USER MANUAL

Z-TWS4

Z-PASS2-S

S6001-RTU

SENECA s.r.l.

Via Austria, 26 – 35127 – Z.I. CAMIN – PADOVA – ITALY

Tel. +39.049.8705359 – 8705408 Fax. +39.049.8706287

Web site: www.seneca.it

Support: supporto@seneca.it (IT), support@seneca.it (Other)

Sales: commerciale@seneca.it (IT), sales@seneca.it (Other)

UNI EN ISO 9001 CERTIFICATE Nr. 9115.SENE

To use the product safely and effectively, read carefully the following instructions before use. The product must be used only for the use for which it was designed and built. Any other use must be considered with full responsibility of the user. The installation, programmation and set-up is allowed only for authorized operators; these ones must be people physically and intellectually suitable. Set up must be performed only after a correct installation and the user must perform every operation described in the installation manual carefully. Seneca is not considered liable of failure, breakdown, accident caused for ignorance or failure to apply the indicated requirements. Seneca is not considered liable of any unauthorized changes. Seneca reserves the right to modify the device, for any commercial or construction requirements, without the obligation to promptly update the reference manuals.

MI003770_110

Table of contents

1 Preliminary information / Informazioni preliminari

WARNING!

IN NO EVENT WILL SENECA OR ITS SUPPLIERS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF CAUSE (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE Z-TWS4/Z-PASS2-S/S6001-RTU, EVEN IF SENECA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SENECA, ITS SUBSIDIARIES AND AFFILIATES COMPANY OR GROUP OF DISTRIBUTORS AND SENECA RETAILERS NOT WARRANT THAT THE FUNCTIONS WILL MEET YOUR EXPECTATIONS, AND THAT Z-TWS4/Z-PASS2-S/S6001-RTU, ITS FIRMWARE AND SOFTWARE WILL BE FREE FROM ERRORS OR IT OPERATES UNINTERRUPTED.

SENECA SRL CAN MODIFY THE CONTENTS OF THIS MANUAL IN ANY TIME WITHOUT NOTICE TO CORRECT, EXTEND OR INTEGRATING FUNCTION AND CHARACTERISTICS OF THE PRODUCT.

ATTENZIONE!

IN NESSUN CASO SENECA O I SUOI FORNITORI SARANNO RITENUTI RESPONSABILI PER EVENTUALI PERDITE DI DATI ENTRATE O PROFITTI, O PER CAUSE INDIRETTE, CONSEQUENZIALI O INCIDENTALI, PER CAUSE (COMPRESA LA NEGLIGENZA), DERIVANTI O COLLEGATE ALL' USO O ALL' INCAPACITÀ DI USARE Z-TWS4/Z-PASS2-S/S6001-RTU, ANCHE SE SENECA È STATA AVVISATA DELLA POSSIBILITÀ DI TALI DANNI.

SENECA, LE SUSSIDIARIE O AFFILIATE O SOCIETÀ DEL GRUPPO O DISTRIBUTORI E RIVENDITORI SENECA NON GARANTISCONO CHE LE FUNZIONI SODDISFERANNO FEDELMENTE LE ASPETTATIVE E CHE Z-TWS4/Z-PASS2-S/S6001-RTU, IL SUO FIRMWARE E SOFTWARE SIA ESENTE DA ERRORI O CHE FUNZIONI ININTERROTTAMENTE.

SENECA SRL PUO' MODIFICARE IL CONTENUTO DI QUESTO MANUALE IN QUALUNQUE MOMENTO E SENZA PREAVVISO AL FINE DI CORREGGERE, ESTENDERE O INTEGRARE FUNZIONALITA' E CARATTERISTICHE DEL PRODOTTO.

Date	Revision	Notes
06/09/2016	07	- Chapter "Features": new features for Z-TWS4-R01/Z-PASS2-S-R01 - Chapter "LEDs signalling": new par. "Z-TWS4-R01/Z-PASS2-S-R01" - New chapter "Ethernet Mode (Z-TWS4-R01/Z-PASS2-S-R01)" - Chapter: "Discovering the IP address": network parameters setting - Chapter "Upgrading the firmware by a USB pen": revision - Par. "Web Configuration Pages/Administrator pages": changed paragraphs: - "Main View" - "Network and Services" - "Router Configuration" - "FW Upgrade" new paragraphs: - "VPN Configuration/OpenVPN Client/LED signalling (Z-TWS4-R01/Z-PASS2-S-R01)" - "VPN Configuration/VPN Box/LED signalling (Z-TWS4-R01/Z-PASS2-S-R01)" - Par. "Web Configuration Pages/User pages" changed paragraphs: - "Main View" - "Network and Services"
11/01/2017	08	- Renamed “Z-TWS4-1” → “Z-TWS4-R01”, “Z-PASS2-S-1” → ”, “Z-PASS2-S-R01” - Chapter “Discovering the IP address”: discovery working on both LAN and WAN interfaces - New chapter “Network Redundancy” - Paragraph “Main View” revision (also for “User Pages”) - Paragraph “Network and Services”: added “DNS Mode” parameter and Network Redundancy parameters; changed some default values (also for “User Pages”) - Paragraph “Real Time Clock Setup”: added “Central Europe” time zone value - Paragraph "VPN Configuration/OpenVPN Client": revision into "VPN Configuration/OpenVPN”; added packet/byte counters description - Paragraph "VPN Configuration/VPN Box”: added packet/byte counters description - Paragraph “Mobile Network”: added packet/byte counters description - Paragraph “Router Configuration”: Port Mapping parameters no more disabled when “Use Local Addresses” is ON - Paragraph “Users Configuration”: added “guest” user credentials - New paragraph “Ethernet Interfaces” - New paragraph “Modbus Modules” - New paragraph “Data Logs”

		- New paragraph “Guest Pages” - StratON FBs and Functions, new paragraphs: GET_ALARMS, PUT_ALARM, SET_ALARMS_STAT, FM_WRITE_NCRLF, TXBAPPENDFILE, GET_MIN_SINCE2K - Chapter Z-NET4: added note to “Remote Control Functions”
01/03/2017	09	- New paragraph “Configuration Management” - PLC application name shown in the web pages header - “Use Local Address through VPN” parameter: “ON” option always available - Paragraph “Network and Services” (Admin and User): changed default value for “Default Gateway” and “DNS Server” parameters; “Default Gateway” always in the WAN subnet, in LAN/WAN mode; “DHCP on LAN” disabled, in LAN/WAN mode - OpenVPN, Configuration File: added rules on “dev” and “log” options - StratON FBs and Functions, new paragraphs: S7_DB_READ, S7_DB_WRITE
23/05/2017	10	- Chapter "Features": new features for Z-TWS4-R02/Z-PASS2-S-R02 - New “LEDs signaling” sub-paragraph for R02 HW revision - New chapter “Remote Access Disable” - New chapter “Auto-APN” - Paragraph “Network and Services”: added screen-shots for “R02” version; added “COM1/Mode” parameter - Paragraph “VPN Box”: added “License Limit Reached” error reason - Paragraph “FW Upgrade”: changed “Stop TWS Services” pop-up - Paragraph “Configuration Management”: added “Save Debug Logs” feature - Paragraph “Mobile Network”: added “APN Mode” parameter - New paragraph “Digital I/O Configuration” - Paragraph “PPP_CONNECT”: changes for “Auto-APN” - StratON FBs and Functions, new paragraphs: PPP_CONNECT_R2, VPNBOX_STATUS, WDOG_KEEP_ALIVE, WDOG_SET_TMO

2 Features

Z-TWS4, Z-PASS2-S and S6001-RTU are programmable, communication oriented PLCs.

The Z-TWS4/Z-PASS2-S/S6001-RTU StratON™ PLC is programmable according to the IEC 61131-3 standard, by means of the StratON development environment.

All three devices provide the following features:

- OpenVPN connectivity
- full configuration by means of an integrated web site
- FW upgrade, that can be performed locally, by means of a USB pen, or remotely, through the web site

Z-PASS2-S and S6001-RTU[1] integrate a 3G HSPA modem, while Z-TWS4 can be connected to an external 3G (UMTS/HSPA) modem (Seneca Z-MODEM-3G[2]).

S6001-RTU is equipped with a rich set of analog and digital inputs/outputs.

Z-PASS2-S, S6001-RTU and Z-TWS4 (when connected to an external modem) can be used as a Router, routing packets between the WAN (Mobile Network) and the LAN (Ethernet).

All three devices are based on a 32bits ARM9 processor, equipped with the Linux operating system (Linux kernel 2.6.28).

Z-TWS4-R01 and Z-PASS2-S-R01 are new versions of the Z-TWS4 and Z-PASS2-S products, providing the following new features:

- the two available Ethernet ports can be configured as two fully separated network interfaces (“LAN” and “WAN”), whereas in the older versions they could only work as ports of an Ethernet switch; the user can choose if the two ports shall work in “LAN/WAN” mode or “Switch” mode, by means of a new configuration parameter (“Ethernet Mode”);
- there are 4 more LEDs, providing information about the “Ethernet Mode” and the VPN functionalities.

Z-TWS4-R02 and Z-PASS2-S-R02 are new versions of the Z-TWS4 and Z-PASS2-S products, providing the following new features:

- one digital input which can be used to disable remote access to the device
- one digital output which goes HIGH when the device is remotely accessed
- one digital input which can also be used as a local alarm
- one digital output which can also be used as a remote command
- two configurable digital inputs/outputs
- a new set of LEDs
- COM1 RS232/RS485 mode set by software (configuration parameter), instead of HW DIP switch

NOTE:
in the following chapters, the term “Device” will be used when describing features or characteristics that are available in all three products.

3 Technical specifications

[1] S6001-RTU is also available without modem.

[2] Please contact Seneca for more information about Z-MODEM-3G product.

COMMUNICATION PORTS (Z-TWS4/Z-PASS2-S)	
RS 485	Baud rate: maximum 115 Kbps, minimum 110 bps COM 4 (screw terminals 4-5-6) COM 2 (screw terminals 1-2-3 or IDC10 connector) COM 1 (removable 4 pin connector, as an alternative to RS232)
RS 232	Baud rate: maximum 115 Kbps, minimum 110 bps COM 1 (removable 4 pin connector, as an alternative to RS485)
CAN	CAN bus port 2.0A and 2.0B Baud rate: maximum 500 Kbps, minimum 20 Kbps (screw terminals 10-11-12 or IDC10 connector) available only in Z-TWS4
Ethernet 1 and Ethernet 2	Ethernet 10/100 Mbps Two RJ45 connectors on front-panel Maximum connection length 100 m In Z-TWS4-R01/Z-PASS2-S-R01/Z-TWS4-R02/Z-PASS2-S-R02, the two ports can work either as LAN/WAN ports (**ETH1=LAN, ETH2=WAN**) or ports of an Ethernet switch. In Z-TWS4/Z-PASS2-S, the two ports can work only as ports of an Ethernet switch.
USB #1 HOST	Plug-in: USB type A
USB #2 HOST	Plug-in: micro USB (available only in Z-TWS4)
COMMUNICATION PORTS (S6001-RTU)	
RS 485	Baud rate: maximum 115 Kbps, minimum 110 bps COM 4 (screw terminals 54-55-56) COM 2 (screw terminals 57-58-59)
RS 232	Baud rate: maximum 115 Kbps, minimum 110 bps COM 1 (DB9 male connector)
Optional Bus for future extensions	screw terminals 60-61-62
Ethernet	Ethernet 10/100 Mbps RJ45 connector

	Maximum connection length 100 m
USB #1 HOST	Plug-in: USB type A
CPU AND MEMORY	
Microprocessor	ARM 9, 32 bits, 400 MHz
Memories	64 Mbytes of RAM 1 Gbyte of FLASH 8 Kbytes of FeRAM, split in 2 partitions (4 Kbytes each) for redundancy
Slot for external memory	Micro SD card: max 32 Gbytes
I/O CPU (S6001-RTU)	
Microprocessor	8 bits, 24 MHz
MODEM (Z-PASS2-S/S6001-RTU)	
HSPA Modem	14.4 Mbps in downlink, 5.76 Mbps in uplink
Slot for SIM card	Mini SIM with push-push connector
POWER SUPPLY (Z-TWS4/Z-PASS2-S)	
Power supply	11..40 Vdc or 19..28 Vac @ 50..60 Hz
Consumption	Typical 4 W @ 24 Vdc; Max 6 W
POWER SUPPLY (S6001-RTU)	
Power supply	24 Vac/dc ± 15% @ 50/60Hz
Consumption	10 VA max , 6 VA typical
ENVIRONMENTAL CONDITIONS (Z-TWS4/Z-PASS2-S)	
Temperature	-20..+55 °C
Humidity	30..90 % @ 40 °C not condensing
Storage temperature	-20..+85 °C
Protection degree	IP20
ENVIRONMENTAL CONDITIONS (S6001-RTU)	
Temperature	-10..+65 °C
Humidity	10..90 % not condensing
Storage temperature	-40..+85 °C

Protection degree	IP20
CONNECTIONS (Z-TWS4/Z-PASS2-S)	
Connections	Removable 3 way screw terminals, 5.08 pitch Rear IDC10 connector for DIN 46277 rail Removable 4 pin connector Two RJ45 connectors Type A USB connector and micro USB connector (only in Z-TWS4) Plug in: micro SD card Two SMA antenna connectors, for Main and Diversity antennas (only in Z-PASS2-S)
CONNECTIONS (S6001-RTU)	
Connections	Removable screw terminals DB9 male connector RJ45 connector Type A USB connector Plug in: micro SD card Two SMA antenna connectors, for Main and Diversity antennas
BOX / DIMENSIONS (Z-TWS4/Z-PASS2-S)	
Dimensions	Z-TWS4: L: 100 mm; H: 112 mm; W: 35 mm Z-PASS2-S: L: 100 mm; H: 112 mm; W: 53 mm
Case	Nylon 6 with 30% fiberglass field, self-extinguishing class V0, black color
WEIGHT / DIMENSIONS (S6001-RTU)	
Dimensions	190 mm x 160 mm x 105 mm
Weight	600 g
INPUTS / OUTPUTS (S6001-RTU)[3]	
Analog inputs	4, current, 0..20 mA resolution: 12 bit accuracy: += 0.3% of full scale input impedance: 50 Ω

[3] For more detailed information about S6001-RTU I/Os, see S6001-RTU Installation Manual.

Analog outputs	1, current, 0..20 mA 1, voltage, 0..10 Vdc resolution: 12 bit accuracy: += 0.3% of full scale output load: current: <= 500 Ω, voltage: >= 1 kΩ
Digital inputs	15, PNP, with optoisolation ON current > 4 mA, OFF current < 3 mA
Digital outputs	8, SPDT relays max peak current: 3 A operating current: 2 A operating voltage: 250 Vac minimum load: 0.5 W isolation: 3 kV
Liquid level control inputs	conductive liquid level switch, 2 channels adjustable sensitivity

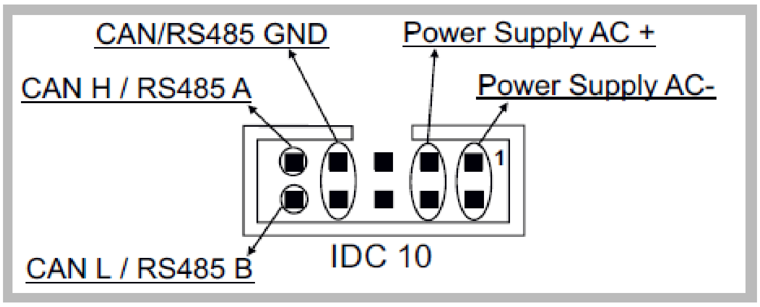
The following table shows which frequency bands are supported by the HSPA modem available in Z-PASS2-S, Z-PASS2-S-R01 and S6001-RTU products; TBD for Z-PASS2-S-R02 modem.

Standard	Frequency	Z-PASS2-S/S6001-RTU Modem
GSM	GSM 850 MHz	OK
	EGSM 900 MHz	OK
	DCS 1800 MHz	OK
	PCS 1900 MHz	OK
WCDMA	WCDMA 850 MHz	
	WCDMA 900 MHz	OK
	WCDMA 1900 MHz	
	WCDMA 2100 MHz	OK
HSPA	HSDPA	OK
	HSUPA	OK
	Dual-Cell HSPA+	
DRX	Receiver Diversity	OK

4 Electrical Connections

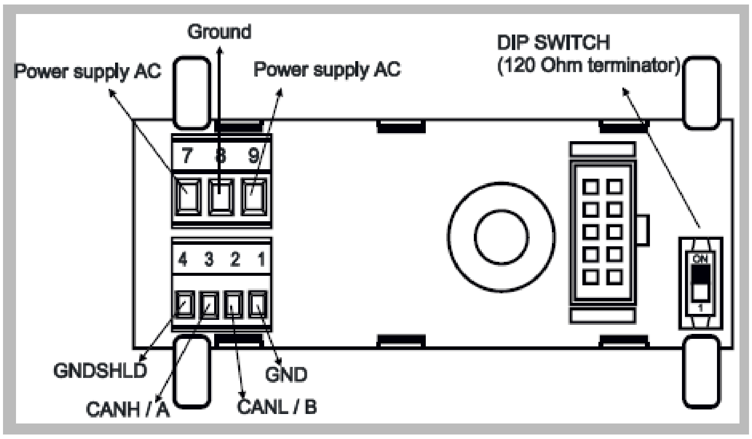
4.1 Z-TWS4, Z-PASS2-S, Z-TWS4-R01, Z-PASS2-S-R01, Z-TWS4-R02, Z-PASS2-S-R02

Power Supply and Modbus interface are available by using the bus for the Seneca DIN rail, by the rear IDC10 connector or by Z-PC-DINAL1-35 accessory for Z-TWS4, Z-PC-DINAL2-52.5-17 for Z-PASS2-S. The following picture shows the meaning of the IDC10 connector pins.

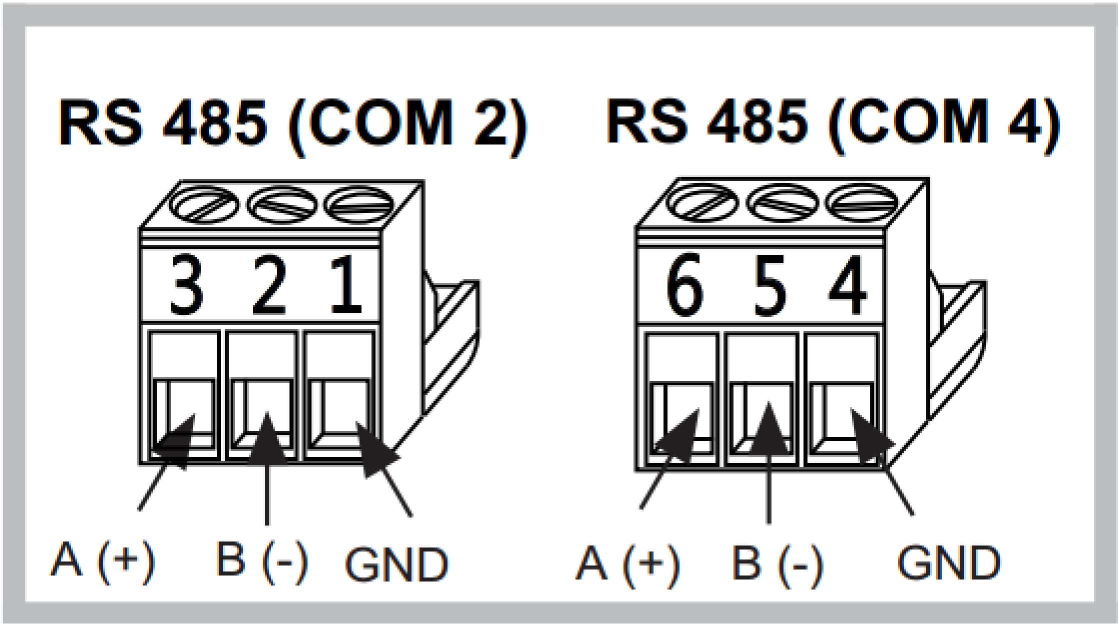


Power supply is available only from the rear connector for Z-TWS4, while Z-PASS2-S can be powered also through 14-15 screw terminals.

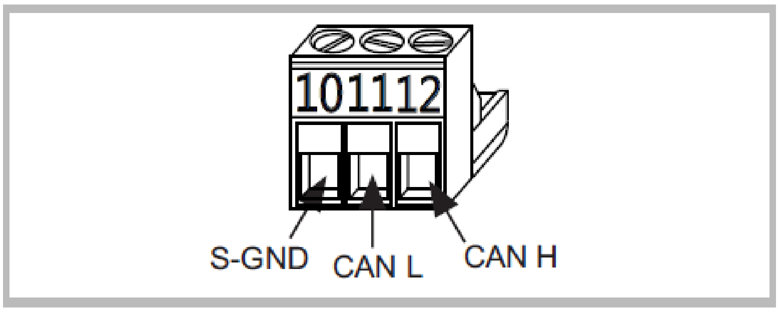
If ***Z-PC-DINAL1-35*** or ***Z-PC-DINAL2-52.5-17*** accessory is used, the power supply signals and communication signals may be provided by the terminals block into the DIN rail support. In the following figure the meaning and the position of the terminal blocks are shown. The DIP-switch that sets the 120 Ω terminator is used only for CAN communication (Z-TWS4 only).
GNDSHLD: shield to protect the connection cables against interference (recommended).



The Device has two RS 485 serial ports for Modbus communication: COM 4 and COM 2. The RS485 connection for COM 2 can be set up by means of the corresponding screw terminals or by the IDC10 connector. On Z-TWS4, to select RS 485 on IDC10 connector, put the SW1 DIP-switch on OFF position; on Z-PASS2-S, no operation is needed.

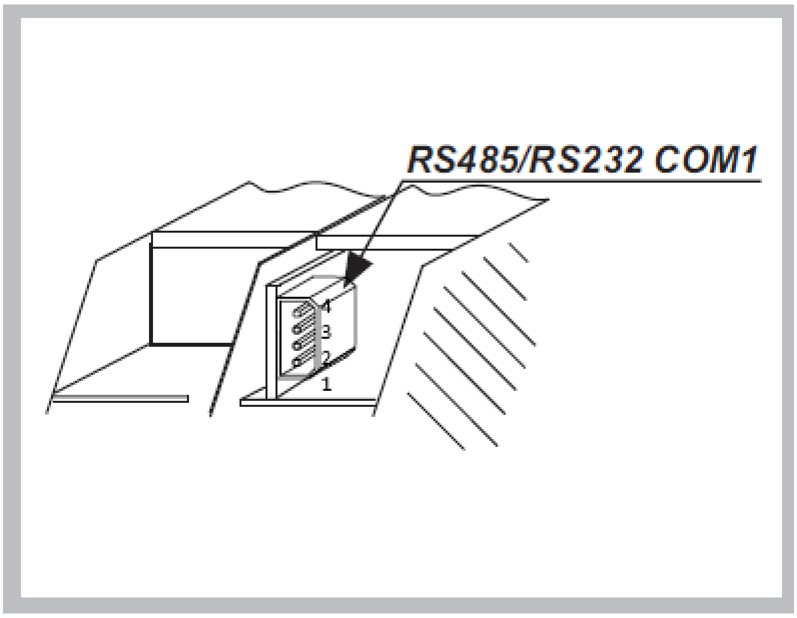


The Z-TWS4 has a CAN port available on screw terminals 10-11-12. As an alternative, the connection can be set up on the IDC10 connector. To select CAN port on IDC10 connector, put the SW1 DIP-switch on ON position.



Through a removable 4 pin connector, the Device provides a serial RS232 port or, as an alternative, a third RS485 port. In order to select the RS232 port on the removable 4 pin connector, put the SW2 DIP-switch on ON position; to select the RS485 port on the removable 4 pin connector, put the SW2 DIP-switch on OFF position[4].
The cable length for the RS232 interface must be less than 3 meters.

[4] While in Z-TWS4 the SW2 DIP-switch position can be changed by the user, in Z-PASS2-S the DIP-switch is internal and its position is permanently set in the factory.

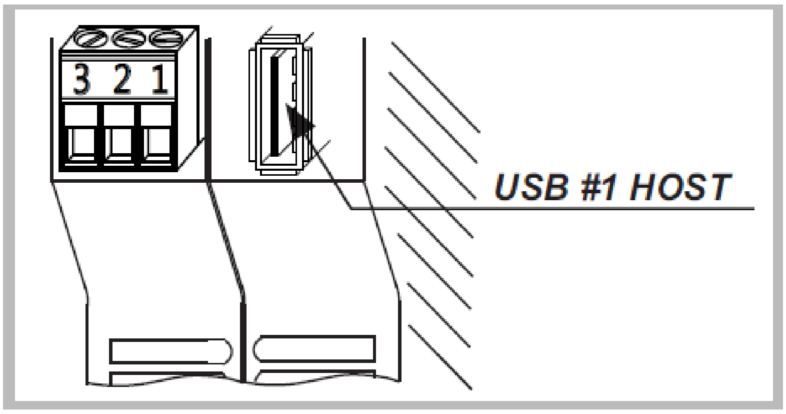


The connector pin-out is given in the following table:

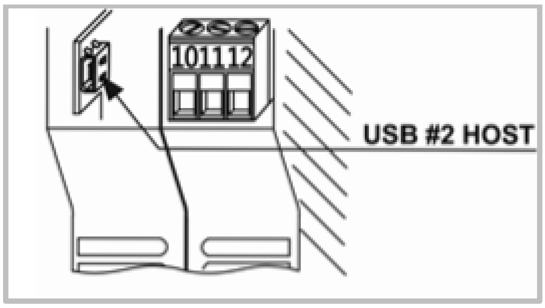
Pin	RS232	RS485
1 (bottom)	CTS	-
2	Tx	B
3	Rx	A
4 (top)	GND	GND

The Device has a USB HOST type A connector, that can be used as an additional serial port (using a Seneca S117P1, for example) or to connect an external USB memory; this is used for FW upgrade (see chapter 15).

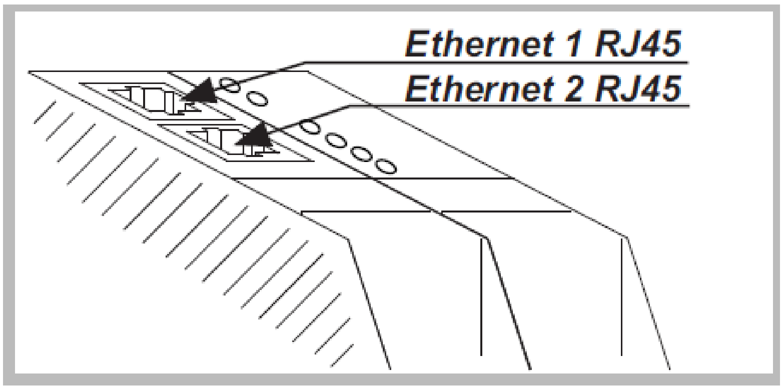
Please note that, on this USB port, the "hotplug" feature is not available; so, after plugging the USB device, it is necessary to power off/on the Z-TWS4/Z-PASS2-S to let it detect the USB device.



The Z-TWS4 also has a second USB HOST connector, with micro-USB plug-in, that can be used to connect a USB device by means of a "Micro USB to USB" adapter.

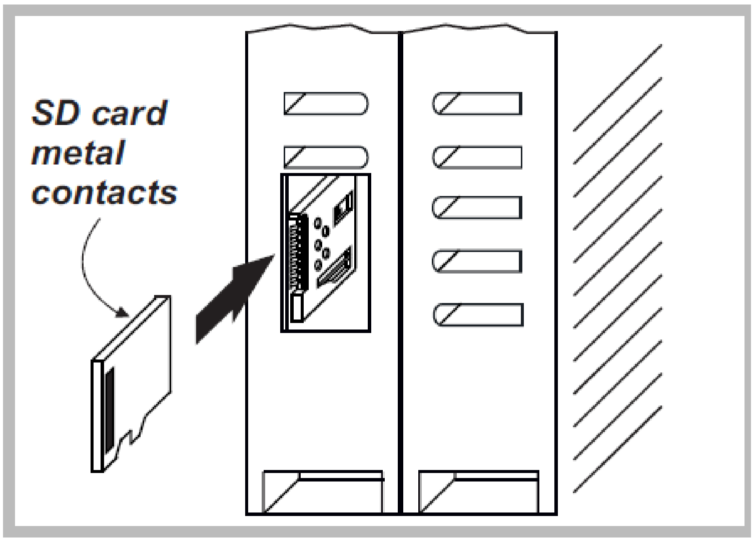


The Device has two Ethernet ports with RJ45 connectors on the front panel. The two ports are internally connected in HUB/SWITCH mode. The two ports have the same MAC Address.

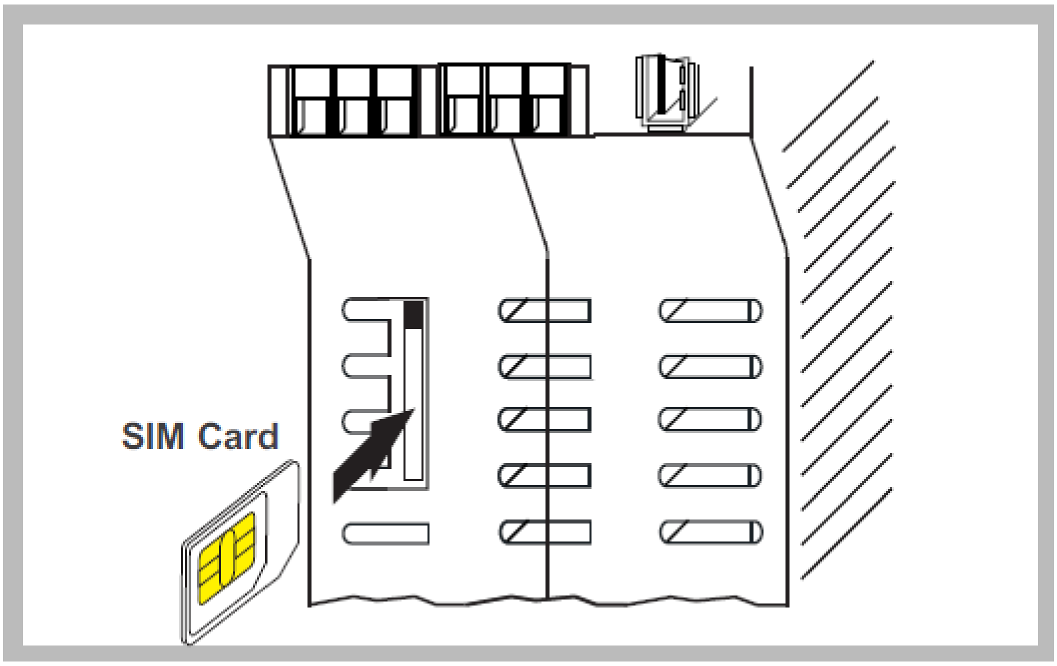


The Device has a plug-in connector for micro SD card placed in the side part of the case.
To insert the SD card into the connector, be sure that the SD card is oriented with metal contacts facing towards left (with reference to the figure).

The SD card can be of any class.

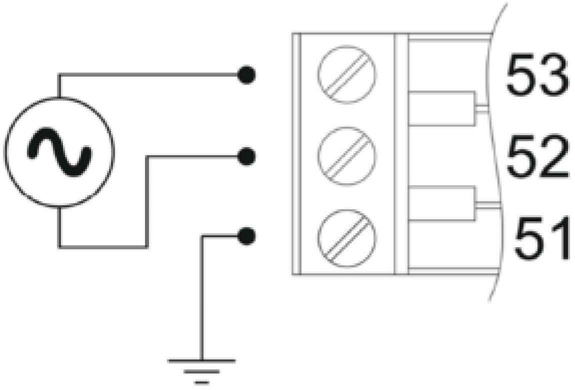


The Z-PASS2-S has a slot for SIM card, placed on the side of the case. Before pushing the SIM card into this slot, please be sure that the SIM card golden contacts are facing towards right (please see the figure below).



4.2 S6001-RTU

Power supply must be connected to screw terminals 52 and 53. The supply voltage must be 24 ± 15 % Vac/dc (any polarity).



Upper limits must not be exceeded to avoid serious damage to the device. It is necessary to protect the power supply source against any failure of the device by means of an appropriately sized fuse.

S6001-RTU has two RS485 serial ports (COM2 and COM4) available on removable screw terminals, as specified in the following table.

Signal	COM2	COM4
GND	57	54
B	58	55
A	59	56

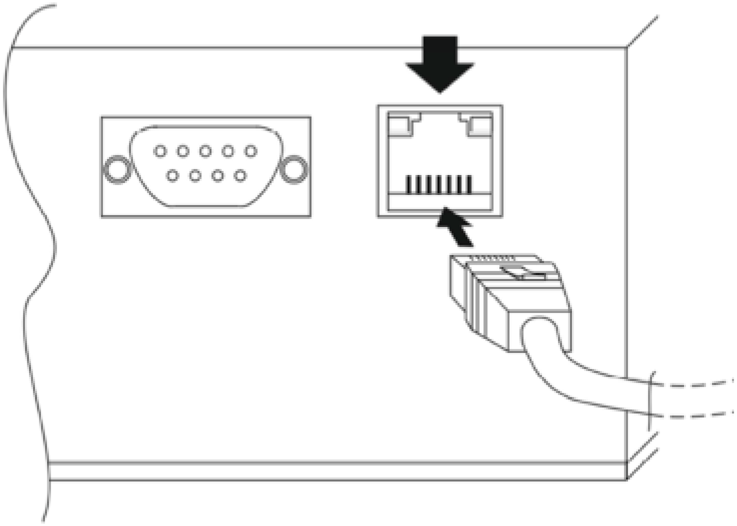
An RS232 serial port with full handshaking signals is available on DB9 male connector on the left side of S6001-RTU. Use the CS-DB9F-DB9F cable[5] to connect RS232 devices.
Signals on DB9 connector are listed in the table below.

Pin	Name	Description	IN/OUT
1	DCD	Data carrier detect	In
2	RXD	Receive data	In
3	TXD	Transmit data	Out
4	DTR	Data terminal ready	Out
5	SG	Signal ground	
6	DSR	Data set ready	In
7	RTS	Request to send	Out
8	CTS	Clear to send	In
9	RI	Ring indicator	In

An optional communication bus is available on removable screw terminals 60,61,62, for future extensions.

S6001-RTU has 1 USB port which is an USB HOST with connector type “A”, suitable to connect, for example, a mass storage (e.g.: a USB pen) with maximum consumption of 300 mA @ 5 Vdc.

An Ethernet port is available on the left side of S6001-RTU on an RJ45 connector.



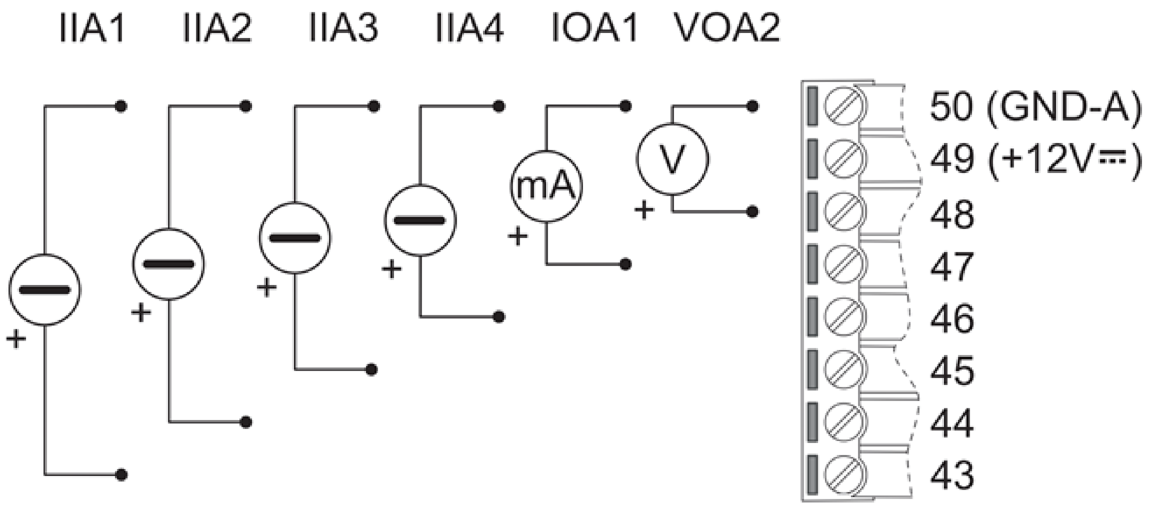
An SD card slot is available, near the optional bus screw terminals; SD cards with storage capacity up to 32 GB can be used.

A SIM card slot, with a push-push connector, is available; 3V mini SIM cards can be used.

Two SMA antenna connectors are available, for Main and Diversity antennas.

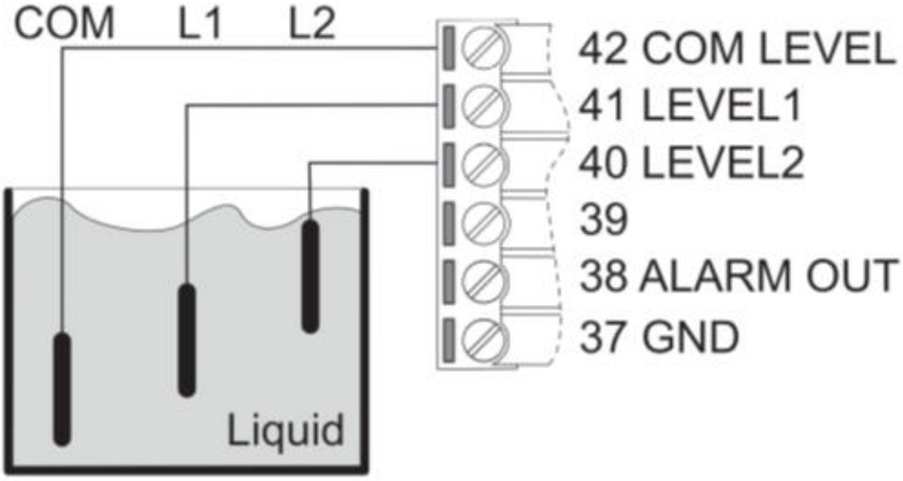
Analog inputs and outputs are available on screw terminals 43-50, as shown in the following figure and table.

[5] The CS-DB9F-DB9F cable is supplied on request.



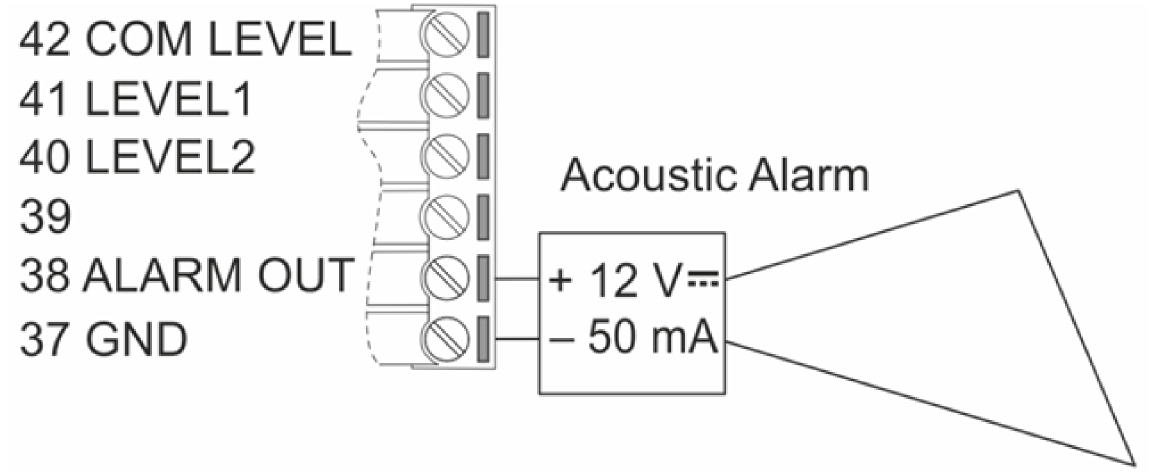
4 analog current inputs (0-20 mA)	Four active sensors are available from 43 to 46 screw terminals. Screw terminal 49 is a supply voltage (+12 Vdc) for passive current sensor.
1 analog current output (0-20 mA)	Available between 47 and 50 screw terminals.
1 analog voltage output (0-10 Vdc)	Available between 48 and 50 screw terminals.

The Liquid Level Inputs are available on screw terminals 40-42, as shown in the following figure.

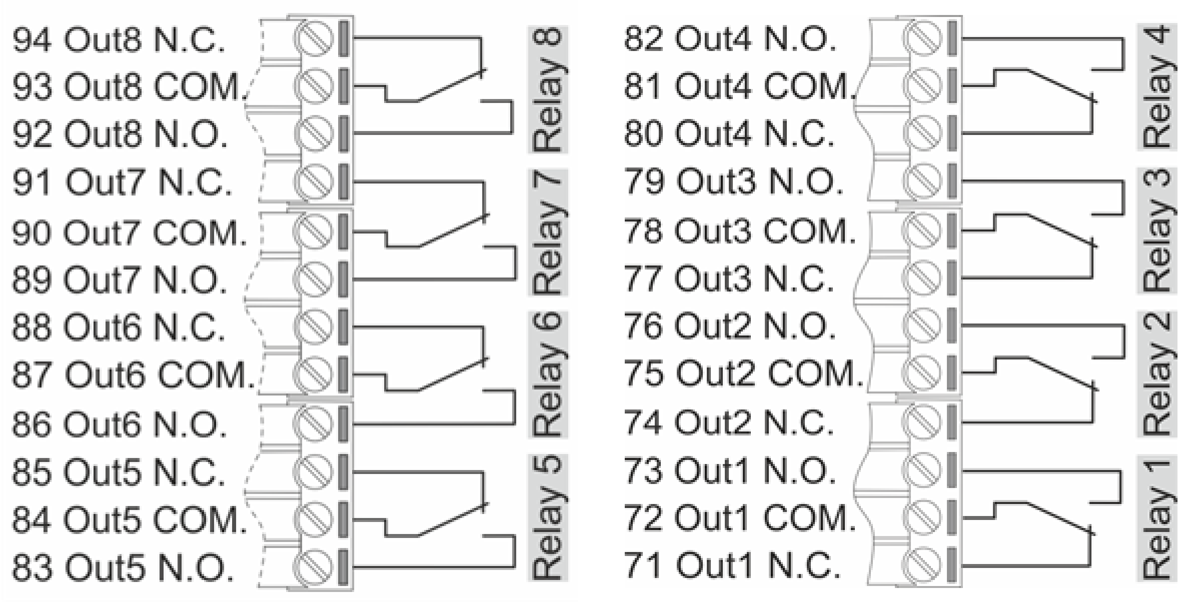


The analog level signals from screw terminals 40, 41, 42 can be used to control the level of liquid in a tank.

The supply voltage (12 Vdc @ 50mA) from screw terminals 38 and 37 can be used to connect, for example, an acoustic alarm. Screw terminal 39 must not be connected.

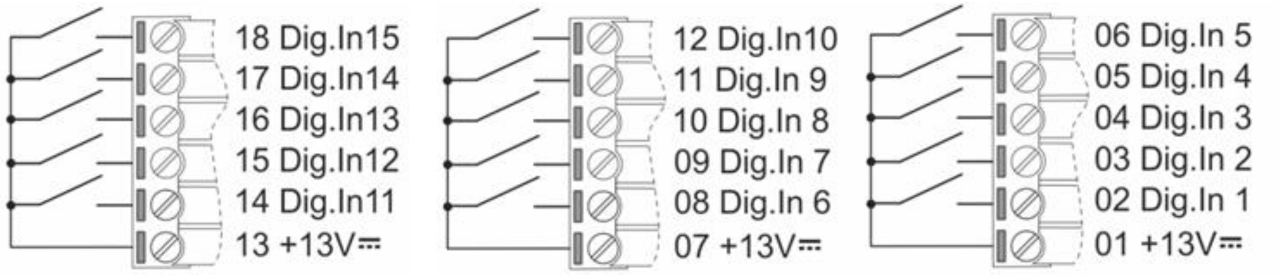


The 8 digital outputs (relays) are available on screw terminals 71-94, as shown in the following figure.



Eight SPDT relays are available to control, for example, external pumps. The operating voltage is 250 Vdc @ 2 A.

The 15 digital inputs are available on screw terminals 1-18, as shown in the following figure.



All digital inputs are PNP type with optoisolation.

5 LEDs signaling

5.1 Z-TWS4, Z-PASS2-S

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Red	Blinking	The module is ready for use
LINK1 Yellow	ON OFF	Ethernet 1 connection detected Ethernet 1 connection absent
ACT1 Green	Blinking OFF	There is data activity (Ethernet 1) There is no data activity (Ethernet 1)
LINK2 Yellow	ON OFF	Ethernet 2 connection detected Ethernet 2 connection absent
ACT2 Green	Blinking OFF	There is data activity (Ethernet 2) There is no data activity (Ethernet 2)
RX1-2-4 Red	Blinking ON OFF	Data reception (COM 1-2-4) Check the connection (COM 1-2-4) No data reception (COM 1-2-4)
TX1-2-4 Red	Blinking ON OFF	Data transmission (COM 1-2-4) Check the connection (COM 1-2-4) No data transmission (COM 1-2-4)
3G PWR Green (Z-PASS2-S only)	ON	The 3G Modem is powered on
STAT Yellow (Z-PASS2-S only)	ON Slow Blinking Fast Blinking	Not registered on GSM network Registered on GSM network Mobile Network connection active

5.2 Z-TWS4-R01, Z-PASS2-S-R01

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Red	Blinking	The module is ready for use
LAN/WAN	ON	The Ethernet ports are working in “LAN/WAN” mode

Yellow	OFF	-
SWITCH Green	ON OFF	The Ethernet ports are working in “Switch” mode -
VPN Yellow	ON Blinking OFF	VPN connection is working properly VPN connection is not working properly VPN functionality is disabled or VPN Box/Point-to-Point functionality is enabled but no client is connected or VPN Box/Single LAN functionality is enabled but the Device is not configured yet
SERV Green	ON Blinking OFF	VPN Box “SERVICE” connection is working properly VPN Box “SERVICE” connection is not working properly VPN Box functionality is disabled
RX1-2-4 Red	Blinking ON OFF	Data reception (COM 1-2-4) Check the connection (COM 1-2-4) No data reception (COM 1-2-4)
TX1-2-4 Red	Blinking ON OFF	Data transmission (COM 1-2-4) Check the connection (COM 1-2-4) No data transmission (COM 1-2-4)
3G PWR Green (Z-PASS2-S-R01 only)	ON	The 3G Modem is powered on
STAT Yellow (Z-PASS2-S-R01 only)	ON Slow Blinking Fast Blinking	Not registered on GSM network Registered on GSM network Mobile Network connection active

Ethernet Connector LEDS

LED	Status	Meaning
ETH1-2 Green	ON OFF	Ethernet 1-2 connection detected Ethernet 1-2 connection absent
ETH1-2 Yellow	Blinking OFF	There is data activity (Ethernet 1-2) There is no data activity (Ethernet 1-2)

5.3 Z-TWS4-R02, Z-PASS2-S-R02

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Green	Blinking	The module is ready for use
DIDO1 Green	ON OFF	Configurable Digital Input/Output 1 state is HIGH Configurable Digital Input/Output 1 state is LOW
DIDO2 Green	ON OFF	Configurable Digital Input/Output 2 state is HIGH Configurable Digital Input/Output 2 state is LOW
DI Green	ON OFF	Digital Input state is HIGH Digital Input state is LOW
DO Green	ON OFF	Digital Output state is HIGH Digital Output state is LOW
REM.DIS. Green	ON OFF	Remote Access is disabled Remote Access is enabled
VPN Green	ON Blinking OFF	VPN connection is working properly VPN connection is not working properly VPN functionality is disabled or VPN Box/Point-to-Point functionality is enabled but no client is connected or VPN Box/Single LAN functionality is enabled but the Device is not configured yet
LAN/WAN Green	ON OFF	The Ethernet ports are working in “LAN/WAN” mode The Ethernet ports are working in “Switch” mode
SERV Green	ON Blinking OFF	VPN Box “SERVICE” connection is working properly VPN Box “SERVICE” connection is not working properly VPN Box functionality is disabled
RX2-4 Green	Blinking ON OFF	Data reception (COM 2-4) Check the connection (COM 2-4) No data reception (COM 2-4)
TX2-4 Green	Blinking ON OFF	Data transmission (COM 2-4) Check the connection (COM 2-4) No data transmission (COM 2-4)

3G PWR Green (Z-PASS2-S-R02 only)	ON	The 3G Modem is powered on
STAT Yellow (Z-PASS2-S-R02 only)	TBD	TBD

Ethernet Connector LEDS

LED	Status	Meaning
ETH1-2 Green	ON OFF	Ethernet 1-2 connection detected Ethernet 1-2 connection absent
ETH1-2 Yellow	Blinking OFF	There is data activity (Ethernet 1-2) There is no data activity (Ethernet 1-2)

5.4 S6001-RTU

Frontal LEDS

Group	Number	Colour	Status		Meaning
Digital Inputs	1,2,3,4,5,6,7,8 9,10,11,12,13,14,15	Green	ON OFF	High Low	
Digital Outputs	1,2,3,4,5,6,7,8	Red	ON OFF	Closed Open	
3G Power Signal	2,3,4,5,6	Yellow	OFF	ON	6 ON = Max
	1		Blinking	ON	1 Blinking = Min
Comm. Port COM2	RX, TX	Red	Blinking		RS485 activity
		Red	Fixed ON		Verify connection
Comm. Port COM4	RX, TX	Red	Blinking		RS485 activity
		Red	Fixed ON		Verify connection
Run	1	Red	Blinking	Run	
Level switch	L1, L2	Green	OFF, OFF (value 0) ON, OFF (value 1) ON, ON (value 2)		Under min level Between min and max levels Over max level

Following are some further notes about LED behavior:

- at power on, during the bootstrap phase, all LEDS, except for the COM PORT LEDs, are ON; when the system is fully operational, RUN LED is blinking
- when Straton application is not running, all LEDS, except for the COM PORT LEDs, are blinking
- 3G PWR SIG LED 1 is blinking, synchronously with RUN LED, in the following situations:
  - GSM/3G network is not available (or signal level is too low)
  - SIM is not inserted

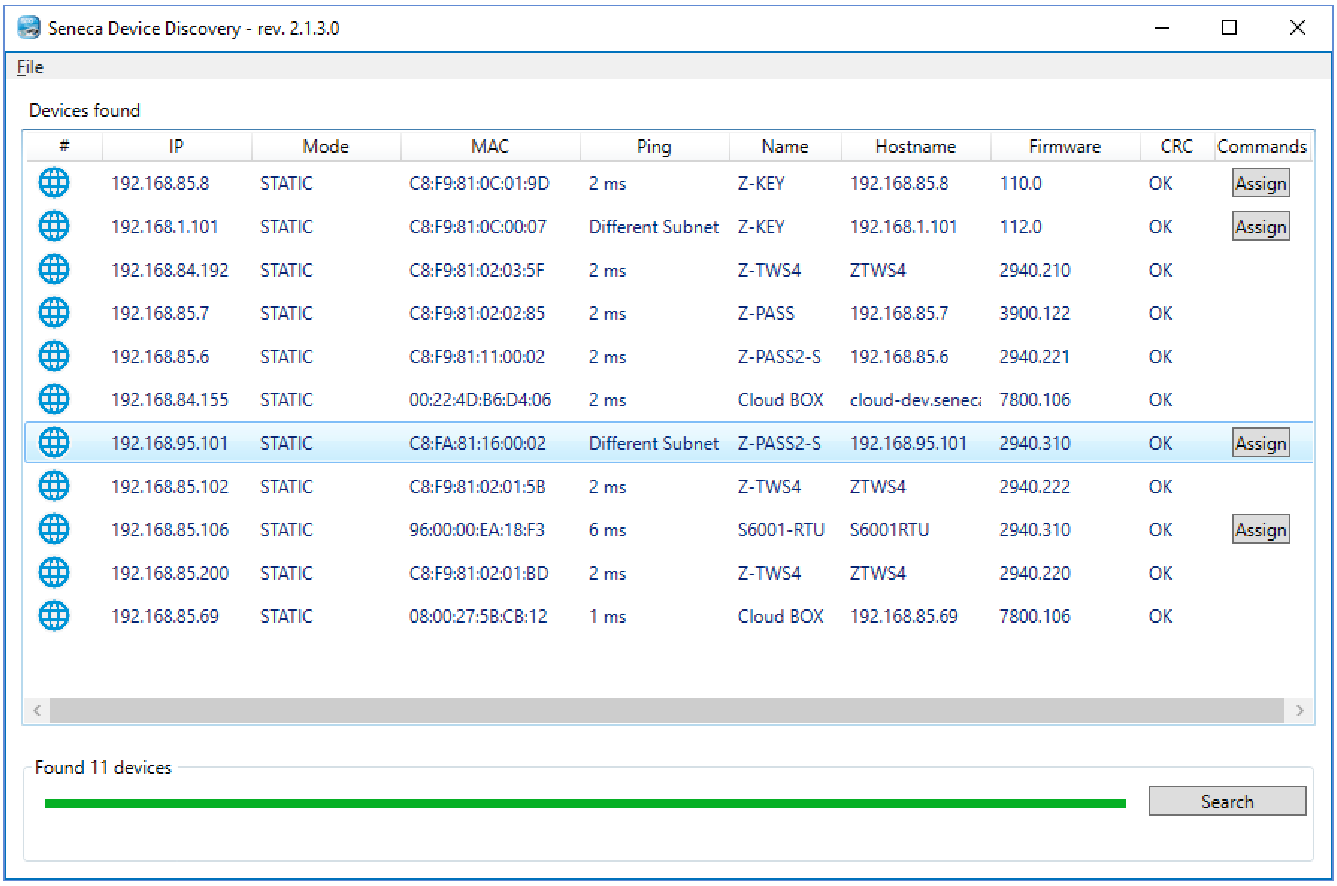
Modem LEDS

LED	Status	Meaning
3G PWR Green	ON	The 3G Modem is powered on
STAT Yellow	ON Slow Blinking Fast Blinking	Not registered on GSM network Registered on GSM network Mobile Network connection active

6 Discovering the IP address

Z-TWS4/Z-PASS2-S/S6001-RTU devices come out of the factory with the default 192.168.90.101 IP address on the Ethernet network interface.

If this address is changed, *and forgotten*, it can be retrieved by running the “Seneca Device Discovery” (SDD) application, as shown in the following figure:

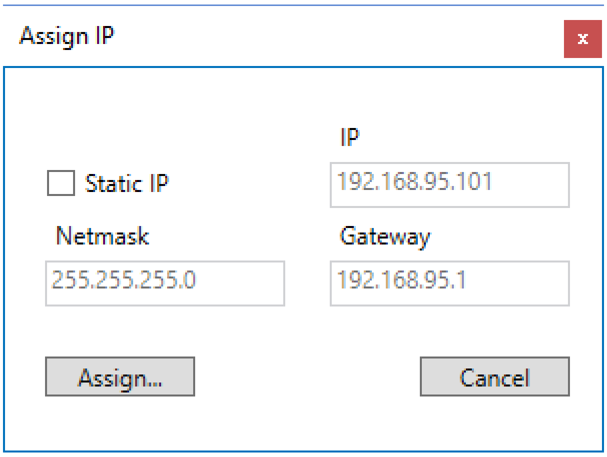


#	IP	Mode	MAC	Ping	Name	Hostname	Firmware	CRC	Commands
🌐	192.168.85.8	STATIC	C8:F9:81:0C:01:9D	2 ms	Z-KEY	192.168.85.8	110.0	OK	Assign
🌐	192.168.1.101	STATIC	C8:F9:81:0C:00:07	Different Subnet	Z-KEY	192.168.1.101	112.0	OK	Assign
🌐	192.168.84.192	STATIC	C8:F9:81:02:03:5F	2 ms	Z-TWS4	ZTWS4	2940.210	OK	
🌐	192.168.85.7	STATIC	C8:F9:81:02:02:85	2 ms	Z-PASS	192.168.85.7	3900.122	OK	
🌐	192.168.85.6	STATIC	C8:F9:81:11:00:02	2 ms	Z-PASS2-S	192.168.85.6	2940.221	OK	
🌐	192.168.84.155	STATIC	00:22:4D:B6:D4:06	2 ms	Cloud BOX	cloud-dev.senec	7800.106	OK	
🌐	192.168.95.101	STATIC	C8:FA:81:16:00:02	Different Subnet	Z-PASS2-S	192.168.95.101	2940.310	OK	Assign
🌐	192.168.85.102	STATIC	C8:F9:81:02:01:5B	2 ms	Z-TWS4	ZTWS4	2940.222	OK	
🌐	192.168.85.106	STATIC	96:00:00:EA:18:F3	6 ms	S6001-RTU	S6001RTU	2940.310	OK	Assign
🌐	192.168.85.200	STATIC	C8:F9:81:02:01:BD	2 ms	Z-TWS4	ZTWS4	2940.220	OK	
🌐	192.168.85.69	STATIC	08:00:27:5B:CB:12	1 ms	Cloud BOX	192.168.85.69	7800.106	OK	

Found 11 devices

This application shows the IP address, MAC address, FW version and some other useful information, for every Z-TWS4/Z-PASS2-S/S6001-RTU device (and other Seneca products) found in the LAN.

Moreover, by clicking on the “Assign” button, it is possible to change the network configuration parameters of a device, as shown in the following figure:



Assign IP

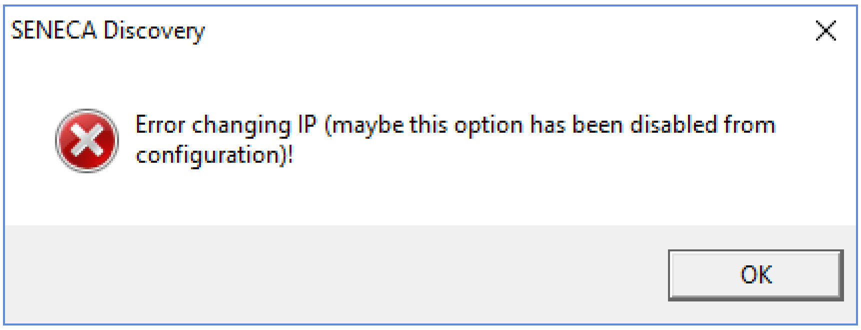
□ Static IP

IP: 192.168.95.101

Netmask: 255.255.255.0

Gateway: 192.168.95.1

For security reasons, this feature can be disabled on the Device (see paragraph 16.1.2); in this case, the following error message is shown, after clicking on the "Assign" button".



SENECA Discovery

Error changing IP (maybe this option has been disabled from configuration)!

The SDD can be easily installed by running the installer program available at the following link:

http://www.seneca.it/products/sdd

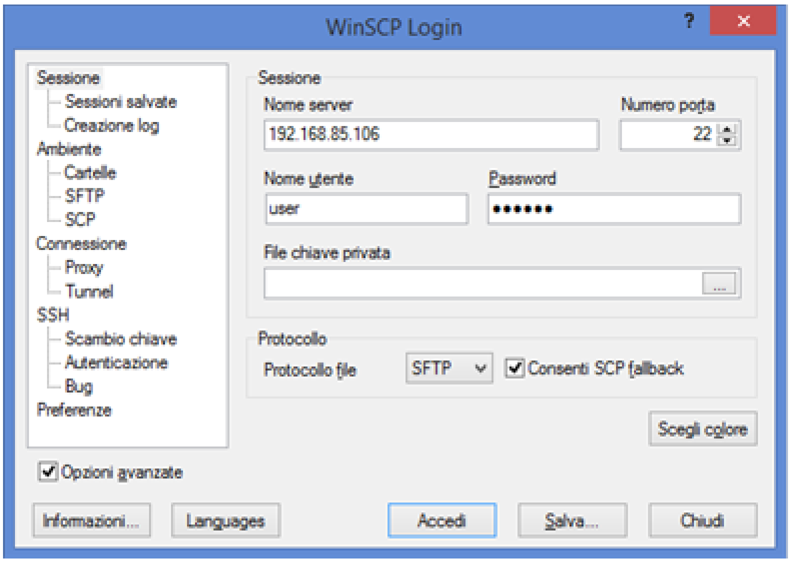
NOTE:
- when the Device is working in "Switch" mode, the IP Address shown by the SDD is the same regardless of the Ethernet port which the PC running the SDD is connected to;
- when the Device is working in "LAN/WAN" mode, the IP Address shown by the SDD is the LAN IP Address when the PC is connected to the LAN port, the WAN IP Address when the PC is connected to the WAN port; moreover, the network configuration parameter changes apply to the relevant port.

7 FTP/SFTP access

To easily access the Device by means of FTP/SFTP, you can use the WINSCP™ program; you can free download WINSCP™ from:

http://winscp.net/eng/download.php

You must set the connection as in the following figure (the screenshot shows a connection to the 192.168.85.106 IP address):



Nome server: 192.168.85.106

Numero porta: 22

Nome utente: user

Password: ••••••

File chiave privata:

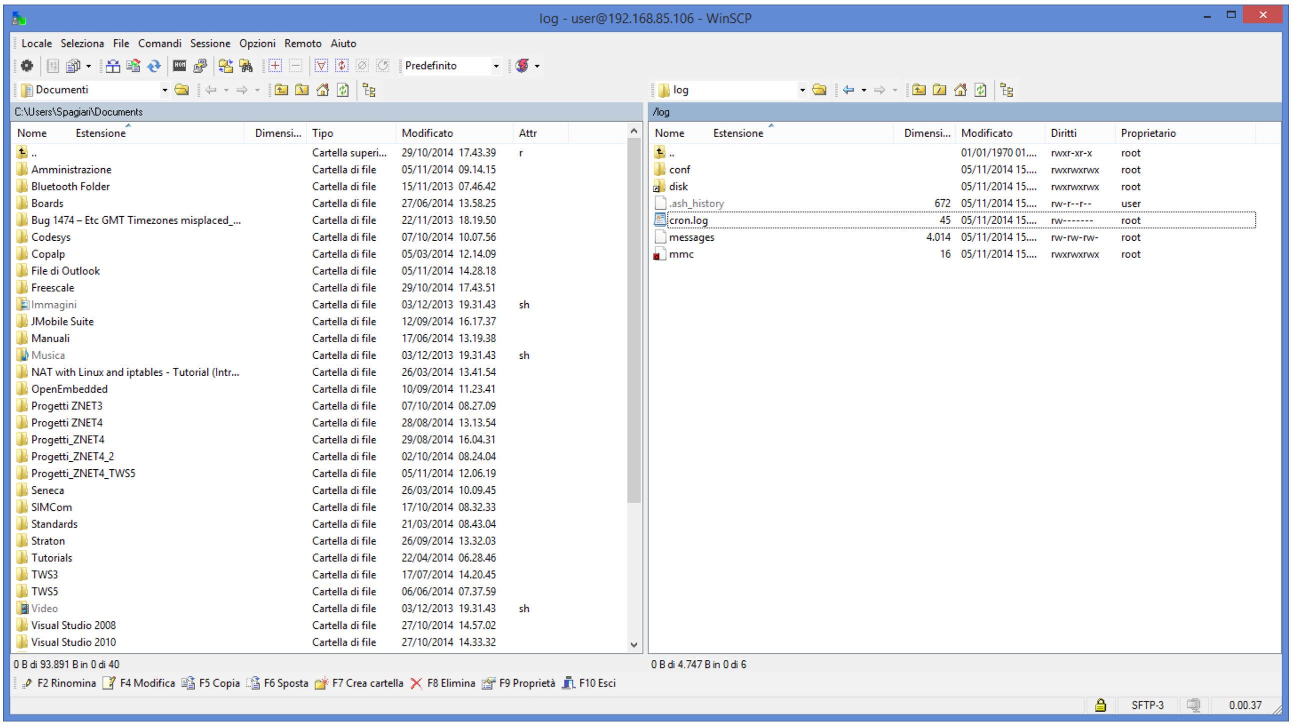
Protocollo file: SFTP

☑ Consenti SCP fallback

☑ Opzioni avanzate

The credentials (username and password) are those (“user”, “123456”) set for the “FTP USER” (see “Users Configuration” web page in paragraph 16.1.6).

After clicking the “Access” button, you will get a new window, as in the following screenshot; on the right, you can copy and delete files directly to/from the Device.



C:\Users\Spagiari\Documents

Nome	Estensione	Dimensi...	Tipo	Modificato	Attr
..			Cartella superi...	29/10/2014 17.43.39	r
Amministrazione			Cartella di file	05/11/2014 09.14.15	
Bluetooth Folder			Cartella di file	15/11/2013 07.46.42	
Boards			Cartella di file	27/06/2014 13.58.25	
Bug 1474 – Etc GMT Timezones misplaced_...			Cartella di file	22/11/2013 18.19.50	
Codesys			Cartella di file	07/10/2014 10.07.56	
Copalp			Cartella di file	05/03/2014 12.14.09	
File di Outlook			Cartella di file	05/11/2014 14.28.18	
Freescale			Cartella di file	29/10/2014 17.43.51	
Immagini			Cartella di file	03/12/2013 19.31.43	sh
JMobile Suite			Cartella di file	12/09/2014 16.17.37	
Manuali			Cartella di file	17/06/2014 13.19.38	
Musica			Cartella di file	03/12/2013 19.31.43	sh
NAT with Linux and iptables - Tutorial (Intr...			Cartella di file	26/03/2014 13.41.54	
OpenEmbedded			Cartella di file	10/09/2014 11.23.41	
Progetti ZNET3			Cartella di file	07/10/2014 08.27.09	
Progetti ZNET4			Cartella di file	28/08/2014 13.13.54	
Progetti_ZNET4			Cartella di file	29/08/2014 16.04.31	
Progetti_ZNET4_2			Cartella di file	02/10/2014 08.24.04	
Progetti_ZNET4_TWS5			Cartella di file	05/11/2014 12.06.19	
Seneca			Cartella di file	26/03/2014 10.09.45	
SIMCom			Cartella di file	17/10/2014 08.32.33	
Standards			Cartella di file	21/03/2014 08.43.04	
Straton			Cartella di file	26/09/2014 13.32.03	
Tutorials			Cartella di file	22/04/2014 06.28.46	
TWS3			Cartella di file	17/07/2014 14.20.45	
TWS5			Cartella di file	06/06/2014 07.37.59	
Video			Cartella di file	03/12/2013 19.31.43	sh
Visual Studio 2008			Cartella di file	27/10/2014 14.57.02	
Visual Studio 2010			Cartella di file	27/10/2014 14.33.32	

0 B di 93.891 B in 0 di 40

/log

Nome	Estensione	Dimensi...	Modificato	Diritti	Proprietario
..			01/01/1970 01....	rwxr-xr-x	root
conf			05/11/2014 15....	rwxrwxrwx	root
disk			05/11/2014 15....	rwxrwxrwx	root
.ash_history		672	05/11/2014 15....	rw-r--r--	user
cron.log		45	05/11/2014 15....	rw-------	root
messages		4.014	05/11/2014 15....	rw-rw-rw-	root
mmc		16	05/11/2014 15....	rwxrwxrwx	root

0 B di 4.747 B in 0 di 6

SFTP-3 0.00.37

The WinSCP program can be used both as an FTP or SFTP client to transfer files to/from the Device; just select “FTP” or “SFTP” protocol in the “WinSCP Login” window; normally, it’s better to use SFTP, since it provides a secure (i.e. encrypted) service.

8 StratON PLC

Z-TWS4/Z-PASS2-S/S6001-RTU StratON PLC provides the full support for IEC 61131-3 PLC Standard; an Integrated Development Environment (IDE) is available for Windows™ PCs.

The StratON IDE includes several tools such as: a fieldbus configuration tool, an analog signal editor and program editors compliant with the five languages of the IEC 61131-3 Standard: Sequential Function Chart (SFC), Function Block Diagram (FBD), Ladder Diagram (LD), Structured Text (ST), Instruction List (IL).

With StratON IDE, it’s simple to write, download and debug IEC 61131-3 code.

8.1 Writing, downloading and running the first program

To let the PLC developer easily create StratON applications for Seneca CPUs, the following libraries are available:

- a Function Block (FB) and Functions library, which provides some frequently used functionalities, particularly related to communication and data transfer tasks, compiled in the CPU firmware; the direct use of these FBs and functions is targeted at skilled PLC developers (a detailed description of the FBs and Functions is given in chapter 17);
- a “Profiles” library, which provides access to the CPU I/Os by means of “profiled” variables; this is needed for S6001-RTU, Z-PASS2-S-RO2 and Z-TWS4-R02 CPUs;
- a “User Defined Function Block” (UDFB) library, in ST language, which simplifies the use of the above FBs, providing a simpler and “higher level” access to their functionalities.

Furthermore, two project templates are available for Z-PASS2-S and S6001-RTU CPUs, respectively.

An installer program, called *“Seneca StratON Package setup”*, is available which automatically installs the above Seneca libraries and templates. The installer can also be used to install the StratON IDE and Z-NET4 SW (see chapter 18).

The installer is available at the following link:

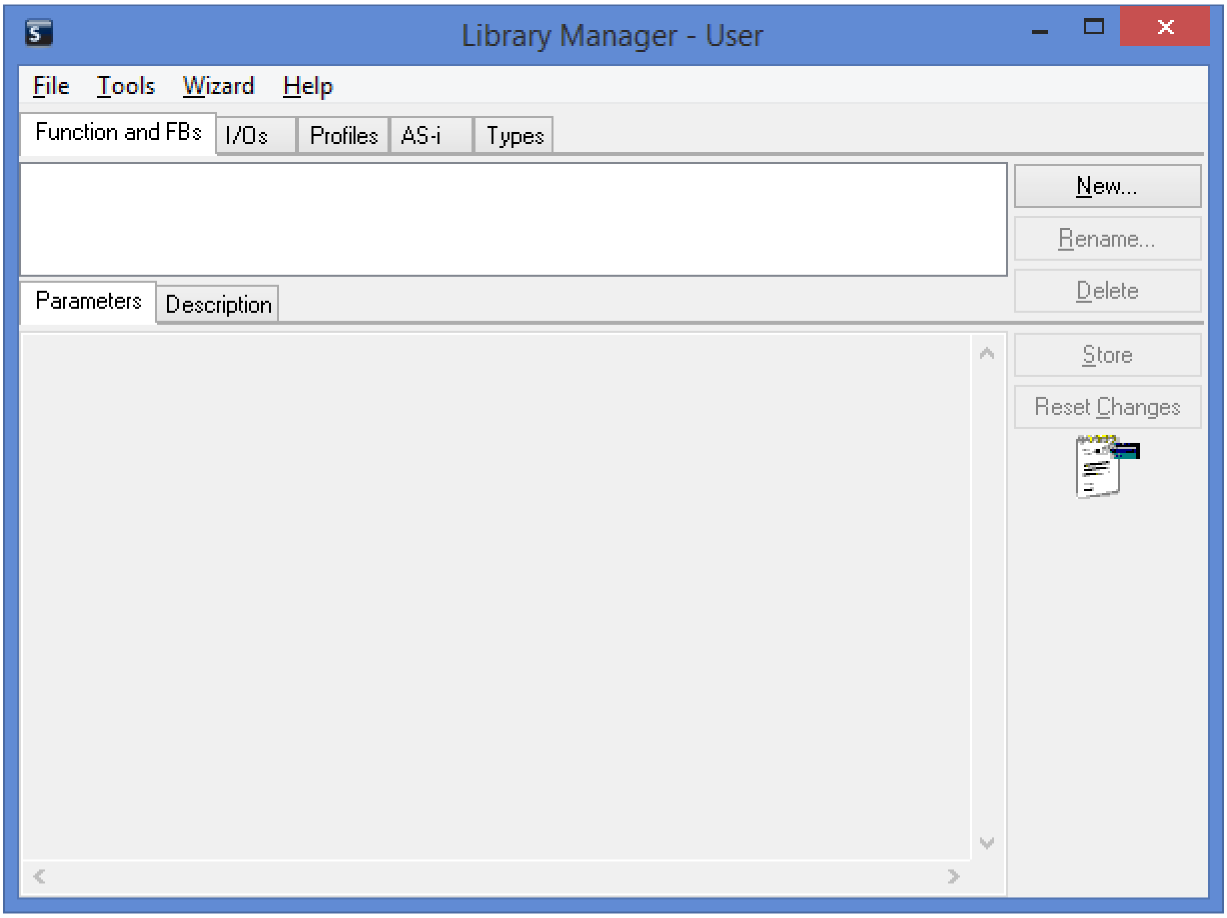
http://www.seneca.it/products/seneca-straton-package

If, for some reasons, the installer can’t be run, the above libraries and templates can be installed manually as described in the following sub-paragraph.

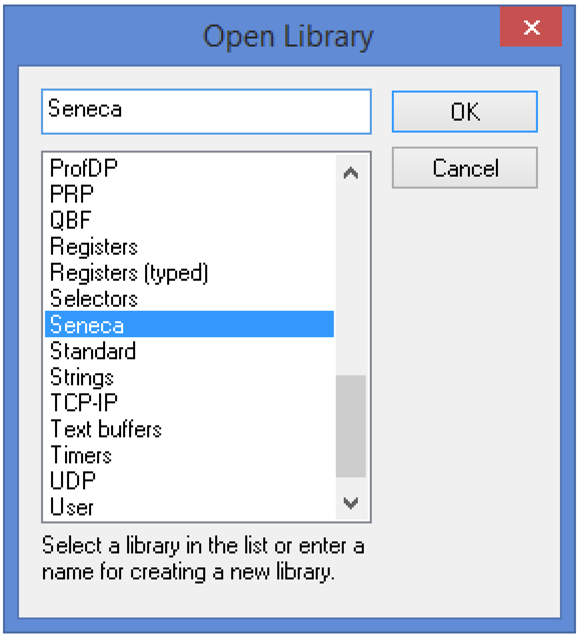
8.1.1 Seneca libraries and templates installation

The following steps are needed to integrate the Seneca libraries and templates in the StratON IDE.

First, we must add the Seneca FB Library (file *SenecaStratonLibrary.XL5*) to the IDE, using the “Library Manager” tool:



Select the “File / Open Library” option and enter the “Seneca” name to create the new Seneca library.

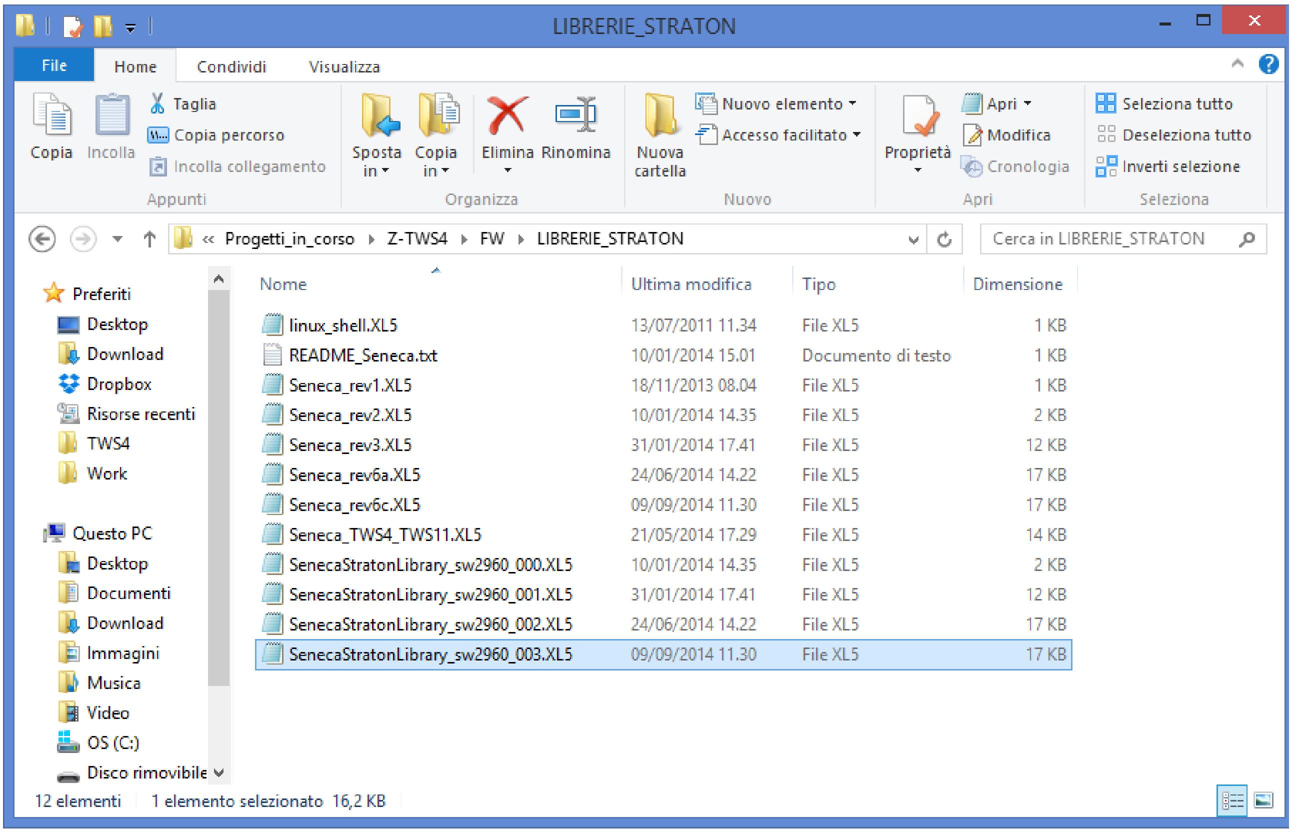


Seneca

- ProfDP
- PRP
- QBF
- Registers
- Registers (typed)
- Selectors
- Seneca
- Standard
- Strings
- TCP-IP
- Text buffers
- Timers
- UDP
- User

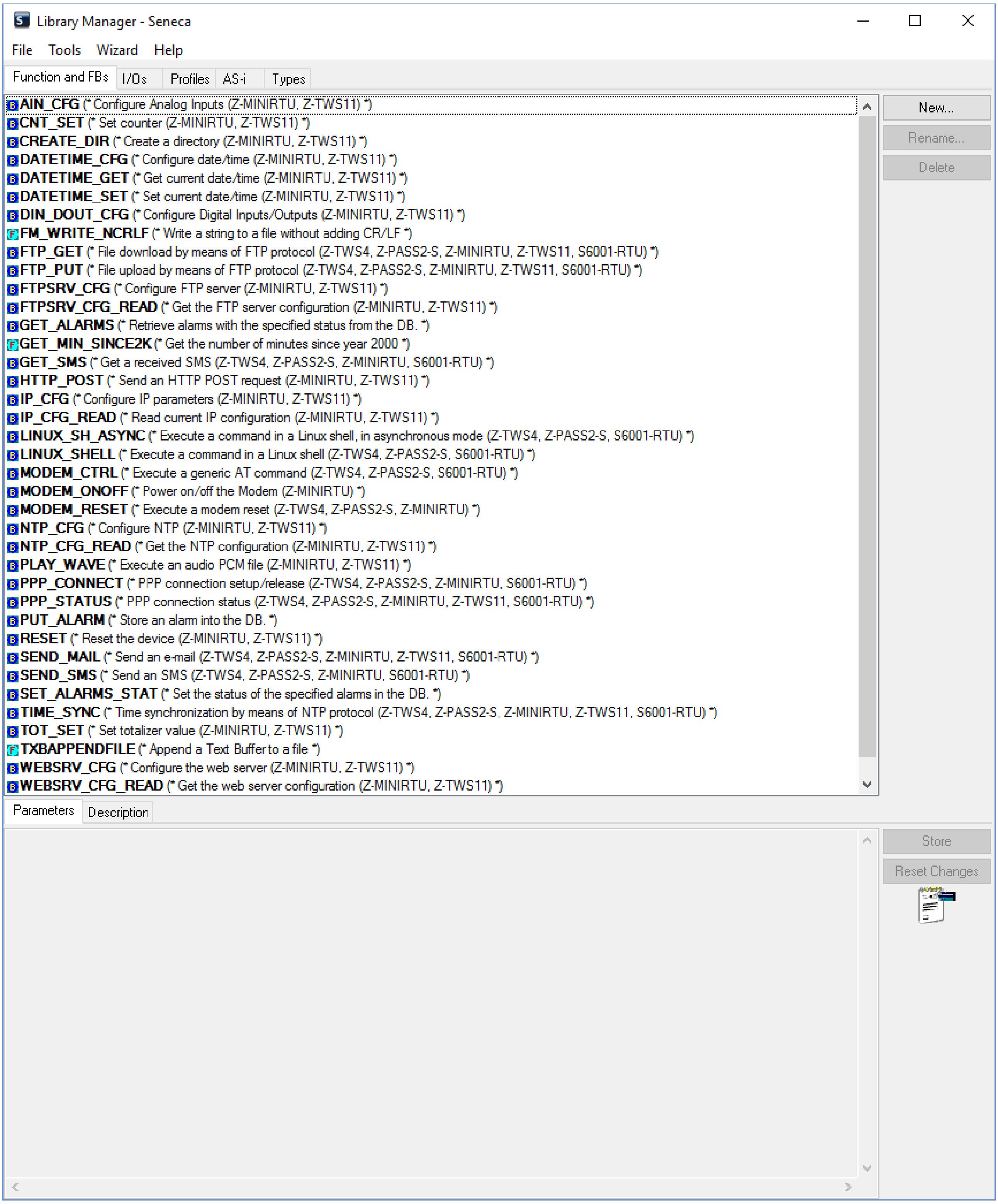
Select a library in the list or enter a name for creating a new library.

Then, import the Library (menu “Tools / Import”):



Nome	Ultima modifica	Tipo	Dimensione
linux_shell.XL5	13/07/2011 11.34	File XL5	1 KB
README_Seneca.txt	10/01/2014 15.01	Documento di testo	1 KB
Seneca_rev1.XL5	18/11/2013 08.04	File XL5	1 KB
Seneca_rev2.XL5	10/01/2014 14.35	File XL5	2 KB
Seneca_rev3.XL5	31/01/2014 17.41	File XL5	12 KB
Seneca_rev6a.XL5	24/06/2014 14.22	File XL5	17 KB
Seneca_rev6c.XL5	09/09/2014 11.30	File XL5	17 KB
Seneca_TWS4_TWS11.XL5	21/05/2014 17.29	File XL5	14 KB
SenecaStratonLibrary_sw2960_000.XL5	10/01/2014 14.35	File XL5	2 KB
SenecaStratonLibrary_sw2960_001.XL5	31/01/2014 17.41	File XL5	12 KB
SenecaStratonLibrary_sw2960_002.XL5	24/06/2014 14.22	File XL5	17 KB
SenecaStratonLibrary_sw2960_003.XL5	09/09/2014 11.30	File XL5	17 KB

12 elementi 1 elemento selezionato 16,2 KB



```
AIN_CFG (* Configure Analog Inputs (Z-MINIRTU, Z-TWS11) *)
CNT_SET (* Set counter (Z-MINIRTU, Z-TWS11) *)
CREATE_DIR (* Create a directory (Z-MINIRTU, Z-TWS11) *)
DATETIME_CFG (* Configure date/time (Z-MINIRTU, Z-TWS11) *)
DATETIME_GET (* Get current date/time (Z-MINIRTU, Z-TWS11) *)
DATETIME_SET (* Set current date/time (Z-MINIRTU, Z-TWS11) *)
DIN_DOUT_CFG (* Configure Digital Inputs/Outputs (Z-MINIRTU, Z-TWS11) *)
FM_WRITE_NCRLF (* Write a string to a file without adding CR/LF *)
FTP_GET (* File download by means of FTP protocol (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
FTP_PUT (* File upload by means of FTP protocol (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
FTPSRV_CFG (* Configure FTP server (Z-MINIRTU, Z-TWS11) *)
FTPSRV_CFG_READ (* Get the FTP server configuration (Z-MINIRTU, Z-TWS11) *)
GET_ALARMS (* Retrieve alarms with the specified status from the DB. *)
GET_MIN_SINCE2K (* Get the number of minutes since year 2000 *)
GET_SMS (* Get a received SMS (Z-TWS4, Z-PASS2-S, Z-MINIRTU, S6001-RTU) *)
HTTP_POST (* Send an HTTP POST request (Z-MINIRTU, Z-TWS11) *)
IP_CFG (* Configure IP parameters (Z-MINIRTU, Z-TWS11) *)
IP_CFG_READ (* Read current IP configuration (Z-MINIRTU, Z-TWS11) *)
LINUX_SH_ASYNC (* Execute a command in a Linux shell, in asynchronous mode (Z-TWS4, Z-PASS2-S, S6001-RTU) *)
LINUX_SHELL (* Execute a command in a Linux shell (Z-TWS4, Z-PASS2-S, S6001-RTU) *)
MODEM_CTRL (* Execute a generic AT command (Z-TWS4, Z-PASS2-S, S6001-RTU) *)
MODEM_ONOFF (* Power on/off the Modem (Z-MINIRTU) *)
MODEM_RESET (* Execute a modem reset (Z-TWS4, Z-PASS2-S, Z-MINIRTU) *)
NTP_CFG (* Configure NTP (Z-MINIRTU, Z-TWS11) *)
NTP_CFG_READ (* Get the NTP configuration (Z-MINIRTU, Z-TWS11) *)
PLAY_WAVE (* Execute an audio PCM file (Z-MINIRTU, Z-TWS11) *)
PPP_CONNECT (* PPP connection setup/release (Z-TWS4, Z-PASS2-S, Z-MINIRTU, S6001-RTU) *)
PPP_STATUS (* PPP connection status (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
PUT_ALARM (* Store an alarm into the DB. *)
RESET (* Reset the device (Z-MINIRTU, Z-TWS11) *)
SEND_MAIL (* Send an e-mail (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
SEND_SMS (* Send an SMS (Z-TWS4, Z-PASS2-S, Z-MINIRTU, S6001-RTU) *)
SET_ALARMS_STAT (* Set the status of the specified alarms in the DB. *)
TIME_SYNC (* Time synchronization by means of NTP protocol (Z-TWS4, Z-PASS2-S, Z-MINIRTU, Z-TWS11, S6001-RTU) *)
TOT_SET (* Set totalizer value (Z-MINIRTU, Z-TWS11) *)
TXBAPPENDFILE (* Append a Text Buffer to a file *)
WEBSRV_CFG (* Configure the web server (Z-MINIRTU, Z-TWS11) *)
WEBSRV_CFG_READ (* Get the web server configuration (Z-MINIRTU, Z-TWS11) *)
```

Save the library (menu "File / Save Library").

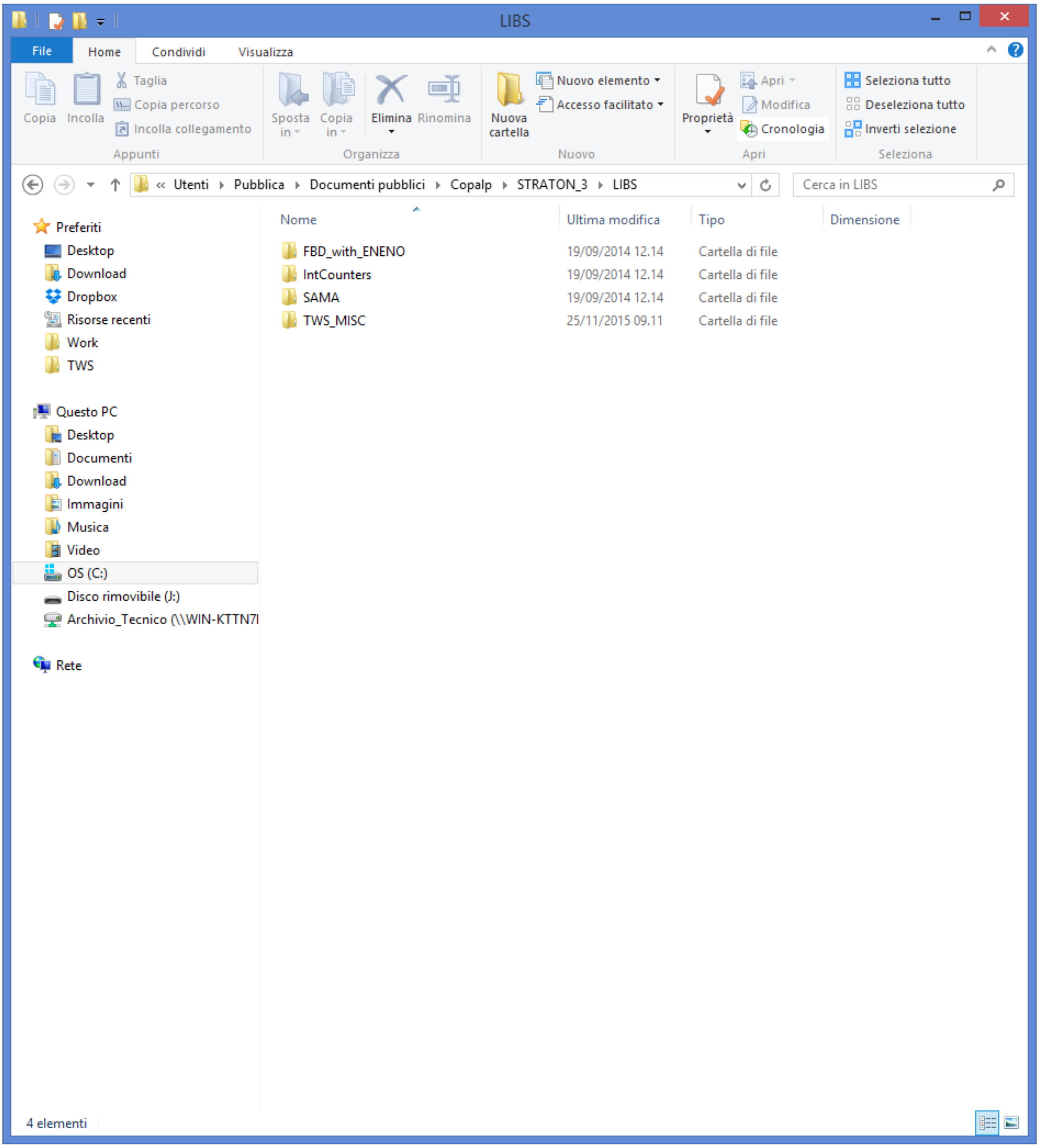
The procedure to add the "Profiles library" to the IDE is identical to the one just explained; the only difference is that the *SenecaStratonProfiles.XL5* file shall be selected (instead of the *SenecaStratonLibrary.XL5* file).

Now that the "low-level" FBs are available, we have to install the UDFB library.

The UDFB library is provided as a zip file, containing the following folders:

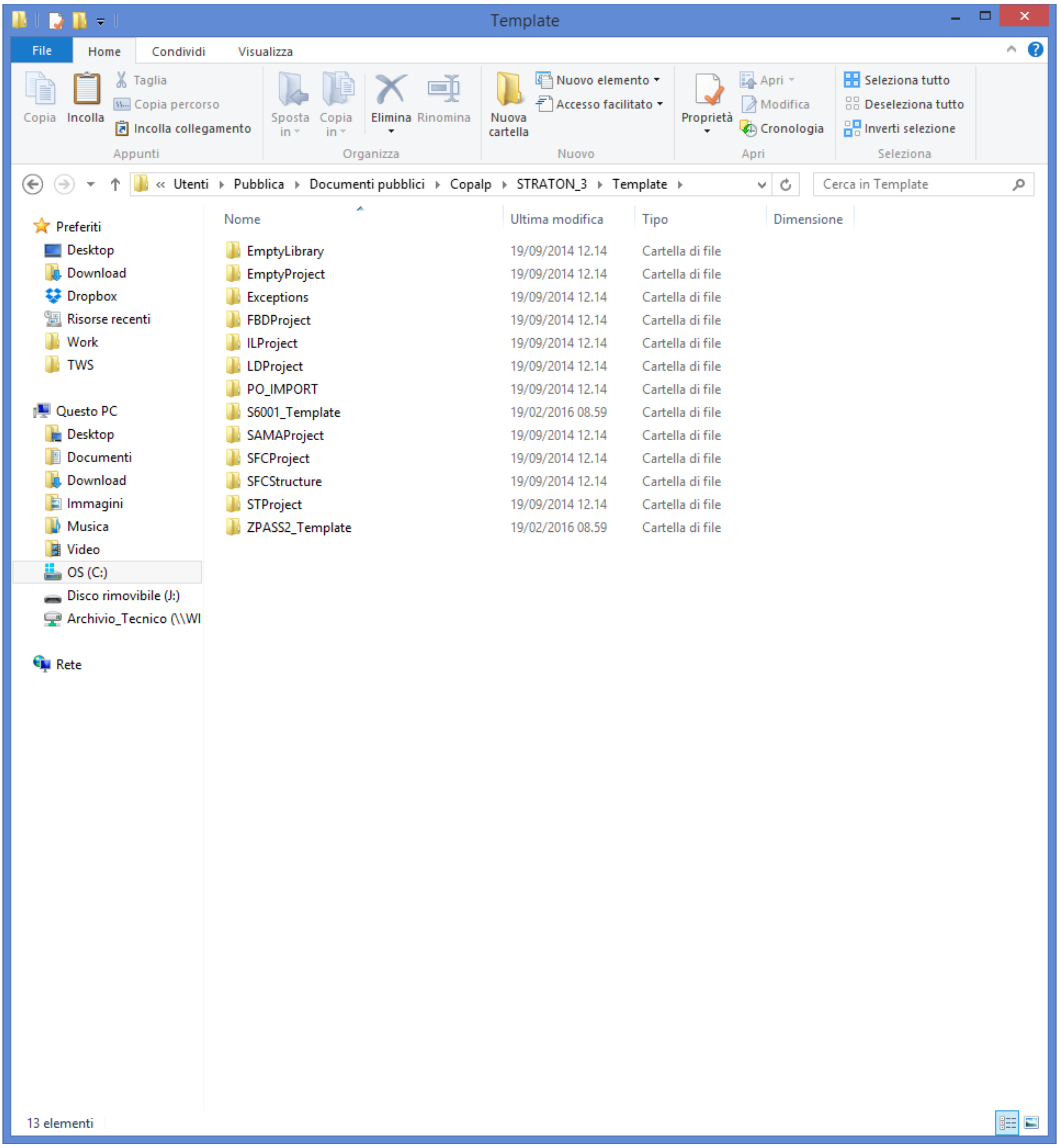
- *TWS_MISC*
- *ZPASS2_Template*
- *S6001_Template*

The *TWS_MISC* folder shall be copied into the following directory:
C:\Users\Public\Documents\Copalp\STRATON\LIBS



Nome	Ultima modifica	Tipo	Dimensione
FBD_with_ENENO	19/09/2014 12.14	Cartella di file	
IntCounters	19/09/2014 12.14	Cartella di file	
SAMA	19/09/2014 12.14	Cartella di file	
TWS_MISC	25/11/2015 09.11	Cartella di file	

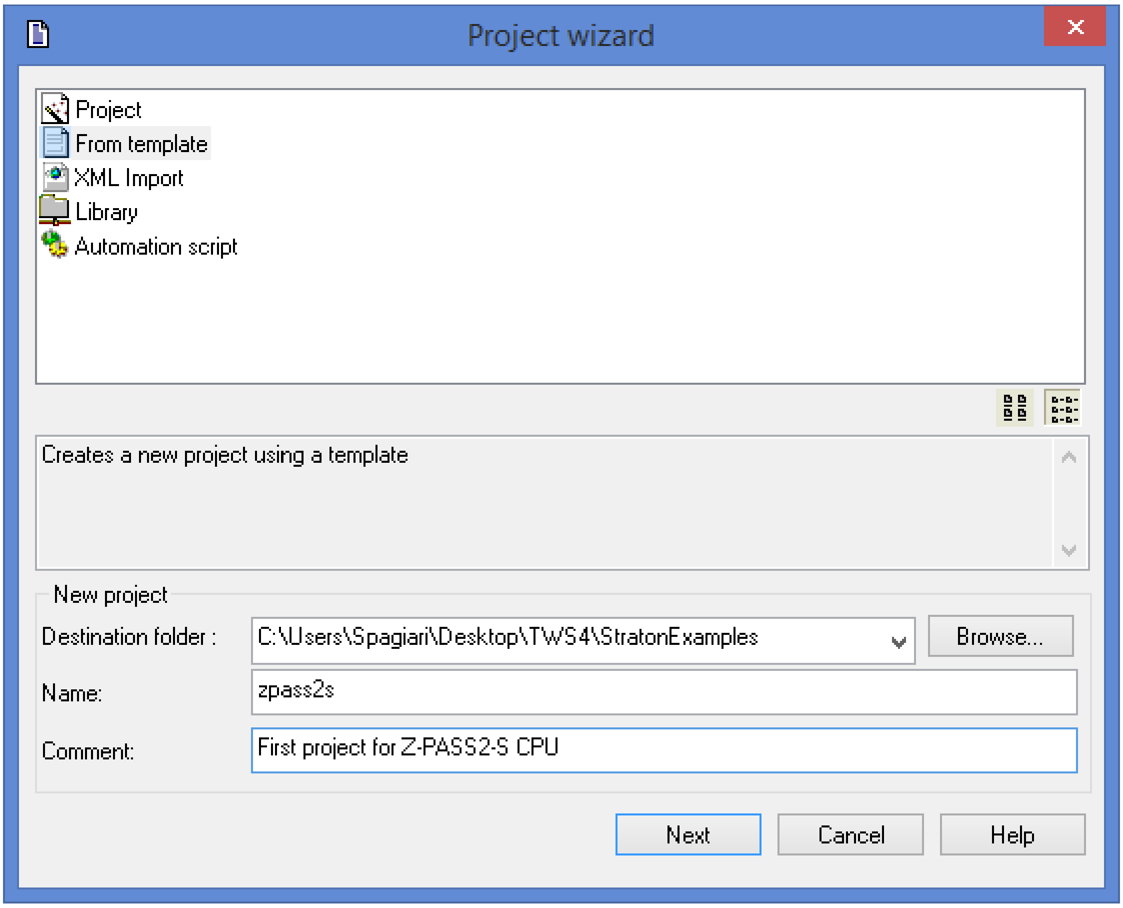
The *ZPASS2_Template* and *S6001_Template* folders shall be copied into the following directory:
C:\Users\Public\Documents\Copalp\STRATON\Template



Nome	Ultima modifica	Tipo	Dimensione
EmptyLibrary	19/09/2014 12.14	Cartella di file	
EmptyProject	19/09/2014 12.14	Cartella di file	
Exceptions	19/09/2014 12.14	Cartella di file	
FBDProject	19/09/2014 12.14	Cartella di file	
ILProject	19/09/2014 12.14	Cartella di file	
LDProject	19/09/2014 12.14	Cartella di file	
PO_IMPORT	19/09/2014 12.14	Cartella di file	
S6001_Template	19/02/2016 08.59	Cartella di file	
SAMAProject	19/09/2014 12.14	Cartella di file	
SFCProject	19/09/2014 12.14	Cartella di file	
SFCStructure	19/09/2014 12.14	Cartella di file	
STProject	19/09/2014 12.14	Cartella di file	
ZPASS2_Template	19/02/2016 08.59	Cartella di file	

8.1.2 Creating a project for Seneca CPUs

Run the StratON IDE and create a new project based on a template, as in the following figure:



Creates a new project using a template

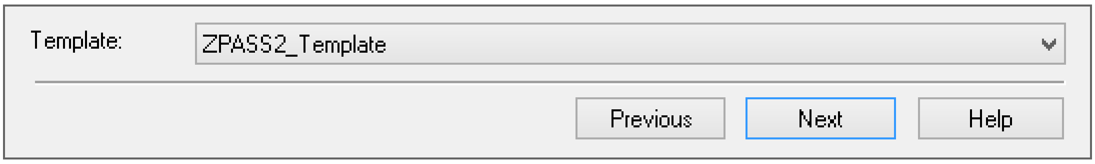
New project

Destination folder : C:\Users\Spagiari\Desktop\TWS4\StratonExamples

Name: zpass2s

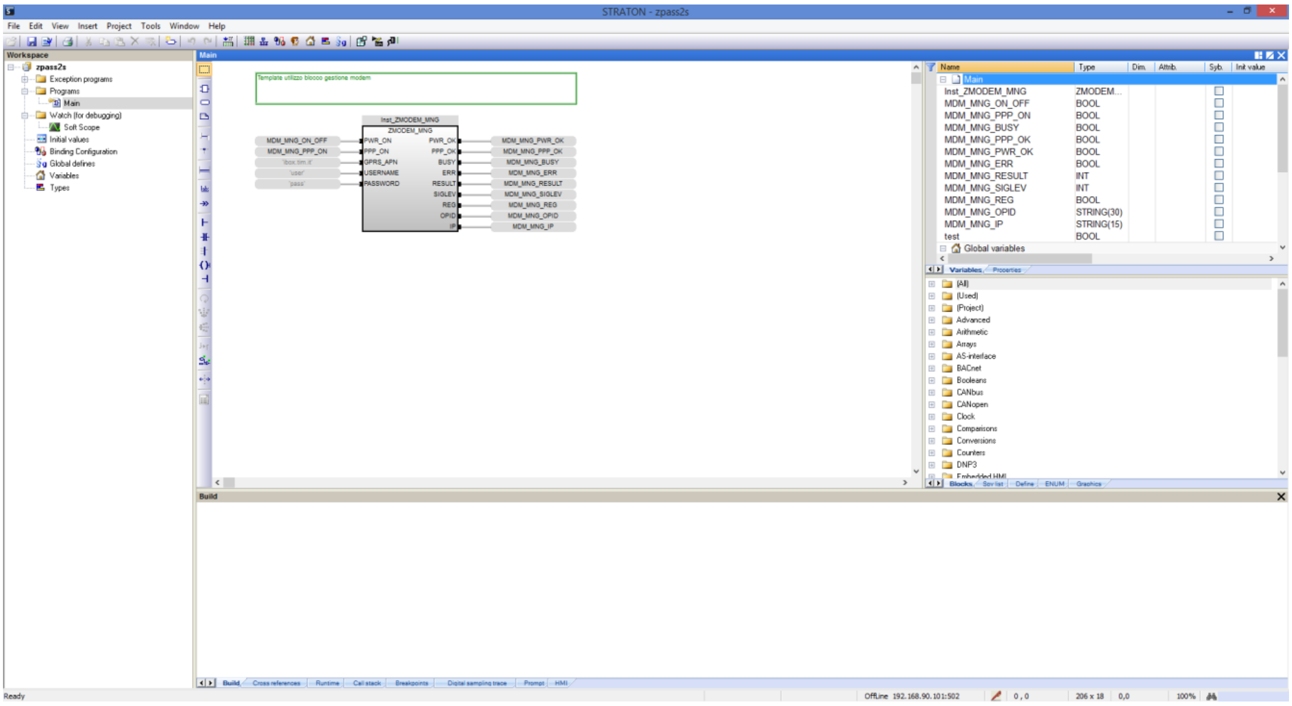
Comment: First project for Z-PASS2-S CPU

Select the “ZPASS2_Template” (or “S6001_Template”) in the template list.



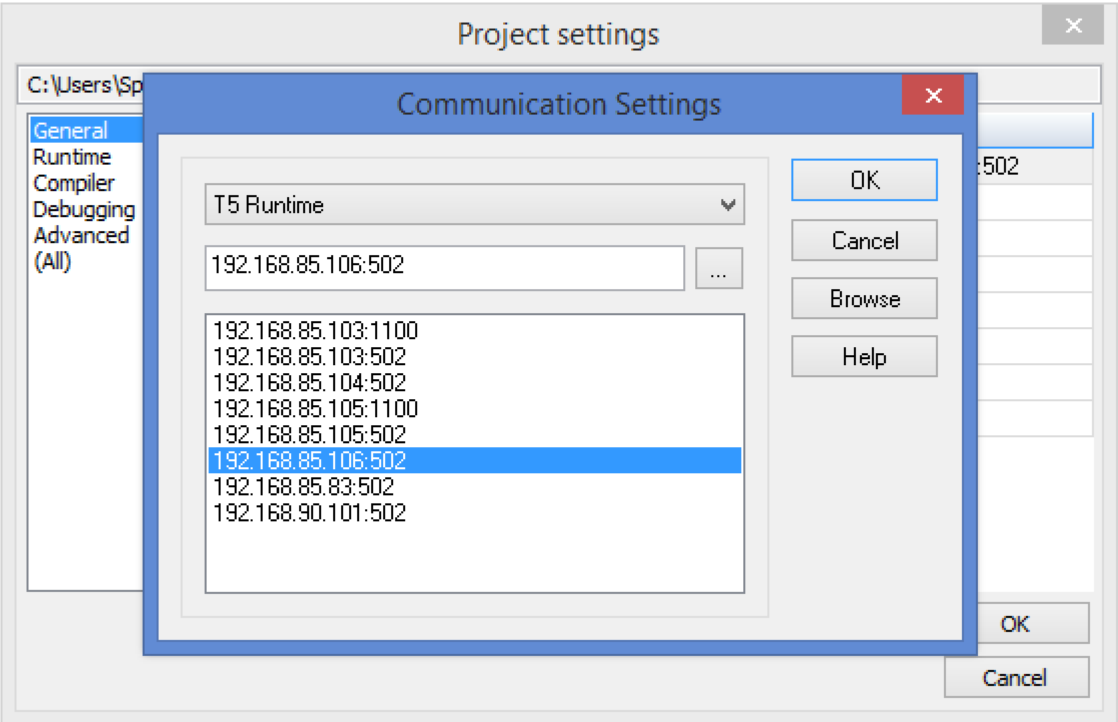
Template: ZPASS2_Template

Now, as you can see in the following figure, in the *Main* program a *ZMODEM_MNG* UDFB instance is already available, which lets you easily control the Z-PASS2-S/S6001-RTU modem.



Name	Type	Dim.	Attrib.	Syb.	Init value
Main					
Inst_ZMODEM_MNG	ZMODEM...			□	
MDM_MNG_ON_OFF	BOOL			□	
MDM_MNG_PPP_ON	BOOL			□	
MDM_MNG_BUSY	BOOL			□	
MDM_MNG_PPP_OK	BOOL			□	
MDM_MNG_PWR_OK	BOOL			□	
MDM_MNG_ERR	BOOL			□	
MDM_MNG_RESULT	INT			□	
MDM_MNG_SIGLEV	INT			□	
MDM_MNG_REG	BOOL			□	
MDM_MNG_OPID	STRING(30)			□	
MDM_MNG_IP	STRING(15)			□	
test	BOOL			□	
Global variables					

Set the correct target IP address (for example 192.168.85.106); normally, the port shall be set to 502:



T5 Runtime

192.168.85.106:502

192.168.85.103:1100
192.168.85.103:502
192.168.85.104:502
192.168.85.105:1100
192.168.85.105:502
192.168.85.106:502
192.168.85.83:502
192.168.90.101:502

Then press the icon:

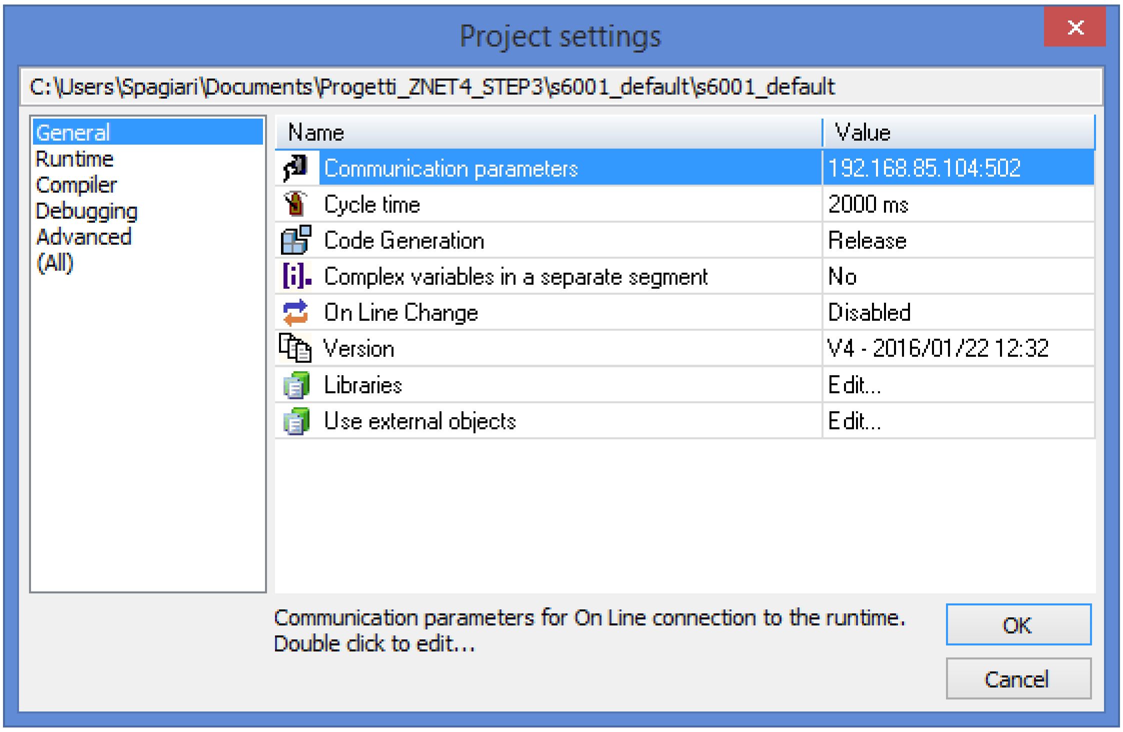
to compile the project.

Download the code by pressing the icon:

The project file will be placed into the */disk* directory of the Device.

If the Straton project is not based on “ZPASS2_Template”/”S6001_Template”, the Seneca UDFB library can still be used, as described in the following.

In the Straton IDE, go to the “Project Settings” window, shown below (menu “Project/Settings”):

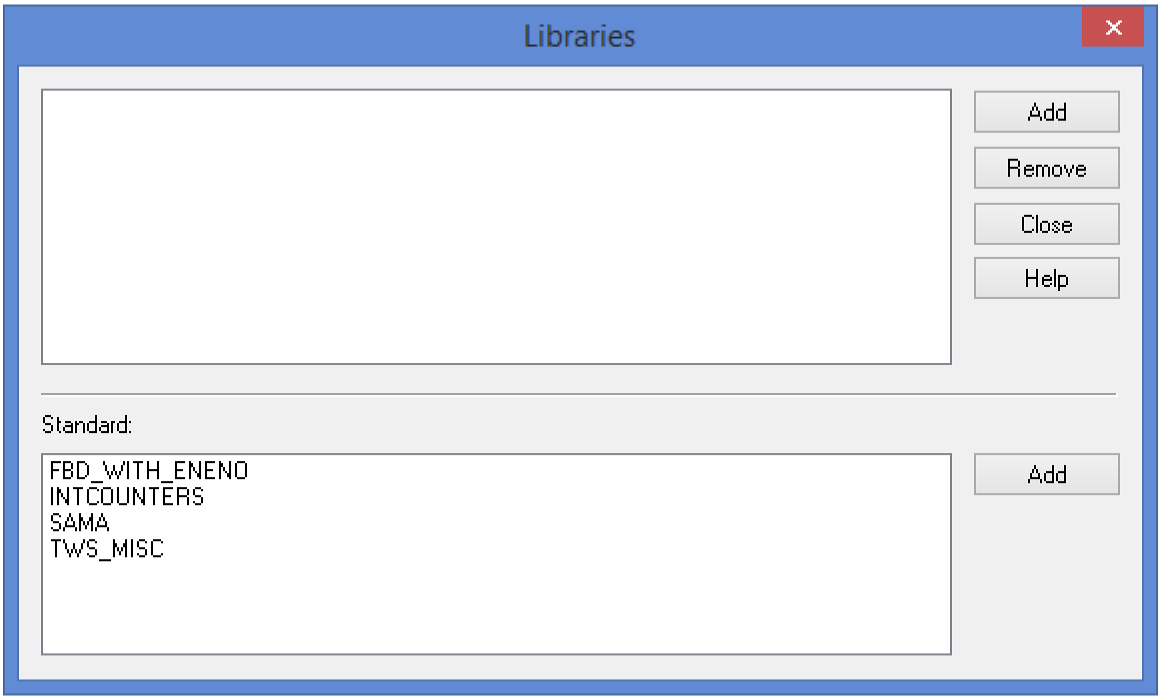


C:\Users\Spagiari\Documents\Progetti_ZNET4_STEP3\s6001_default\s6001_default

Name	Value
Communication parameters	192.168.85.104:502
Cycle time	2000 ms
Code Generation	Release
Complex variables in a separate segment	No
On Line Change	Disabled
Version	V4 - 2016/01/22 12:32
Libraries	Edit...
Use external objects	Edit...

Communication parameters for On Line connection to the runtime.
Double click to edit...

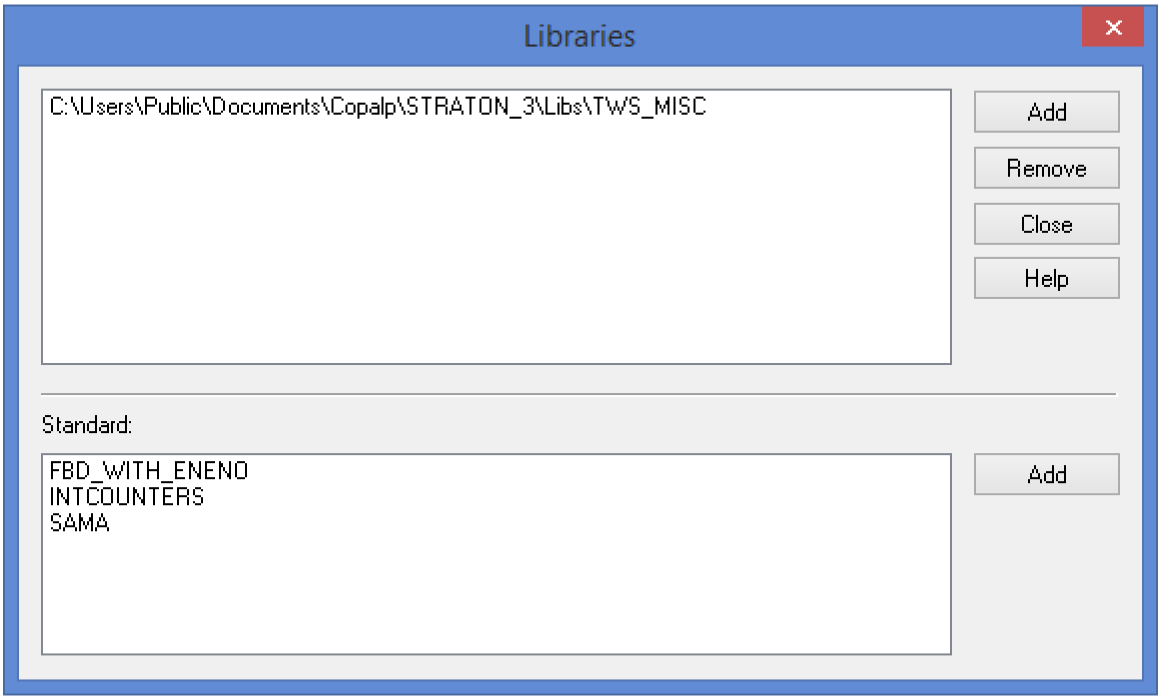
Click on “Libraries / Edit…”; the following window is shown:



Standard:

FBD_WITH_ENENO
INTCOUNTERS
SAMA
TWS_MISC

Select the “TWS_MISC” library and click on “Add”.



Libraries

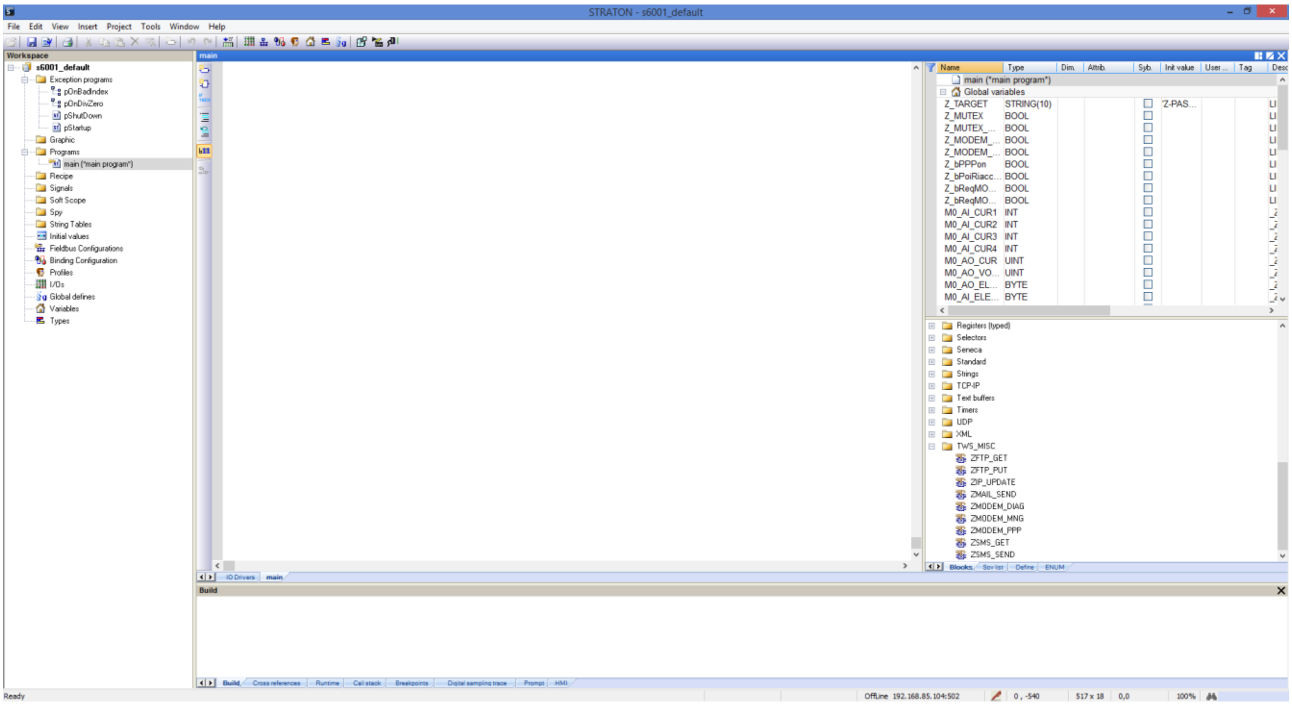
C:\Users\Public\Documents\Copalp\STRATON_3\Libs\TWS_MISC

Standard:

FBD_WITH_ENENO
INTCOUNTERS
SAMA

Finally, click on “Close”.

Now, the UDFB library is available in the project, as shown in the following figure:

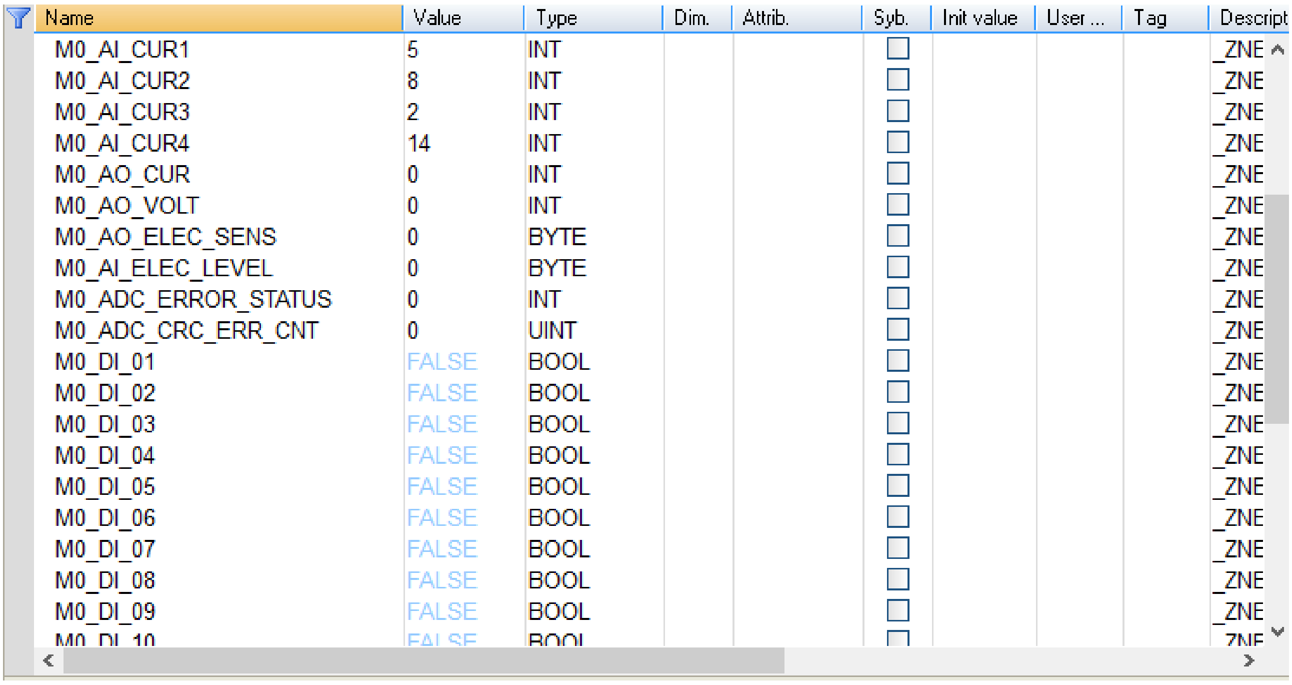


STRATON - s6001_default

Name	Type	Dim.	Attrib.	Syb.	Init value	User ...	Tag	Desc
main (*main program*)								
Global variables								
Z_TARGET	STRING(10)			□	'Z-PAS...			LI
Z_MUTEX	BOOL			□				LI
Z_MUTEX_...	BOOL			□				LI
Z_MODEM_...	BOOL			□				LI
Z_MODEM_...	BOOL			□				LI
Z_bPPPon	BOOL			□				LI
Z_bPoiRiacc...	BOOL			□				LI
Z_bReqMO...	BOOL			□				LI
Z_bReqMO...	BOOL			□				LI
M0_AI_CUR1	INT			□				_Z
M0_AI_CUR2	INT			□				_Z
M0_AI_CUR3	INT			□				_Z
M0_AI_CUR4	INT			□				_Z
M0_AO_CUR	UINT			□				_Z
M0_AO_VO...	UINT			□				_Z
M0_AO_EL...	BYTE			□				_Z
M0_AI_ELE...	BYTE			□				_Z

If the Straton project has been built using the Seneca Z-NET4 SW (see chapter 18), the *TWS_MISC* is already included, so the above procedure is not needed.

In particular, when using S6001-RTU CPU, Z-NET4 SW provides a simple way to create the base Straton project; in fact, all the variables corresponding to the CPU I/Os will be inserted in the project, as shown in the following figure.



Name	Value	Type	Dim.	Attrib.	Syb.	Init value	User ...	Tag	Descript
M0_AI_CUR1	5	INT			□				_ZNE
M0_AI_CUR2	8	INT			□				_ZNE
M0_AI_CUR3	2	INT			□				_ZNE
M0_AI_CUR4	14	INT			□				_ZNE
M0_AO_CUR	0	INT			□				_ZNE
M0_AO_VOLT	0	INT			□				_ZNE
M0_AO_ELEC_SENS	0	BYTE			□				_ZNE
M0_AI_ELEC_LEVEL	0	BYTE			□				_ZNE
M0_ADC_ERROR_STATUS	0	INT			□				_ZNE
M0_ADC_CRC_ERR_CNT	0	UINT			□				_ZNE
M0_DI_01	FALSE	BOOL			□				_ZNE
M0_DI_02	FALSE	BOOL			□				_ZNE
M0_DI_03	FALSE	BOOL			□				_ZNE
M0_DI_04	FALSE	BOOL			□				_ZNE
M0_DI_05	FALSE	BOOL			□				_ZNE
M0_DI_06	FALSE	BOOL			□				_ZNE
M0_DI_07	FALSE	BOOL			□				_ZNE
M0_DI_08	FALSE	BOOL			□				_ZNE
M0_DI_09	FALSE	BOOL			□				_ZNE
M0_DI_10	FALSE	BOOL			□				_ZNE

For more information about Straton IDE and related tools, please refer to StratON tutorials and on-line help.

8.2 Energy Management Protocols

The StratON soft-PLC installed on Z-TWS4/Z-PASS2-S/S6001-RTU supports the following "Energy Management" protocols:

- IEC 60870-5-101 (Master/Slave)
- IEC 60870-5-104 (Master/Slave)
- IEC 61850 (Master/Slave)

The activation of these protocols is license-based.

Please contact Seneca to get more information about getting the license for Energy Management protocols.

8.3 StratON Redundancy

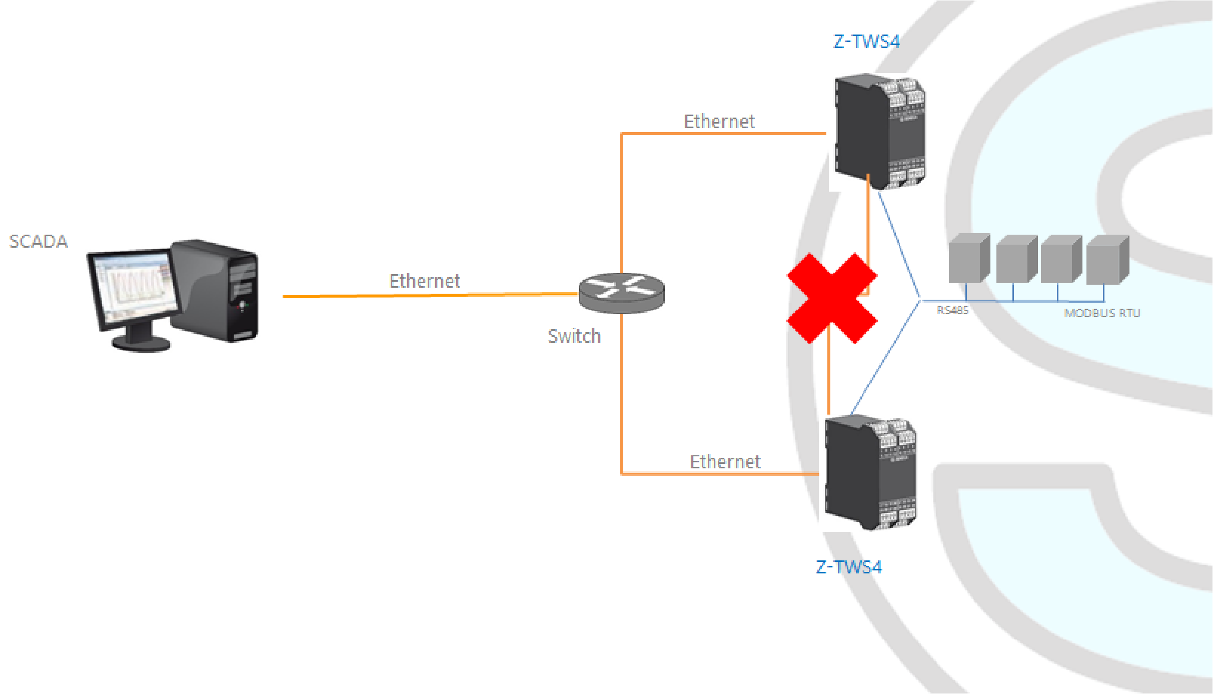
WARNING!

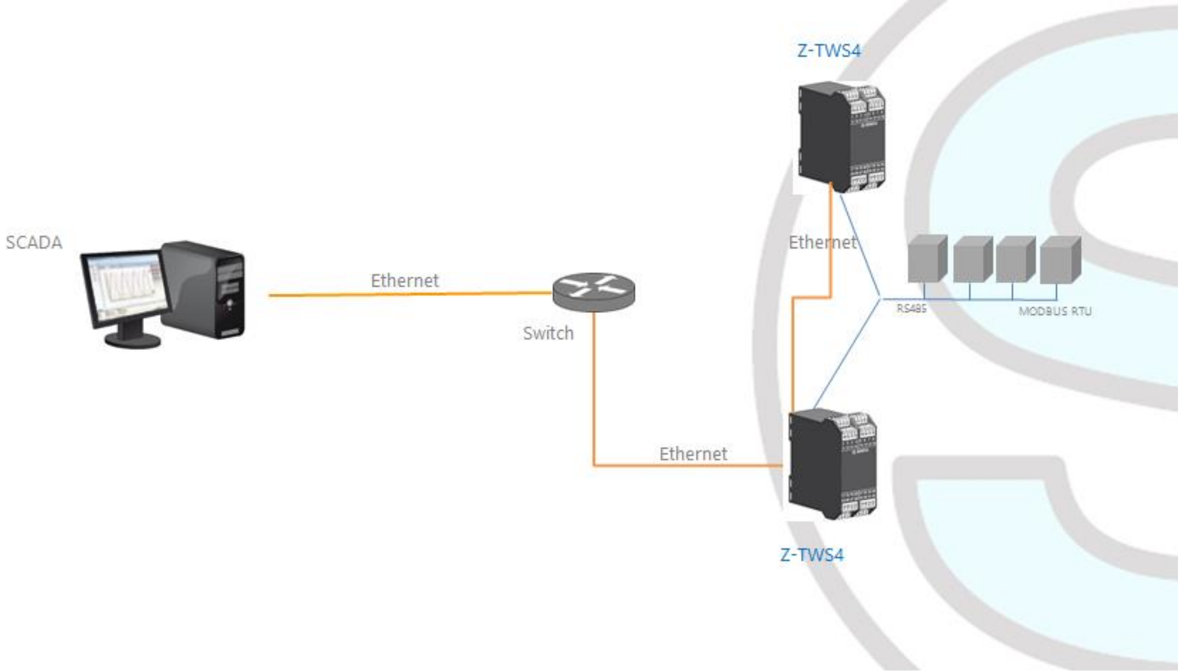
At the date of this manual, the "StratON Redundancy" functionality is still in a "Beta version"; this means that the proper operation of this functionality is not guaranteed for every kind of application; please contact Seneca for further information.

The StratON PLC provides a "Redundancy" functionality:

when this feature is enabled, two CPUs (Z-TWS4 or Z-PASS2-S or S6001-RTU) run the same StratON application; the two CPUs connect each other via the Ethernet, in order to keep variables, state-machines etc. synchronized between them; in each moment, only one of the two CPUs actually runs the application and drives the fieldbus; if, for any reason, that CPU stops running, the application execution is handed over to the second CPU.

When the redundancy is used, some care must be taken when connecting the devices, in order to avoid Ethernet loops; the Ethernet connections shall be set up as shown in the following figures.





Please see paragraph 16.1.2 for a description of the configuration parameters related to StratON Redundancy.

8.4 Updating the StratON application by a USB pen

You can install or update the StratON application, by means of a USB pen, as described in the following.

In the USB pen root directory, create a folder named *t5_update* containing:

- the *APPLI.XTI* file, which can be found in the PC directory containing the StratON project
- optionally, a folder named *Custom* containing some configuration files, needed by the StratON application

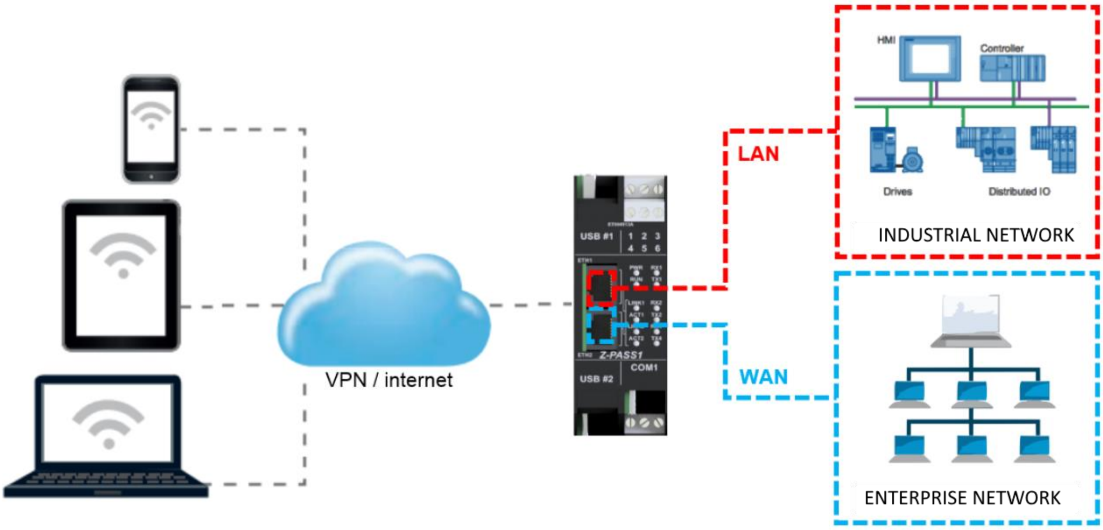
Plug the USB pen into the Device USB#1 port and reboot the device.

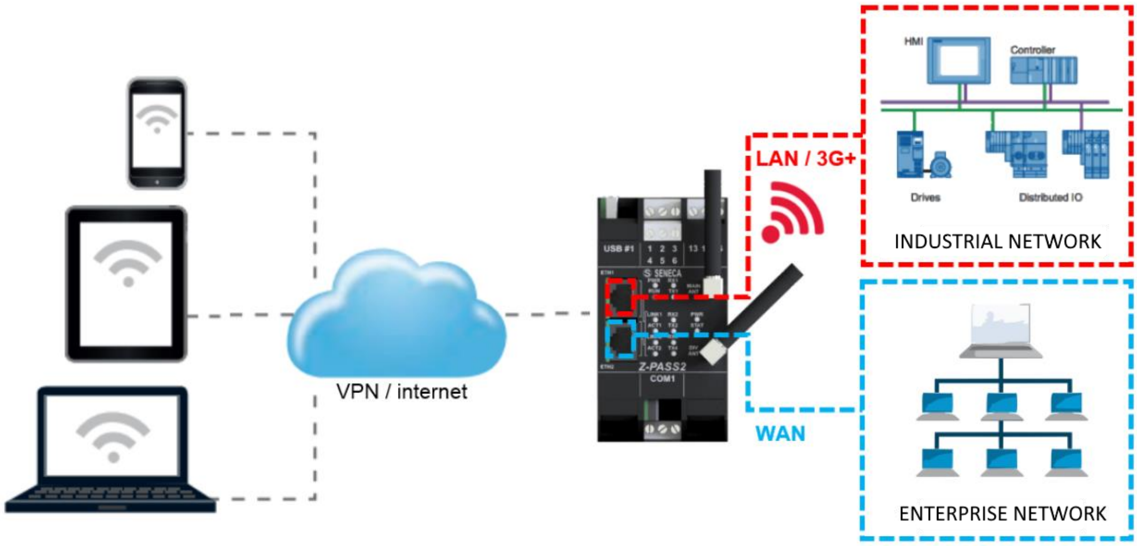
Once the reboot is done, the new application will be run by the StratON PLC.

9 Ethernet Mode (Z-TWS4-R01/Z-PASS2-S-R01/Z-TWS4-R02/Z-PASS2-S-R02)

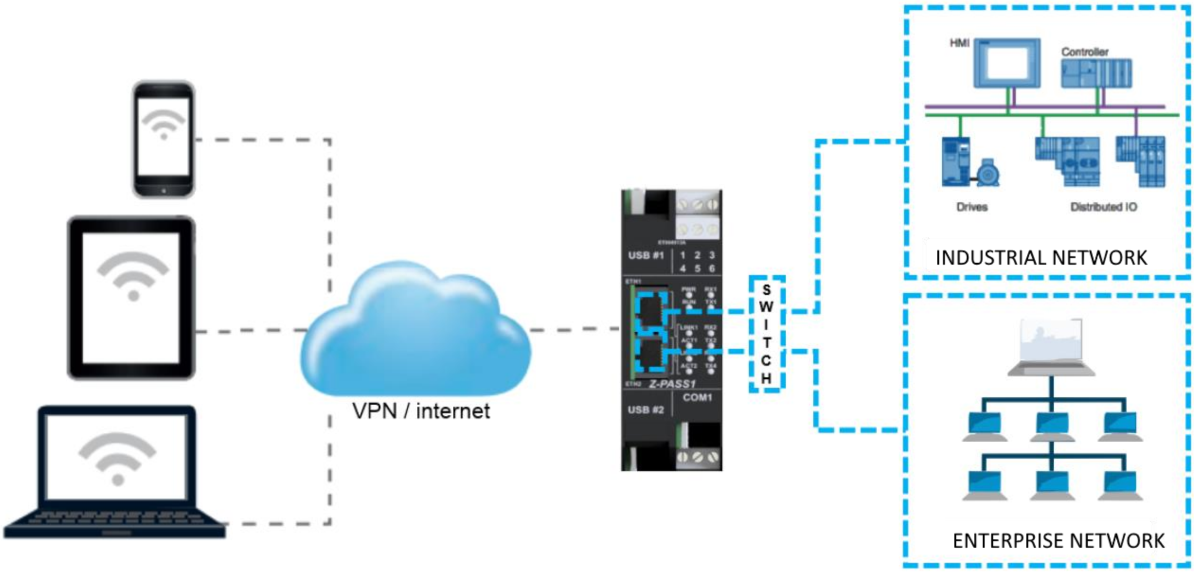
In Z-TWS4-R01/Z-PASS2-S-R01/Z-TWS4-R02/Z-PASS2-S-R02 products, the two available Ethernet ports can be configured as two fully separated network interfaces (“LAN” and “WAN”) or, as in the older versions, they can work as ports of an Ethernet switch; the user can choose between the “LAN/WAN” mode and the “Switch” mode, by means of a new configuration parameter (“Ethernet Mode”) (see paragraph 16.1.2).

The “LAN/WAN” mode is needed when the “industrial” network connected to the LAN interface (comprising e.g. HMI and PLC devices) shall be separated from the “enterprise” network connected to the WAN interface (comprising enterprise PCs and servers); when the Device is remotely accessed through the WAN interface, only devices connected to the LAN interface can be reached, while access to machines lying in the enterprise network is forbidden; this is depicted in the following two figures.

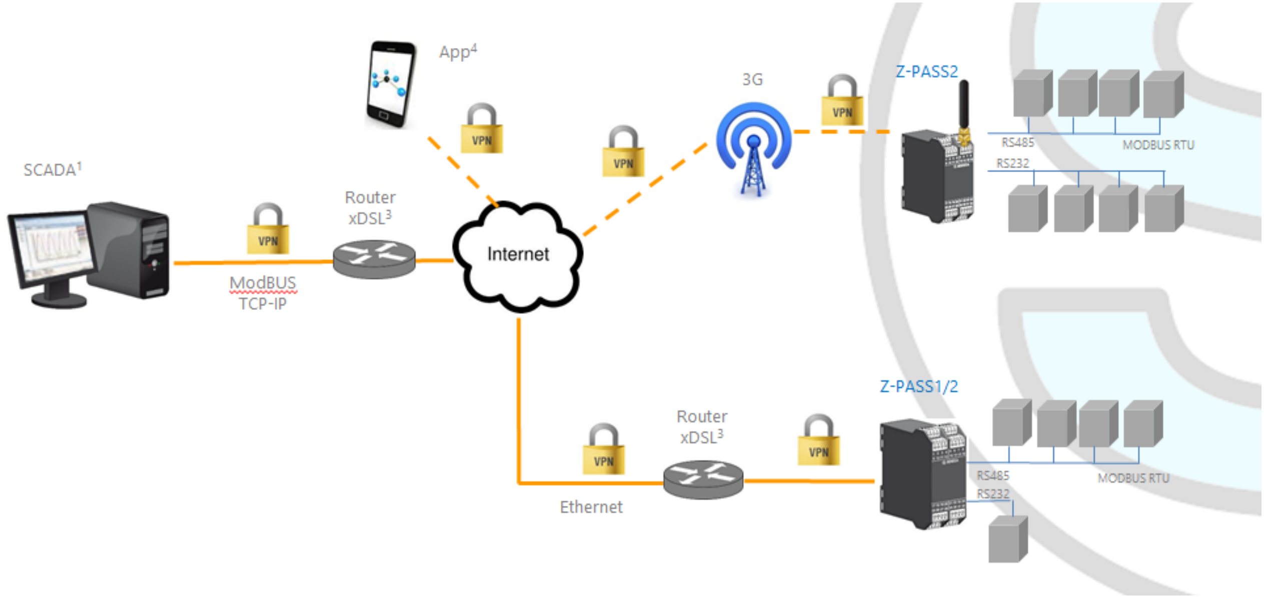




When this separation is not needed or when the Internet access is achieved only through the mobile (3G+) interface, the “Switch” mode still lets the Device be used as an Ethernet switch, as shown in the following figure.



10 VPN



Z-TWS4/Z-PASS2-S/S6001-RTU support the standard OpenVPN protocol.

The main advantages that come from using a VPN are:

- secure connections, since transported data are encrypted;
- the ability to establish connections without interfering with the corporate LAN;
- no need to have a static/public IP address on the WAN side;
- remote configurability by a built-in Web Server.

Two “VPN modes“ are available, named “OpenVPN” and “VPN Box”, respectively.

The “OpenVPN” mode can be used when the Device shall be installed in an already existing VPN. In this case, an OpenVPN server shall be available and the certificate and key files for the Device client shall be provided by the VPN administrator; the files can be uploaded to the Device using the “VPN configuration” page of Device Web Server.

If the VPN infrastructure does not exist yet, the advisable choice is to adopt the “VPN Box” solution, developed by Seneca. The “VPN Box” is an hardware appliance (or a virtual machine) which lets the user easily setup two alternative kinds of VPN:

- “Single LAN” VPN
- “Point-to-Point” VPN

In the “Single LAN” VPN, all devices and PCs (and associated local subnets) configured into VPN are always connected in the same network. In this scenario any PC Client can connect to any Device and to other machines which lie in the Device LAN, but also any device/machine can connect to any other remote device/machine which belongs to the same VPN network. This VPN architecture puts some constraints on the device sub-networks definition, in fact all VPN clients must have a different IP address and different local LAN, to avoid conflicts. The software named “VPN BOX Manager” configures VPN BOX and will help you to avoid errors defining local subnets.

In the “Point-to-Point” VPN, a client PC, in a given moment, can perform a single connection, on demand, to only one Device (and to machines which lie in the Device LAN) at time. Furthermore, devices can’t communicate each other also if they belong to the same VPN. The advantage of this architecture is that the same sub-network can be used in all sites. Point to point mode makes it possible to define user groups and manage them. This VPN modality must be configured on “VPN Box” by VPN BOX Manager.

In details, the “VPN Box” is supplied with two Windows applications:

- the “VPN Box Manager”, which allows to configure the VPN[6] mode on the VPN Box and manage the devices[7]
- the “VPN Client Communicator”, which lets the user connect the PC to the network (in the “Single LAN” case) or to a specific device (in the “Point-to-Point” case)

A detailed description of “VPN Box” can be found in the “VPN Box User Manual”.

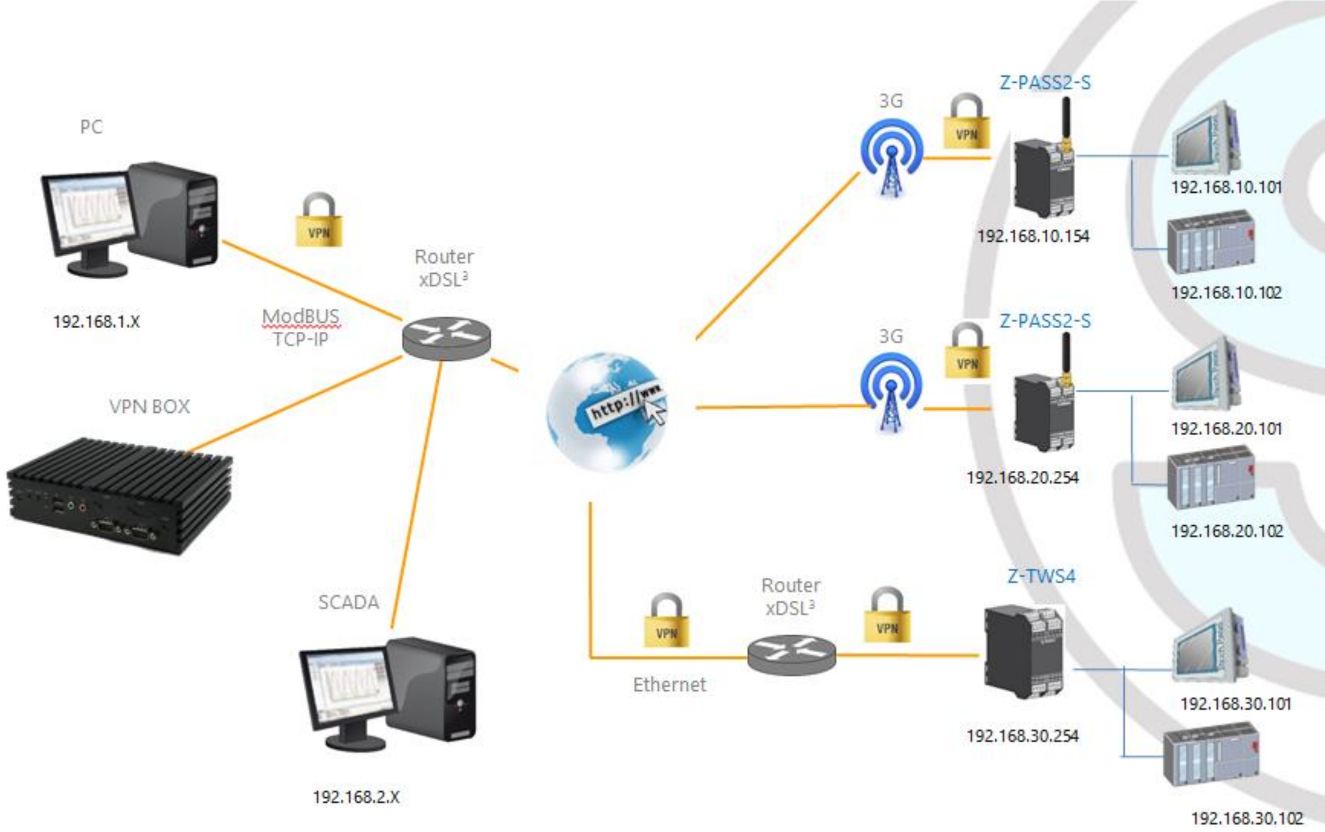
A detailed description of Z-TWS4/Z-PASS2-S/S6001-RTU VPN configuration parameters is given in 16.1.4 paragraph.

The following two sub-paragraphs give some more info about the two kinds of VPN.

[6] Only one of the two kinds of VPN can be configured on a given VPN Box.

[7] “VPN Box” functionality is available also on Seneca Z-PASS1 and Z-PASS2 products.

10.1 “Single LAN” VPN



The above figure gives an example of a “Single LAN” VPN.

The client PC (with IP address 192.168.1.X) can connect, just as an example, to the first Z-PASS2-S by using its 192.168.10.154 IP address and to the PLC in the Z-PASS2-S LAN by using its local IP address 192.168.10.102.

Also, two devices which lie in two different LANs of the same VPN network (e.g.: 192.168.10.101 and 192.168.20.102) can connect to each other, again using their local IP addresses.

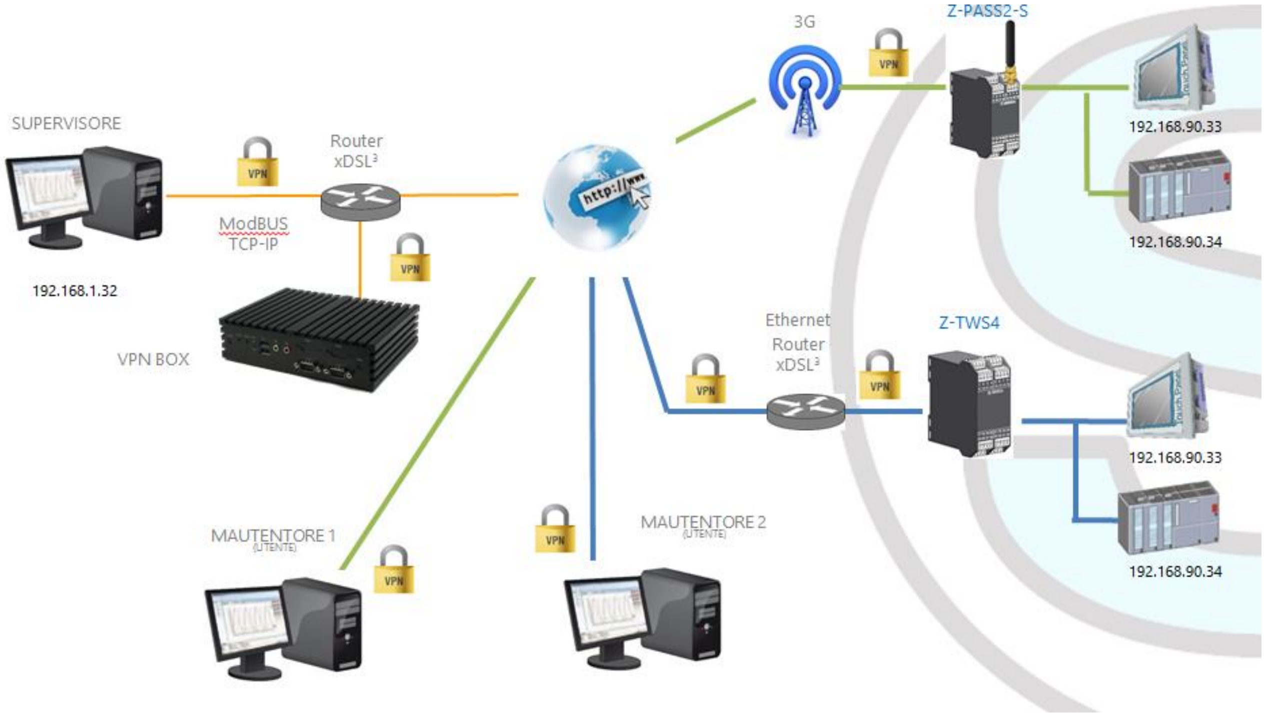
To let this scenario work correctly, an essential rule must always be followed: the Device LANs and the PC LAN shall have different and not colliding subnets; so, in the above figure, the following subnets allocation has been depicted:

PC LAN	192.168.1.0/24
SCADA LAN	192.168.2.0/24
Z-PASS2 LAN	192.168.10.0/24
Z-PASS2 LAN	192.168.20.0/24
Z-PASS1 LAN	192.168.30.0/24

The “VPN Box Manager” application guides you in the configuration task, checking that no subnet/IP address conflict is present in the network.

If subnet/conflicts cannot be avoided, using a “Single LAN” VPN is still possible if local IP addresses are not used; devices can be reached by means of their VPN IP addresses and machines beyond them can be reached by configuring some “port forwarding” rules on the Device Router (see 16.1.5 paragraph).

10.2 “Point-to-Point” VPN



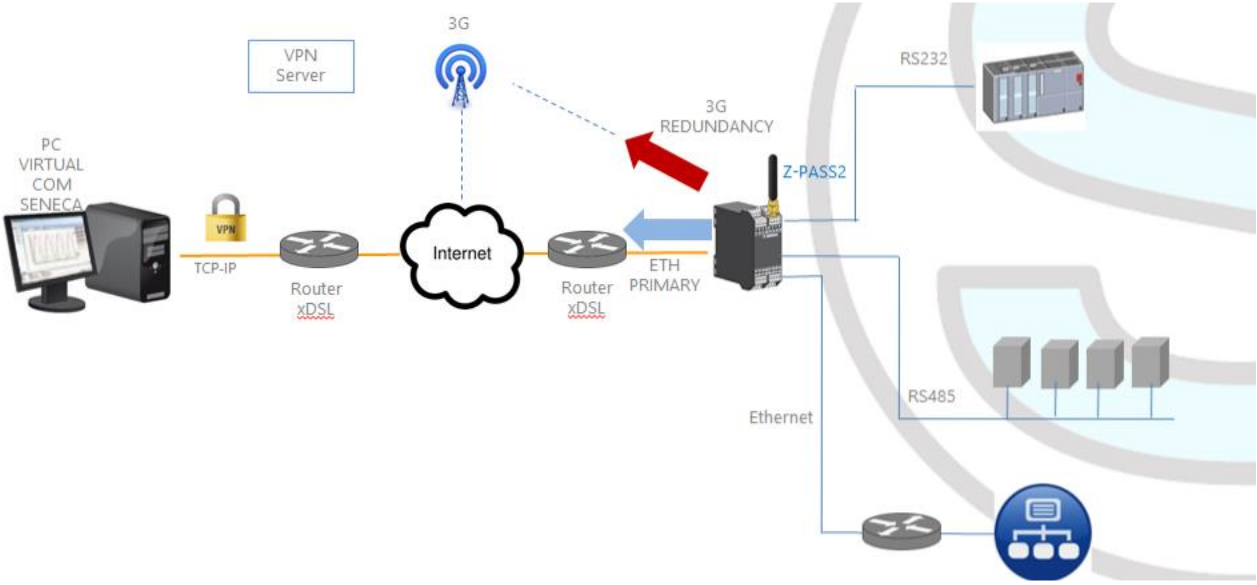
The above figure gives an example of a “Point-to-Point” VPN.

In this scenario a PC (acting as a VPN Client) can connect, on demand, to only one Device and its subnet, using local IP addresses. Since the client “sees” just one Z-TWS4/Z-PASS2-S/S6001-RTU (and attached devices) at time, the same subnet configuration can be assigned to different sites, without creating conflicts.

For this kind of VPN, the “VPN Box Manager” application lets define group of users that can connect only to assigned devices.

The “VPN Client Communicator” application retrieves the list of devices which are available for the logged user; then the user can select one device on the list and connect to it.

11 Network Redundancy

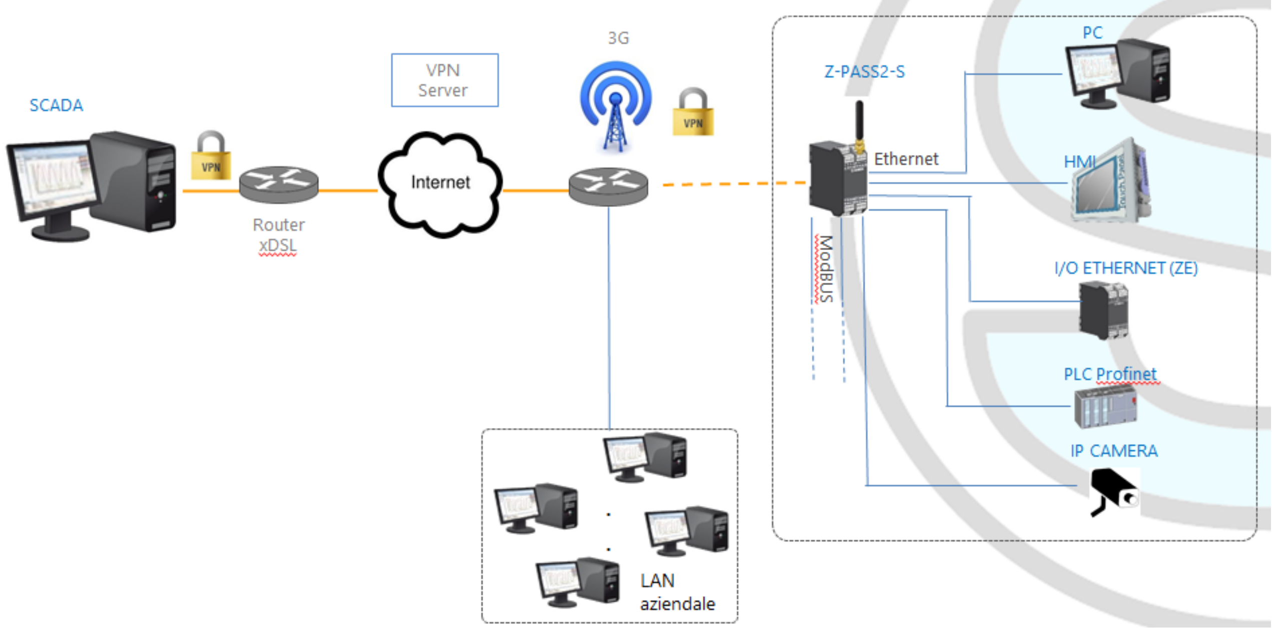


“Network Redundancy” is a functionality than can be enabled on the Device when a 3G modem is available (always true for Z-PASS2-S and S6001-RTU, true for Z-TWS4 when connected to Seneca Z-MODEM-3G modem).

This functionality switches the network interface used to access the Internet from the Ethernet (“primary” interface) to the Mobile/3G (“secondary” interface), when Internet access through the primary interface becomes unavailable; when access through the primary interface become available again, the network interface is switched back to Ethernet.

The parameters provided to configure Network Redundancy are explained in paragraph 16.1.2 “Network and Services”.

12 Router



As already told before, “Router” functionality routes packets between the WAN (Mobile Network) interface and the LAN (Ethernet) interface and vice versa; so, this functionality especially makes sense when a 3G connection is active, which needs the availability of a 3G modem (always true for Z-PASS2-S and S6001-RTU, true for Z-TWS4 when connected to Seneca Z-MODEM-3G modem).

More specifically, an important feature of the Router is what is known as “IP forwarding”; this means that when the Device receives a packet not targeted for it, it does not discard the packet but forwards it to its actual destination; when a packet is routed from the LAN to the WAN, the Device also performs what is known as “IP masquerading”, meaning that the original source IP address is replaced with the IP address of the WAN (Mobile Network) interface.

Another important feature is the availability of a DNS server/forwarder, which can resolve names either by itself or querying the external configured DNS server.

Also, a DHCP server is available which assigns IP addresses to clients connected on the Device LAN; here, you can configure the range of addresses used by the server and the lease time.

There is also the possibility to define up to five “Port Forwarding” rules or “Virtual Servers”; using these rules, you can, for example, redirect packets received on a TCP or UDP port to another Device port or to another machine, with a different IP address, on the same or another port.

As an alternative to using “Port Forwarding” rules, Router + VPN functionalities allow the use of local addresses, as shown in the previous chapter; in the router configuration, a flag is given to enable this feature.

A detailed description of the Router configuration can be found in paragraph 16.1.5.

13 Remote Access Disable

Z-TWS4-R02 and Z-PASS2-S-R02 products provide a dedicated digital input and a dedicated digital output to control and monitor remote access to the device.

In details:

- when "Remote Access Disable" digital input is set to HIGH state, remote access to the device is disabled; conversely, when "Remote Access Disable" digital input is set to LOW state, remote access to the device is enabled; "Remote Access Disable" digital input state is reported by the "REM.DIS." LED;
- "Remote Access Active" digital output is set to HIGH state when the device is remotely accessed (VPN connection is active); it is set to LOW state when VPN connection is not active.

Four levels of security can be configured to disable remote access, providing increasing security levels:

- Level 0 ("None"): no remote access service is disabled;
- Level 1 ("VPN Connection"): VPN connections are disabled in any VPN mode (VPN Box Point-to-Point, VPN Box Single LAN, OpenVPN), but VPN Box Service is still running, so the device can still be monitored on VPN Box Manager;
- Level 2 ("VPN Service"): VPN Box Service is disabled, but the device can still access the Internet and receive SMSs (on Z-PASS2-S-R02);
- Level 3 ("Internet Connection"): any Internet access is disabled and, on Z-PASS2-S-R02, modem is off, so SMSs can't be received.

See "Digital I/O Configuration" paragraph to learn how to set the desired security level.

14 Auto-APN

The Auto-APN feature lets the Device establish mobile data connections without requiring the user to configure APN data[8] for the SIM in use.

This is accomplished by using the SIM IMSI and, possibly, some other data available on the SIM, to select the proper APN record in an internal DB[9], containing APN records for all mobile operators in the world.

In some particular cases, however, when a "custom APN" shall be used, the Auto-APN feature can be disabled, setting the "APN Mode" parameter to "Manual", in the "Mobile Network" page (see paragraph 16.1.9).

15 Upgrading the firmware by a USB pen

The Device firmware can be upgraded by means of a USB pen; a pen drive formatted with FAT32 file-system is needed.

[8] APN data are: APN, Username, Password and Authentication Type.

[9] This DB is updated to the one used in the last Android O.S. version.

The procedure is the following:

1) download the FW file from one of the following links:

   http://www.seneca.it/products/z-tws4
   http://www.seneca.it/products/z-pass2-s
   http://www.seneca.it/products/s6001-rtu

   the downloaded file is a .zip file; extract the FW file from it;
   the FW file shall have a name like the following:

   SW002940_xxx.bin

2) copy the file into the root of the USB pen
3) switch off the Device
4) insert the USB pen into the USB#1 port
5) switch on the Device; the upgrade procedure will take some minutes to be completed; during this time, the Device MUST NOT be switched off; during the procedure, the Device will be rebooted several times
6) the upgrade procedure is ended when the LED "RUN" is blinking
7) remove the USB pen

16 Web Configuration Pages

NOTE: in this chapter, the web pages screen-shots are shown for only one of the products (Z-TWS4, Z-TWS4-R01, Z-TWS4-R02, Z-PASS2-S, Z-PASS2-S-R01, Z-PASS2-S-R02, S6001-RTU); the pages for the other products are identical, except for the product name shown in the top of the pages and for some details explained in the following paragraphs.

Furthermore, for S6001-RTU one more page ("I/O View") is available.

16.1 Administrator pages

The Device can be fully configured by means of a set of web configuration pages.

To access the Device configuration site, you have to connect the browser to the Device IP address on port 8080, e.g.:

http://192.168.90.101:8080[10]

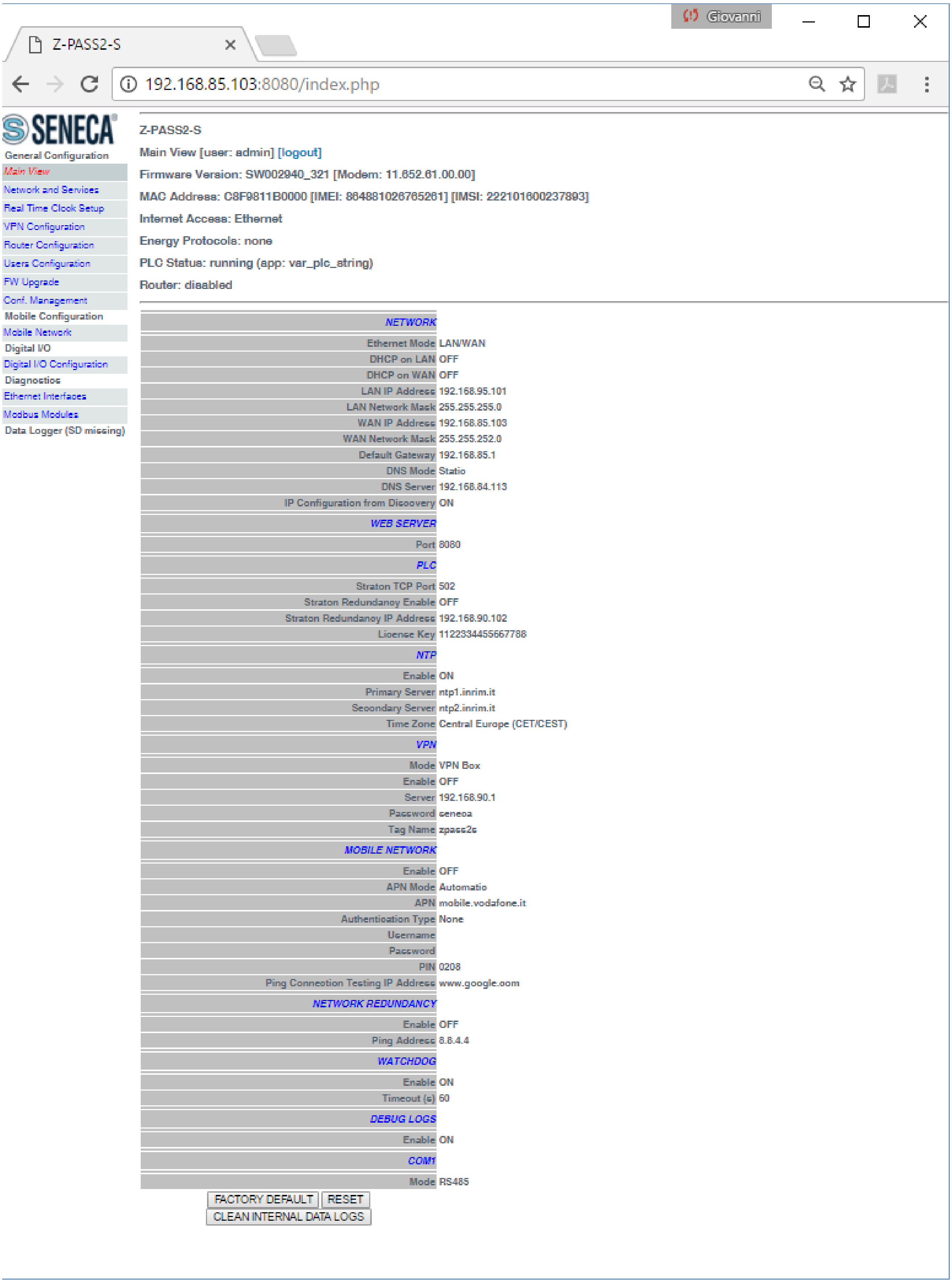
and, when asked, provide the following credentials (default values):

Username: admin
Password: admin

You come to the "Main View" page, described in the following paragraph.

16.1.1 Main View

[10] The default 80 HTTP port has been left available for customer pages.



General Configuration
Main View
Network and Services
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Mobile Configuration
Mobile Network
Digital I/O
Digital I/O Configuration
Diagnostics
Ethernet Interfaces
Modbus Modules
Data Logger (SD missing)

Z-PASS2-S

Main View [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

NETWORK	
Ethernet Mode	LAN/WAN
DHCP on LAN	OFF
DHCP on WAN	OFF
LAN IP Address	192.168.95.101
LAN Network Mask	255.255.255.0
WAN IP Address	192.168.85.103
WAN Network Mask	255.255.252.0
Default Gateway	192.168.85.1
DNS Mode	Static
DNS Server	192.168.84.113
IP Configuration from Discovery	ON
WEB SERVER	
Port	8080
PLC	
Straton TCP Port	502
Straton Redundancy Enable	OFF
Straton Redundancy IP Address	192.168.90.102
License Key	1122334455667788
NTP	
Enable	ON
Primary Server	ntp1.inrim.it
Secondary Server	ntp2.inrim.it
Time Zone	Central Europe (CET/CEST)
VPN	
Mode	VPN Box
Enable	OFF
Server	192.168.90.1
Password	seneca
Tag Name	zpass2s
MOBILE NETWORK	
Enable	OFF
APN Mode	Automatic
APN	mobile.vodafone.it
Authentication Type	None
Username	
Password	
PIN	0208
Ping Connection Testing IP Address	www.google.com
NETWORK REDUNDANCY	
Enable	OFF
Ping Address	8.8.4.4
WATCHDOG	
Enable	ON
Timeout (s)	60
DEBUG LOGS	
Enable	ON
COM1	
Mode	RS485

FACTORY DEFAULT | RESET
CLEAN INTERNAL DATA LOGS

In this page, main Device configuration parameters are shown, with their current values.

On the left side of the page, like in all the other pages, a menu is shown which lets you access all the configuration pages; the menu is divided in several sections:

- General Configuration
- Mobile Configuration
- Digital I/O Configuration (on Z-TWS4-R02, Z-PASS2-S-R02 products)
- Diagnostics
- Data Logger

In S6001-RTU, a "S6001-RTU" section is also present.

On top of the page, like in all the other pages, the following information are shown:

- the page name
- the FW version, along with the modem FW revision, for Z-PASS2-S/S6001-RTU[11]; for S6001-RTU, the FW version of the I/O board is also shown
- the MAC address; the modem IMEI, for Z-PASS2-S/S6001-RTU; the SIM IMSI, for Z-PASS2-S/S6001-RTU, when a SIM is present
- the network interface used for Internet Access (i.e.: "Ethernet" or "Mobile")
- which energy protocols are enabled (on a license base)
- the Soft PLC status (i.e.: "running" or "stopped"); if the PLC application execution is stopped or no application is loaded on the Device, the status "app not running" is also shown; if the PLC application is running, the name of the application is also shown
- the Router status (i.e.: "running" or "disabled")

The currently logged user (e.g.: "admin") and the "Logout" link are also present, near the page name.

In this page, the following buttons are available:

- "RESET", to perform the Device reboot
- "FACTORY DEFAULT", to reset the Device to its factory state
- "CLEAN INTERNAL DATA LOGS", to delete internal data log files (this does not affect the data log files stored on the SD card, see paragraph 16.1.14)

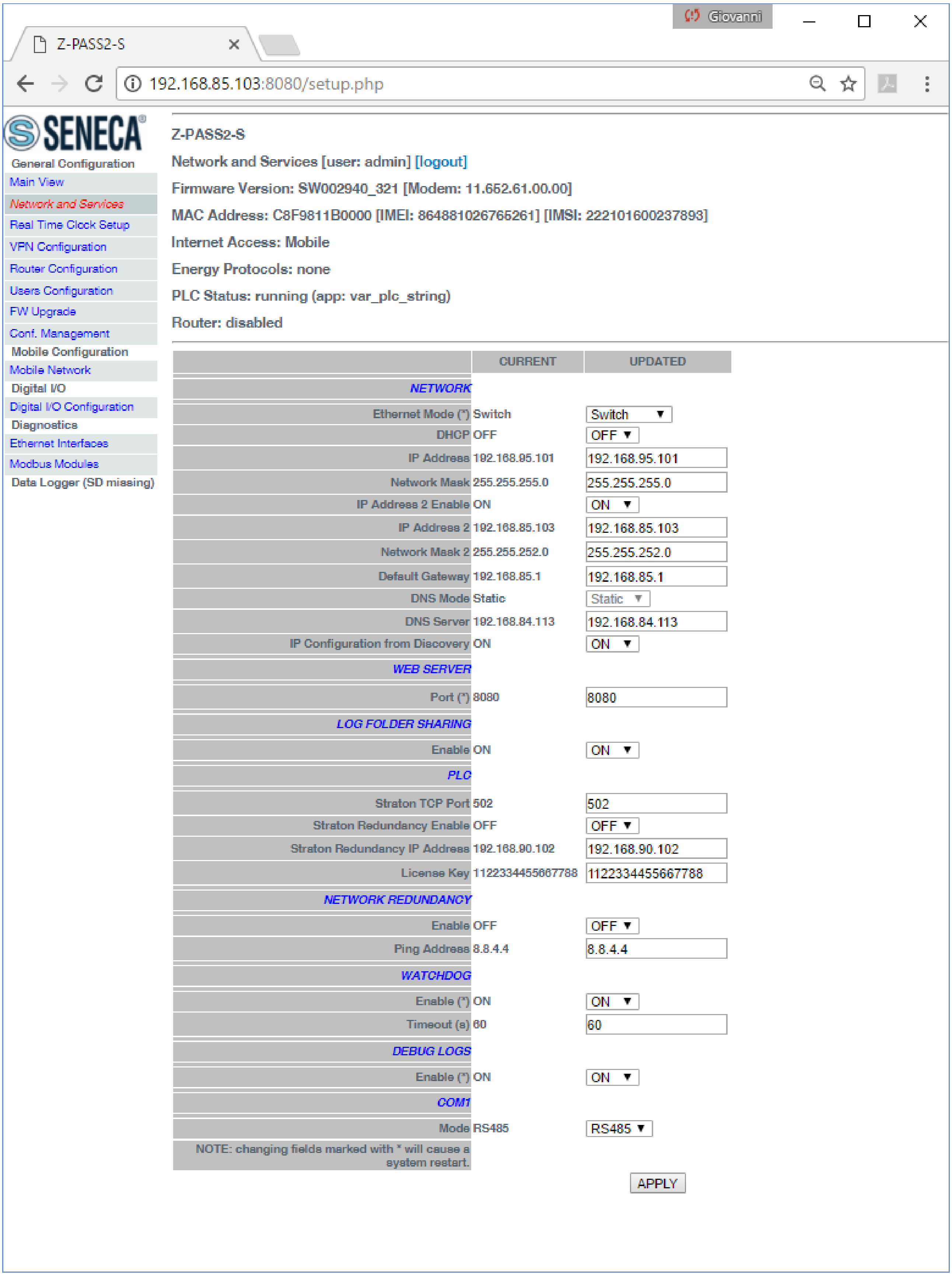
Probably, the first parameters you need to change when setting up a new Device are those related to its network configuration.

You can accomplish this in the "Network and Services" page, described in the following paragraph.

16.1.2 Network and Services

The parameters shown in this page slightly change, depending on the HW version of the product (Z-TWS4/Z-PASS2-S or Z-TWS4-R01/Z-PASS2-S-R01 or Z-TWS4-R02/Z-PASS2-S-R02) and, for new HW versions, on the selected "Ethernet Mode"; this is shown in the following figures.

[11] Also for Z-TWS4, when an external Z-MODEM-3G modem is connected.



Z-PASS2-S

Network and Services [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Mobile

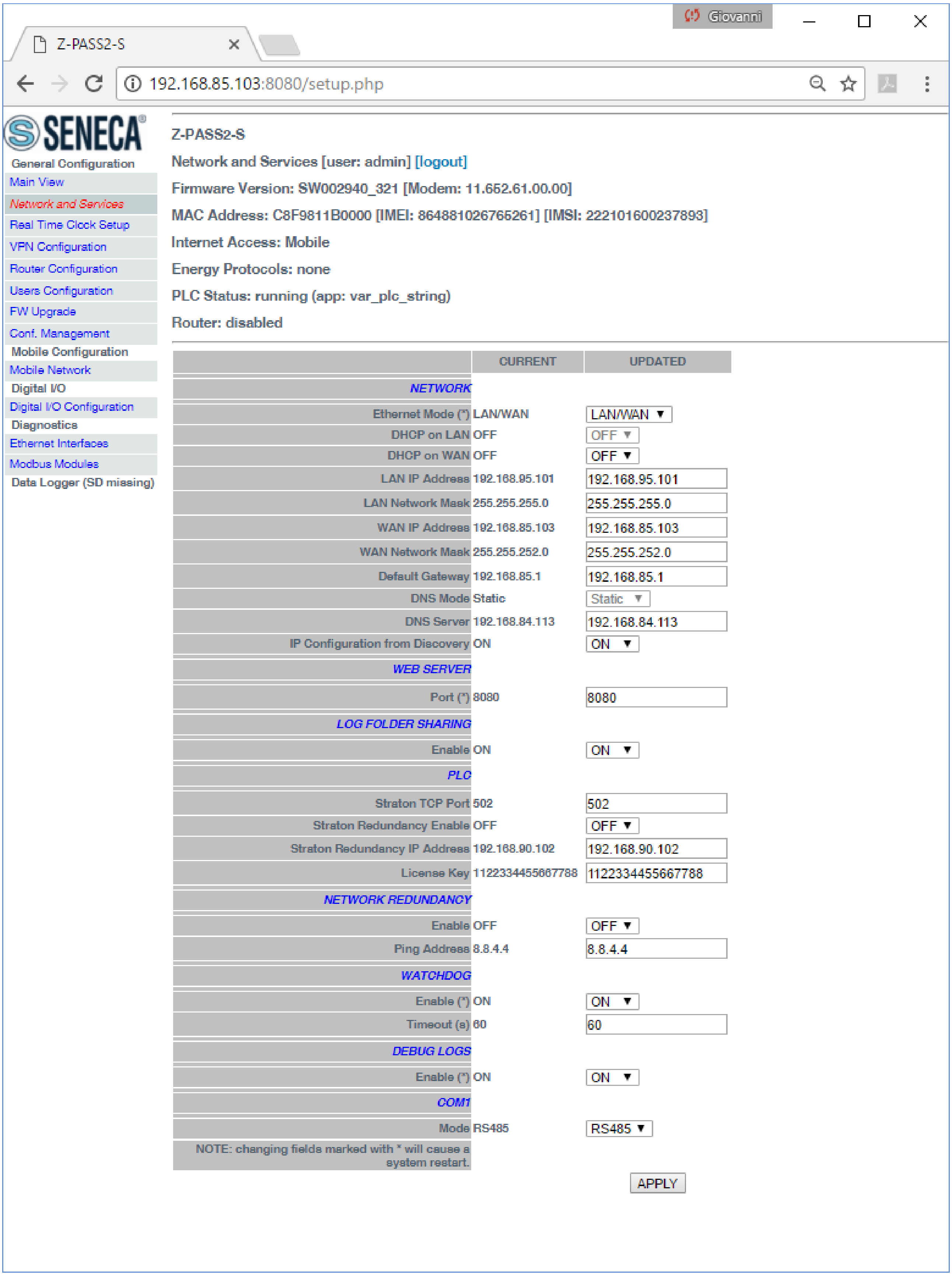
Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

	CURRENT	UPDATED
NETWORK		
Ethernet Mode (*)	Switch	Switch ▼
DHCP	OFF	OFF ▼
IP Address	192.168.95.101	192.168.95.101
Network Mask	255.255.255.0	255.255.255.0
IP Address 2 Enable	ON	ON ▼
IP Address 2	192.168.85.103	192.168.85.103
Network Mask 2	255.255.252.0	255.255.252.0
Default Gateway	192.168.85.1	192.168.85.1
DNS Mode	Static	Static ▼
DNS Server	192.168.84.113	192.168.84.113
IP Configuration from Discovery	ON	ON ▼
WEB SERVER		
Port (*)	8080	8080
LOG FOLDER SHARING		
Enable	ON	ON ▼
PLC		
Straton TCP Port	502	502
Straton Redundancy Enable	OFF	OFF ▼
Straton Redundancy IP Address	192.168.90.102	192.168.90.102
License Key	1122334455667788	1122334455667788
NETWORK REDUNDANCY		
Enable	OFF	OFF ▼
Ping Address	8.8.4.4	8.8.4.4
WATCHDOG		
Enable (*)	ON	ON ▼
Timeout (s)	60	60
DEBUG LOGS		
Enable (*)	ON	ON ▼
COM1		
Mode	RS485	RS485 ▼
NOTE: changing fields marked with * will cause a system restart.		

The previous figure shows the “Network and Services” page for a Z-PASS2-S-R02, when the “Ethernet Mode” parameter is set to “Switch”; it also applies to a Z-TWS4-R02 in “Switch” mode.



Z-PASS2-S

Network and Services [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Mobile

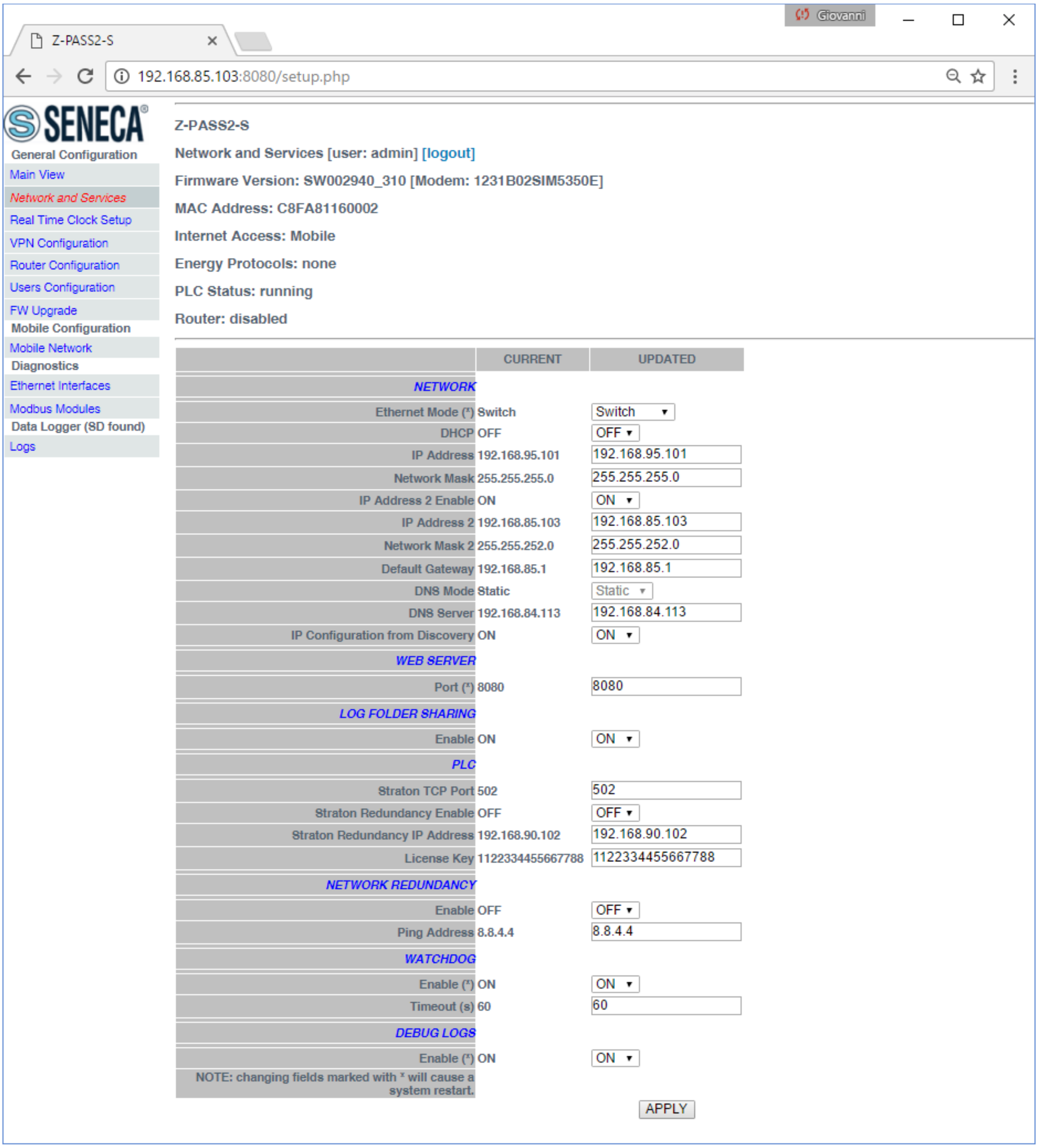
Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

	CURRENT	UPDATED
NETWORK		
Ethernet Mode (*)	LAN/WAN	LAN/WAN ▼
DHCP on LAN	OFF	OFF ▼
DHCP on WAN	OFF	OFF ▼
LAN IP Address	192.168.95.101	192.168.95.101
LAN Network Mask	255.255.255.0	255.255.255.0
WAN IP Address	192.168.85.103	192.168.85.103
WAN Network Mask	255.255.252.0	255.255.252.0
Default Gateway	192.168.85.1	192.168.85.1
DNS Mode	Static	Static ▼
DNS Server	192.168.84.113	192.168.84.113
IP Configuration from Discovery	ON	ON ▼
WEB SERVER		
Port (*)	8080	8080
LOG FOLDER SHARING		
Enable	ON	ON ▼
PLC		
Straton TCP Port	502	502
Straton Redundancy Enable	OFF	OFF ▼
Straton Redundancy IP Address	192.168.90.102	192.168.90.102
License Key	1122334455667788	1122334455667788
NETWORK REDUNDANCY		
Enable	OFF	OFF ▼
Ping Address	8.8.4.4	8.8.4.4
WATCHDOG		
Enable (*)	ON	ON ▼
Timeout (s)	60	60
DEBUG LOGS		
Enable (*)	ON	ON ▼
COM1		
Mode	RS485	RS485 ▼
NOTE: changing fields marked with * will cause a system restart.		

The previous figure shows the “Network and Services” page for a Z-PASS2-S-R02, when the “Ethernet Mode” parameter is set to “LAN/WAN”; it also applies to a Z-TWS4-R02 in “LAN/WAN” mode.



Z-PASS2-S

Network and Services [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

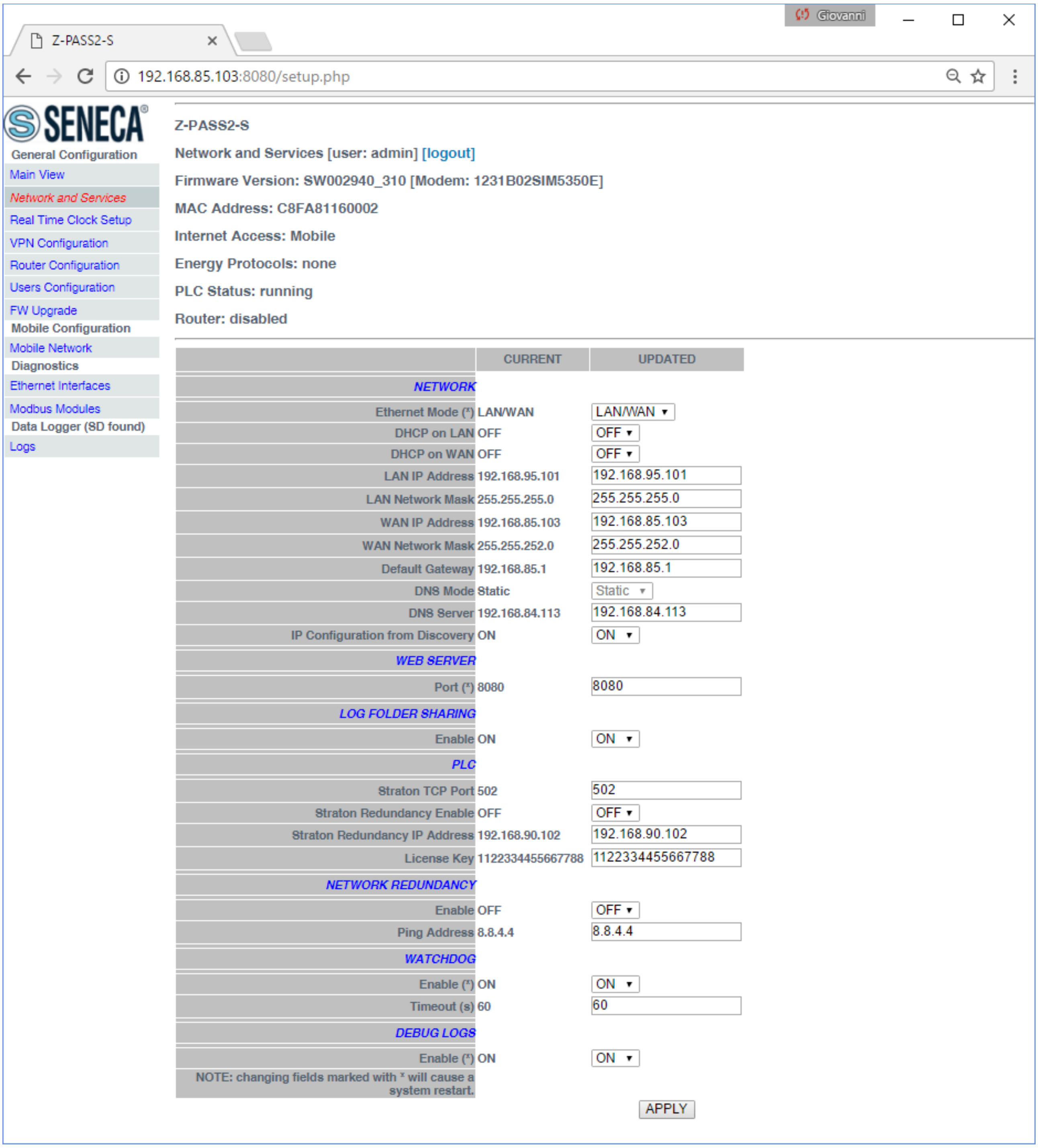
PLC Status: running

Router: disabled

	CURRENT	UPDATED
NETWORK		
Ethernet Mode (*)	Switch	Switch ▾
DHCP	OFF	OFF ▾
IP Address	192.168.95.101	192.168.95.101
Network Mask	255.255.255.0	255.255.255.0
IP Address 2 Enable	ON	ON ▾
IP Address 2	192.168.85.103	192.168.85.103
Network Mask 2	255.255.252.0	255.255.252.0
Default Gateway	192.168.85.1	192.168.85.1
DNS Mode	Static	Static ▾
DNS Server	192.168.84.113	192.168.84.113
IP Configuration from Discovery	ON	ON ▾
WEB SERVER		
Port (*)	8080	8080
LOG FOLDER SHARING		
Enable	ON	ON ▾
PLC		
Straton TCP Port	502	502
Straton Redundancy Enable	OFF	OFF ▾
Straton Redundancy IP Address	192.168.90.102	192.168.90.102
License Key	1122334455667788	1122334455667788
NETWORK REDUNDANCY		
Enable	OFF	OFF ▾
Ping Address	8.8.4.4	8.8.4.4
WATCHDOG		
Enable (*)	ON	ON ▾
Timeout (s)	60	60
DEBUG LOGS		
Enable (*)	ON	ON ▾
NOTE: changing fields marked with * will cause a system restart.		

APPLY

The previous figure shows the “Network and Services” page for a Z-PASS2-S-R01, when the “Ethernet Mode” parameter is set to “Switch”; it also applies to a Z-TWS4-R01 in “Switch” mode.



Z-PASS2-S

Network and Services [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

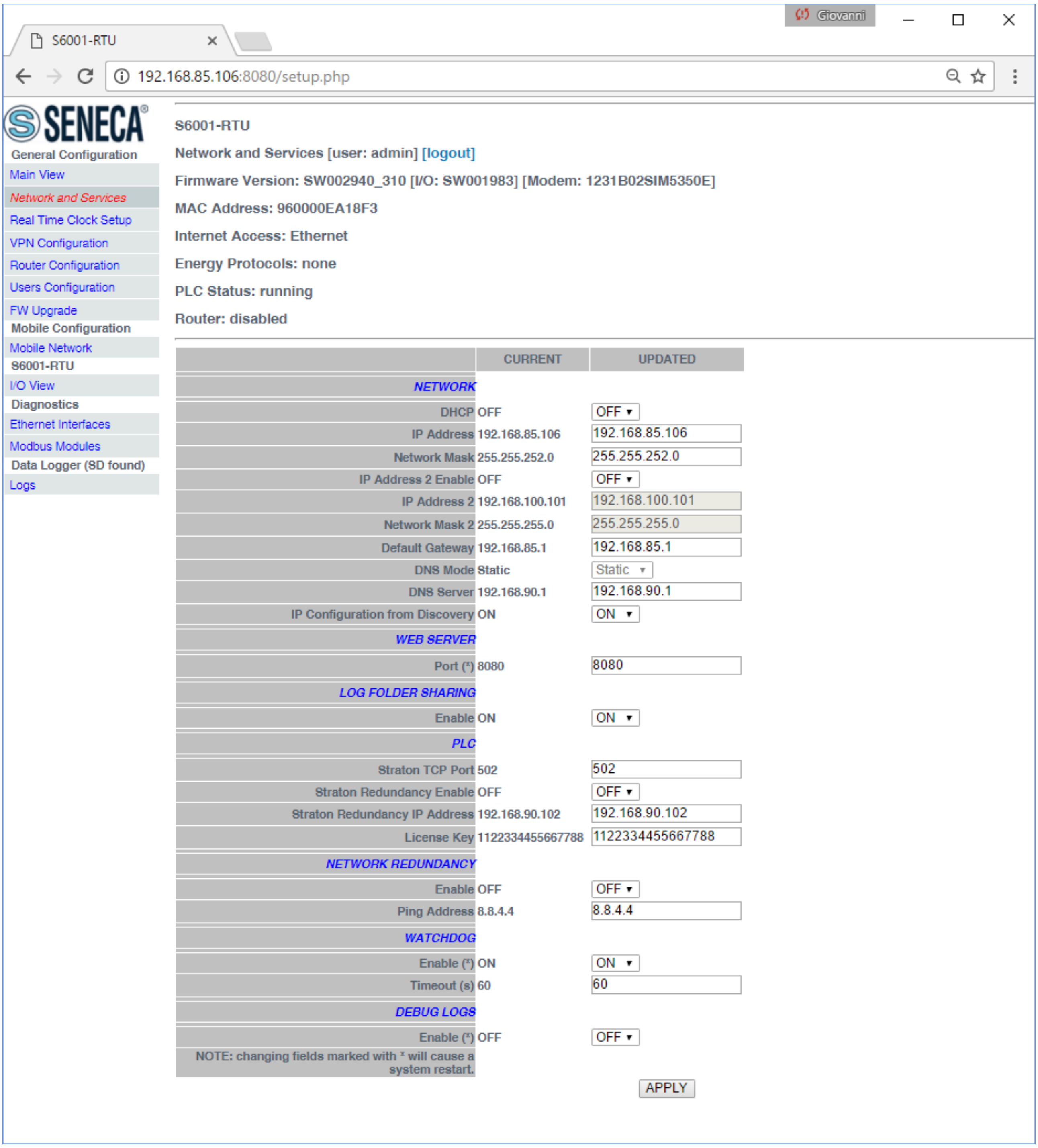
Energy Protocols: none

PLC Status: running

Router: disabled

	CURRENT	UPDATED
NETWORK		
Ethernet Mode (*)	LAN/WAN	LAN/WAN ▾
DHCP on LAN	OFF	OFF ▾
DHCP on WAN	OFF	OFF ▾
LAN IP Address	192.168.95.101	192.168.95.101
LAN Network Mask	255.255.255.0	255.255.255.0
WAN IP Address	192.168.85.103	192.168.85.103
WAN Network Mask	255.255.252.0	255.255.252.0
Default Gateway	192.168.85.1	192.168.85.1
DNS Mode	Static	Static ▾
DNS Server	192.168.84.113	192.168.84.113
IP Configuration from Discovery	ON	ON ▾
WEB SERVER		
Port (*)	8080	8080
LOG FOLDER SHARING		
Enable	ON	ON ▾
PLC		
Straton TCP Port	502	502
Straton Redundancy Enable	OFF	OFF ▾
Straton Redundancy IP Address	192.168.90.102	192.168.90.102
License Key	1122334455667788	1122334455667788
NETWORK REDUNDANCY		
Enable	OFF	OFF ▾
Ping Address	8.8.4.4	8.8.4.4
WATCHDOG		
Enable (*)	ON	ON ▾
Timeout (s)	60	60
DEBUG LOGS		
Enable (*)	ON	ON ▾
NOTE: changing fields marked with * will cause a system restart.		

The previous figure shows the “Network and Services” page for a Z-PASS2-S-R01, when the “Ethernet Mode” parameter is set to “LAN/WAN”; it also applies to a Z-TWS4-R01 in “LAN/WAN” mode.



S6001-RTU

Network and Services [user: admin] [logout]

Firmware Version: SW002940_310 [I/O: SW001983] [Modem: 1231B02SIM5350E]

MAC Address: 960000EA18F3

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running

Router: disabled

	CURRENT	UPDATED
NETWORK		
DHCP	OFF	OFF
IP Address	192.168.85.106	192.168.85.106
Network Mask	255.255.252.0	255.255.252.0
IP Address 2 Enable	OFF	OFF
IP Address 2	192.168.100.101	192.168.100.101
Network Mask 2	255.255.255.0	255.255.255.0
Default Gateway	192.168.85.1	192.168.85.1
DNS Mode	Static	Static
DNS Server	192.168.90.1	192.168.90.1
IP Configuration from Discovery	ON	ON
WEB SERVER		
Port (*)	8080	8080
LOG FOLDER SHARING		
Enable	ON	ON
PLC		
Straton TCP Port	502	502
Straton Redundancy Enable	OFF	OFF
Straton Redundancy IP Address	192.168.90.102	192.168.90.102
License Key	1122334455667788	1122334455667788
NETWORK REDUNDANCY		
Enable	OFF	OFF
Ping Address	8.8.4.4	8.8.4.4
WATCHDOG		
Enable (*)	ON	ON
Timeout (s)	60	60
DEBUG LOGS		
Enable (*)	OFF	OFF
NOTE: changing fields marked with * will cause a system restart.		

The previous figure shows the “Network and Services” page for a S6001-RTU; it also applies to a Z-TWS4 and Z-PASS2-S (old version).

There is an important difference between the parameter values shown in this page and those shown in the “Main View” page: the former are configured values, whereas the latter are actual values.

To better explain this difference, let’s consider the case when the DHCP parameter is set to ON; in the “Network and Services” page, you may see the 192.168.90.101 default value for the “IP Address” parameter, whereas the “Main View” page shows the actual IP Address, assigned by the DHCP server.

In the following table, all configuration parameters available in the page are listed, with a short explanation and the parameter default value for each of them.

Field	**Meaning**	**Default value**
NETWORK/Ethernet Mode	This parameter determines if the two Ethernet ports work as two fully separated network interfaces (“LAN/WAN”) or as the ports of an Ethernet switch (“Switch”); depending on the value of this parameter, some other network parameters are hidden/shown or renamed as described below. This parameter is available only for Z-TWS4-R01, Z-PASS2-S-R01, Z-TWS4-R02 and Z-PASS2-S-R02 products. For all other products, only “Switch” mode is available, hence the parameter is not shown.	LAN/WAN
Ethernet Mode = “Switch”		
NETWORK/DHCP	Flag to enable/disable the DHCP functionality on the Ethernet interface.	OFF
NETWORK/IP Address	IP address of the Ethernet interface (disabled when “DHCP” is set to “ON”)	192.168.90.101
NETWORK/Network Mask	Network mask of the Ethernet interface (disabled when “DHCP” is set to “ON”)	255.255.255.0
NETWORK/IP Address 2 Enable	Flag to enable/disable the second IP address on the Ethernet interface. Note that the second IP address can be enabled also when the DHCP functionality is active.	OFF
NETWORK/IP Address 2	Second IP address of the Ethernet interface	192.168.100.101
NETWORK/Network Mask 2	Second network mask of the Ethernet interface	255.255.255.0
Ethernet Mode = “LAN/WAN”		
NETWORK/DHCP on LAN	When “Ethernet Mode” is set to “LAN/WAN”, this parameter is disabled (always OFF)	OFF
NETWORK/DHCP on WAN	Flag to enable/disable the DHCP functionality on the WAN Ethernet interface	ON

NETWORK/LAN IP Address	IP address of the LAN Ethernet interface	192.168.90.101
NETWORK/LAN Network Mask	Network mask of the LAN Ethernet interface	255.255.255.0
NETWORK/WAN IP Address	IP address of the WAN Ethernet interface (disabled when “DHCP on WAN” is set to “ON”)	192.168.100.101
NETWORK/WAN Network Mask	Network mask of the WAN Ethernet interface (disabled when “DHCP on WAN” is set to “ON”)	255.255.255.0
NETWORK/Default Gateway	Default Gateway IP address (disabled when DHCP functionality is enabled on any interface). When “Ethernet Mode” is set to “LAN/WAN”, the Default Gateway shall be in the WAN subnet.	192.168.100.1 , for Z-TWS4-R0x and Z-PASS2-S-R0x (x=1,2) 192.168.90.1, for all other products
NETWORK/DNS Mode	Tells if the DNS Server shall be set statically (value: “Static”) or dinamically assigned by the DHCP Server (value: “DHCP”)	DHCP, for Z-TWS4-R0x and Z-PASS2-S-R0x (x=1,2) Static, for all other products
NETWORK/DNS Server	DNS server IP address (disabled when DHCP functionality is enabled on any interface and DNS Mode = DHCP)	192.168.100.1 , for Z-TWS4-R0x and Z-PASS2-S-R0x (x=1,2) 192.168.90.1, for all other products
NETWORK/IP Configuration from Discovery	Flag to enable/disable the possibility of changing some of the network configuration parameters by means of the SDD application (see chapter 6)	ON
WEB SERVER/Port	TCP port to access the web configuration site. Please note that if this parameter is set to 80 (standard HTTP port), the web user site won’t be available anymore.	8080
LOG FOLDER SHARING/Enable	Flag to enable/disable the sharing of the “/log” directory (by means of “Samba” service)	ON
PLC/Straton TCP Port	TCP port to connect to the Straton server	502
PLC/Straton Redundancy Enable	Flag to enable/disable the Straton Redundancy functionality	OFF
PLC/Straton Redundancy IP Address	IP address of the second Device used	192.168.90.102

	for Straton Redundancy	
PLC/License Key	Key to enable/disable Energy Protocol functionalities in Straton (see paragraph 8.2)	1122334455667788 (dummy value)[12]
NETWORK REDUNDANCY/Enable	Flag to enable/disable the “Network Redundancy” functionality, that is using the Ethernet interface as the primary interface to access the Internet and the Mobile interface as the secondary interface, if the access through the primary interface becomes unavailable	OFF
NETWORK REDUNDANCY/Ping Address	IP Address used as ping destination to check if access to the Internet through the primary interface (Ethernet) is available. This address shall be different from the one set for “DNS Server” parameter, otherwise an error is shown.	8.8.4.4
WATCHDOG/Enable	Flag to enable/disable the watchdog functionality	ON
WATCHDOG/Timeout (s)	Watchdog timeout, in seconds; when watchdog is enabled, if it’s not refreshed for this amount of seconds, the system will be rebooted. Possible values are in the range [30..3600].	60
DEBUG LOGS/Enable	Flag to enable/disable the debug logs	OFF
COM1/Mode	Operating mode of the COM1 serial port Possible values: RS485 | RS232	RS485

Some notes about the “DHCP” parameters:

- the “DHCP” parameter can be set to “ON” only if the “DHCP Server” parameter of the “Router Configuration” page is set to “OFF” (see paragraph 16.1.5);
- only the “DHCP on WAN” parameter can be set to “ON”.

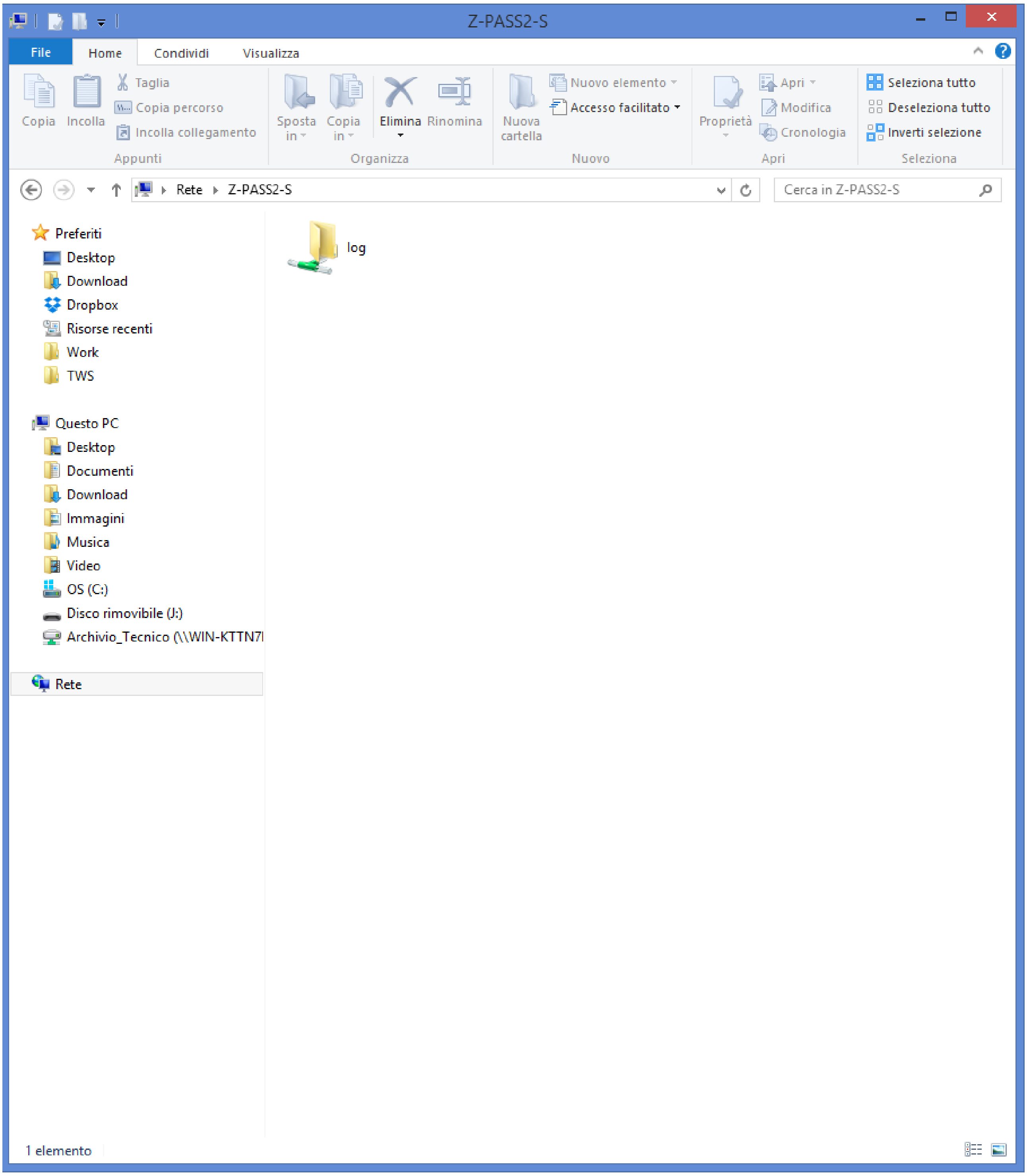
You can change any of the above parameters; to apply the changes, press the “APPLY” button; as warned by the note on the page, only for some parameters, the parameter change requires rebooting the Device; these parameters are:

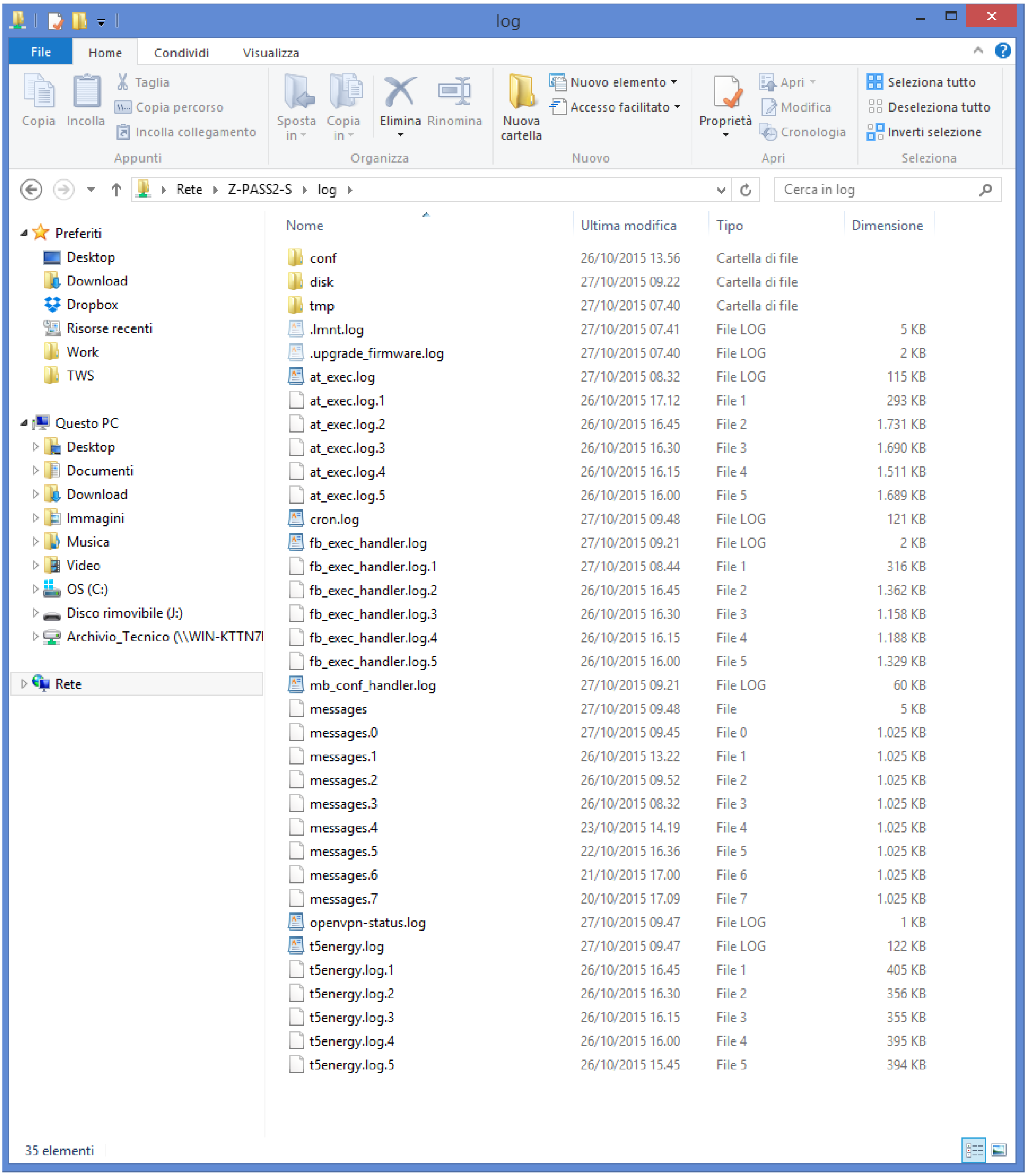
- NETWORK/Ethernet Mode
- WEB SERVER/Port

[12] The correct License Key string is provided by Seneca.

- WATCHDOG/Enable, only when changing ON -> OFF
- DEBUG LOGS/Enable, only when changing ON -> OFF

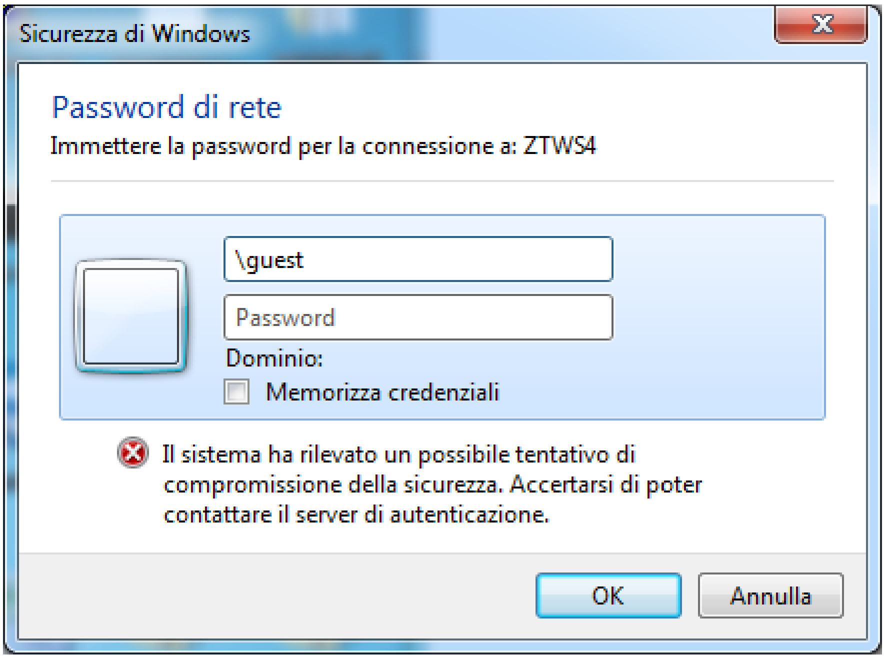
If the “LOG FOLDER SHARING/Enable” parameter is ON, on a Windows PC, you can directly access the “/log” directory, as shown in the following pictures (the sharing name is equal to the product name, without ‘-‘ character, that is “ZPASS2S”, “ZTWS4” or “S6001RTU”):





Nome	Ultima modifica	Tipo	Dimensione
conf	26/10/2015 13.56	Cartella di file	
disk	27/10/2015 09.22	Cartella di file	
tmp	27/10/2015 07.40	Cartella di file	
.lmnt.log	27/10/2015 07.41	File LOG	5 KB
.upgrade_firmware.log	27/10/2015 07.40	File LOG	2 KB
at_exec.log	27/10/2015 08.32	File LOG	115 KB
at_exec.log.1	26/10/2015 17.12	File 1	293 KB
at_exec.log.2	26/10/2015 16.45	File 2	1.731 KB
at_exec.log.3	26/10/2015 16.30	File 3	1.690 KB
at_exec.log.4	26/10/2015 16.15	File 4	1.511 KB
at_exec.log.5	26/10/2015 16.00	File 5	1.689 KB
cron.log	27/10/2015 09.48	File LOG	121 KB
fb_exec_handler.log	27/10/2015 09.21	File LOG	2 KB
fb_exec_handler.log.1	27/10/2015 08.44	File 1	316 KB
fb_exec_handler.log.2	26/10/2015 16.45	File 2	1.362 KB
fb_exec_handler.log.3	26/10/2015 16.30	File 3	1.158 KB
fb_exec_handler.log.4	26/10/2015 16.15	File 4	1.188 KB
fb_exec_handler.log.5	26/10/2015 16.00	File 5	1.329 KB
mb_conf_handler.log	27/10/2015 09.21	File LOG	60 KB
messages	27/10/2015 09.48	File	5 KB
messages.0	27/10/2015 09.45	File 0	1.025 KB
messages.1	26/10/2015 13.22	File 1	1.025 KB
messages.2	26/10/2015 09.52	File 2	1.025 KB
messages.3	26/10/2015 08.32	File 3	1.025 KB
messages.4	23/10/2015 14.19	File 4	1.025 KB
messages.5	22/10/2015 16.36	File 5	1.025 KB
messages.6	21/10/2015 17.00	File 6	1.025 KB
messages.7	20/10/2015 17.09	File 7	1.025 KB
openvpn-status.log	27/10/2015 09.47	File LOG	1 KB
t5energy.log	27/10/2015 09.47	File LOG	122 KB
t5energy.log.1	26/10/2015 16.45	File 1	405 KB
t5energy.log.2	26/10/2015 16.30	File 2	356 KB
t5energy.log.3	26/10/2015 16.15	File 3	355 KB
t5energy.log.4	26/10/2015 16.00	File 4	395 KB
t5energy.log.5	26/10/2015 15.45	File 5	394 KB

Depending on the LAN configuration, a login may be needed to access the shared folder; if so, use the credentials shown in the following figure (username: “\guest”, password: “” [empty]).



Password di rete

Immettere la password per la connessione a: ZTWS4

\guest

Password

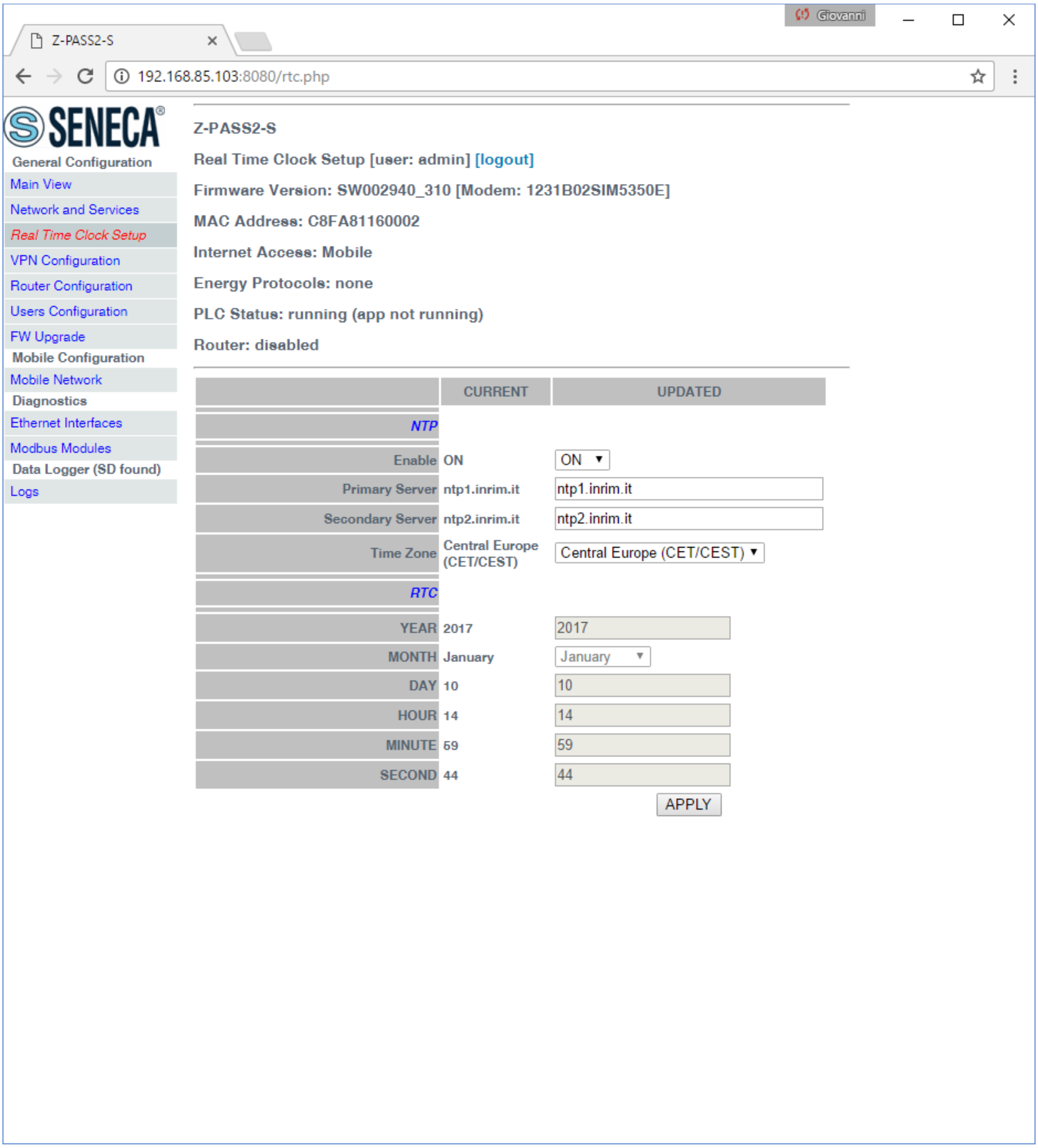
Dominio:

□ Memorizza credenziali

Il sistema ha rilevato un possibile tentativo di compromissione della sicurezza. Accertarsi di poter contattare il server di autenticazione.

16.1.3 Real Time Clock Setup

By clicking on the “Real Time Clock Setup” link, in the “General Configuration” menu, you come to the following page:



Z-PASS2-S

Real Time Clock Setup [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

	CURRENT	UPDATED
NTP		
Enable	ON	ON ▾
Primary Server	ntp1.inrim.it	ntp1.inrim.it
Secondary Server	ntp2.inrim.it	ntp2.inrim.it
Time Zone	Central Europe (CET/CEST)	Central Europe (CET/CEST) ▾
RTC		
YEAR	2017	2017
MONTH	January	January ▾
DAY	10	10
HOUR	14	14
MINUTE	59	59
SECOND	44	44
		APPLY

This page is made up of two sections: “NTP” and “RTC”.

In the “NTP” section, you can change the parameters related to the Network Time Protocol and to the Time Zone, as listed in the following table:

Field	Meaning	Default value
NTP/Enable	Flag to enable/disable time synchronization by means of NTP protocol	ON

NTP/Primary Server	IP address or FQDN[13] of the Primary NTP Server	ntp1.inrim.it
NTP/Secondary Server	IP address or FQDN of the Secondary NTP Server	ntp2.inrim.it
NTP/Time Zone	Time Zone	Central Europe (CET/CEST)

When the "Time Zone" parameter is set to "Central Europe (CET/CEST)" value, the Device automatically enables (CEST) / disables (CET) the "Daylight Saving Time" setting.

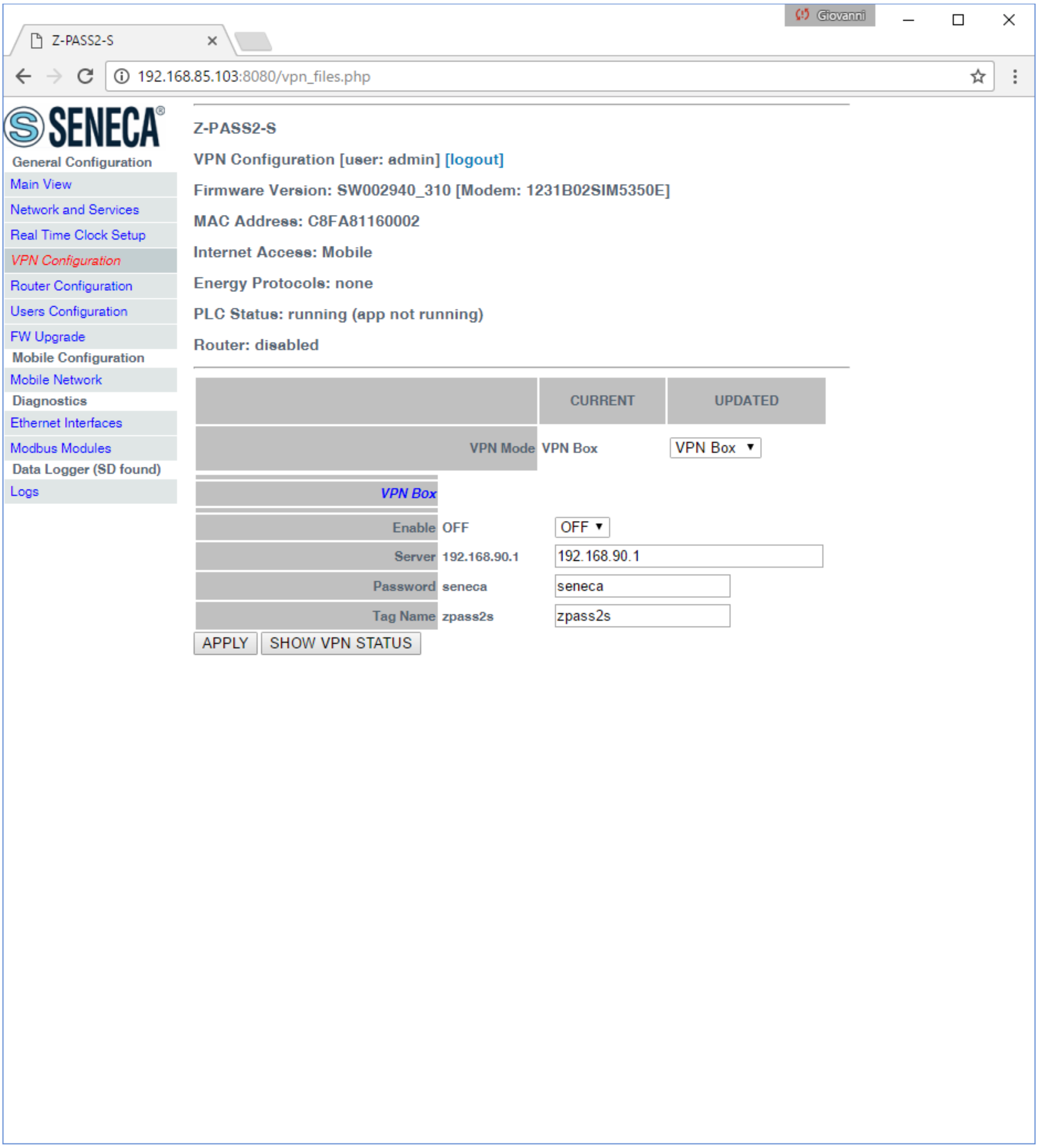
The "RTC" section of the page lets you manually change the Device date/time settings; since this makes sense only if NTP time synchronization is not enabled, when "NTP/Enable" parameter is "ON" the input fields are disabled and the parameters are only for viewing.

Instead, when "NTP/Enable" parameter is "OFF", the input fields in the "NTP" section are still enabled; this lets you change and save the parameter values, even if they are not actually used.

16.1.4 VPN Configuration

By clicking on the "VPN Configuration" link, in the "General Configuration" menu, you come to the following page:

[13] FQDN: Fully Qualified Domain Name, e.g.: "pool.ntp.org".



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

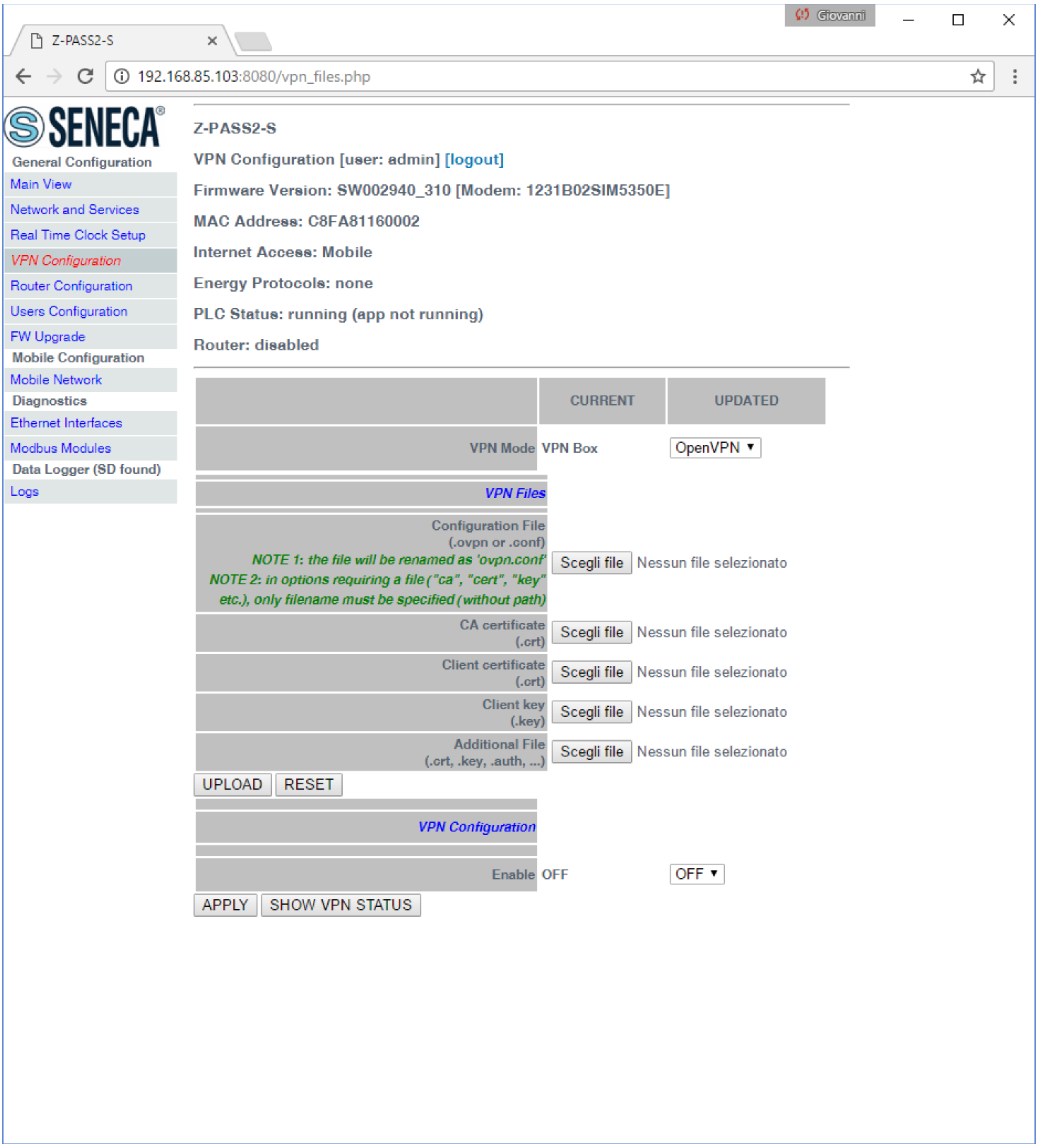
Router: disabled

	CURRENT	UPDATED
VPN Mode	VPN Box	VPN Box ▼
VPN Box		
Enable	OFF	OFF ▼
Server	192.168.90.1	192.168.90.1
Password	seneca	seneca
Tag Name	zpass2s	zpass2s

The page has a different layout depending on the value of the “VPN Mode” parameter, which can be “OpenVPN” or “VPN Box” (for an explanation of these values, see chapter 10).

16.1.4.1 OpenVPN

The page is made up of two sections: “VPN Files” and “VPN Configuration”.



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

	CURRENT	UPDATED
VPN Mode	VPN Box	OpenVPN ▾

VPN Files

Configuration File (.ovpn or .conf) NOTE 1: the file will be renamed as 'ovpn.conf' NOTE 2: in options requiring a file ("ca", "cert", "key" etc.), only filename must be specified (without path)	Scegli file Nessun file selezionato
CA certificate (.crt)	Scegli file Nessun file selezionato
Client certificate (.crt)	Scegli file Nessun file selezionato
Client key (.key)	Scegli file Nessun file selezionato
Additional File (.crt, .key, .auth, ...)	Scegli file Nessun file selezionato

UPLOAD RESET

VPN Configuration

Enable	OFF	OFF ▾

APPLY SHOW VPN STATUS

The “VPN Files” section lets you load the files needed to configure Open VPN and establish a secure VPN connection; these files are described in the following.

16.1.4.1.1 Configuration File

This file shall contain all the information needed to configure the Open VPN behaviour; the main configuration options are[14]:

- if the Device shall act as a client or a server (typically, it will be a client)

[14] For more information about Open VPN configuration options, please refer to the OpenVPN web page (“openvpn.net”).

- the transport protocol (UDP or TCP)
- the server IP address/host name and port
- the files needed to perform authentication procedures
- etc.

This file has the *.ovpn* extension (in Windows systems) or *.conf* extension (in Linux systems); regardless of the original name, it will be renamed as *ovpn.conf* on the Device.

This is the only mandatory file, that is if this file has not been loaded on the Device, VPN can't be enabled.

As reminded in the web page, in options requiring a file argument, only the file name shall be given, with no path, as in the following example:

`ca ca.crt`	**OK**
`ca /home/config/vpn/ca.crt`	**KO !**

Other two important rules that shall be followed are:

- the "dev" option shall be: "`dev tun0`" or "`dev tap0`"
- the "log" option shall be omitted (so that, logs are written to syslog)

An example of a client configuration file is given in paragraph 16.1.4.1.7.

16.1.4.1.2 CA certificate

This file shall contain the Certification Authority (CA) certificate and has the *.crt* extension.

It is needed when the configuration file contains the *"ca"* option.

16.1.4.1.3 Client certificate

This file shall contain the client certificate and has the *.crt* extension.

It is needed when the configuration file contains the *"cert"* option.

16.1.4.1.4 Client key

This file shall contain the client key and has the *.key* extension.

It is needed when the configuration file contains the *"key"* option.

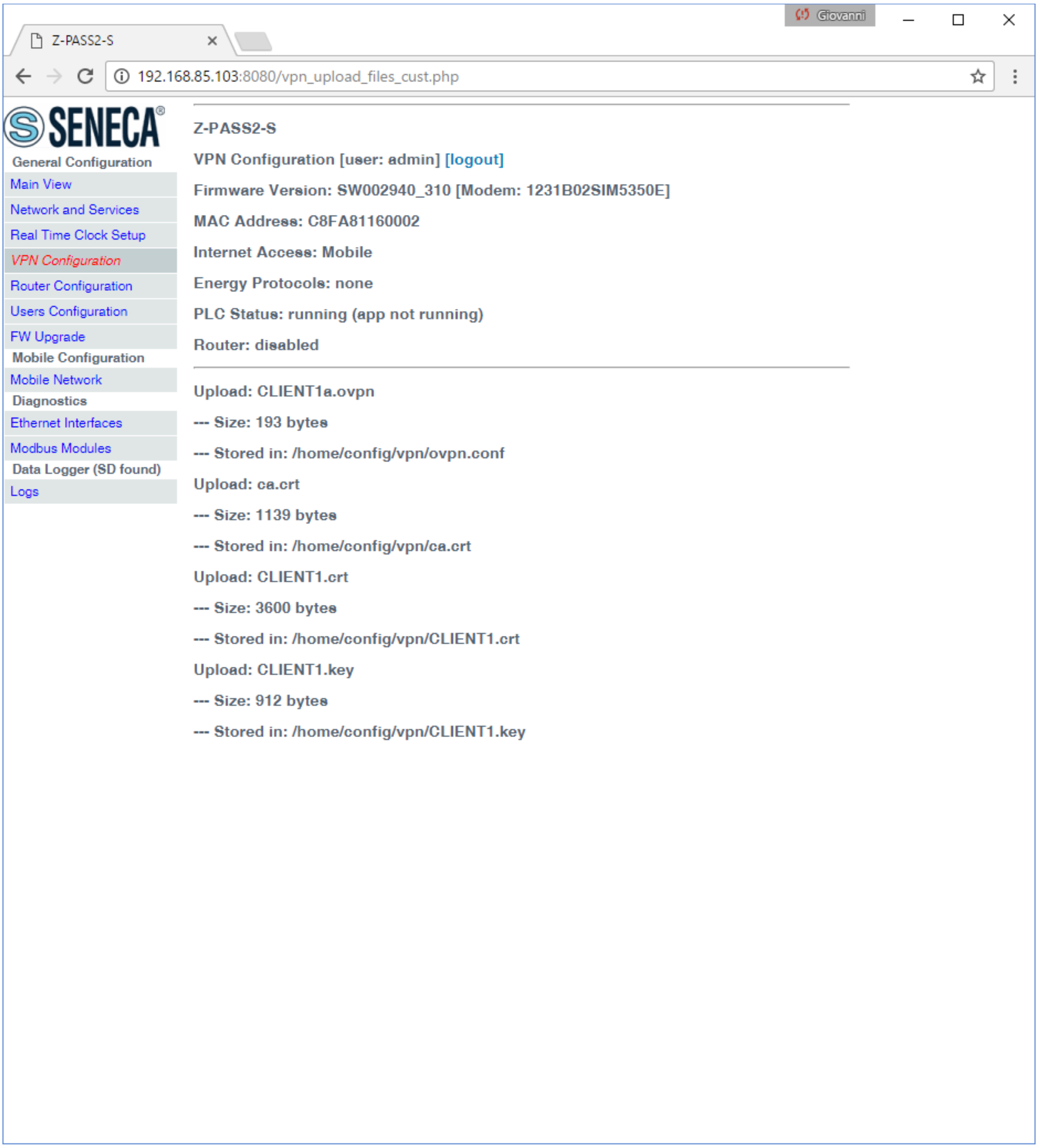
16.1.4.1.5 Additional file

This file can be of any type and may be needed for configuration options other than *"ca"*, *"cert"* and *"key"*.

More than one additional file can be loaded.

You can browse your PC to select the above files and send them to the Device by pressing the "UPLOAD" button.

Once the upload is done, a result page is shown like in the following figure.



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

Upload: CLIENT1a.ovpn

--- Size: 193 bytes

--- Stored in: /home/config/vpn/ovpn.conf

Upload: ca.crt

--- Size: 1139 bytes

--- Stored in: /home/config/vpn/ca.crt

Upload: CLIENT1.crt

--- Size: 3600 bytes

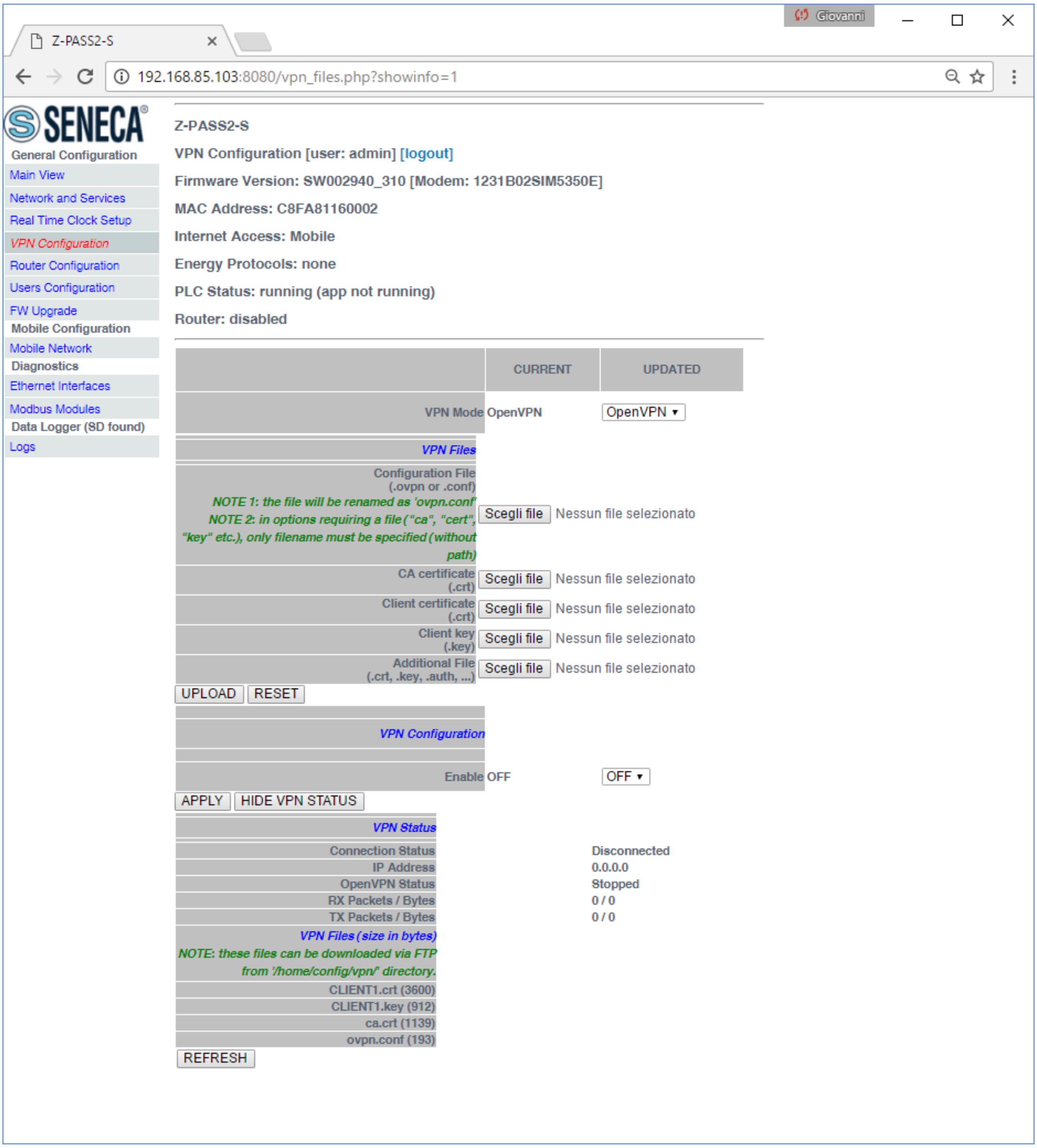
--- Stored in: /home/config/vpn/CLIENT1.crt

Upload: CLIENT1.key

--- Size: 912 bytes

--- Stored in: /home/config/vpn/CLIENT1.key

You can check which VPN files are stored on the Device by clicking on the “SHOW VPN STATUS” button, as shown in the following figure (remember that the configuration file is renamed as “ovpn.conf”):



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

	CURRENT	UPDATED
VPN Mode	OpenVPN	OpenVPN ▾

VPN Files

Configuration File (.ovpn or .conf) NOTE 1: the file will be renamed as 'ovpn.conf' NOTE 2: in options requiring a file ("ca", "cert", "key" etc.), only filename must be specified (without path)	Scegli file Nessun file selezionato
CA certificate (.crt)	Scegli file Nessun file selezionato
Client certificate (.crt)	Scegli file Nessun file selezionato
Client key (.key)	Scegli file Nessun file selezionato
Additional File (.crt, .key, .auth, ...)	Scegli file Nessun file selezionato

VPN Configuration

	CURRENT	UPDATED
Enable	OFF	OFF ▾

VPN Status

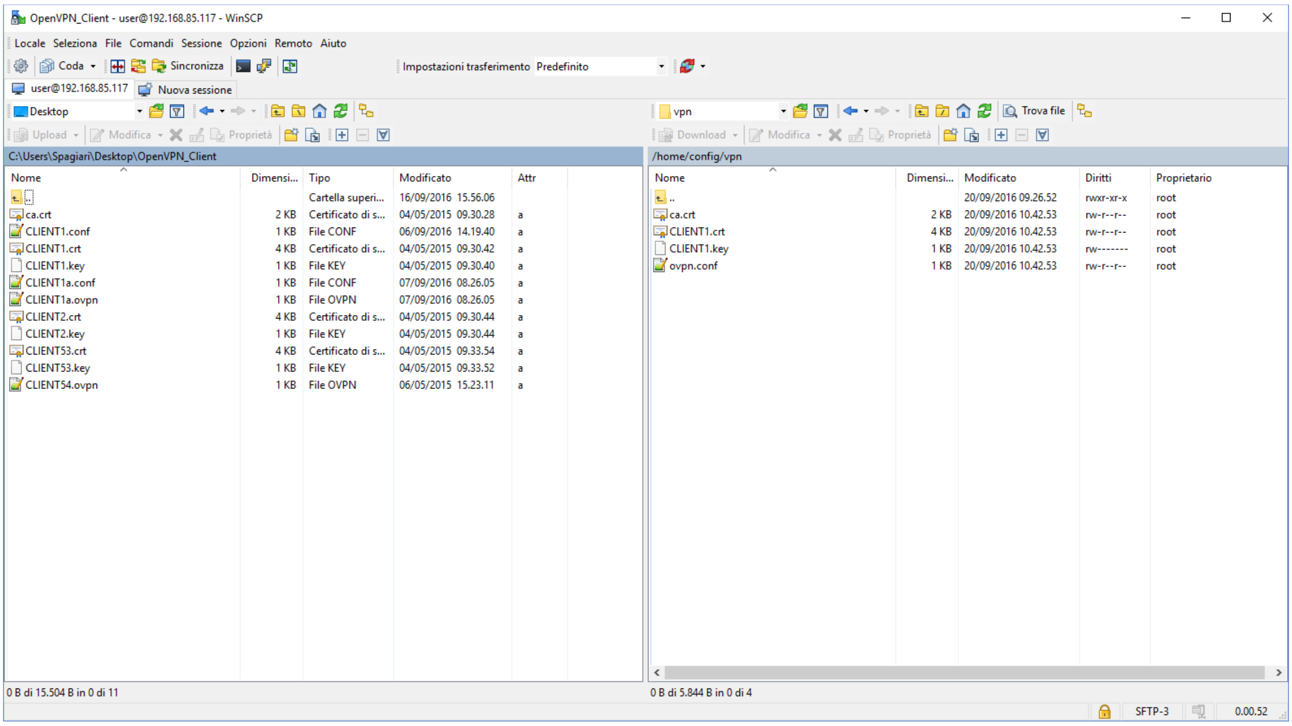
Connection Status	Disconnected
IP Address	0.0.0.0
OpenVPN Status	Stopped
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0

VPN Files (size in bytes)

NOTE: these files can be downloaded via FTP from '/home/config/vpn/' directory.

CLIENT1.crt (3600)
CLIENT1.key (912)
ca.crt (1139)
ovpn.conf (193)

As reminded by the web page, the VPN files can be downloaded from the Device, if needed, via FTP/SFTP; they can be found in the */home/config/vpn* directory, as shown in the following figure.



OpenVPN_Client - user@192.168.85.117 - WinSCP

C:\Users\Spagiari\Desktop\OpenVPN_Client

Nome	Dimensi...	Tipo	Modificato	Attr
..		Cartella superi...	16/09/2016 15.56.06	
ca.crt	2 KB	Certificato di s...	04/05/2015 09.30.28	a
CLIENT1.conf	1 KB	File CONF	06/09/2016 14.19.40	a
CLIENT1.crt	4 KB	Certificato di s...	04/05/2015 09.30.42	a
CLIENT1.key	1 KB	File KEY	04/05/2015 09.30.40	a
CLIENT1a.conf	1 KB	File CONF	07/09/2016 08.26.05	a
CLIENT1a.ovpn	1 KB	File OVPN	07/09/2016 08.26.05	a
CLIENT2.crt	4 KB	Certificato di s...	04/05/2015 09.30.44	a
CLIENT2.key	1 KB	File KEY	04/05/2015 09.30.44	a
CLIENT53.crt	4 KB	Certificato di s...	04/05/2015 09.33.54	a
CLIENT53.key	1 KB	File KEY	04/05/2015 09.33.52	a
CLIENT54.ovpn	1 KB	File OVPN	06/05/2015 15.23.11	a

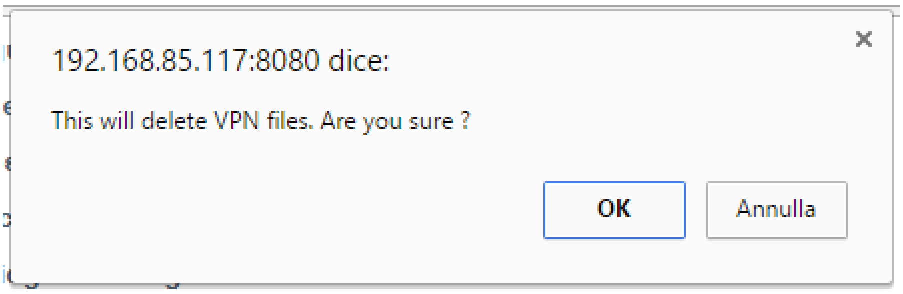
0 B di 15.504 B in 0 di 11

/home/config/vpn

Nome	Dimensi...	Modificato	Diritti	Proprietario
..		20/09/2016 09.26.52	rwxr-xr-x	root
ca.crt	2 KB	20/09/2016 10.42.53	rw-r--r--	root
CLIENT1.crt	4 KB	20/09/2016 10.42.53	rw-r--r--	root
CLIENT1.key	1 KB	20/09/2016 10.42.53	rw-------	root
ovpn.conf	1 KB	20/09/2016 10.42.53	rw-r--r--	root

0 B di 5.844 B in 0 di 4

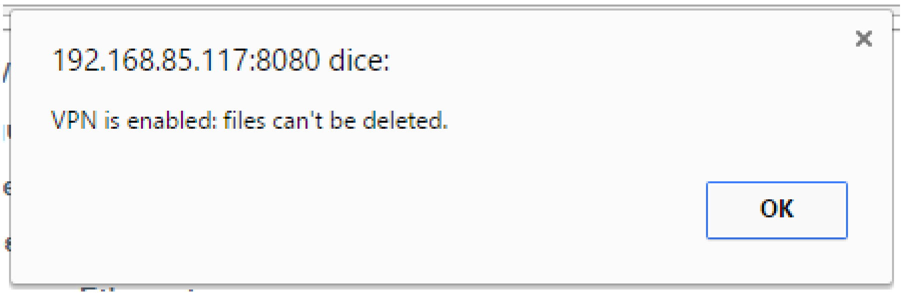
Is is possible to clear all the VPN files, by clicking on the “RESET” button; a pop-up will appear, requiring a confirmation:



192.168.85.117:8080 dice:

This will delete VPN files. Are you sure ?

If VPN is enabled, the user is not allowed to delete VPN files, as warned by the following pop-up:



192.168.85.117:8080 dice:

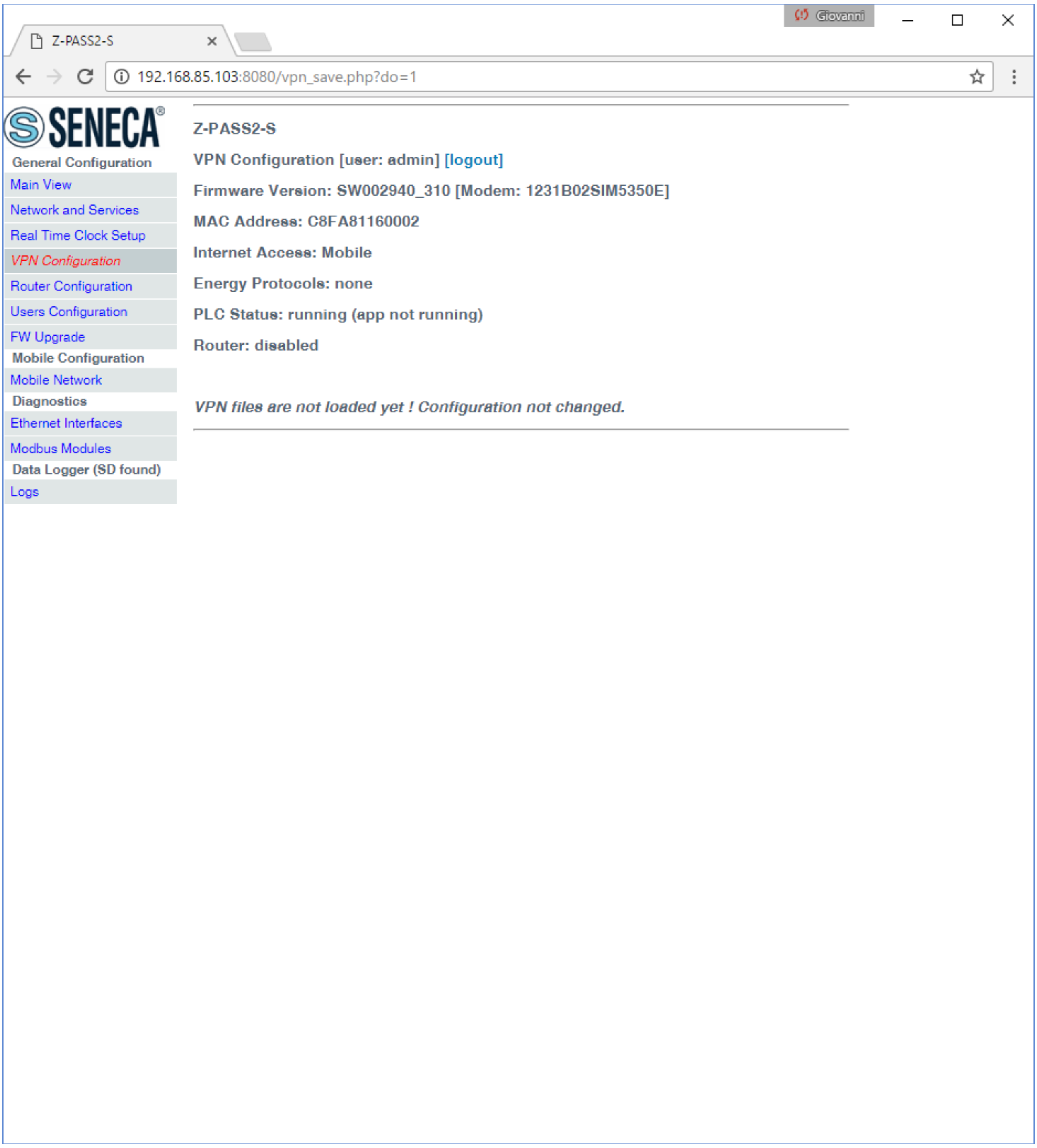
VPN is enabled: files can't be deleted.

In the “VPN Configuration” section, there is only one parameter, as described in the following table:

Field	Meaning	Default value
VPN Configuration/Enable	Flag to enable/disable the VPN connectivity; when enabled, the	OFF

	Device will run the Open VPN process with the loaded configuration	

As already told above, if you try to enable the VPN connectivity, but no configuration file has been uploaded to the Device yet, an error is given as shown in the following figure:



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

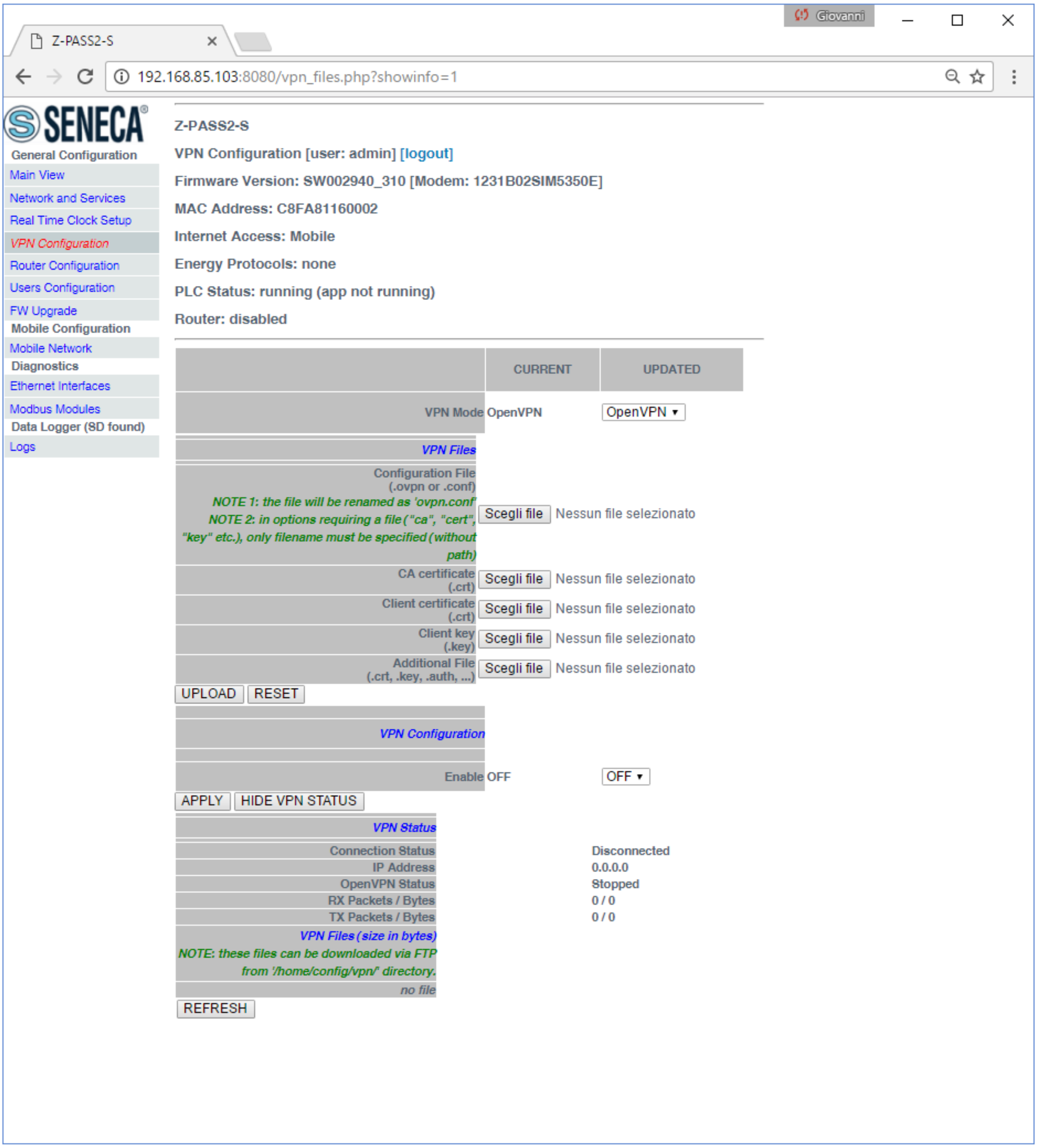
VPN files are not loaded yet ! Configuration not changed.

When you click on the “SHOW VPN STATUS” button, a third section appears, named “VPN Status”, showing:

- the VPN “Connection Status” (i.e.: “Disconnected” or “Connected”)

- the IP address assigned to the VPN interface when "Connected", the "dummy" IP address "0.0.0.0" when "Disconnected"
- the "OpenVPN Status" (i.e.: "Stopped" or "Running")
- the number of packets/bytes received from the VPN interface, when connected; "0/0" when disconnected
- the number of packets/bytes sent to the VPN interface, when connected; "0/0" when disconnected
- the VPN files stored on the Device (see above)

as shown in the following couple of figures:



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

	CURRENT	UPDATED
VPN Mode	OpenVPN	OpenVPN ▾
VPN Files		
Configuration File (.ovpn or .conf) *NOTE 1: the file will be renamed as 'ovpn.conf'* *NOTE 2: in options requiring a file ("ca", "cert", "key" etc.), only filename must be specified (without path)*	Scegli file	Nessun file selezionato
CA certificate (.crt)	Scegli file	Nessun file selezionato
Client certificate (.crt)	Scegli file	Nessun file selezionato
Client key (.key)	Scegli file	Nessun file selezionato
Additional File (.crt, .key, .auth, ...)	Scegli file	Nessun file selezionato

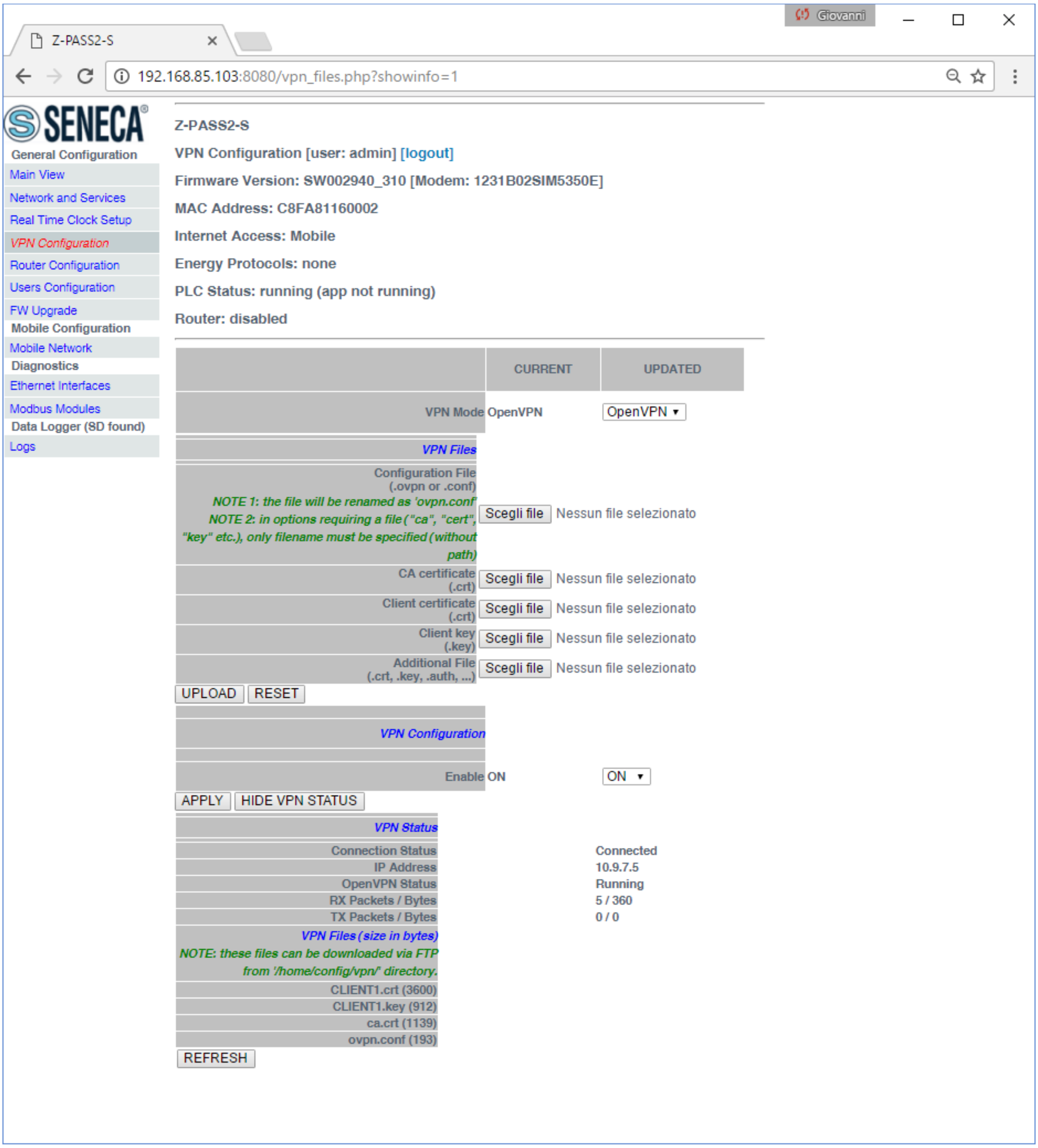
UPLOAD RESET

VPN Configuration		
Enable	OFF	OFF ▾

APPLY HIDE VPN STATUS

VPN Status	
Connection Status	Disconnected
IP Address	0.0.0.0
OpenVPN Status	Stopped
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0
VPN Files (size in bytes)	
NOTE: these files can be downloaded via FTP from '/home/config/vpn/' directory.	
no file	

REFRESH



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

	CURRENT	UPDATED
VPN Mode	OpenVPN	OpenVPN ▾

VPN Files

Configuration File (.ovpn or .conf) *NOTE 1: the file will be renamed as 'ovpn.conf'* *NOTE 2: in options requiring a file ("ca", "cert", "key" etc.), only filename must be specified (without path)*	Scegli file Nessun file selezionato
CA certificate (.crt)	Scegli file Nessun file selezionato
Client certificate (.crt)	Scegli file Nessun file selezionato
Client key (.key)	Scegli file Nessun file selezionato
Additional File (.crt, .key, .auth, ...)	Scegli file Nessun file selezionato

UPLOAD RESET

VPN Configuration

Enable	ON	ON ▾

APPLY HIDE VPN STATUS

VPN Status

Connection Status	Connected
IP Address	10.9.7.5
OpenVPN Status	Running
RX Packets / Bytes	5 / 360
TX Packets / Bytes	0 / 0

VPN Files (size in bytes)

NOTE: these files can be downloaded via FTP from '/home/config/vpn/' directory.

CLIENT1.crt (3600)
CLIENT1.key (912)
ca.crt (1139)
ovpn.conf (193)

REFRESH

An important status information is given by the “OpenVPN Status” field; if VPN is enabled (“ON”), but this status is “Stopped”, Open VPN process could not be correctly started: probably, the configuration file contains some errors or, maybe, some options not supported by the Device Open VPN implementation.

You can refresh the VPN status, by clicking on the “REFRESH” button.

Finally, you can hide the “VPN Status” section, by clicking on the “HIDE VPN STATUS” button.

16.1.4.1.6 OpenVPN Server configuration file

This paragraph gives an example of OpenVPN server configuration; this is the server configuration typically used with Z-TWS4/Z-PASS2-S/S6001-RTU devices.

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.9.7.0 255.255.255.0
ifconfig-pool-persist ipp.txt
client-config-dir ccd
client-to-client
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 3
```

16.1.4.1.7 OpenVPN Client configuration file

This paragraph gives an example of OpenVPN client configuration; this is the client configuration typically loaded on Z-TWS4/Z-PASS2-S/S6001-RTU devices.

```
client
dev tun
port 1194
proto udp
remote 2.192.5.105 1194
nobind
ca ca.crt
cert tws4.crt
key tws4.key
comp-lzo
persist-key
persist-tun
script-security 3 system
verb 3
```

16.1.4.1.8 LED signalling (Z-TWS4-R01/Z-PASS2-S-R01/Z-TWS4-R02/Z-PASS2-S-R02)

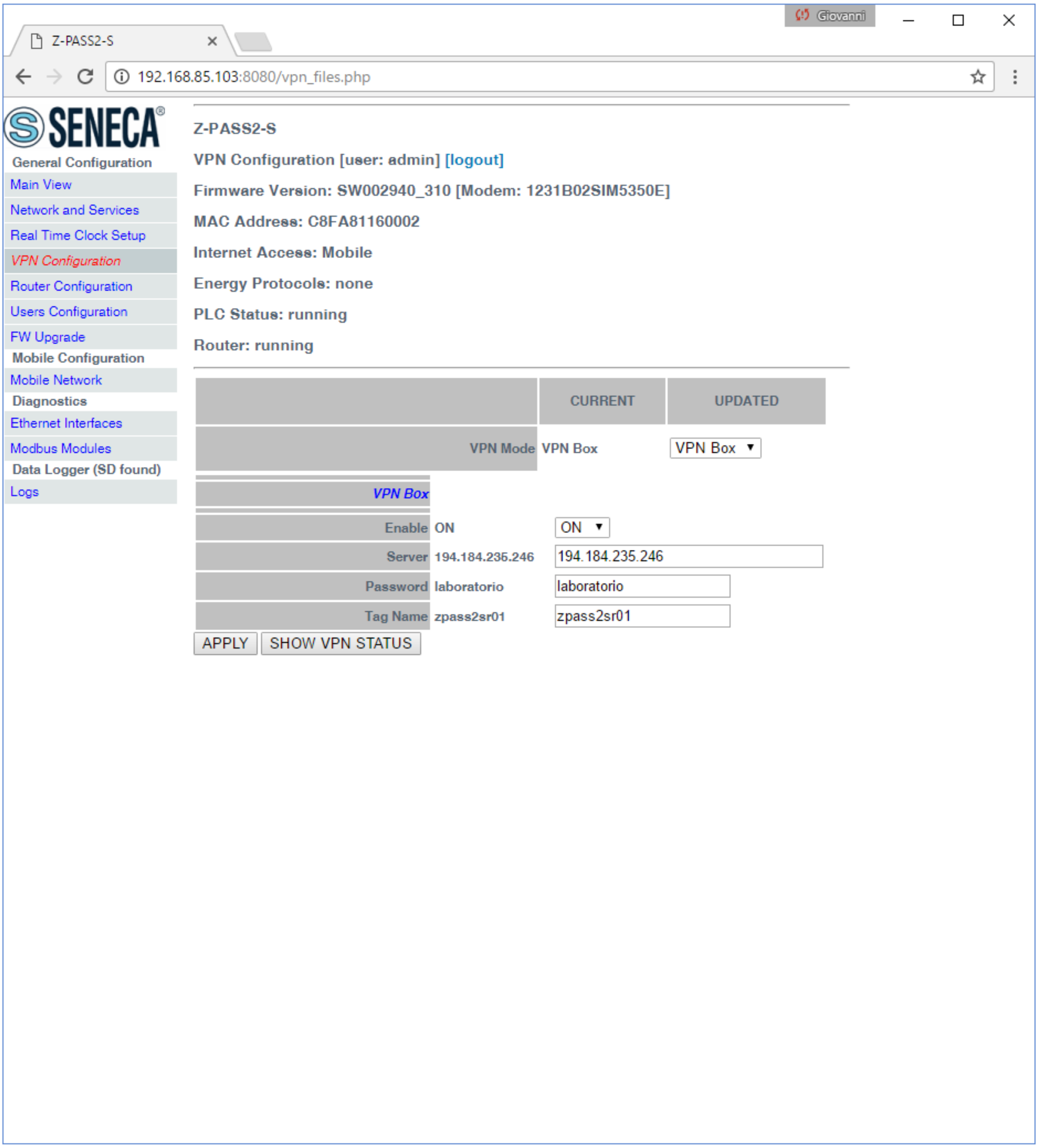
In Z-TWS4-R0x/Z-PASS2-S-R0x (x=1,2) products, when VPN functionality is enabled in “OpenVPN” mode, the “SERV” and “VPN“ LEDs give the following status information (see paragraphs 5.2 and 5.3):

LED	Status	Meaning
VPN Yellow	ON Blinking	VPN connection is working properly VPN connection is not working properly

	OFF	VPN functionality is disabled
SERV Green	-	Not used

16.1.4.2 VPN Box

The page contains only ony section: “VPN Box”, as shown in the following figure.



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running

Router: running

	CURRENT	UPDATED
VPN Mode	VPN Box	VPN Box
VPN Box		
Enable	ON	ON
Server	194.184.235.246	194.184.235.246
Password	laboratorio	laboratorio
Tag Name	zpass2sr01	zpass2sr01

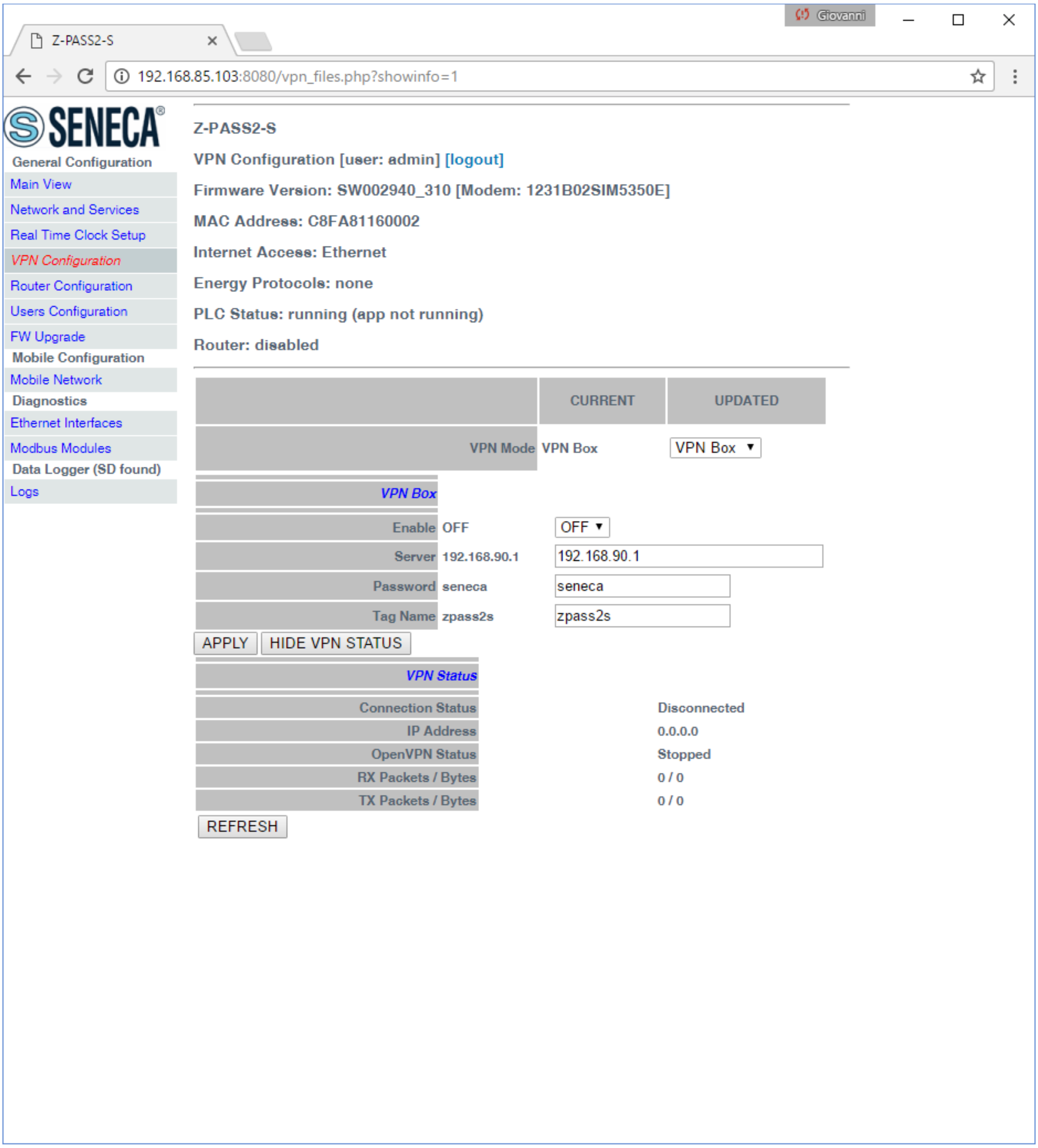
The “VPN Box” section contains the following parameters:

Field	Meaning	Default value
VPN BOX/Enable	Flag to enable/disable the “VPN Box” functionality, that is the procedure/protocol that lets the Device setup the VPN, by interacting with the “VPN Box” server (see “VPN Box User Manual”)	OFF
VPN BOX/Server	IP address or FQDN of the “VPN Box” server	192.168.90.1
VPN BOX/Password	Password to access the “VPN Box” server	seneca
VPN BOX/Tag Name	Mnemonic name used to uniquely identify the Device; if the default (“zpass2s”) value is left, the Device will register as “zpass2s_<MACAddress>” or “ztws4_<MACAddress>” on the VPN Box	zpass2s

When you click on the “SHOW VPN STATUS” button, a new section appears, named “VPN Status”, showing:

- the VPN “Connection Status” (i.e.: “Disconnected” or “Connected”)
- the IP address assigned to the VPN interface when “Connected”, the “dummy” IP address “0.0.0.0” when “Disconnected”
- the “OpenVPN Status” (i.e.: “Stopped” or “Running”)
- the number of packets/bytes received from the VPN interface, when connected; “0/0” when disconnected
- the number of packets/bytes sent to the VPN interface, when connected; “0/0” when disconnected
- the “VPN Box Type”, which can be “Point-to-Point” or “Single LAN”, if VPN Box is enabled
- the “VPN Box Status”, if VPN Box is enabled

as shown in the following couple of figures:



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

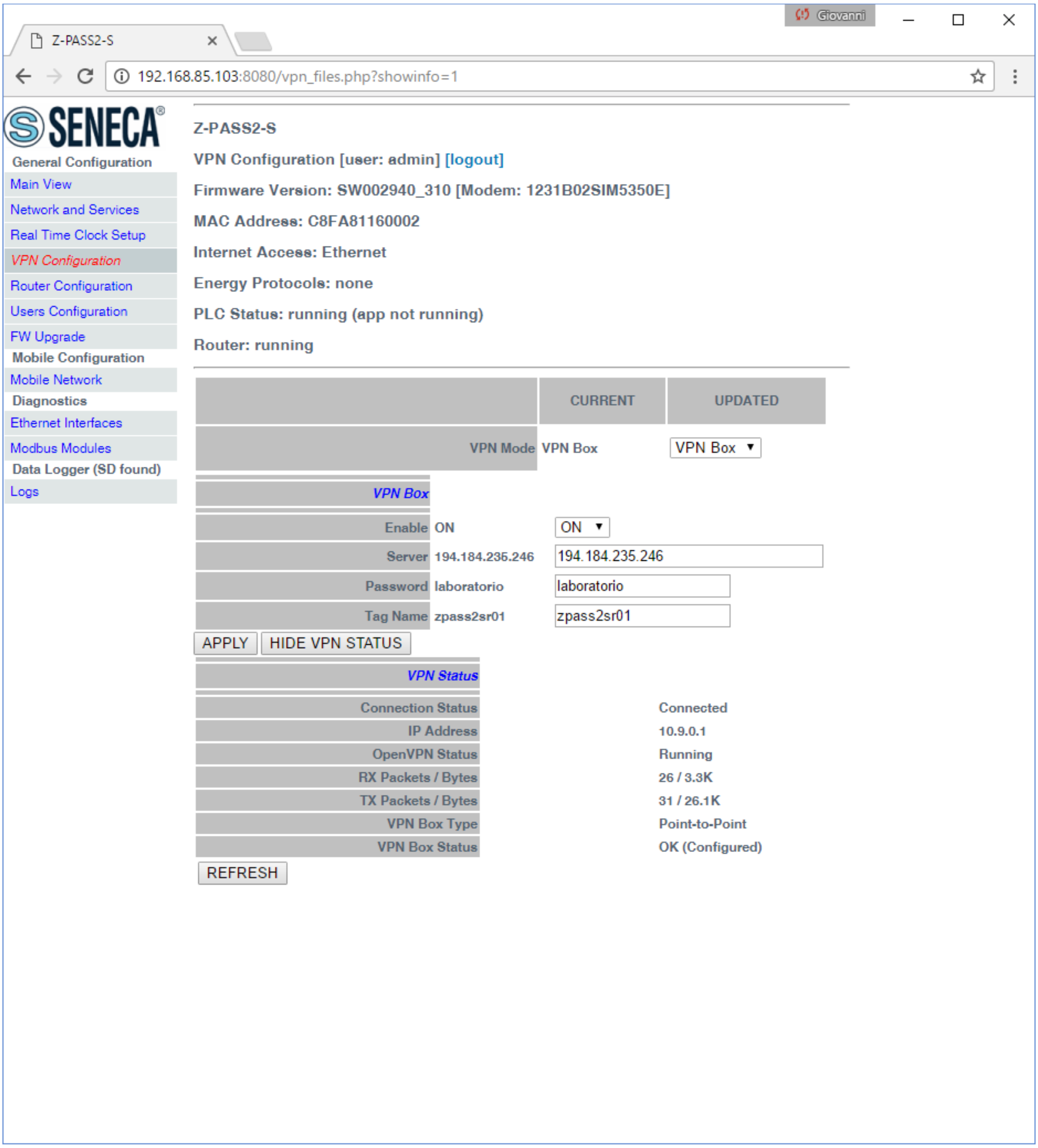
	CURRENT	UPDATED
VPN Mode	VPN Box	VPN Box ▼

VPN Box		
Enable	OFF	OFF ▼
Server	192.168.90.1	192.168.90.1
Password	seneca	seneca
Tag Name	zpass2s	zpass2s

APPLY | HIDE VPN STATUS

VPN Status	
Connection Status	Disconnected
IP Address	0.0.0.0
OpenVPN Status	Stopped
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0

REFRESH



Z-PASS2-S

VPN Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running (app not running)

Router: running

	CURRENT	UPDATED
VPN Mode	VPN Box	VPN Box ▾

VPN Box		
Enable	ON	ON ▾
Server	194.184.235.246	194.184.235.246
Password	laboratorio	laboratorio
Tag Name	zpass2sr01	zpass2sr01

APPLY HIDE VPN STATUS

VPN Status	
Connection Status	Connected
IP Address	10.9.0.1
OpenVPN Status	Running
RX Packets / Bytes	26 / 3.3K
TX Packets / Bytes	31 / 26.1K
VPN Box Type	Point-to-Point
VPN Box Status	OK (Configured)

REFRESH

For an explanation of the differences between a “Single LAN” VPN and a “Point-to-Point” VPN, see chapter 10.

The “VPN Box Status” string has the following format:

Result (Status)

The following table gives a short explanation of the possible “Result” and “Status” strings:

Result	Status	Meaning
Error (Unexpected response)		A response code has been received that is not

		handled by the Device (it should never occur)
Error (No response from VPN Box)		No response has been received from the VPN Box (response timeout); this is normally due to connectivity problems
Error (Invalid response from VPN Box)		A response has been received whose content is not valid for the Device (it should never occur)
Error (Wrong password)		The password set on the Device is wrong
Error (License Limit Reached)		The maximum number of devices allowed by the license are already registered on VPN Box
Error (VPN Box not configured)		The VPN Box has not been configured yet
Error (Generic error)		A generic error has occurred on the VPN Box
OK		The Device has just been registered on the VPN Box
OK	New	The Device is registered on the VPN Box, but it is not configured yet (“Single LAN” only)
OK	Configuration updated	The Device configuration has just been updated
OK	Configured	The Device is properly configured and available for VPN connection
OK	Ban	The Device has been banned
OK	Not found	The Device is unknown for the VPN Box; this happens when Device registration is deleted on the VPN Box
OK	Unknown	The Device has an “unknown” status in the VPN Box (it should never occur)
OK	Not bound	The “tunnel” between the Device and the VPN Box is not up; this may occur when the tunnel port is blocked (“not open”) in the ADSL router on the VPN Box side (“Point-to-Point” only)
OK	Unexpected status	A status code has been received that is not handled by the Device (it should never occur)

You can refresh the VPN status, by clicking on the “REFRESH” button.

Finally, you can hide the “VPN Status” section, by clicking on the “HIDE VPN STATUS” button.

16.1.4.2.1 LED signalling (Z-TWS4-R01/Z-PASS2-S-R01/Z-TWS4-R02/Z-PASS2-S-R02)

In Z-TWS4-R0x/Z-PASS2-S-R0x (x=1,2) products, when VPN functionality is enabled in “VPN Box/Single LAN” mode, the “SERV” and “VPN“ LEDs give the following status information (see paragraph 5.2 and 5.3):

LED	Status	Meaning
VPN Yellow	ON	VPN connection is working properly
	Blinking	VPN connection is not working properly
	OFF	The Device has not been configured by the VPN Box yet or VPN Box functionality is disabled
SERV Green	ON	VPN Box “SERVICE” connection is working properly

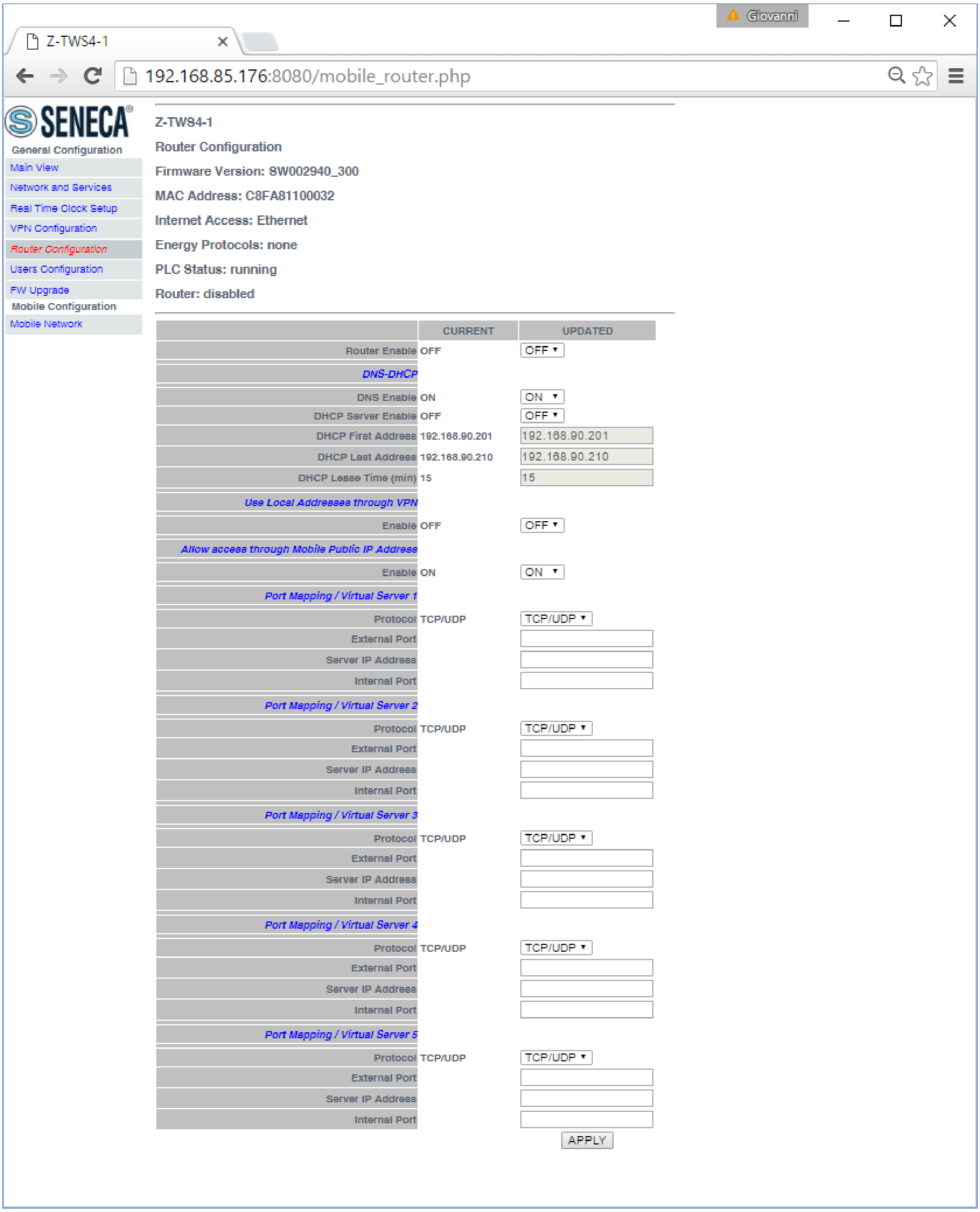
	Blinking OFF	VPN Box “SERVICE” connection is not working properly VPN Box functionality is disabled

Similarly, when VPN functionality is enabled in “VPN Box/Point-to-Point” mode, the “SERV” and “VPN“ LEDs give the following status information (see paragraph 5.2 and 5.3):

LED	Status	Meaning
VPN Yellow	ON OFF	A VPN client is connected to the Device No VPN client is connected to the Device or VPN Box functionality is disabled
SERV Green	ON Blinking OFF	VPN Box “SERVICE” connection is working properly VPN Box “SERVICE” connection is not working properly VPN Box functionality is disabled

16.1.5 Router Configuration

By clicking on the “Router Configuration” link, in the “General Configuration” menu, you come to the following page:



Z-TWS4-1

Router Configuration

Firmware Version: SW002940_300

MAC Address: C8FA81100032

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running

Router: disabled

	CURRENT	UPDATED
Router Enable	OFF	OFF
DNS-DHCP		
DNS Enable	ON	ON
DHCP Server Enable	OFF	OFF
DHCP First Address	192.168.90.201	192.168.90.201
DHCP Last Address	192.168.90.210	192.168.90.210
DHCP Lease Time (min)	15	15
Use Local Addresses through VPN		
Enable	OFF	OFF
Allow access through Mobile Public IP Address		
Enable	ON	ON
Port Mapping / Virtual Server 1		
Protocol	TCP/UDP	TCP/UDP
External Port		
Server IP Address		
Internal Port		
Port Mapping / Virtual Server 2		
Protocol	TCP/UDP	TCP/UDP
External Port		
Server IP Address		
Internal Port		
Port Mapping / Virtual Server 3		
Protocol	TCP/UDP	TCP/UDP
External Port		
Server IP Address		
Internal Port		
Port Mapping / Virtual Server 4		
Protocol	TCP/UDP	TCP/UDP
External Port		
Server IP Address		
Internal Port		
Port Mapping / Virtual Server 5		
Protocol	TCP/UDP	TCP/UDP
External Port		
Server IP Address		
Internal Port		

In this page, you can change the parameters related to the Router functionality.

First, you have a set of general parameters, as listed in the following table:

Field	**Meaning**	**Default value**
Router Enable	Flag to enable/disable the Router	OFF

	functionality	
DNS Enable	Flag to enable/disable the DNS forwarding service	ON
DHCP Server Enable	Flag to enable/disable the DHCP service (DHCP server) NOTE: this parameter can be set to "ON" only if the "DHCP"/"DHCP on LAN" parameter of the "Network and Services" page is set to "OFF".	OFF
DHCP First Address DHCP Last Address	These parameters define the range of IP addresses assigned by the DHCP server to requesting clients	192.168.90.201 192.168.90.210
DHCP Lease Time (min)	Validity period for the IP address assignment, in minutes. Possible values are in the range [1..60].	15

Then, you have the parameter shown in the following table.

Field	**Meaning**	**Default value**
Use Local Addresses Through VPN	Flag to enable/disable the access to the Device and other devices which are in the Device LAN by using their local (LAN) IP addresses	OFF

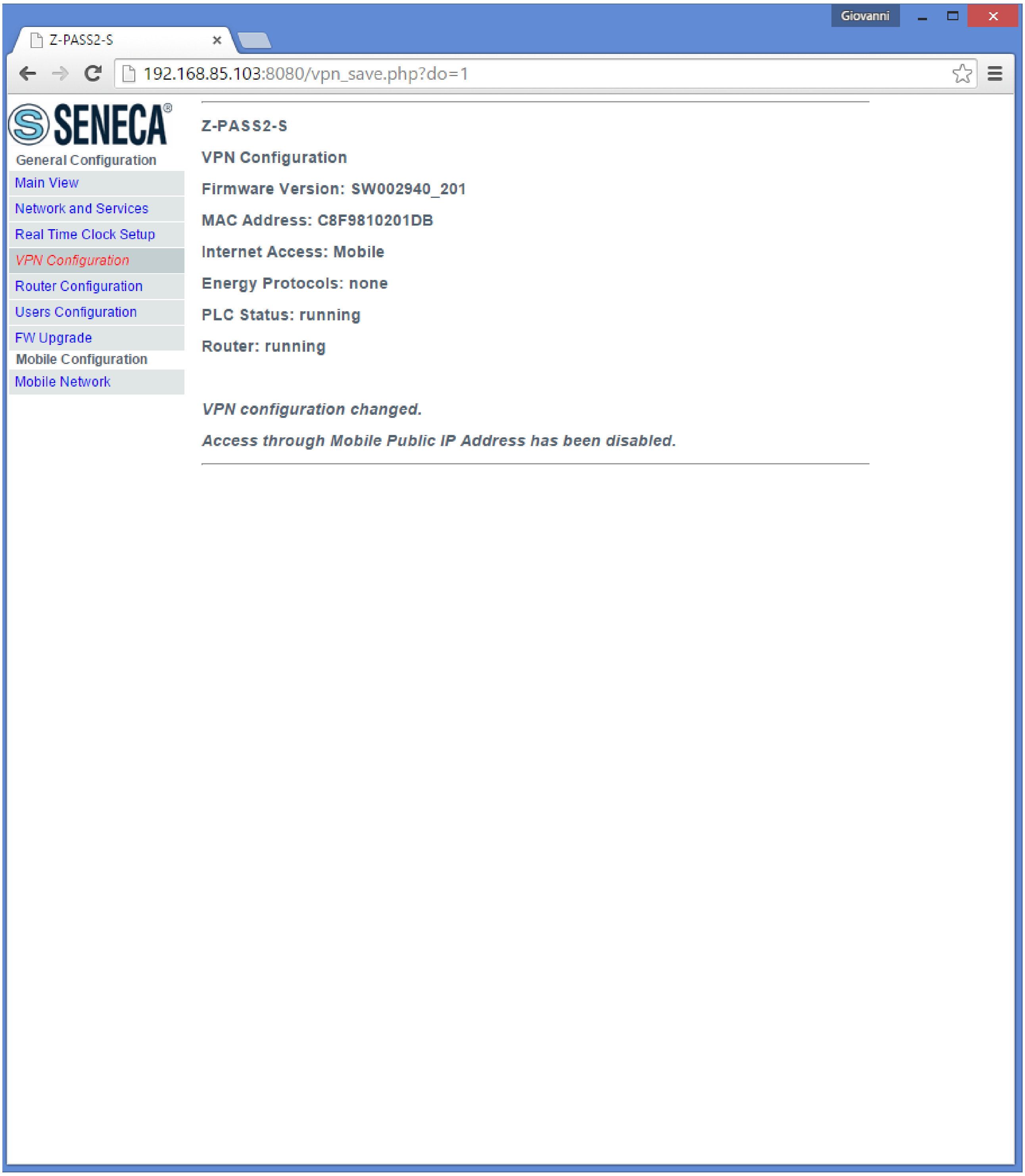
Then, you have another important parameter, which is shown in the following table.

Field	**Meaning**	**Default value**
Allow access through Mobile Public IP Address/Enable	Flag to enable/disable access to the Device and other devices which are in the Device LAN, by using the IP address assigned to the Mobile Network (3G) interface	ON

The above parameter shall be set to OFF, to protect the Device against undesired (maybe malicious) accesses.

This is the only parameter in the "Router Configuration" page that is working also when the Router functionality is disabled (Router Enable = OFF).

It is important to note that, when the VPN is activated (see 16.1.4 paragraph), the parameter is automatically set to OFF, as warned by the message shown in the following figure.



Z-PASS2-S

VPN Configuration

Firmware Version: SW002940_201

MAC Address: C8F9810201DB

Internet Access: Mobile

Energy Protocols: none

PLC Status: running

Router: running

VPN configuration changed.

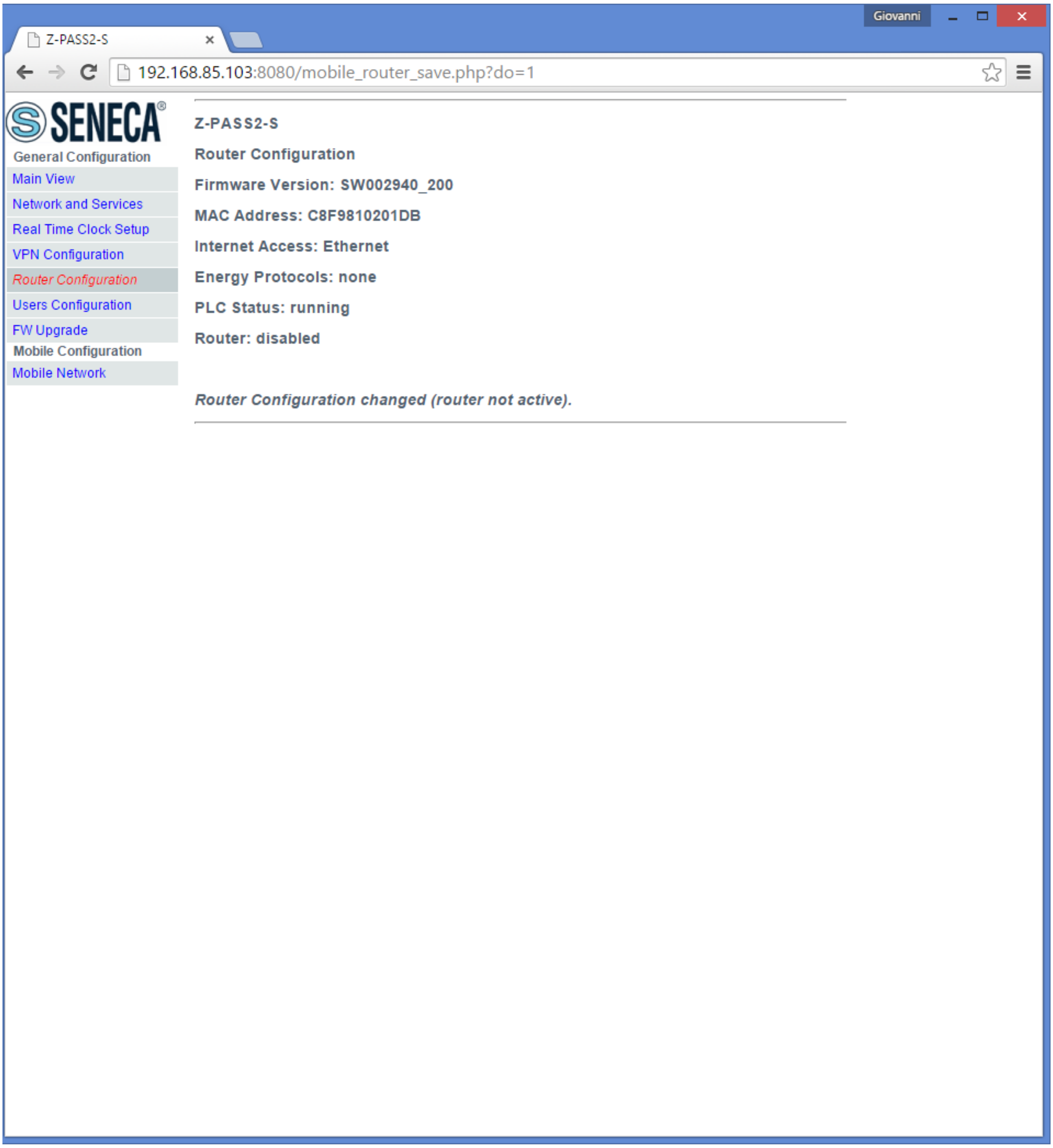
Access through Mobile Public IP Address has been disabled.

Finally, there are 5 sections which let you define up to 5 “Port Mapping” rules (also known as “Virtual Servers”); in each section, the available parameters are the following:

Field	**Meaning**	**Default value**
Protocol	This parameter defines the transport protocol (or kind of port) which is affected by the rule: TCP, UDP or both	TCP/UDP

External Port	TCP or UDP port which a packet was originally sent to	*Empty*
Server IP Address	IP address which the received packet is forwarded to	*Empty*
Internal Port	TCP or UDP port which the received packet is forwarded to	*Empty*

If Router is left disabled (Router Enabled = OFF), you can still change parameters; changes will be saved without actually applying them (except for the "Allow access…" parameter, as told before); the following message will be given, after clicking the "APPLY" button:



Z-PASS2-S

Router Configuration

Firmware Version: SW002940_200

MAC Address: C8F9810201DB

Internet Access: Ethernet

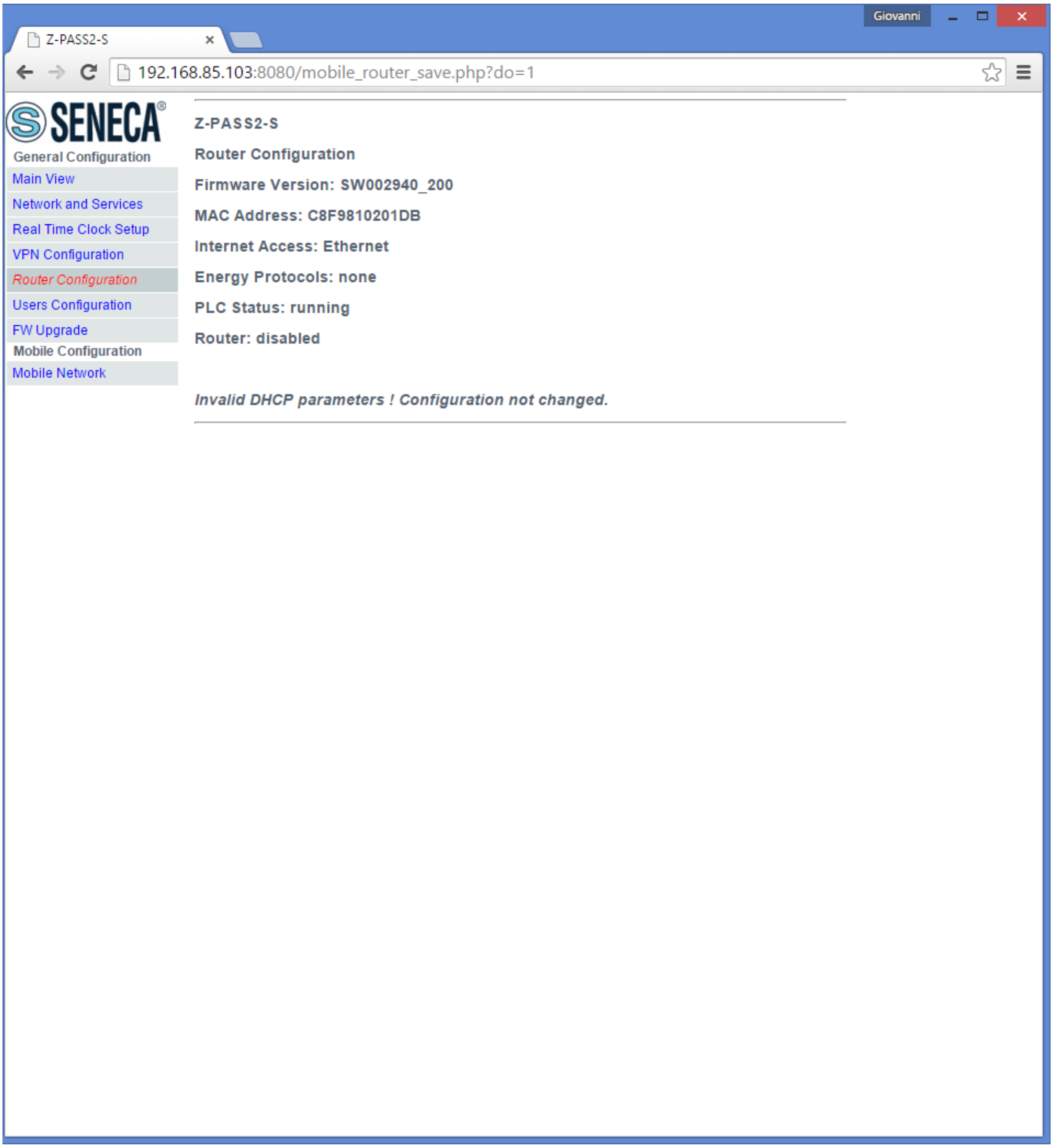
Energy Protocols: none

PLC Status: running

Router: disabled

Router Configuration changed (router not active).

If you try to enable the DHCP server functionality (DHCP Server Enable = ON), but the “DHCP First Address” and “DHCP Last Address” parameters define an address range that is not congruent with the Ethernet configuration (IP address and network mask), an error is given, as shown in the following figure:



Z-PASS2-S

Router Configuration

Firmware Version: SW002940_200

MAC Address: C8F9810201DB

Internet Access: Ethernet

Energy Protocols: none

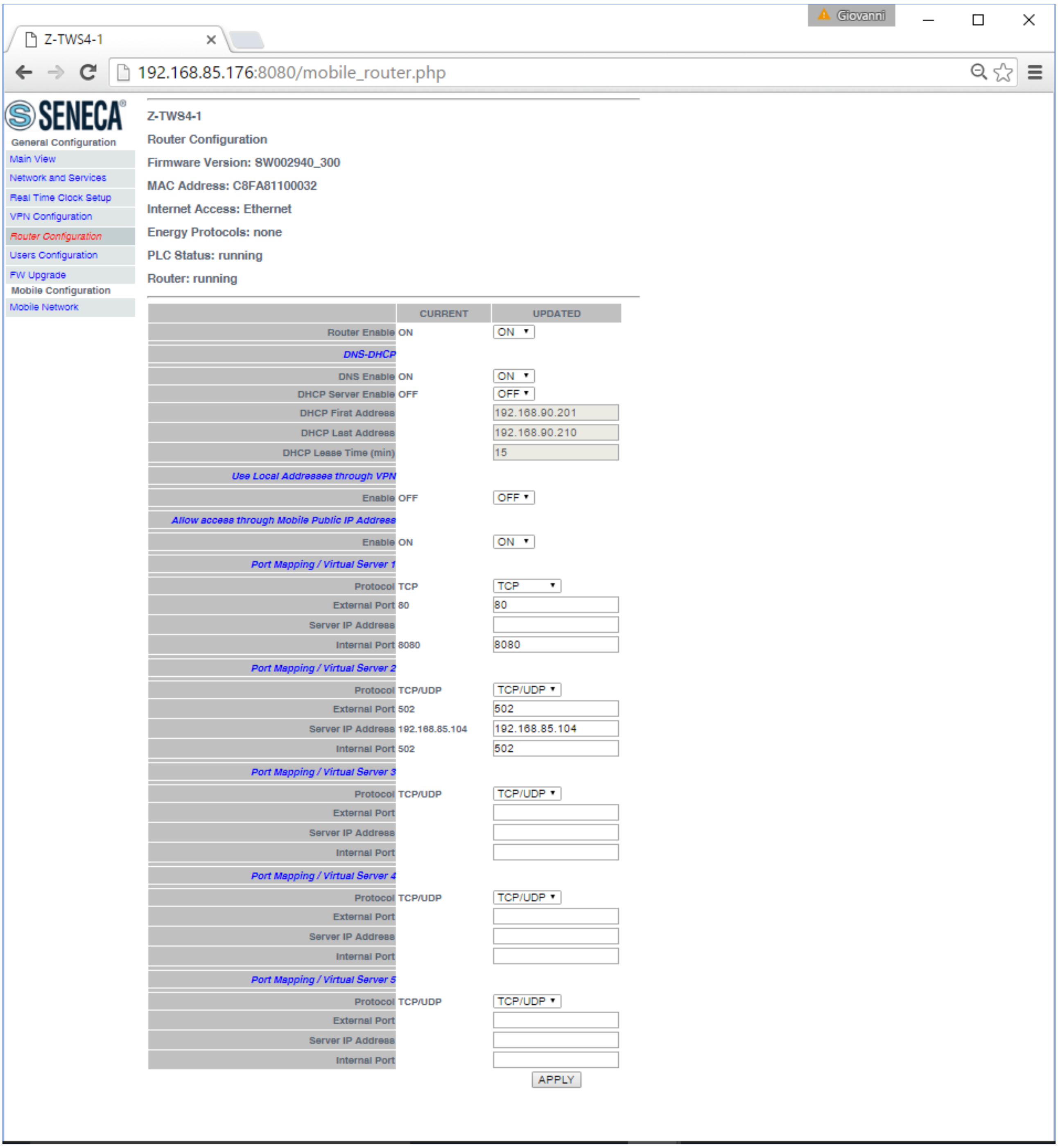
PLC Status: running

Router: disabled

Invalid DHCP parameters ! Configuration not changed.

As already told before, the Router configuration page lets you define up to 5 “Port Forwarding” rules or “Virtual Servers”.

An example is given in the following figure:



Z-TWS4-1

Router Configuration

Firmware Version: SW002940_300

MAC Address: C8FA81100032

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running

Router: running

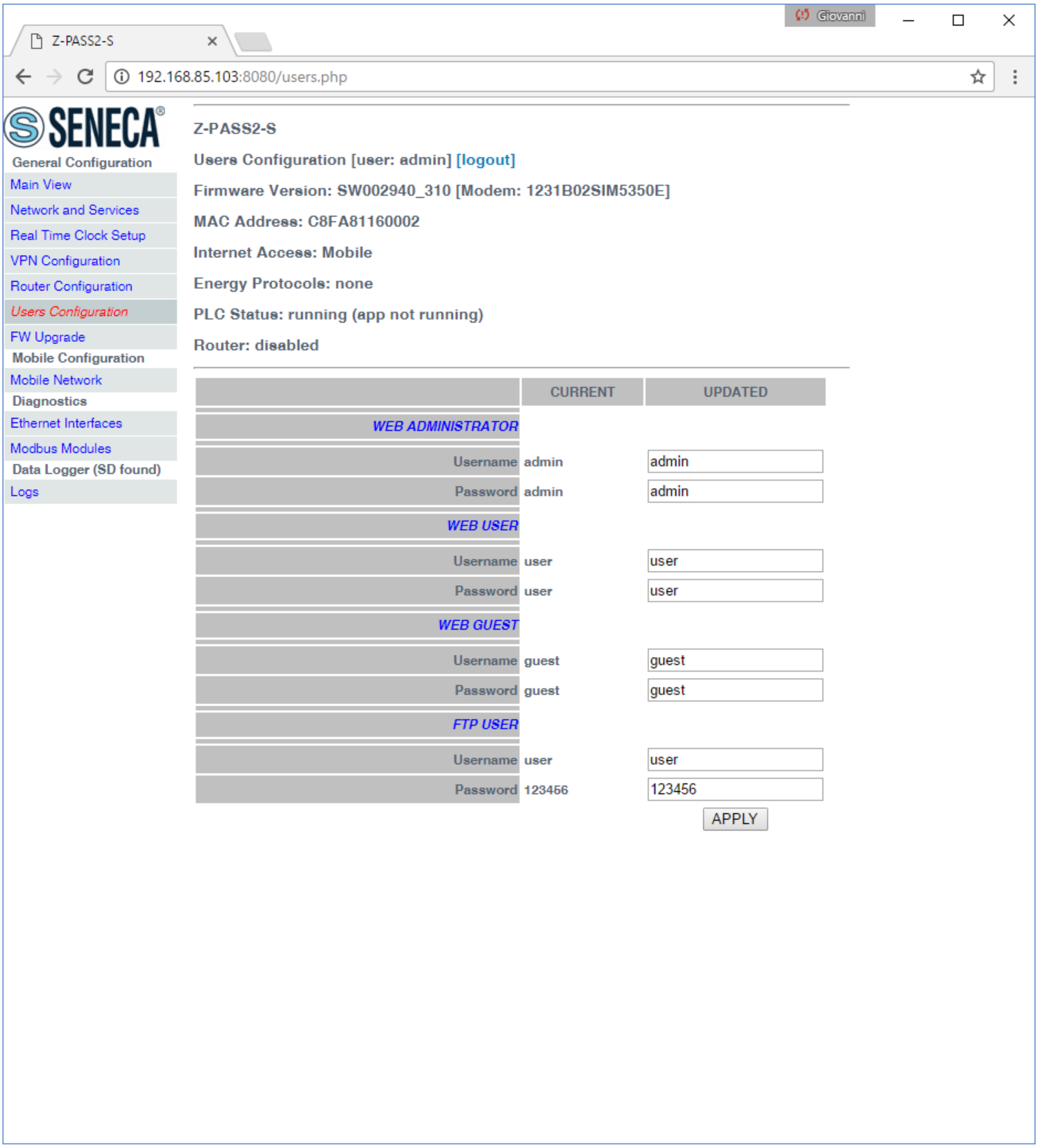
	CURRENT	UPDATED
Router Enable	ON	ON
DNS-DHCP		
DNS Enable	ON	ON
DHCP Server Enable	OFF	OFF
DHCP First Address		192.168.90.201
DHCP Last Address		192.168.90.210
DHCP Lease Time (min)		15
Use Local Addresses through VPN		
Enable	OFF	OFF
Allow access through Mobile Public IP Address		
Enable	ON	ON
Port Mapping / Virtual Server 1		
Protocol	TCP	TCP
External Port	80	80
Server IP Address		
Internal Port	8080	8080
Port Mapping / Virtual Server 2		
Protocol	TCP/UDP	TCP/UDP
External Port	502	502
Server IP Address	192.168.85.104	192.168.85.104
Internal Port	502	502
Port Mapping / Virtual Server 3		
Protocol	TCP/UDP	TCP/UDP
External Port		
Server IP Address		
Internal Port		
Port Mapping / Virtual Server 4		
Protocol	TCP/UDP	TCP/UDP
External Port		
Server IP Address		
Internal Port		
Port Mapping / Virtual Server 5		
Protocol	TCP/UDP	TCP/UDP
External Port		
Server IP Address		
Internal Port		

In this example, 2 rules have been set:

- the first rule tells the Device that any TCP packet received on the 80 (HTTP) port has to be forwarded to the 8080 port, leaving the original destination IP address unchanged; so, this rule lets you access the Device configuration web site on the standard HTTP port; however, by doing this, the access to the custom user's pages won't be possible anymore !
- the second rule tells the Device that any TCP or UDP packet received on the 502 port (which is often used for Modbus TCP protocol) shall be forwarded to the 192.168.85.104 IP address (which corresponds to another device) on the same (502) destination port.

16.1.6 Users Configuration

By clicking on the “Users Configuration” link, in the “General Configuration” menu, you come to the following page:



Z-PASS2-S

Users Configuration [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

	CURRENT	UPDATED
WEB ADMINISTRATOR		
Username	admin	admin
Password	admin	admin
WEB USER		
Username	user	user
Password	user	user
WEB GUEST		
Username	guest	guest
Password	guest	guest
FTP USER		
Username	user	user
Password	123456	123456

In this page, you can change the “Web Administrator”, “Web User”, “Web Guest” and “FTP User” credentials, as explained in the following table:

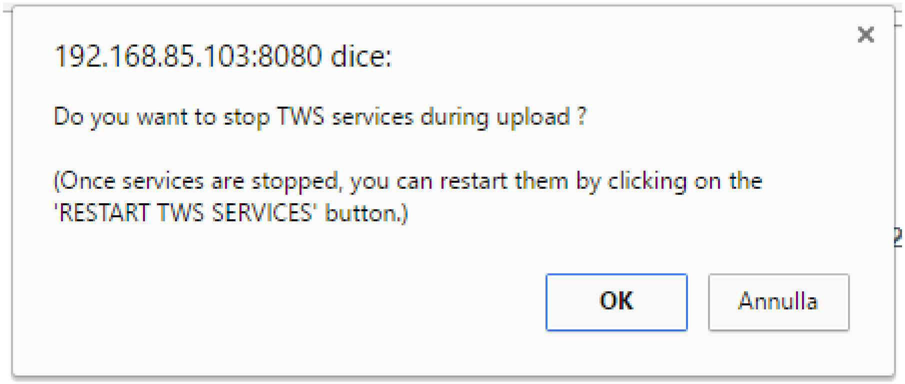
Field	Meaning	Default value
WEB ADMINISTRATOR/Username	Username to access the web configuration site (full access)	admin

WEB ADMINISTRATOR/Password	Password to access the web configuration site (full access)	admin
WEB USER/Username	Username to access the web configuration site (limited access) (see paragraph 16.2)	user
WEB USER/Password	Password to access the web configuration site (limited access) (see paragraph 16.2)	user
WEB GUEST/Username	Username to access the web configuration site, in "view-only mode" (see paragraph 16.3)	guest
WEB GUEST/Password	Password to access the web configuration site, in "view-only mode" (see paragraph 16.3)	guest
FTP USER/Username	Username to access the Device FTP/SFTP site (see chapter 7)	user
FTP USER/Password	Password to access the Device FTP/SFTP site (see chapter 7)	123456

Please note that, after changing the Web Administrator credentials, a new login will be required to access any page.

16.1.7 FW Upgrade

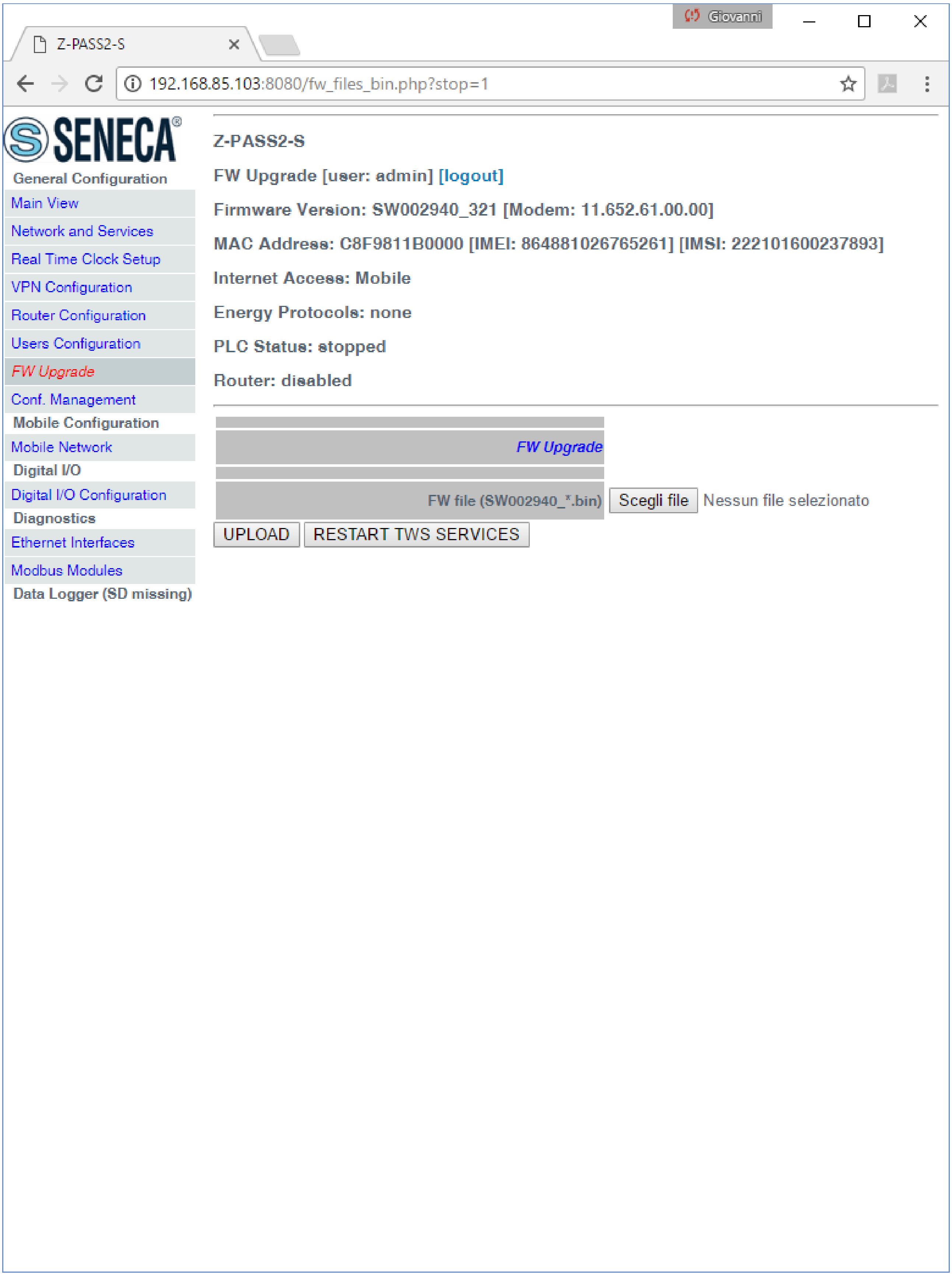
When clicking on the "FW Upgrade" link, in the "General Configuration" menu, the following pop-up is shown:


192.168.85.103:8080 dice:

Do you want to stop TWS services during upload ?

(Once services are stopped, you can restart them by clicking on the 'RESTART TWS SERVICES' button.)

If you click on the "OK" button, TWS Services (i.e. Soft-PLC) are stopped and you come to the "FW Upgrade" page, shown in the following figure.



Z-PASS2-S

FW Upgrade [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Mobile

Energy Protocols: none

PLC Status: stopped

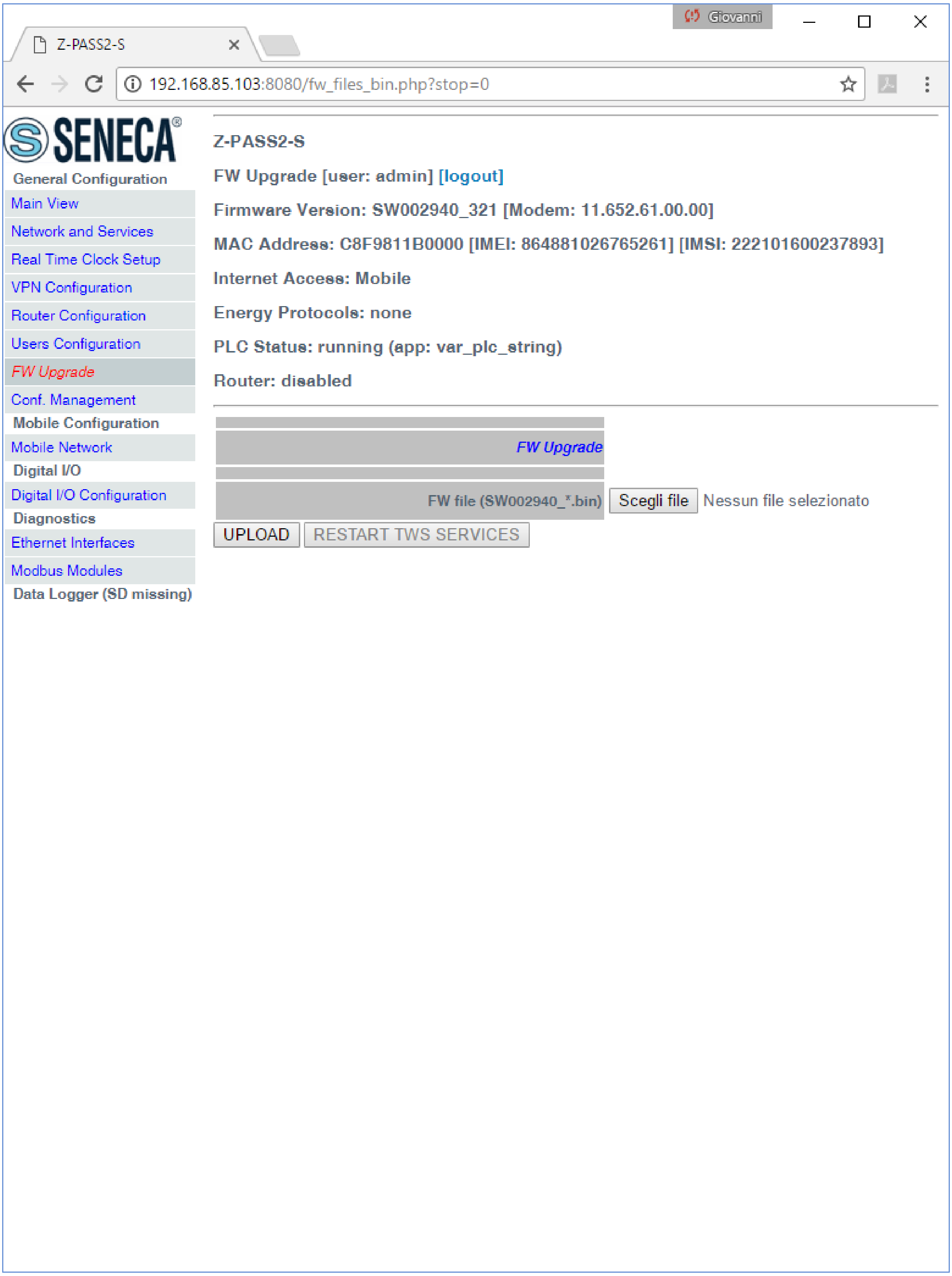
Router: disabled

FW Upgrade

FW file (SW002940_*.bin) Nessun file selezionato

Now, if you want to leave this page without performing the FW upgrade, the “RESTART TWS SERVICES” button lets you restart the TWS services which, otherwise, would remain in the “stopped” state.

Otherwise, if you click on the “Cancel” button of the pop-up, TWS Services are not stopped and you come to the same page where the “RESTART TWS SERVICES” is disabled.



Z-PASS2-S

FW Upgrade [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

FW Upgrade

FW file (SW002940_*.bin) Scegli file Nessun file selezionato

UPLOAD RESTART TWS SERVICES

So, it is up to the user to choose if Soft PLC shall be stopped or not, during FW Upload; on one side, stopping it is more safe and let the upload be completed in a shorter time; on the other side, there are situations in which PLC stop time shall be as short as possible.

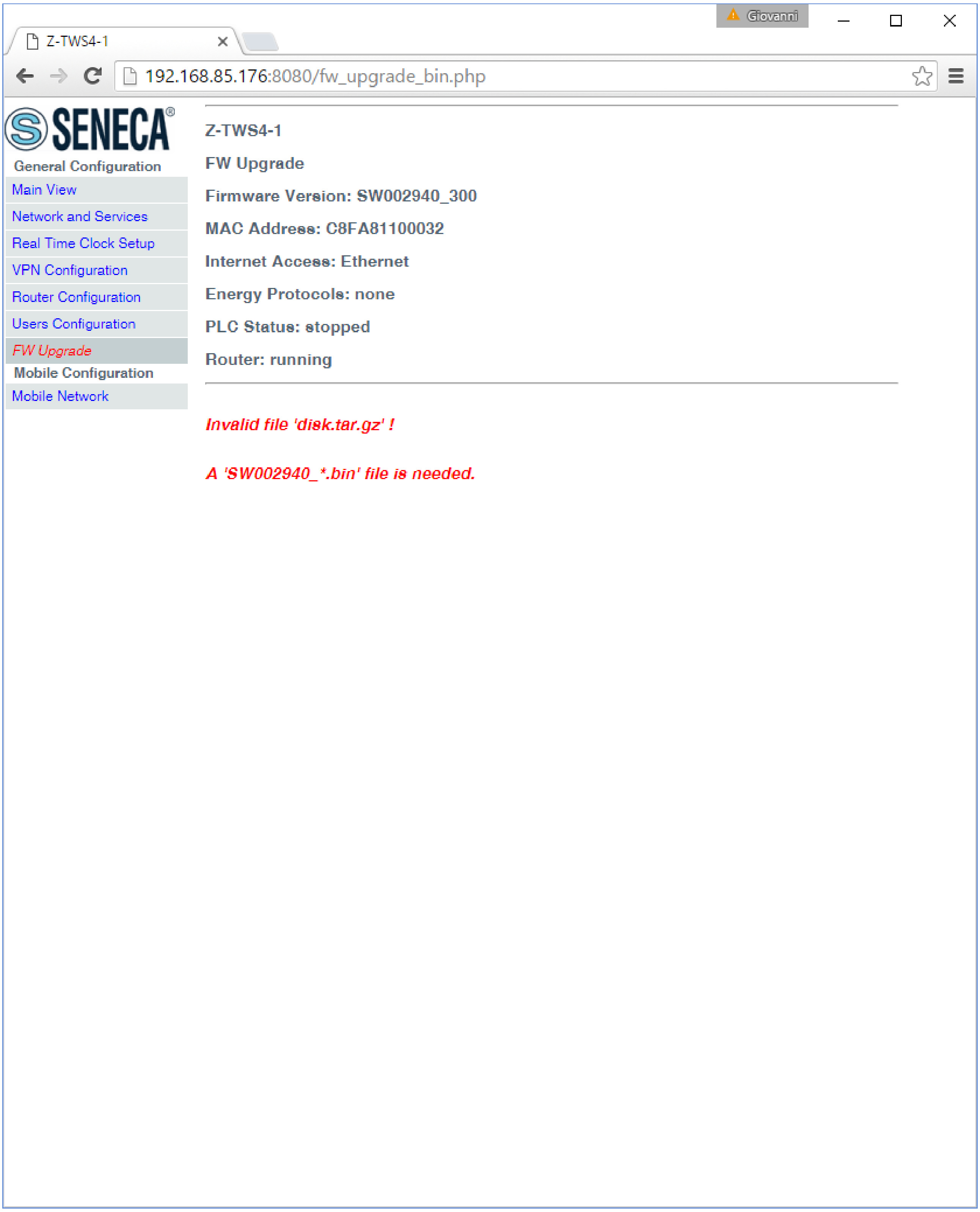
Since an erroneous use of the FW Upgrade functionality might compromise the proper Device operation, use this page only to apply upgrades provided by Seneca, with the support of Seneca personnel.

This page lets you browse your PC to select the file containing the FW, which shall have a name of the following type:

SW002940_xxx.bin[15]

If you select a file with a different name, an error will be shown at the end of the upload, as in the following figure.

[15] The FW file can be downloaded from Seneca website (see chapter 15).



Z-TWS4-1

FW Upgrade

Firmware Version: SW002940_300

MAC Address: C8FA81100032

Internet Access: Ethernet

Energy Protocols: none

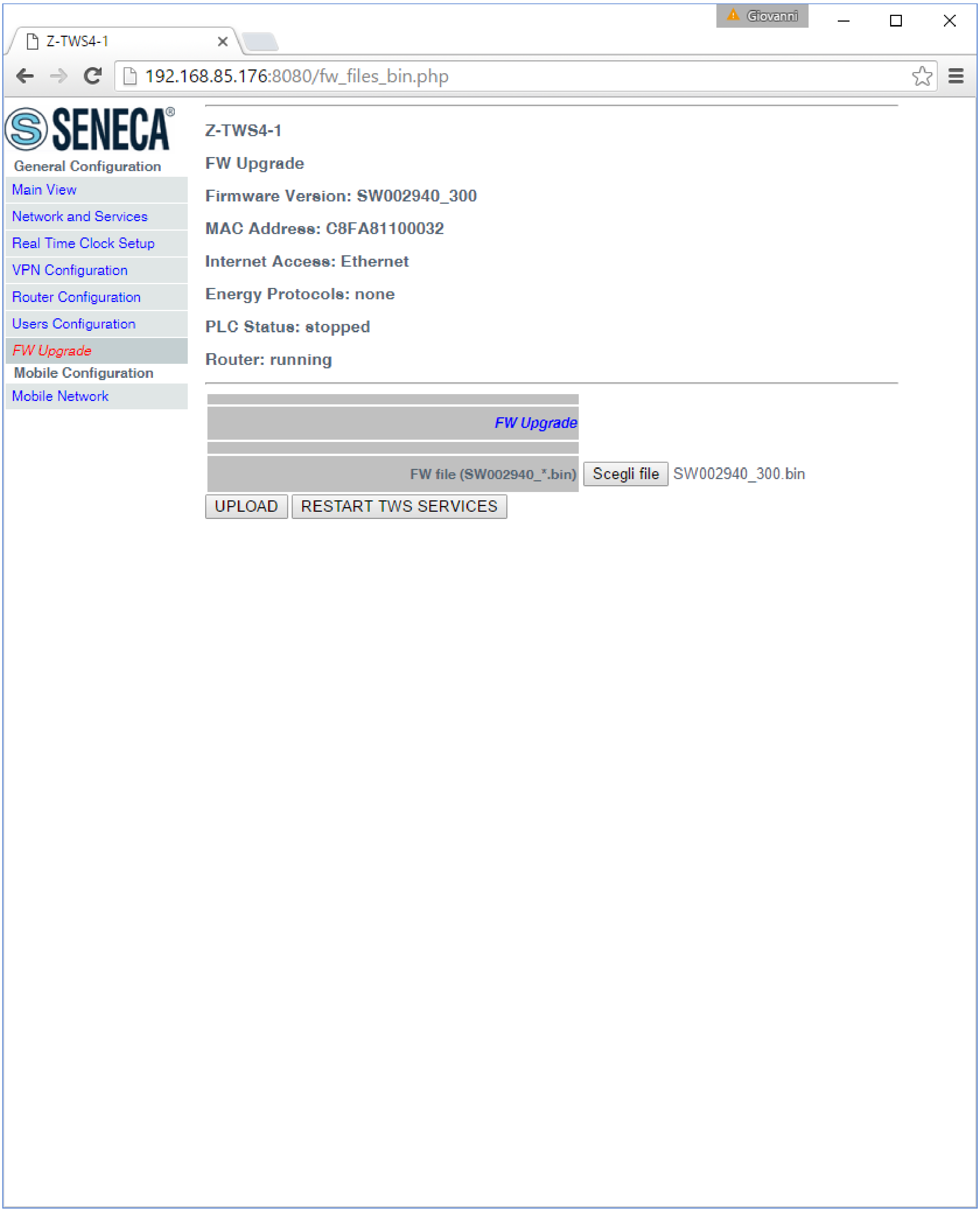
PLC Status: stopped

Router: running

Invalid file 'disk.tar.gz' !

A 'SW002940_*.bin' file is needed.

Once a file is selected, you can start the upload, by pressing the “UPLOAD” button.



Z-TWS4-1

FW Upgrade

Firmware Version: SW002940_300

MAC Address: C8FA81100032

Internet Access: Ethernet

Energy Protocols: none

PLC Status: stopped

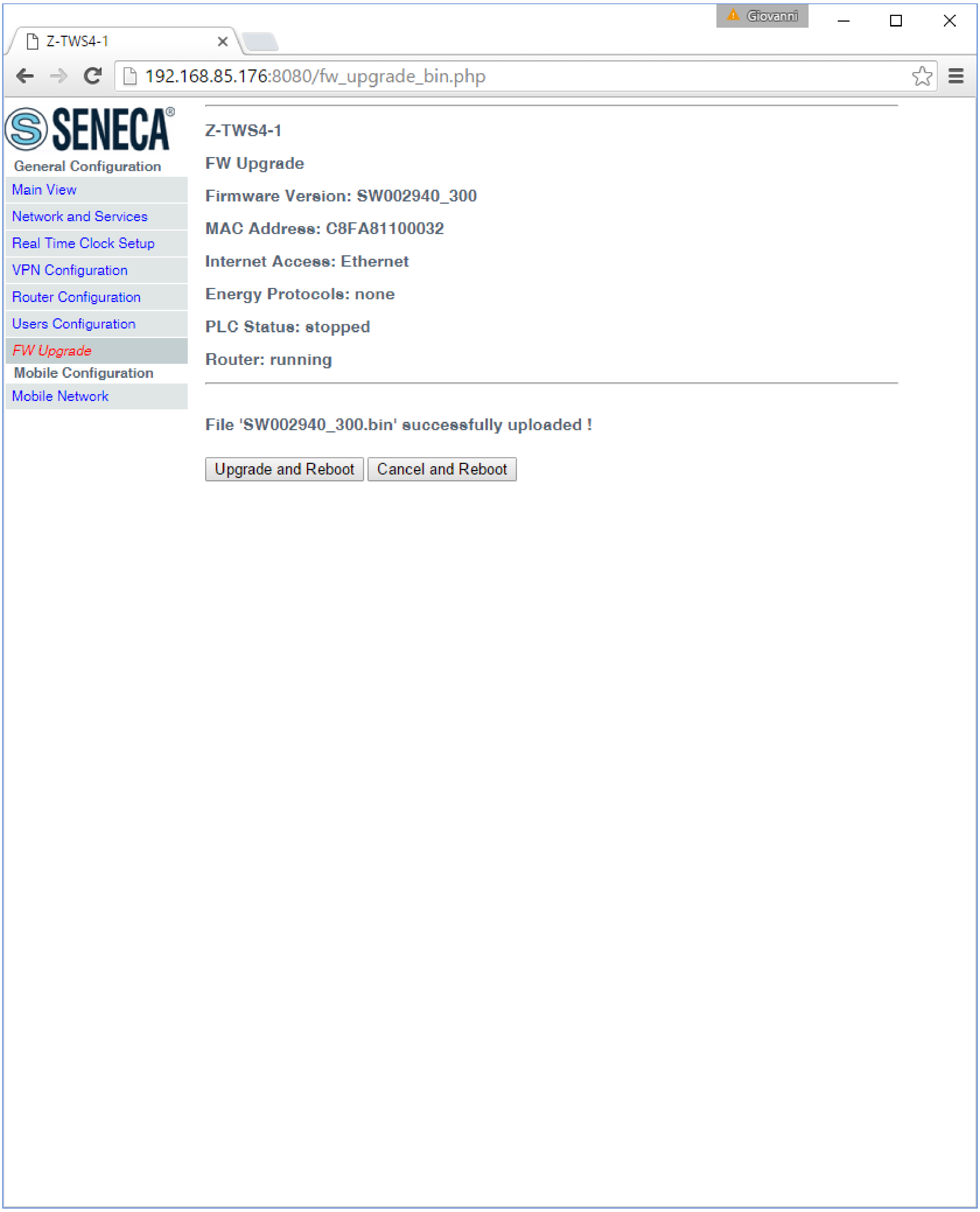
Router: running

FW Upgrade

FW file (SW002940_*.bin) Scegli file SW002940_300.bin

UPLOAD RESTART TWS SERVICES

Once the upload is successfully completed, the following page is shown:



Z-TWS4-1

FW Upgrade

Firmware Version: SW002940_300

MAC Address: C8FA81100032

Internet Access: Ethernet

Energy Protocols: none

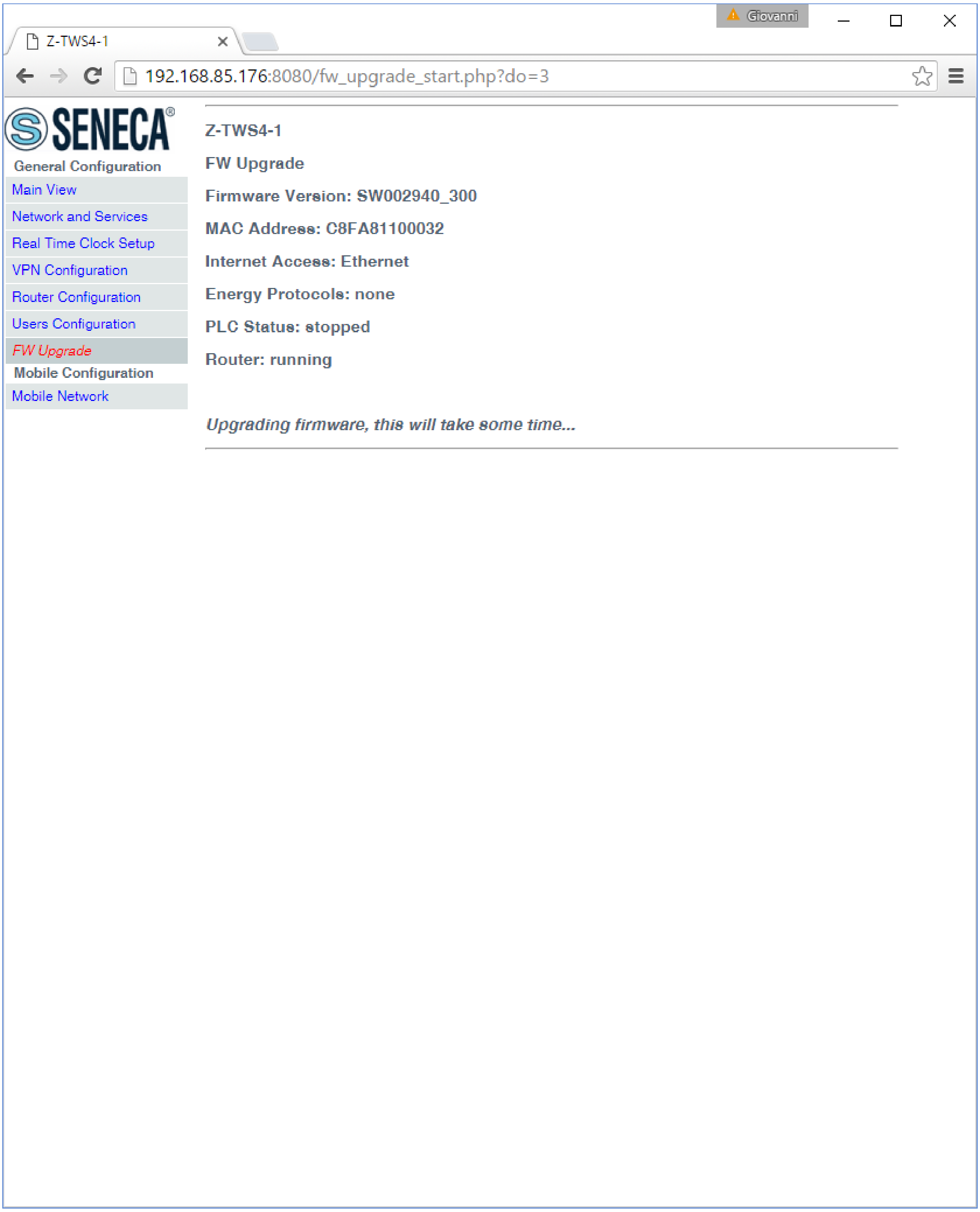
PLC Status: stopped

Router: running

File 'SW002940_300.bin' successfully uploaded !

In this page, you can:

- press the “Upgrade and Reboot” button: this will start the upgrade procedure, which takes some minutes to be completed; during this time, the Device MUST NOT be switched off; during the procedure, the Device will be rebooted several times; the end of the procedure is signalled by the “RUN” LED blinking.



Z-TWS4-1

FW Upgrade

Firmware Version: SW002940_300

MAC Address: C8FA81100032

Internet Access: Ethernet

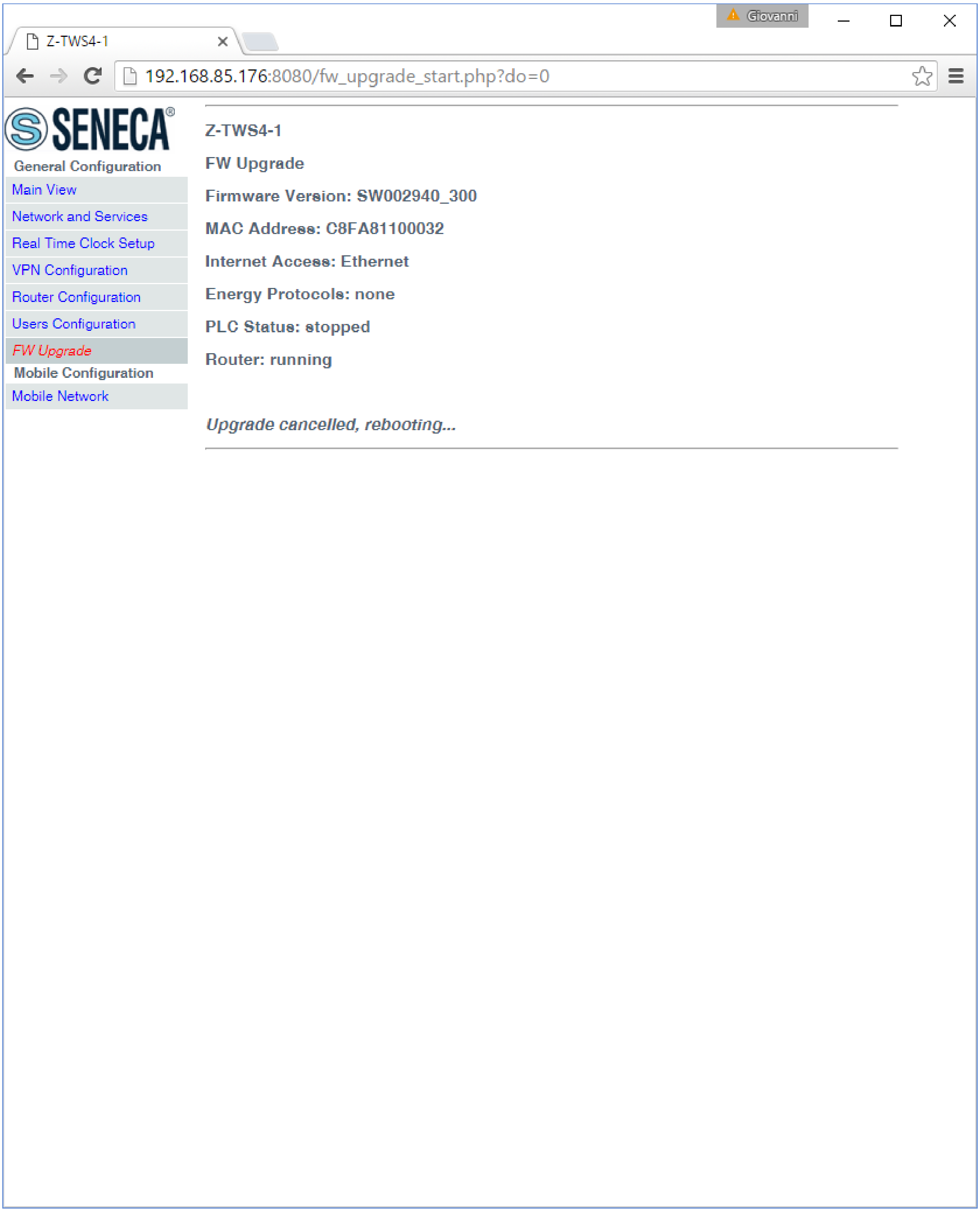
Energy Protocols: none

PLC Status: stopped

Router: running

Upgrading firmware, this will take some time...

- press the “Cancel and Reboot” button: this will delete the uploaded file on the Device and perform the reboot.



Z-TWS4-1

FW Upgrade

Firmware Version: SW002940_300

MAC Address: C8FA81100032

Internet Access: Ethernet

Energy Protocols: none

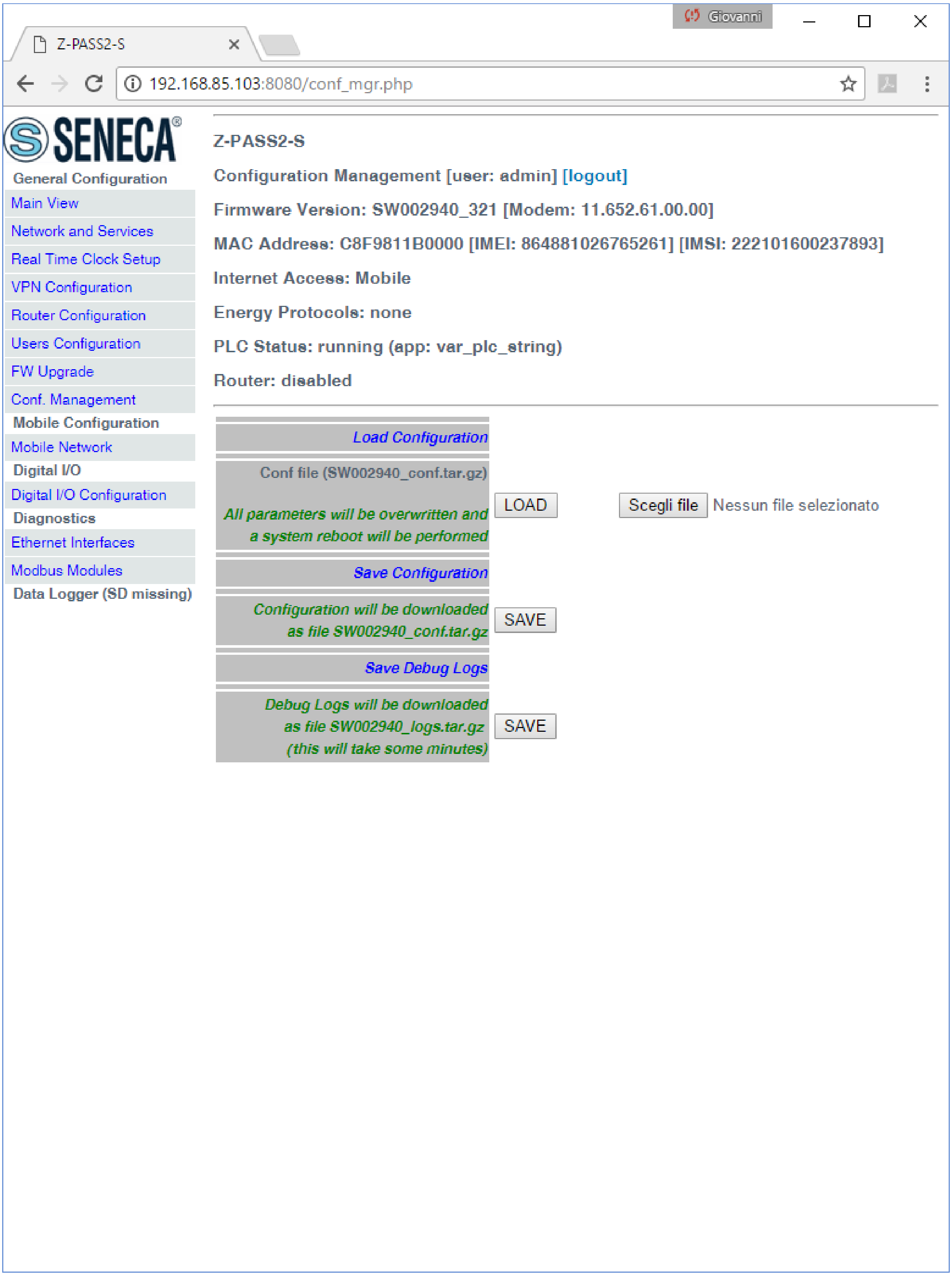
PLC Status: stopped

Router: running

Upgrade cancelled, rebooting...

16.1.8 Configuration Management

By clicking on the “Conf. Management” link, in the “General Configuration” menu, you come to the following page:



Z-PASS2-S

Configuration Management [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

Load Configuration

Conf file (SW002940_conf.tar.gz) LOAD Scegli file Nessun file selezionato

All parameters will be overwritten and a system reboot will be performed

Save Configuration

Configuration will be downloaded as file SW002940_conf.tar.gz SAVE

Save Debug Logs

Debug Logs will be downloaded as file SW002940_logs.tar.gz (this will take some minutes) SAVE

This page lets you save and load the whole Device configuration; this is very useful, for example, when you have to apply the same configuration to many devices.

The configuration archive file is named *SW002940_conf.tar.gz* and carries:

- files containing all configuration parameter values;
- files containing the PLC (Straton) application, if loaded on the Device;
- web user pages, if present.

The configuration archive, once created and downloaded by means of the “SAVE” button can be uploaded to the same or another device, in two ways:

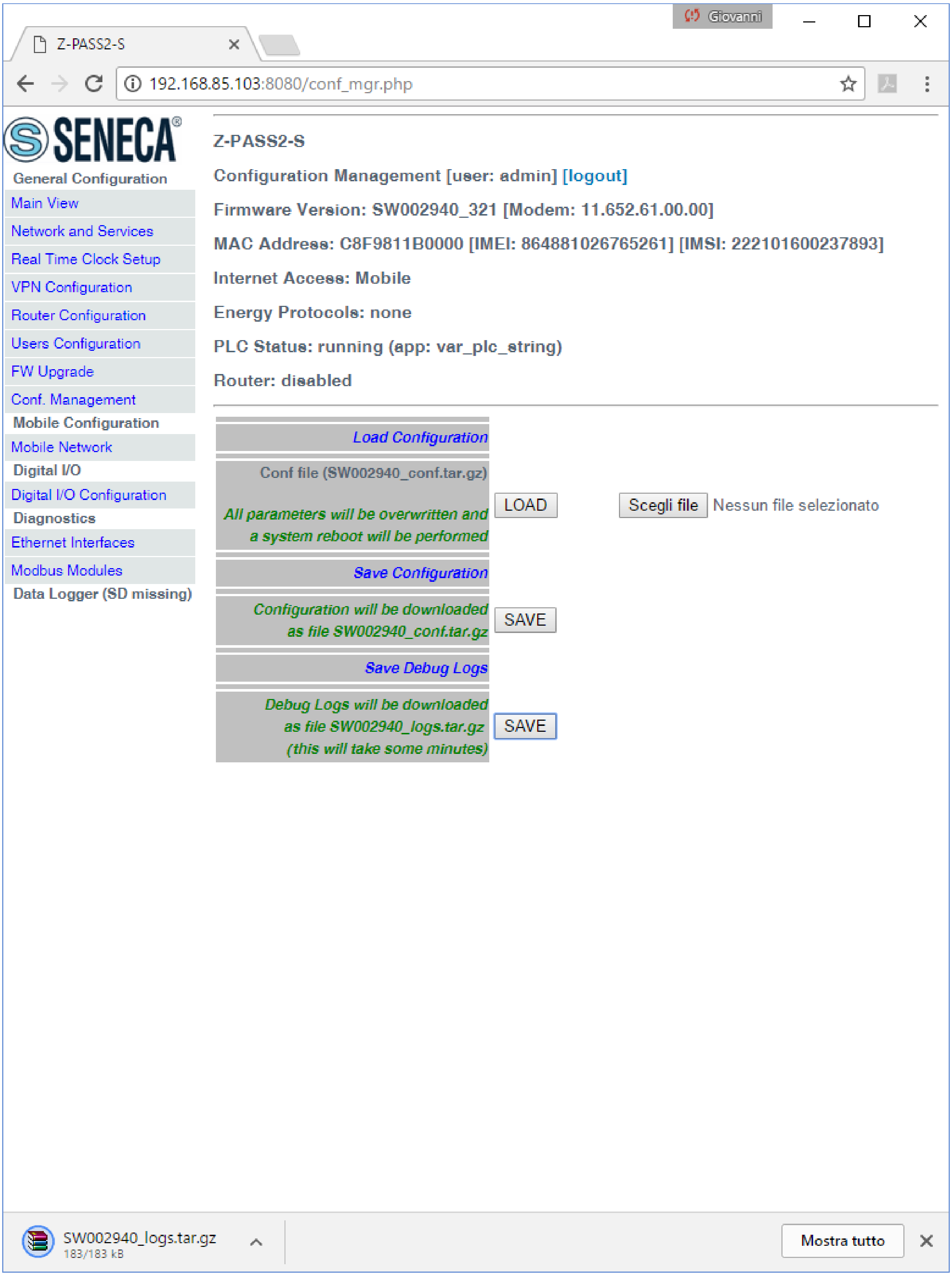
- by means of the “LOAD” button, in this page
- by means of a USB pen

The procedure to load the configuration into the Device by means of a USB pen is very simple:

- copy the *SW002940_conf.tar.gz* file into the root folder of the USB pen;
- insert the USB pen into the USB#1 port of the Device;
- switch off and on the Device;
- wait until you see the red “RUN” LED blinking;
- extract the USB pen;
- the configuration has been applied to the Device.

The only care when you carry the configuration archive from a device to another one is that the two devices should be the same product model; for example, it’s not safe to load the configuration archive saved on a Z-PASS2-S-R01 into a Z-PASS2-S.

Another useful feature available in this page is the one provided by the “Save Debug Logs / SAVE” button: when you click on it, a file named *SW002940_logs.tar.gz* is downloaded, which contains the debug logs stored by the CPU during its operation.



Z-PASS2-S

Configuration Management [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

Load Configuration

Conf file (SW002940_conf.tar.gz)

All parameters will be overwritten and a system reboot will be performed

Save Configuration

Configuration will be downloaded as file SW002940_conf.tar.gz

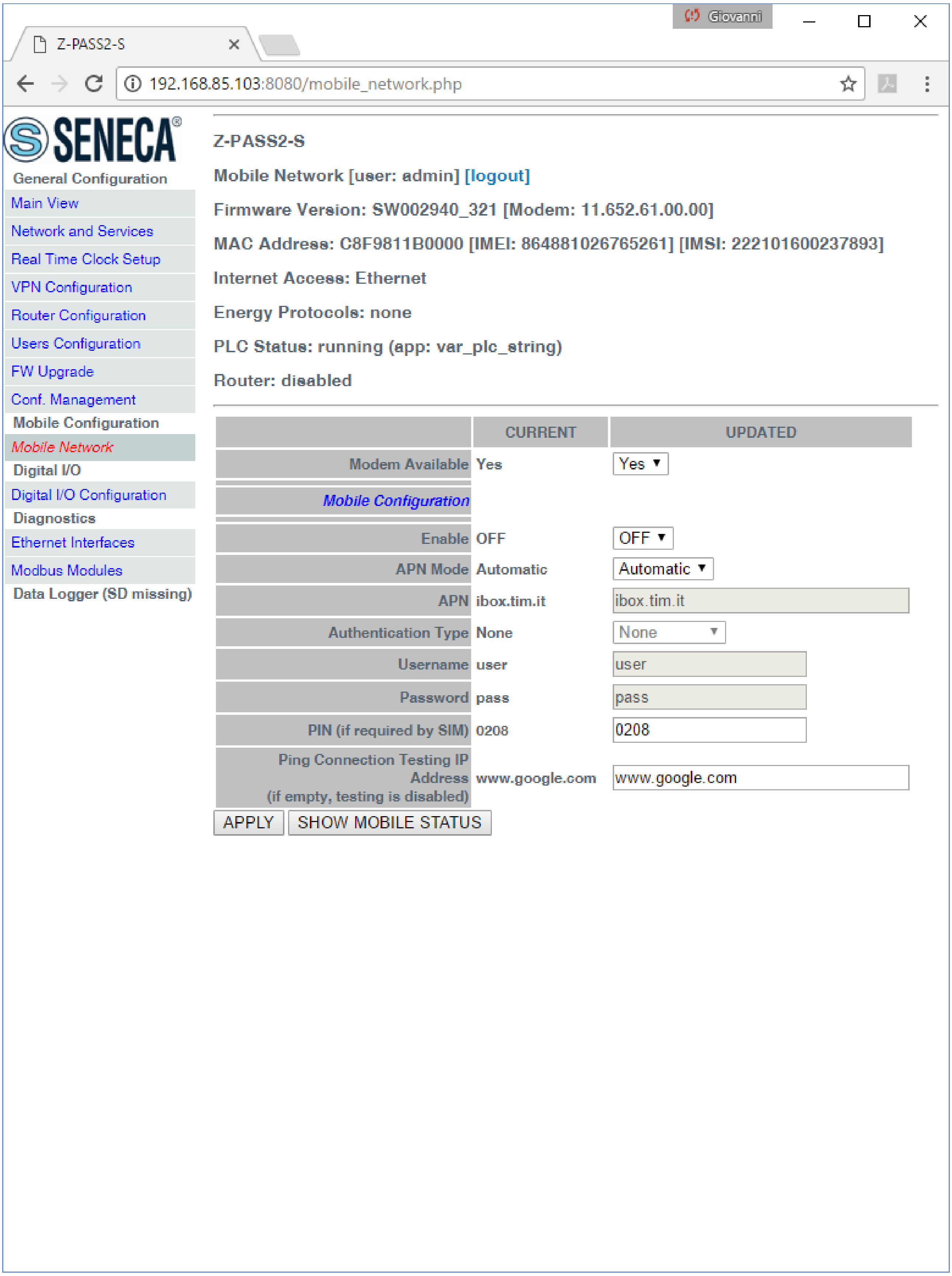
Save Debug Logs

Debug Logs will be downloaded as file SW002940_logs.tar.gz (this will take some minutes)

Please note that, to get detailed debug logs, the “DEBUG LOGS / Enable” parameter, in “Network and Services” page, shall be set to ON.

16.1.9 Mobile Network

By clicking on the “Mobile Network” link, in the “Mobile Configuration” menu, you come to the following page:



Z-PASS2-S

Mobile Network [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

	CURRENT	UPDATED
Modem Available	Yes	Yes ▾
Mobile Configuration		
Enable	OFF	OFF ▾
APN Mode	Automatic	Automatic ▾
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None ▾
Username	user	user
Password	pass	pass
PIN (if required by SIM)	0208	0208
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

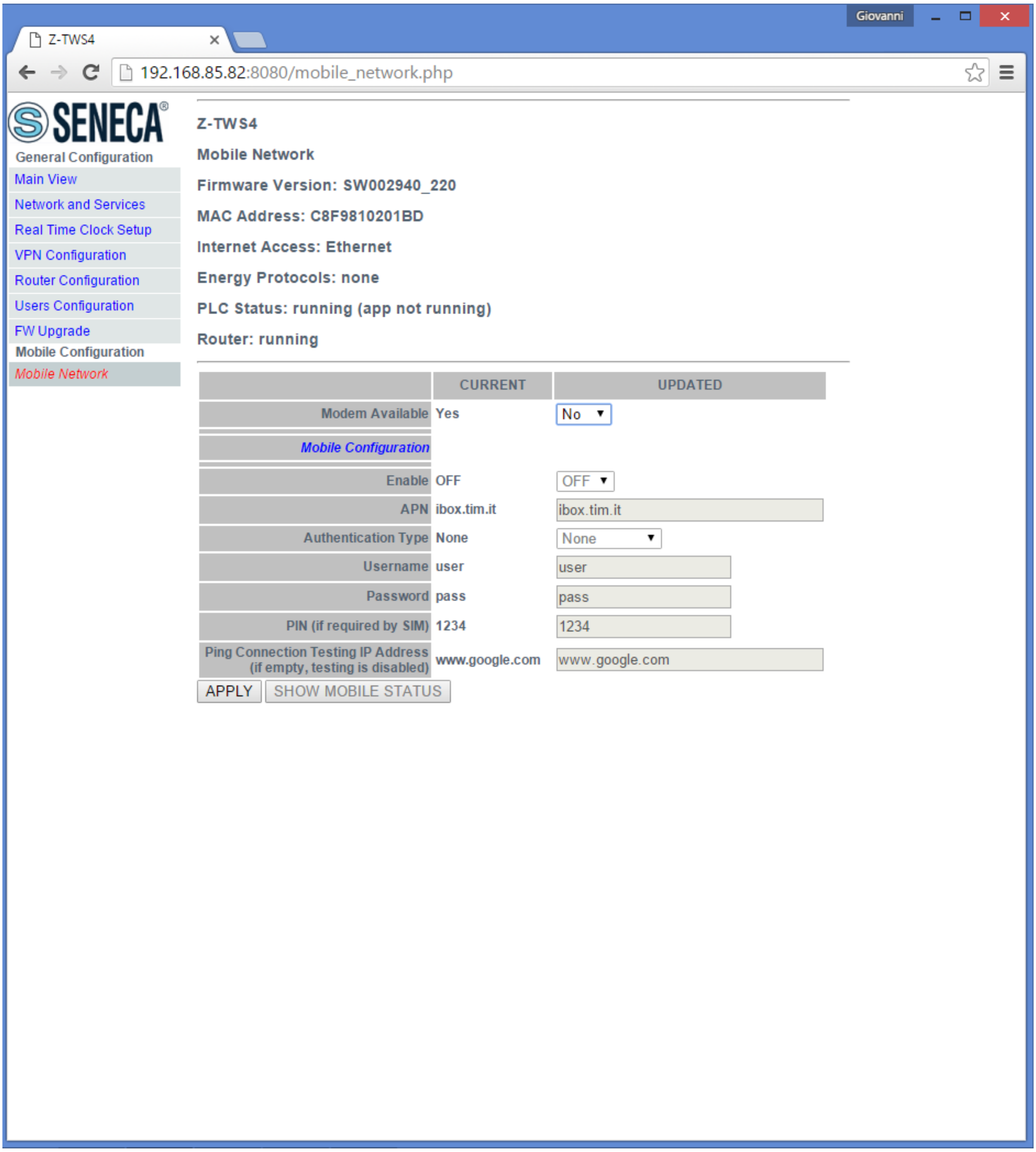
In this page, you can change the parameters related to the Mobile Network, as listed in the following table:

Field	Meaning	Default value
Modem Available	This parameter shall be set according to modem availability; possible values are: ”Yes”/“No” for Z-TWS4 and S6001-RTU; only “Yes” for Z-PASS2-S. When value is “No”, all other parameters in the page are disabled	No (Z-TWS4) Yes (Z-PASS2-S/S6001-RTU)
Enable	Flag to enable/disable the Mobile Network connectivity	OFF
APN Mode	This parameter tells if the APN and related parameters are automatically retrieved (based on SIM IMSI) (Mode=Automatic) or the values given in this page are used. When APN Mode = Automatic, APN, Authentication Type, Username and Password parameters are disabled.	Automatic
APN	Access Point Name, as given by the Mobile Network Operator	ibox.tim.it
Authentication Type	Type of authentication required; possible values are: “None”, “CHAP/PAP”, “CHAP only”, “PAP only”	None
Username	Username needed for UMTS/GPRS connectivity, as given by the Mobile Network Operator; it may be empty, if “Authentication Type” parameter is “None”	user
Password	Password needed for UMTS/GPRS connectivity, as given by the Mobile Network Operator; it may be empty, if “Authentication Type” parameter is “None”	pass
PIN (if required by SIM)	PIN needed to unlock the SIM card, if PIN locking functionality is enabled on it[16]	1234
Ping Connection Testing IP Address (if empty, testing is disabled)	FQDN or IP address used to periodically check, by means of “ping” packets, if the mobile connection is actually working; if the field is lefty empty, the check is not performed.	www.google.com

[16] Please note that the procedure to enable/disable the PIN locking functionality on the SIM is not performed by the Device.

	It is important to note that the FQDN or IP address specified must be reachable from the Device mobile network, otherwise the Device will detect that the mobile connection is not working and will drop it.	

If “Modem Available” parameter is set to “No”, all other parameters in the page are disabled, as shown in the following figure:



Z-TWS4

Mobile Network

Firmware Version: SW002940_220

MAC Address: C8F9810201BD

Internet Access: Ethernet

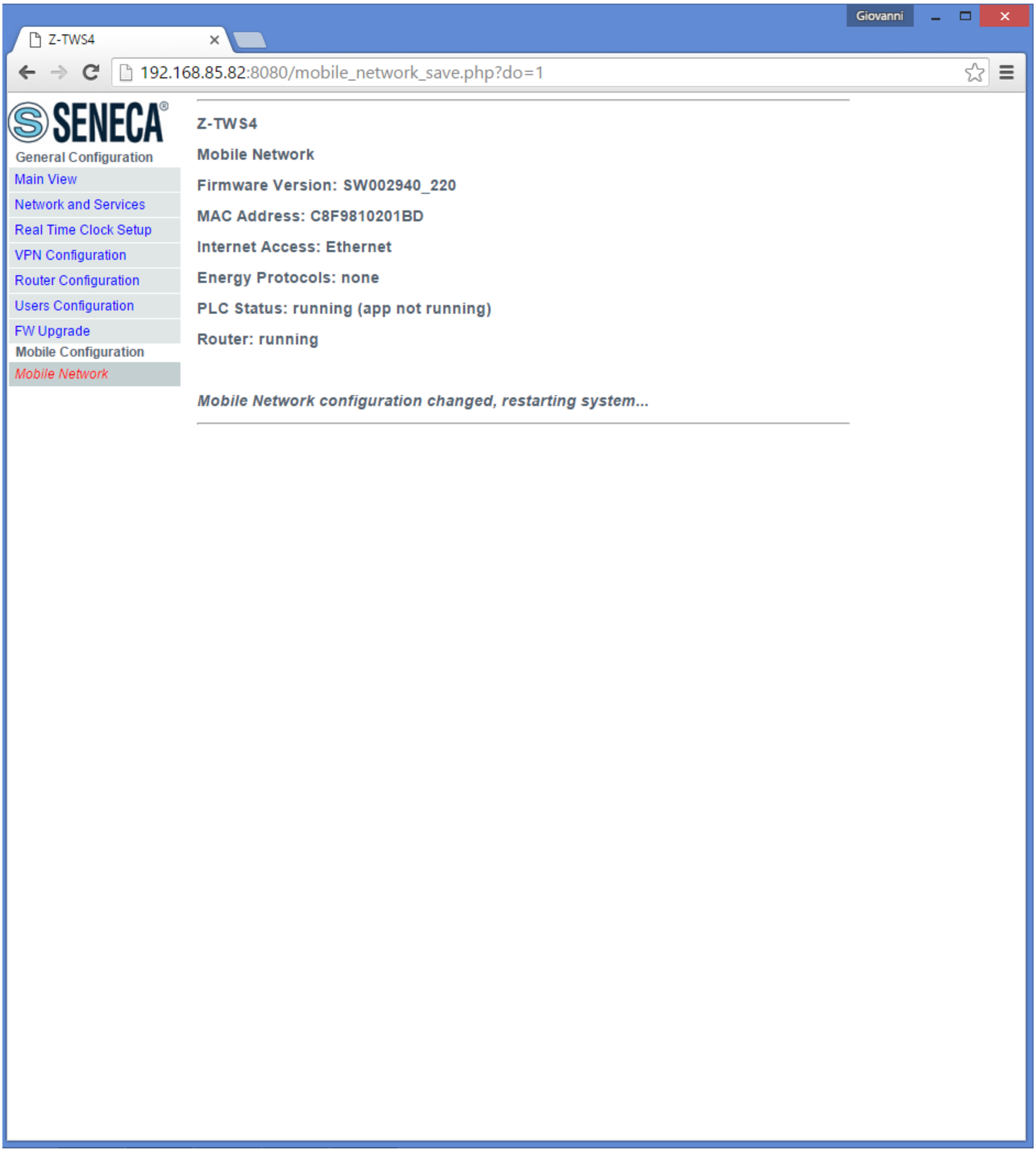
Energy Protocols: none

PLC Status: running (app not running)

Router: running

	CURRENT	UPDATED
Modem Available	Yes	No
Mobile Configuration		
Enable	OFF	OFF
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None
Username	user	user
Password	pass	pass
PIN (if required by SIM)	1234	1234
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

If “Modem Available” parameter value is changed, when clicking on the “APPLY” button the system is restarted, as shown in the following figure:



Z-TWS4

Mobile Network

Firmware Version: SW002940_220

MAC Address: C8F9810201BD

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running (app not running)

Router: running

Mobile Network configuration changed, restarting system...

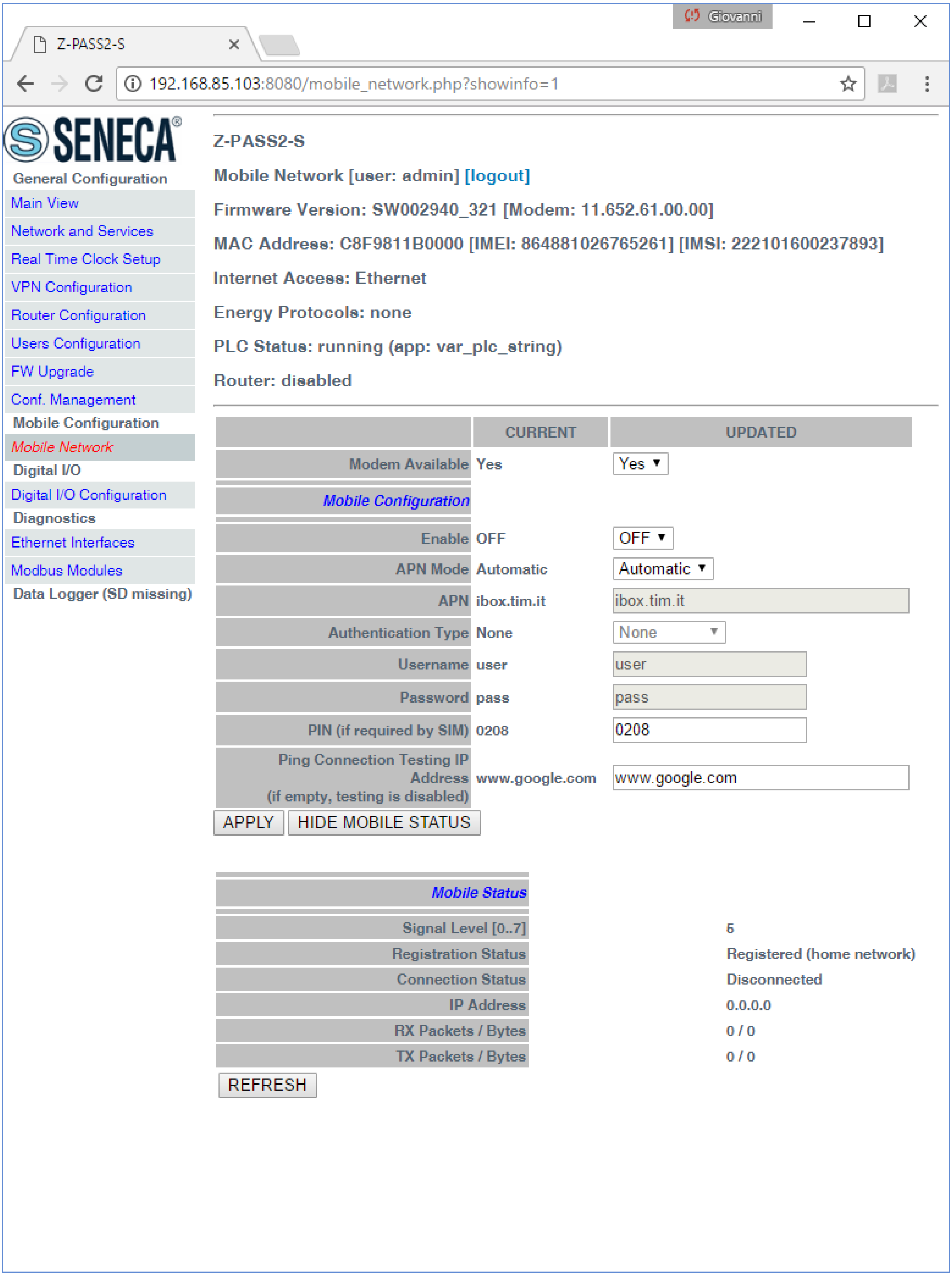
The “Modem Available” parameter value should be changed only in the following situations:

- for Z-TWS4, when an external Z-MODEM-3G modem is connected, the value shall be set to “Yes” and, conversely, when the modem is disconnected, the value shall be set back to “No”

In the “Mobile Network” page, when you click on the “SHOW MOBILE STATUS” button, a new section appears, named “Mobile Status”, showing:

- the radio “Signal Level”, in the range [0..7]
- the GSM “Registration Status”
- the Mobile Network “Connection Status” (i.e.: “Disconnected” or “Connected”)
- the IP address assigned to the Mobile Network interface when connected, the “dummy” IP address “0.0.0.0” when disconnected
- the number of packets/bytes received from the Mobile Network interface, when connected; “0/0” when disconnected
- the number of packets/bytes sent to the Mobile Network interface, when connected; “0/0” when disconnected

as shown in the following couple of figures:



Z-PASS2-S

Mobile Network [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Ethernet

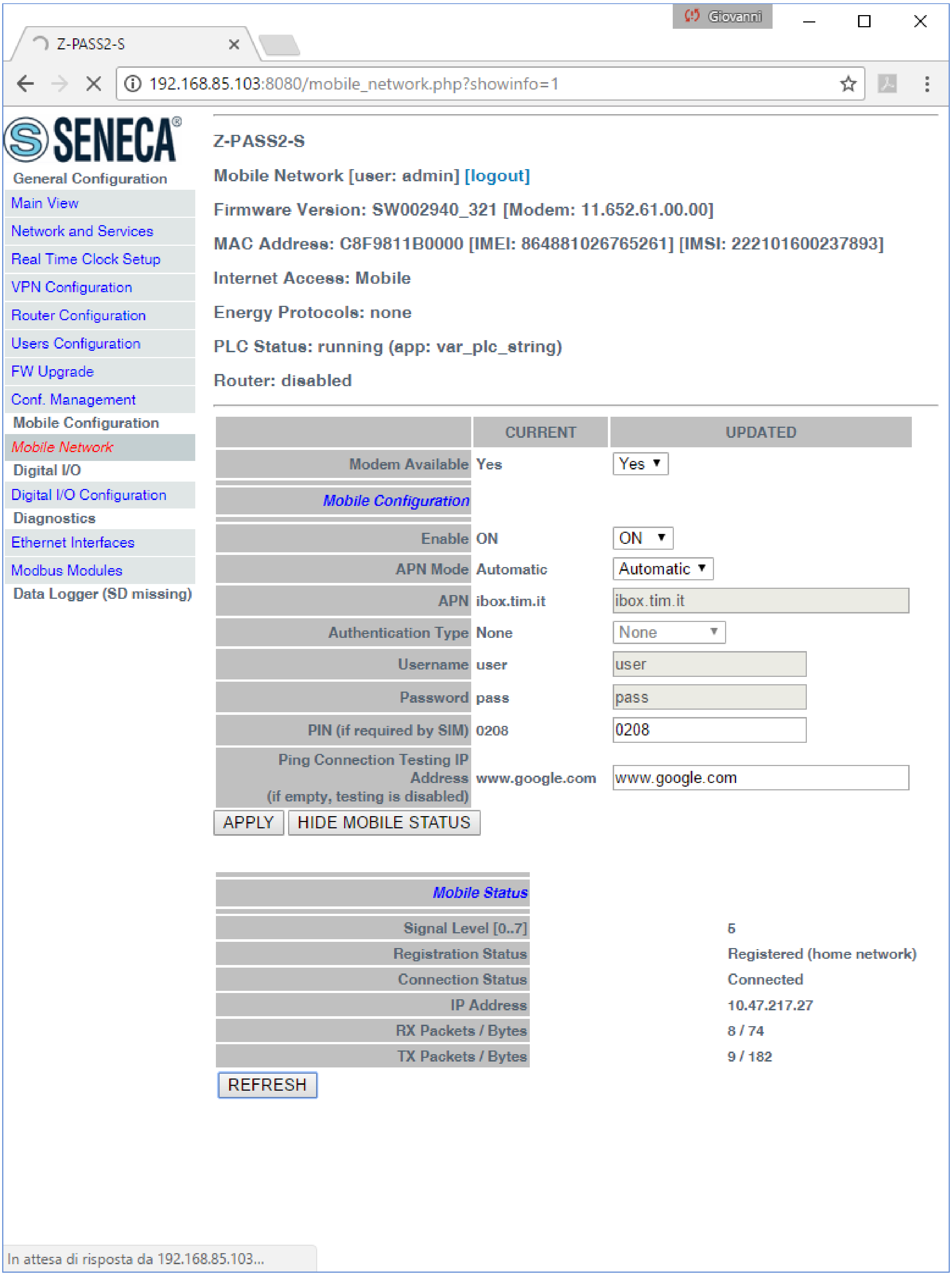
Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

	CURRENT	UPDATED
Modem Available	Yes	Yes ▼
Mobile Configuration		
Enable	OFF	OFF ▼
APN Mode	Automatic	Automatic ▼
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None ▼
Username	user	user
Password	pass	pass
PIN (if required by SIM)	0208	0208
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

Mobile Status	
Signal Level [0..7]	5
Registration Status	Registered (home network)
Connection Status	Disconnected
IP Address	0.0.0.0
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0



Z-PASS2-S

Mobile Network [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

	CURRENT	UPDATED
Modem Available	Yes	Yes ▾
Mobile Configuration		
Enable	ON	ON ▾
APN Mode	Automatic	Automatic ▾
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None ▾
Username	user	user
Password	pass	pass
PIN (if required by SIM)	0208	0208
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

Mobile Status	
Signal Level [0..7]	5
Registration Status	Registered (home network)
Connection Status	Connected
IP Address	10.47.217.27
RX Packets / Bytes	8 / 74
TX Packets / Bytes	9 / 182

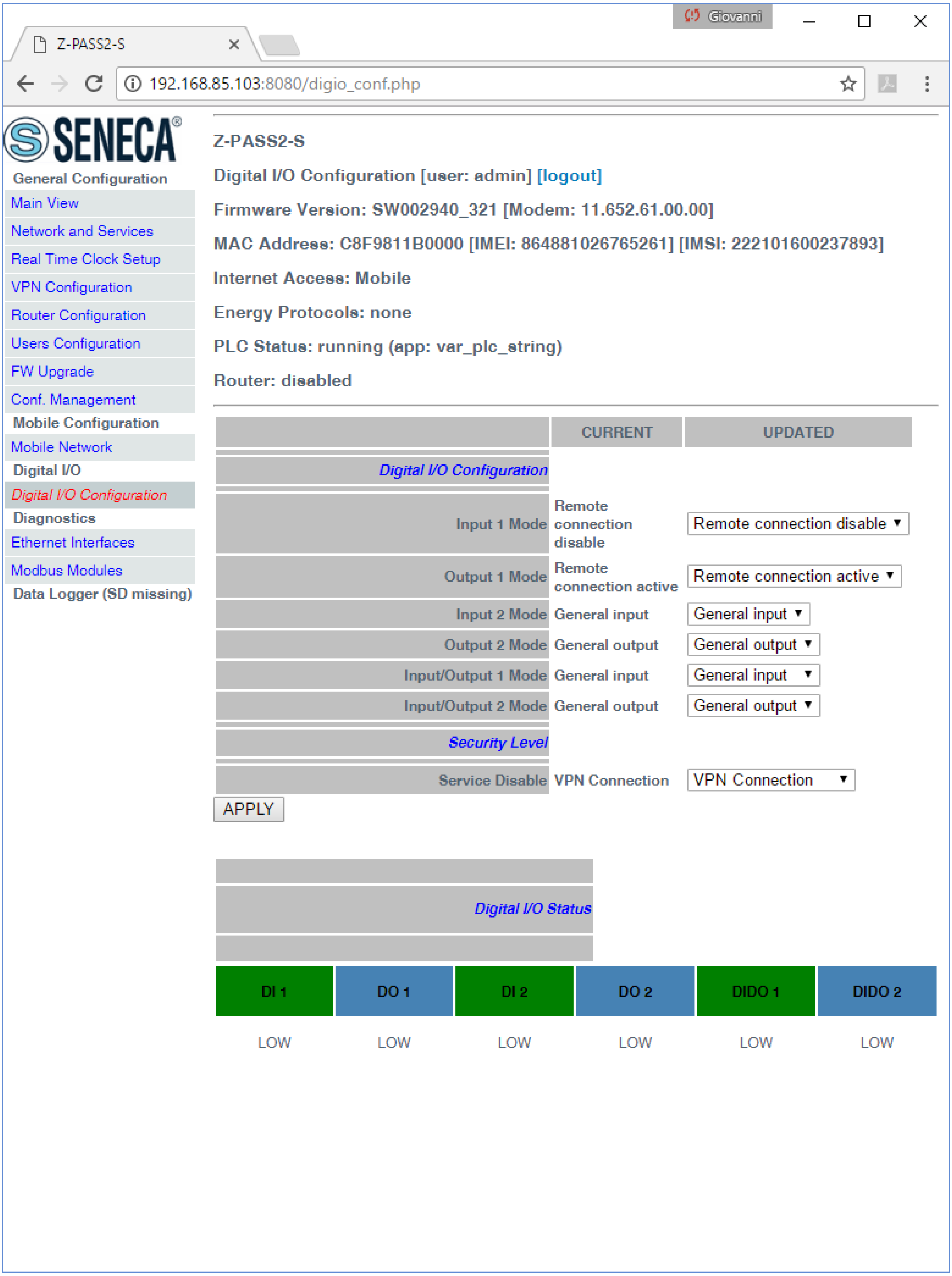
You can refresh the Mobile Network status, by clicking on the “REFRESH” button.

Finally, you can hide the "Mobile Status" section, by clicking on the "HIDE MOBILE STATUS" button.

16.1.10 Digital I/O Configuration

By clicking on the "Digital I/O Configuration" link, in the "Digital I/O" menu, you come to the following page[17]:

[17] This page is available only for Z-TWS4-R02 and Z-PASS2-S-R02 products.



Z-PASS2-S

Digital I/O Configuration [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

	CURRENT	UPDATED
Digital I/O Configuration		
Input 1 Mode	Remote connection disable	Remote connection disable ▼
Output 1 Mode	Remote connection active	Remote connection active ▼
Input 2 Mode	General input	General input ▼
Output 2 Mode	General output	General output ▼
Input/Output 1 Mode	General input	General input ▼
Input/Output 2 Mode	General output	General output ▼
Security Level		
Service Disable	VPN Connection	VPN Connection ▼

Digital I/O Status

DI 1	DO 1	DI 2	DO 2	DIDO 1	DIDO 2
LOW	LOW	LOW	LOW	LOW	LOW

In this page, you can configure the operating modes of the Digital I/Os and the security level applied by the "Remote Access Disable" feature (see chapter 13).

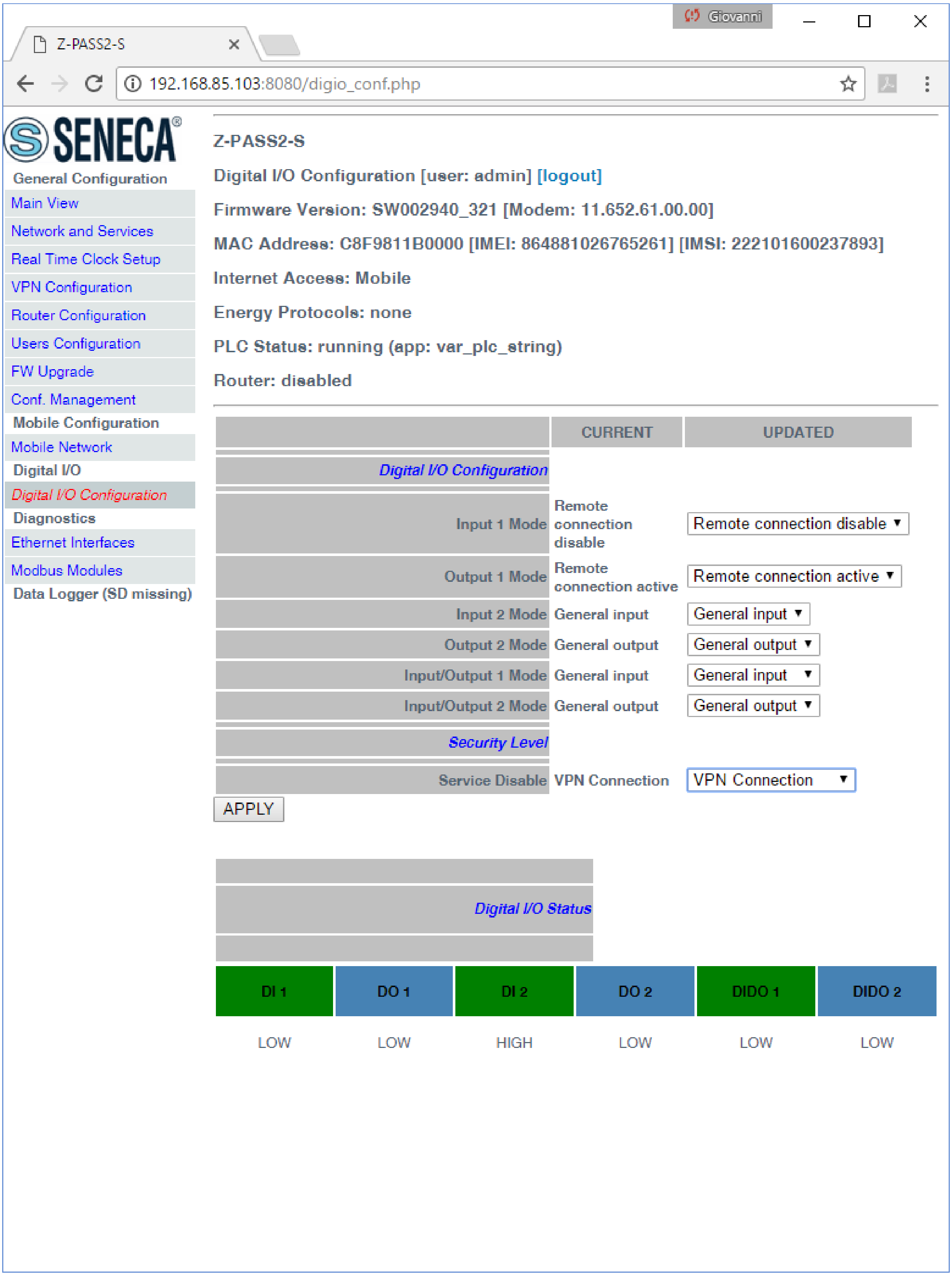
Field	Meaning	Default value
Input 1 Mode	This parameter represents the operating mode of the Digital Input 1 (DI 1). Since this is the digital input used for "Remote Access Disable" feature, its value ("Remote connection disable") cannot be changed.	Remote connection disable
Output 1 Mode	This parameter represents the operating mode of the Digital Output 1 (DO 1). Since this is the digital output used to monitor remote access, its value ("Remote connection active") cannot be changed.	Remote connection active
Input 2 Mode	This parameter represents the operating mode of the Digital Input 2 (DI 2). Possible modes are: "General input" | "Local alarm"[18].	General input
Output 2 Mode	This parameter represents the operating mode of the Digital Output 2 (DO 2). Possible modes are: "General output" | "Remote toggle"[19].	General output
Input/Output 1 Mode	This parameter represents the operating mode of the Digital Input/Output 1 (first configurable digital I/O) (DIDO 1). Possible modes are: "General input" | "General output".	General input
Input/Output 2 Mode	This parameter represents the operating mode of the Digital Input/Output 2 (second configurable digital I/O) (DIDO 2). Possible modes are: "General input" | "General output".	General output
Service Disable	This parameter determines which access services are disabled when "Remote Connection Disable" digital input is HIGH. Possible values are: "None" | "VPN	VPN Connection

[18] "Local alarm" function is to be defined yet.

[19] "Remote toggle" function is to be defined yet.

	Connection” | “VPN Service” | “Internet Connection”. See chapter 13, for a detailed description of these values.	

The “Digital I/O Status” section of the page gives the current status values (“LOW”/”HIGH”) for each of the six available digital I/Os.



Z-PASS2-S

Digital I/O Configuration [user: admin] [logout]

Firmware Version: SW002940_321 [Modem: 11.652.61.00.00]

MAC Address: C8F9811B0000 [IMEI: 864881026765261] [IMSI: 222101600237893]

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app: var_plc_string)

Router: disabled

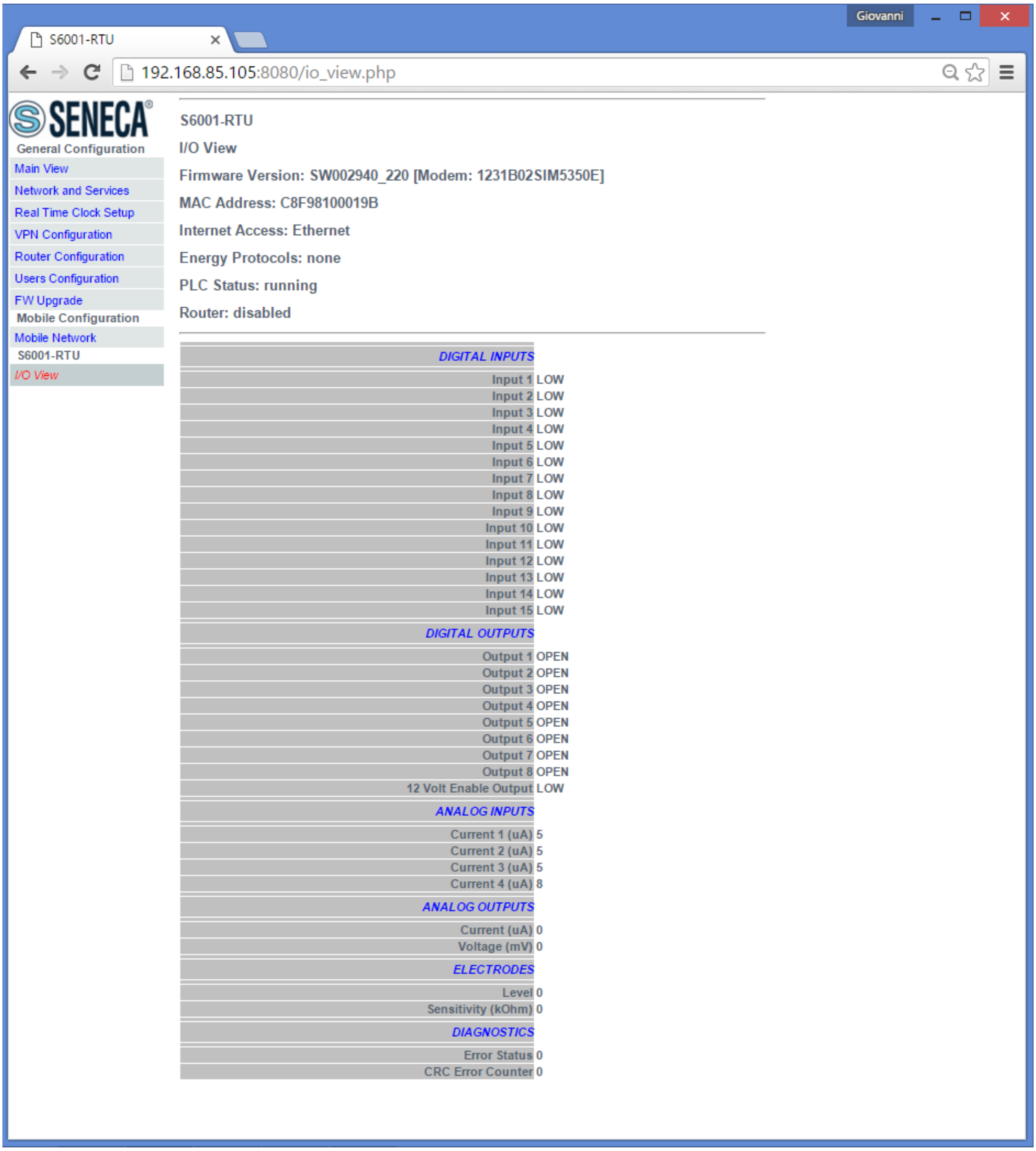
	CURRENT	UPDATED
Digital I/O Configuration		
Input 1 Mode	Remote connection disable	Remote connection disable ▾
Output 1 Mode	Remote connection active	Remote connection active ▾
Input 2 Mode	General input	General input ▾
Output 2 Mode	General output	General output ▾
Input/Output 1 Mode	General input	General input ▾
Input/Output 2 Mode	General output	General output ▾
Security Level		
Service Disable	VPN Connection	VPN Connection ▾

Digital I/O Status

DI 1	DO 1	DI 2	DO 2	DIDO 1	DIDO 2
LOW	LOW	HIGH	LOW	LOW	LOW

16.1.11 I/O View (S6001-RTU)

In S6001-RTU CPU, one more page is available called “I/O View”; in this page, the current status of all the inputs/outputs is shown, along with some diagnostic information.



S6001-RTU

I/O View

Firmware Version: SW002940_220 [Modem: 1231B02SIM5350E]

MAC Address: C8F98100019B

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running

Router: disabled

DIGITAL INPUTS

Input 1 LOW
Input 2 LOW
Input 3 LOW
Input 4 LOW
Input 5 LOW
Input 6 LOW
Input 7 LOW
Input 8 LOW
Input 9 LOW
Input 10 LOW
Input 11 LOW
Input 12 LOW
Input 13 LOW
Input 14 LOW
Input 15 LOW

DIGITAL OUTPUTS

Output 1 OPEN
Output 2 OPEN
Output 3 OPEN
Output 4 OPEN
Output 5 OPEN
Output 6 OPEN
Output 7 OPEN
Output 8 OPEN
12 Volt Enable Output LOW

ANALOG INPUTS

Current 1 (uA) 5
Current 2 (uA) 5
Current 3 (uA) 5
Current 4 (uA) 8

ANALOG OUTPUTS

Current (uA) 0
Voltage (mV) 0

ELECTRODES

Level 0
Sensitivity (kOhm) 0

DIAGNOSTICS

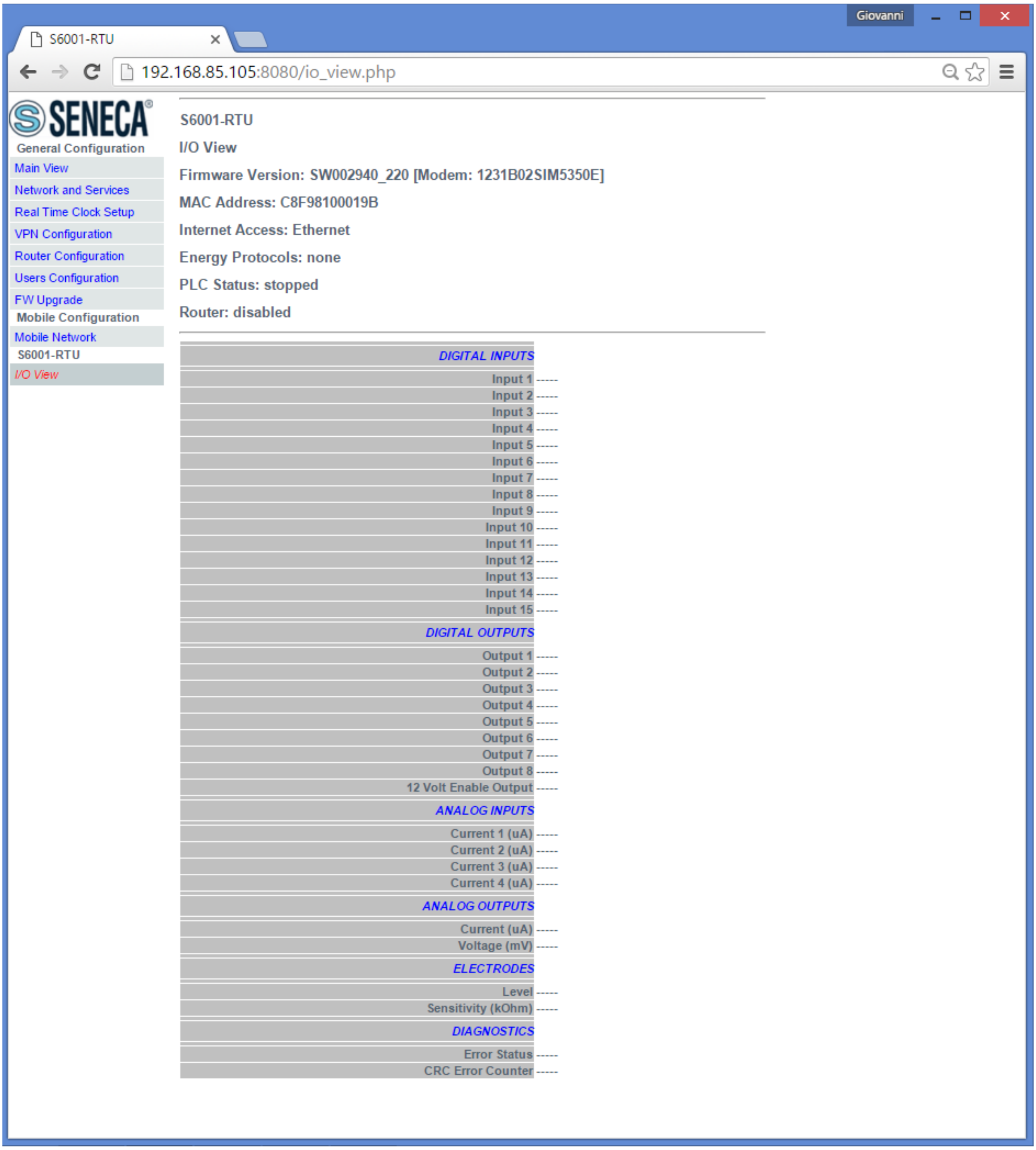
Error Status 0
CRC Error Counter 0

The following parameters are shown:

Field	Meaning	Values
DIGITAL INPUTS/Input 1..Input 15	Status of Digital Input	LOW/HIGH
DIGITAL OUTPUTS/Output 1..Output 8	Status of Digital Output (relay)	OPEN/CLOSED
DIGITAL OUTPUTS/12 Volt Enable	Status of Digital Output enabling 12	LOW/HIGH

Output	Vdc voltage on screw terminals 37 and 38	
ANALOG INPUTS/Current 1.. Current 4	Value of analog current input (in uA)	0..20000
ANALOG OUTPUT/Current	Value of analog current output (in uA)	0..20000
ANALOG OUTPUT/Voltage	Value of analog voltage output (in mV)	0..10000
ELECTRODES/Level	Liquid level value	0,1,2
ELECTRODES/Sensitivity	Sensitivity value applied in liquid level measurement (in kΩ)	0..255
DIAGNOSTICS/Error Status	This parameter gives an information about errors that might occur in the I/O board. The value is a bitmask, as specified in the column “Values”.	0: no error Bit 9: flash memory error
DIAGNOSTICS/CRC Error Counter	This parameter counts the CRC errors occurring in the communication between the CPU board and the I/O board; if the value continuously increases, it means that there is some HW problem	>= 0 0 means “no CRC error”

If the Soft PLC application is not running, inputs/outputs values are not available, so the page appears like in the following figure:



S6001-RTU

I/O View

Firmware Version: SW002940_220 [Modem: 1231B02SIM5350E]

MAC Address: C8F98100019B

Internet Access: Ethernet

Energy Protocols: none

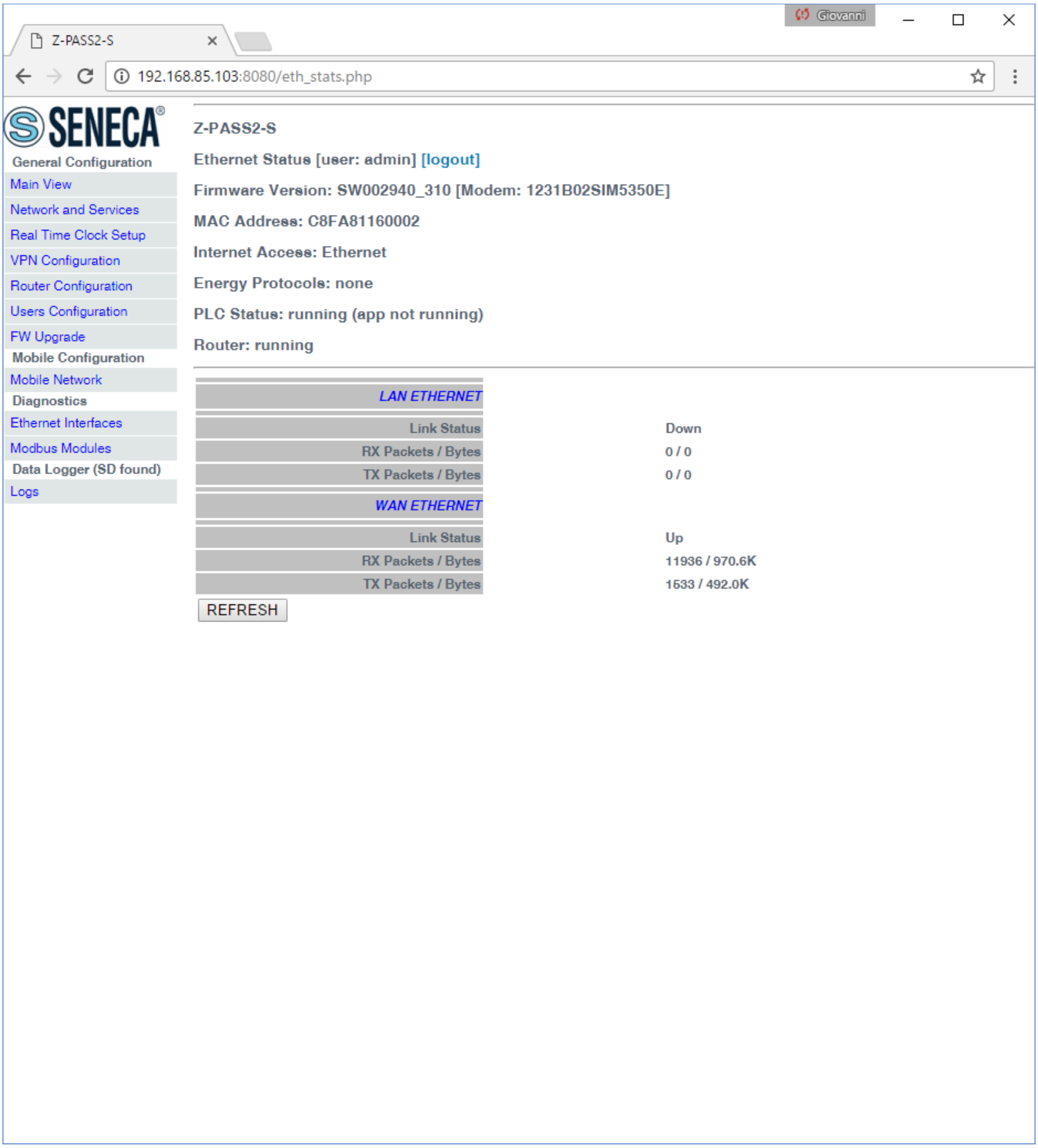
PLC Status: stopped

Router: disabled

DIGITAL INPUTS	
Input 1	-----
Input 2	-----
Input 3	-----
Input 4	-----
Input 5	-----
Input 6	-----
Input 7	-----
Input 8	-----
Input 9	-----
Input 10	-----
Input 11	-----
Input 12	-----
Input 13	-----
Input 14	-----
Input 15	-----
DIGITAL OUTPUTS	
Output 1	-----
Output 2	-----
Output 3	-----
Output 4	-----
Output 5	-----
Output 6	-----
Output 7	-----
Output 8	-----
12 Volt Enable Output	-----
ANALOG INPUTS	
Current 1 (uA)	-----
Current 2 (uA)	-----
Current 3 (uA)	-----
Current 4 (uA)	-----
ANALOG OUTPUTS	
Current (uA)	-----
Voltage (mV)	-----
ELECTRODES	
Level	-----
Sensitivity (kOhm)	-----
DIAGNOSTICS	
Error Status	-----
CRC Error Counter	-----

16.1.12 Ethernet Interfaces

By clicking on the “Ethernet Interfaces” link, in the “Diagnostics” menu, you come to the following page:



Z-PASS2-S

Ethernet Status [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running (app not running)

Router: running

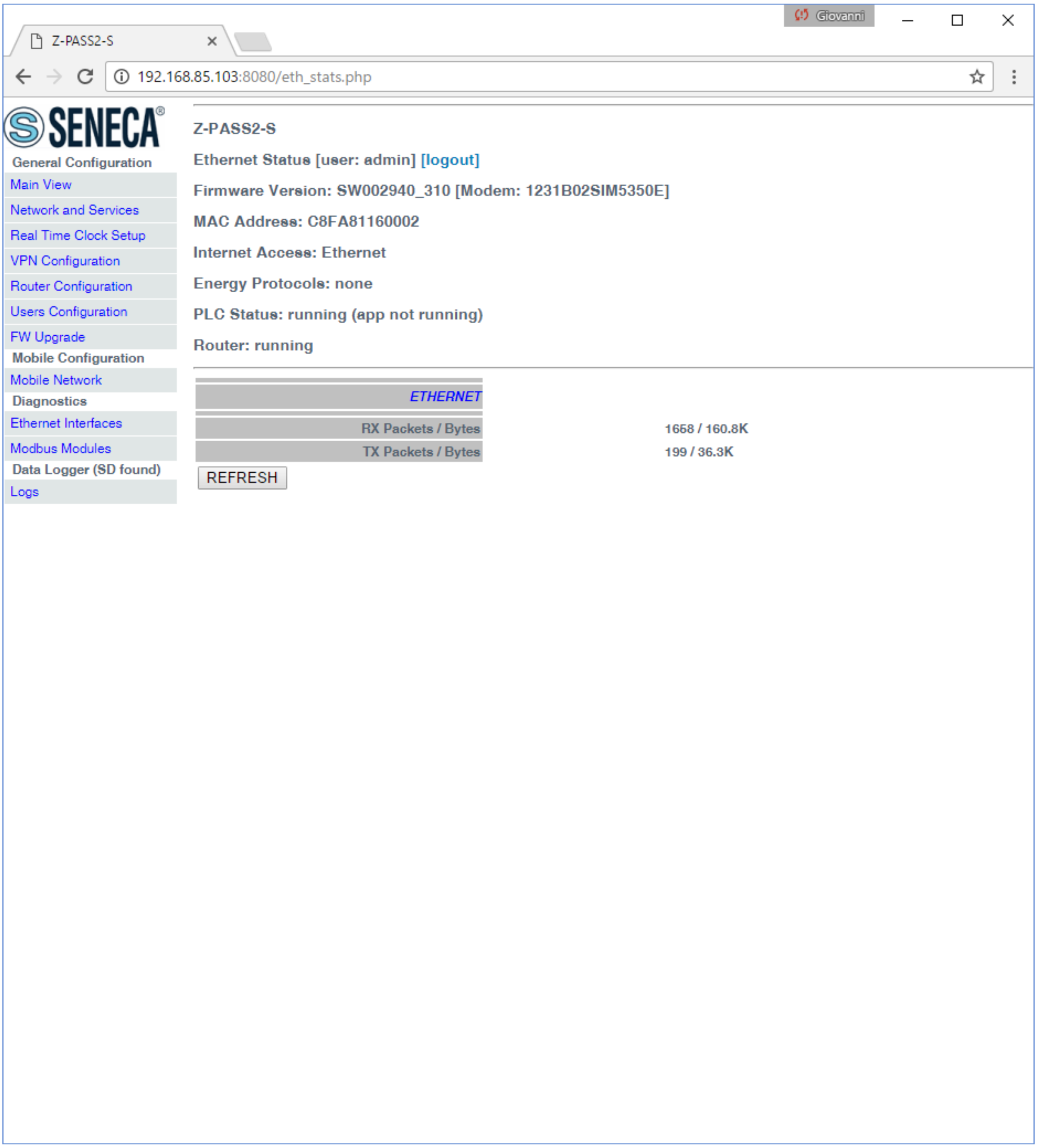
LAN ETHERNET	
Link Status	Down
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0
WAN ETHERNET	
Link Status	Up
RX Packets / Bytes	11936 / 970.6K
TX Packets / Bytes	1533 / 492.0K

The above figure applies to a Z-PASS2-S-R01/Z-PASS2-S-R02 CPU, when the “Ethernet Mode” is “LAN/WAN”; a similar page also applies to a Z-TWS4-R01/Z-TWS4-R02 CPU.

In this page, for each of the two available Ethernet interfaces (LAN and WAN), the following information is shown:

- the Ethernet link status (i.e. “Down” or “Up”)
- the number of packets/bytes received from the Ethernet interface, when the link is up; “0/0” when the link is down
- the number of packets/bytes sent to the Ethernet interface, when the link is up; “0/0” when the link is down

For Z-TWS4, Z-PASS2-S, S6001-RTU and for Z-TWS4-R01/Z-TWS4-R02, Z-PASS2-S-R01/Z-PASS2-S-R02 when the "Ethernet Mode" is "Switch", the "Ethernet Interfaces" page is similar to the one shown in the following figure.



Z-PASS2-S

Ethernet Status [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running (app not running)

Router: running

ETHERNET	
RX Packets / Bytes	1658 / 160.8K
TX Packets / Bytes	199 / 36.3K

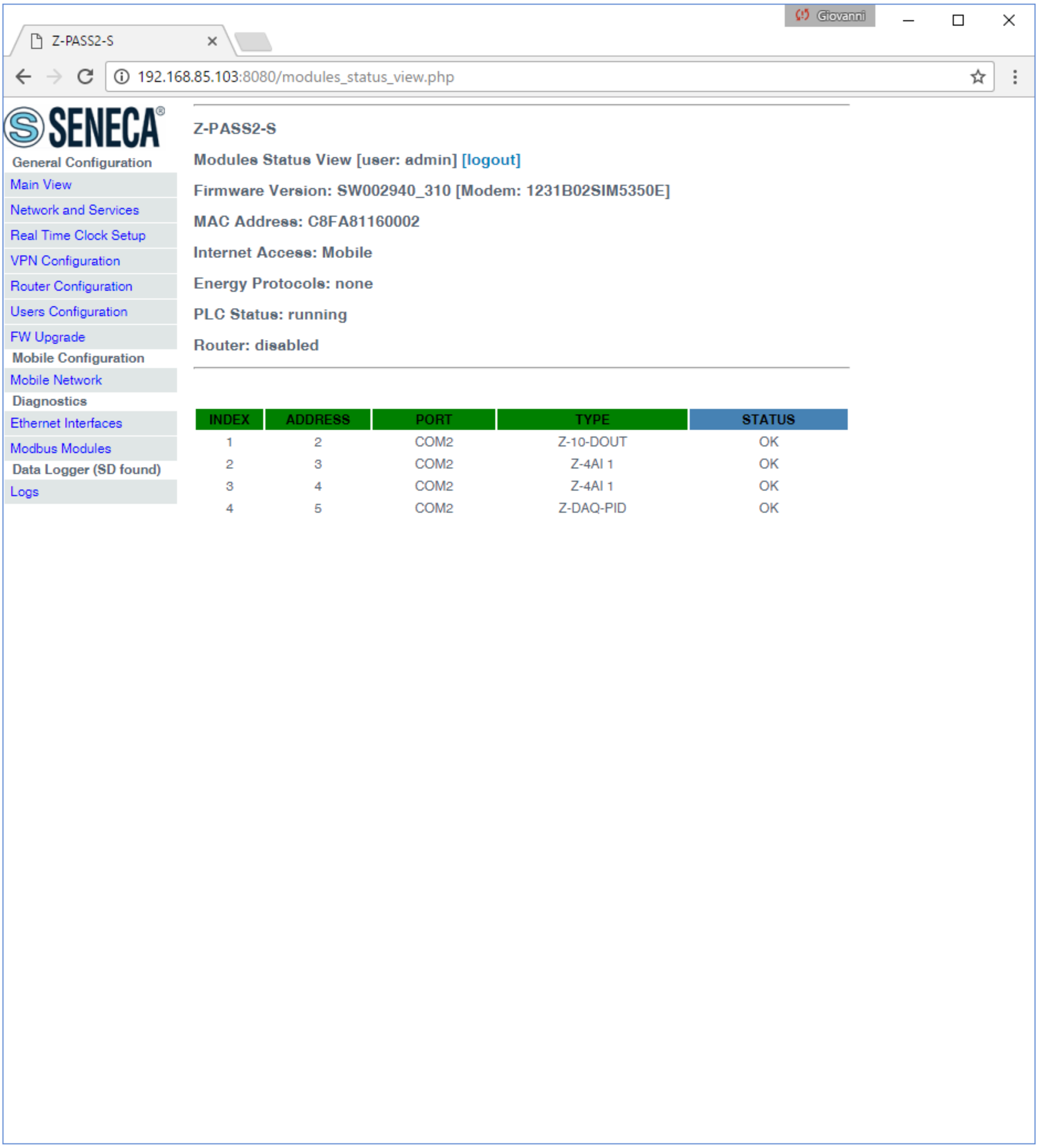
In this page, for the one available Ethernet interface, the following information is shown:

- the number of packets/bytes received from the Ethernet interface
- the number of packets/bytes sent to the Ethernet interface

You can refresh the Ethernet status, by clicking on the "REFRESH" button.

16.1.13 Modbus Modules

By clicking on the “Modbus Modules” link, in the “Diagnostics” menu, you come to a page similar to the one in the following figure:



Z-PASS2-S

Modules Status View [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running

Router: disabled

INDEX	ADDRESS	PORT	TYPE	STATUS
1	2	COM2	Z-10-DOUT	OK
2	3	COM2	Z-4AI 1	OK
3	4	COM2	Z-4AI 1	OK
4	5	COM2	Z-DAQ-PID	OK

This page shows a table containing a row for each Modbus RTU Slave modules configured in the Z-NET4[20]/Straton project; each row contains the following information:

- a progressive index
- the Modbus Slave Address

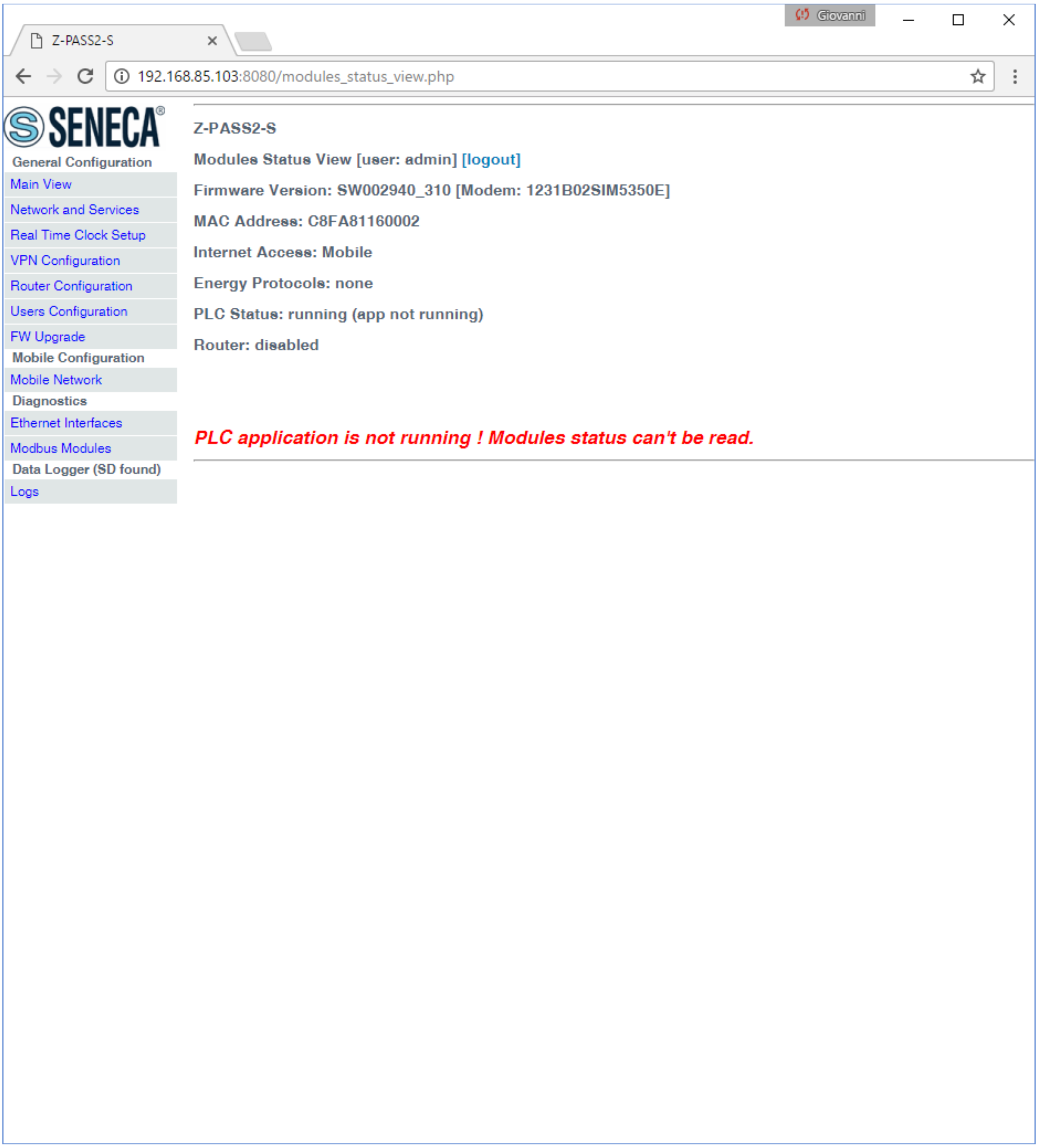
[20] For information on Z-NET4 SW, please see chapter 18.

- the name of the serial port (i.e. COM1/COM2/COM4) which the module is connected to
- the type of module
- the module status, which can be:
    - “OK”, if the module is correctly responding to Modbus requests
    - “TIMEOUT”, if the module is not responding to Modbus requests
    - “ERROR”, if any other error occurs

The Modbus Modules page can’t be shown in the following situations:

- if a Z-NET4 project is not loaded on the Device
- if TWS/PLC services are not running
- if a PLC application is not running, i.e. not present or stopped

As an example, for the third of the above cases, the following message is shown:



Z-PASS2-S

Modules Status View [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

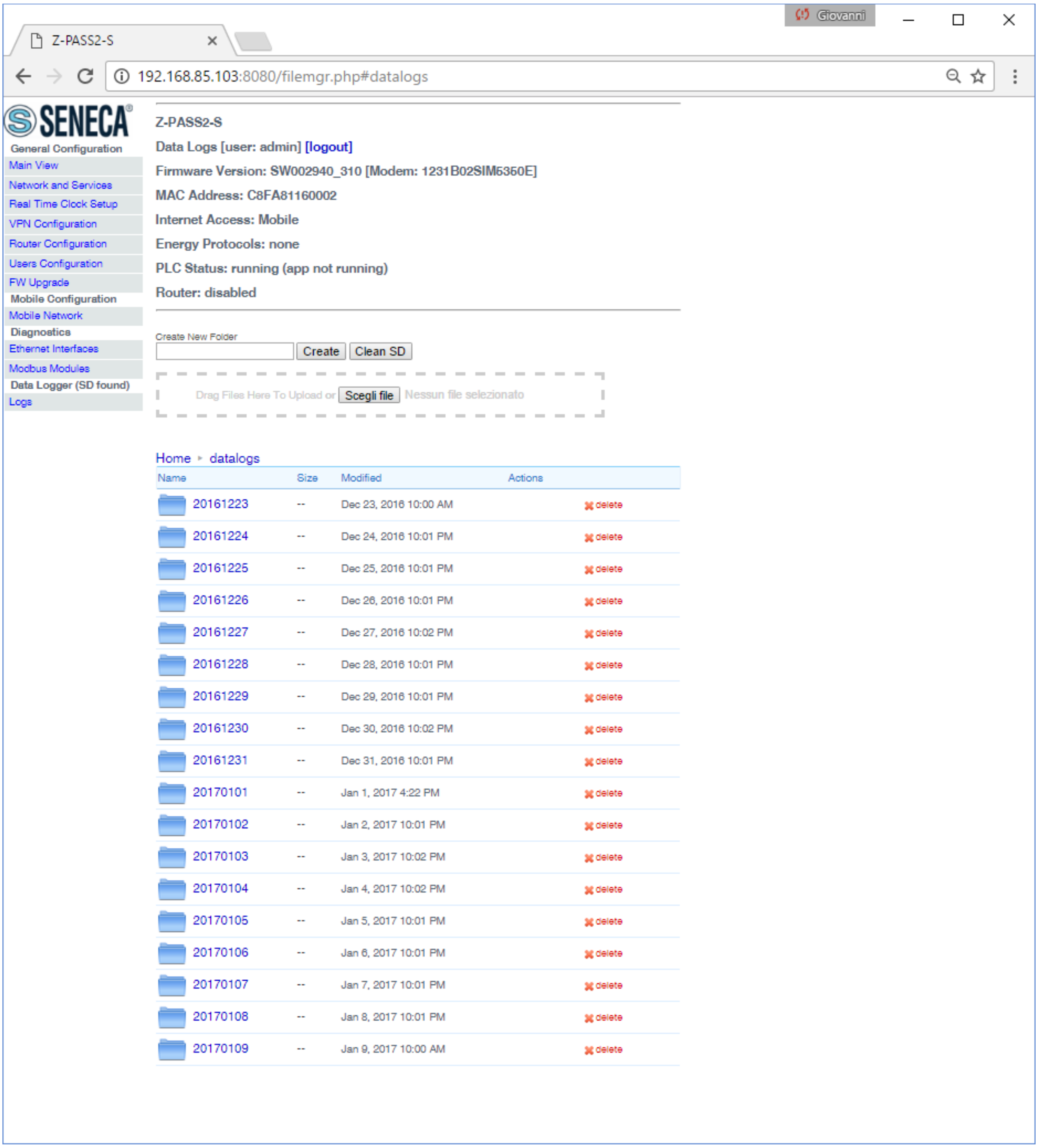
PLC Status: running (app not running)

Router: disabled

PLC application is not running ! Modules status can't be read.

16.1.14 Data Logs

By clicking on the “Logs” link, in the “Data Logger” menu, you come to a page similar to those in the following figures:



Z-PASS2-S

Data Logs [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5360E]

MAC Address: C8FA81160002

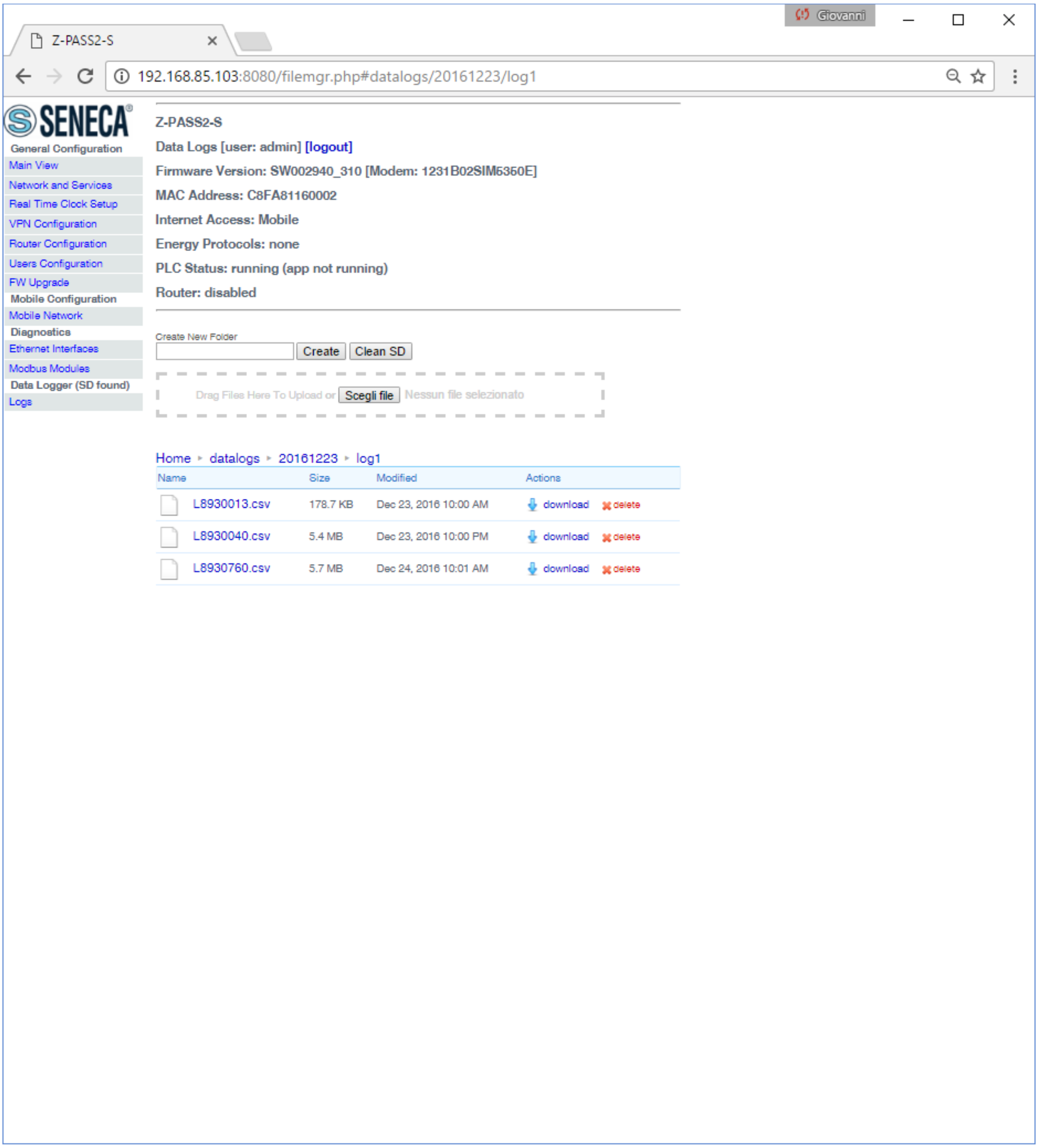
Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

Name	Size	Modified	Actions
20161223	--	Dec 23, 2016 10:00 AM	delete
20161224	--	Dec 24, 2016 10:01 PM	delete
20161225	--	Dec 25, 2016 10:01 PM	delete
20161226	--	Dec 26, 2016 10:01 PM	delete
20161227	--	Dec 27, 2016 10:02 PM	delete
20161228	--	Dec 28, 2016 10:01 PM	delete
20161229	--	Dec 29, 2016 10:01 PM	delete
20161230	--	Dec 30, 2016 10:02 PM	delete
20161231	--	Dec 31, 2016 10:01 PM	delete
20170101	--	Jan 1, 2017 4:22 PM	delete
20170102	--	Jan 2, 2017 10:01 PM	delete
20170103	--	Jan 3, 2017 10:02 PM	delete
20170104	--	Jan 4, 2017 10:02 PM	delete
20170105	--	Jan 5, 2017 10:01 PM	delete
20170106	--	Jan 6, 2017 10:01 PM	delete
20170107	--	Jan 7, 2017 10:01 PM	delete
20170108	--	Jan 8, 2017 10:01 PM	delete
20170109	--	Jan 9, 2017 10:00 AM	delete



Z-PASS2-S

Data Logs [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5360E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

Create New Folder

Create | Clean SD

Drag Files Here To Upload or Scegli file Nessun file selezionato

Home ▸ datalogs ▸ 20161223 ▸ log1

Name	Size	Modified	Actions
L8930013.csv	178.7 KB	Dec 23, 2016 10:00 AM	download delete
L8930040.csv	5.4 MB	Dec 23, 2016 10:00 PM	download delete
L8930760.csv	5.7 MB	Dec 24, 2016 10:01 AM	download delete

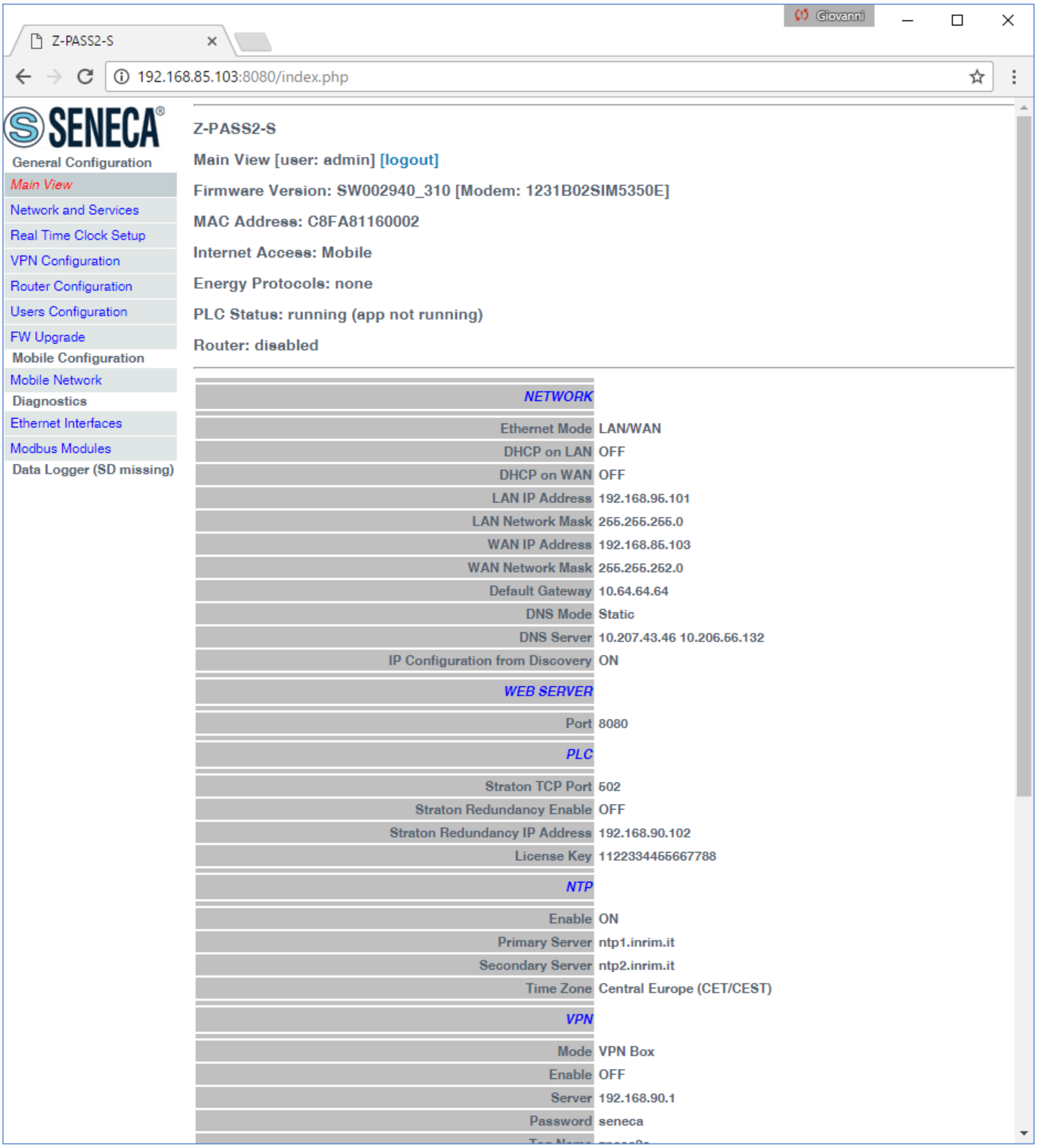
This page shows the contents of the SD card which, typically, is used to store “Data Logs” files; these files are created by the “Data Logger” functionality available in Z-NET4 “Remote Control Functions” (see chapter 18).

The page lets you perform the following operations:

- browse the SD folder tree, clicking on the folder name links
- delete a folder, clicking on the “delete” link
- create a new folder, by means of the “Create New Folder” text-box and “Create” button; the new folder is created in the folder currently shown
- download a file, clicking on the filename link or on the “download” link

- delete a file, clicking on the “delete” link
- uploading a file, selecting it by means of the “Choose file” button or dragging it into the dashed area; the file is created in the folder currently shown
- clean the SD, by means of the “Clean SD” button; please note that this is done by formatting the SD, so all SD contents will be lost

If an SD card is not available on the Device, the “Logs” link is not shown, as in the following figure.



Z-PASS2-S

Main View [user: admin] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

NETWORK	
Ethernet Mode	LAN/WAN
DHCP on LAN	OFF
DHCP on WAN	OFF
LAN IP Address	192.168.95.101
LAN Network Mask	255.255.255.0
WAN IP Address	192.168.85.103
WAN Network Mask	255.255.252.0
Default Gateway	10.64.64.64
DNS Mode	Static
DNS Server	10.207.43.46 10.206.56.132
IP Configuration from Discovery	ON
WEB SERVER	
Port	8080
PLC	
Straton TCP Port	502
Straton Redundancy Enable	OFF
Straton Redundancy IP Address	192.168.90.102
License Key	1122334455667788
NTP	
Enable	ON
Primary Server	ntp1.inrim.it
Secondary Server	ntp2.inrim.it
Time Zone	Central Europe (CET/CEST)
VPN	
Mode	VPN Box
Enable	OFF
Server	192.168.90.1
Password	seneca

16.2 User pages

It is also possible to access the Device configuration site as a “non-administrator” user; this user is allowed to access only the “Main View” and “Network and Services” pages, viewing and setting only a limited number of configuration parameters; in S6001-RTU, the “I/O View” page is also available.

Also the “Ethernet Interfaces” and “Modbus Modules” pages of the “Diagnostics” section are available for this kind of user; they will not be shown again here, as they are identical to those for administrator user.

To login as “non-administrator” user, connect the browser to the Device IP address on port 8080, e.g.:

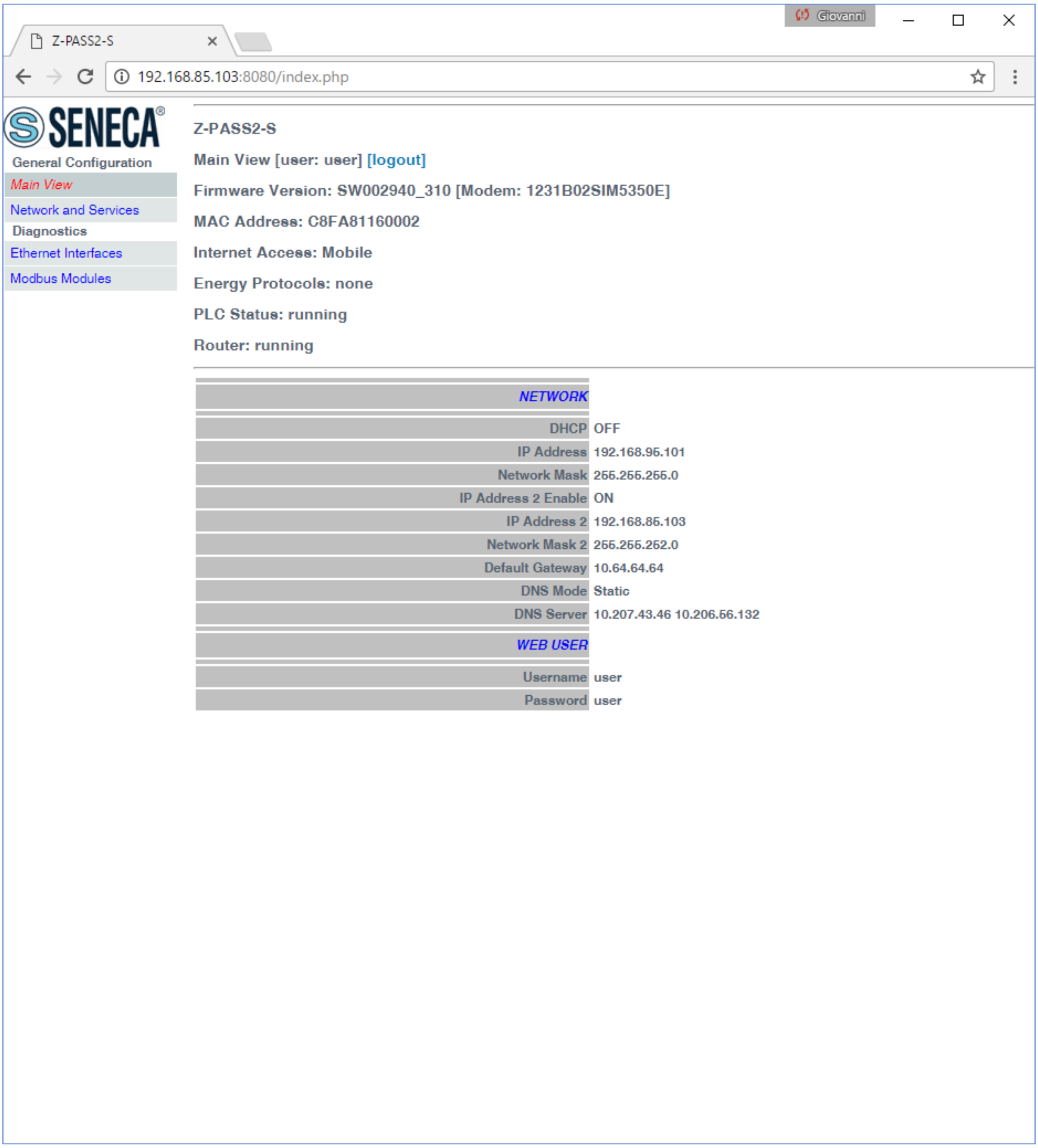
http://192.168.90.101:8080

and, when asked, provide the following credentials (default values):

Username: user
Password: user

You come to the “Main View” page, described in the following paragraph.

16.2.1 Main View



Z-PASS2-S

Main View [user: user] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running

Router: running

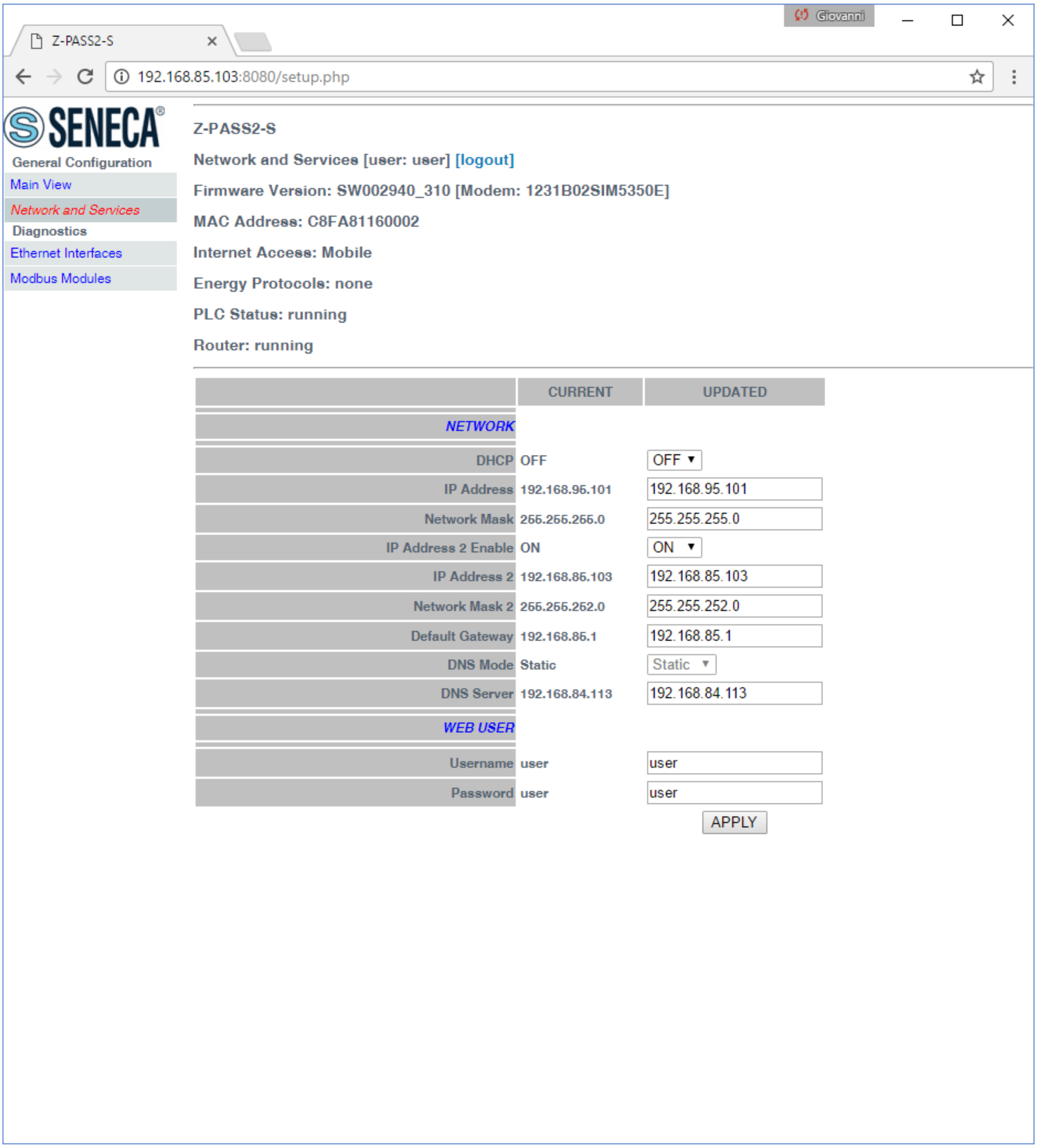
NETWORK	
DHCP	OFF
IP Address	192.168.95.101
Network Mask	255.255.255.0
IP Address 2 Enable	ON
IP Address 2	192.168.85.103
Network Mask 2	255.255.252.0
Default Gateway	10.64.64.64
DNS Mode	Static
DNS Server	10.207.43.46 10.206.56.132
WEB USER	
Username	user
Password	user

In this page, some Network parameters and the Web User credentials are shown, with their current values.

To change the parameter values, you have to go to the “Network and Services” page, described in the following paragraph.

16.2.2 Network and Services

The parameters shown in this page slightly change, depending on the HW version of the product (Z-TWS4/Z-PASS2-S or Z-TWS4-R01/Z-PASS2-S-R01 or Z-TWS4-R02/Z-PASS2-S-R02) and, for new HW versions, on the selected “Ethernet Mode”; this is shown in the following figures.



Z-PASS2-S

Network and Services [user: user] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

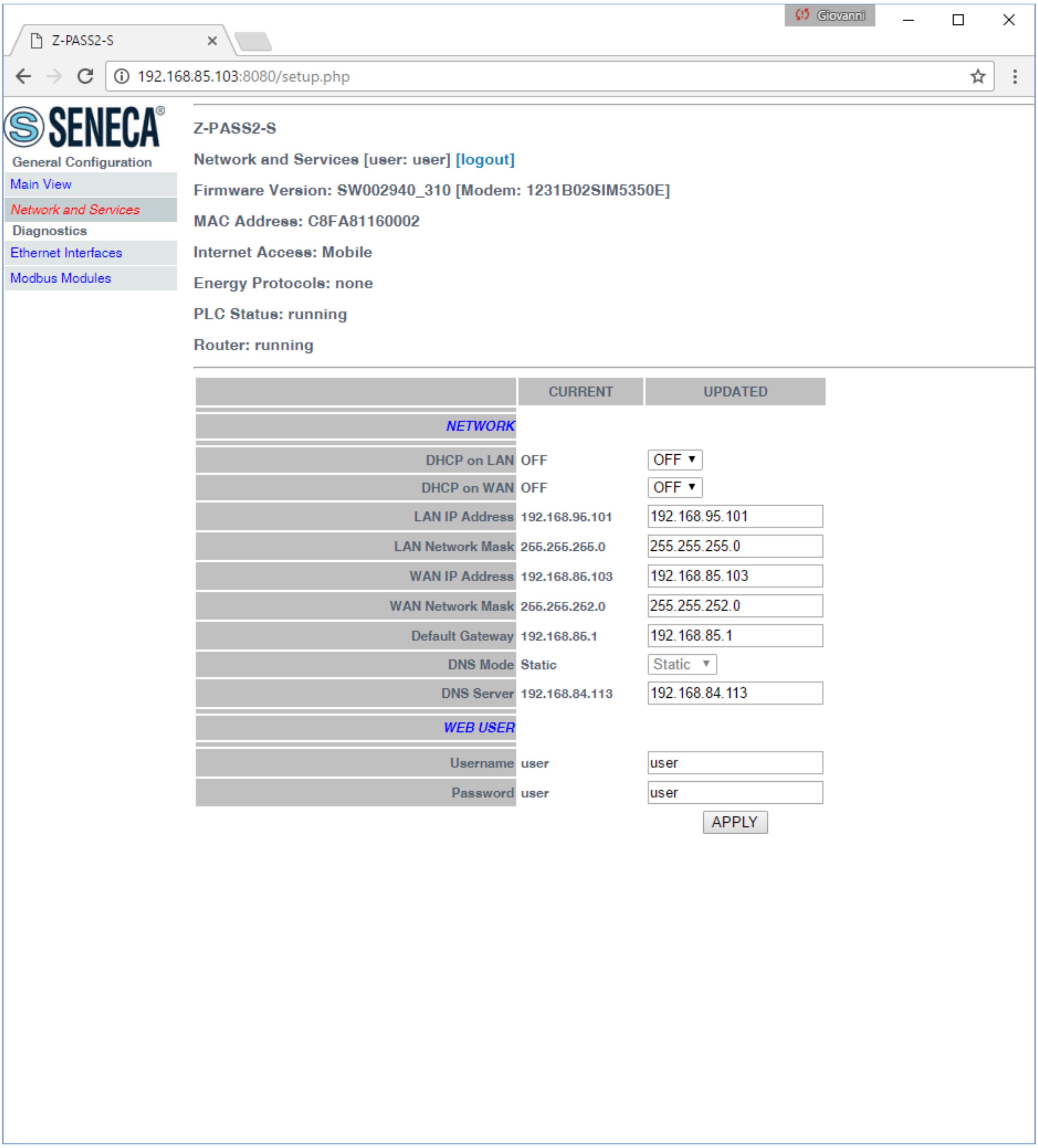
Energy Protocols: none

PLC Status: running

Router: running

	CURRENT	UPDATED
NETWORK		
DHCP	OFF	OFF ▾
IP Address	192.168.95.101	192.168.95.101
Network Mask	255.255.255.0	255.255.255.0
IP Address 2 Enable	ON	ON ▾
IP Address 2	192.168.85.103	192.168.85.103
Network Mask 2	255.255.252.0	255.255.252.0
Default Gateway	192.168.85.1	192.168.85.1
DNS Mode	Static	Static ▾
DNS Server	192.168.84.113	192.168.84.113
WEB USER		
Username	user	user
Password	user	user

The previous figure shows the “Network and Services” page for a Z-PASS2-S-R01/Z-PASS2-S-R02, when the “Ethernet Mode” parameter is set to “Switch”; it also applies to a Z-TWS4-R01/Z-TWS4-R02 in “Switch” mode, to a Z-TWS4 and Z-PASS2-S (old versions) and to a S6001-RTU.



Z-PASS2-S

Network and Services [user: user] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running

Router: running

	CURRENT	UPDATED
NETWORK		
DHCP on LAN	OFF	OFF
DHCP on WAN	OFF	OFF
LAN IP Address	192.168.95.101	192.168.95.101
LAN Network Mask	255.255.255.0	255.255.255.0
WAN IP Address	192.168.85.103	192.168.85.103
WAN Network Mask	255.255.252.0	255.255.252.0
Default Gateway	192.168.85.1	192.168.85.1
DNS Mode	Static	Static
DNS Server	192.168.84.113	192.168.84.113
WEB USER		
Username	user	user
Password	user	user

The previous figure shows the "Network and Services" page for a Z-PASS2-S-R01/Z-PASS2-S-R02, when the "Ethernet Mode" parameter is set to "LAN/WAN"; it also applies to a Z-TWS4-R01/Z-TWS4-R02 in "LAN/WAN" mode.

There is an important difference between the parameter values shown in this page and those shown in the "Main View" page: the former are configured values, whereas the latter are actual values.

To better explain this difference, let's consider the case when the DHCP parameter is set to ON; in the "Network and Services" page, you may see the 192.168.90.101 default value for the "IP Address" parameter, whereas the "Main View" page shows the actual IP Address, assigned by the DHCP server.

In the following table, all configuration parameters available in this page are listed, with a short explanation and the parameter default value for each of them.

Note that "Ethernet Mode" parameter is not shown in user pages.

Field	**Meaning**	**Default value**
Ethernet Mode = "Switch"		
NETWORK/DHCP	Flag to enable/disable the DHCP functionality on the Ethernet interface.	OFF
NETWORK/IP Address	IP address of the Ethernet interface (disabled when "DHCP" is set to "ON")	192.168.90.101
NETWORK/Network Mask	Network mask of the Ethernet interface (disabled when "DHCP" is set to "ON")	255.255.255.0
NETWORK/IP Address 2 Enable	Flag to enable/disable the second IP address on the Ethernet interface. Note that the second IP address can be enabled also when the DHCP functionality is active.	OFF
NETWORK/IP Address 2	Second IP address of the Ethernet interface	192.168.100.101
NETWORK/Network Mask 2	Second network mask of the Ethernet interface	255.255.255.0
Ethernet Mode = "LAN/WAN"		
NETWORK/DHCP on LAN	When "Ethernet Mode" is set to "LAN/WAN", this parameter is disabled (always OFF)	OFF
NETWORK/DHCP on WAN	Flag to enable/disable the DHCP functionality on the WAN Ethernet interface	ON
NETWORK/LAN IP Address	IP address of the LAN Ethernet interface	192.168.90.101
NETWORK/LAN Network Mask	Network mask of the LAN Ethernet interface	255.255.255.0
NETWORK/WAN IP Address	IP address of the WAN Ethernet interface (disabled when "DHCP on WAN" is set to "ON")	192.168.100.101
NETWORK/WAN Network Mask	Network mask of the WAN Ethernet interface (disabled when "DHCP on WAN" is set to "ON")	255.255.255.0
NETWORK/Default Gateway	Default Gateway IP address	192.168.100.1 , for Z-TWS4-

	(disabled when DHCP functionality is enabled on any interface). When "Ethernet Mode" is set to "LAN/WAN", the Default Gateway shall be in the WAN subnet.	R0x and Z-PASS2-S-R0x (x=1,2) 192.168.90.1, for all other products
NETWORK/DNS Mode	Tells if the DNS Server shall be set statically (value: "Static") or dinamically assigned by the DHCP Server (value: "DHCP")	DHCP, for Z-TWS4-R0x and Z-PASS2-S-R0x (x=1,2) Static, for all other products
NETWORK/DNS Server	DNS server IP address (disabled when DHCP functionality is enabled on any interface and DNS Mode = DHCP)	192.168.100.1 , for Z-TWS4-R0x and Z-PASS2-S-R0x (x=1,2) 192.168.90.1, for all other products
WEB USER/Username	Username to access the web configuration site (limited access)	User
WEB USER/Password	Password to access the web configuration site (limited access)	user

Some notes about the "DHCP" parameters:

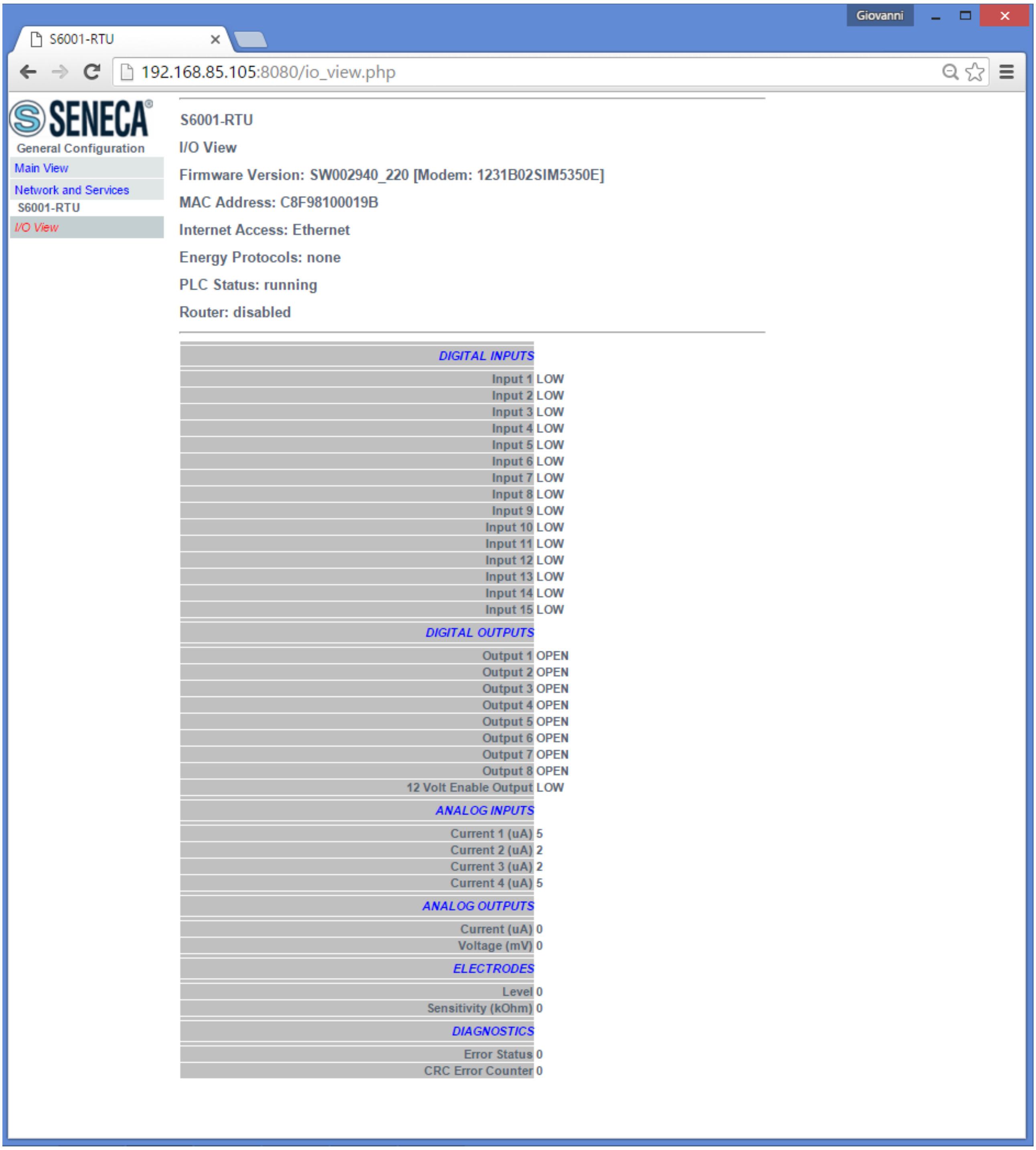
- the "DHCP" parameter can be set to "ON" only if the "DHCP Server" parameter of the "Router Configuration" page is set to "OFF";
- only the "DHCP on WAN" parameter can be set to "ON".

You can change any of the above parameters; to apply the changes, press the "APPLY" button.

Please note that, after changing the Web User credentials, a new login will be required to access any page.

16.2.3 I/O View (S6001-RTU)

This page is identical to that shown for "administrator user" (see 16.1.10).



S6001-RTU

I/O View

Firmware Version: SW002940_220 [Modem: 1231B02SIM5350E]

MAC Address: C8F98100019B

Internet Access: Ethernet

Energy Protocols: none

PLC Status: running

Router: disabled

DIGITAL INPUTS	
Input 1	LOW
Input 2	LOW
Input 3	LOW
Input 4	LOW
Input 5	LOW
Input 6	LOW
Input 7	LOW
Input 8	LOW
Input 9	LOW
Input 10	LOW
Input 11	LOW
Input 12	LOW
Input 13	LOW
Input 14	LOW
Input 15	LOW
DIGITAL OUTPUTS	
Output 1	OPEN
Output 2	OPEN
Output 3	OPEN
Output 4	OPEN
Output 5	OPEN
Output 6	OPEN
Output 7	OPEN
Output 8	OPEN
12 Volt Enable Output	LOW
ANALOG INPUTS	
Current 1 (uA)	5
Current 2 (uA)	2
Current 3 (uA)	2
Current 4 (uA)	5
ANALOG OUTPUTS	
Current (uA)	0
Voltage (mV)	0
ELECTRODES	
Level	0
Sensitivity (kOhm)	0
DIAGNOSTICS	
Error Status	0
CRC Error Counter	0

16.3 Guest pages

It is also possible to access the Device configuration site as a “guest” user; this user is allowed to access all the pages except for “FW Upgrade”, “Configuration Management”” and “Data Logs” pages, viewing all configuration parameters and status information, without changing any parameter; so, in all the pages, the “APPLY” buttons (and any other button used to perform changes) are disabled.

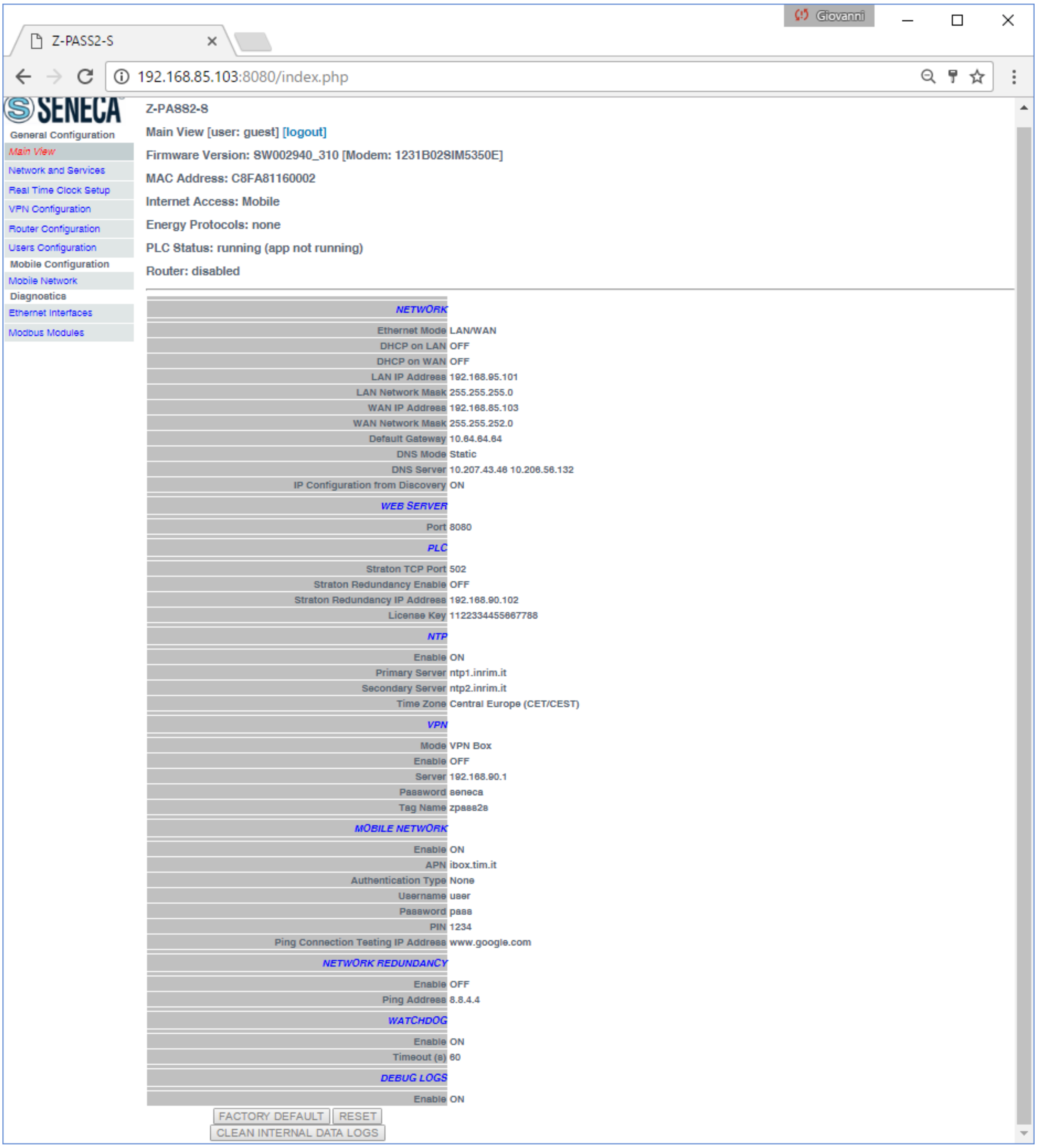
To login as “guest” user, connect the browser to the Device IP address on port 8080, e.g.:

http://192.168.90.101:8080

and, when asked, provide the following credentials (default values):

Username: guest
Password: guest

You come to the “Main View” page, shown in the following figure.



Z-PASS2-S

Main View [user: guest] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

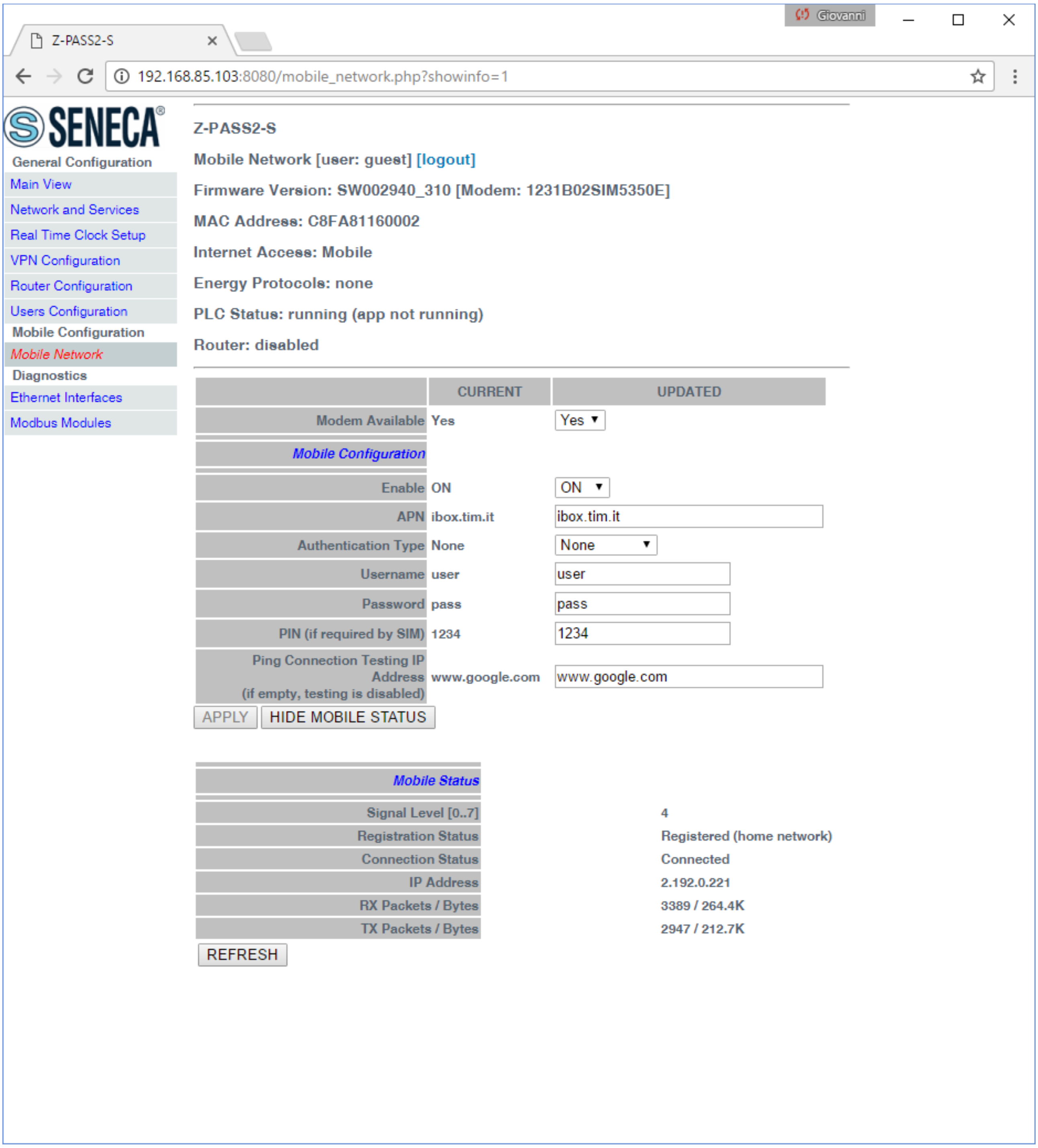
PLC Status: running (app not running)

Router: disabled

NETWORK	
Ethernet Mode	LAN/WAN
DHCP on LAN	OFF
DHCP on WAN	OFF
LAN IP Address	192.168.95.101
LAN Network Mask	255.255.255.0
WAN IP Address	192.168.85.103
WAN Network Mask	255.255.252.0
Default Gateway	10.64.64.64
DNS Mode	Static
DNS Server	10.207.43.46 10.206.56.132
IP Configuration from Discovery	ON
WEB SERVER	
Port	8080
PLC	
Straton TCP Port	502
Straton Redundancy Enable	OFF
Straton Redundancy IP Address	192.168.90.102
License Key	1122334455667788
NTP	
Enable	ON
Primary Server	ntp1.inrim.it
Secondary Server	ntp2.inrim.it
Time Zone	Central Europe (CET/CEST)
VPN	
Mode	VPN Box
Enable	OFF
Server	192.168.90.1
Password	seneca
Tag Name	zpass2s
MOBILE NETWORK	
Enable	ON
APN	ibox.tim.it
Authentication Type	None
Username	user
Password	pass
PIN	1234
Ping Connection Testing IP Address	www.google.com
NETWORK REDUNDANCY	
Enable	OFF
Ping Address	8.8.4.4
WATCHDOG	
Enable	ON
Timeout (s)	60
DEBUG LOGS	
Enable	ON

Note that, as told above, the “FACTORY DEFAULT”, “RESET” and “CLEAN INTERNAL DATA LOGS” buttons are disabled.

Another example of a page accessed by the “guest” user is given in the following figure.



Z-PASS2-S

Mobile Network [user: guest] [logout]

Firmware Version: SW002940_310 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Energy Protocols: none

PLC Status: running (app not running)

Router: disabled

	CURRENT	UPDATED
Modem Available	Yes	Yes ▾
Mobile Configuration		
Enable	ON	ON ▾
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None ▾
Username	user	user
Password	pass	pass
PIN (if required by SIM)	1234	1234
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

APPLY   HIDE MOBILE STATUS

Mobile Status	
Signal Level [0..7]	4
Registration Status	Registered (home network)
Connection Status	Connected
IP Address	2.192.0.221
RX Packets / Bytes	3389 / 264.4K
TX Packets / Bytes	2947 / 212.7K

REFRESH

In the “Mobile Network” page, the “APPLY” button is disabled, whereas the “SHOW MOBILE STATUS”/”HIDE MOBILE STATUS” and “REFRESH” buttons are enabled, letting the “guest” user to view the Mobile Status.

17 Seneca StratON Library

To let the users exploit Z-TWS4/Z-PASS2-S/S6001-RTU features in their IEC 61131-3 programs, Seneca has developed a set of “Function Blocks” and Functions, supplied with the Seneca library for StratON.

In this chapter, all the FBs and functions available on Z-TWS4/Z-PASS2-S/S6001-RTU are listed, providing a description of input/output parameters and some notes for each of them.

17.1 Function Blocks

17.1.1 General FB behavior

The description given in this paragraph apply to all the FBs available on Z-TWS4/Z-PASS2-S/S6001-RTU, except for the LINUX_SHELL FB, which has a particular behavior (see related paragraph).

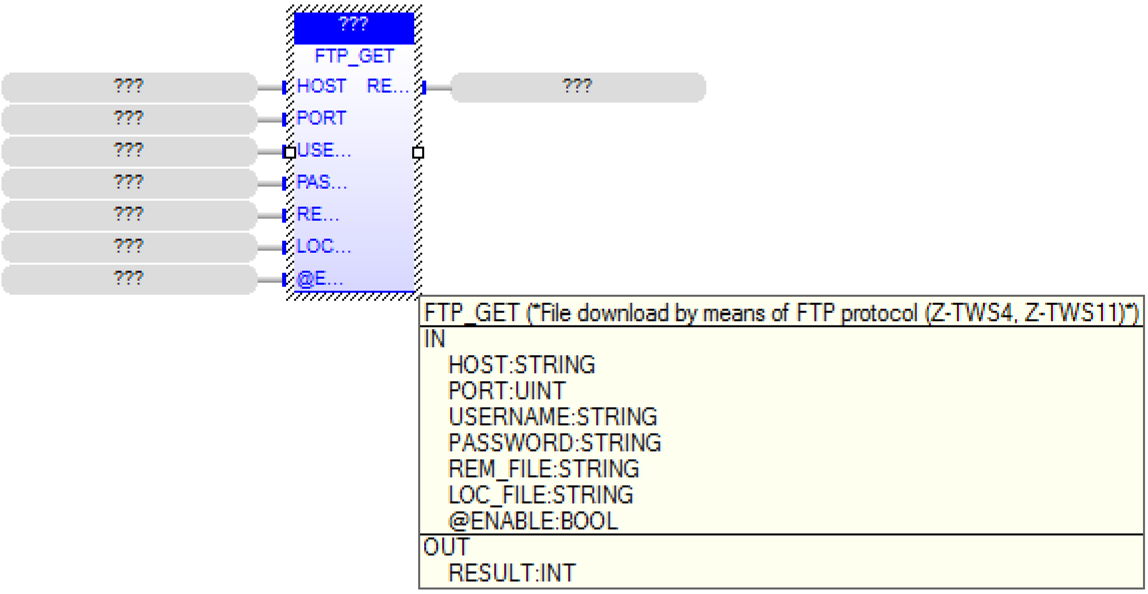
All the FBs require more than one PLC cycle to be completed (Asynchronous Function Block); so, the application shall run them for a number of cycles until it detects that the FB execution has ended.

Every FB has an "ENABLE" parameter, which is an input/output parameter: to let the FB actually run, the application shall put ENABLE=TRUE (input), not changing the parameter value during the FB execution; when the execution is completed, the FB code itself will put ENABLE=FALSE (output); when the FB is called with ENABLE=FALSE, it does nothing and returns the *NOT_DONE* (-2) result value.

All the FBs return the *FAILED* (-1) result value to signal that the FB execution has failed, for a generic reason; some FBs provide further failure result values, in particular the *TIMEOUT* (2) result value.

All the FBs return the *RUNNING* (0) result value to tell the application that the FB processing is still running and the *DONE* (1) result value when the FB processing has successfully ended.

17.1.2 FTP_GET

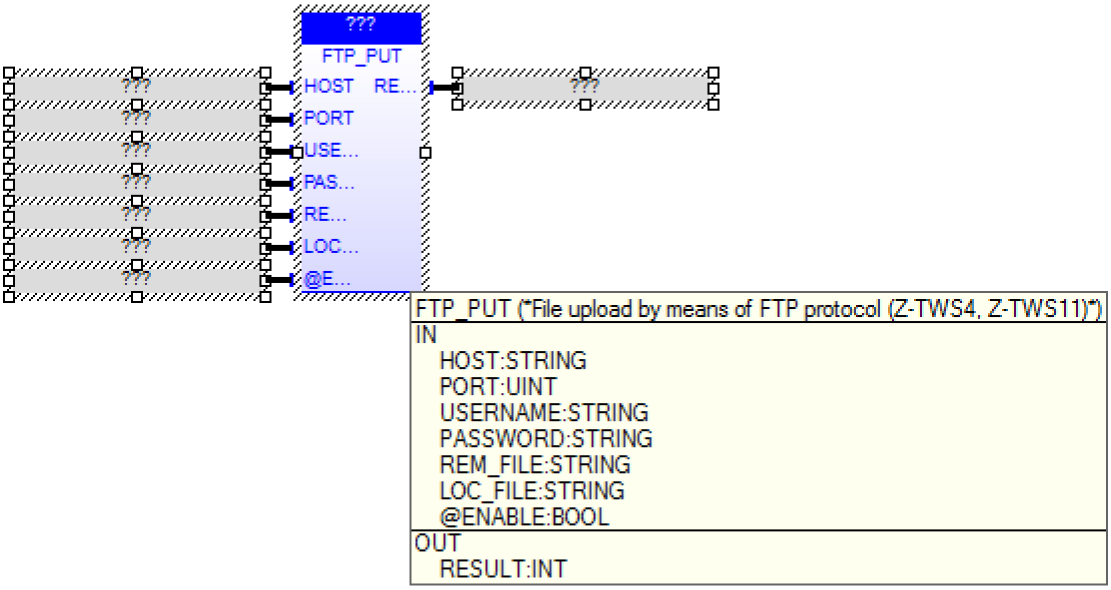


```
FTP_GET (*File download by means of FTP protocol (Z-TWS4, Z-TWS11)*)
IN
   HOST:STRING
   PORT:UINT
   USERNAME:STRING
   PASSWORD:STRING
   REM_FILE:STRING
   LOC_FILE:STRING
   @ENABLE:BOOL
OUT
   RESULT:INT
```

```
The FTP_GET FB downloads a file, by means of the FTP protocol.

When first called, the FB runs a process which starts performing the download;
on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:
- HOST     : IP address or host name of the FTP server
- PORT     : TCP port for the FTP protocol (normally: 21)
- USERNAME : username for authentication
- PASSWORD : password for authentication
- REM_FILE : name of the file (with path) on the remote server
- LOC_FILE : name of the file (with path) on the local device
- @ENABLE  : TRUE  -> FB is executed
             FALSE -> FB is skipped
```

```
The FB has the following output parameter:
- RESULT : -2, when called with ENABLE=FALSE
           -1, in case of any failure
            0, if the process is still running
            1, if the process has successfully finished.
```

17.1.3 FTP_PUT



FTP_PUT (*File upload by means of FTP protocol (Z-TWS4, Z-TWS11)*)

IN
- HOST:STRING
- PORT:UINT
- USERNAME:STRING
- PASSWORD:STRING
- REM_FILE:STRING
- LOC_FILE:STRING
- @ENABLE:BOOL

OUT
- RESULT:INT

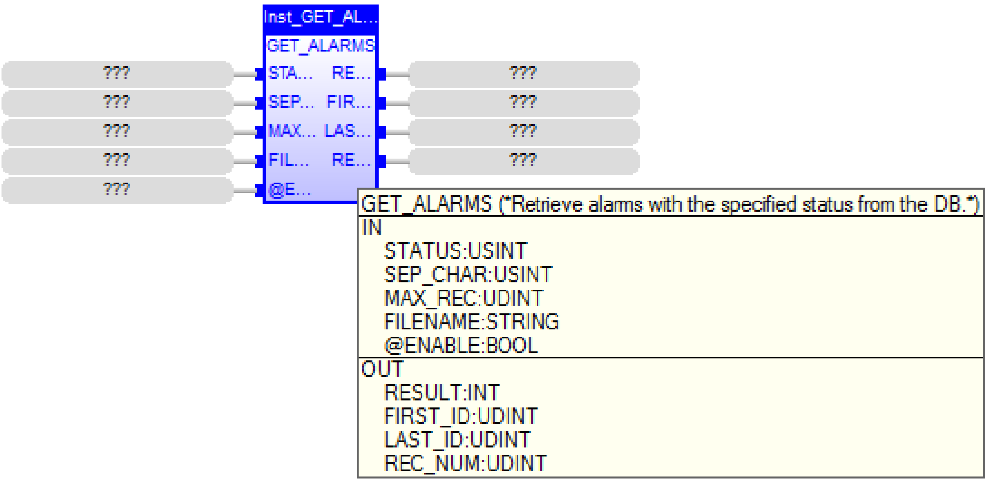
The FTP_PUT FB uploads a file, by means of the FTP protocol.

When first called, the FB runs a process which starts performing the upload; on subsequent calls, it only checks if the process has finished its job.

```
The FB has the following input parameters:
- HOST     : IP address or host name of the FTP server
- PORT     : TCP port for the FTP protocol (normally: 21)
- USERNAME : username for authentication
- PASSWORD : password for authentication
- REM_FILE : name of the file (with path) on the remote server
- LOC_FILE : name of the file (with path) on the local device
- @ENABLE  : TRUE  -> FB is executed
             FALSE -> FB is skipped
```

```
The FB has the following output parameter:
- RESULT : -2, when called with ENABLE=FALSE
           -1, in case of any failure
            0, if the process is still running
            1, if the process has successfully finished.
```

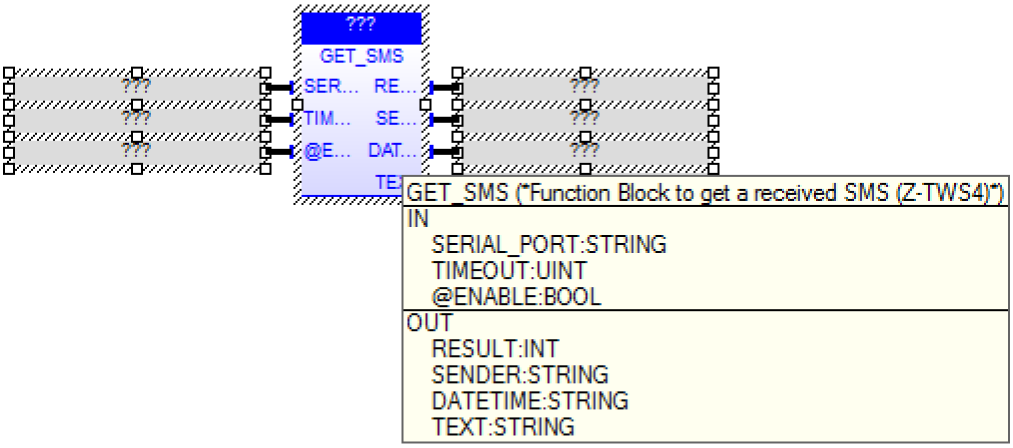
17.1.4 GET_ALARMS



GET_ALARMS ("Retrieve alarms with the specified status from the DB.")
IN
STATUS:USINT
SEP_CHAR:USINT
MAX_REC:UDINT
FILENAME:STRING
@ENABLE:BOOL
OUT
RESULT:INT
FIRST_ID:UDINT
LAST_ID:UDINT
REC_NUM:UDINT

```
This FB retrieves all alarm records with the specified status from the DB;
the records are written as lines into the specified file.

INPUTS:
- STATUS : this parameter is handled as a "negative bitmask", meaning that this
FB will provide alarm records such that:
   (alarms.stat & STATUS) = 0, where:
  alarms.stat: DB field
  STATUS: this parameter
- SEP_CHAR : the field separator to be used in the file lines; possible values:
" "|","|";"
- MAX_REC : the maximum number of records (lines) to be retrieved
- FILENAME : the file name, with absolute path
- @ENABLE: TRUE  -> FB is executed
           FALSE -> FB is skipped
           the parameter is set to FALSE by the FB at the end of execution

OUTPUTS:
- RESULT: the FB result; possible values are:
   0: FB still running
   1: FB successfully executed
  -1: FB execution failed
  -2: FB execution timeout
- FIRST_ID : the id of the first record retrieved; this value shall be passed as
an argument to the SET_ALARMS_STAT FB
- LAST_ID : the id of the last record retrieved; this value shall be passed as
an argument to the SET_ALARMS_STAT FB
- REC_NUM : the number of records retrieved
```

17.1.5 GET_SMS



GET_SMS (*Function Block to get a received SMS (Z-TWS4)*)
IN
SERIAL_PORT:STRING
TIMEOUT:UINT
@ENABLE:BOOL
OUT
RESULT:INT
SENDER:STRING
DATETIME:STRING
TEXT:STRING

The GET_SMS FB gets an SMS, previously received, by means of a GSM modem; once read, the SMS is deleted.

When first called, the FB runs a process which starts getting the SMS; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

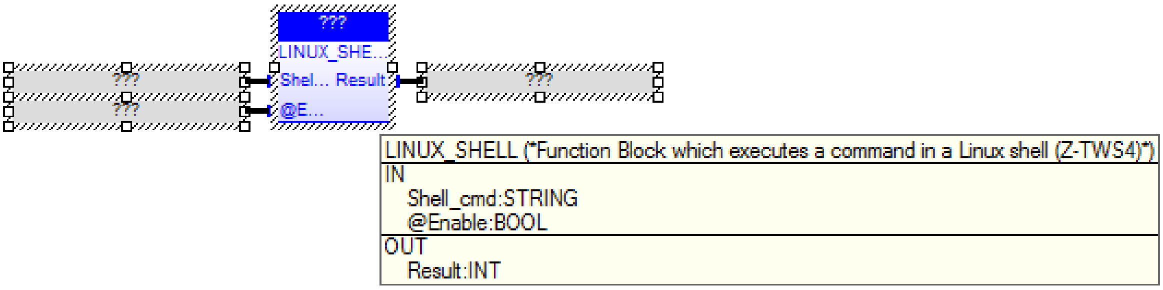
- SERIAL_PORT : this parameter is not used (it is still present only for compatibility reasons); it can be set to '' (empty string)
- TIMEOUT : timeout, in seconds
- @ENABLE : TRUE -> FB is executed
  FALSE -> FB is skipped

The FB has the following output parameters:

- RESULT : -2, when called with ENABLE=FALSE
  -1, in case of any failure
  0, if the process is still running
  1, if the process has successfully finished and an SMS has been found
  2, if timeout has expired
  3, if the process has successfully finished but no SMS has been found
  4, if PPP is active, on Z-MINIRTU
  5, if MODEM_RESET FB is running
- SENDER : SMS sender (only if RESULT=1)
- DATETIME : Date/time of SMS reception (only if RESULT=1)
- TEXT : SMS text (only if RESULT=1)

Please note that the GET_SMS FB can't be successfully executed while the PPP connection is active, on Z-MINIRTU.

17.1.6 LINUX_SHELL



```
LINUX_SHELL (*Function Block which executes a command in a Linux shell (Z-TWS4)*)
IN
   Shell_cmd:STRING
   @Enable:BOOL
OUT
   Result:INT
```

Seneca FB for access to the Linux Shell.
Max 255 command line characters.
For access to the output use "> output.txt"

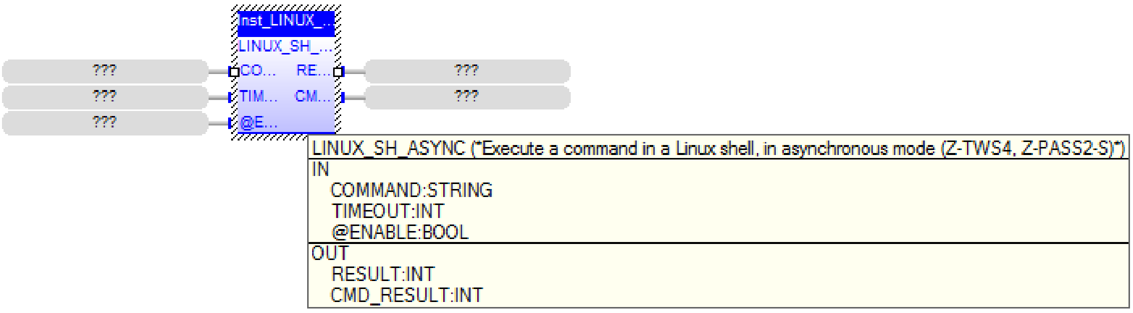
```
Shell_cmd : string command
@Enable   : if true execute the shell command
Result    : the return value of the "system" C function
```

Usage Example:

"ls > output1.txt"

create the directory list into output1.txt

17.1.7 LINUX_SH_ASYNC



```
LINUX_SH_ASYNC (*Execute a command in a Linux shell, in asynchronous mode (Z-TWS4, Z-PASS2-S)*)
IN
   COMMAND:STRING
   TIMEOUT:INT
   @ENABLE:BOOL
OUT
   RESULT:INT
   CMD_RESULT:INT
```

The LINUX_SH_ASYNC FB executes a command in a Linux shell, in asynchronous mode.

When first called, the FB runs a Linux shell process which starts performing the command; on subsequent calls, it only checks if the process has finished the command execution.

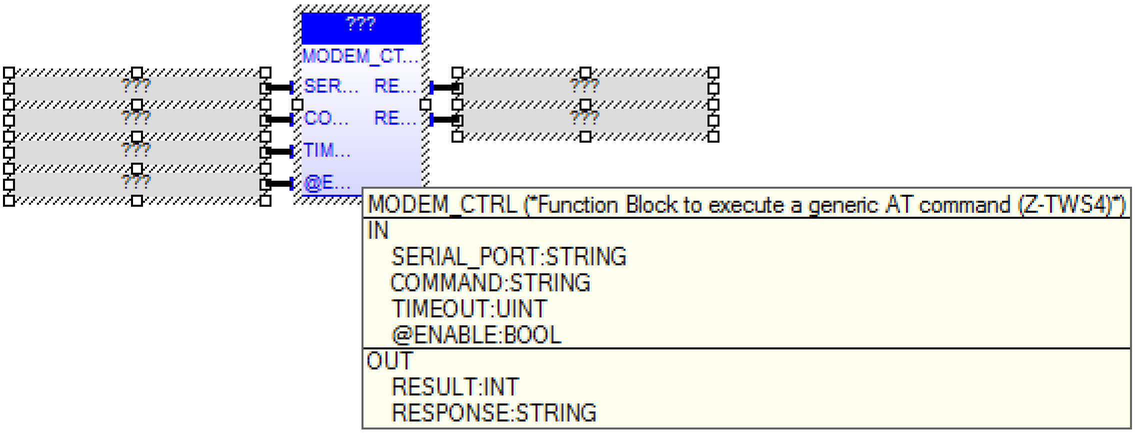
The FB has the following input parameters:

```
- COMMAND : the command to be executed
- TIMEOUT : timeout, in seconds
- @ENABLE : TRUE  -> FB is executed
            FALSE -> FB is skipped
```

The FB has the following output parameters:

```
- RESULT : -2, when called with ENABLE=FALSE
           -1, in case of any failure
            0, if the process is still running
            1, if the process has successfully finished
            2, if timeout has expired
- CMD_RESULT: command exit code
```

17.1.8 MODEM_CTRL



MODEM_CTRL (*Function Block to execute a generic AT command (Z-TWS4)*)
IN
SERIAL_PORT:STRING
COMMAND:STRING
TIMEOUT:UINT
@ENABLE:BOOL
OUT
RESULT:INT
RESPONSE:STRING

The MODEM_CTRL FB sends a generic AT command to the GSM modem and receives the corresponding response.

When first called, the FB runs a process which starts sending the command; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

```
- SERIAL_PORT : this parameter is not used (it is still present only for
compatibility reasons); it can be set to '' (empty string)
- COMMAND     : AT command to be executed
- TIMEOUT     : timeout, in seconds
- @ENABLE     : TRUE  -> FB is executed
                FALSE -> FB is skipped
```

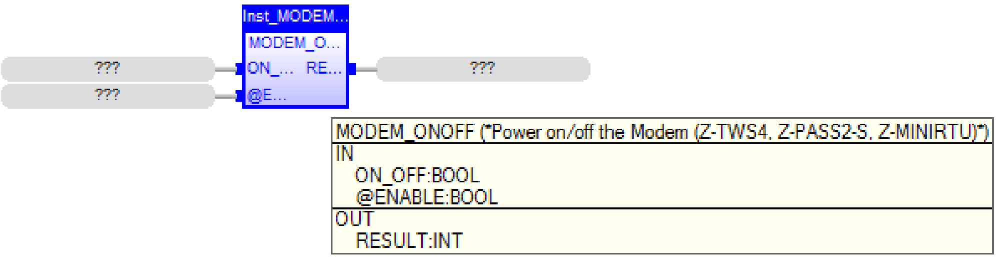
The FB has the following output parameters:

```
- RESULT   : -2, when called with ENABLE=FALSE
             -1, in case of any failure
              0, if the process is still running
              1, if the process has successfully finished
                 (NOTE: this only means that the command was successfully sent
and the response was successfully received;
                 it does not necessarily mean that the AT command was
successfully executed;
                 in other words, it is up to the application to tell if the
response means success or failure)
              2, if timeout has expired
              4, if PPP is active, on Z-MINIRTU
              5, if MODEM_RESET FB is running
- RESPONSE : the response to the AT command, as sent by the modem; it can
contain more lines, separated by a '\' character;
if the whole response is longer than 255 characters, it will be truncated.
```

Please note that the MODEM_CTRL FB can't be successfully executed while the PPP

```
connection is active, on Z-MINIRTU.

This FB cannot be used (i.e.: it won't work) in the following situations:
- if modem is set to send numeric result codes (see "ATV" command)
- for commands using a prompt (e.g.: "AT+CMGS" command)
- for call-handling commands (e.g.: "ATD", "ATA", "ATH").
```

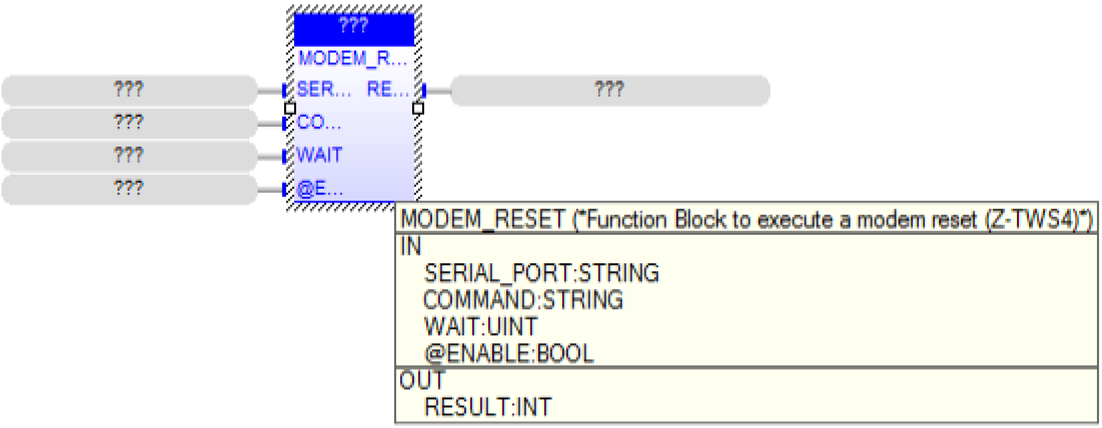
17.1.9 MODEM_ONOFF



```
MODEM_ONOFF (*Power on/off the Modem (Z-TWS4, Z-PASS2-S, Z-MINIRTU)*)
IN
   ON_OFF:BOOL
   @ENABLE:BOOL
OUT
   RESULT:INT
```

```
This FB permits to control the power ON/OFF digital input of the MODEM.

The params are :

ON_OFF : if True power-up the modem
@ENABLE : if True the FB is executed

RESULT : -2 FB executed with @ENABLE set to False
-1 Error
0 operation not completed
+1 OK
+2 modem is already ON/OFF
```

17.1.10 MODEM_RESET



```
MODEM_RESET (*Function Block to execute a modem reset (Z-TWS4)*)
IN
   SERIAL_PORT:STRING
   COMMAND:STRING
   WAIT:UINT
   @ENABLE:BOOL
OUT
   RESULT:INT
```

```
The MODEM_RESET FB sends an AT reset command to the GSM modem and waits for a
specified time.
```

When first called, the FB runs a process which starts sending the command; on subsequent calls, it only checks if the process has finished its job.

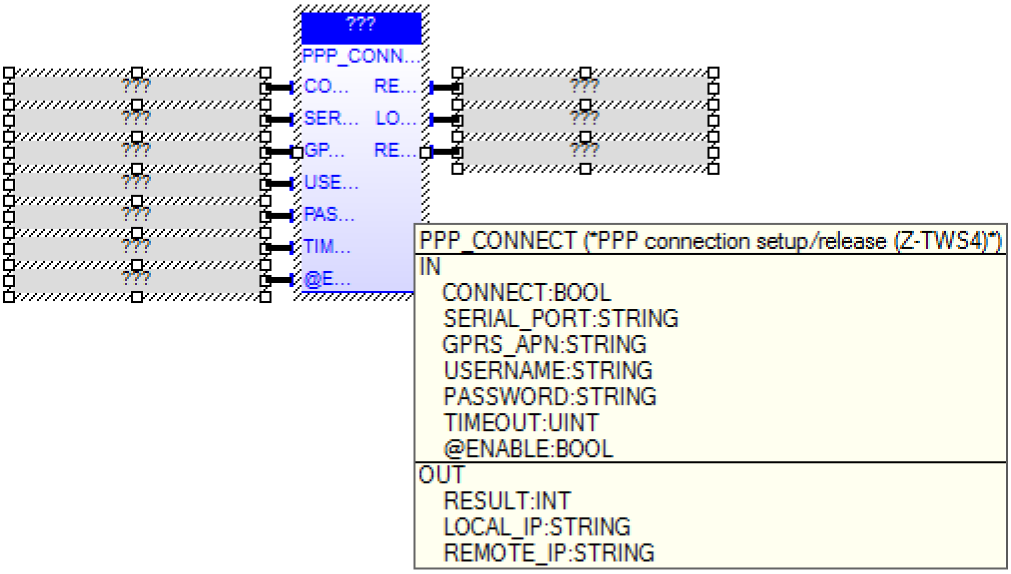
The FB has the following input parameters:

```
- SERIAL_PORT : this parameter is not used (it is still present only for
compatibility reasons); it can be set to '' (empty string)
- COMMAND     : reset AT command to be sent;
                if left empty, the "AT+CFUN=1,1" command will be sent
- WAIT        : wait duration, in seconds, after sending the command;
                valid values are: [30..300]
- @ENABLE     : TRUE  -> FB is executed
                FALSE -> FB is skipped
```

```
The FB has the following output parameter:
- RESULT : -2, when called with ENABLE=FALSE
           -1, in case of any failure
            0, if the process is still running
            1, if the process has successfully finished
            2, if timeout has expired (timeout = WAIT + 5 seconds)
            4, if PPP is active, on Z-MINIRTU
            5, if MODEM_RESET FB is already running
```

Please note that the MODEM_RESET FB can't be successfully executed while the PPP connection is active, on Z-MINIRTU.
Also note that, when MODEM_RESET FB is running, all other "modem related" FBs (PPP_CONNECT, SEND_SMS, GET_SMS, MODEM_CTRL and MODEM_RESET itself) are rejected.

17.1.11 PPP_CONNECT



PPP_CONNECT (*PPP connection setup/release (Z-TWS4)*)
IN
CONNECT:BOOL
SERIAL_PORT:STRING
GPRS_APN:STRING
USERNAME:STRING
PASSWORD:STRING
TIMEOUT:UINT
@ENABLE:BOOL
OUT
RESULT:INT
LOCAL_IP:STRING
REMOTE_IP:STRING

The PPP_CONNECT FB performs PPP connection setup or release, by means of a GPRS/UMTS modem.

When first called, it runs a process which starts the connection setup or release; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

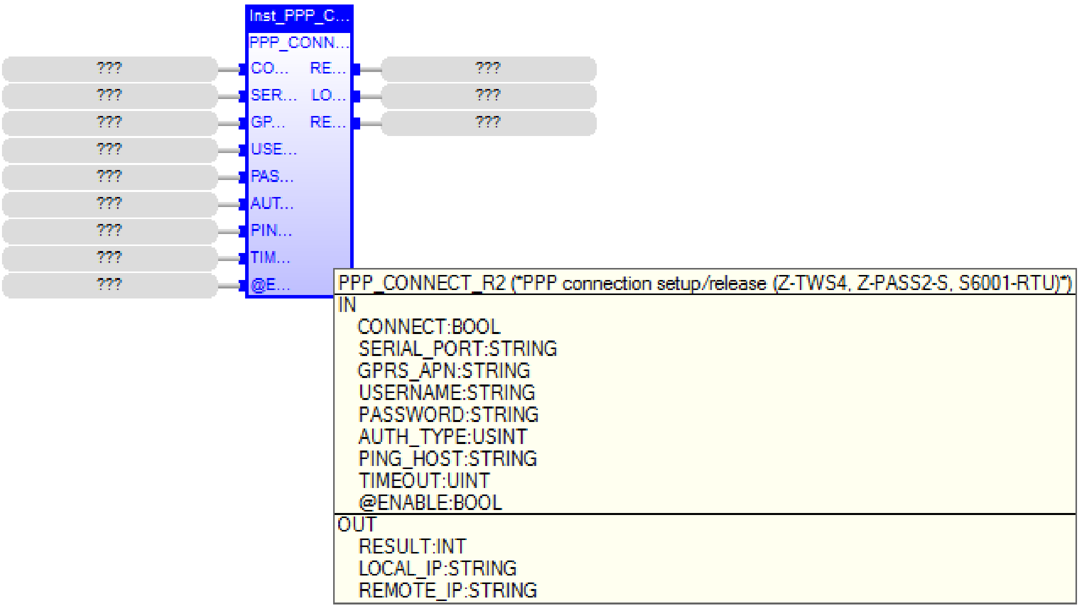
```
- CONNECT     : TRUE  -> connection setup
                FALSE -> connection release
- SERIAL_PORT : this parameter is not used (it is still present only for
compatibility reasons); it can be set to '' (empty string)
- GPRS_APN    : GPRS Access Point Name (as given by the mobile operator);
                if this parameter is left empty, "Automatic APN" functionality
is activated
- USERNAME    : username required for authentication
                (it can be empty, if authentication is not required);
                not used with "Automatic APN" functionality
- PASSWORD    : password required for authentication
                (it can be empty, if authentication is not required)
                not used with "Automatic APN" functionality
- TIMEOUT     : timeout, in seconds
- @ENABLE     : TRUE  -> FB is executed
                FALSE -> FB is skipped
```

When CONNECT=FALSE, GPRS_APN, USERNAME and PASSWORD parameters can be empty.

The FB has the following output parameters:

```
- RESULT    : -2, when called with ENABLE=FALSE
              -1, in case of any failure
               0, if the process is still running
               1, if the process has successfully finished
               2, if timeout has expired
               5, if MODEM_RESET FB is running
- LOCAL_IP  : IP address assigned to the PPP network interface (only if
RESULT=1, when CONNECT=TRUE)
- REMOTE_IP : IP address of the remote host (set as default gateway) (only if
RESULT=1, when CONNECT=TRUE)
```

17.1.12 PPP_CONNECT_R2



PPP_CONNECT_R2 (*PPP connection setup/release (Z-TWS4, Z-PASS2-S, S6001-RTU)*)
IN
CONNECT:BOOL
SERIAL_PORT:STRING
GPRS_APN:STRING
USERNAME:STRING
PASSWORD:STRING
AUTH_TYPE:USINT
PING_HOST:STRING
TIMEOUT:UINT
@ENABLE:BOOL
OUT
RESULT:INT
LOCAL_IP:STRING
REMOTE_IP:STRING

The PPP_CONNECT_R2 FB performs PPP connection setup or release, by means of a GPRS/UMTS modem.

When first called, it runs a process which starts the connection setup or release; on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

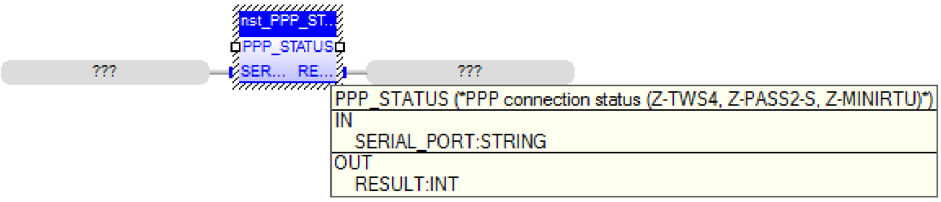
```
- CONNECT     : TRUE  -> connection setup
                FALSE -> connection release
- SERIAL_PORT : this parameter is not used (it is still present only for
compatibility reasons); it can be set to '' (empty string)
- GPRS_APN    : GPRS Access Point Name (as given by the mobile network
operator); if this parameter is left empty, "Automatic APN" functionality is
activated
- USERNAME    : username required for authentication
                (it can be empty, if authentication is not required);
                not used with "Automatic APN" functionality
- PASSWORD    : password required for authentication
                (it can be empty, if authentication is not required);
                not used with "Automatic APN" functionality
- AUTH_TYPE   : authentication type:
                0 : None
                1 : CHAP/PAP
                2 : CHAP only
                3 : PAP only
                not used with "Automatic APN" functionality
- PING_HOST   : IP address or Host Name used to check that PPP connectivity is
available, running ping test;
                if this parameter is left empty, ping test is not performed
- TIMEOUT     : timeout, in seconds
- @ENABLE     : TRUE  -> FB is executed
                FALSE -> FB is skipped
```

When CONNECT=FALSE, GPRS_APN, USERNAME, PASSWORD and PING_HOST parameters can be empty.

The FB has the following output parameters:

```
- RESULT    : -2, when called with ENABLE=FALSE
              -1, in case of any failure
               0, if the process is still running
               1, if the process has successfully finished
               2, if timeout has expired
               5, if MODEM_RESET FB is running
- LOCAL_IP  : IP address assigned to the PPP network interface (only if
RESULT=1, when CONNECT=TRUE)
- REMOTE_IP : IP address of the remote host (set as default gateway) (only if
RESULT=1, when CONNECT=TRUE)
```

17.1.13 PPP_STATUS



```
PPP_STATUS (*PPP connection status (Z-TWS4, Z-PASS2-S, Z-MINIRTU)*)
IN
   SERIAL_PORT:STRING
OUT
   RESULT:INT
```

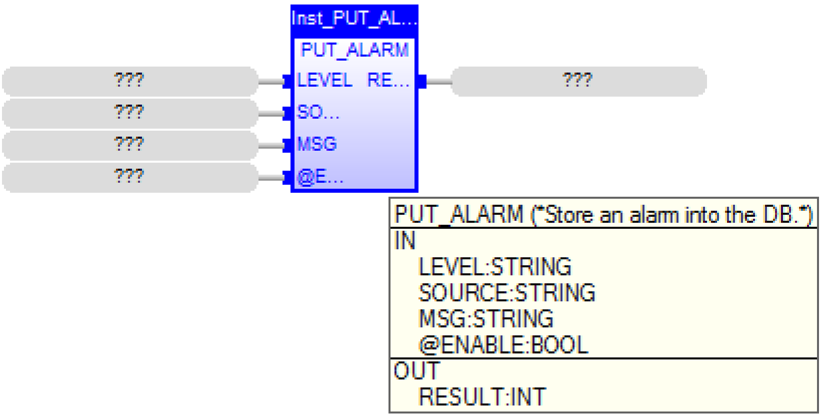
The PPP_STATUS FB returns PPP connection status.

The FB has the following input parameters:
- SERIAL_PORT : this parameter is not used (it is still present only for compatibility reasons); it can be set to '' (empty string)

The FB has the following output parameters:

```
- RESULT     :  0, PPP DISCONNECTED
                1, PPP CONNECTED
                2, PPP CONNECTING
                3, PPP DISCONNECTING
```

17.1.14 PUT_ALARM



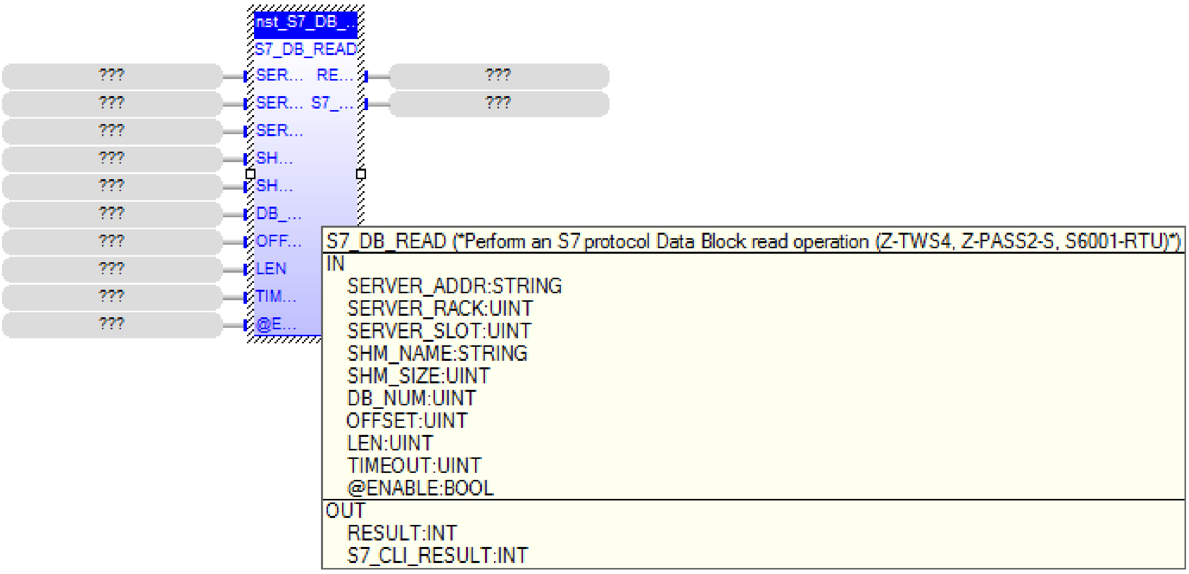
```
PUT_ALARM (*Store an alarm into the DB.*)
IN
   LEVEL:STRING
   SOURCE:STRING
   MSG:STRING
   @ENABLE:BOOL
OUT
   RESULT:INT
```

This FB stores an alarm record into the DB;
the "index" and "timestamp" fields are set by the FB;
the "status" field is set to 0 by the FB.
The FB is also responsible for keeping the DB size (number of records) under a specified limit (e.g.: 1000).

INPUTS:
- LEVEL: a string representing the alarm/event level (e.g.: "INFO") (max_len=10);
  possible values are defined by the application

```
- SOURCE: a string representing the alarm/event source (e.g.: "GRP1")
(max_len=10);
  possible values are defined by the application
- MSG: the text message of the alarm (max_len=255)
- @ENABLE: TRUE  -> FB is executed
           FALSE -> FB is skipped
           the parameter is set to FALSE by the FB at the end of execution

OUTPUTS:
- RESULT: the FB result; possible values are:
   0: FB still running
   1: FB successfully executed
  -1: FB execution failed
  -2: FB execution timeout
```

17.1.15 S7_DB_READ



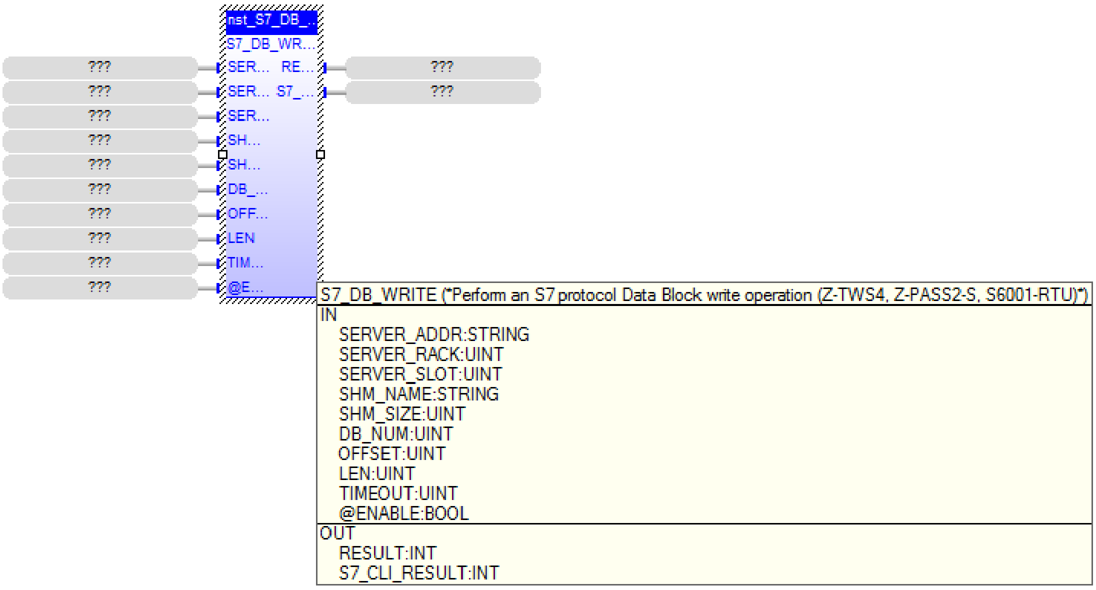
S7_DB_READ (*Perform an S7 protocol Data Block read operation (Z-TWS4, Z-PASS2-S, S6001-RTU)*)

```
IN
   SERVER_ADDR:STRING
   SERVER_RACK:UINT
   SERVER_SLOT:UINT
   SHM_NAME:STRING
   SHM_SIZE:UINT
   DB_NUM:UINT
   OFFSET:UINT
   LEN:UINT
   TIMEOUT:UINT
   @ENABLE:BOOL
OUT
   RESULT:INT
   S7_CLI_RESULT:INT
```

This FB performs an S7 protocol Data Block read operation.
It connects to the specified S7 server IP address, rack and slot, performs the operation and then disconnects.
The data read are written to the Straton shared-memory specified in the SHM_NAME parameter.

```
INPUTS:
- SERVER_ADDR: the S7 server IP address
- SERVER_RACK: the S7 server rack number
- SERVER_SLOT: the S7 server slot number
- SHM_NAME: name of the Straton shared-memory which the data are written to
- SHM_SIZE: size of the Straton shared-memory which the data are written to
- DB_NUM: the number of the Data Block to be read
- OFFSET: start offset for the read operation in the Data Block
- LEN: number of bytes to be read
- TIMEOUT: timeout for the FB execution, in seconds
- @ENABLE: TRUE -> FB is executed
FALSE -> FB is skipped
the parameter is set to FALSE by the FB at the end of execution

OUTPUTS:
- RESULT: the FB result; possible values are:
   0: FB still running
   1: FB successfully executed
  -1: FB execution failed
  -2: FB execution timeout
- S7_CLI_RESULT: the S7 Client result; possible values are:
   0: no failure
  -1: invalid arguments failure
  -2: initialization failure (e.g.: error opening the shared-memory)
  -3: connection failure
  -4: read operation failure
```

17.1.16 S7_DB_WRITE



S7_DB_WRITE (*Perform an S7 protocol Data Block write operation (Z-TWS4, Z-PASS2-S, S6001-RTU)*)

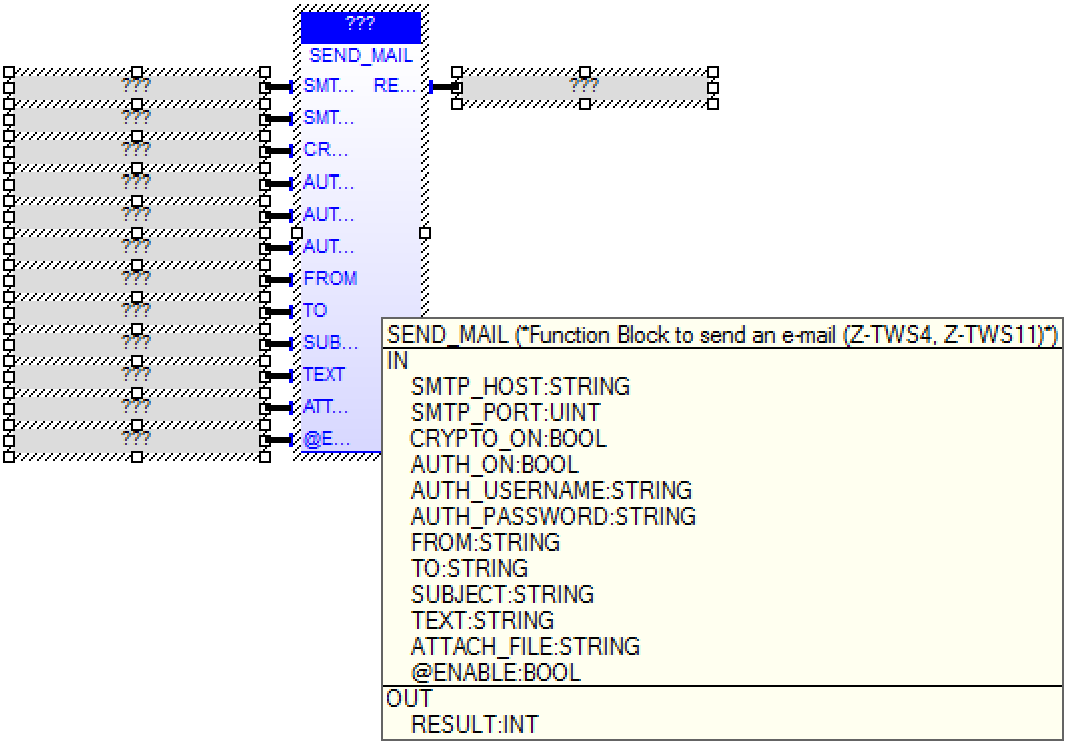
```
IN
   SERVER_ADDR:STRING
   SERVER_RACK:UINT
   SERVER_SLOT:UINT
   SHM_NAME:STRING
   SHM_SIZE:UINT
   DB_NUM:UINT
   OFFSET:UINT
   LEN:UINT
   TIMEOUT:UINT
   @ENABLE:BOOL
OUT
   RESULT:INT
   S7_CLI_RESULT:INT
```

This FB performs an S7 protocol Data Block write operation.
It connects to the specified S7 server IP address, rack and slot, performs the operation and then disconnects.
The data to be written are read from the Straton shared-memory specified in the SHM_NAME parameter.

```
INPUTS:
- SERVER_ADDR: the S7 server IP address
- SERVER_RACK: the S7 server rack number
- SERVER_SLOT: the S7 server slot number
- SHM_NAME: name of the Straton shared-memory which the data are read from
- SHM_SIZE: size of the Straton shared-memory which the data are read from
- DB_NUM: the number of the Data Block to be written
- OFFSET: start offset for the write operation in the Data Block
- LEN: number of bytes to be written
- TIMEOUT: timeout for the FB execution, in seconds
- @ENABLE: TRUE -> FB is executed
```

```
FALSE -> FB is skipped
the parameter is set to FALSE by the FB at the end of execution

OUTPUTS:
- RESULT: the FB result; possible values are:
   0: FB still running
   1: FB successfully executed
  -1: FB execution failed
  -2: FB execution timeout
- S7_CLI_RESULT: the S7 Client result; possible values are:
   0: no failure
  -1: invalid arguments failure
  -2: initialization failure (e.g.: error opening the shared-memory)
  -3: connection failure
  -4: write operation failure
```

17.1.17 SEND_MAIL



```
SEND_MAIL (*Function Block to send an e-mail (Z-TWS4, Z-TWS11)*)
IN
   SMTP_HOST:STRING
   SMTP_PORT:UINT
   CRYPTO_ON:BOOL
   AUTH_ON:BOOL
   AUTH_USERNAME:STRING
   AUTH_PASSWORD:STRING
   FROM:STRING
   TO:STRING
   SUBJECT:STRING
   TEXT:STRING
   ATTACH_FILE:STRING
   @ENABLE:BOOL
OUT
   RESULT:INT
```

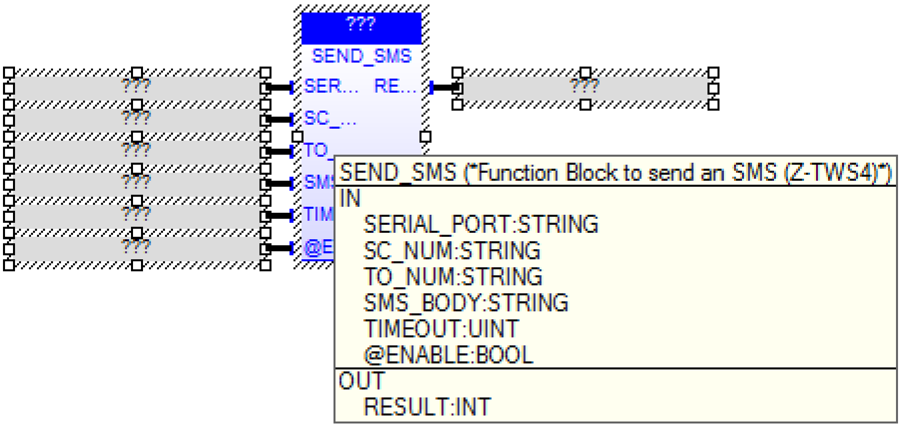
```
The SEND_MAIL FB sends an e-mail, by means of the SMTP/SMTPS protocol.

When first called, the FB runs a process which starts sending the e-mail;
on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:
- SMTP_HOST     : IP address or host name of the SMTP/SMTPS server
- SMTP_PORT     : TCP port for the SMTP/SMTPS protocol (normally: 25, for SMTP;
465, for SMTPS)
- CRYPTO_ON     : if cryptography (SSL) shall be used (FALSE -> SMTP, TRUE ->
SMTPS)
                  (CRYPTO_ON=TRUE is available only for Z-TWS4/Z-PASS2-S)
- AUTH_ON       : if authentication shall be executed
- AUTH_USERNAME : username for authentication
```

- AUTH_PASSWORD : password for authentication
- FROM : e-mail sender
- TO : e-mail recipient
  more than one recipient can be specified, using the ',' character as separator
- SUBJECT : e-mail subject
- TEXT : e-mail text
- ATTACH_FILE : name of the file (with path) to be attached to the e-mail (it can be empty)
- @ENABLE : TRUE -> FB is executed
  FALSE -> FB is skipped

The FB has the following output parameter:

- RESULT : -2, when called with ENABLE=FALSE
  -1, in case of any failure
  0, if the process is still running
  1, if the process has successfully finished.

17.1.18 SEND_SMS



SEND_SMS (*Function Block to send an SMS (Z-TWS4)*)
IN
SERIAL_PORT:STRING
SC_NUM:STRING
TO_NUM:STRING
SMS_BODY:STRING
TIMEOUT:UINT
@ENABLE:BOOL
OUT
RESULT:INT

The SEND_SMS FB sends an SMS, by means of a GSM modem.

When first called, it runs a process which starts sending the SMS;
on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameters:

- SERIAL_PORT : this parameter is not used (it is still present only for compatibility reasons); it can be set to '' (empty string)
- SC_NUM : SMS Service Center (as given by the mobile operator) (it can be empty, if the SC number is already set on the modem/SIM)
- TO_NUM : recipient number
- SMS_BODY : SMS text
- TIMEOUT : timeout, in seconds
- @ENABLE : TRUE -> FB is executed
  FALSE -> FB is skipped

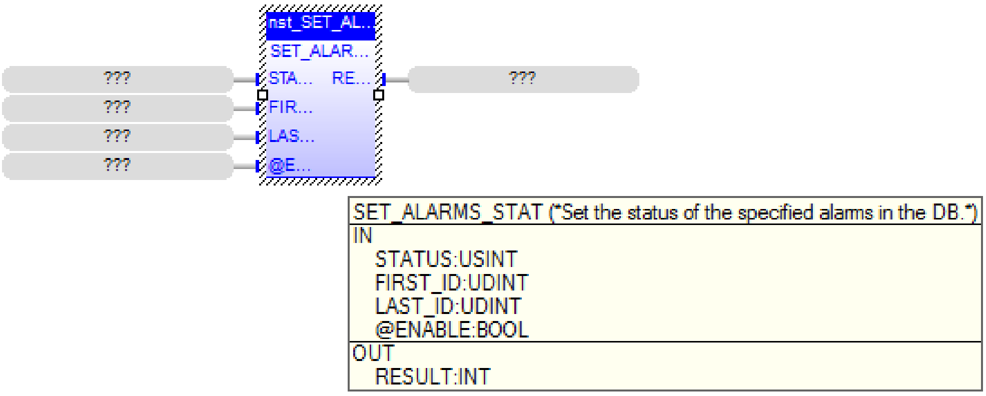
The FB has the following output parameter:

- RESULT : -2, when called with ENABLE=FALSE
  -1, in case of any failure
  0, if the process is still running
  1, if the process has successfully finished
  2, if timeout has expired

            4, if PPP is active, on Z-MINIRTU
            5, if MODEM_RESET FB is running

Please note that the SEND_SMS FB can't be successfully executed while the PPP connection is active, on Z-MINIRTU.

17.1.19 SET_ALARMS_STAT



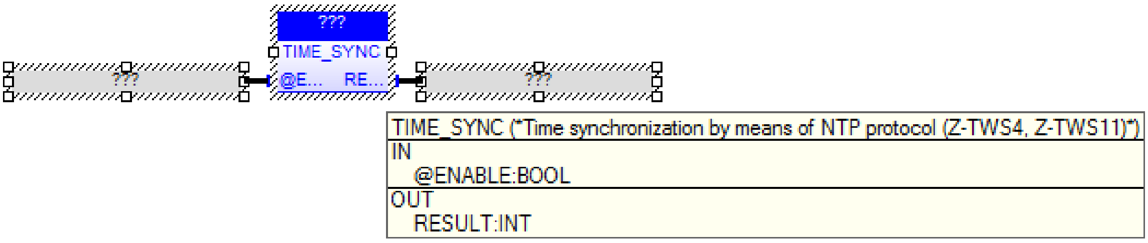
SET_ALARMS_STAT (*Set the status of the specified alarms in the DB.*)
IN
   STATUS:USINT
   FIRST_ID:UDINT
   LAST_ID:UDINT
   @ENABLE:BOOL
OUT
   RESULT:INT

This FB sets the value of the "status" field for the alarm records specified by the passed arguments.

INPUTS:
- STATUS : this parameter is handled as a bitmask, meaning that the status of the relevant alarm records will be set as:
  alarms.stat = (alarms.stat | STATUS), where:
  alarms.stat: DB field
  STATUS: this parameter
- FIRST_ID : the id of the first record retrieved by the GET_ALARMS FB
- LAST_ID : the id of the last record retrieved by the GET_ALARMS FB
- @ENABLE: TRUE -> FB is executed
           FALSE -> FB is skipped
           the parameter is set to FALSE by the FB at the end of execution

OUTPUTS:
- RESULT: the FB result; possible values are:
   0: FB still running
   1: FB successfully executed
  -1: FB execution failed
  -2: FB execution timeout

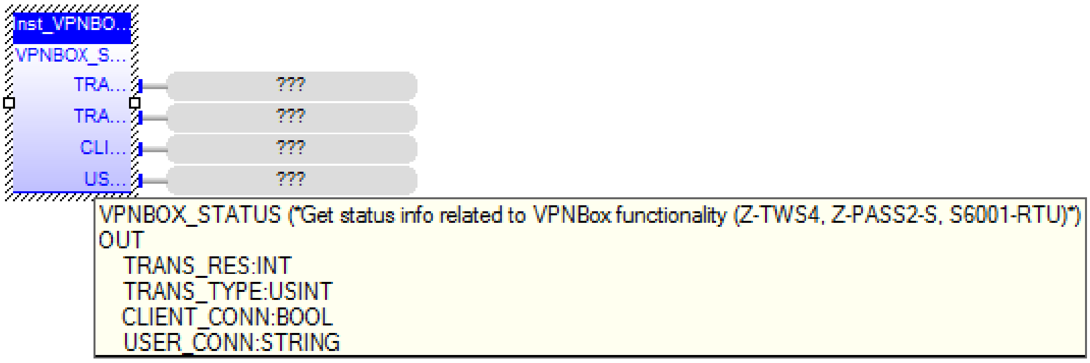
17.1.20 TIME_SYNC



TIME_SYNC (*Time synchronization by means of NTP protocol (Z-TWS4, Z-TWS11)*)
IN
@ENABLE:BOOL
OUT
RESULT:INT

```
The TIME_SYNC FB performs time synchronization, by means of the NTP protocol.

When first called, the FB runs a process which starts performing the
synchronization;
on subsequent calls, it only checks if the process has finished its job.

The FB has the following input parameter:

- @ENABLE : TRUE  -> FB is executed
            FALSE -> FB is skipped

The FB has the following output parameter:
- RESULT : -2, when called with ENABLE=FALSE
           -1, in case of any failure
            0, if the process is still running
            1, if the process has successfully finished.
```

17.1.21 VPNBOX_STATUS



VPNBOX_STATUS (*Get status info related to VPNBox functionality (Z-TWS4, Z-PASS2-S, S6001-RTU)*)
OUT
TRANS_RES:INT
TRANS_TYPE:USINT
CLIENT_CONN:BOOL
USER_CONN:STRING

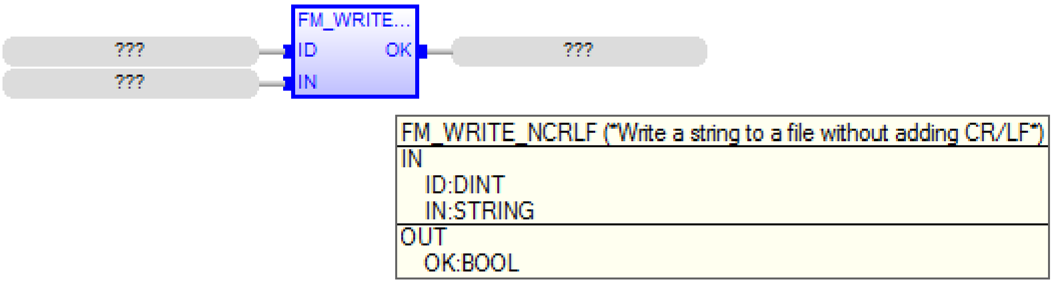
```
This FB provides information about the VPN Box functionality.

INPUTS:
none

OUTPUTS:
- TRANS_RES : the result of the last VPN Box transaction performed by the CPU;
```

possible values:
 -2: No response from VPN Box
 -1: Invalid response from VPN Box
 0: OK
 3: Wrong password
 7: License limit reached
 201: Generic error
 202: VPN Box not configured
 1000: No transaction has been performed (e.g.: VPN Box functionality is disabled)
other: Unexpected response

- TRANS_TYPE : the type of the last VPN Box transaction performed by the CPU; possible values:
  0: None (no transaction performed)
  1: Register
  2: Poll
- CLIENT_CONN : flag telling if a VPN Client is connected (meaningful only for "Point-to-Point" VPN Box)
  0: no VPN client is connected
  1: a VPN client is connected
- USER_CONN : if a VPN Client is connected, this parameter provides the authenticated username; otherwise, it is an empty string ('') (meaningful only for "Point-to-Point" VPN Box)

17.2 Functions

17.2.1 FM_WRITE_NCRLF



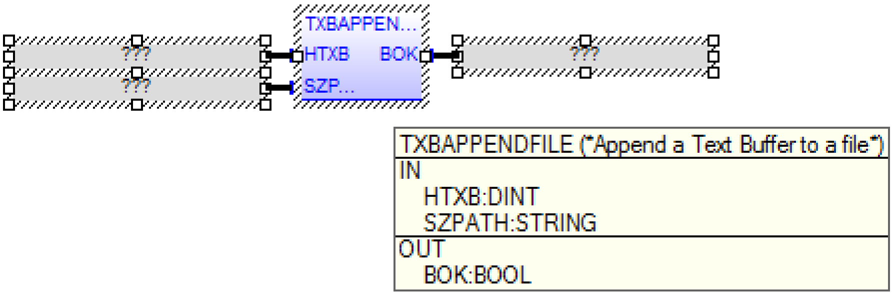
FM_WRITE_NCRLF (*Write a string to a file without adding CR/LF*)
IN
 ID:DINT
 IN:STRING
OUT
 OK:BOOL

Same behaviour as FM_WRITE but without inserting final CR-LF

Input parameters:
- ID: id of the file (already open)
- IN: string to write into the file

Output parameters:
- OK: boolean result value: (TRUE:success, FALSE:failure)

17.2.2 TXBAPPENDFILE



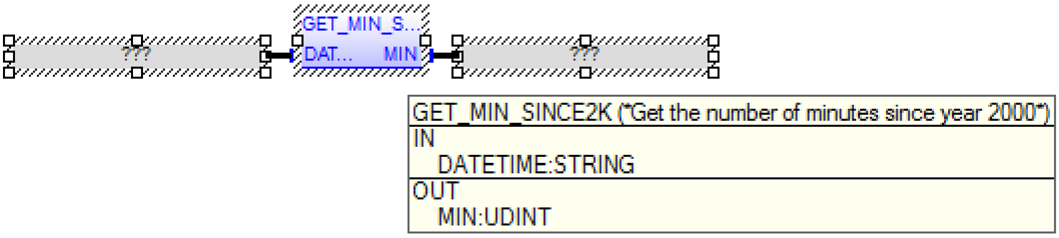
TXBAPPENDFILE (*Append a Text Buffer to a file*)
IN
HTXB:DINT
SZPATH:STRING
OUT
BOK:BOOL

Append a Text Buffer to a file (without reloading the file).

Input parameters
- HTXB: Text Buffer handle
- SZPATH: file absolute path

Output parameters
- BOK: boolean result value: (TRUE:success, FALSE:failure)

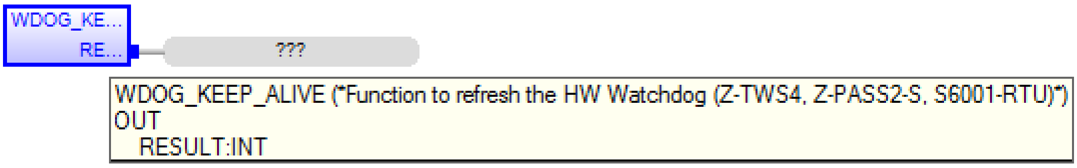
17.2.3 GET_MIN_SINCE2K



GET_MIN_SINCE2K (*Get the number of minutes since year 2000*)
IN
DATETIME:STRING
OUT
MIN:UDINT

This function returns the current number of minutes since January 1, 2000 0:00:00, if DATETIME is empty or DATETIME is not a valid date/time; otherwise, it returns the number of minutes since January 1, 2000 0:00:00, corresponding to DATETIME.
DATETIME shall have the following format:
"dd/mt/yyyy hh:mm:ss"

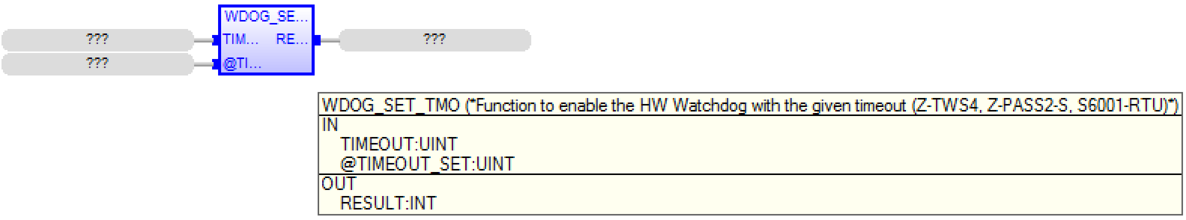
17.2.4 WDOG_KEEP_ALIVE



WDOG_KEEP_ALIVE (*Function to refresh the HW Watchdog (Z-TWS4, Z-PASS2-S, S6001-RTU)*)
OUT
RESULT:INT

```
This function restarts the HW Watchdog timer.
NOTICE: once enabled, the HW Watchdog cannot be disabled; the WDOG_KEEP_ALIVE
function shall be called to restart the timer; if timeout elapses, an HW reboot
is triggered.

To let this function actually work, the "WATCHDOG/Enable" parameter in the CPU
configuration shall be set to "OFF"; otherwise, the function will return the -2
value (see below).

INPUTS:
none

OUTPUTS:
- RESULT: the function result; possible values are:
    0: OK
   -1: watchdog setting failed (WDOG_SET_TMO function has not been called or
failed)
   -2: watchdog controlled by system ("WATCHDOG/Enable" parameter set to "ON")
   -3: watchdog keep-alive failed
```

17.2.5 WDOG_SET_TMO



WDOG_SET_TMO (*Function to enable the HW Watchdog with the given timeout (Z-TWS4, Z-PASS2-S, S6001-RTU)*)
IN
TIMEOUT:UINT
@TIMEOUT_SET:UINT
OUT
RESULT:INT

```
This function enables the HW Watchdog.
NOTICE: once enabled, the HW Watchdog cannot be disabled; the WDOG_KEEP_ALIVE
function shall be called to restart the timer; if timeout elapses, an HW reboot
is triggered.

The function can be called many times; if the timeout value is the same already
set, it will do nothing; otherwise, the new timeout value will be set.
```

```
To let this function actually work, the "WATCHDOG/Enable" parameter in the CPU
configuration shall be set to "OFF"; otherwise, the function will return the -2
value (see below).

INPUTS:
- TIMEOUT: Watchdog timeout, in seconds; possibile values: [30..3600];
  if an out-of-range value is given, the default value 60 will be set
- @TIMEOUT_SET: at the end of the execution, this parameter will contain the
timeout value actually set (in seconds)

OUTPUTS:
- RESULT: the function result; possible values are:
   0: OK
  -1: watchdog setting failed
  -2: watchdog controlled by system ("WATCHDOG/Enable" parameter set to "ON")
```

18 Z-NET4

When using Z-TWS4/Z-PASS2-S/S6001-RTU with Modbus RTU I/O Modules, a very useful and powerful tool is provided by the Z-NET4 program suite, running on Windows PCs.

Among other things, these programs let you:

- automatically discover the I/O modules available on the bus;
- configure the CPU (Z-TWS4/Z-PASS2-S/S6001-RTU) and the I/O modules;
- automatically create a StratON project containing the I/O variables, with the Modbus tasks needed to acquire/control them; for S6001-RTU, variables corresponding to the CPU I/Os are also inserted into the project
- automatically generate code for the StratON project, performing "Remote Control Functions", such as:
    - Data Logging
    - Command and Status SMS
    - Alarm generation
- easily create custom web pages, with graphic widgets, and upload them to the CPU (these pages can be accessed on the standard HTTP [80] TCP port).

The Z-NET4 SW is available at the following link:

http://www.seneca.it/products/z-net4

Please contact Seneca to get more information about the Z-NET4 suite.

19 Access to Straton variables

The aim of this chapter is to explain how an application (typically, web-based) can access the variables of the Straton Soft-PLC running on Z-TWS4/Z-PASS2-S/S6001-RTU.

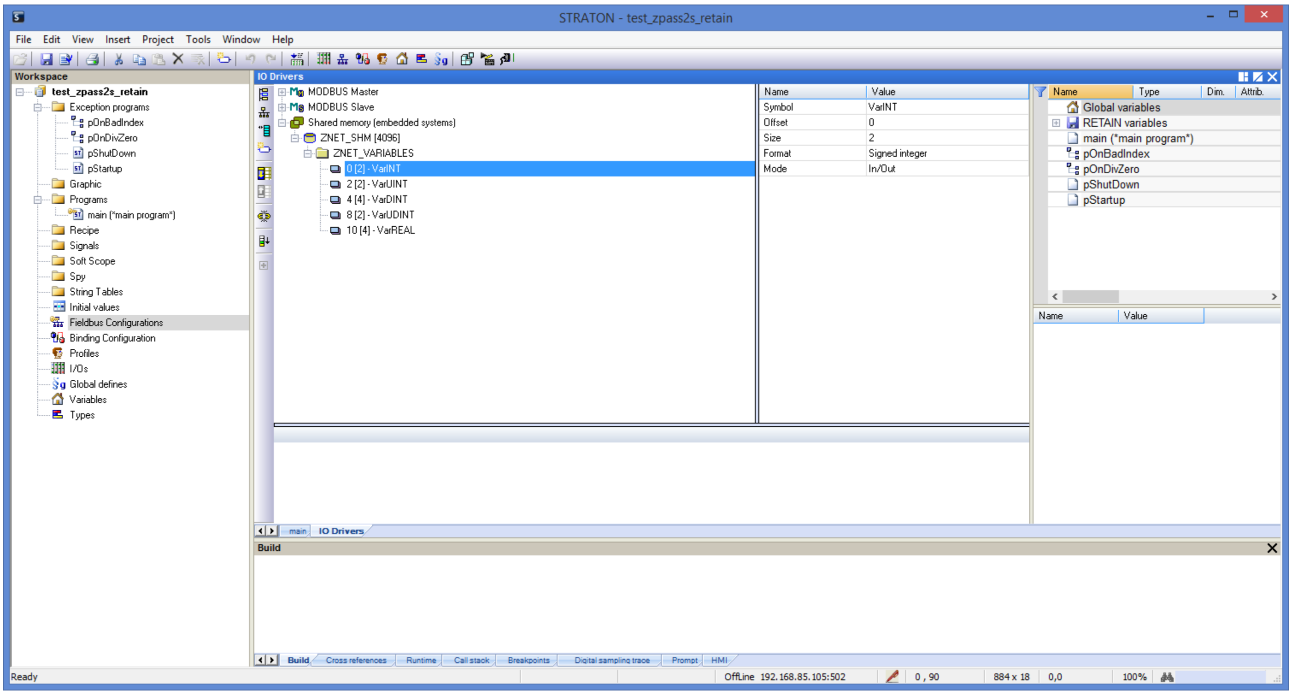
Currently, there are two ways to access Straton variables:

- direct access to Straton shared-memory
- access by means of CGI

The main differences between the two methods is that the first requires developing a C program, running on the Device, typically invoked by the *lighttpd* web server, while the second does not require any changes in the Device FW, provided that the currently supported CGIs are used.

19.1 Shared Memory

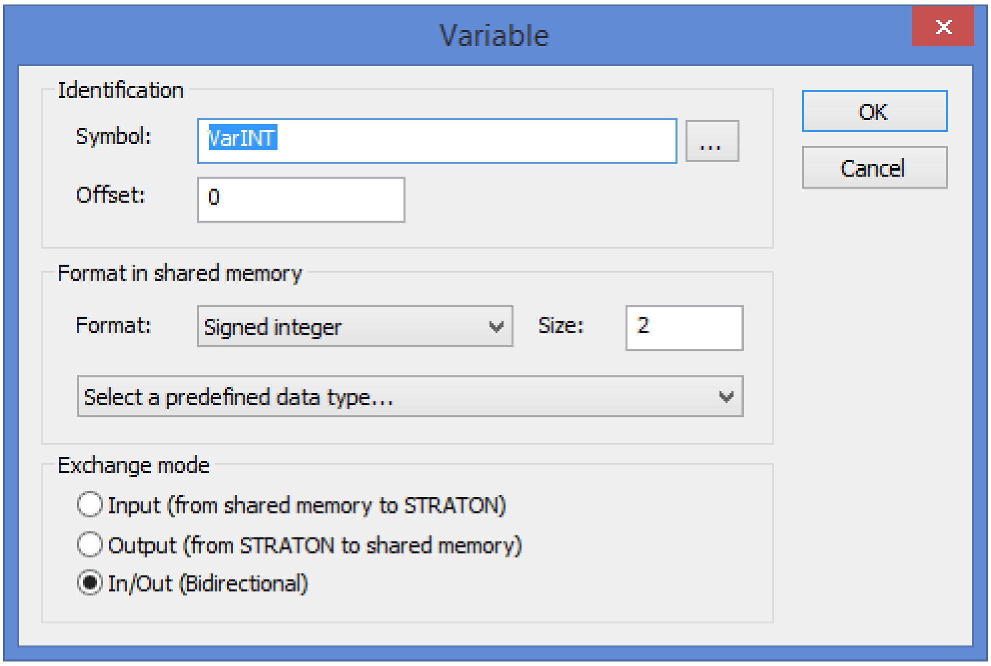
Straton Workbench lets you define a shared-memory area and tell which PLC variables shall be put in it.



Name	Value
Symbol	VarINT
Offset	0
Size	2
Format	Signed integer
Mode	In/Out

For each variable in the shared-memory, the Workbench lets you define the following properties:

- *Symbol*: the name of a Straton variable defined elsewhere (Global Variables, Retain Variables etc.)
- *Offset*: the offset in the shared-memory
- *Size*: the variable size, in bytes
- *Format*: the kind of variable, i.e. “signed integer”
- *Mode*: if the variable is an *Input*, an *Output* or an *In/Out* (from the Straton point of view)



Identification

Symbol: VarINT

Offset: 0

Format in shared memory

Format: Signed integer

Size: 2

Select a predefined data type...

Exchange mode

○ Input (from shared memory to STRATON)

○ Output (from STRATON to shared memory)

● In/Out (Bidirectional)

The list of variables in the shared-memory, along with their properties, can be saved to / loaded from a *csv* file; the format of this file is as in the following example:

```
"NAME";"OFFSET";"SIZE";"FORMAT";"MODE";"ERROR_REPORT"
"VarINT";"0";"2";"0";"2";"CPU_ErrorReport_dummy"
"VarUINT";"2";"2";"1";"2";"CPU_ErrorReport_dummy"
"VarDINT";"4";"4";"0";"2";"CPU_ErrorReport_dummy"
"VarUDINT";"8";"4";"1";"2";"CPU_ErrorReport_dummy"
"VarREAL";"12";"4";"2";"2";"CPU_ErrorReport_dummy"
```

19.2 C program example

In this paragraph, an example is given of a simple C program which can be used to access a shared-memory.

The program arguments lets you specify:

- the shared-memory name
- the shared-memory size
- the offset, used to tell the program from which address in the shared-memory it shall start printing byte values

```
int main(int argc, char* argv[])
{
    long shmid;
    char *pMap;
    sem_t *sem;
    int i, iCpt ;

    for (i=1; i<argc; i++)
    {
        if (strcmp (argv[i], "?") == 0 || strcmp (argv[i], "/?") == 0)
        {
            printf ("Syntax:  shmtest [options]\n");
            printf ("Options:\n");
            printf ("  /name=       Named memory\n");
            printf ("  /size=       Memory size\n");
            printf ("  /offset=     Memory offset\n");

            return 0;
        }

        if (strncmp (argv[i], "/name=", 6) == 0)
        {
            strcpy (szName,  (argv[i] + 6)) ;
        }
        else if (strncmp (argv[i], "/size=", 6) == 0)
        {
            wSize = atoi (argv[i] + 6);
        }
        else if (strncmp (argv[i], "/offset=", 8) == 0)
        {
            wOffset = atoi (argv[i] + 8);
        }
    }

    shmid = shm_open(szName, O_RDWR, S_IRWXO|S_IRWXG|S_IRWXU) ;
    if (shmid < 0L)
    {
        printf("Error shm_open : <%s>\n", szName) ;
        return 0;
    }
    ftruncate(shmid, wSize) ;

    pMap = mmap(NULL, wSize, PROT_READ | PROT_WRITE, MAP_SHARED, shmid, 0);
    if (pMap == MAP_FAILED)
    {
        printf("Error mmap : <%s> size <%d>\n", szName, wSize) ;
        return 0;
    }

    sem = sem_open(szName, O_RDWR, S_IRUSR | S_IWUSR, 0);
    if (sem == SEM_FAILED)
    {
        printf("Error sem_open : <%s>\n", szName) ;
        return 0;
    }
    init_keyboard() ;

    iCpt = 0 ;
    while(_ShouldTerminate()==0)
    {
        sem_wait(sem) ;
        printf("Iteration %d\n", iCpt++) ;
        for (i=0+wOffset ; i<wSize ; i++)
        {
          printf ("%02X ", (unsigned char)pMap[i]);
          if ((i+1)%16 == 0)
            printf("\n") ;
        }
        sem_post(sem);
        usleep(100*1000) ;
        system("clear") ;
    }

    close_keyboard() ;
    munmap(pMap, wSize);
    sem_close(sem);
    close (shmid) ;

    return 0;
}
```

Note that the above code will print shared-memory byte values, without any knowledge of the variables properties.

Indeed, it is important to understand that the shared-memory contains only the variables values; the variables properties shall be retrieved, for example, by loading them from the *csv* file, shown above.

Below, some lines of code are given providing some definitions useful for variables properties handling.

```
#define VAR_NAME_MAX_LEN 50

#define VAR_MAX_NUM 100

typedef enum
{
    VAR_FORMAT_INT,
    VAR_FORMAT_UINT,
    VAR_FORMAT_FLOAT,
    VAR_FORMAT_STRING,
    VAR_FORMAT_NUM
} VAR_FORMAT_T;

const char *var_format_str[] =
{
    "integer",
    "unsigned integer",
    "float",
    "string"
};

typedef enum
{
    VAR_MODE_IN,
    VAR_MODE_OUT,
    VAR_MODE_INOUT,
    VAR_MODE_NUM
} VAR_MODE_T;

const char *var_mode_str[] =
{
    "input",
    "output",
    "input/output"
};

typedef struct VarDescrS
{
    char name[VAR_NAME_MAX_LEN+1];
    unsigned int offset;
    unsigned int size;
    VAR_FORMAT_T format;
    VAR_MODE_T mode;
} VarDescrT;

static VarDescrT *vars[VAR_MAX_NUM];
```

19.3 CGI

Another way to gain access to the Straton variables is by means of CGIs.

The variables that can be read/written by means of CGIs are those which are placed in the Straton shared-memory.

In the Device FW, a daemon is running which:

- parses the CGI requests
- reads/writes the requested variables from/to the shared-memory
- gives back the values/results in the CGI responses

Two CGIs are defined, one to read and one to write variables, as described in the following.

Both CGIs shall be inserted into HTTP POST requests.

It is important to note that, as far as the variables properties are concerned, normally the application sending the CGIs doesn't need to know the offset, size and format of a variable, while it needs to know the variables names and, possibly, the variables modes, to tell which variables can be read/written and which can only be read.

19.3.1 CGI "readVariable"

To read one variable:

request:
```
goform/readVariable?nVars=1&var1=<var_name1>
```
response:
```
#<var_name1>                <var_code1> <var_add_info1>
<var_value1>
```

Example:
request:
```
goform/readVariable?nVars=1&var1=M1_Output_1
```
response (successful case):
```
# M1_Output_1              0
1
```
response (failure case):
```
# M1_Output_1              5 Operation timeout
```

The CGI can be extended to read N variables (N>1), for example to read 2 variables:

```
goform/readVariable?nVars=2&var1=<var_name1>&var2=<var_name2>
```

The response contains N sections with the format described above.

19.3.2 CGI "writeVariable"

To write one variable:

request:
```
goform/writeVariable?nVars=1&var1=<var_name1>&value1=<var_value1>
```
response:
```
#<var_name1>                <var_code1> <var_add_info1>
```

Example:

request
```
goform/writeVariable?nVars=1&var1=M1_Output_1&value1=1
```
response (successful case):
```
# M1_Output_1              0
```
response (failure case):
```
# M1_Output_1              5 Operation timeout
```

The CGI can be extended to write N variables (N>1), for example to write 2 variables:

```
goform/writeVariable?nVars=2&var1=<var_name1>&var2=<var_name2>&value1=<va
r_value1>&value2=<var_value2>
```

The response contains N sections with the format described above.

20 Glossary

Router: a networking device that forwards data packets between computer networks, e.g. between a LAN and a WAN (the Internet).

Switch: a networking device that connects devices together on a computer network, by using a form of packet switching to forward data to the destination device.

VPN: a Virtual Private Network extends a private network across a public network, such as the Internet. It enables a device to send and receive data across the public network as if it were directly connected to the private network. A VPN is created by establishing a virtual point-to-point connection through the use of tunnelling protocols, with traffic encryption.

Tunnel: an IP tunnel is an Internet Protocol (IP) network communications channel between two networks. It is used to transport another network protocol by encapsulation of its packets.