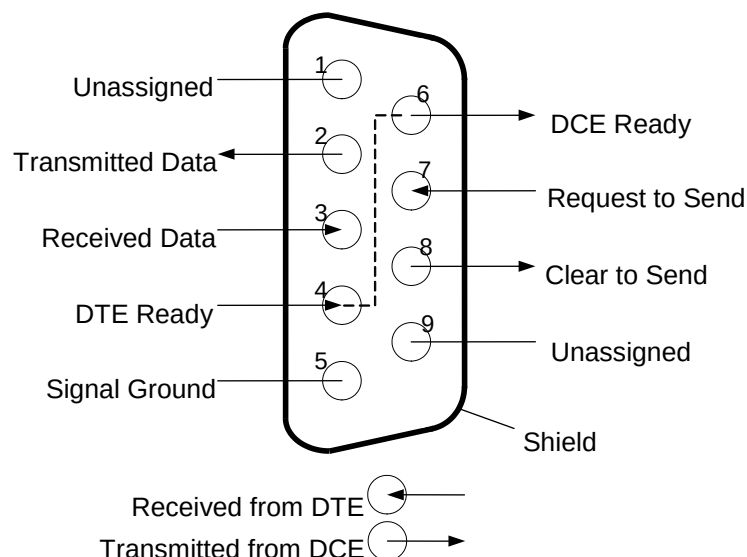


Figure 10.4 RS232 DB9 port pinouts

10.5 1+1 protection port (RJ-45)

The pinouts of RJ45 socket are as follows:

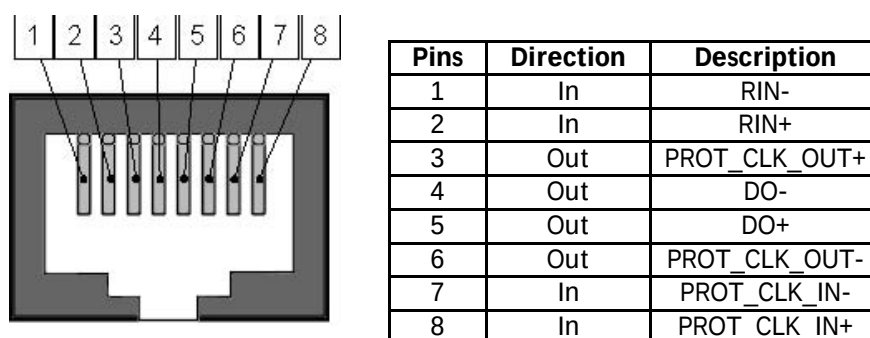


Figure 10.5 1+1 protection port pinouts

10.6 1+1 protection cable

Connector 1 pin	Wire	Connector 2 pin
1	Pair 1A	4
2	Pair 1B	5
3	Pair 2A	7
4	Pair 3A	1
5	Pair 3B	2
6	Pair 2B	8
7	Pair 4A	3
8	Pair 4B	6

Figure 10.6 1+1 protection cable pinouts

10.7 Power protection port

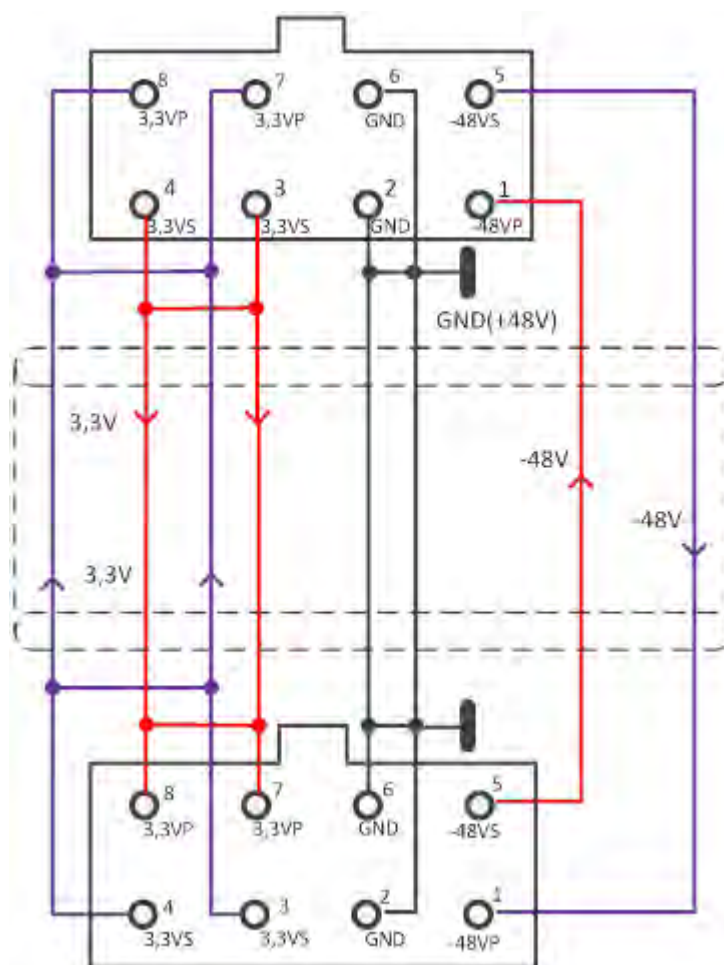
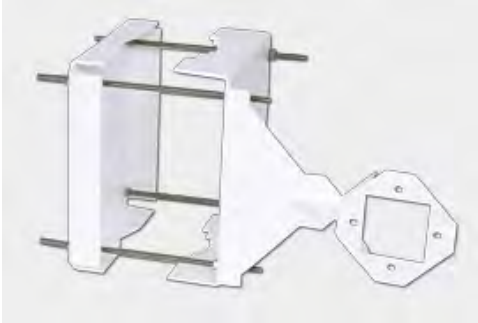


Figure 10.7 Power protection port and cable (P/N S0ACPR11) pinouts

11 Available Accessories

	
Surge protection P/N: CLALA001	Surge Protection with gas tube P/N: CLALA003
	
AC/DC Power supply, 48VDC, 80W EU - P/N IOAB4810, US - P/N IOAB4811, AUS - P/N IOAB4818	Flexible Waveguide UBR-PBR (See the list of available test equipment below)
	
CFIP Phoenix 1+1 protection bus cable CAT6 0,3m P/N S0ACPP11	Power protection cable 160mm; compatible with IDU P/N S0GIP*11 P/N S0ACPR11
	
IDU 1+1 grounding cable, 180 mm P/N S0ACGD02	Ethertnet Cat5e STP patch cable P/N IOACPP02

	
Coaxial attenuator 40 dB P/N CLA40A01	SAF adapted OMT for Arkivator antenna for dual-polarization (See the list of available test equipment below)
	
RSSI cable for ODU align 1m BNC – 2 plug-in P/N CLGCRS01	CFIP ODU Mounting Bracket (for 1xODU P/N: CLGRFB05; for 2xODU P/N: CLGRFB06)
	
Test equipment (See the list of available test equipment below)	FODU RJ-45 connector 8P shield solid P/N FOACNR02

11.1 Other Available Accessories

P/N	Name	Description
CLGC2131	Outdoor cable ODU-IDU RG213	Outdoor cable RG213 for ODU-IDU connecting, maximum length of cable is 100m.
CLACLMR4	Outdoor IF cable LMR-400	Outdoor IF cable LMR-400 for connecting IDU-ODU, maximum length - 300m
CLACNN01	N-type cable connector	N-type cable connector, provided for manufacturing the coaxial cable for interconnection of ODU and IDU
CLACNN02	N-type coax cable w.connector 1,5m	N-type coax cable w.connector 1,5m
SOACPK22	CFIP IDU/FIDU 1+1 IDU protection kit	CFIP IDU/FIDU 1+1 IDU protection kit

CFIP Test Equipment

P/N	Name:	Description
C06TST02	Test equipment 6 GHz	Test equipment 6 GHz

C08TST02	Test equipment 7/8 GHz	7/8GHz test suite, contains two waveguide-to-coaxial adapters, two attenuators, 40 dB, coaxial cable, 40 cm long
C11TST02	Test equipment 10/11 GHz	Test equipment 10/11 GHz
C15TST02	Test equipment 13/15 GHz	13/15GHz test suite, contains two waveguide-to-coaxial adapters, two attenuators, 40 dB, coaxial cable, 40 cm long
C22TST02	Test equipment 18/23GHz	18/23GHz test suite, contains two waveguide-to-coaxial adapters, two attenuators, 40 dB, coaxial cable, 40 cm long
C26TST02	Test equipment 26GHz	26 GHz test suite, contains flexible waveguide, waveguide attenuators (60dB)
C38TST02	Test equipment 38GHz	38 GHz test suite, contains flexible waveguide, waveguide attenuators (60dB)

UBR-PBR Waveguides

P/N	Name	Description
C07WF201	7/8GHz Flexible Waveguide 60cm UBR-PBR	Flexible Waveguide 2ft/60cm, 7-8GHz for connection of ODU to antenna (if installed separately) /for connection between splitter and antenna (1+1 protected installation)
C07WF301	7/8GHz Flexible Waveguide 90cm UBR-PBR	7/8GHz Flexible Waveguide 90cm UBR-PBR
C11WF301	10/11GHz Flex Waveguide 90cm PBR-UBR	10/11GHz Flex Waveguide 90cm PBR-UBR
C15WF301	13-15 GHz Flexible Waveguide 3ft/90cm UBR	13-15 GHz Flexible Waveguide 3ft/90cmUBR
C15WF201	13/15GHz Flexible Waveguide 60cm UBR-PBR	Flexible Waveguide 2ft/60cm, 13-15Ghz for connection of ODU to antenna (if installed separately) /for connection between splitter and antenna (1+1 protected installation)
C13WF301	13GHz Flexible Waveguide 90cm UBR-PBR	13/15 GHz Flexible Waveguide 90cm UBR-PBR
C22WF101	18/23GHz Flexible Waveguide 1ft/30cm	18/23GHz Flexible Waveguide 1ft/30cm
C22WF201	18/23GHz Flexible Waveguide 2ft/60cm	18-23GHz flexible waveguide to connect 18/23GHz coupler to antenna
C22WF401	18/23GHz Flexible Waveguide 4ft/120cm	18/23GHz Flexible Waveguide 4ft/120cm

OMT

P/N	Name	Description
C07OM31001i	OMT (Arkivator) 7GHz	7Ghz OMT (orthomode transducer) SAF adapted for direct mount to Arkivator 0.3, 0.6, 0.99 and 1.2m antennas
C11OM31001i	OMT (Arkivator) 11GHz	11Ghz OMT (orthomode transducer) SAF adapted for direct mount to Arkivator 0.3, 0.6, 0.99 and 1.2m antennas
C13OM31001i	OMT (Arkivator) 13GHz	13Ghz OMT (orthomode transducer) SAF adapted for direct mount to Arkivator 0.3, 0.6, 0.99 and 1.2m antennas
C15OM31001i	OMT (Arkivator) 15GHz	15Ghz OMT (orthomode transducer) SAF adapted for direct mount to Arkivator 0.3, 0.6, 0.99 and 1.2m antennas
C18OM31001i	OMT (Arkivator) 18GHz	18Ghz OMT (orthomode transducer) SAF adapted for direct mount to Arkivator 0.3, 0.6, 0.99 and 1.2m antennas
C23OM31001i	OMT (Arkivator) 23GHz	23Ghz OMT (orthomode transducer) SAF adapted for direct mount to Arkivator 0.3, 0.6, 0.99 and 1.2m antennas
C26OM31001i	OMT (Arkivator) 26GHz	26Ghz OMT (orthomode transducer) SAF adapted for direct mount to Arkivator 0.3, 0.6, 0.99 and 1.2m antennas
C38OM31001i	OMT (Arkivator) 38GHz	38Ghz OMT (orthomode transducer) SAF adapted for direct mount to Arkivator 0.3, 0.6, 0.99 and 1.2m antennas

12 List of Abbreviations

3G – third generation
AC – Alternating Current
ACI – Adjacent-Channel Interference
ACM – Adaptive Coding and Modulation
AGC – Automatic Gain Control
ASCII - American Standard Code for Information Interchange
ATPC – Automatic Transmit Power Control
BER – Bit-Error Ratio
BNC connector - Bayonet Neill-Concelman coaxial connector
CCI – Co-Channel Interference
CLI – Command-Line Interface
CPU – Central Processing Unit
CRC – Cyclic Redundancy Check
DC – Direct Current
DiffServ – Differentiated Services
DSCP - Differentiated Services Code Point
EEPROM - Electrically Erasable Programmable Read-Only Memory
EMI – Electromagnetic Interference
ETS – European Telecommunication Standard
ETSI – European Telecommunications Standards Institute
FIR – Finite Impulse Response
FO – Fiber Optics
FODU – Full Outdoor Unit
FTP – File Transfer Protocol
GFP – Generic Framing Procedure
GND - Ground
GSM - Global System for Mobile communications
GUI – Graphical User Interface
IEEE - Institute of Electrical and Electronics Engineers
IF – Intermediate Frequency
ISP – Internet Service Provider
ITU-T – International Telecommunication Union – Telecommunication Standardization Sector
LAN – Local Area Network
LDPC – Low-Density Parity-Check Code
LED – Light-Emitting Diode
LTE – Long-Term Evolution
MAC – Media Access Control
MSE – Mean Square Error
NMS – Network Management System
PC – Personal Computer
PDH – Plesiochronous Digital Hierarchy
PLL – Phase-Locked Loop
PoE - Power over Ethernet
QAM - Quadrature amplitude modulation
QoS – Quality of Service
4QAM - Quadrature Phase-Shift Keying

RAM – Random Access Memory

RSL – Received Signal Level

RSSI – Received Signal Strength Indicator

Rx – Receive

SNMP - Simple Network Management Protocol

SNR – Signal-to-Noise Ratio

STM-1 – Synchronous Transport Module - 1

TCP/IP – Internet Protocol Suite (Transmission Control Protocol / Internet Protocol)

TDM – Time-Division Multiplexing

TFTP – Trivial File Transfer Protocol

TM – Tide Mark

TP – Twisted Pair

TS – Threshold Seconds

Tx – Transmission

UART – Universal Asynchronous Receiver/Transmitter

USB – Universal Serial Bus

UTP – Unshielded Twisted Pair

VLAN – Virtual Local Area Network

WAN – Wide Area Network

13 SAF Tehnika JSC Contacts

SAF Tehnika A/S technical support can be reached by:

- Email: techsupport@saftehnika.com
- Telephone: +371 67046840
- Fax: +371 67046809