

USER MANUAL

Z-PASS1

Z-PASS2

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)



This document is property of SENECA srl. Duplication and reproduction are forbidden, if not authorized. Contents of the present documentation refers to products and technologies described in it. All technical data contained in the document may be modified without prior notice Content of this documentation is subject to periodical revision.

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, programming 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.

No liability for the contents of this documents can be accepted. Use the concepts, examples and other content at your own risk. There may be errors and inaccuracies in this document, that may of course be damaging to your system. Proceed with caution, and although this is highly unlikely, the author(s) do not take any responsibility for that. Technical features subject to change without notice.

Seneca Z-PC Line modules: **Z-PASS1, Z-PASS2**

Table of Contents

Table of Contents	2
1 Preliminary information / Informazioni preliminari	5
2 Firmware Licensing Terms	8
2.1 Firmware with Open Source GPL.....	8
3 Features	8
4 Technical specifications	10
5 Electrical Connections	13
5.1.1 Z-PASS1-IO Digital I/Os	17
5.1.2 Z-PASS2-IO Digital I/Os	17
6 LEDs signaling	18
6.1 Z-PASS1/Z-PASS2	18
6.2 Z-PASS1-R01/Z-PASS2-R01	19
6.3 Z-PASS2-IO	20
6.4 Z-PASS1-IO	21
7 Upgrading the firmware by USB pen	23
8 Discovering the Z-PASS IP address	23
9 Ethernet Mode (Z-PASS1-R01/Z-PASS2-R01/Z-PASS1-IO/Z-PASS2-IO)	25
10 Modbus Ethernet to Serial Gateway	27
11 Transparent Gateway	28
11.1 Virtual COM (with RFC 2217).....	28
11.1.1 Seneca Serial to Ethernet Connect	30
11.2 Serial Tunnel Point-to-Point on TCP	39
11.3 Serial Tunnel Point-to-Point on UDP	39
11.4 Serial Tunnel Point-to-Multipoint.....	40
12 Modbus Shared Memory Gateway.....	41
13 VPN	43
13.1 “Single LAN” VPN.....	45
13.2 “Point-to-Point” VPN	46
14 Router	47
15 Network Redundancy	48

16	Remote Connection Disable	48
17	Auto-APN	49
18	SMS Commands	49
18.1	PPP ON	50
18.2	PPP OFF	51
18.3	PPP IP	51
18.4	PPP CNF	51
18.5	VPN ON	52
18.6	VPN OFF	53
18.7	VPN CNF	53
18.8	FWL ON	54
18.9	FWL OFF	54
18.10	GET DIN	54
18.11	GET DOUT	55
18.12	SET DOUT	55
18.13	SET PULSE	56
18.14	SET USER.PHONE	57
18.15	RESET PHONE	57
18.16	STATUS	58
18.17	GET GPS	58
18.18	RESET	58
18.19	Initial Configuration	59
19	Web Configuration Pages	59
19.1	Main View	60
19.2	Network and Services	61
19.3	Serial Ports	71
19.4	Gateway Configuration	73
19.4.1	Modbus Ethernet to Serial Gateway	75
19.4.2	Transparent Gateway	81
19.4.3	Modbus Shared Memory Gateway	84
19.5	Shared Memory Tag Configuration	88
19.5.1	Tag Setup	88
19.5.2	Tag View	104
19.5.3	Microsoft Excel™ Template for Tag Setup	107

19.6	Real Time Clock Setup	109
19.7	VPN Configuration	112
19.7.1	OpenVPN	112
19.7.2	VPN Box	124
19.8	Router Configuration	130
19.9	Users Configuration	139
19.10	FW Upgrade	141
19.11	Configuration Management	149
19.11.1	Factory reset by USB pen.....	152
19.12	Mobile Network.....	153
19.13	DDNS Configuration.....	167
19.14	Digital I/O Configuration.....	171
19.15	SMS Configuration	176
19.16	Phonebook.....	178
19.17	FW Versions	184
19.18	Ethernet Interfaces	186
19.19	Guest pages	188
20	FTP/SFTP access.....	190
21	Glossary	192

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-PASS1/Z-PASS2, 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-PASS1/Z-PASS2, 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, CONSEGUENZIALI O INCIDENTALI, PER CAUSE (COMPRESA LA NEGLIGENZA), DERIVANTI O COLLEGATE ALL' USO O ALL' INCAPACITÀ DI USARE Z-PASS1/Z-PASS2, 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-PASS1/Z-PASS2, 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	06	- Chapter "Features": new features for Z-PASS1-R01/Z-PASS2-R01 - Chapter "LEDs signalling": new par. "Z- PASS1-R01/Z-PASS2-R01" - New chapter "Ethernet Mode (Z- PASS1-R01/Z-PASS2-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- PASS1-1/Z-PASS2-R01)" - "VPN Configuration/VPN Box/LED signalling (Z- PASS1-1/Z-PASS2-R01)"
20/09/2016	07	- Paragraph "VPN Configuration/Open VPN Client": revision into "VPN Configuration/Open VPN"
15/12/2016	08	Renamed "Z-PASS1-1" → "Z-PASS1-R01"; "Z-PASS2-1" → "Z-PASS2-R01"; added "DNS Mode" parameter
18/01/2017	09	- Chapter "Electrical Connections": added SD Card figure - Chapter "Discovering the IP address": discovery working on both LAN and WAN interfaces - Paragraph "Main View" revision - Paragraph "Network and Services": changed some default values - Paragraph "Real Time Clock Setup": added "Central Europe" time zone value - Paragraph "VPN Configuration/OpenVPN Client": 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" and FTP user credentials - New paragraph "Ethernet Interfaces" - New paragraph "Guest Pages" - New chapter "FTP/SFTP access"
29/05/2017	10	- Chapter "Features": new features for Z-PASS1-IO/Z-PASS2-IO - Fixed COM1 connector pin numbers - New "LEDs signaling" sub-paragraph for IO HW revision - New chapter "Remote Access Disable" - New chapter "Auto-APN" - Paragraph "Network and Services": added screen-shots for "IO" version; added "COM1/Mode" parameter - Paragraph "VPN Box": added "License Limit Reached" error reason - "Use Local Address through VPN" parameter: "ON" option always available

		- Paragraph “FW Upgrade”: changed “Stop Gateway Services” pop-up - New paragraph “Configuration Management” - Paragraph “Mobile Network”: added “APN Mode” parameter - New paragraph “Digital I/O Configuration”
15/09/2017	11	- Chapter “Features”: HW IO features split between Z-PASS1 and Z-PASS2 - Chapter “Technical Specifications”: some fixes; added I/Os for Z-PASS1-IO/ZPASS2-IO; added features for Z-PASS2-IO modem - Chapter “Electrical Connections”: some fixes for Z-PASS1-IO/ZPASS2-IO - Paragraph “LEDs signaling”/IO: split between Z-PASS1 and Z-PASS2; added info about modem “STAT “ LED - Chapter “Upgrading the firmware...”: added notes about LEDs blinking - Chapter “VPN”: added description of Layer 2 and Layer 3 VPN - Paragraph “Main View”: updated figure - Paragraph “Network and Services”: added info about new Web Server and File Transfer parameters; updated figures - Paragraph “Gateway Configuration/Modbus Bridge”: updated figures; added sub-paragraph “Embedded I/O” - Paragraph “Gateway Tag Setup”: added sub-paragraph “Tags for Embedded I/O” - Paragraph “Real Time Clock Setup”: updated figure - Paragraph “VPN Configuration/VPN Box”: changes related to L2 VPN and info about connected user; updated figures - Paragraph “Router Configuration”: changed default value for “Allow Access through Mobile Public IP Address” parameter - Paragraph “Configuration Management”: added info about zip archive; updated figures - Paragraph “Mobile Network”: updated figures - Paragraph “Digital I/O Configuration”: split between Z-PASS1 and Z-PASS2; updated figures - “Remote Access Disable” → “Remote Connection Disable”
06/10/2017	12	- Changed “-R02” → “-IO” - Chapters “Features”, “Technical Specifications”: note about GPS module and antenna - Chapter “Electrical Connections”: added sub-paragraph for Z-PASS1-IO/Z-PASS2-IO Digital I/Os - Paragraphs “Main View”, “Network and Services”: updated figures - Paragraph “Real Time Clock Setup”: added figure with new time zones - Paragraph “VPN Box”: updated first figure - Paragraph “Router Configuration”: updated figures - Paragraph “Users Configuration”: updated figure and added info about allowed characters - Paragraph “FW Upgrade”: updated figures - New sub-paragraph “Factory reset by USB pen” - Paragraph “Mobile Network”: added info and figure about “GPS Location”; updated some figures - New paragraph “FW Versions” - Deleted “DHCP on LAN” parameter
19/12/2017	13	- Chapter “Features”: added Z-PASS2-IO-4G product - Chapter “Technical specifications”: updated info about modem - “Modbus Bridge” → “Modbus Ethernet to Serial Gateway”

		- “Transparent Bridge” → “Transparent Gateway” - “Modbus Gateway” → “Modbus Shared Memory Gateway” - “Remote Serial COM” → “Virtual COM” - Paragraph “Router Configuration”: parameter “Allow access through Mobile Public IP Address” changed to “Mobile Network Firewall” - Paragraph “Mobile Network”: changes related to “Operator Selection” and PIN handling - New paragraph “DDNS Configuration” - Paragraphs “Main View” and “Guest pages”: “RESET” button renamed to “RESTART”; updated figures - Chapter “Remote Connection Disable”: added “Security Level 4 (SMS Service)” - Paragraph “Digital I/O Configuration”: added “Security Level 4 (SMS Service)” - Modbus Ethernet to Serial Gateway, sub-paragraph “Embedded I/O”: added GPS info registers table - Modbus Shared Memory Gateway: added sub-paragraph “Tags for GPS Info” - Paragraph “Digital I/O Configuration”: added procedure to toggle digital output status - Users Configuration: maximum length of 32 characters changed to 100 characters - Deleted references to Z-MODEM-3G - Nearly all web pages screen-shots updated
25/01/2018	14	- Removed CTS signal from COM1 port. - Removed “None” value of “Security Level / Service Disable” parameter - Paragraph “Gateway Configuration”: reviewed for “Gateway Mode” selection on each serial port
13/03/2018	15	- New chapter “SMS Commands” - Paragraph “Main View”: added “Logic Configuration” section; updated figure - New paragraph “SMS Configuration” - New paragraph “Phonebook”

2 Firmware Licensing Terms

2.1 Firmware with Open Source GPL

The Z-PASS firmware contains Open Source software under GPL. According to Section 3b of GPL, we offer you the source code. You can obtain the source code with licensing terms of the Open Source software from Seneca s.r.l. on request. Send your request to support@seneca.it with the subject "Open Source Z-PASS".

3 Features

The Z-PASS1 and Z-PASS2 devices are “**Ethernet to Serial Gateways**” (also known as “**Serial Device Servers**”) with three main operating modes:

- Modbus Ethernet to Serial Gateway
- Transparent Gateway (Virtual COM, Serial Tunneling)
- Modbus Shared Memory Gateway

Both devices provide the following features:

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

The main difference between the two devices is that Z-PASS2 integrates a 3G HSPA modem. Actually, Z-PASS1 is aimed at applications where an Internet connection is already available, while Z-PASS2 provides connectivity by itself.

Z-PASS2 and Z-PASS1 (when connected to an external modem) can be used as a Router, routing packets between the WAN (Mobile Network) and the LAN (Ethernet).

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

Z-PASS1-R01 and Z-PASS2-R01 are new versions of the Z-PASS1 and Z-PASS2 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-PASS1-IO is a new version of the Z-PASS1 product, providing the following new features:

- one digital input which can be used to disable remote connection 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

Z-PASS2-IO is a new version of the Z-PASS2 product, providing the following new features:

- one digital input which can be used to disable remote connection to the device
- one digital output which goes HIGH when the device is remotely accessed
- one digital output which can also be used as a remote command
- one configurable digital input/output which can also be used as a local alarm
- a new set of LEDs
- COM1 RS232/RS485 mode set by software (configuration parameter), instead of HW DIP switch
- a new penta-band 3G+ modem, which also features a GPS module

Z-PASS2-IO-4G is a new version of the Z-PASS2-IO product, providing a new 4G LTE Cat.1 modem, instead of the 3G+ modem.

NOTE 1:

in the following chapters, the term “Z-PASS” will be used when describing features or characteristics that are available in both Z-PASS1 and Z-PASS2 products.

NOTE 2:

in the following chapters, any reference to 3G modem/connection applies also to 4G modem/connection.

4 Technical specifications

COMMUNICATION PORTS	
RS 485	Baud rate: maximum 115 Kbps, minimum 200 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 200 bps COM 1 (removable 4 pin connector, as an alternative to RS485)
Ethernet 1 and Ethernet 2	Ethernet 10/100 Mbps Two RJ45 connectors on front-panel Maximum connection length 100 m <u>In Z-PASS1-R01/Z-PASS2-R01/Z-PASS1-IO/Z-PASS2-IO, the two ports can work either as LAN/WAN ports (ETH1=LAN, ETH2=WAN) or ports of an Ethernet switch.</u> <u>In Z-PASS1/Z-PASS2, the two ports can work only as ports of an Ethernet switch.</u>
USB #1 HOST	Plug-in: USB type A
USB #2 HOST	Plug-in: micro USB (available only in Z-PASS1, Z-PASS1-R01)
CPU AND MEMORY	
Microprocessor	ARM 9, 32 bits, 400 MHz
Memories	64 Mbytes of RAM 1 Gbyte of FLASH
Slot for external memory	Micro SD card: max 32 Gbytes
3G+ MODEM (Z-PASS2)	
HSPA Modem	14.4 Mbps in downlink, 5.76 Mbps in uplink
Slot for SIM card	Mini SIM with push-push connector
3G+ MODEM (Z-PASS2-IO)	

Speed	HSPA+: max 14.4 Mbps DL, max 5.76 Mbps UL UMTS: max 384 Kbps (DL), max 384 Kbps (UL) EDGE: max 236.8 Kbps (DL), max 236.8 Kbps (UL) GPRS: max 85.6 Kbps (DL), max 85.6 Kbps (UL)
GNSS	GPS/GLONASS 16 GPS channels 14 GLONASS channels Accuracy <1.5m CEP-50 @ Open Sky
Approvals	RoHS Compliant, CE/GCF/Vodafone (Europe), DoC (Russia), FCC/PTCRB/AT&T (North America), RCM (Australia), ICASA (South Africa), SRRC/NAL/OFCA (China), JATE & TELEC (Japan), NCC (Taiwan), KC/SKT (Korea), IC/Rogers (Canada), Anatel (Brazil), NBTC (Thailand)
Slot for mini SIM	Mini SIM with push-push connector
4G (LTE Cat. 1) MODEM (Z-PASS2-IO-4G)	
Speed	LTE FDD: max 10 Mbps (DL), max 5Mbps (UL) LTE TDD: max 8.96 Mbps (DL), max 3.1 Mbps (UL) DC-HSPA+: max 42Mbps (DL), max 5.76 Mbps (UL) UMTS: max 384 Kbps (DL), max 384 Kbps (UL) EDGE: max 296 Kbps (DL), max 236.8 Kbps (UL) GPRS: max 107 Kbps (DL), max 85.6 Kbps (UL)
GNSS	GPS/GLONASS/BeiDou/Galileo/QZSS
Approvals	RoHS Compliant, CE/GCF/Vodafone (Europe), FCC/PTCRB/AT&T/Verizon* (North America), RCM/Telstra (Australia), JATE/TELEC/DOCOMO* (Japan), NCC (Taiwan), KC/SKT/KT*/LGU+* (Korea), IC/Rogers (Canada), Anatel (Brazil), CCC/SRRC/NAL (China) *= Under Development
Slot for mini SIM	Mini SIM with push-push connector
POWER SUPPLY	
Power supply	11..40 Vdc or 19..28 Vac @ 50..60 Hz
Consumption	Typical 4 W @ 24 Vdc; Max 6 W
ENVIRONMENTAL CONDITIONS	
Temperature	-20..+55 °C
Humidity	30..90 % @ 40 °C not condensing
Storage temperature	-20..+85 °C
Degree protection	IP20
CONNECTIONS	
Connections	Removable 3 way screw terminals, 5.08 pitch

	Rear IDC10 connector for DIN 46277 rail Removable 4 pin connector, two RJ45 connectors, USB connector and micro USB connector (only in Z-PASS1, Z-PASS1-R01) Two SMA antenna connectors: - for Main and Diversity antennas (only in Z-PASS2, Z-PASS2-R01) - for 3G and GPS antennas (only in Z-PASS2-IO)
BOX / DIMENSIONS	
Dimensions	Z-PASS1: L:100 mm; H:112 mm; W:35 mm Z-PASS2: L:100 mm; H:112 mm; W:53 mm
Case	Nylon 6 with 30% fiberglass field, self-extinguishing class V0, black color
INPUTS / OUTPUTS (Z-PASS1-IO)	
Digital Inputs	Max. number of channels: 2 Voltage: OFF<4V ON>8V; Max. Current (Vout+): 20mA Current absorbed: 3mA at 12VC; 6mA at 24VC
Digital Outputs	Max. number of channels: 3 Voltage (+Vext): 10 – 24VC Max. current delivered: 400mA
INPUTS / OUTPUTS (Z-PASS2-IO)	
Digital Inputs	Max. number of channels: 4 Voltage: OFF<4V ON>8V; Max. Current (Vout+): 20mA Current absorbed: 3mA at 12VC; 6mA at 24VC
Digital Outputs	Max. number of channels: 4 Voltage (+Vext): 10 – 24VC Max. current delivered: 400mA

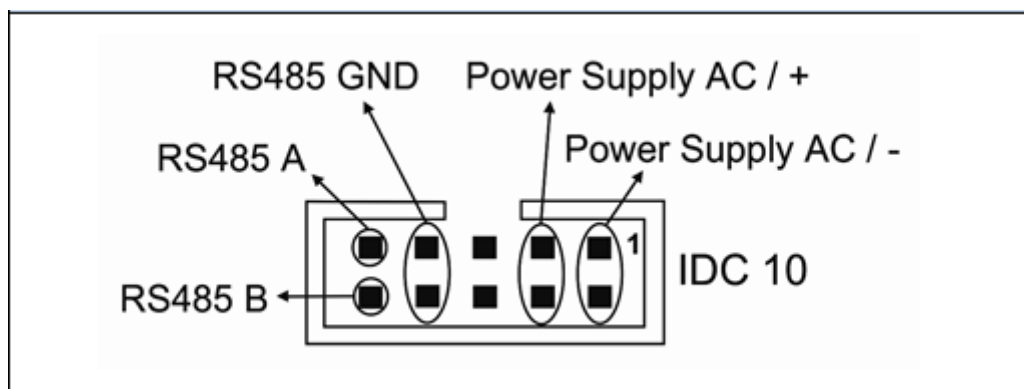
The following table shows which frequency bands are supported by the 3G/4G modem available in Z-PASS2, Z-PASS2-R01, Z-PASS2-IO and Z-PASS2-IO-4G products.

Standard	Frequency/Feature	Z-PASS2, Z-PASS2-R01	Z-PASS2-IO	Z-PASS2-IO-4G
GSM	GSM 850 MHz	OK	OK	
	EGSM 900 MHz	OK	OK	OK
	DCS 1800 MHz	OK	OK	OK
	PCS 1900 MHz	OK	OK	
WCDMA	WCDMA 800 MHz		OK	
	WCDMA 850 MHz		OK	OK
	WCDMA 900 MHz	OK	OK	OK
	WCDMA 1900 MHz		OK	
	WCDMA 2100 MHz	OK	OK	OK
LTE	LTE 800 DD			OK
	LTE 850			OK
	LTE 900			OK
	LTE 1800			OK
	LTE 2100			OK
	LTE 2600			OK
HSPA	HSDPA	OK	OK	

	HSUPA	OK	OK	
	HSPA+		OK	
	DC-HSPA+			OK
DRX	Receiver Diversity	OK		

5 Electrical Connections

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-PASS1, Z-PC-DINAL2-52.5-17 for Z-PASS2. The following picture shows the meaning of the IDC10 connector pins.



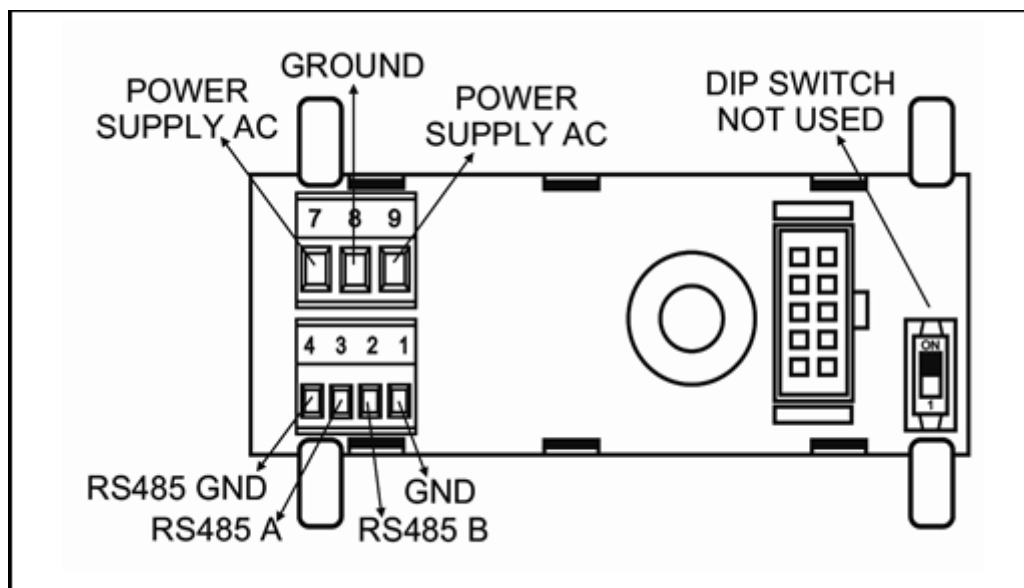
Power supply is available only from the rear connector for Z-PASS1/ZPASS1-R01, while:

Z-PASS1-IO can be powered also through 17-18 screw terminals;

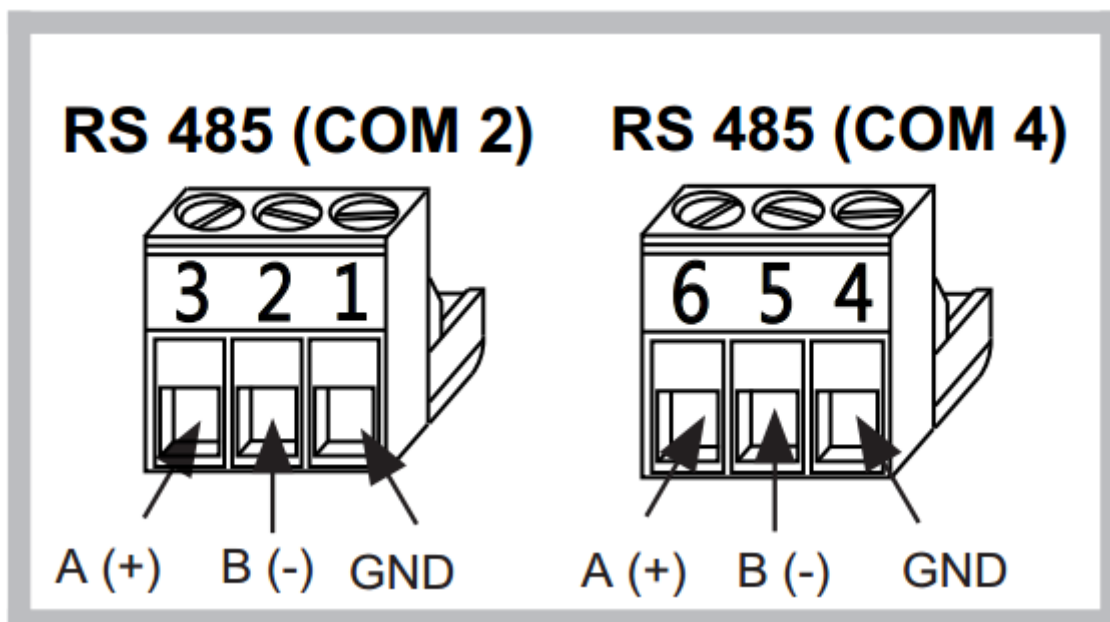
Z-PASS2/ZPASS2-R01/ZPASS2-IO can be powered also through 14-15 screw terminals.

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.

GNDSHLD: Shield to protect the connection cables against interference (recommended).



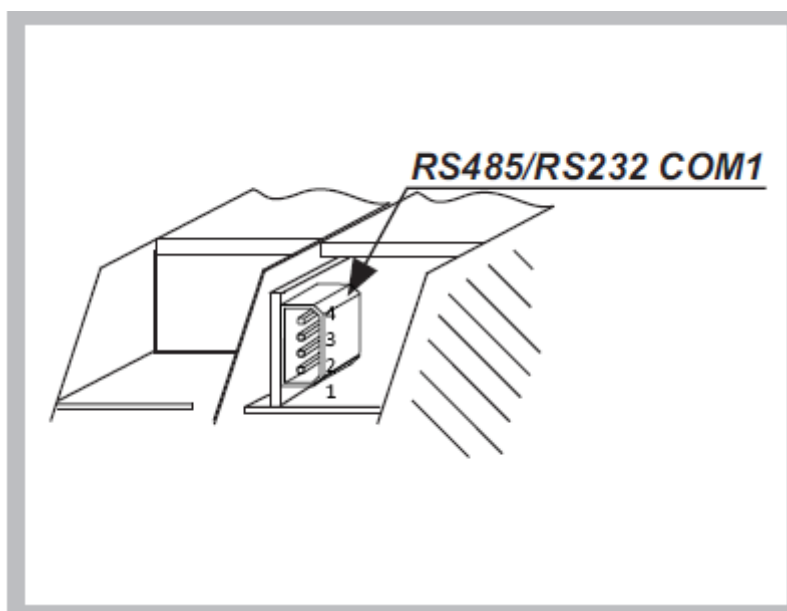
The Z-PASS has two RS 485 serial ports for Modbus communication: COM 2 and COM 4. The RS485 connection for COM 2 can be set up by means of the corresponding screw terminals or by the IDC10 connector.



Through a removable 4 pin connector, the Z-PASS 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-switch¹ on ON position; to select the RS485 port on the removable 4 pin connector, put the SW2 DIP-switch on OFF position.

In Z-PASS1-IO/Z-PASS2-IO, the mode (RS485/RS232) of this port is set as a parameter in software configuration.

The cable length for the RS232 interface must be less than 3 meters.



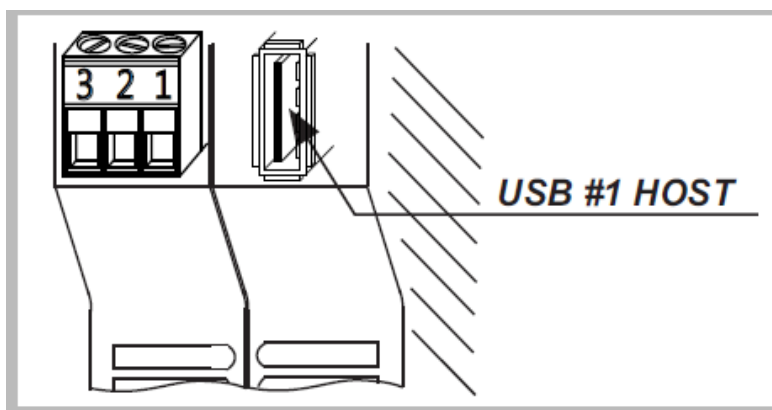
¹ While in Z-PASS1 the SW2 DIP-switch position can be changed by the user, in Z-PASS2 the DIP-switch is internal and its position is permanently set in the factory.

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

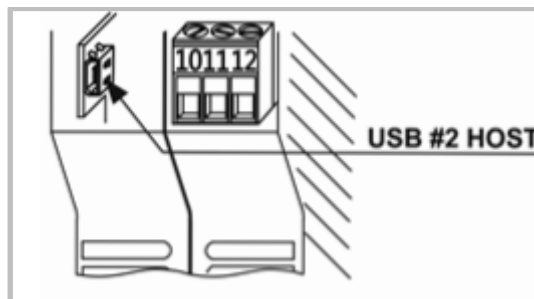
Pin	RS232	RS485
1 (bottom)	-	-
2	Tx	B
3	Rx	A
4 (top)	GND	GND

The Z-PASS has a USB HOST type A connector, that can be used to connect an external USB memory; this is used for FW upgrade (see chapter “Upgrading the firmware by USB pen”).

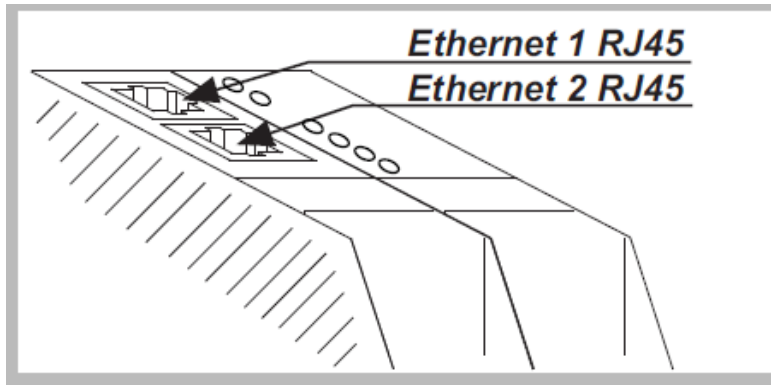
Please note that, on this USB port, the “hotplug” feature is not available; so, after plugging the USB device, it is necessary to power off/on the Z-PASS to let it detect the USB device.



The Z-PASS1 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; this port is no more available in Z-PASS1-IO.

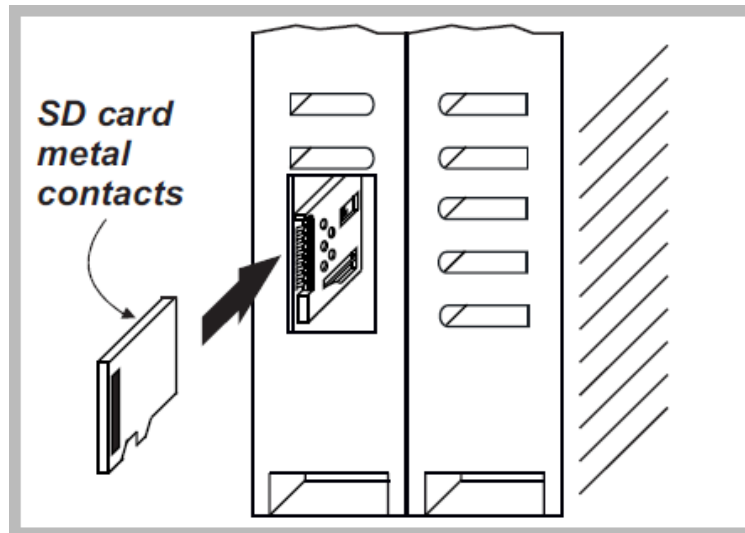


The Z-PASS has two Ethernet ports with RJ45 connectors on the front panel. The two ports are internally connected in HUB/SWITCH mode. The two ports have the same MAC Address.

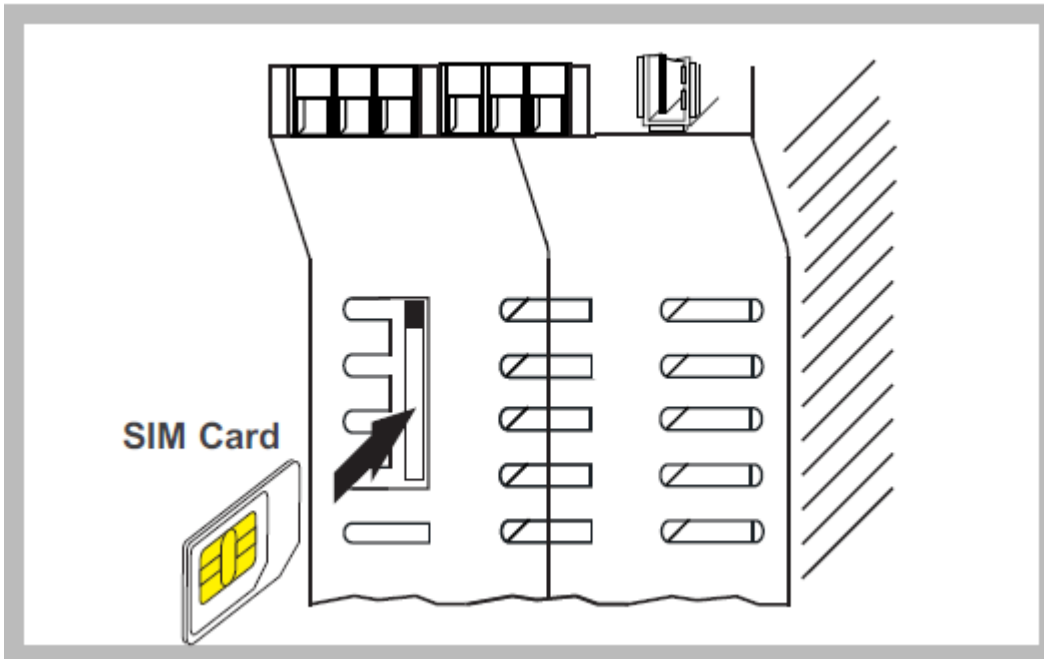


The Z-PASS has a plug-in connector for micro SD card placed in the side part of the case. To insert the SD card into the connector, be sure that the SD card is oriented with metal contacts facing towards left (with reference to the figure).

The SD card can be of any class.

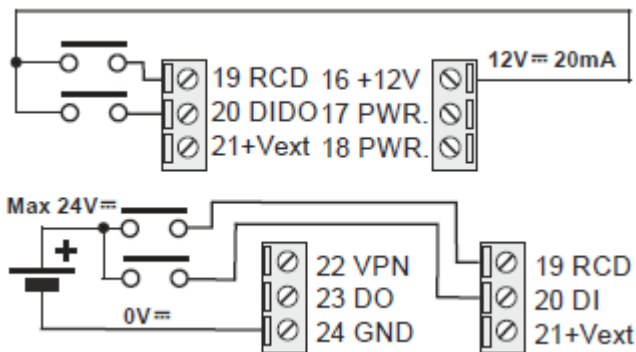


The Z-PASS2 has a slot for SIM card, placed on the side of the case. Before pushing the SIM card into this slot, please be sure that the SIM card golden contacts are facing towards right (please see the figure below).

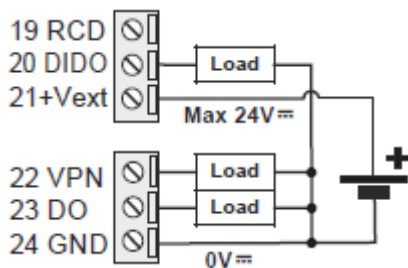


5.1.1 Z-PASS1-IO Digital I/Os

In Z-PASS1-IO, the electrical connections for the Digital Inputs shall be arranged as in the following figures.

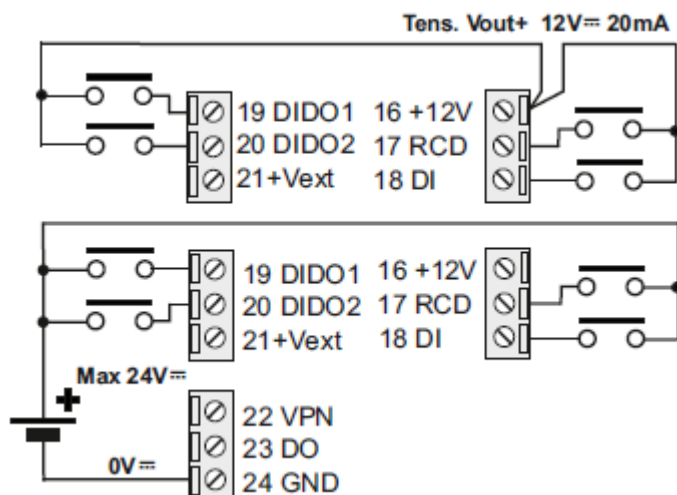


The electrical connections for the Digital Outputs shall be arranged as in the following figure.

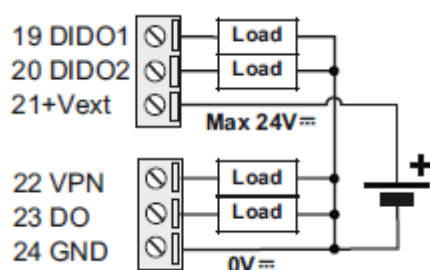


5.1.2 Z-PASS2-IO Digital I/Os

In Z-PASS2-IO, the electrical connections for the Digital Inputs shall be arranged as in the following figures.



The electrical connections for the Digital Outputs shall be arranged as in the following figure.



6 LEDs signaling

6.1 Z-PASS1/Z-PASS2

LED	STATUS	LED meaning
PWR Green	ON	The module is powered on
RUN Red	Blinking	The module is ready for use
LINK1 Yellow	ON	Ethernet 1 connection detected
	OFF	Ethernet 1 connection absent
ACT1 Green	Blinking	There is data activity (Ethernet 1)
	OFF	There is no data activity (Ethernet 1)
LINK2 Yellow	ON	Ethernet 2 connection detected
	OFF	Ethernet 2 connection absent
ACT2 Green	Blinking	There is data activity (Ethernet 2)
	OFF	There is no data activity (Ethernet 2)

RX1/TX1 Red	Blinking	Data reception/transmission on COM1 port
	OFF	No data reception/transmission on COM1 port
RX2/TX2 Red	Blinking	Data reception/transmission on COM2 port
	OFF	No data reception/transmission on COM2 port
RX4/TX4 Red	Blinking	Data reception/transmission on COM4 port
	OFF	No data reception/transmission on COM4 port
3G PWR Green (Z-PASS2 only)	ON	The 3G Modem is powered on
STAT Yellow (Z-PASS2 only)	ON	Not registered on GSM network
	Slow Blinking	Registered on GSM network
	Fast Blinking	PPP connection active

6.2 Z-PASS1-R01/Z-PASS2-R01

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Red	Blinking	The module is ready for use
LAN/WAN Yellow	ON	The Ethernet ports are working in “LAN/WAN” mode
	OFF	-
SWITCH Green	ON	The Ethernet ports are working in “Switch” mode
	OFF	-
VPN Yellow	ON	VPN connection is working properly
	Blinking	VPN connection is not working properly
	OFF	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	VPN Box “SERVICE” connection is working properly
	Blinking	VPN Box “SERVICE” connection is not working properly
	OFF	VPN Box functionality is disabled
RX1-2-4 Red	Blinking	Data reception (COM 1-2-4)
	ON	Check the connection (COM 1-2-4)

	OFF	No data reception (COM 1-2-4)
TX1-2-4 Red	Blinking	Data transmission (COM 1-2-4)
	ON	Check the connection (COM 1-2-4)
	OFF	No data transmission (COM 1-2-4)
3G PWR Green (Z-PASS2-R01 only)	ON	The 3G Modem is powered on
STAT Yellow (Z-PASS2-R01 only)	ON	Not registered on GSM network
	Slow Blinking	Registered on GSM network
	Fast Blinking	PPP connection active

6.3 Z-PASS2-10

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Green	Blinking	The module is ready for use
DIDO1 Green	ON	Configurable Digital Input/Output 1 state is HIGH
	OFF	Configurable Digital Input/Output 1 state is LOW
DIDO2 Green	ON	Configurable Digital Input/Output 2 state is HIGH
	OFF	Configurable Digital Input/Output 2 state is LOW
DI Green	ON	Digital Input state is HIGH
	OFF	Digital Input state is LOW
DO Green	ON	Digital Output state is HIGH
	OFF	Digital Output state is LOW
RCD Green	ON	Remote Connection is disabled
	OFF	Remote Connection is enabled
VPN Green	ON	VPN connection is working properly
	Blinking	VPN connection is not working properly
	OFF	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	ON	The Ethernet ports are working in "LAN/WAN" mode

Green	OFF	The Ethernet ports are working in “Switch” mode
SERV Green	ON	VPN Box “SERVICE” connection is working properly
	Blinking	VPN Box “SERVICE” connection is not working properly
	OFF	VPN Box functionality is disabled
RX2-4 Green	Blinking	Data reception (COM 2-4)
	ON	Check the connection (COM 2-4)
	OFF	No data reception (COM 2-4)
TX2-4 Green	Blinking	Data transmission (COM 2-4)
	ON	Check the connection (COM 2-4)
	OFF	No data transmission (COM 2-4)
3G PWR Green	ON	The 3G Modem is powered on
STAT Yellow	Slow blinking (200 ms OFF, 1800 ms ON)	Searching for GSM network
	Slow blinking (1800 ms OFF, 200 ms ON)	Registered on GSM network
	Fast blinking (125 ms OFF, 125 ms ON)	Data transfer is ongoing

Ethernet Connector LEDS

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

6.4 Z-PASS1-10

LED	Status	Meaning
PWR Green	ON	The module is powered on
RUN Green	Blinking	The module is ready for use

DIDO Green	ON	Configurable Digital Input/Output state is HIGH
	OFF	Configurable Digital Input/Output state is LOW
DO Green	ON	Digital Output state is HIGH
	OFF	Digital Output state is LOW
RCD Green	ON	Remote Connection is disabled
	OFF	Remote Connection is enabled
VPN Green	ON	VPN connection is working properly
	Blinking	VPN connection is not working properly
	OFF	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	The Ethernet ports are working in “LAN/WAN” mode
	OFF	The Ethernet ports are working in “Switch” mode
SERV Green	ON	VPN Box “SERVICE” connection is working properly
	Blinking	VPN Box “SERVICE” connection is not working properly
	OFF	VPN Box functionality is disabled
RX2-4 Green	Blinking	Data reception (COM 2-4)
	ON	Check the connection (COM 2-4)
	OFF	No data reception (COM 2-4)
TX2-4 Green	Blinking	Data transmission (COM 2-4)
	ON	Check the connection (COM 2-4)
	OFF	No data transmission (COM 2-4)

Ethernet Connector LEDS

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

7 Upgrading the firmware by USB pen

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

The procedure is the following:

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

<http://www.seneca.it/products/z-pass1>

<http://www.seneca.it/products/z-pass2>

the downloaded file is a .zip file; extract the FW file from it;

the FW file shall have a name like the following:

SW003900_xxx.bin

- 2) copy the file into the root of the USB pen
- 3) switch off the Z-PASS
- 4) insert the USB pen into the USB#1 port
- 5) switch on the Z-PASS; the upgrade procedure will take some minutes to be completed; during this time, the Z-PASS MUST NOT be switched off; during the procedure, the Z-PASS will be rebooted several times; also, during the procedure, several LEDS will blink simultaneously²
- 6) the upgrade procedure is ended when only the LED “RUN” is blinking³
- 7) remove the USB pen

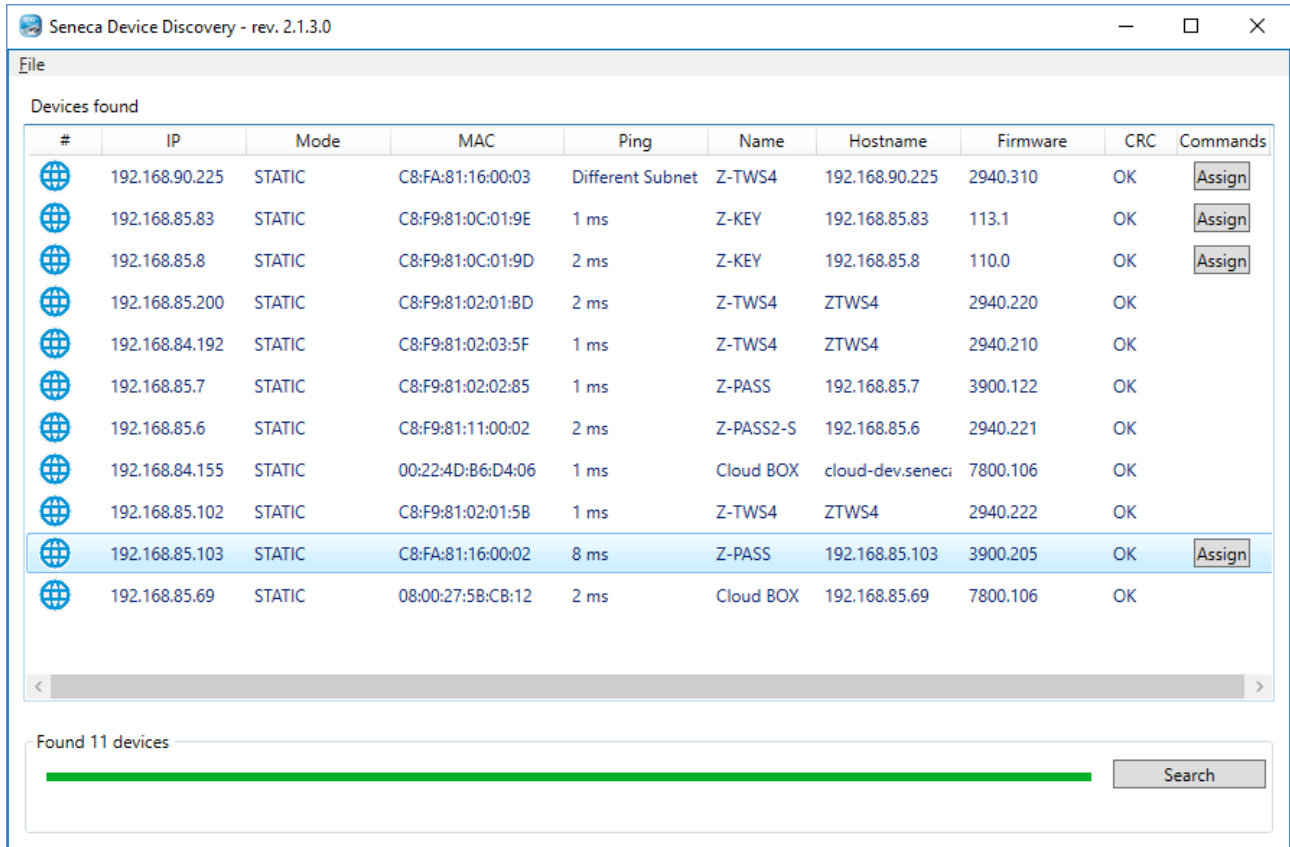
8 Discovering the Z-PASS IP address

Z-PASS devices come out of the factory with the default IP address 192.168.90.101, on the Ethernet (LAN) network interface.

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

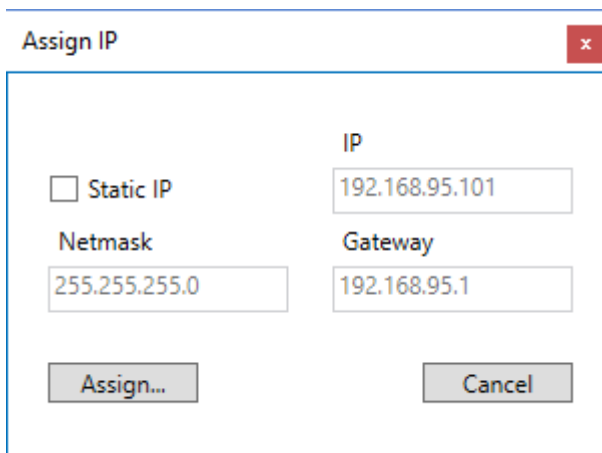
² This applies only to products with HW revisions IO and R01; in details: for IO HW revision, all LEDs will blink simultaneously, except for Power, LAN/WAN, COM and modem LEDs; for R01 HW revision, RUN, VPN and SERV LEDs will blink.

³ Also SERV and VPN LEDs might blink, depending on the Device configuration and status.

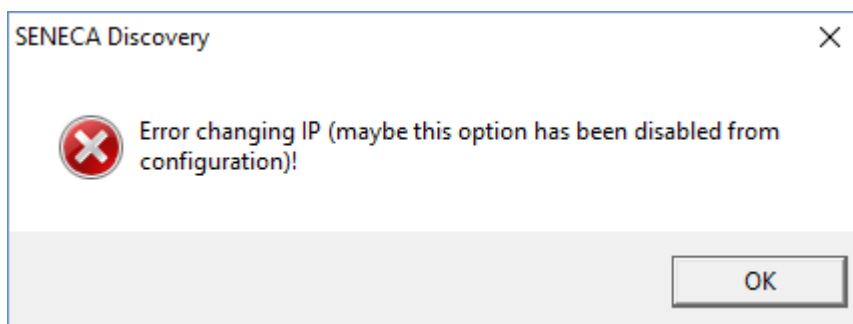


This application shows the IP address, MAC address, FW version and some other useful information, for every Z-PASS device (and other Seneca products) found in the LAN.

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:



For security reasons, this feature can be disabled on the device (see paragraph 19.2); in this case, the following error message is shown, after clicking on the “Assign” button”.



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

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

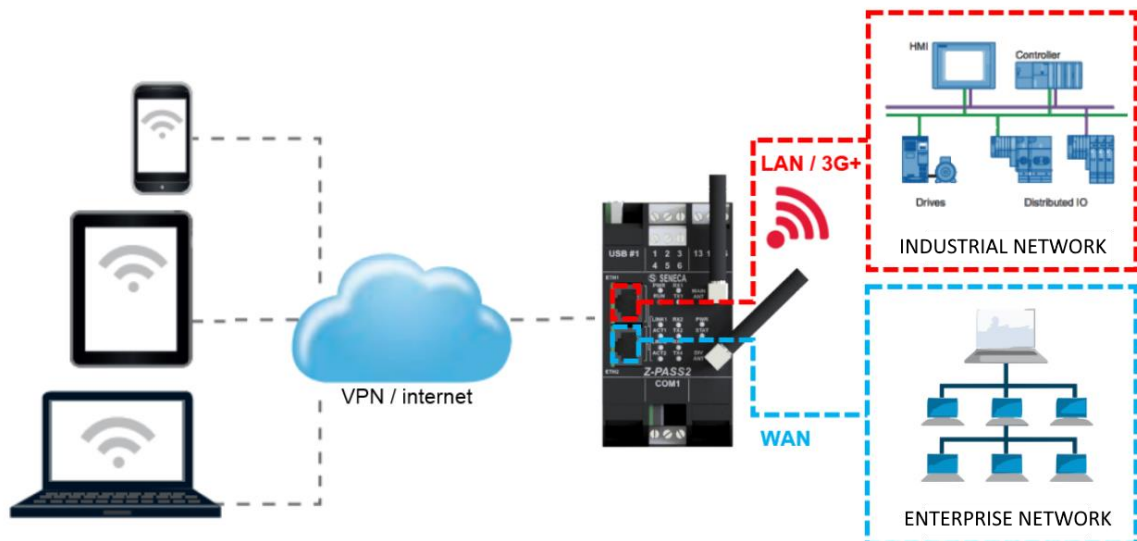
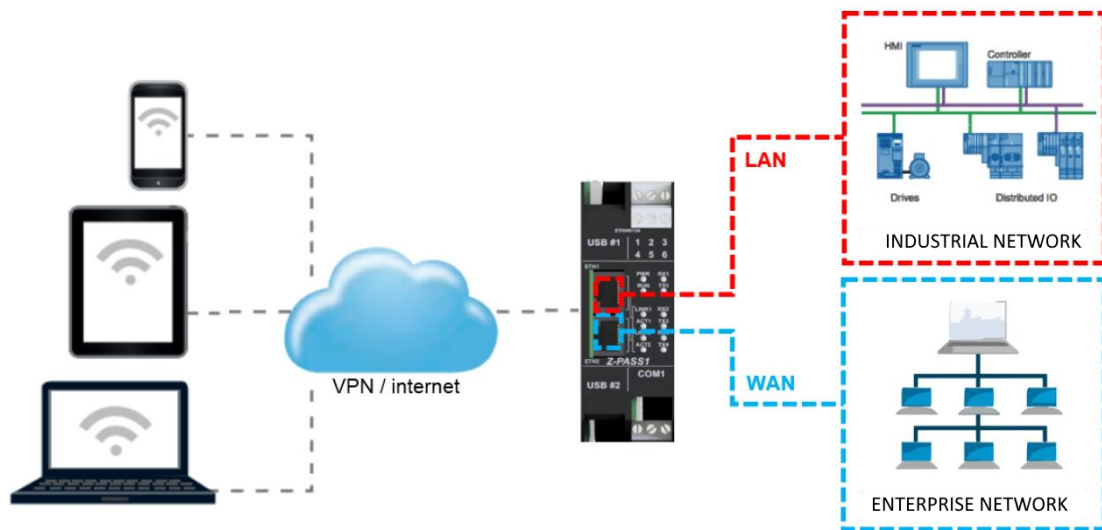
NOTE:

- when Z-PASS 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 Z-PASS 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.

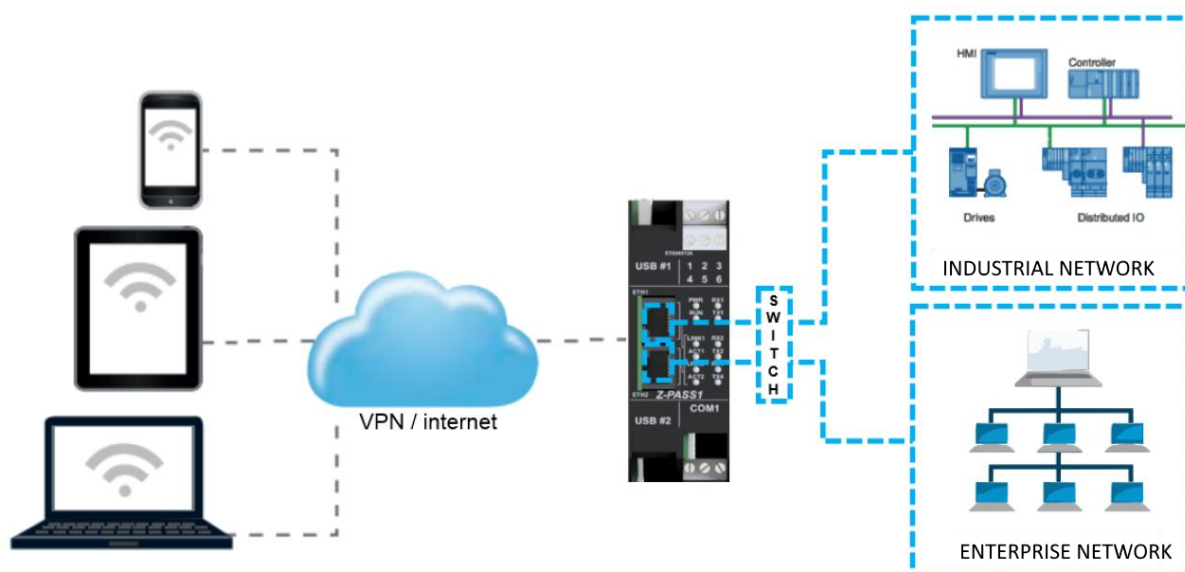
9 Ethernet Mode (Z-PASS1-R01/Z-PASS2-R01/Z-PASS1-IO/Z-PASS2-IO)

In Z-PASS1-R01/Z-PASS2-R01/Z-PASS1-IO/Z-PASS2-IO 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 19.2).

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 Z-PASS 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 Z-PASS to be used as an Ethernet switch, as shown in the following figure.



10 Modbus Ethernet to Serial Gateway

Z-PASS can be configured to run as a Modbus Ethernet to Serial Gateway: Modbus TCP requests received from the Ethernet interface (but also from the PPP [Mobile Network] and VPN interfaces) are converted into Modbus RTU requests and sent to the serial interface; in the same way, the Modbus RTU responses received from the serial interface are converted to Modbus TCP responses and sent back to the source network interface.

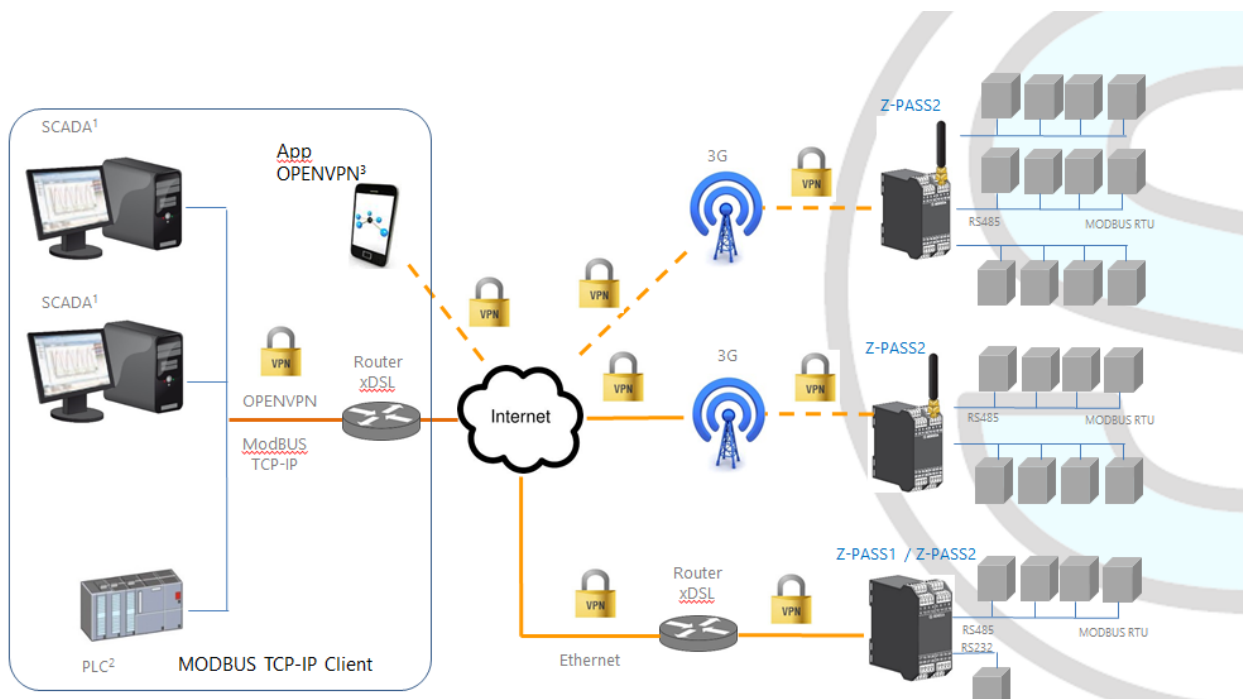
A Modbus Ethernet to Serial Gateway instance can be activated for each of the three available serial ports: COM1 (RS232/RS485), COM2 (RS485) and COM4 (RS485); each one can receive the Modbus TCP requests on a different TCP port (e.g.: 501, 502, 503).

Another possible configuration is to run a Modbus Ethernet to Serial Gateway instance, receiving Modbus TCP requests on a single TCP port (e.g.: 502) and handling two or all the three serial ports. In this case, Modbus RTU requests are simultaneously sent to all the configured ports; obviously, in this configuration, each slave module on the two or three buses shall have a distinct Modbus address;

Each Modbus Ethernet to Serial Gateway instance can support up to 32 simultaneous TCP connections.

The TCP connection can be established over a VPN tunnel, as shown in the following figure.

A detailed description of the Modbus Ethernet to Serial Gateway configuration can be found in 19.4.1 paragraph.



11 Transparent Gateway

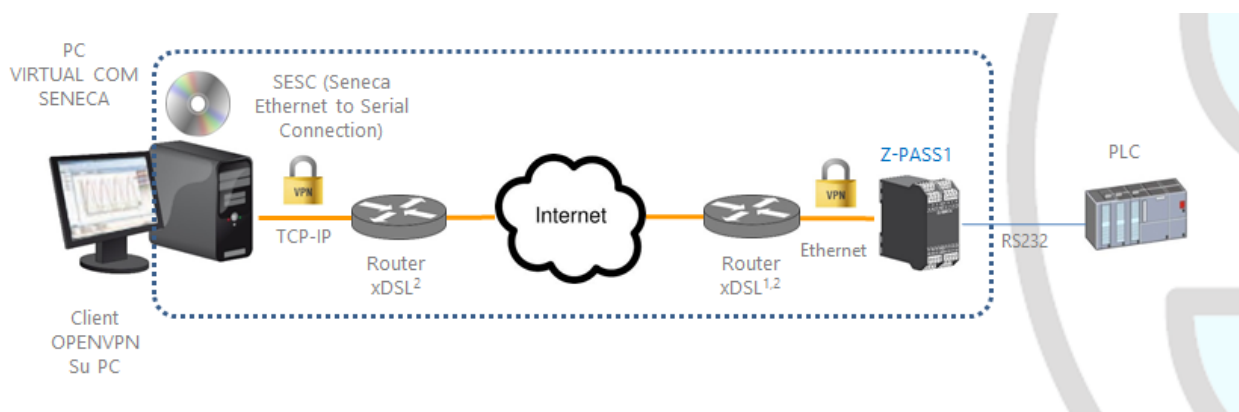
As an alternative to Modbus Ethernet to Serial Gateway, Z-PASS can be configured to run as a “Transparent Gateway”. The big difference between these two modes is that, while the first works just with the Modbus protocol, the second could virtually be applied to any serial protocol that can be transported over the TCP/IP stack.

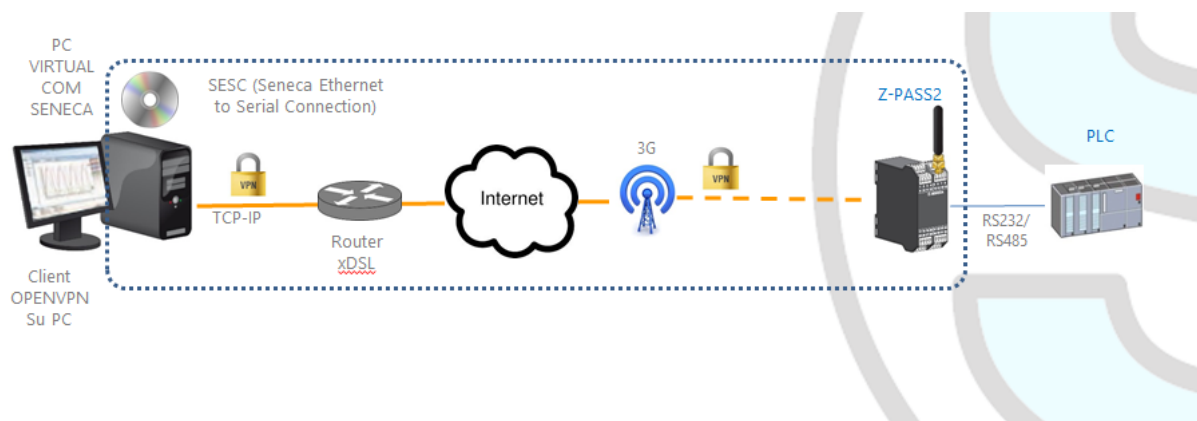
As a Transparent Gateway, Z-PASS provides the following operating modes:

- Virtual COM (with RFC 2217 support)
- Serial Tunnel Point-to-Point on TCP
- Serial Tunnel Point-to-Point on UDP
- Serial Tunnel Point-to-Multipoint on UDP

Each mode will be fully described in a specific paragraph below.

11.1 Virtual COM (with RFC 2217)





The Virtual COM functionality lets to a PC Application, which transmits data only over a serial line, to communicate with a remote serial device, using Ethernet/Internet; in other word, through a Z-PASS, a PC and a serial device, placed in sites distant from each other, can communicate as they are directly connected.

In this mode, data sent over the LAN or WAN network, are received by the Z-PASS and sent to the serial port; response packets follow the reverse path.

RFC 2217 defines some features that let the PC remotely set the properties (baud rate, data bits, stop bits and parity) of the Z-PASS serial port; so, when the Virtual COM operating mode is selected for one port, the port is reconfigured regardless of the previous settings and the values configured by means of the “Serial Ports” web page are overwritten.

To let the Virtual COM work, an utility called “Seneca Ethernet to Serial Connection” shall be installed on the PC; this is explained in details in 11.1.1 paragraph.

The TCP connection can be established over a VPN tunnel, as shown in the figures at the beginning of the paragraph.

Once the connection is established, a program using the virtual COM port will transmit data to the Z-PASS serial port; for example, Modbus RTU requests sent by a Modbus Master program will reach Modbus slave devices connected to the COM2 RS485 bus.

A particular notice shall be given about the “Data Packing Interval” parameter, that can be set when Virtual COM operating mode is selected: this parameter lets you define the time interval, in milliseconds, used by Z-PASS as a criterion to pack the data bytes received from the serial port before sending them to the network; in other words, when Z-PASS does not receive any more bytes from the serial port for the given time interval, it packs the received bytes and send them over the established TCP connection; the optimal value to be set for this parameter depends on the protocol that is transparently routed from the TCP/IP network to the serial line and vice versa.

WARNING!

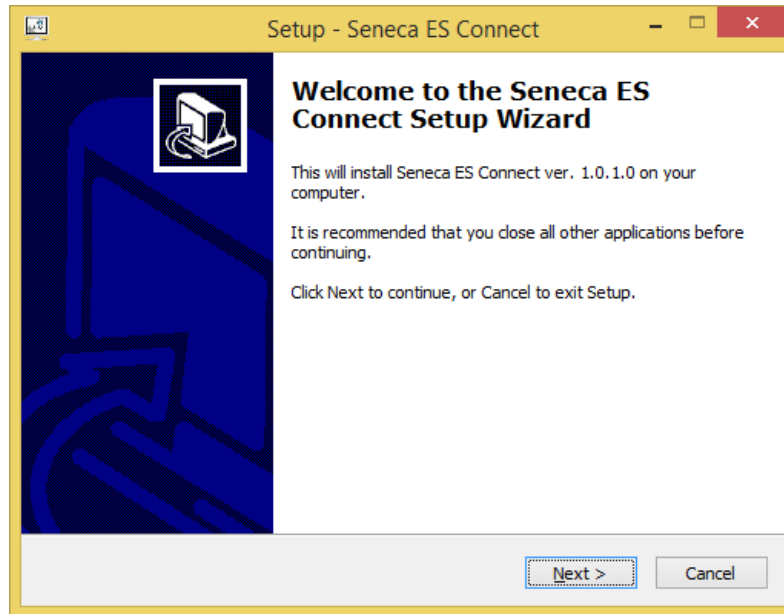
In the Virtual COM operating mode, just one connection is accepted for a given serial port.

11.1.1 Seneca Serial to Ethernet Connect

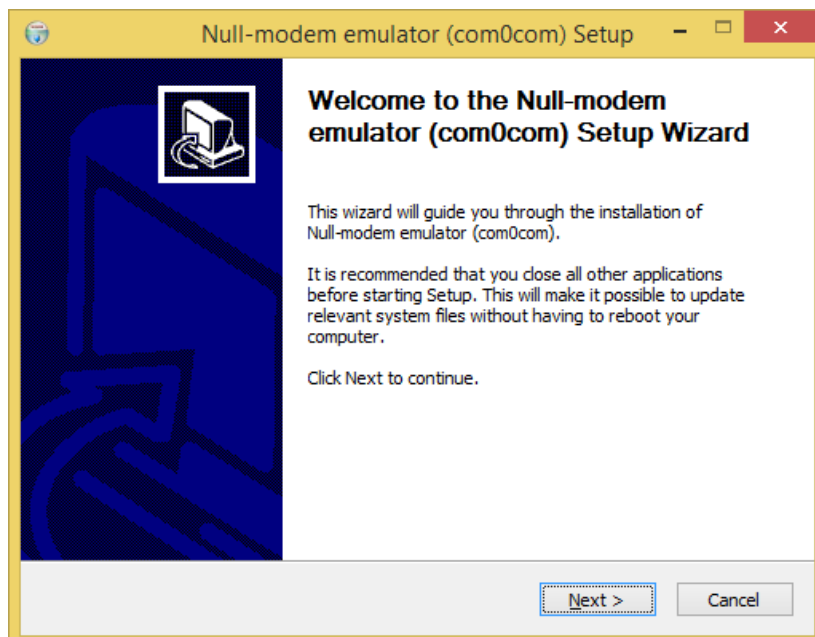
11.1.1.1 Installing Seneca Serial to Ethernet Connect driver

Seneca Ethernet to Serial Connect runs on Windows Vista™, Windows 7™ and Windows 8.1™.

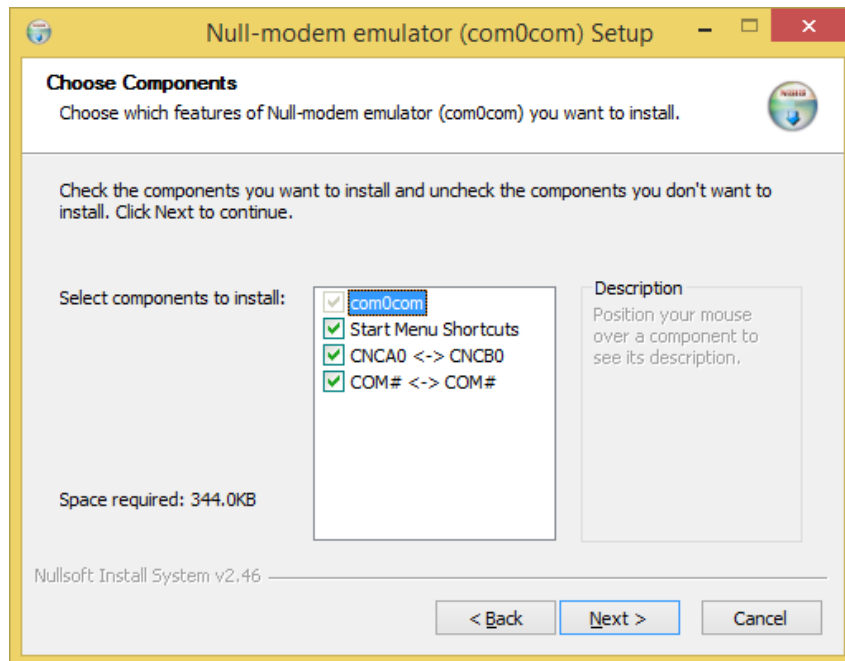
Double click the installer:



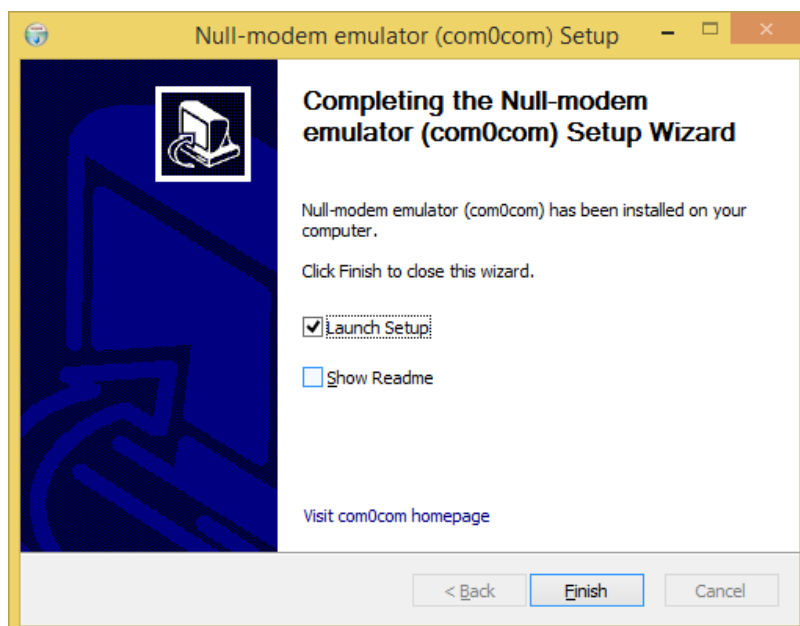
After that, the com0com driver will be installed:



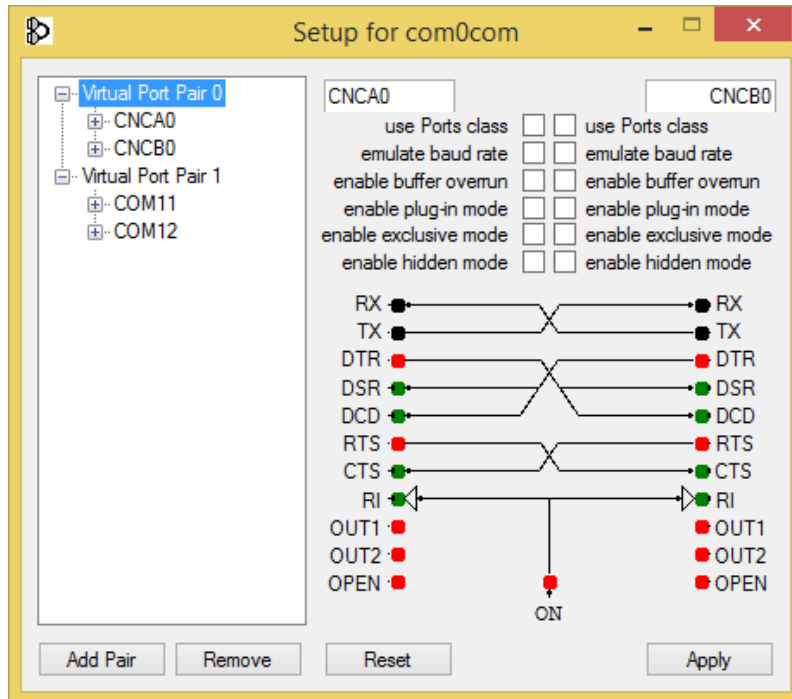
Select the CNCA0<->CNCB0 and the COM#<->COM# virtual port names:



Now Click on “Launch Setup”:



Press Finish, the com0com setup will open:



We have installed two pairs of Virtual Ports:

CNCA0, CNCB0

and also:

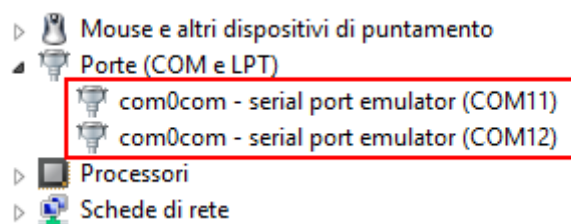
COM11, COM12 (note that in your system the com# can be different).

The first pair can be used in software that support the CNCA names, the other in software that support only the Ports class.

If you need to add more virtual ports, press the “Add Pair” button, then select if you need or not a port class.

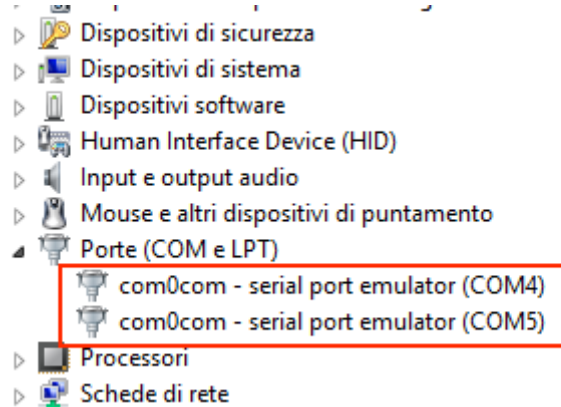
Confirm the driver installation with “Apply”.

The serial port emulator couple COM11-COM12 will be available:



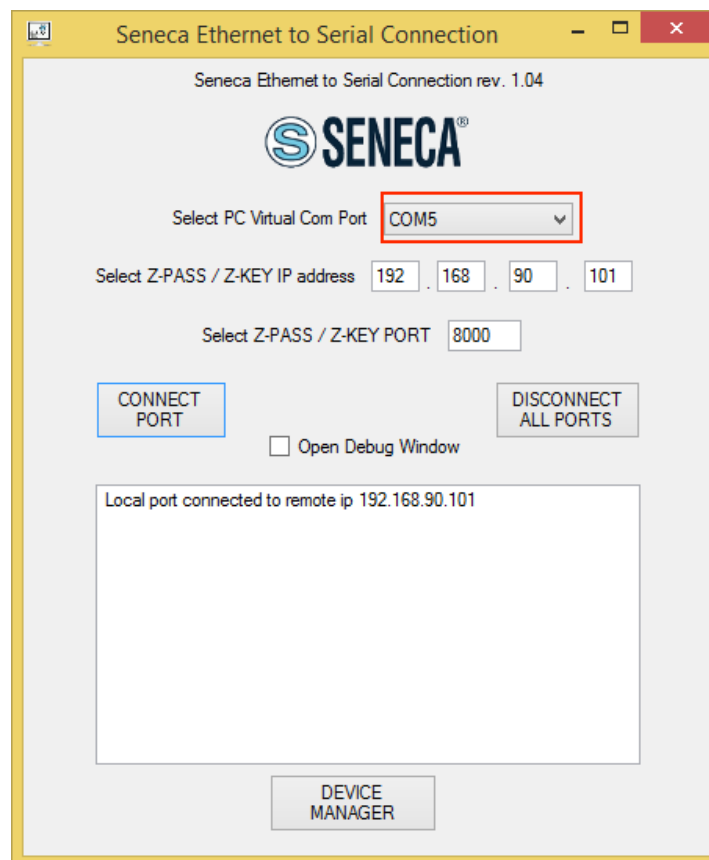
11.1.1.2 Select the COM port for Seneca Serial to Ethernet Connect

The driver installation will use the first 2 serial ports that are free (in our case the driver has created the COM4 and COM5 pair):

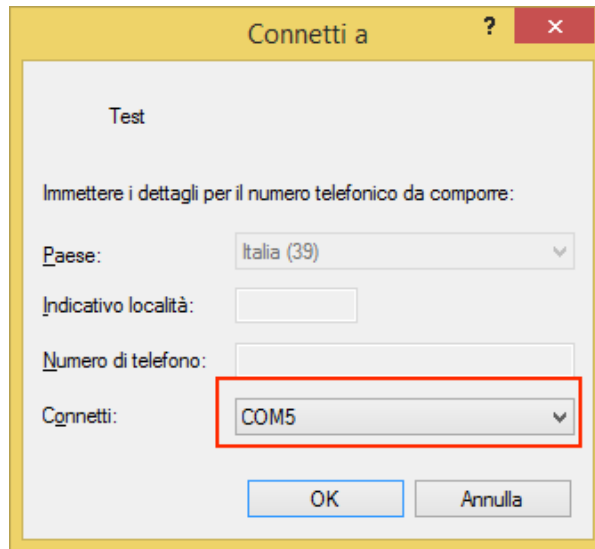


The Ethernet to Serial Connection software will use only one port (the right port in the com0com setup), only the com0com ports will be displayed.

We connect the COM5 to the Seneca ES Connector:

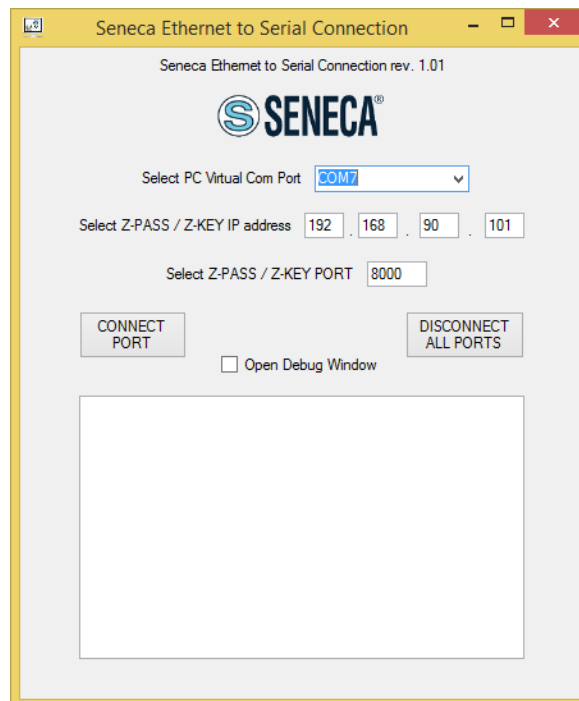


Now use the same COM5 (for example in a terminal software):



The COM5 is now connected to Z-PASS, on the TCP port 8000:

11.1.1.3 Configuring Seneca Serial to Ethernet Connect



- Select the Virtual COM Port
- Select the Z-PASS IP address (default 192.168.90.101).
- Select the TCP-IP port (default 8000).

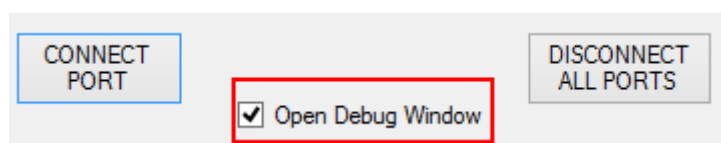
Then click on “CONNECT PORT”.

If you need to connect another serial com to another Z-PASS, configure the new com port and the new IP address, then click on “CONNECT PORT”.

To disconnect all ports, click on “DISCONNECT ALL PORTS”.

11.1.1.4 Debugging the Connection

Before clicking on “CONNECT PORT”, you can choose to open a debug window to verify the connection:



Then click on “CONNECT PORT”:

If you see “Connect Error” like here:

```

C:\WINDOWS\system32\cmd.exe
Connect(98) TCP(1) ERROR 10060 - <null>
TCP(1): Close(98) = OK
Socket(0.0.0.0:0) = c4
TCP(1): Connect(c4, 192.168.90.101:8000) ...
Connect(c4) TCP(1) ERROR 10060 - <null>
TCP(1): Close(c4) = OK
Socket(0.0.0.0:0) = 17c
TCP(1): Connect(17c, 192.168.90.101:8000) ...
Connect(17c) TCP(1) ERROR 10060 - <null>
TCP(1): Close(17c) = OK
Socket(0.0.0.0:0) = 17c
TCP(1): Connect(17c, 192.168.90.101:8000) ...
Connect(17c) TCP(1) ERROR 10060 - <null>
TCP(1): Close(17c) = OK
Socket(0.0.0.0:0) = c4
TCP(1): Connect(c4, 192.168.90.101:8000) ...
Connect(c4) TCP(1) ERROR 10060 - <null>
TCP(1): Close(c4) = OK
Socket(0.0.0.0:0) = c4
TCP(1): Connect(c4, 192.168.90.101:8000) ...
Connect(c4) TCP(1) ERROR 10060 - <null>
TCP(1): Close(c4) = OK
Socket(0.0.0.0:0) = 98
TCP(1): Connect(98, 192.168.90.101:8000) ...
    
```

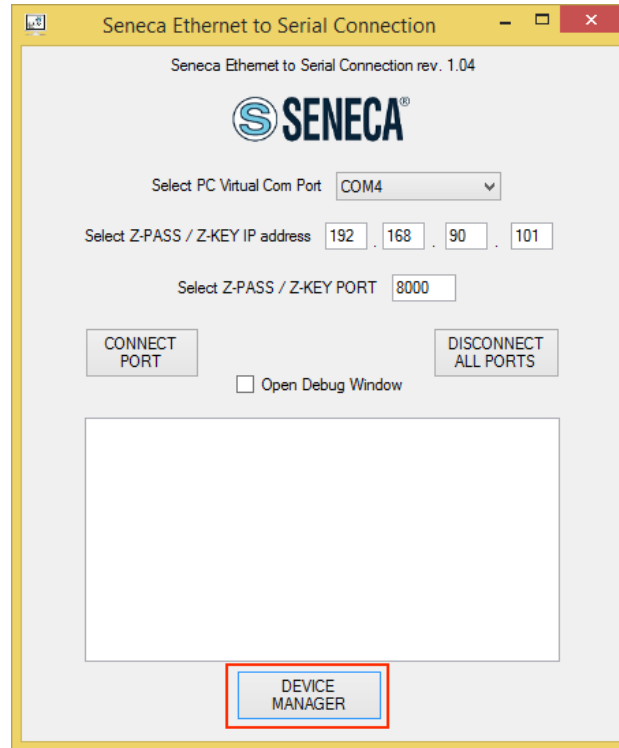
check the configuration (Z-PASS IP address and TCP port).

11.1.1.5 Changing the COM port number

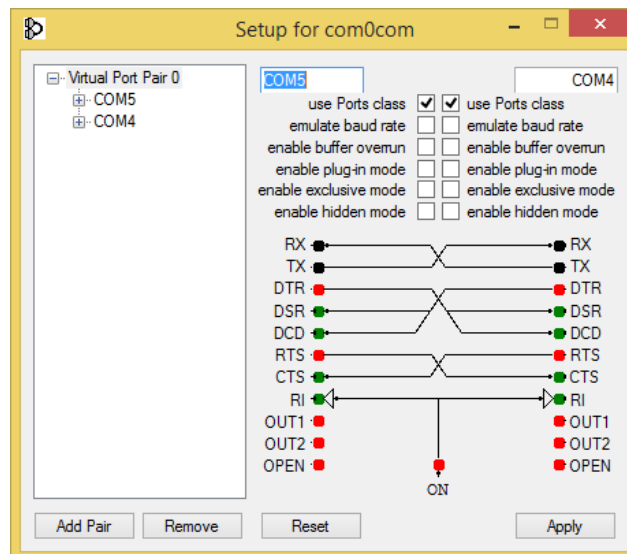
Old software applications can use only a little range of COM ports, so you may need to change the virtual COM number.

In our case the COM pair created is COM4/COM5, but we want to change it to COM2/COM3:

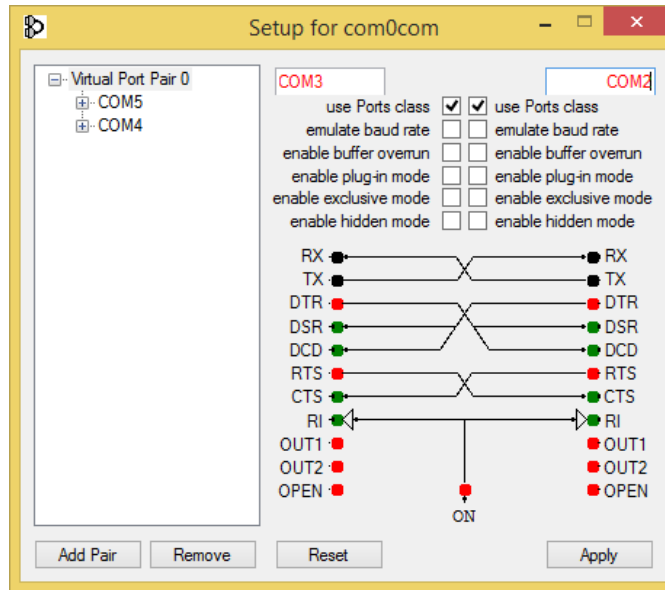
Click on “DEVICE MANAGER” button:



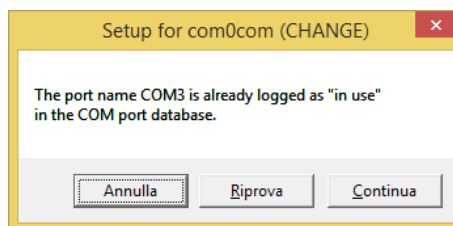
The com0com setup window will open:



Now change COM5 to COM3 and COM4 to COM2, then click “Apply”:

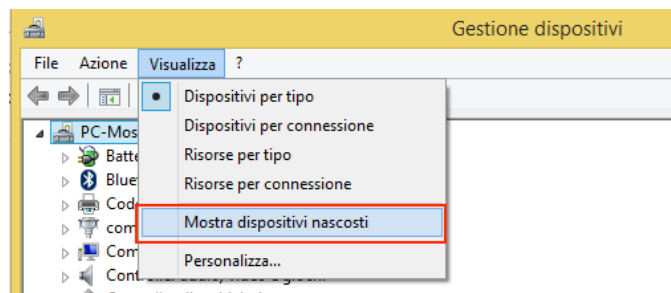


Sometimes the COM can be marked as “in use”:

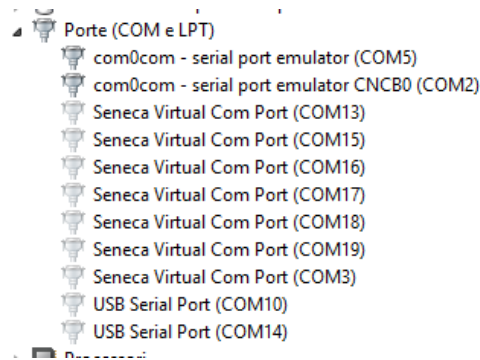


If you need to use this COM number, click on “Continue”, then go to the device manager.

We must uncheck the “in use” flag by uninstalling the port. Since the port is not connected, click on “Show hidden peripherals”:



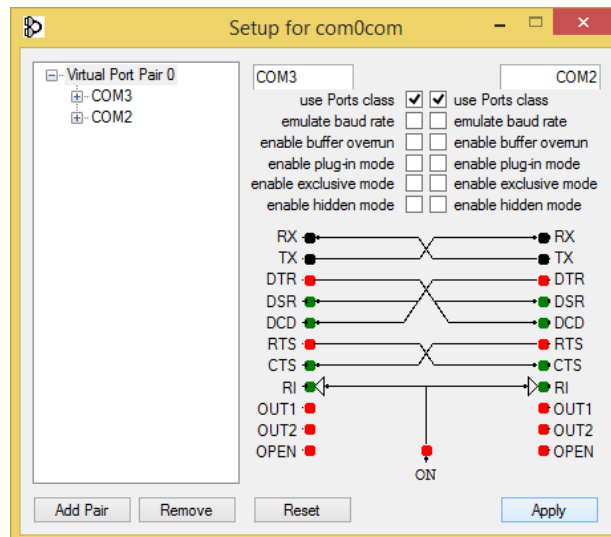
Now all the ports that are not in use are displayed in transparent (also our COM3):



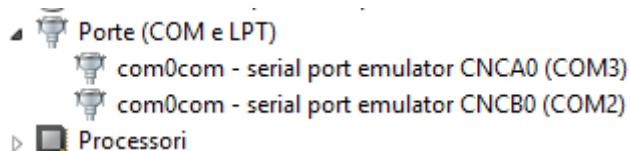
Now select the COM3 port and click on “Uninstall”:



Now the COM3 is free and we can use it on the com0com setup:

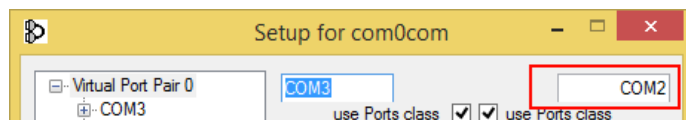


Finally click on “Apply”, now the COM3/COM2 pair is created:

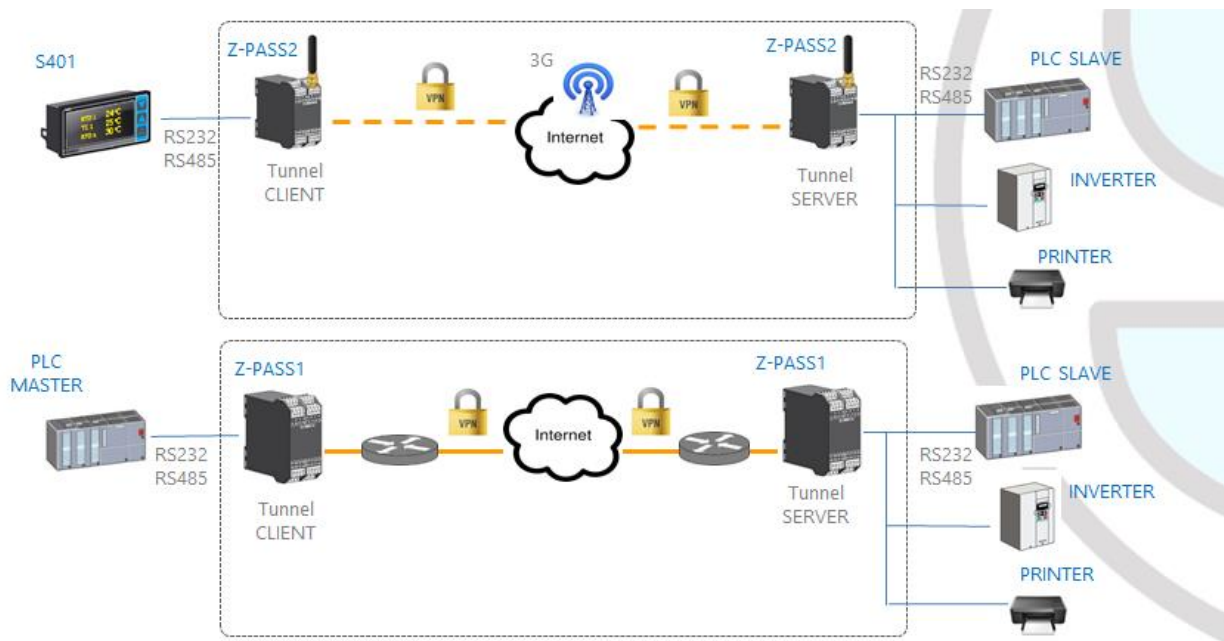


WARNING!

Seneca Serial to Ethernet connector always uses the right port in the com0com setup (in our case COM2).



11.2 Serial Tunnel Point-to-Point on TCP



The Serial Tunnel Point-to-Point allows to extend a serial connection between two serial devices that support the same serial protocol by a TCP/UDP connection.

In TCP operating mode, one Z-PASS is defined as the “Master” and another Z-PASS is the “Slave”: the first is a Tunnel Client, which receives data from the serial line and sends them to an outgoing TCP connection, while the second is a Tunnel Server, which receives data from an incoming TCP connection and sends them to the serial line; in this mode a “tunnel” is established between the two serial ports.

In configuration phase, on the Master it is necessary to set the Destination IP Address and the Destination Port that defines the outgoing TCP connection; on the Slave, you have to set the Listen Port on which the incoming TCP connection is accepted.

The tunnel can be established through the LAN (Ethernet) or through the WAN (Mobile Network), also exploiting VPN connectivity.

WARNING!

In the Serial Tunnel Point-to-Point on TCP operating mode, just one connection is accepted for a given serial port.

11.3 Serial Tunnel Point-to-Point on UDP

The Serial Tunnel Point-to-Point on UDP operating mode is much like that on TCP.

The only difference is that no TCP connection is established and serial data are transported by UDP packets.

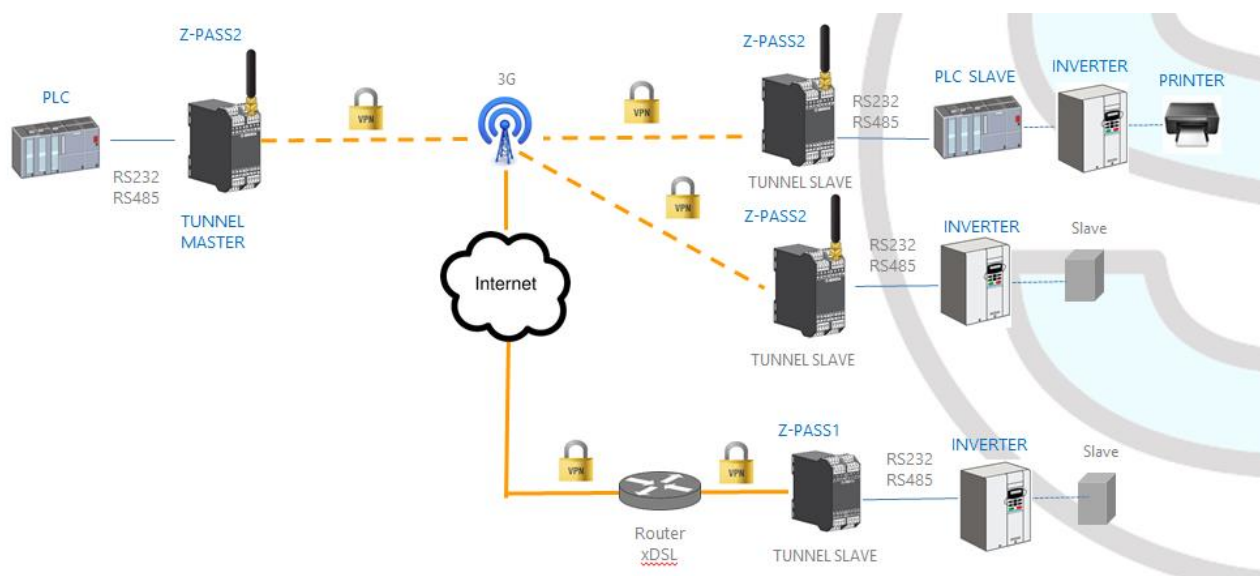
The configuration parameters are the same as those for the serial tunnel on TCP.

Also in this case, the tunnel can be established through the LAN (Ethernet) or through the WAN (Mobile Network), also exploiting VPN connectivity.

WARNING!

In the Serial Tunnel Point-to-Point on UDP operating mode, just one connection is accepted for a given serial port.

11.4 Serial Tunnel Point-to-Multipoint



The Serial Tunnel Point-to-Multipoint allows to create a tunnel with a master and more than one slave; on the master side, the data received from the serial line are sent to all the slaves, by means of *multicast* transmission mode, in UDP packets.

To let the multicast work, the master and the slaves shall be part of the same *multicast group*, so there is a “Multicast Group” parameter that shall be properly set; furthermore, for the Master Configuration have to be defined “Destination Port” and “Multicast Interface” parameters, the latter shall be set to select the network interface that allows to send the packets; for the slave configuration, “Listen Port” and “Multicast Interface” are requested; the latter shall be set to select the network interface which allows to receive the packets.

The tunnel can be established through the LAN (Ethernet) or through the VPN (Ethernet or 3G based).

WARNING!

In the Serial Tunnel Point-to-Multipoint operating mode, just one connection is accepted for a given serial port.

12 Modbus Shared Memory Gateway

Z-PASS can be configured to run as a Modbus Shared Memory Gateway: in this mode, a set of configured tags are periodically and continuously read from Modbus RTU devices and these values are always available in a shared memory, readable via Modbus TCP.

Z-PASS Modbus Shared Memory Gateway supports up to 2000 tags and up to 32 Modbus TCP Client simultaneously.

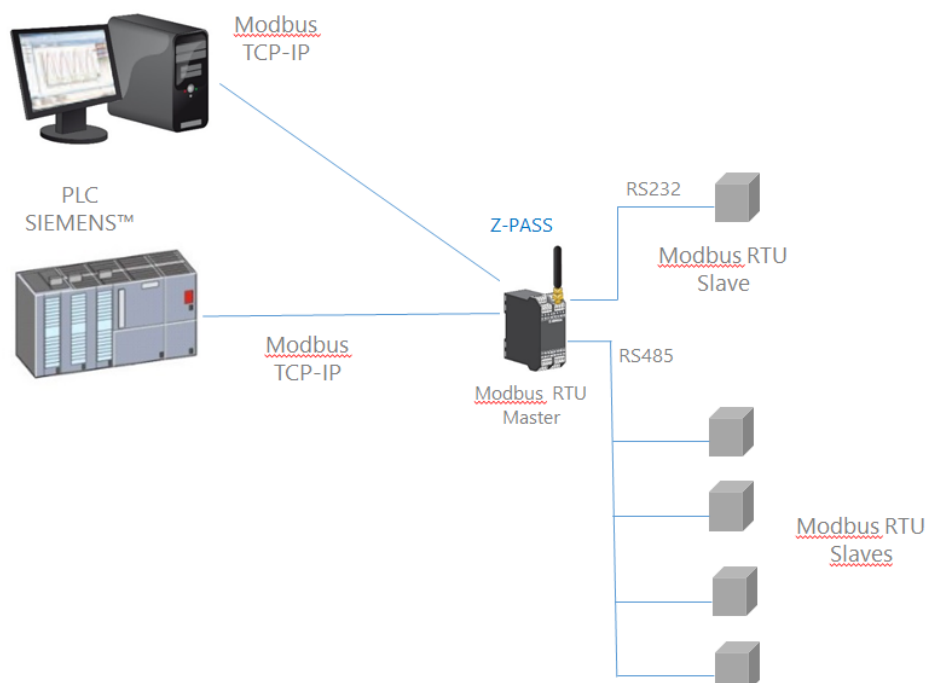
In the Z-PASS Modbus Shared Memory Gateway, a Modbus TCP/IP Server (or slave) is always running on a configured TCP port.

As for Modbus Ethernet to Serial Gateway functionality (see chapter 10), the Modbus TCP requests can be forwarded through the Ethernet interface or through the Mobile/VPN interface.

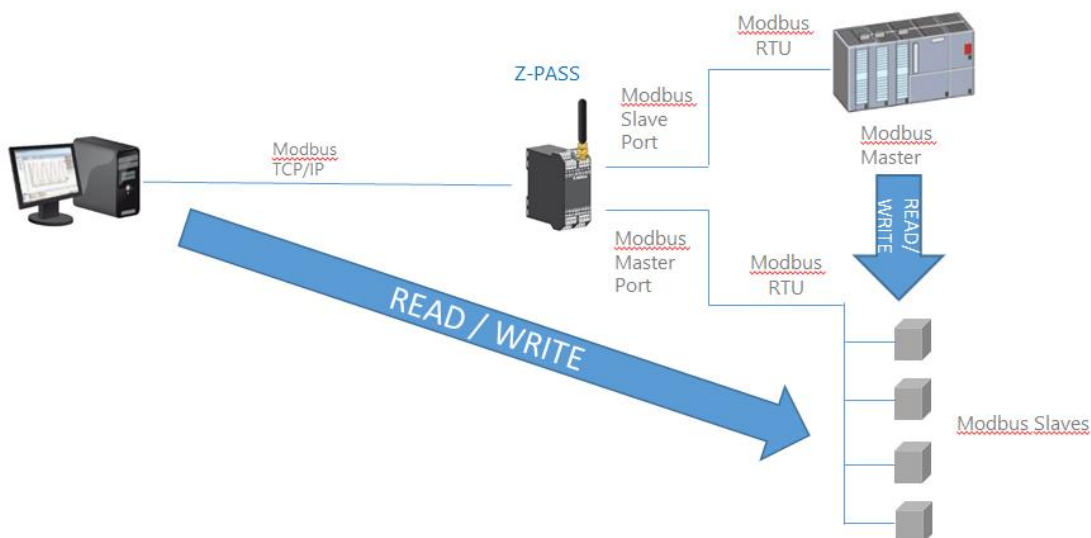
Then, for each of the three available serial ports (COM1, COM2, COM4), the kind of “Task” can be defined: a serial port can be Configured as a Modbus RTU Master or Modbus RTU Slave or not running at all.

In this manner, a number of possible combinations are available, to a maximum of three Modbus RTU Masters or three Modbus RTU Slaves; normally, a combination of the two will be chosen, for example: Modbus RTU Slave on COM1 and Modbus RTU Masters on COM2,COM4.

In the following pictures are shown, some typical scenarios.



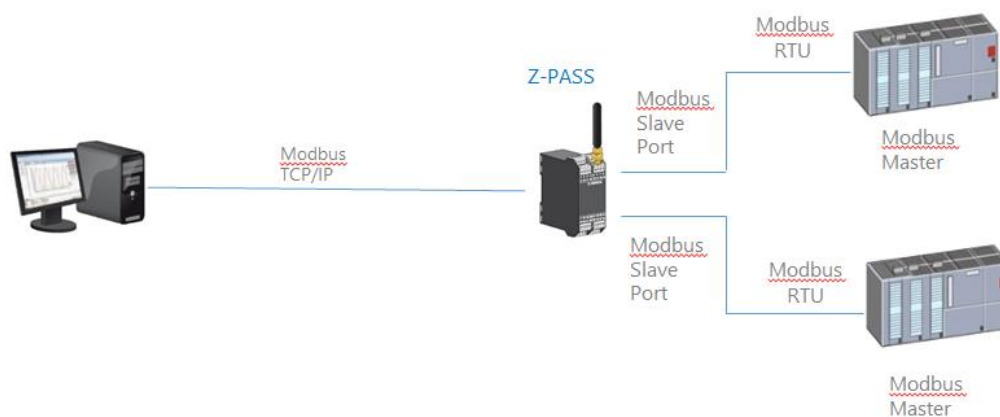
In the above picture, two serial ports (RS232 – COM1, RS485 – COM2) are configured as Modbus RTU Master.



In this case, one serial port (e.g. COM1) is configured as Modbus Slave and another (e.g. COM2) is configured as Modbus Master.

When some measures acquired from the Modbus Slaves must be available for a PLC, which supports only Modbus Master protocol, and also for a SCADA/Datalogger, the Z-PASS can be configured with one serial port defined as Modbus Slave (connected to the PLC) and another in Modbus Master (connected to the Modbus Slaves bus).

The PLC Modbus RTU Master and the Modbus TCP client(s) write/read the Z-PASS shared memory registers, while the Z-PASS Modbus Shared Memory Gateway keeps the shared memory aligned with the Modbus Slaves registers.



In the above picture, two serial ports (e.g. COM2 and COM4) are configured as Modbus Slave and connected to a PLC Modbus Master port; so, the two PLCs and the Modbus TCP Client can write/read the Z-PASS shared memory to share data among them.

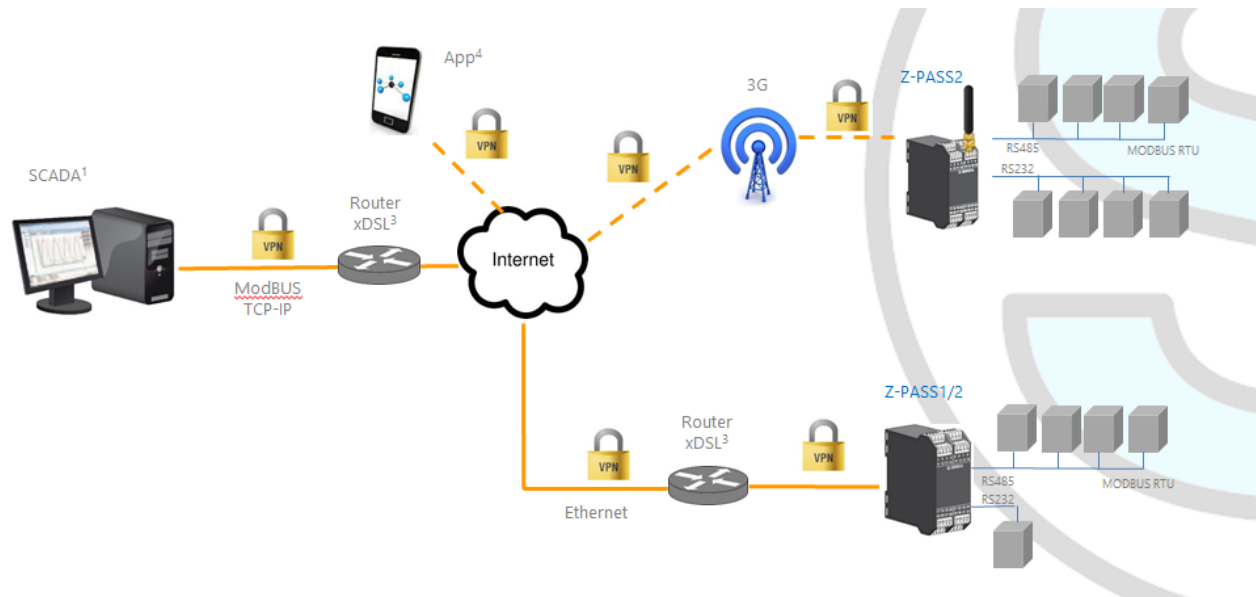
The Z-PASS Modbus Shared Memory Gateway provides some interesting features as explained in the following.

Besides “classic” gateway behavior, Tags can be configured to work in “Bridge” mode; this mode allows to acquire Tag values from the serial side, only when Gateway receives Modbus TCP Requests; that can be very useful when in the serial line there are RTU devices with “Fail safe” outputs⁴, as explained in details in 19.5.1 paragraph.

Z-PASS Modbus Shared Memory Gateway performs Requests optimization on the RTU side, inserting as many tags as possible in a single read/write request; the maximum number of registers in a request can be set independently for each serial port and for read and write operations; this option can be useful to connect RTU devices which support different maximum number of registers on different serial ports.

Tag configuration can be created using a Microsoft Excel™ Template provided by Seneca (see 19.5.3 paragraph); this can largely reduce configuration time, particularly when a large number of tags shall be configured.

13 VPN



Z-PASS supports 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;

⁴ This feature is available in many Seneca products.

- 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 Z-PASS shall be installed in an already existing VPN. In this case, an OpenVPN server shall be available and the configuration, certificate and key files for the Z-PASS client shall be provided by the VPN administrator; the files can be uploaded to the Z-PASS using the “VPN configuration” page of Z-PASS 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 (Z-PASS) and to other machines which lie in the Z-PASS 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 subnet.

In the “Point-to-Point” VPN, a client PC, in a given moment, can perform a single connection, on demand, to only one device (Z-PASS) (and to machines which lie in the Z-PASS 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.

There are two kinds of “Point-to-Point” VPN:

- routing Layer 3 VPN
- bridging Layer 2 VPN

In “Routing Layer 3 VPN”, only IP (Layer 3) packets are transported over the VPN tunnel and a new virtual LAN is created with a network subnet which must be different from the LAN subnets of the server and clients.

Conversely, in “Bridging Layer 2 VPN”, all Ethernet frames are transported over the VPN tunnel and the clients are inserted in the server LAN.

Each of the two kinds has benefits and drawbacks:

Layer 2 benefits/drawbacks:

- can transport any network protocol
- broadcast traffic (e.g.: DHCP) is transported
- causes much more traffic overhead on the VPN tunnel

Layer 3 benefits/drawbacks:

- can transport only IP traffic
- broadcast traffic (e.g.: DHCP) is not transported

- lower traffic overhead, transports only traffic which is destined for the VPN clients

The “VPN Box” is supplied with two Windows applications:

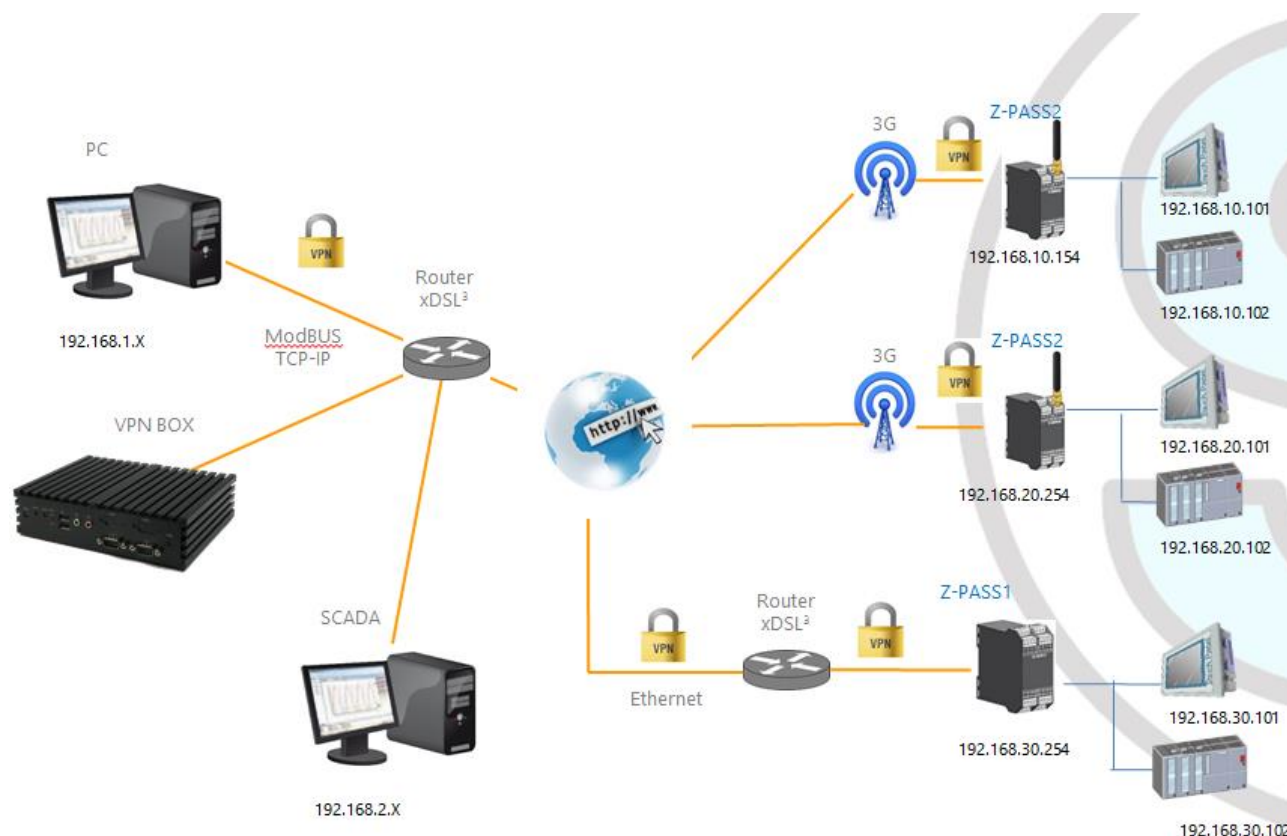
- the “VPN Box Manager”, which allows to configure the VPN⁵ mode on the VPN Box and manage the devices⁶
- the “VPN Client Communicator”, which lets the user connect the PC to the network (in the “Single LAN” case) or to a specific device (in the “Point-to-Point” case)

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

A detailed description of Z-PASS VPN configuration parameters is given in 19.7 paragraph.

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

13.1 “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 by using its 192.168.10.154 IP address and to the PLC in the Z-PASS 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.

⁵ Only one of the two kinds of VPN can be configured on a given VPN Box.

⁶ “VPN Box” functionality is available also on Seneca Z-TWS4, Z-PASS2-S and S6001-RTU products.

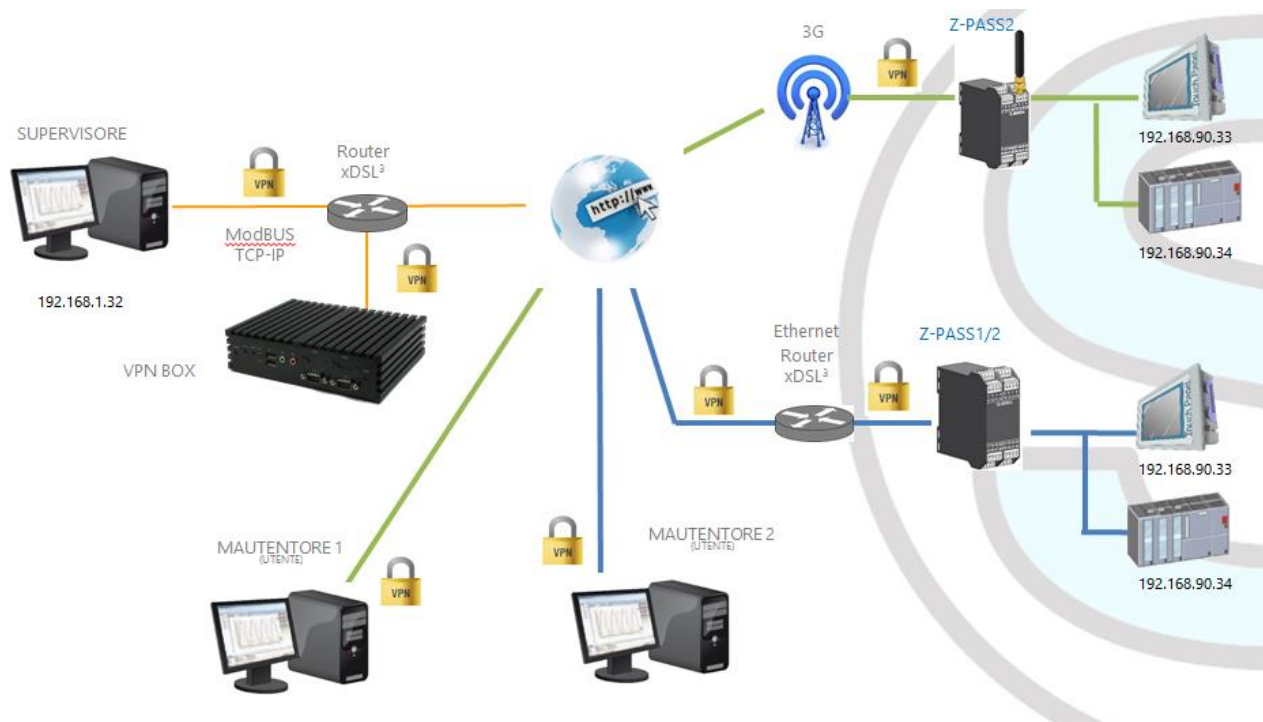
To let this scenario work correctly, an essential rule must always be followed: the Z-PASS LANs and the PC LAN shall have different and not colliding subnets; so, in the above figure, the following subnets allocation has been depicted:

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 19.8 paragraph).

13.2 “Point-to-Point” VPN



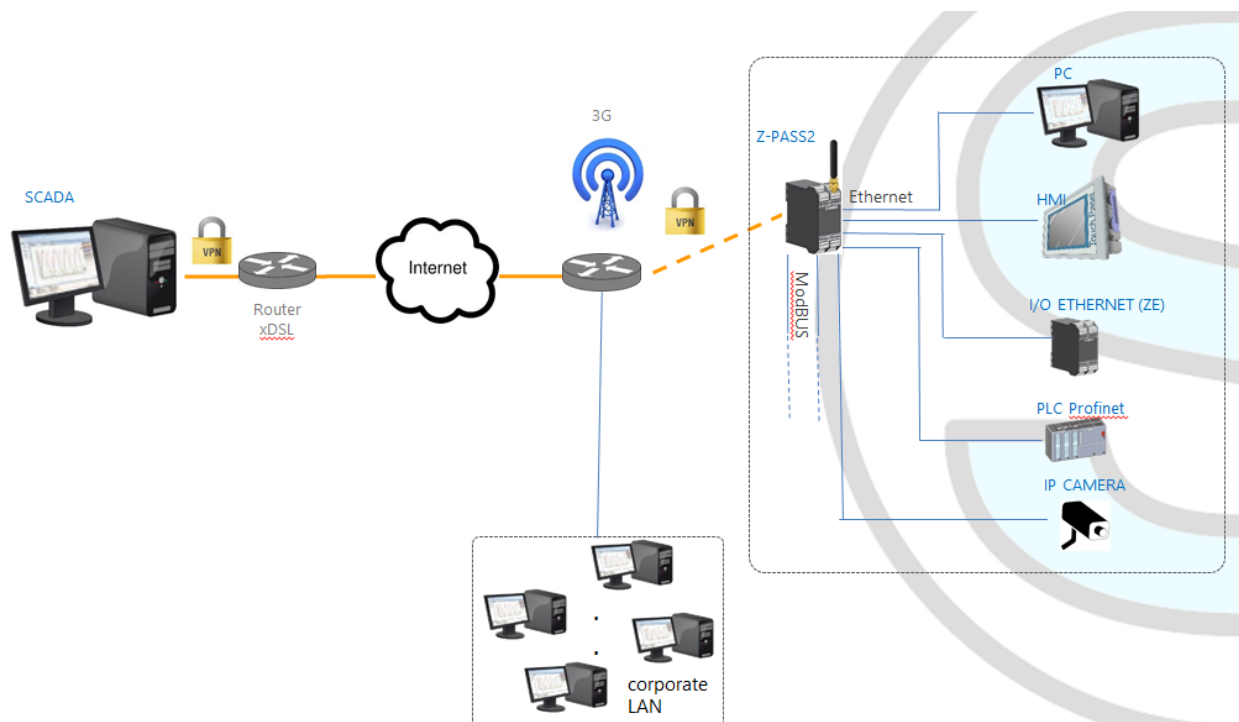
The above figure gives an example of a “Point-to-Point” VPN.

In this scenario a PC (acting as a VPN Client) can connect, on demand, to only one Z-PASS and its subnet, using local IP addresses. Since the client “sees” just one Z-PASS (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.

14 Router



As already told before, “Router” functionality routes packets between the LAN (Ethernet) interface and the WAN (Mobile Network) interface; so, this functionality specially makes sense when a mobile connection is active, which needs the availability of a 3G modem (true for Z-PASS2).

More specifically, an important feature of the Router is what is known as “IP forwarding”; this means that when Z-PASS 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, Z-PASS also performs what is known as “IP masquerading”, meaning that the original source IP address is replaced with the IP address of the WAN (PPP) 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.

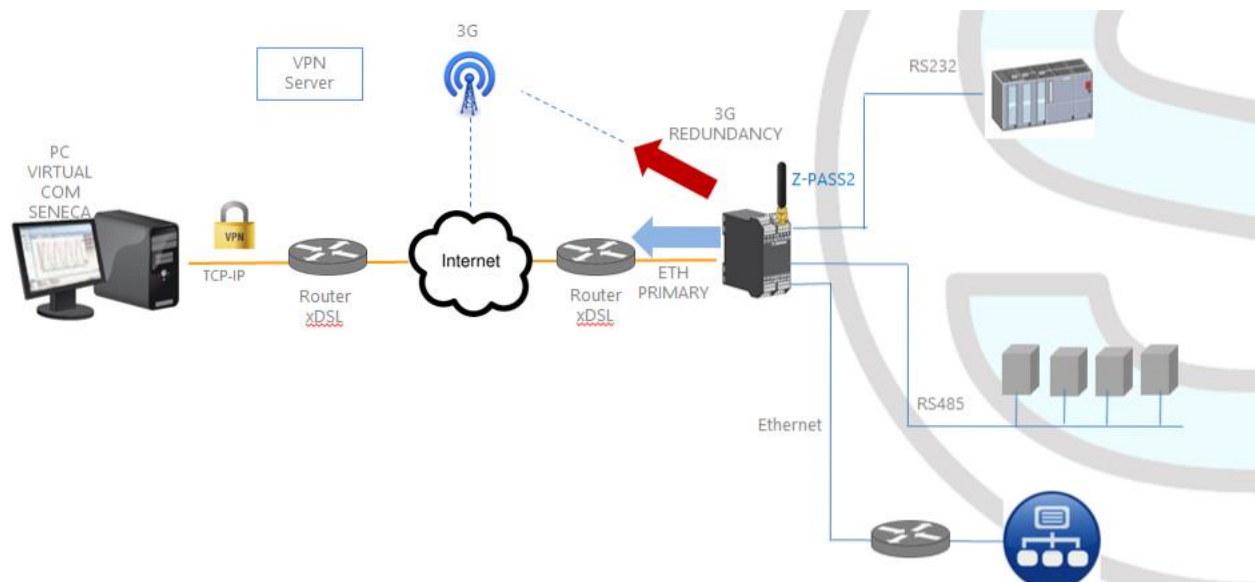
Also, a DHCP server is available which assigns IP addresses to clients connected on the Z-PASS LAN; here, you can configure the range of addresses used by the server and the lease time.

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 from a TCP or UDP port to another Z-PASS 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 19.8 paragraph.

15 Network Redundancy



“Network Redundancy” is a functionality that can be enabled on Z-PASS2 devices, where a 3G modem is available.

This functionality is aimed at switching 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 becomes available again, the network interface is switched back to Ethernet.

The parameters provided to configure Network Redundancy are explained in paragraph 19.2 “Network and Services”.

16 Remote Connection Disable

Z-PASS1-IO and Z-PASS2-IO products provide a dedicated digital input and a dedicated digital output to control and monitor remote connection to the device.

In details:

- when “Remote Connection Disable” digital input is set to HIGH state, remote connection to the device is disabled; conversely, when “Remote Connection Disable” digital input is set to LOW state, remote connection to the device is enabled; “Remote Connection Disable” digital input state is reported by the “RCD” LED;
- “Remote Connection 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 connection:

- 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 send/receive SMSs;
- Level 3 (“Internet Connection”): any Internet access is disabled, but the device can still send/receive SMSs;
- Level 4 (“SMS Service”): modem is off, so SMSs can’t be sent/received.

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

17 Auto-APN

The Auto-APN feature lets the Z-PASS establish mobile data connections without requiring the user to configure APN data⁷ 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 DB⁸, 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 19.12).

18 SMS Commands

On Z-PASS devices, a number of features can be controlled by means of “SMS commands”; such features include setting up a mobile data (PPP) connection, activating the VPN Box functionality, setting a digital output etc.

SMS Commands can be sent by phone numbers that are present in the Z-PASS Phonebook as “admin” or “manager” users; as an alternative, any phone number can send an SMS command, provided that the command contains a “password”; the password is made by the last four digits of the Z-PASS modem IMEI; so the command will have the following format (there must be a blank character between the “password” and the command text):

```
<last four IMEI digits> <command text>
```

Example:

```
6172 PPP ON
```

Please note that the command text can be written in any letter case, all uppercase, all lowercase or a mix between the two.

⁷ APN data are: APN, Username, Password and Authentication Type.

⁸ This DB is updated to the one used in the last Android O.S. version.

Any SMS command received from a number that is not recognized as an “admin” or “manager” user and does not contain the password will be discarded; as an option, these messages and all messages that are not recognized as valid commands can be “relayed” to the “admin” user (see paragraph 19.15).

Example:

```
PPP ON RELAYED
```

SMS commands substantially fall into two categories:

- “set” commands which execute an action
- “get” commands which ask for some information

While “get” commands always have an answer, “set commands” can be given an answer (“acknowledge”) or not, depending on a configuration parameter (see paragraph 19.15).

Any response to a command, both “set” or “get”, will contain the original message text, plus a result string, which can be:

“EXECUTING”

meaning that the command has been correctly processed; the “ING” form is used to tell that the procedure started by the command might not be completed yet

“FAILED”

meaning that the command could not be processed or something failed; in this case, an error string is present giving the failure reason

Examples:

```
PPP ON EXECUTING (100.70.179.88)
```

```
PPP ON FAILED (System PPP ON)
```

Obviously, the response to a “get” command also contains the requested info, if the command has been successfully processed.

Example:

```
GET DIN EXECUTING (1,0,0,0)
```

Finally, the whole SMS commands functionality can be disabled, if not needed, by means of a configuration parameter (see paragraph 19.15).

Obviously, SMS commands are available only in Z-PASS2 product (for all HW revisions), where a GSM model is available.

In the following paragraphs, the full list of supported commands is given along with the corresponding responses.

18.1 PPP ON

This command can be used to setup the mobile data (PPP) connection; the connection is setup using system configuration parameters (APN Mode, APN, Auth Type etc.).

If the command is successfully processed, the response contains the IP address assigned to the PPP network interface.

This command is rejected in the following cases:

- if the mobile data (PPP) connection is enabled in the system configuration (parameter "Data Connection/Enable" = ON), the command will fail with the "System PPP ON" error;
- if "Remote Connection Disable" (RCD) digital input is HIGH and "Security Level/Service Disable" parameter is set to "Internet Connection", the command will fail with the "Security Level error" error.

Also, if the connection setup procedure is not completed after a timeout (currently fixed to 30 seconds), the command will fail with the "Timeout error" error.

Please note that this command that does not enable the mobile data connection in a persistent way, so if the Z-PASS is restarted, the mobile data (PPP) connection is not re-established.

Example:

```
→ PPP ON
← PPP ON EXECUTING (100.70.179.88)
```

18.2 PPP OFF

This command can be used to drop down the mobile data (PPP) connection setup by a previous "PPP ON" command.

This command is rejected in the following case:

- if the mobile data (PPP) connection is enabled in the system configuration (parameter "Data Connection/Enable" = ON), the command will fail with the "System PPP ON" error.

Example:

```
→ PPP OFF
← PPP OFF EXECUTING
```

18.3 PPP IP

This command can be used to get the IP address assigned to the mobile data (PPP) connection; if the PPP connection is not active, the "dummy" IP address (0.0.0.0) will be given.

This command is never rejected.

Example:

```
→ PPP IP
← PPP IP EXECUTING (100.70.179.88)
```

18.4 PPP CNF

This command can be used to change the value of the system configuration parameters related to the mobile data (PPP) connection.

The command shall have the following format, where parameter values shall be separated by a blank character:

```
PPP CNF <APN mode> <APN> <Authentication Type> <Username> <Password> <PPP Connection
Testing IP Address>
```

Please note that all the parameters shall be present, in the above order; no parameter can be left empty.

For the meaning of these parameters, please see 19.12 paragraph.

<APN> and <Authentication Type> are numeric fields with the following values.

APN Mode

```
0:    Automatic
1:    Manual
```

Authentication Type

```
0:    None
1:    CHAP/PAP
2:    CHAP only
3:    PAP only
```

This command is rejected in the following cases:

- if the mobile data (PPP) connection is enabled in the system configuration (parameter “Data Connection/Enable” = ON), the command will fail with the "System PPP ON" error;
- if any of the command parameters is missing or invalid, the command will fail with the “Command parameter error”.

Example:

```
→ PPP CNF 0 mobile.vodafone.it 0 user pass www.google.com
← PPP CNF EXECUTING
```

18.5 VPN ON

This command can be used to activate the VPN Box functionality; the functionality is activated using system configuration parameters (Server, Password, Tag Name).

The command has two optional parameters, so its format is the following:

```
VPN ON [PPP] [NOFWL]9
```

“ppp”

if this parameter is present, the mobile data (PPP) connection is setup (if it’s not already active), before activating the VPN Box functionality

“NOFWL”

if this parameter is present, the “Mobile Network Firewall” is disabled, in the system configuration

This command is rejected in the following cases:

⁹ Square brackets tell that parameter is optional.

- if the VPN Box functionality is enabled in the system configuration (parameter “VPN Box/Enable” = ON, “VPN Mode” = “VPN Box”), the command will fail with the "System VPN ON" error;
- if the “custom” VPN functionality is enabled in the system configuration (parameter “VPN/Enable” = ON, “VPN Mode” = “OpenVPN”), the command will fail with the "System VPN ON" error;
- if “Remote Connection Disable” (RCD) digital input is HIGH and “Security Level/Service Disable” parameter is set to “VPN Connection” or “VPN Service” or “Internet Connection”, the command will fail with the "Security Level error" error.

Please note that this command that does not activate the VPN Box functionality in a persistent way, so if the Z-PASS is restarted, the functionality is not re-activated.

Examples:

```
→ VPN ON
← VPN ON EXECUTING

→ VPN ON PPP
← VPN ON PPP EXECUTING

→ VPN ON NOFWL
← VPN ON NOFWL EXECUTING

→ VPN ON PPP NOFWL
← VPN ON PPP NOFWL EXECUTING
```

18.6 VPN OFF

This command can be used to deactivate the VPN Box functionality activated by a previous “VPN ON” command; it also drops down the mobile data (PPP) connection setup by a previous “VPN ON PPP” command or “PPP ON” command.

This command is rejected in the following case:

- if the VPN Box functionality is enabled in the system configuration (parameter “VPN Box/Enable” = ON, “VPN Mode” = “VPN Box”), the command will fail with the "System VPN ON" error.

Example:

```
→ VPN OFF
← VPN OFF EXECUTING
```

18.7 VPN CNF

This command can be used to change the value of the system configuration parameters related to the VPN Box.

The command shall have the following format, where parameter values shall be separated by a blank character:

```
VPN CNF <Server> <Password> <Tag Name>
```

Please note that all the parameters shall be present, in the above order; no parameter can be left empty.

For the meaning of these parameters, please see 19.7.2 paragraph.

This command is rejected in the following cases:

- if the VPN Box functionality is enabled in the system configuration (parameter “VPN Box/Enable” = ON, “VPN Mode” = “VPN Box”), the command will fail with the "System VPN ON" error;
- if any of the command parameters is missing or invalid, the command will fail with the “Command parameter error”.

Example:

```
→ VPN CNF myvpnbox.seneca.it myvpnbox zpass2-GSP
← VPN CNF EXECUTING
```

18.8 FWL ON

This command can be used to enable the “Mobile Network Firewall” in the system configuration (parameter “Mobile Network Firewall/Enable” = ON).

This command is never rejected.

Example:

```
→ FWL ON
← FWL ON EXECUTING
```

18.9 FWL OFF

This command can be used to disable the “Mobile Network Firewall” in the system configuration (parameter “Mobile Network Firewall/Enable” = OFF).

This command is never rejected.

Example:

```
→ FWL OFF
← FWL OFF EXECUTING
```

18.10 GET DIN

This command can be used to get the status of one or all of the four digital inputs; if a digital input is not available (since it is used as an output)¹⁰, the “0” value is given.

The command can have two formats:

GET DIN<n>	with <n>=1..4	get the status of a single digital input
GET DIN		get the status of all the digital inputs

This command is rejected in the following cases:

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which has no digital I/Os, the command will fail with the “Digital I/O not available” error;

¹⁰ This can be true for DI3 and DI4.

- if the digital I/O number in the command is out of range (e.g.: 0 or 5), the command will fail with the “Command parameter error” error.

Examples:

```
→ GET DIN
← GET DIN EXECUTING (1,0,0,0)

→ GET DIN1
← GET DIN1 EXECUTING (1)

→ GET DIN2
← GET DIN2 EXECUTING (0)
```

18.11 GET DOUT

This command can be used to get the status of one or all of the four digital outputs; if a digital output is not available (since it is used as an input)¹¹, the “0” value is given.

The command can have two formats:

GET DOUT<n>	with <n>=1..4	get the status of a single digital output
GET DOUT		get the status of all the digital outputs

This command is rejected in the following cases:

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which has no digital I/Os, the command will fail with the “Digital I/O not available” error;
- if the digital I/O number in the command is out of range (e.g.: 0 or 5), the command will fail with the “Command parameter error” error.

Examples:

```
→ GET DOUT
← GET DOUT EXECUTING (0,1,0,0)

→ GET DOUT1
← GET DOUT1 EXECUTING (0)

→ GET DOUT2
← GET DOUT2 EXECUTING (1)
```

18.12 SET DOUT

This command can be used to set the status of one of the four digital outputs.

The command can have two formats:

SET DOUT<n>.CLOSE	with <n>=1..4	set the digital output to the HIGH state
SET DOUT<n>.OPEN	with <n>=1..4	set the digital output to the LOW state

This command is rejected in the following cases:

¹¹ This can be true for DO3 and DO4.

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which has no digital I/Os, the command will fail with the “Digital I/O not available” error;
- if the digital output is not configured as “General output” or the digital I/O is used as an input¹², the command will fail with the “Digital I/O mode error” error;
- if the digital I/O number in the command is out of range (e.g.: 0 or 5), the command will fail with the “Command parameter error” error;
- if the requested state is neither “.CLOSE”, nor “.OPEN”, the command will fail with the “Command parameter error” error.

Example:

```
→ SET DOUT2.CLOSE
← SET DOUT2.CLOSE EXECUTING
```

18.13 SET PULSE

This command can be used to generate a pulse on one of the four digital outputs.

The command can have two formats:

SET PULSE<n>.CLOSE <duration> with <n>=1..4

to generate a LOW-HIGH-LOW pulse, with the HIGH state set for the number of seconds given by the <duration> parameter

SET PULSE<n>.OPEN <duration> with <n>=1..4

to generate a HIGH-LOW-HIGH pulse, with the LOW state set for the number of seconds given by the <duration> parameter

This command is rejected in the following cases:

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which has no digital I/Os, the command will fail with the “Digital I/O not available” error;
- if the digital output is not configured as “General output” or the digital I/O is used as an input¹³, the command will fail with the “Digital I/O mode error” error;
- if the digital I/O number in the command is out of range (e.g.: 0 or 5), the command will fail with the “Command parameter error” error;
- if the requested state is neither “.CLOSE”, nor “.OPEN”, the command will fail with the “Command parameter error” error;
- if the <duration> parameter is missing or invalid, the command will fail with the “Command parameter error” error;
- if the “.CLOSE” parameter is given and the digital output is already in the HIGH state, the command will fail with the “No pulse generated” error;
- if the “.OPEN” parameter is given and the digital output is already in the LOW state, the command will fail with the “No pulse generated” error.

Example:

```
→ SET PULSE2.CLOSE 10
```

¹² This can be true for DO3 and DO4.

¹³ This can be true for DO3 and DO4.

← SET PULSE2.CLOSE 10 EXECUTING

18.14 SET USER.PHONE

This command can be used to insert a user with the specified telephone number and type into the Phonebook; it can also be used to change the type of an already existing user.

The command has the following format:

SET USER.PHONE +<number> <type>, with <type>=ADM|MGR|USR

Please note that the telephone number shall always be given in the “international format”, so the initial ‘+’ character shall always be present.

This command is rejected in the following cases:

- if the specified <number> already exists in the Phonebook, with the specified <type>, the command will fail with the “Number already exists” error;
- if the <number> parameter is missing or invalid (including the case when the ‘+’ character is missing), the command will fail with the “Command parameter error” error;
- if the <type> parameter is missing or invalid, the command will fail with the “Command parameter error” error.

Example:

→ SET USER.PHONE +390123456789 ADM
← SET USER.PHONE +390123456789 ADM EXECUTING

18.15 RESET PHONE

This command can be used to delete a user with the specified telephone number from the Phonebook.

The command has the following format:

RESET PHONE +<number>

Please note that the telephone number shall always be given in the “international format”, so the initial ‘+’ character shall always be present.

This command is rejected in the following cases:

- if the specified <number> does not exist in the Phonebook, the command will fail with the “Number does not exist” error;
- if the <number> parameter is missing or invalid (including the case when the ‘+’ character is missing), the command will fail with the “Command parameter error” error.

Example:

→ RESET PHONE +390123456789
← RESET PHONE +390123456789 EXECUTING

18.16 STATUS

This command can be used to get some status information from the device.

The status info given in the response has the following format:

```
Z-PASS2<hwrev> <date> <time> RUNNING <service status>,<vpn status>
<DI1>,<DI2>,<DO1>,<DO2>,<DIDO1>,<DIDO2>
```

where:

<hwrev>: "", "-R01", "-IO"

<date> is in the form "yyyy/mm/dd"

<hour> is in the form "hh:mm:ss"

<service status> reports the status of the "SERV" LED¹⁴ ("OFF"|"ON"|"FAIL")

<vpn status> reports the status of the "VPN" LED ("OFF"|"ON"|"FAIL")

<DI1>,<DI2>,<DO1>,<DO2>,<DIDO1>,<DIDO2> status ("LO"|"HI") of the digital I/Os (only for Z-PASS2-IO)

This command is never rejected.

Example:

```
→ STATUS
← STATUS EXECUTING (Z-PASS2-IO 2018/03/09 08:01:31 RUNNING OFF,OFF
HI,LO,HI,LO,LO,LO)
```

18.17 GET GPS

This command can be used to get GPS location info from the device.

The response is given as an URL to Google Maps™:

<https://www.google.com/maps/?q=<latitude>,<longitude>>

This command is rejected in the following cases:

- if the command is received on a Z-PASS2, Z-PASS2-R01 device, which does not have a GPS module, the command will fail with the "GPS not available" error;
- If the GPS signal is not available, the command will fail with the "GPS not fixed" error.

Example:

```
→ GET GPS
← GET GPS EXECUTING (https://www.google.com/maps/?q=45.3742,11.94557)
```

18.18 RESET

This command can be used to restart ("reboot") the device.

This command is never rejected.

¹⁴ See Chapter "LEDs signaling".

Example:

```
→      RESET
←      RESET EXECUTING
```

18.19 Initial Configuration

This paragraph describes a possible procedure to configure a new Z-PASS device, starting from “factory default” situation.

Firstly, a SIM with PIN check disabled is needed; this SIM shall also be usable with Auto-APN feature (that is it should not require a private custom APN); obviously, the SIM shall support SMS service.

Since no user is present in the Phonebook yet, SMS commands shall be sent with the password, so the modem IMEI shall be known.

If the previous conditions are satisfied, only two commands are needed to let the device connect to the VPN Box; these are:

```
<password> VPN CFG <parameters>
<password> VPN ON PPP
```

Once these commands are successfully processed, the new device appears in the device list presented by the VPN Box Manager SW; after inserting the device in a user’s group (in case of Point-to-Point VPN Box) or applying the device configuration (in case of Single-LAN VPN Box), the device will be reachable via the VPN, letting the user fully configure it.

19 Web Configuration Pages

Z-PASS can be fully configured by means of a set of web configuration pages.

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

<http://192.168.90.101:8080>

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.

19.1 Main View

The screenshot shows the Z-PASS2 web interface. The browser address bar displays '192.168.85.104:8080'. The page title is 'Z-PASS2'. The left sidebar contains a menu with the following items: General Configuration, Main View (selected), Network and Services, Serial Ports, Gateway Configuration, Real Time Clock Setup, VPN Configuration, Router Configuration, Users Configuration, FW Upgrade, Conf. Management, Mobile Configuration, Mobile Network, DDNS Configuration, Digital I/O Configuration, Logic Configuration, SMS Configuration, Phonebook, Diagnostics, FW Versions, and Ethernet Interfaces. The main content area shows the 'Main View [user: admin] [logout]' page. It displays the following information: Firmware Version: SW003900_226 [Modem: UC20GQBR03A14E1G], MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237893], Internet Access: Ethernet, Gateway: running, and Router: disabled. Below this, there are several configuration sections: NETWORK (Ethernet Mode: LAN/WAN, DHCP on WAN: OFF, LAN IP Address: 192.168.90.101, LAN Network Mask: 255.255.255.0, WAN IP Address: 192.168.85.104, 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 (Protocol: HTTP/HTTPS, HTTP Conf Port: 8080, HTTP User Port: 80, HTTPS Port: 443), FILE TRANSFER (Protocol: FTP/SFTP, FTP Port: 21, SFTP Port: 22), 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: zpass), MOBILE NETWORK (Enable: OFF, APN Mode: Automatic, APN: mobile.vodafone.it, Authentication Type: None, Username: , Password: , Ping Connection Testing IP Address: www.google.com), NETWORK REDUNDANCY (Enable: OFF, Ping Address: 8.8.4.4), and WATCHDOG (Enable: ON).

In this page, main Z-PASS configuration parameters are shown, with their current values.

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

- General Configuration
- Shared Memory Tag Configuration (when Gateway Mode is set to Modbus Shared Memory Gateway, see paragraph 19.4)
- Mobile Configuration (not available on Z-PASS1, Z-PASS1-R01 and Z-PASS1-IO)
- Digital I/O Configuration (on Z-PASS1-IO, Z-PASS2-IO products)
- Logic Configuration (not available on Z-PASS1, Z-PASS1-R01 and Z-PASS1-IO)

- Diagnostics

Furthermore, in this like in any other page, the following information are shown:

- the page name
- the Z-PASS FW version (along with the modem FW revision, for Z-PASS2)
- the Z-PASS MAC address; the modem IMEI, for Z-PASS2; the SIM IMSI, for Z-PASS2, when a SIM is present
- the network interface used for Internet Access (i.e.: “Ethernet” or “Mobile”)
- the Modbus Ethernet to Serial/Transparent/Modbus Shared Memory Gateway status (i.e.: “running” or “stopped”)
- 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, two buttons are available:

- “RESTART”, to perform Z-PASS reboot;
- “FACTORY DEFAULT”, to reset Z-PASS to its factory state.

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

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

19.2 Network and Services

The parameters shown in this page slightly change, depending on the HW version of the product (Z-PASS1/Z-PASS2 or Z-PASS1-R01/Z-PASS2-R01 or Z-PASS1-IO/Z-PASS2-IO) and, for new HW versions, on the selected “Ethernet Mode”; this is shown in the following figures.

Z-PASS2

192.168.85.104:8080/setup.php

General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces

Z-PASS2
Network and Services [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running

	CURRENT	UPDATED
NETWORK		
Ethernet Mode (*)	LAN/WAN	LAN/WAN ▾
DHCP on WAN	OFF	OFF ▾
LAN IP Address	192.168.90.101	192.168.90.101
LAN Network Mask	255.255.255.0	255.255.255.0
WAN IP Address	192.168.85.104	192.168.85.104
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		
Protocol (*)	HTTP/HTTPS	HTTP/HTTPS ▾
HTTP Conf Port (*)	8080	8080
HTTP User Port (*)	80	80
HTTPS Port (*)	443	443
FILE TRANSFER		
Protocol	FTP/SFTP	FTP/SFTP ▾
FTP Port	21	21
SFTP Port	22	22
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.

APPLY

The previous figure shows the “Network and Services” page for a Z-PASS2-IO, when the “Ethernet Mode” parameter is set to “LAN/WAN”; it also applies to a Z-PASS1-IO in “LAN/WAN” mode.

Z-PASS2

Network and Services [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Ethernet

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
NETWORK		
Ethernet Mode (*) Switch	Switch	v
DHCP OFF	OFF	v
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	v
IP Address 2 192.168.85.104	192.168.85.104	
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	v
DNS Server 192.168.84.113	192.168.84.113	
IP Configuration from Discovery ON	ON	v
WEB SERVER		
Protocol (*) HTTP/HTTPS	HTTP/HTTPS	v
HTTP Conf Port (*) 8080	8080	
HTTP User Port (*) 80	80	
HTTPS Port (*) 443	443	
FILE TRANSFER		
Protocol FTP/SFTP	FTP/SFTP	v
FTP Port 21	21	
SFTP Port 22	22	
NETWORK REDUNDANCY		
Enable OFF	OFF	v
Ping Address 8.8.4.4	8.8.4.4	
WATCHDOG		
Enable (*) ON	ON	v
Timeout (s) 60	60	
DEBUG LOGS		
Enable ON	ON	v
COM1		
Mode RS485	RS485	v

NOTE: changing fields marked with * will cause a system restart.

The previous figure shows the “Network and Services” page for a Z-PASS2-IO, when the “Ethernet Mode” parameter is set to “Switch”; it also applies to a Z-PASS1-IO in “Switch” mode.

Z-PASS2

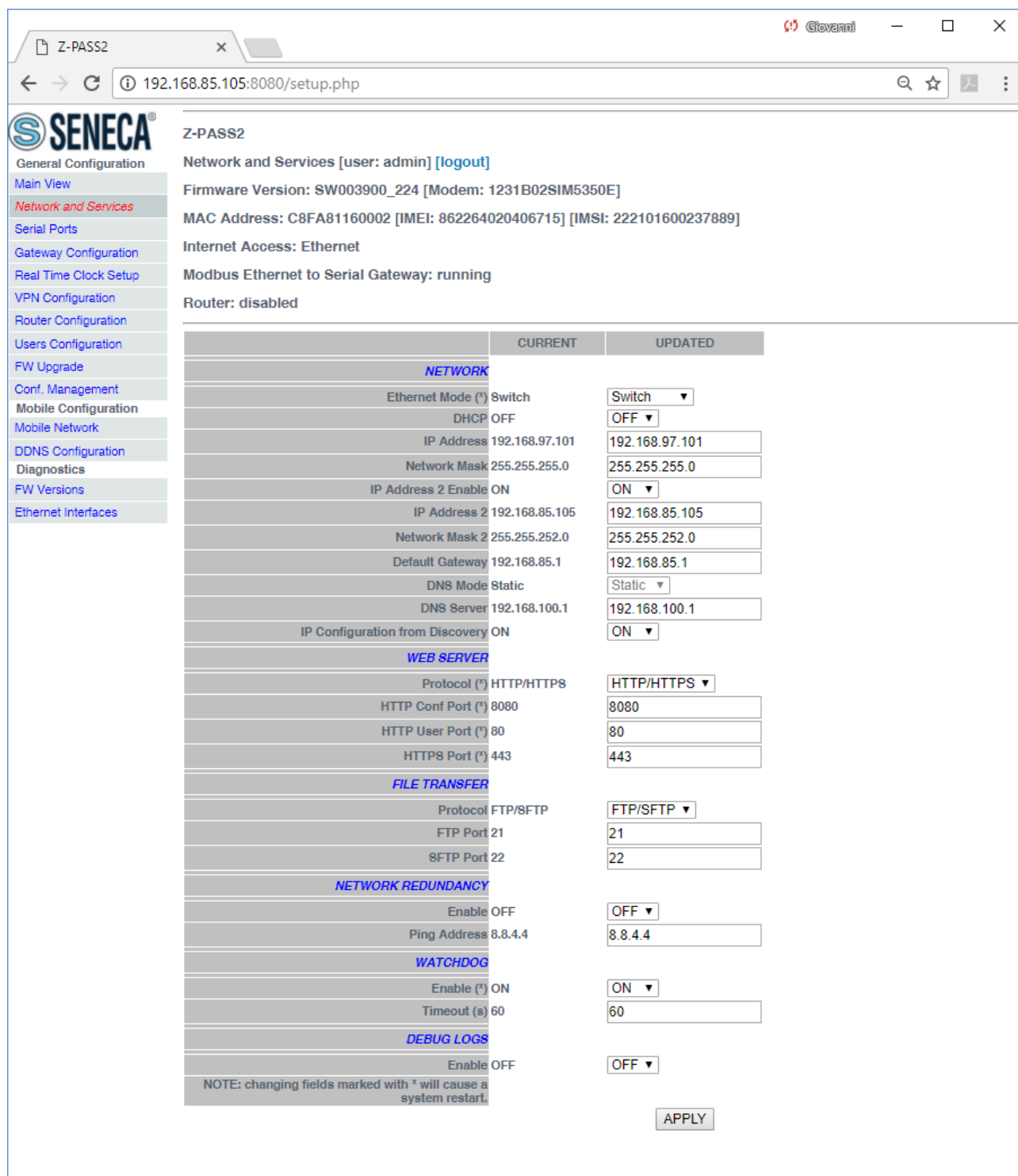
192.168.85.105:8080/setup.php

General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Mobile Configuration
Mobile Network
DDNS Configuration
Diagnostics
FW Versions
Ethernet Interfaces

Z-PASS2
Network and Services [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: 1231B02SIM5350E]
MAC Address: C8FA81160002 [IMEI: 862264020406715] [IMSI: 222101600237889]
Internet Access: Ethernet
Modbus Ethernet to Serial Gateway: running
Router: disabled

	CURRENT	UPDATED
NETWORK		
Ethernet Mode (*)	LAN/WAN	LAN/WAN ▾
DHCP on WAN	OFF	OFF ▾
LAN IP Address	192.168.90.101	192.168.90.101
LAN Network Mask	255.255.255.0	255.255.255.0
WAN IP Address	192.168.85.105	192.168.85.105
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	192.168.100.1	192.168.100.1
IP Configuration from Discovery	ON	ON ▾
WEB SERVER		
Protocol (*)	HTTP/HTTPS	HTTP/HTTPS ▾
HTTP Conf Port (*)	8080	8080
HTTP User Port (*)	80	80
HTTPS Port (*)	443	443
FILE TRANSFER		
Protocol	FTP/SFTP	FTP/SFTP ▾
FTP Port	21	21
SFTP Port	22	22
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.		
APPLY		

The previous figure shows the “Network and Services” page for a Z-PASS2-R01, when the “Ethernet Mode” parameter is set to “LAN/WAN”; it also applies to a Z-PASS1-R01 in “LAN/WAN” mode.



SENECA®

General Configuration

- Main View
- Network and Services**
- Serial Ports
- Gateway Configuration
- Real Time Clock Setup
- VPN Configuration
- Router Configuration
- Users Configuration
- FW Upgrade
- Conf. Management
- Mobile Configuration
- Mobile Network
- DDNS Configuration
- Diagnostics
- FW Versions
- Ethernet Interfaces

Z-PASS2

Network and Services [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002 [IMEI: 862264020406715] [IMSI: 222101600237889]

Internet Access: Ethernet

Modbus Ethernet to Serial Gateway: running

Router: disabled

	CURRENT	UPDATED
NETWORK		
Ethernet Mode (*) Switch	Switch	
DHCP OFF	OFF	
IP Address 192.168.97.101	192.168.97.101	
Network Mask 255.255.255.0	255.255.255.0	
IP Address 2 Enable ON	ON	
IP Address 2 192.168.85.105	192.168.85.105	
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 192.168.100.1	192.168.100.1	
IP Configuration from Discovery ON	ON	
WEB SERVER		
Protocol (*) HTTP/HTTPS	HTTP/HTTPS	
HTTP Conf Port (*) 8080	8080	
HTTP User Port (*) 80	80	
HTTPS Port (*) 443	443	
FILE TRANSFER		
Protocol FTP/SFTP	FTP/SFTP	
FTP Port 21	21	
SFTP Port 22	22	
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.

APPLY

The previous figure shows the “Network and Services” page for a Z-PASS2-R01, when the “Ethernet Mode” parameter is set to “Switch”; it also applies to a Z-PASS1-R01 in “Switch” mode.

SENECA®

General Configuration

- Main View
- Network and Services**
- Serial Ports
- Gateway Configuration
- Real Time Clock Setup
- VPN Configuration
- Router Configuration
- Users Configuration
- FW Upgrade
- Conf. Management
- Mobile Configuration
- Mobile Network
- DDNS Configuration
- Diagnostics
- FW Versions
- Ethernet Interfaces

Z-PASS2

Network and Services [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: 1231B02SIM5350E_20141015]

MAC Address: C8F9810201D7 [IMEI: 862264020120878]

Internet Access: Ethernet

Modbus Ethernet to Serial Gateway: running

Router: disabled

	CURRENT	UPDATED
NETWORK		
DHCP	OFF	OFF ▼
IP Address	192.168.85.105	192.168.85.105
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	192.168.84.113	192.168.84.113
IP Configuration from Discovery	ON	ON ▼
WEB SERVER		
Protocol (*)	HTTP/HTTPS	HTTP/HTTPS ▼
HTTP Conf Port (*)	8080	8080
HTTP User Port (*)	80	80
HTTPS Port (*)	443	443
FILE TRANSFER		
Protocol	FTP/SFTP	FTP/SFTP ▼
FTP Port	21	21
SFTP Port	22	22
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.

APPLY

The previous figure shows the “Network and Services” page for a Z-PASS2 (old version); it also applies to a Z-PASS1 (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 this 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. <u>This parameter is available only for Z-PASS1-R01, Z-PASS2-R01, Z-PASS1-IO and Z-PASS2-IO products.</u> For Z-PASS1 and Z-PASS2 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 WAN	Flag to enable/disable the DHCP	ON

	functionality on the WAN Ethernet interface	
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). When “Ethernet Mode” is set to “LAN/WAN”, the Default Gateway shall be in the WAN subnet.	192.168.100.1 , for Z-PASS1-R0x and Z-PASS2-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 dynamically assigned by the DHCP Server (value: “DHCP”)	DHCP, for Z-PASS1-R0x and Z-PASS2-R0x (x=1,2) Static, for Z-PASS1 and Z-PASS2
NETWORK/DNS Server	DNS server IP address (disabled when DHCP functionality is enabled and DNS Mode = DHCP)	192.168.100.1 , for Z-PASS1-R0x and Z-PASS2-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 8)	ON
WEB SERVER/Protocol	Protocol used to access the web pages: HTTP/HTTPS, HTTPS, HTTP	HTTP/HTTPS
WEB SERVER/HTTP Conf Port	TCP port to access the configuration pages, using HTTP protocol. <u>Please note that if this parameter is set to 80 (standard HTTP port), the web user site won't be available anymore.</u>	8080 Default URL for conf pages: <a href="http://<IP_address>:8080">http://<IP_address>:8080
WEB SERVER/HTTP User Port	TCP port to access the user pages, using HTTP protocol.	80 Default URL for user pages: <a href="http://<IP_address>">http://<IP_address>

WEB SERVER/HTTPS Port	TCP port to access the configuration and user pages, using HTTPS protocol.	443 Default URL for conf pages: <a href="https://<IP_address>/maintenance">https://<IP_address>/maintenance Default URL for user pages: <a href="https://<IP_address>">https://<IP_address>
FILE TRANSFER/Protocol	Protocol used for File Transfer: FTP/SFTP, SFTP, FTP	FTP/SFTP
FTP Port	TCP Port for FTP protocol	21
SFTP Port	TCP Port for SFTP protocol	22
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 (see figure below).	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 <u>This parameter is available only for Z-PASS1-IO and Z-PASS2-IO products.</u>	RS485

One note 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 19.8).

In the “Network and Services” page, 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 Z-PASS; these parameters are:

- NETWORK/Ethernet Mode
- WEB SERVER/Port
- WATCHDOG/Enable, only when changing ON -> OFF
- DEBUG LOGS/Enable, only when changing ON -> OFF



19.3 Serial Ports

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

Z-PASS2

Serial Ports [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
COM1 (RS232/RS485)		
Baud Rate	115200	115200 ▼
Data Bits	8	8 ▼
Parity	None	None ▼
Stop Bits	1	1 ▼
COM2 (RS485)		
Baud Rate	38400	38400 ▼
Data Bits	8	8 ▼
Parity	None	None ▼
Stop Bits	1	1 ▼
COM4 (RS485)		
Baud Rate	38400	38400 ▼
Data Bits	8	8 ▼
Parity	None	None ▼
Stop Bits	1	1 ▼

APPLY

This page is made up of three sections, corresponding to the three serial ports available in Z-PASS devices:

- COM1 RS232 or RS485¹⁵
- COM2 RS485
- COM4 RS485

For each serial port, the following configuration parameters are available:

¹⁵ Depending on the position of the SW2 DIP switch.

Field	Meaning	Default value
Baud Rate	Baud rate (in bps); possible values are: 200 300 600 1200 2400 4800 9600 19200 38400 57600 115200	38400
Data Bits	Data bits; possible values are: 5/6/7/8	8
Parity	Parity; possible values are: None/Even/Odd	None
Stop Bits	Stop bits; possible values are: 1/2	1

In the “Serial Ports” page, you can change any of the above parameters; to apply the changes, press the “APPLY” button.

Note that when you change the serial ports configuration, the Gateway services are automatically restarted, to actually apply the changes.

19.4 Gateway Configuration

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

Z-PASS2
Gateway Configuration [user: admin] [logout]
Firmware Version: SW003900_225 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 901280990053007]
Internet Access: Ethernet
Gateway: running
Router: running

	CURRENT	UPDATED
COM1 Gateway Mode		
	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM2 Gateway Mode		
	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM4 Gateway Mode		
	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
Slave ID for Embedded I/O		
	254	254
COM1		
Enable	ON	ON ▼
Port	501	501
Response Wait Time (ms) [10-10000]	1000	1000
COM2		
Enable	ON	ON ▼
Port	502	502
Response Wait Time (ms) [10-10000]	1000	1000
COM4		
Enable	ON	ON ▼
Port	503	503
Response Wait Time (ms) [10-10000]	1000	1000

APPLY

The first thing you have to do in this page is to select, for each serial port, the type of gateway bound to the port, by means of the “Gateway Mode” parameter; the possible modes are “Modbus Ethernet to Serial”, “Transparent” and “Modbus Shared Memory”.

The page is substantially made up of three sections, corresponding to the three serial ports available in Z-PASS devices.

The configuration parameters available in each of these sections depend on the selected mode, as described in the following sub-paragraphs.

19.4.1 Modbus Ethernet to Serial Gateway

For each serial port with “Gateway Mode” = “Modbus Ethernet to Serial”, the following configuration parameters are available:

Field	Meaning	Default value
Enable	Flag to enable/disable the Modbus Ethernet to Serial Gateway functionality on the port	ON
Port	TCP port to access the Modbus Ethernet to Serial Gateway If three distinct values are set, three Modbus Ethernet to Serial Gateway instances are run, each handling a single serial port. If the same port value is set for more than one serial port, the same Modbus Ethernet to Serial Gateway instance will handle two or three serial ports, that is the Modbus RTU requests will be simultaneously sent to the serial ports.	COM1: 501 COM2: 502 COM4: 503
Response Wait Time	Timeout on the reception of the Modbus RTU responses The value is in milliseconds; possible values are in the range [10 - 10000].	1000

The following screen-shots give some examples of Modbus Ethernet to Serial Gateway configurations.

SENECA®

Z-PASS2

Gateway Configuration [user: admin] [logout]

Firmware Version: SW003900_225 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 901280990053007]

Internet Access: Ethernet

Gateway: running

Router: running

	CURRENT	UPDATED
COM1 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM2 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM4 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
Slave ID for Embedded I/O	254	254
COM1		
Enable	ON	ON ▼
Port	502	502
Response Wait Time (ms) [10-10000]	1000	1000
COM2		
Enable	ON	ON ▼
Port	502	502
Response Wait Time (ms) [10-10000]	1000	1000
COM4		
Enable	ON	ON ▼
Port	502	502
Response Wait Time (ms) [10-10000]	1000	1000

APPLY

In the above configuration, all the Modbus requests received on the 502 TCP port will be sent to all the three serial ports (COM1, COM2 and COM4); the communication parameters on the serial ports are those set in the “Serial Ports” page (see 19.3).

SENECA®

Z-PASS2

Gateway Configuration [user: admin] [logout]

Firmware Version: SW003900_225 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 901280990053007]

Internet Access: Ethernet

Gateway: running

Router: running

	CURRENT	UPDATED
COM1 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM2 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM4 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
Slave ID for Embedded I/O	254	254
COM1		
Enable	ON	ON ▼
Port	501	501
Response Wait Time (ms) [10-10000]	1000	1000
COM2		
Enable	ON	ON ▼
Port	502	502
Response Wait Time (ms) [10-10000]	1000	1000
COM4		
Enable	ON	ON ▼
Port	502	502
Response Wait Time (ms) [10-10000]	1000	1000

APPLY

In the above configuration, the Modbus requests received on the 501 TCP port will be sent to the COM1 port, while those received on the 502 TCP port will be sent to the COM2 and COM4 ports.

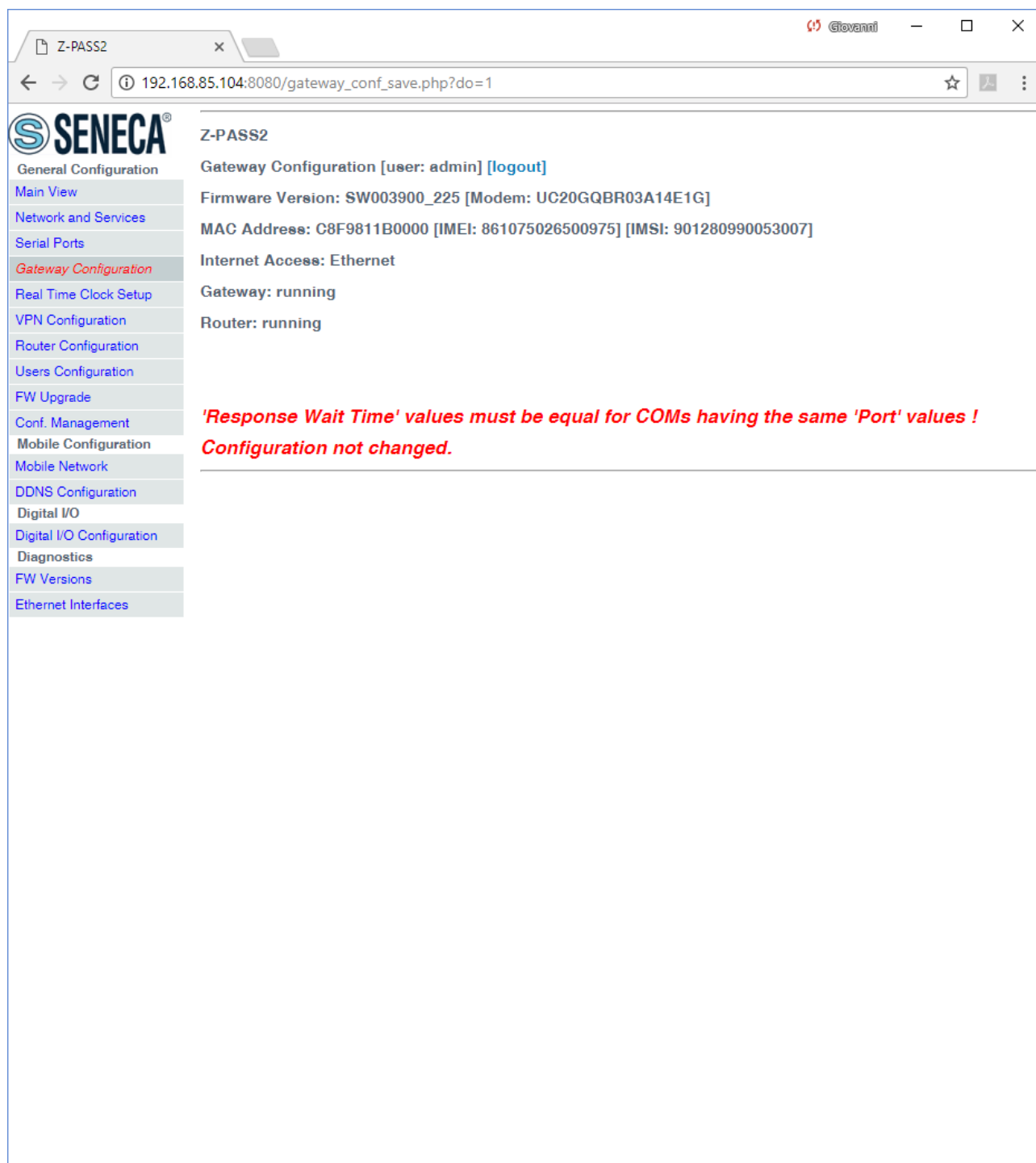
Z-PASS2
Gateway Configuration [user: admin] [logout]
Firmware Version: SW003900_225 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 901280990053007]
Internet Access: Ethernet
Gateway: running
Router: running

	CURRENT	UPDATED
COM1 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM2 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM4 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
Slave ID for Embedded I/O	254	254
COM1		
Enable	ON	ON ▼
Port	501	501
Response Wait Time (ms) [10-10000]	1000	1000
COM2		
Enable	ON	ON ▼
Port	502	502
Response Wait Time (ms) [10-10000]	1000	1000
COM4		
Enable	ON	ON ▼
Port	503	503
Response Wait Time (ms) [10-10000]	1000	1000

APPLY

Finally, in the above configuration, each TCP port corresponds to a single serial port, that is Modbus requests received on a TCP port are sent to a single serial port.

Please note that if you set the same TCP port value for more than one serial port, the “Response Wait Time” values shall also be the same for those serial ports; otherwise, clicking on the “APPLY” button, the following error message is shown.



19.4.1.1 Embedded I/O (Z-PASS1-IO, Z-PASS2-IO)

As shown in the above figures, when at least one port has “Gateway Mode” = “Modbus Ethernet to Serial”, the “Gateway Configuration” page contains the following parameter:

Field	Meaning	Default value
Slave ID for Embedded I/O	Slave ID used to access the Modbus Registers corresponding to the “embedded” digital I/Os (for “IO” HW	254

	revision). In Z-PASS2-IO, this id can also be used to access Modbus Registers containing GPS information. Possible values: [1..255]. This parameter is meaningful only for Z-PASS1-IO and Z-PASS2-IO products.	
--	---	--

The Modbus Registers representing the Digital I/Os are given in the following table:

Data Type	Digital I/Os	Address
Holding Registers	Bit 0: DI1 (LSB) Bit 1: DI2 Bit 2: DI3 Bit 3: DI4	0 (40001)
Holding Registers	Bit 0: DO1 (LSB) Bit 1: DO2 Bit 2: DO3 Bit 3: DO4	0 (40002)
Discrete Inputs	DI1	0 (10001)
Discrete Inputs	DI2	1 (10002)
Discrete Inputs	DI3	2 (10003)
Discrete Inputs	DI4	3 (10004)
Coils	DO1	0
Coils	DO2	1
Coils	DO3	2
Coils	DO4	3

The mapping between DI1..DI4, DO1..DO4 and the Digital I/O names described in the “Digital I/O Configuration” paragraph is as follows:

DI1	DI 1
DI2	DI 2
DI3	DIDO 1, if input
DI4	DIDO 2, if input
DO1	DO 1
DO2	DO 2
DO3	DIDO 1, if output
DO4	DIDO 2, if output

If DIx or DOx is not available (e.g.: DI4, when DIDO 2 is configured as an output), the corresponding bit value is always 0.

DOx can be actually set only if the corresponding Digital I/O Mode is “General Output” (see “Digital I/O Configuration” paragraph); otherwise, the write request will have no effect.

The Modbus Registers containing the GPS information are given in the following table (all Holding Registers):

Info	Address	Data Type
GPS_ERROR	9 (40010)	INT (0: OK, -1: Not fixed -2: Internal error)
GPS_UTC_HH	10 (40011)	UINT
GPS_UTC_MM	11 (40012)	UINT
GPS_UTC_SS	12 (40013)	UINT
GPS_DATE_DD	13 (40014)	UINT
GPS_DATE_MM	14 (40015)	UINT
GPS_DATE_YY	15 (40016)	UINT
GPS_LATITUDE	16 – 19 (40017 – 40020)	LREAL
GPS_LONGITUDE	20 – 23 (40021 – 40024)	LREAL
GPS_HDOP	24 – 27 (40025 – 40028)	LREAL
GPS_ALTITUDE	28 – 31 (40029 – 40032)	LREAL
GPS_COG	32 – 35 (40033 – 40036)	LREAL
GPS_SPEED_KM	36 – 39 (40037 – 40040)	LREAL
GPS_SPEED_KN	40 - 43 (40041 – 40044)	LREAL
GPS_FIX	44 (40045)	UINT
GPS_NSAT	45 (40046)	UINT

19.4.2 Transparent Gateway

Selecting “Transparent” as the gateway mode for one of the serial ports, e.g. “COM1”, the “Gateway Configuration” page will change to look like the one shown in the following figure:

Z-PASS2

Gateway Configuration [user: admin] [logout]

Firmware Version: SW003900_225 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 901280990053007]

Internet Access: Ethernet

Gateway: running

Router: running

	CURRENT	UPDATED
COM1 Gateway Mode	Transparent	Transparent ▼
COM2 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM4 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
Slave ID for Embedded I/O	254	254
COM1		
Operating Mode	Virtual COM	Virtual COM ▼
Listen Port	8000	8000
Destination Address	192.168.85.104	192.168.85.104
Destination Port	8000	8000
Multicast Group	224.1.0.1	224.1.0.1
Multicast Interface	Ethernet	Ethernet ▼
Tunnel Role	Master	Master ▼
Data Packing Interval (ms) [0-1000]	20	20
COM2		
Enable	ON	ON ▼
Port	502	502
Response Wait Time (ms) [10-10000]	1000	1000
COM4		
Enable	ON	ON ▼
Port	502	502
Response Wait Time (ms) [10-10000]	1000	1000

APPLY

For each serial port with “Gateway Mode” = “Transparent”, the available configuration parameters depend on the value of the “Operating Mode” parameter selected for the port.

The possible values for the “Operating Mode” parameter are:

- None (default value)
- Virtual COM
- Serial Tunnel Point-to-Point on TCP
- Serial Tunnel Point-to-Point on UDP
- Serial Tunnel Point-to-Multipoint

Furthermore, for the “Serial Tunnel” operating modes, the available parameters depend on the selected “Tunnel Role” (Master or Slave).

The following tables describe the relevant parameters for the various operating modes.

Virtual COM

Field	Meaning	Default value
Listen Port	TCP port to access the transparent gateway	COM1: 8000 COM2: 8001 COM4: 8002
Data Packing Interval	Time interval used as a criterion to pack data bytes received from the serial port, before sending them to the network; that is, if no byte is received for this time, available bytes are sent to the network. The value is in milliseconds; possible values are in the range [0 - 1000].	20

Serial Tunnel Point-to-Point on TCP (Slave)

Serial Tunnel Point-to-Point on UDP (Slave)

Field	Meaning	Default value
Listen Port	TCP/UDP port to access the transparent gateway	COM1: 8000 COM2: 8001 COM4: 8002

Serial Tunnel Point-to-Point on TCP (Master)

Serial Tunnel Point-to-Point on UDP (Master)

Field	Meaning	Default value
Destination Address	The IP Address which the transparent gateway will connect to	COM1: 192.168.90.102 COM2: 192.168.90.103 COM4: 192.168.90.104
Destination Port	The TCP/UDP port which the transparent gateway will connect to	COM1: 8000 COM2: 8001 COM4: 8002

Serial Tunnel Point-to-Multipoint (Master)

Field	Meaning	Default value
Destination Port	The UDP port which the packets will be sent to	COM1: 8000 COM2: 8001 COM4: 8002
Multicast Group	IP Address which identifies the Multicast Group	224.1.0.1

Multicast Interface	Network Interface which the UDP packets are sent to; possible values: Ethernet VPN; <u>“VPN” option is available only when VPN is active</u>	Ethernet
---------------------	--	----------

Serial Tunnel Point-to-Multipoint (Slave)

Field	Meaning	Default value
Listen Port	The UDP port which the packets will be received from	COM1: 8000 COM2: 8001 COM4: 8002
Multicast Group	IP Address which identifies the Multicast Group	224.1.0.1
Multicast Interface	Network Interface which the UDP packets are received from; possible values: Ethernet VPN; <u>“VPN” option is available only when VPN is active</u>	Ethernet

19.4.3 Modbus Shared Memory Gateway

Selecting “Modbus Shared Memory” as the gateway mode for one of the serial ports, e.g. “COM4”, the “Gateway Configuration” page will change to look like the one shown in the following figure:

Z-PASS2
Gateway Configuration [user: admin] [logout]

Firmware Version: SW003900_225 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 901280990053007]

Internet Access: Ethernet
Gateway: running
Router: running

	CURRENT	UPDATED
COM1 Gateway Mode	Transparent	Transparent ▼
COM2 Gateway Mode	Modbus Ethernet to Serial	Modbus Ethernet to Serial ▼
COM4 Gateway Mode	Modbus Shared Memory	Modbus Shared Memory ▼

Slave ID for Embedded I/O 254

TCP Port 1100

TCP Connections Max Number [1-50] 32

Response Mode when Resource in Fail Exception

COM1

Operating Mode Virtual COM

Listen Port 8000

Destination Address 192.168.85.104

Destination Port 8000

Multicast Group 224.1.0.1

Multicast Interface Ethernet

Tunnel Role Slave

Data Packing Interval (ms) [0-1000] 20

COM2

Enable ON

Port 502

Response Wait Time (ms) [10-10000] 1000

COM4

Task Master

Slave Address 1

Timeout (ms) [10-10000] 100

Delay between Polls (ms) [10-1000] 100

Read/Write Retries [0-10] 0

Multiple Read Max Number [1-32] 16

Multiple Write Max Number [1-32] 16

As shown in the above figure, when at least one port has “Gateway Mode” = “Modbus Shared Memory”, the “Gateway Configuration” page contains the following parameters:

Field	Meaning	Default value
TCP Port	Listening port for the Modbus TCP server	502
TCP Connections Max Number [1-50]	Maximum number of TCP connections that can be accepted by the Modbus TCP server	32

Response Mode when Resource in Fail	This parameter defines how the response to a Modbus TCP (read) request is built for a tag corresponding to a Modbus RTU slave which is not responding; when mode is “Last read value”, the last available value is given in the Modbus TCP response; when mode is “Exception”, the response contains an exception with the value 11 (“Gateway target device failed to respond”).	Exception
-------------------------------------	--	-----------

Then, for each serial port with “Gateway Mode” = “Modbus Shared Memory”, the parameters described in the following table are available.

Field	Meaning	Default value
Task	This parameter defines which Modbus Shared Memory Gateway task is running on the serial port; possible values are: None, Master, Slave	None
Slave Address	Modbus Address for the RTU Slave; this is the only parameter available when Task=Slave	1
Timeout (ms) [10 – 10000]	Response timeout for Modbus RTU requests, in milliseconds (available only when Task=Master)	100
Delay between Polls (ms) [10 – 1000]	Interval between Modbus RTU requests, in milliseconds (available only when Task=Master)	100
Read/Write Retries [0 – 10]	Maximum number of retries for Modbus RTU requests; this always applies to write requests; for read requests, it applies only to tags with “Gateway Tag Mode”=“BRIDGE” (see 19.5.1.1 paragraph)	0
Multiple Read Max Number [1 – 32]	Maximum number of Modbus registers that can be read in a single Modbus RTU request; this is used to reduce the number of read requests sent on the serial bus, thus performing optimization	16
Multiple Write Max Number [1 – 32]	Maximum number of Modbus registers that can be written in a single Modbus RTU request; this is	16

	used to reduce the number of write requests sent on the serial bus, thus performing optimization	
--	--	--

Please note that, if any of the configured TCP/UDP port values collide, the configuration is not applied and the following error message is shown:

The screenshot shows a web browser window with the address bar displaying `192.168.85.104:8080/gateway_conf_save.php?do=1`. The page title is "Z-PASS2". On the left, there is a sidebar menu with the "SENECA" logo at the top. The menu items include: General Configuration, Main View, Network and Services, Serial Ports, Gateway Configuration (highlighted in red), Real Time Clock Setup, VPN Configuration, Router Configuration, Users Configuration, FW Upgrade, Conf. Management, Shared Memory Tag Conf., Tag Setup, Tag View, Mobile Configuration, Mobile Network, DDNS Configuration, Digital I/O, Digital I/O Configuration, Diagnostics, FW Versions, and Ethernet Interfaces. The main content area displays the "Gateway Configuration" page for user "admin" with a [logout] link. It shows system information: Firmware Version: SW003900_225 [Modem: UC20GQBR03A14E1G], MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 901280990053007], Internet Access: Ethernet, Gateway: running, and Router: running. Below this information, a red error message is displayed: "Port values must be distinct !" and "Configuration not changed.".

19.5 Shared Memory Tag Configuration

When the “Gateway Mode” parameter, in the “Gateway Configuration” page, is set to “Modbus Shared Memory”, in the left side menu, a new section named “Shared Memory Tag Configuration” is available, containing two links, as shown in the following figure.

General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces

19.5.1 Tag Setup

This page is used to perform Modbus Shared Memory Gateway tag configuration.

Z-PASS2
Gateway Tag Setup [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running

Scegli file Nessun file selezionato Import tag configuration
Export tag configuration Save current tag configuration
ADD MODIFY DELETE
Page : 1/20 PREVIOUS PAGE NEXT PAGE

GATEWAY TAG NR	GATEWAY MODBUS TCP/IP START REGISTER	GATEWAY TAG NAME	TARGET MODBUS RTU DEVICE	TARGET RESOURCE	TARGET MODBUS RTU START REGISTER	TARGET MODBUS REQUEST TYPE	TARGET REGISTER DATA TYPE	TARGET CONNECTED TO SERIAL PORT	TARGET MODBUS SLAVE ADDRESS	GATEWAY TAG MODE
1	1	TAG1	CUSTOM		1	COIL	BOOL	COM4	1	GATEWAY
2	2	TAG2	CUSTOM		2	COIL	BOOL	COM4	1	GATEWAY
3	3	TAG3	CUSTOM		3	COIL	BOOL	COM4	1	GATEWAY
4	4	TAG4	CUSTOM		4	COIL	BOOL	COM4	1	GATEWAY
5	5	TAG5	CUSTOM		5	COIL	BOOL	COM4	1	GATEWAY
6	6	TAG6	CUSTOM		6	COIL	BOOL	COM4	1	GATEWAY
7	7	TAG7	CUSTOM		7	COIL	BOOL	COM4	1	GATEWAY
8	8	TAG8	CUSTOM		8	COIL	BOOL	COM4	1	GATEWAY
9	9	TAG9	CUSTOM		9	COIL	BOOL	COM4	1	GATEWAY
10	10	TAG10	CUSTOM		10	COIL	BOOL	COM4	1	GATEWAY
11	11	TAG11	CUSTOM		11	COIL	BOOL	COM4	1	GATEWAY
12	12	TAG12	CUSTOM		12	COIL	BOOL	COM4	1	GATEWAY
13	13	TAG13	CUSTOM		13	COIL	BOOL	COM4	1	GATEWAY
14	14	TAG14	CUSTOM		14	COIL	BOOL	COM4	1	GATEWAY
15	15	TAG15	CUSTOM		15	COIL	BOOL	COM4	1	GATEWAY
16	16	TAG16	CUSTOM		16	COIL	BOOL	COM4	1	GATEWAY
17	17	TAG17	CUSTOM		17	COIL	BOOL	COM4	1	GATEWAY
18	18	TAG18	CUSTOM		18	COIL	BOOL	COM4	1	GATEWAY
19	19	TAG19	CUSTOM		19	COIL	BOOL	COM4	1	GATEWAY
20	20	TAG20	CUSTOM		20	COIL	BOOL	COM4	1	GATEWAY

In this page, the following buttons (i.e. functionalities) are available.

Import tag configuration

This button allows the user to upload a binary file containing the tag configuration to the Z-PASS; this file shall have been exported from the “Microsoft Excel™ Template” (see 19.5.3 paragraph).

Export tag configuration

This button allows the user to download a binary file containing the tag configuration from the Z-PASS; this file can be imported into the “Microsoft Excel™ Template” (see 19.5.3 paragraph).

Save current tag configuration

This button allows the user to save the current tag configuration in Z-PASS memory, in a permanent way. In fact, it is important to note that, when you add, modify or delete a tag, the corresponding changes are not saved to non-volatile memory. To have those changes stored permanently, you have to click on this button.

ADD

This button allows the user to add a new tag (see paragraph below); up to 2000 tags can be configured.

MODIFY

This button allows the user to modify an existing tag (see paragraph below); the tag shall have been previously selected, by clicking on the corresponding table row, as shown in the following figure.

General Configuration

Main View

Network and Services

Serial Ports

Gateway Configuration

Real Time Clock Setup

VPN Configuration

Router Configuration

Users Configuration

FW Upgrade

Conf. Management

Shared Memory Tag Conf.

Tag Setup

Tag View

Mobile Configuration

Mobile Network

DDNS Configuration

Digital I/O

Digital I/O Configuration

Diagnostics

FW Versions

Ethernet Interfaces

Z-PASS2

Gateway Tag Setup [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

Scegli file Nessun file selezionato Import tag configuration

Export tag configuration Save current tag configuration

ADD MODIFY DELETE

Page : 1/20 PREVIOUS PAGE NEXT PAGE

GATEWAY TAG NR	GATEWAY MODBUS TCP/IP START REGISTER	GATEWAY TAG NAME	TARGET MODBUS RTU DEVICE	TARGET RESOURCE	TARGET MODBUS RTU START REGISTER	TARGET MODBUS REQUEST TYPE	TARGET REGISTER DATA TYPE	TARGET CONNECTED TO SERIAL PORT	TARGET MODBUS SLAVE ADDRESS	GATEWAY TAG MODE
1	1	TAG1	CUSTOM		1	COIL	BOOL	COM4	1	GATEWAY
2	2	TAG2	CUSTOM		2	COIL	BOOL	COM4	1	GATEWAY
3	3	TAG3	CUSTOM		3	COIL	BOOL	COM4	1	GATEWAY
4	4	TAG4	CUSTOM		4	COIL	BOOL	COM4	1	GATEWAY
5	5	TAG5	CUSTOM		5	COIL	BOOL	COM4	1	GATEWAY
6	6	TAG6	CUSTOM		6	COIL	BOOL	COM4	1	GATEWAY
7	7	TAG7	CUSTOM		7	COIL	BOOL	COM4	1	GATEWAY
8	8	TAG8	CUSTOM		8	COIL	BOOL	COM4	1	GATEWAY
9	9	TAG9	CUSTOM		9	COIL	BOOL	COM4	1	GATEWAY
10	10	TAG10	CUSTOM		10	COIL	BOOL	COM4	1	GATEWAY
11	11	TAG11	CUSTOM		11	COIL	BOOL	COM4	1	GATEWAY
12	12	TAG12	CUSTOM		12	COIL	BOOL	COM4	1	GATEWAY
13	13	TAG13	CUSTOM		13	COIL	BOOL	COM4	1	GATEWAY
14	14	TAG14	CUSTOM		14	COIL	BOOL	COM4	1	GATEWAY
15	15	TAG15	CUSTOM		15	COIL	BOOL	COM4	1	GATEWAY
16	16	TAG16	CUSTOM		16	COIL	BOOL	COM4	1	GATEWAY
17	17	TAG17	CUSTOM		17	COIL	BOOL	COM4	1	GATEWAY
18	18	TAG18	CUSTOM		18	COIL	BOOL	COM4	1	GATEWAY
19	19	TAG19	CUSTOM		19	COIL	BOOL	COM4	1	GATEWAY
20	20	TAG20	CUSTOM		20	COIL	BOOL	COM4	1	GATEWAY

DELETE

This button allows the user to delete a tag; the tag shall have been previously selected, by clicking on the corresponding table row.

19.5.1.1 Tag Creation/Modification

By clicking on the “ADD” or “MODIFY” button, you come to the following page.

Z-PASS2
Gateway Tag Setup [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running

TAG 27

	CURRENT	UPDATED
GATEWAY TAG NAME		TAG
GATEWAY MODBUS TCP/IP START REGISTER ADDRESS	1	
TARGET MODBUS RTU DEVICE	CUSTOM	
TARGET RESOURCE		
TARGET CONNECTED TO SERIAL PORT	COM2	
TARGET MODBUS SLAVE STATION ADDRESS	1	
TARGET MODBUS RTU START REGISTER ADDRESS	1	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	
TARGET REGISTER DATA TYPE	16BIT SIGNED	
GATEWAY TAG MODE	GATEWAY	

Equivalent to the address in the Seneca documentation : 40001

Equivalent to the address in the Seneca documentation : 40001

APPLY

The following table describes the available parameters.

Field	Meaning	Default value
Gateway Tag Name	Mnemonic name to identify the tag	TAG
Gateway Modbus TCP/IP Start Register Address	Start Register Address of the tag on the Modbus TCP/IP side	1
Target Modbus RTU Device	Type of RTU device: "CUSTOM" or one of the following Seneca devices: "Z-D-IN" "Z-10-D-IN" "Z-D-OUT" "Z-10-D-OUT" "Z-D-IO" "ZC-24-DI" "ZC-24-DO" "ZC-16DI-8DO" "Z-4-AI-1" "Z-8-AI-1" "Z-3-AO" "Z-4-TC" "Z-8-TC" "Z-203" "Z-4RTD-2" "Z-SG" "Z-DAQ-PID" "S-203T" "S-203TA" "ZE-4DI-2AI-2DO" "ZE-2AI" "Z-4DI-2AI-2DO" "S203TA-D" "S203RC-D" "Z-PASS-IO"	CUSTOM
Target Resource	This field identifies a particular resource (tag) on one of Seneca devices; possible values depend on the selected RTU device, in "Target Modbus RTU Device" field; if that field is set to "CUSTOM", "Target Resource" field is empty; when "Target Resource" field is set, "Target Modbus RTU Start Register Address", "Target Modbus Request Type" and "Target Register Data Type" fields are automatically set	<i>Empty</i>
Target connected to Serial Port	This field identifies the serial port the target RTU device is connected to; possible values are: COM1,	The first available serial port, that is the first port with "Task" other than "None"

	COM2, COM4; if, for one serial port, "Task" parameter is set to "None", the port is labelled as "COMx – <i>UNUSED</i> " and can't be selected; if "Task" parameter is set to "Slave", the port is labelled as "COMx – <i>SHARED</i> "; if such a port is selected, a number of fields are no more available, as shown in the figure below	
Target Modbus Slave Station Address	Modbus Address of the target RTU device	1
Target Modbus RTU Start Register Address	Start Register Address of the tag on the Modbus RTU device	1
Target Modbus Request Type	Possible Modbus data types: COIL DISCRETE INPUT HOLDING REGISTER INPUT REGISTER	HOLDING REGISTER
Target Register Data Type	Possible data types: 16BIT SIGNED 16BIT UNSIGNED 32BIT SIGNED MSW 32BIT UNSIGNED MSW 32BIT SIGNED LSW 32BIT UNSIGNED LSW 32BIT REAL MSW 32BIT REAL LSW BOOL For more information about the above data types, see table below	16 BIT SIGNED
Gateway Tag Mode	This field defines how the tag will be handled by the gateway processes; possible values are: GATEWAY or BRIDGE if Task=Master on the selected port SHARED MEMORY if Task=Slave on the selected port	GATEWAY, if Task=Master SHARED MEMORY, if Task=Slave

Data Type	Meaning
16BIT SIGNED	1 register, from -32768 to +32767
16BIT UNSIGNED	1 register, from 0 to 65535
32BIT SIGNED MSW	2 registers with the lowest address register holding the Most Significant Word, from -2147483648 to +2147483647
32BIT UNSIGNED MSW	2 registers with the lowest address register holding the Most

	Significant Word, from 0 to 4294967295
32BIT SIGNED LSW	2 registers with the lowest address register holding the Least Significant Word, from -2147483648 to +2147483647
32BIT UNSIGNED LSW	2 registers with the lowest address register holding the Least Significant Word, from 0 to 4294967295
32BIT REAL MSW	2 registers with the lowest address register holding the Most Significant Word, Floating Point single precision (IEEE 758-2008)
32BIT REAL LSW	2 registers with the lowest address register holding the Least Significant Word, Floating Point single precision (IEEE 758-2008)
BOOL	1 Boolean Coil or Discrete Input register

Z-PASS2

192.168.85.104:8080/mbgw_tag_mod.php?sid=0.36794437584863626&r=27

SENECA®

General Configuration

Main View

Network and Services

Serial Ports

Gateway Configuration

Real Time Clock Setup

VPN Configuration

Router Configuration

Users Configuration

FW Upgrade

Conf. Management

Shared Memory Tag Conf.

Tag Setup

Tag View

Mobile Configuration

Mobile Network

DDNS Configuration

Digital I/O

Digital I/O Configuration

Diagnostics

FW Versions

Ethernet Interfaces

Z-PASS2

Gateway Tag Setup [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

TAG 27

	CURRENT	UPDATED
GATEWAY TAG NAME	TAG	
GATEWAY MODBUS TCP/IP START REGISTER ADDRESS	1	Equivalent to the address in the Seneca documentation : 40001
TARGET MODBUS RTU DEVICE	CUSTOM ▼	
TARGET RESOURCE	▼	
TARGET CONNECTED TO SERIAL PORT	COM2 ▼ COM1 - UNUSED COM2 COM4 - SHARED EMBEDDED	
TARGET MODBUS SLAVE STATION ADDRESS	1	
TARGET MODBUS RTU START REGISTER ADDRESS	Equivalent to the address in the Seneca documentation : 40001	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER ▼	
TARGET REGISTER DATA TYPE	16BIT SIGNED ▼	
GATEWAY TAG MODE	GATEWAY ▼	

APPLY

Z-PASS2

Gateway Tag Setup [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

TAG 27

	CURRENT	UPDATED
GATEWAY TAG NAME		TAG
GATEWAY MODBUS TCP/IP START REGISTER ADDRESS		1
TARGET CONNECTED TO SERIAL PORT		COM4 - SHARED ▼
TARGET MODBUS REQUEST TYPE		HOLDING REGISTER ▼
TARGET REGISTER DATA TYPE		16BIT SIGNED ▼
GATEWAY TAG MODE		SHARED MEMORY ▼

APPLY

Equivalent to the address in the Seneca documentation : 40001

Some more explanations are needed for “Gateway Tag Mode” parameter.

Tags with Mode=GATEWAY are handled in the “classic” Modbus Shared Memory Gateway way, that is tags are read periodically, even if no Modbus read request is received for those tags on the Modbus TCP/IP side.

Tags with Mode=BRIDGE are read only when a Modbus read request is received for those tags on the Modbus TCP/IP side.

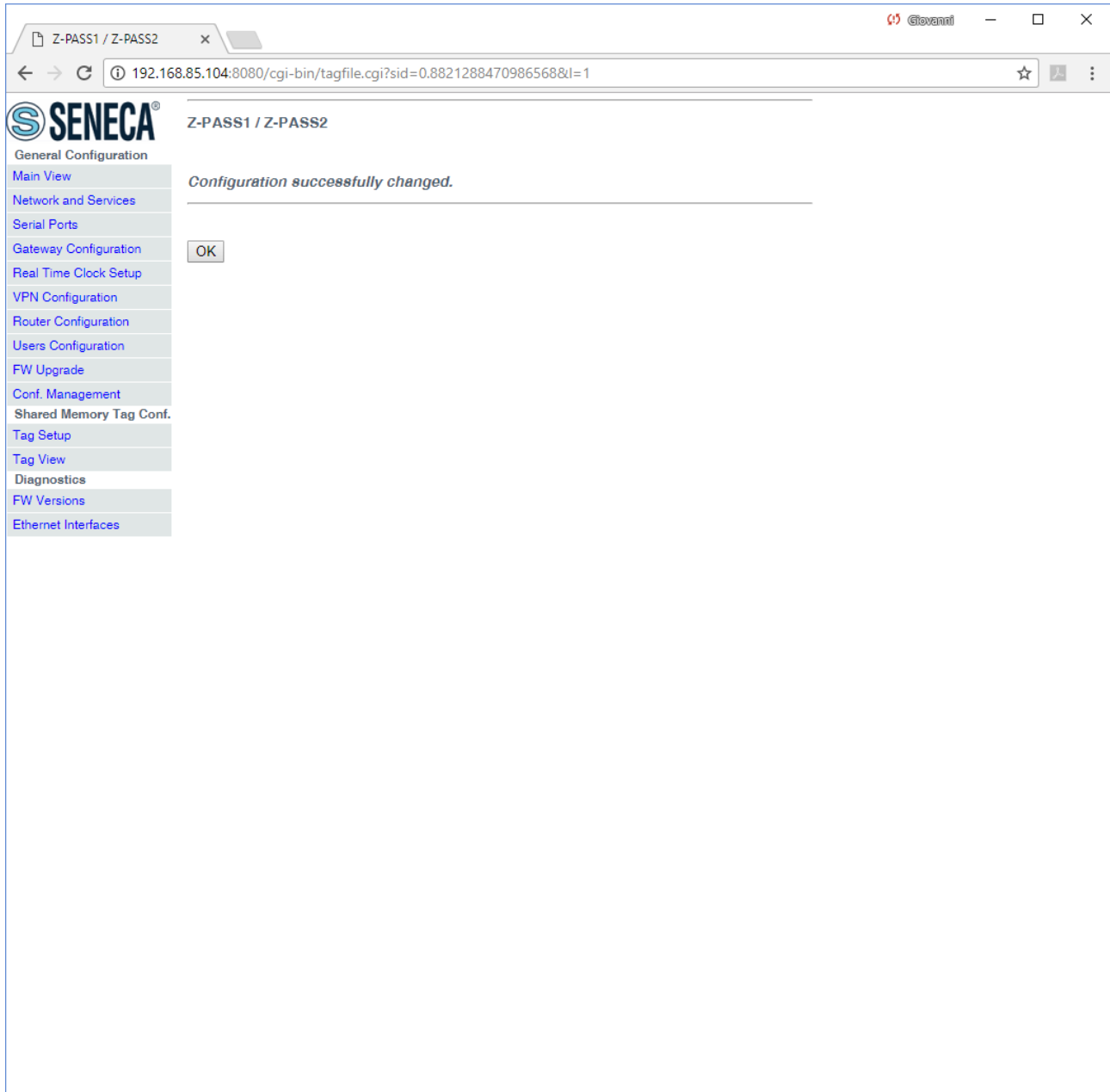
Instead, for write operations, tags with Mode=GATEWAY and tags with Mode=BRIDGE are handled in the same way, that is tags are written only when a Modbus write request is received for those tags on the Modbus TCP/IP side.

The Mode=BRIDGE option is particularly useful for Modbus RTU devices with the “Fail Safe” feature available for output lines, as for many Seneca devices; normally, those devices are designed to put their output lines to “fail safe” value, when the connection to the master (e.g. a SCADA system) goes down; since the criterion to detect the “connection failure” is that no Modbus (write and read) request is received, the “fail safe” mode can’t be entered with “classic” gateway behaviour.

Finally, tags with Mode=SHARED MEMORY are stored only in CPU memory, not in any RTU device, so their values are written/read only when a Modbus write/read request is received for those tags on the Modbus TCP/IP side.

NOTE: all considerations related to requests received on the Modbus TCP/IP side identically apply to requests received on a serial port configured as Modbus RTU Slave.

By clicking on the “APPLY” button, the tag is added/modified and the following page is shown.



By clicking on the “OK” button, you go back to the “Gateway Tag Setup” page.

19.5.1.2 Tags for Embedded I/O (Z-PASS1-IO, Z-PASS2-IO)

A special value for “TARGET MODBUS RTU DEVICE” parameter is “Z-PASS-IO”: this value lets you define tags corresponding to the Z-PASS1-IO/Z-PASS2-IO embedded digital I/Os, as shown in the following figure:

Z-PASS2
Giovanni

General Configuration

- Main View
- Network and Services
- Serial Ports
- Gateway Configuration
- Real Time Clock Setup
- VPN Configuration
- Router Configuration
- Users Configuration
- FW Upgrade
- Conf. Management
- Shared Memory Tag Conf.
- Tag Setup
- Tag View
- Mobile Configuration
- Mobile Network
- DDNS Configuration
- Digital I/O
- Digital I/O Configuration
- Diagnostics
- FW Versions
- Ethernet Interfaces

Z-PASS2

Gateway Tag Setup [user: admin] [\[logout\]](#)

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

TAG 1

	CURRENT	UPDATED
GATEWAY TAG NAME	ZPASS_DI	ZPASS_DI
GATEWAY MODBUS TCP/IP START REGISTER ADDRESS	1	1
TARGET MODBUS RTU DEVICE	Z-PASS-IO	Z-PASS-IO
TARGET RESOURCE	DIGITAL INPUTS	DIGITAL INPUTS - DIGITAL INPUTS - DIGITAL OUTPUTS - DIGITAL INPUT 1 - DIGITAL INPUT 2 - DIGITAL INPUT 3 - DIGITAL INPUT 4 - DIGITAL OUTPUT 1 - DIGITAL OUTPUT 2 - DIGITAL OUTPUT 3 - DIGITAL OUTPUT 4
TARGET CONNECTED TO SERIAL PORT	EMBEDDED	
TARGET MODBUS SLAVE STATION ADDRESS	1	
TARGET MODBUS RTU START REGISTER ADDRESS	1	
TARGET MODBUS REQUEST TYPE	HOLDING REGISTER	
TARGET REGISTER DATA TYPE	16BIT UNSIGNED	16BIT UNSIGNED
GATEWAY TAG MODE	EMBEDDED	EMBEDDED

Equivalent to the address
in the Seneca
documentation : 40001

Equivalent to the address
in the Seneca
documentation : 40001

Depending on the value of the “TARGET RESOURCE” parameter, the other parameters are set to the values shown in the following table:

TARGET RESOURCE	TARGET MODBUS RTU START REGISTER ADDRESS	TARGET MODBUS REQUEST TYPE	TARGET REGISTER DATA TYPE
DIGITAL INPUTS	1 (40001)	HOLDING REGISTER	16BIT UNSIGNED
DIGITAL OUTPUTS	2 (40002)	HOLDING REGISTER	16BIT UNSIGNED
DIGITAL INPUT 1	1 (10001)	DISCRETE INPUT	BOOL
DIGITAL INPUT 2	2 (10002)	DISCRETE INPUT	BOOL

DIGITAL INPUT 3	3 (10003)	DISCRETE INPUT	BOOL
DIGITAL INPUT 4	4 (10004)	DISCRETE INPUT	BOOL
DIGITAL OUTPUT 1	1 (1)	COIL	BOOL
DIGITAL OUTPUT 2	2 (2)	COIL	BOOL
DIGITAL OUTPUT 3	3 (3)	COIL	BOOL
DIGITAL OUTPUT 4	4 (4)	COIL	BOOL

You can easily check that these tags correspond to Modbus Registers defined in paragraph 19.4.1.1.

For these tags, other parameter values are fixed:

- TARGET MODBUS SLAVE STATION ADDRESS 1
- TARGET CONNECTED TO SERIAL PORT EMBEDDED
- GATEWAY TAG MODE EMBEDDED

“EMBEDDED” tag mode is similar to “BRIDGE” mode, that is the values of these tags are updated only when there is a Modbus (read or write) request related to them.

The default configuration for Z-PASS1-IO and Z-PASS2-IO already contain tags for embedded I/Os, as shown in the following figure.

Z-PASS2
Gateway Tag Setup [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running

Scegli file Nessun file selezionato Import tag configuration
Export tag configuration Save current tag configuration

ADD MODIFY DELETE

Page : 1/20 PREVIOUS PAGE NEXT PAGE

GATEWAY TAG NR	GATEWAY MODBUS TCP/IP START REGISTER	GATEWAY TAG NAME	TARGET MODBUS RTU DEVICE	TARGET RESOURCE	TARGET MODBUS RTU START REGISTER	TARGET MODBUS REQUEST TYPE	TARGET REGISTER DATA TYPE	TARGET CONNECTED TO SERIAL PORT	TARGET MODBUS SLAVE ADDRESS
1	1	ZPASS_DI	Z-PASS-IO	DIGITAL INPUTS	1	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1
2	2	ZPASS_DO	Z-PASS-IO	DIGITAL OUTPUTS	2	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1
3	1	ZPASS_DI_1	Z-PASS-IO	DIGITAL INPUT 1	1	DISCRETE INPUT	BOOL	EMBEDDED	1
4	2	ZPASS_DI_2	Z-PASS-IO	DIGITAL INPUT 2	2	DISCRETE INPUT	BOOL	EMBEDDED	1
5	3	ZPASS_DI_3	Z-PASS-IO	DIGITAL INPUT 3	3	DISCRETE INPUT	BOOL	EMBEDDED	1
6	4	ZPASS_DI_4	Z-PASS-IO	DIGITAL INPUT 4	4	DISCRETE INPUT	BOOL	EMBEDDED	1
7	1	ZPASS_DO_1	Z-PASS-IO	DIGITAL OUTPUT 1	1	COIL	BOOL	EMBEDDED	1
8	2	ZPASS_DO_2	Z-PASS-IO	DIGITAL OUTPUT 2	2	COIL	BOOL	EMBEDDED	1
9	3	ZPASS_DO_3	Z-PASS-IO	DIGITAL OUTPUT 3	3	COIL	BOOL	EMBEDDED	1
10	4	ZPASS_DO_4	Z-PASS-IO	DIGITAL OUTPUT 4	4	COIL	BOOL	EMBEDDED	1
11	10	GPS_ERROR	Z-PASS-GPS	GPS_ERROR	10	HOLDING REGISTER	16BIT SIGNED	EMBEDDED	1

19.5.1.3 Tags for GPS Info (Z-PASS2-IO)

A special value for “TARGET MODBUS RTU DEVICE” parameter is “Z-PASS-GPS”: this value lets you define tags corresponding to the Z-PASS2-IO GPS information, as shown in the following figure:

SENECA®

General Configuration

Main View

Network and Services

Serial Ports

Gateway Configuration

Real Time Clock Setup

VPN Configuration

Router Configuration

Users Configuration

FW Upgrade

Conf. Management

Shared Memory Tag Conf.

Tag Setup

Tag View

Mobile Configuration

Mobile Network

DDNS Configuration

Digital I/O

Digital I/O Configuration

Diagnostics

FW Versions

Ethernet Interfaces

Z-PASS2

Gateway Tag Setup [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

TAG 27

	CURRENT	UPDATED
GATEWAY TAG NAME		TAG
GATEWAY MODBUS TCP/IP START REGISTER ADDRESS	1	
TARGET MODBUS RTU DEVICE	Z-PASS-GPS	
TARGET RESOURCE	GPS_ERROR	
TARGET CONNECTED TO SERIAL PORT		
TARGET MODBUS SLAVE STATION ADDRESS		
TARGET MODBUS RTU START REGISTER ADDRESS		
TARGET MODBUS REQUEST TYPE		
TARGET REGISTER DATA TYPE		
GATEWAY TAG MODE		

Equivalent to the address in the Seneca documentation : 40001

Equivalent to the address in the Seneca documentation : 40010

Depending on the value of the “TARGET RESOURCE” parameter, the other parameters are set to the values shown in the following table:

TARGET RESOURCE	TARGET MODBUS RTU START REGISTER ADDRESS	TARGET MODBUS REQUEST TYPE	TARGET REGISTER DATA TYPE
GPS_ERROR	10 (40010)	HOLDING REGISTER	16BIT SIGNED
GPS_UTC_HH	11 (40011)	HOLDING REGISTER	16BIT UNSIGNED
GPS_UTC_MM	12 (40012)	HOLDING REGISTER	16BIT UNSIGNED

GPS_UTC_SS	13 (40013)	HOLDING REGISTER	16BIT UNSIGNED
GPS_DATE_DD	14 (40014)	HOLDING REGISTER	16BIT UNSIGNED
GPS_DATE_MM	15 (40015)	HOLDING REGISTER	16BIT UNSIGNED
GPS_DATE_YY	16 (40016)	HOLDING REGISTER	16BIT UNSIGNED
GPS_LATITUDE	17 – 20 (40017 – 40020)	HOLDING REGISTER	64BIT REAL
GPS_LONGITUDE	21 – 24 (40021 – 40024)	HOLDING REGISTER	64BIT REAL
GPS_HDOP	25 – 28 (40025 – 40028)	HOLDING REGISTER	64BIT REAL
GPS_ALTITUDE	29 – 32 (40029 – 40032)	HOLDING REGISTER	64BIT REAL
GPS_COG	33 – 36 (40033 – 40036)	HOLDING REGISTER	64BIT REAL
GPS_SPEED_KM	37 – 40 (40037 – 40040)	HOLDING REGISTER	64BIT REAL
GPS_SPEED_KN	41 – 44 (40041 – 40044)	HOLDING REGISTER	64BIT REAL
GPS_FIX	45 (40045)	HOLDING REGISTER	16BIT UNSIGNED
GPS_NSAT	46 (40046)	HOLDING REGISTER	16BIT UNSIGNED

For these tags, other parameter values are fixed:

- TARGET MODBUS SLAVE STATION ADDRESS 1
- TARGET CONNECTED TO SERIAL PORT EMBEDDED
- GATEWAY TAG MODE EMBEDDED

“EMBEDDED” tag mode is similar to “BRIDGE” mode, that is the values of these tags are updated only when there is a Modbus (read or write) request related to them.

The default configuration for Z-PASS2-IO already contain tags for GPS information, as shown in the following figure.

Z-PASS2

Gateway Tag Setup [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

Scegli file Nessun file selezionato Import tag configuration

Export tag configuration Save current tag configuration

ADD MODIFY DELETE

Page : 1/20 PREVIOUS PAGE NEXT PAGE

11	10	GPS_ERROR	Z-PASS-GPS	GPS_ERROR	10	HOLDING REGISTER	16BIT SIGNED	EMBEDDED	1	EI
12	11	GPS_HOUR	Z-PASS-GPS	GPS_UTC_HH	11	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1	EI
13	12	GPS_MINUTE	Z-PASS-GPS	GPS_UTC_MM	12	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1	EI
14	13	GPS_SECOND	Z-PASS-GPS	GPS_UTC_SS	13	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1	EI
15	14	GPS_DAY	Z-PASS-GPS	GPS_DATE_DD	14	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1	EI
16	15	GPS_MONTH	Z-PASS-GPS	GPS_DATE_MM	15	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1	EI
17	16	GPS_YEAR	Z-PASS-GPS	GPS_DATE_YY	16	HOLDING REGISTER	16BIT UNSIGNED	EMBEDDED	1	EI
18	17	GPS_LATITUDE	Z-PASS-GPS	GPS_LATITUDE	17	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI
19	21	GPS_LONGITUDE	Z-PASS-GPS	GPS_LONGITUDE	21	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI
20	25	GPS_HDOP	Z-PASS-GPS	GPS_HDOP	25	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI
21	29	GPS_ALTITUDE	Z-PASS-GPS	GPS_ALTITUDE	29	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI
22	33	GPS_COG	Z-PASS-GPS	GPS_COG	33	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI
23	37	GPS_SPEED_KM	Z-PASS-GPS	GPS_SPKM	37	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI
24	41	GPS_SPEED_KN	Z-PASS-GPS	GPS_SPKN	41	HOLDING REGISTER	64BIT REAL	EMBEDDED	1	EI

19.5.2 Tag View

The “Gateway Tag View” page shows the tag values in real-time, as shown in the following figure.

SENECA
General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Tag Configuration
Gateway Tag Setup
Gateway Tag View
Mobile Configuration
Mobile Network

Z-PASS1 / Z-PASS2
Gateway Tag View
Firmware Version: SW003900_110 [Modem: 1231B02SIM5350E]
MAC Address: C8F981020242
Internet Access: Ethernet
Modbus Gateway: running
Router: disabled

Page : 1/20 [PREVIOUS PAGE](#) [NEXT PAGE](#)

GATEWAY TAG NR	GATEWAY TAG NAME	GATEWAY MODBUS TCP/IP START REGISTER	TAG REQUEST TYPE	TAG DATA TYPE	TAG VALUE	TAG READING STATUS	LAST REFRESH TIME
1	TAG1	1	HOLDING REGISTER	16BIT UNSIGNED	2564	OK	12/11/2015 17:13:16.124270
2	TAG2	2	HOLDING REGISTER	16BIT UNSIGNED	0	OK	12/11/2015 17:13:16.124289
3	TAG3	3	HOLDING REGISTER	16BIT UNSIGNED	7650	OK	12/11/2015 17:13:16.124303
4	TAG4	4	HOLDING REGISTER	16BIT UNSIGNED	3332	FAIL(BRIDGE)	---
5	TAG5	5	HOLDING REGISTER	16BIT UNSIGNED	0	FAIL(BRIDGE)	---
6	TAG6	6	HOLDING REGISTER	16BIT UNSIGNED	0	FAIL(BRIDGE)	---
7	TAG7	7	HOLDING REGISTER	16BIT UNSIGNED	0	-	12/11/2015 17:09:50.285640
8	TAG8	8	HOLDING REGISTER	16BIT UNSIGNED	0	-	12/11/2015 17:09:50.285660
9	TAG9	9	HOLDING REGISTER	16BIT UNSIGNED	0	-	12/11/2015 17:09:50.285671
10	TAG10	10	HOLDING REGISTER	32BIT UNSIGNED LSW	0	-	12/11/2015 17:09:50.285680
11	TAG11	12	HOLDING REGISTER	32BIT UNSIGNED LSW	0	-	12/11/2015 17:09:50.285690
12	TAG12	11	HOLDING REGISTER	32BIT UNSIGNED LSW	0	-	12/11/2015 17:09:50.285700

The view is automatically refreshed.

Some notes are worthy about the “TAG READING STATUS” and “LAST REFRESH TIME” columns.

The possible “TAG READING STATUS” values depend on the “GATEWAY TAG MODE” value, in the following way:

OK / FAIL	for tags with Mode=GATEWAY
OK(BRIDGE) / FAIL(BRIDGE)	for tags with Mode=BRIDGE
-	for tags with Mode=SHARED MEMORY or EMBEDDED

The timestamp in the “LAST REFRESH TIME” column is updated:

- on a successful RTU (Master) read/write operation, for tags with Mode=GATEWAY|BRIDGE
- on Modbus Shared Memory Gateway start and on a successful TCP or RTU (Slave) write operation, for tags with Mode=SHARED MEMORY|EMBEDDED

In the above figure, the first three tags (Mode=GATEWAY) have been successfully read, so the “TAG READING STATUS” column shows “OK” and the “LAST REFRESH TIME” column contains a valid timestamp.

The next three tags (Mode=BRIDGE) have not been read nor written yet, so the “TAG READING STATUS” column shows “FAIL(BRIDGE)” and the “LAST REFRESH TIME” column does not contain a timestamp.

Finally, for the last tags (Mode=SHARED MEMORY), the “TAG READING STATUS” column shows “-” and the “LAST REFRESH TIME” column contains a valid timestamp that, in this example, corresponds to the Modbus Shared Memory Gateway start time.

Just as an example, the tag configuration corresponding to the above figure is show below.

Z-PASS1 / Z-PASS2

Gateway Tag Setup

Firmware Version: SW003900_110 [Modem: 1231B02SIM5350E]

MAC Address: C8F981020242

Internet Access: Ethernet

Modbus Gateway: running

Router: disabled

Scegli file Nessun file selezionato Import tag configuration

Export tag configuration Save current tag configuration

ADD MODIFY DELETE

Page : 1/20 PREVIOUS PAGE NEXT PAGE

GATEWAY TAG NR	GATEWAY MODBUS TCP/IP START REGISTER	GATEWAY TAG NAME	TARGET MODBUS RTU DEVICE	TARGET RESOURCE	TARGET MODBUS RTU START REGISTER	TARGET MODBUS REQUEST TYPE	TARGET REGISTER DATA TYPE	TARGET CONNECTED TO SERIAL PORT	TARGET MODBUS SLAVE ADDRESS	GATEWAY TAG MODE
1	1	TAG1	CUSTOM		1	HOLDING REGISTER	16BIT UNSIGNED	COM2	2	GATEWAY
2	2	TAG2	CUSTOM		2	HOLDING REGISTER	16BIT UNSIGNED	COM2	2	GATEWAY
3	3	TAG3	CUSTOM		3	HOLDING REGISTER	16BIT UNSIGNED	COM2	2	GATEWAY
4	4	TAG4	CUSTOM		1	HOLDING REGISTER	16BIT UNSIGNED	COM2	3	BRIDGE
5	5	TAG5	CUSTOM		2	HOLDING REGISTER	16BIT UNSIGNED	COM2	3	BRIDGE
6	6	TAG6	CUSTOM		3	HOLDING REGISTER	16BIT UNSIGNED	COM2	3	BRIDGE
7	7	TAG7	-	-	-	HOLDING REGISTER	16BIT UNSIGNED	COM4 - SHARED	-	SHARED-MEMORY
8	8	TAG8	-	-	-	HOLDING REGISTER	16BIT UNSIGNED	COM4 - SHARED	-	SHARED-MEMORY
9	9	TAG9	-	-	-	HOLDING REGISTER	16BIT UNSIGNED	COM4 - SHARED	-	SHARED-MEMORY
10	10	TAG10	-	-	-	HOLDING REGISTER	32BIT UNSIGNED LSW	COM4 - SHARED	-	SHARED-MEMORY
11	12	TAG11	-	-	-	HOLDING REGISTER	32BIT UNSIGNED LSW	COM4 - SHARED	-	SHARED-MEMORY

19.5.3 Microsoft Excel™ Template for Tag Setup

Another way to create the tag configuration is by means of the “Microsoft Excel™ Template” provided by Seneca, shown in the following figure.

TAG NR	GATEWAY TAG NAME	GATEWAY MODBUS TCP/IP REGISTER ADDRESS	TARGET MODBUS RTU REGISTER TYPE	TARGET MODBUS RTU DATA TYPE	TARGET CONNECTED TO SERIAL PORT NR	TARGET MODBUS RTU START REGISTER	TARGET MODBUS RTU SLAVE ADDRESS	GATEWAY MODE
1	TAG1	1	HOLDING REGISTER	16BIT UNSIGNED	#2	1	2	GATEWAY
2	TAG2	2	HOLDING REGISTER	16BIT UNSIGNED	#2	2	2	GATEWAY
3	TAG3	3	HOLDING REGISTER	16BIT UNSIGNED	#2	3	2	GATEWAY
4	TAG4	4	HOLDING REGISTER	16BIT UNSIGNED	#2	1	3	GATEWAY
5	TAG5	5	HOLDING REGISTER	16BIT UNSIGNED	#2	2	3	GATEWAY
6	TAG6	6	HOLDING REGISTER	16BIT UNSIGNED	#2	3	3	GATEWAY
7	TAG7	7	HOLDING REGISTER	16BIT UNSIGNED	#3	1	4	GATEWAY
8	TAG8	8	HOLDING REGISTER	16BIT UNSIGNED	#3	2	4	GATEWAY
9	TAG9	9	HOLDING REGISTER	16BIT UNSIGNED	#3	3	4	GATEWAY
10	TAG10	10	HOLDING REGISTER	32BIT UNSIGNED LSW	#3	25	5	GATEWAY
11	TAG11	12	HOLDING REGISTER	32BIT UNSIGNED LSW	#3	27	5	GATEWAY
12	TAG12	14	HOLDING REGISTER	32BIT UNSIGNED LSW	#3	29	5	GATEWAY
13	TAG13	1	COIL	BOOL	#1	1	6	BRIDGE
14	TAG14	2	COIL	BOOL	#1	2	6	BRIDGE
15	TAG15	3	COIL	BOOL	#1	3	6	BRIDGE
16	TAG16	4	COIL	BOOL	#1	4	6	BRIDGE
17	TAG17	5	COIL	BOOL	#1	5	6	BRIDGE
18	TAG18	6	COIL	BOOL	#1	6	6	BRIDGE
19	TAG19	7	COIL	BOOL	#1	7	6	BRIDGE
20	TAG20	8	COIL	BOOL	#1	8	6	BRIDGE
21	TAG21	9	COIL	BOOL	#1	9	6	BRIDGE
22	TAG22	10	COIL	BOOL	#1	10	6	BRIDGE
23	TAG23	1	INPUT REGISTER	16BIT UNSIGNED	#1	1	7	GATEWAY
24	TAG24	2	INPUT REGISTER	16BIT UNSIGNED	#1	2	7	GATEWAY
25	TAG25	3	INPUT REGISTER	16BIT UNSIGNED	#1	3	7	GATEWAY
26	TAG26	4	INPUT REGISTER	16BIT UNSIGNED	#1	4	7	GATEWAY
27	TAG27	5	INPUT REGISTER	32BIT UNSIGNED MSW	#1	5	7	GATEWAY
28	TAG28	7	INPUT REGISTER	32BIT UNSIGNED MSW	#1	7	7	GATEWAY
29	TAG29	1	DISCRETE INPUT	BOOL	#1	1	8	GATEWAY
30	TAG30	2	DISCRETE INPUT	BOOL	#1	2	8	GATEWAY
31	TAG31	3	DISCRETE INPUT	BOOL	#1	3	8	GATEWAY
32	TAG32	4	DISCRETE INPUT	BOOL	#1	4	8	GATEWAY
33	TAG33	5	DISCRETE INPUT	BOOL	#1	5	8	GATEWAY

The tag configuration in the Excel sheet can be exported by clicking on the “Export CGI file...” button; the exported binary file can be uploaded to the Z-PASS, by means of the “Import tag configuration” button in “Gateway Tag Setup” page (see 19.5.1 paragraph).

Conversely, the tag configuration created by means of the web page can be imported into the Excel sheet by clicking on the “Import CGI file...” button.

The following table gives the correspondence between the sheet columns and the parameters in the “Gateway Tag Setup” page; therefore, see 19.5.1.1 paragraph for their meanings.

Column	Parameter
Tag NR	-
Gateway Tag Name	Gateway Tag Name
Gateway Modbus TCP/IP Register Address	Gateway Modbus TCP/IP Start Register Address
Target Modbus RTU Register Type	Target Modbus Request Type
Target Modbus RTU Data Type	Target Register Data Type
Target connected to Serial Port NR	Target connected to Serial Port
Target Modbus RTU Start Register	Target Modbus RTU Start Register Address
Target Modbus RTU Slave Address	Target Modbus Slave Station Address
Gateway Mode	Gateway Tag Mode

19.6 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
Real Time Clock Setup [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Mobile
Modbus Shared Memory Gateway: running
Router: running

	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) ▼
APPLY		
RTC		
YEAR	2017	2017
MONTH	December	December ▼
DAY	19	19
HOUR	12	12
MINUTE	02	02
SECOND	58	58
SET CLOCK		

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 ¹⁶ 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.

A large number of Time Zones are available, as partially shown in the following figure:

¹⁶ FQDN: Fully Qualified Domain Name, e.g.: “pool.ntp.org”.

SENECA®

General Configuration

- Main View
- Network and Services
- Serial Ports
- Gateway Configuration
- Real Time Clock Setup**
- VPN Configuration
- Router Configuration
- Users Configuration
- FW Upgrade
- Conf. Management
- Shared Memory Tag Conf.
- Tag Setup
- Tag View
- Mobile Configuration
- Mobile Network
- DDNS Configuration
- Digital I/O
- Digital I/O Configuration
- Diagnostics
- FW Versions
- Ethernet Interfaces

Z-PASS2

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

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

	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	20	
MONTH	06	
DAY	19	
HOUR	12	
MINUTE	02	
SECOND	58	

UTC-10:00 Hawaii
 UTC-10:00 Aleutian
 UTC-09:30 Marquesas
 UTC-09:00 Alaska
 UTC-08:00 Pacific Coast
 UTC-07:00 Arizona
 UTC-07:00 Chihuahua
 UTC-06:00 Central Zone
 UTC-06:00 Mexico City
 UTC-05:00 Bogota
 UTC-05:00 Eastern Zone
 UTC-05:00 Indiana
 UTC-05:00 Havana
 UTC-04:00 Asuncion
 UTC-04:00 Caracas
 UTC-04:00 Cuiaba
 UTC-04:00 La Paz
 UTC-04:00 Atlantic Coast
 UTC-04:00 Santiago
 UTC-03:00 Araguaina

CK

The “RTC” section of the page lets you manually change the Z-PASS date/time settings; since this makes sense only if NTP time synchronization is not enabled, when “NTP/Enable” parameter is “ON” the input fields and the “SET CLOCK” button 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.

19.7 VPN Configuration

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

Z-PASS2
VPN Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
 MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
 Internet Access: Mobile
 Modbus Shared Memory Gateway: running
 Router: running

	CURRENT	UPDATED
VPN Mode	VPN Box	VPN Box ▼
VPN Box		
Enable	ON	OFF ▼
Server	192.168.85.176	192.168.85.176
Password	seneca	seneca
Tag Name	zpass	zpass

APPLY SHOW VPN STATUS

The page has a different layout depending on the value of the “VPN Mode” parameter, which can be “OpenVPN” or “VPN Box”.

19.7.1 OpenVPN

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

Z-PASS2

VPN Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
VPN Mode	VPN Box	OpenVPN ▼
VPN Files		
Configuration File (.ovpn or .conf)	<i>NOTE 1: the file will be renamed as 'ovpn.conf'</i> <i>NOTE 2: in options requiring a file ("ca", "cert", "key" etc.), only filename must be specified (without path)</i> 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 on the Z-PASS; these files are described in the following.

19.7.1.1 Configuration File

This file shall contain all the information needed to configure the Open VPN behaviour; the main configuration options are¹⁷:

- if Z-PASS shall act as a client or a server (typically, it will be a client)
- 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 Z-PASS.

This is the only mandatory file, that is if this file has not been loaded on the Z-PASS, 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 19.7.1.7.

19.7.1.2 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.

19.7.1.3 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.

19.7.1.4 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.

¹⁷ For more information about configuration options, please refer to the OpenVPN web page (“openvpn.net”).

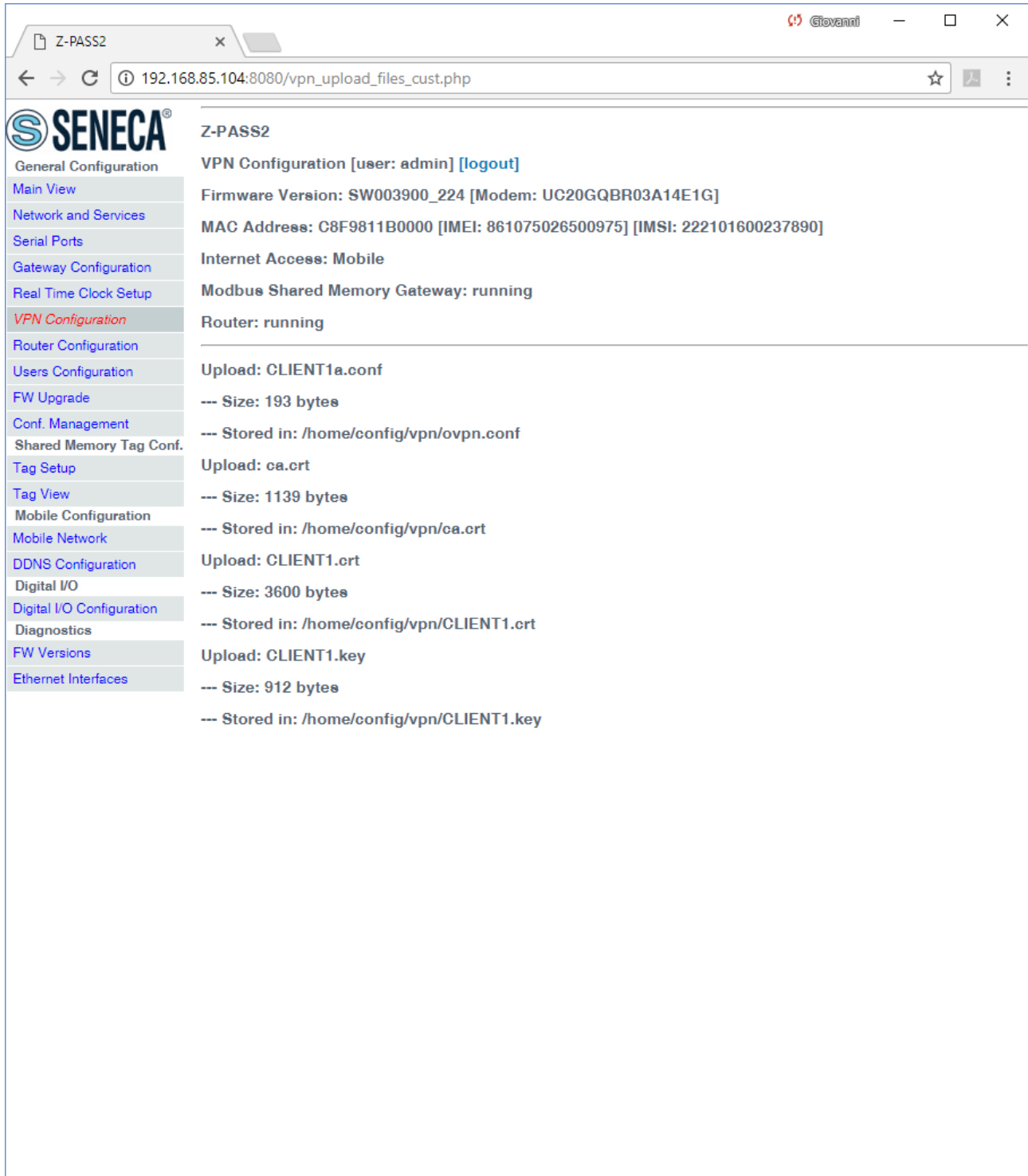
19.7.1.5 Additional file

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

Please note that more than one additional file can be loaded.

You can browse your PC to select the above files and send them to the Z-PASS by pressing the “UPLOAD” button.

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



The screenshot shows a web browser window with the address bar displaying `192.168.85.104:8080/vpn_upload_files_cust.php`. The page title is "Z-PASS2". The left sidebar contains a menu with the following items: General Configuration, Main View, Network and Services, Serial Ports, Gateway Configuration, Real Time Clock Setup, **VPN Configuration** (highlighted), Router Configuration, Users Configuration, FW Upgrade, Conf. Management, Shared Memory Tag Conf., Tag Setup, Tag View, Mobile Configuration, Mobile Network, DDNS Configuration, Digital I/O, Digital I/O Configuration, Diagnostics, FW Versions, and Ethernet Interfaces.

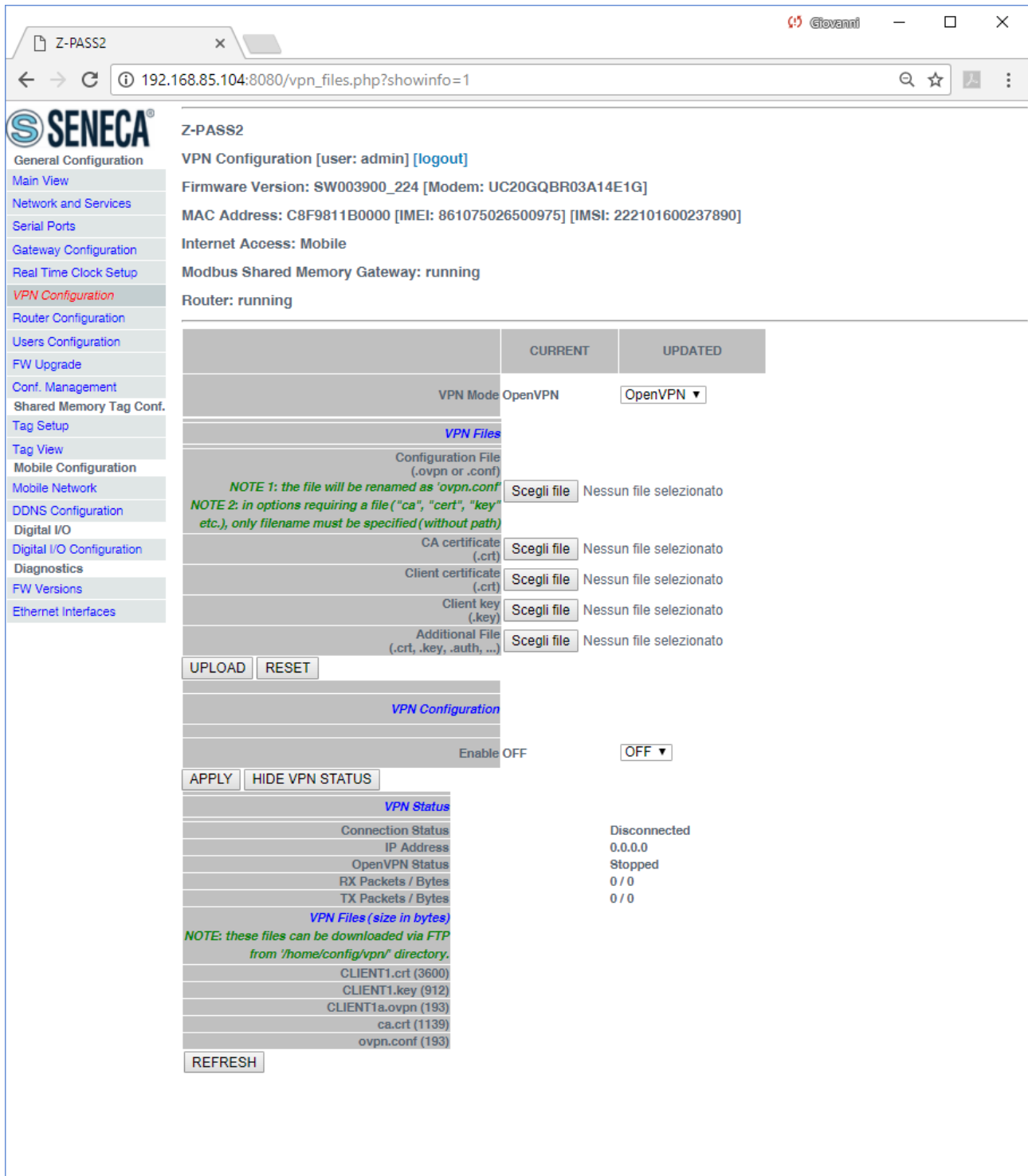
The main content area is titled "Z-PASS2" and shows the "VPN Configuration" page. It includes a "logout" link for the user "admin". The configuration details are as follows:

- Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
- MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
- Internet Access: Mobile
- Modbus Shared Memory Gateway: running
- Router: running

Below these details, there is a section for uploading files:

- Upload: CLIENT1a.conf
 - 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 Z-PASS 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

VPN Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

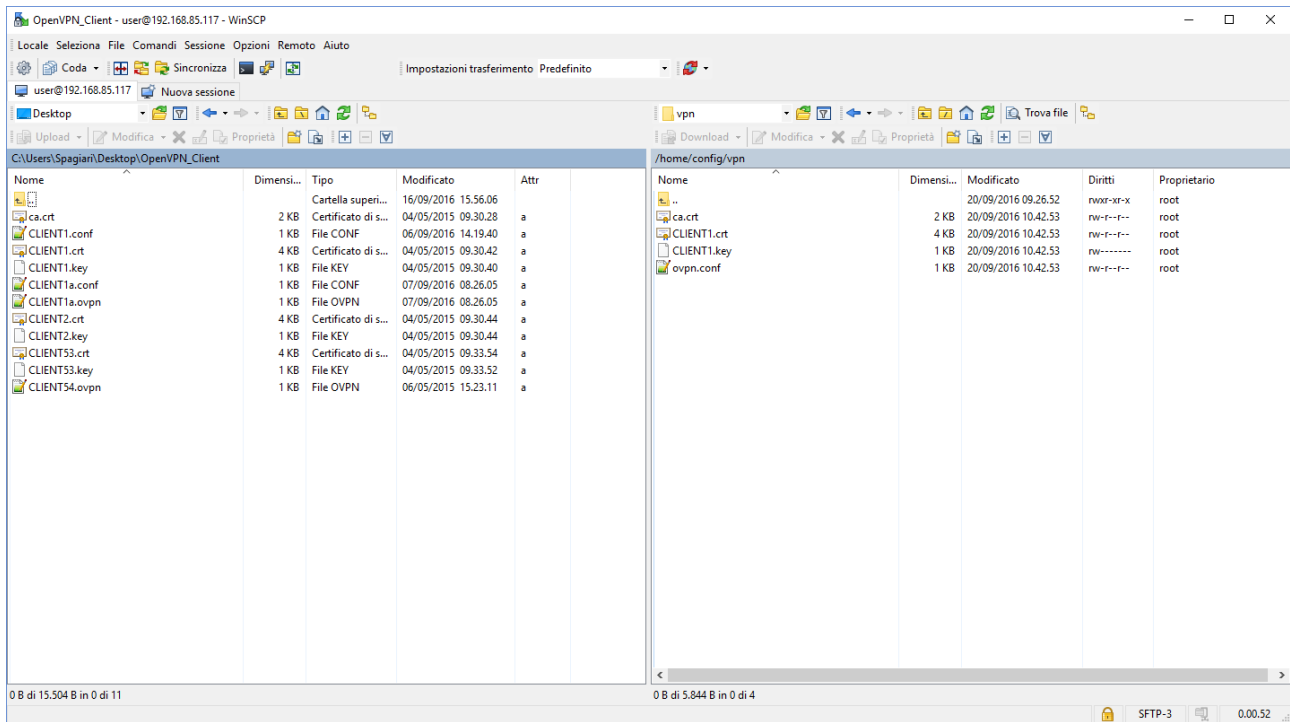
Internet Access: Mobile

Modbus Shared Memory Gateway: running

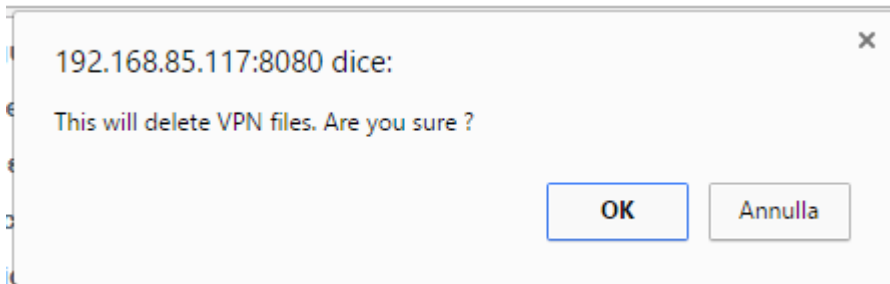
Router: running

	CURRENT	UPDATED
VPN Mode	OpenVPN	OpenVPN ▼
VPN Files		
Configuration File (.ovpn or .conf)	<i>NOTE 1: the file will be renamed as 'ovpn.conf'</i> <i>NOTE 2: in options requiring a file ("ca", "cert", "key" etc.), only filename must be specified (without path)</i> 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)		
<i>NOTE: these files can be downloaded via FTP from '/home/config/vpn/' directory.</i>		
CLIENT1.crt (3600)		
CLIENT1.key (912)		
CLIENT1a.ovpn (193)		
ca.crt (1139)		
ovpn.conf (193)		
REFRESH		

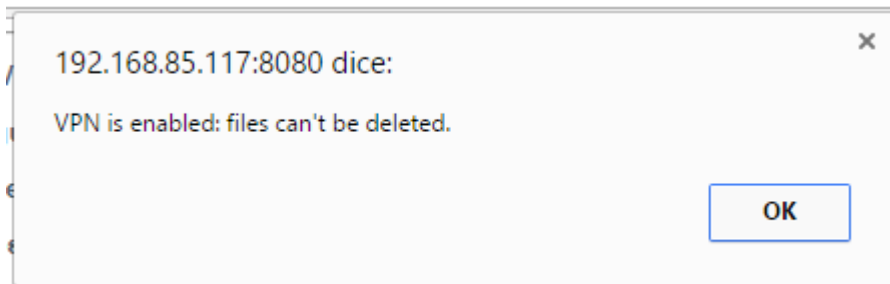
As reminded by the web page, the VPN files can be downloaded from the Z-PASS, if needed, via FTP/SFTP; they can be found in the `/home/config/vpn` directory, as shown in the following figure.



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



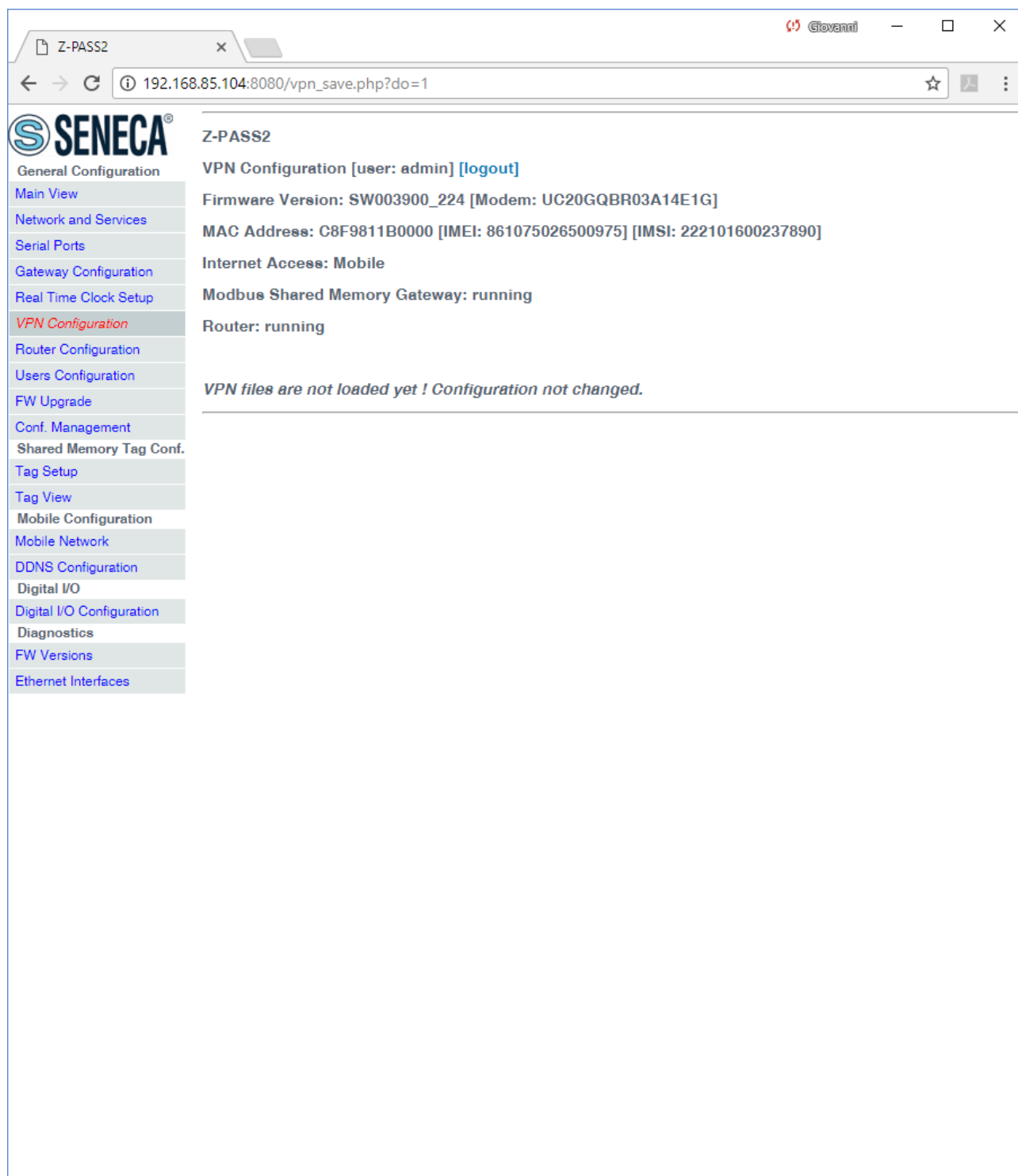
If VPN is enabled, the user is not allowed to delete VPN files, as warned by the following pop-up:



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, Z-PASS will run the Open VPN process with the loaded configuration	OFF

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



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 Z-PASS (see above)

as shown in the following couple of figures:

The screenshot displays the SENECA Z-PASS2 web interface for VPN configuration. The browser address bar shows the URL `192.168.85.104:8080/vpn_files.php?showinfo=1`. The left sidebar contains a menu with options like General Configuration, Main View, Network and Services, Serial Ports, Gateway Configuration, Real Time Clock Setup, VPN Configuration (highlighted), Router Configuration, Users Configuration, FW Upgrade, Conf. Management, Shared Memory Tag Conf., Tag Setup, Tag View, Mobile Configuration, Mobile Network, DDNS Configuration, Digital I/O, Digital I/O Configuration, Diagnostics, FW Versions, and Ethernet Interfaces.

The main configuration area is titled "Z-PASS2" and includes a "VPN Configuration [user: admin] [logout]" link. It displays the following information:

- Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
- MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
- Internet Access: Mobile
- Modbus Shared Memory Gateway: running
- Router: running

The "VPN Files" section contains a table with columns "CURRENT" and "UPDATED". It lists the following files and their current status:

File Name	Current	Updated
Configuration File (.ovpn or .conf)	OpenVPN	OpenVPN ▼
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

Below the table, there are "UPLOAD" and "RESET" buttons. The "VPN Configuration" section includes an "Enable" dropdown menu set to "OFF". There are "APPLY" and "HIDE VPN STATUS" buttons.

The "VPN Status" section shows the following information:

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

The "VPN Files (size in bytes)" section includes a note: "NOTE: these files can be downloaded via FTP from '/home/config/vpn/' directory." It lists the following files and their sizes:

File Name	Size (bytes)
CLIENT1.crt	3600
CLIENT1.key	912
ca.crt	1139
ovpn.conf	218

A "REFRESH" button is located at the bottom of the page.

Z-PASS1 / Z-PASS2

VPN Configuration [user: admin] [logout]

Firmware Version: SW003900_205 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002

Internet Access: Mobile

Modbus Bridge: 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	26 / 2.4K
TX Packets / Bytes	20 / 1.6K

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”, this means that Open VPN process could not be correctly started: probably, the configuration file contains some errors or, maybe, some options not supported by the Z-PASS 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.

19.7.1.6 OpenVPN Server configuration file

This paragraph gives an example of OpenVPN server configuration; this is the server configuration typically used with Z-PASS 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
```

19.7.1.7 OpenVPN Client configuration file

This paragraph gives an example of OpenVPN client configuration; this is the client configuration typically loaded on Z-PASS 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
```

19.7.1.8 LED signalling (Z-PASS1-R01/Z-PASS2-R01/Z-PASS1-IO/Z-PASS2-IO)

In Z-PASS1-R01/Z-PASS2-R01/Z-PASS1-IO/Z-PASS2-IO products, when VPN functionality is enabled in “OpenVPN” mode, the “SERV” and “VPN” LEDs give the following status information (see paragraph 6.2):

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

	OFF	VPN functionality is disabled
SERV Green	-	Not used

19.7.2 VPN Box

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

The screenshot shows a web browser window with the address bar displaying `192.168.85.104:8080/vpn_files.php`. The page title is "Z-PASS2". On the left, there is a navigation menu with the following items: General Configuration, Main View, Network and Services, Serial Ports, Gateway Configuration, Real Time Clock Setup, **VPN Configuration** (highlighted), Router Configuration, Users Configuration, FW Upgrade, Conf. Management, Shared Memory Tag Conf., Tag Setup, Tag View, Mobile Configuration, Mobile Network, DDNS Configuration, Digital I/O, Digital I/O Configuration, Diagnostics, FW Versions, and Ethernet Interfaces.

The main content area is titled "VPN Configuration [user: admin] [logout]". It displays the following information:

- Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
- MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
- Internet Access: Mobile
- Modbus Shared Memory Gateway: running
- Router: running

Below this information is a table with two columns: "CURRENT" and "UPDATED". The table has a header row with "VPN Mode" and "VPN Box". The "VPN Mode" column has a dropdown menu set to "VPN Box". The "VPN Box" column has a dropdown menu set to "VPN Box".

Below the table are several configuration fields:

- Enable: OFF (dropdown menu)
- Server: 192.168.85.176 (text input field)
- Password: seneca (text input field)
- Tag Name: zpass (text input field)

At the bottom of the configuration section are two buttons: "APPLY" and "SHOW VPN STATUS".

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 Z-PASS 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 Z-PASS; if the default (“zpass”) value is left, the Device will register as “zpass_<MACAddress>” on the VPN Box	zpass

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 VPN IP address assigned to the Z-PASS when “Connected”, the “dummy” IP address “0.0.0.0” when “Disconnected”; this row is not shown for “Point-to-Point (L2)” VPN Box, since no IP address is assigned to the VPN interface
- 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”, “Point-to-Point (L2)” or “Single LAN”, if VPN Box is enabled
- the “VPN Box Status”, if VPN Box is enabled
- the username of the connected user, if any

as shown in the following three figures:

Z-PASS2

192.168.85.104:8080/vpn_files.php?showinfo=1

SENECA®

General Configuration

Main View

Network and Services

Serial Ports

Gateway Configuration

Real Time Clock Setup

VPN Configuration

Router Configuration

Users Configuration

FW Upgrade

Conf. Management

Shared Memory Tag Conf.

Tag Setup

Tag View

Mobile Configuration

Mobile Network

DDNS Configuration

Digital I/O

Digital I/O Configuration

Diagnostics

FW Versions

Ethernet Interfaces

Z-PASS2

VPN Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
VPN Mode	VPN Box	VPN Box
VPN Box		
Enable	OFF	OFF
Server	192.168.85.176	192.168.85.176
Password	seneca	seneca
Tag Name	zpass	zpass

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

192.168.85.104:8080/vpn_files.php?showinfo=1

SENECA®

General Configuration

Main View

Network and Services

Serial Ports

Gateway Configuration

Real Time Clock Setup

VPN Configuration

Router Configuration

Users Configuration

FW Upgrade

Conf. Management

Shared Memory Tag Conf.

Tag Setup

Tag View

Mobile Configuration

Mobile Network

DDNS Configuration

Digital I/O

Digital I/O Configuration

Diagnostics

FW Versions

Ethernet Interfaces

Z-PASS2

VPN Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
VPN Mode	VPN Box	VPN Box ▼
VPN Box		
Enable	ON	ON ▼
Server	192.168.85.176	192.168.85.176
Password	seneca	seneca
Tag Name	zpass	zpass

APPLY

HIDE VPN STATUS

VPN Status

Connection Status	Connected
IP Address	10.9.0.1
OpenVPN Status	Running
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0
VPN Box Type	Point-to-Point
VPN Box Status	OK (Configured)

REFRESH

Z-PASS2

VPN Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
VPN Mode	VPN Box	VPN Box ▼
VPN Box		
Enable	ON	ON ▼
Server	192.168.85.176	192.168.85.176
Password	seneca	seneca
Tag Name	zpass	zpass

APPLY HIDE VPN STATUS

VPN Status	
Connection Status	Connected
IP Address	10.9.0.1
OpenVPN Status	Running
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0
VPN Box Type	Point-to-Point
VPN Box Status	OK (Configured)
Connected User	gspagiari

REFRESH

For an explanation of the differences between a “Single LAN” VPN and a “Point-to-Point” VPN, see chapter 13.

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 Z-PASS (it should never occur)
Error (No response from VPN Box)		No response has been received from the VPN Box (response timeout)
Error (Invalid response from VPN Box)		A response has been received whose content is not valid for the Z-PASS (it should never occur)
Error (Wrong password)		The password set on Z-PASS 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 Z-PASS has just been registered on the VPN Box
OK	New	The Z-PASS is registered on the VPN Box, but it is not configured yet ("Single LAN" only)
OK	Configuration updated	The Z-PASS configuration has just been updated
OK	Configured	The Z-PASS is properly configured and available for VPN connection
OK	Ban	The Z-PASS has been banned
OK	Not found	The Z-PASS is unknown for the VPN Box; this happens when Z-PASS registration is deleted on the VPN Box
OK	Unknown	The Z-PASS has an "unknown" status in the VPN Box (it should never occur)
OK	Not bound	The "tunnel" between the Z-PASS 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 Z-PASS (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.

19.7.2.1.1 LED signalling (Z-PASS1-R01/Z-PASS2-R01/Z-PASS1-IO/Z-PASS2-IO)

In Z-PASS1-R01/Z-PASS2-R01/Z-PASS1-IO/Z-PASS2-IO products, when VPN functionality is enabled in "VPN Box/Single LAN" mode, the "SERV" and "VPN" LEDs give the following status information (see paragraph 6.2):

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	VPN Box “SERVICE” connection is not working properly
	OFF	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 6.2):

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

19.8 Router Configuration

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

SENECA®
General Configuration

- Main View
- Network and Services
- Serial Ports
- Gateway Configuration
- Real Time Clock Setup
- VPN Configuration
- Router Configuration**
- Users Configuration
- FW Upgrade
- Conf. Management
- Shared Memory Tag Conf.
- Tag Setup
- Tag View
- Mobile Configuration
- Mobile Network
- DDNS Configuration
- Digital I/O
- Digital I/O Configuration
- Diagnostics
- FW Versions
- Ethernet Interfaces

Z-PASS2
Router Configuration [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861076026600976] [IMSI: 222101600237890]
Internet Access: Ethernet
Modbus Shared Memory Gateway: 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 ▼
Mobile Network Firewall		
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		

APPLY

In this page, you can change the parameters related to the Z-PASS 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 functionality	OFF
DNS Enable	Flag to enable/disable the DNS forwarding service	ON
DHCP Server Enable	Flag to enable/disable the DHCP service (DHCP server) NOTE: <u>this parameter can be set to “ON” only if the “DHCP” parameter of the “Network and Services” page is set to “OFF”.</u>	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 time interval 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/Enable	Flag to enable/disable the access to the Z-PASS and other devices which are in the Z-PASS LAN, by using their local (LAN) IP addresses	OFF

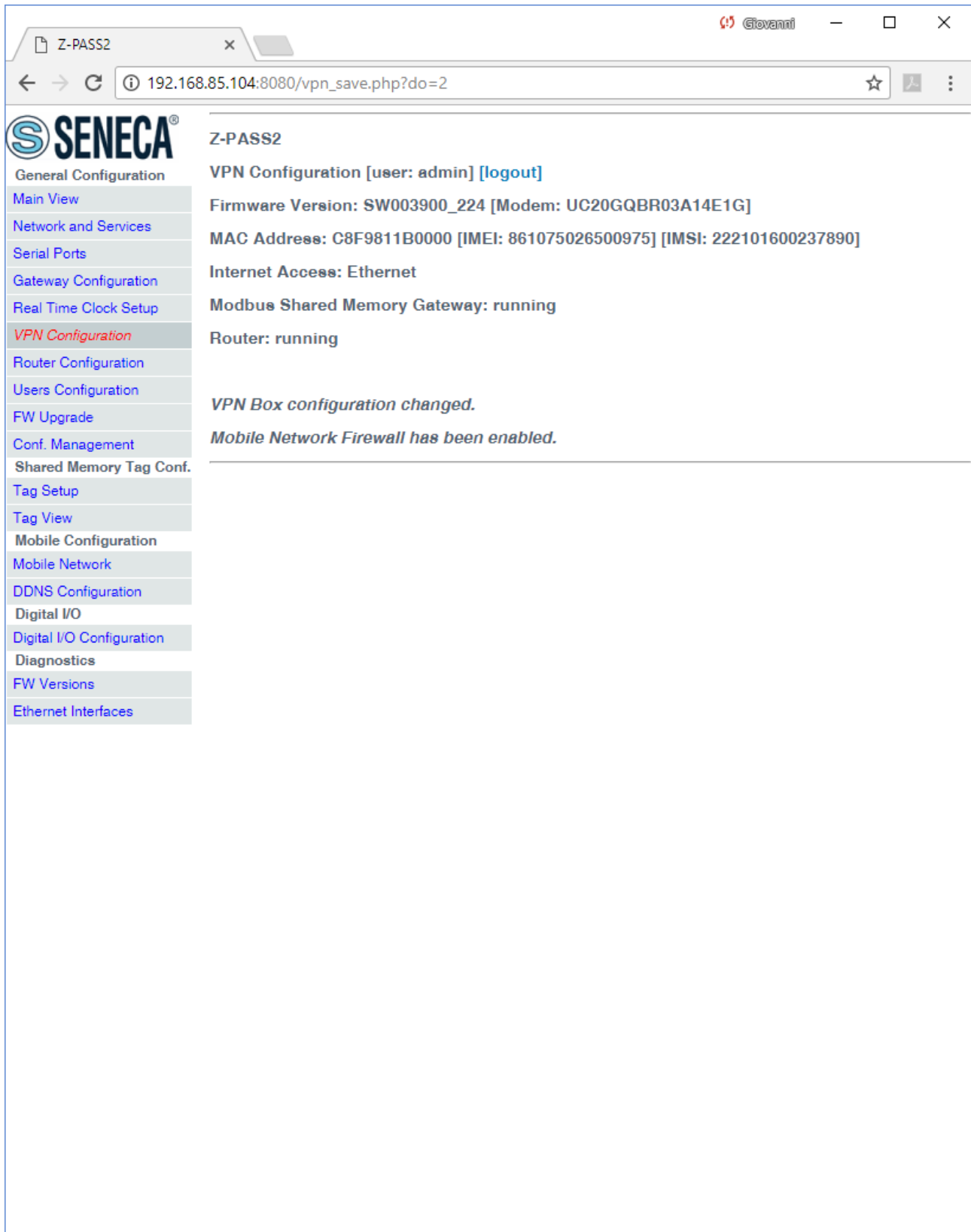
Then, you have another important parameter, which is shown in the following table.

Field	Meaning	Default value
Mobile Network Firewall/Enable	Flag to enable/disable the “Mobile Network Firewall”, that is disable/enable access to the Z-PASS and other devices which are in the Z-PASS LAN, by using the IP address assigned to the Mobile Network (3G) interface. <u>To open a port in the firewall, a “Port Mapping / Virtual Server” rule shall be defined.</u>	OFF

The above parameter shall be set to ON, to protect the Z-PASS 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).

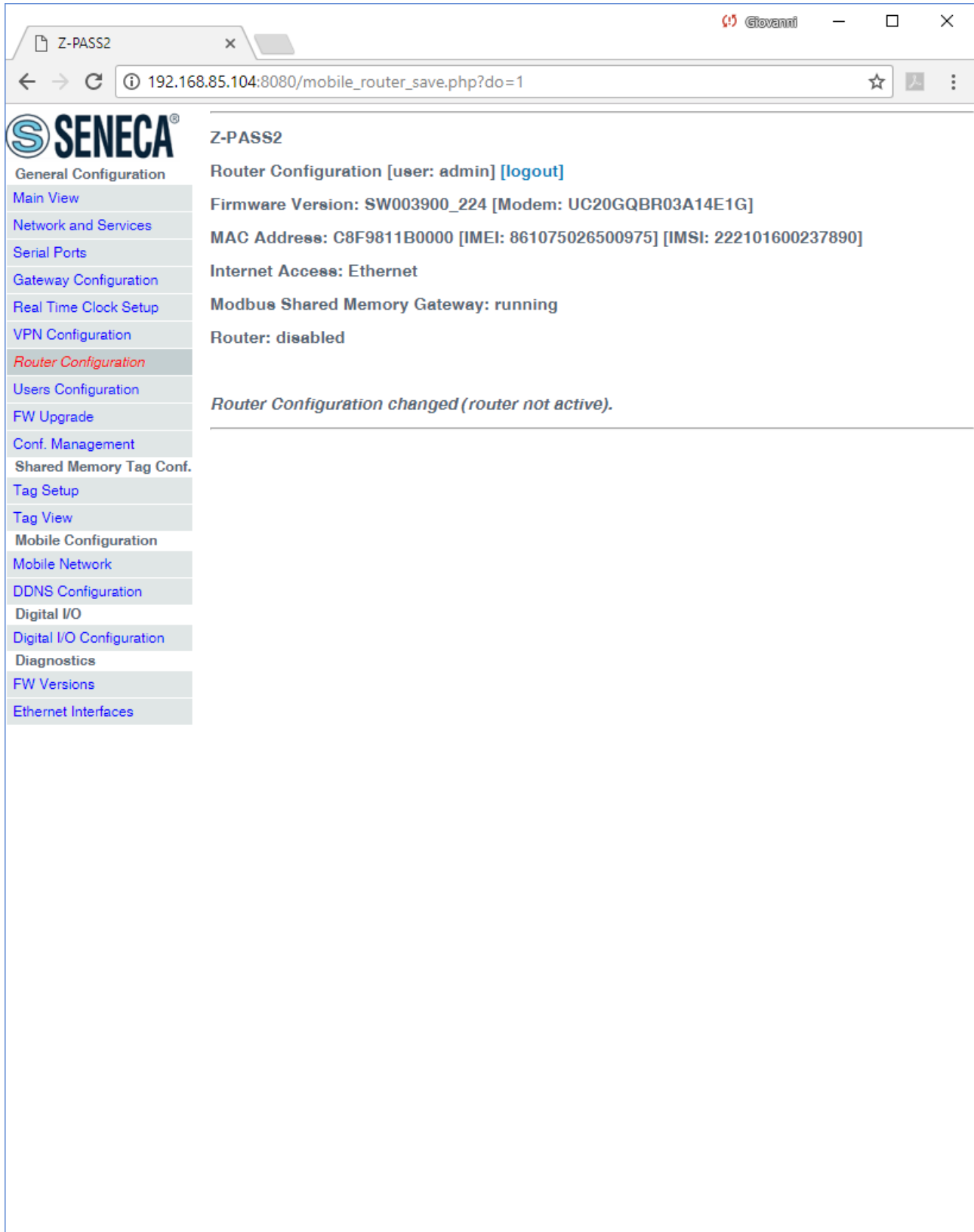
It is important to note that, when the VPN is activated (see 19.7 paragraph), the parameter is automatically set to ON, as warned by the message shown in the following figure.



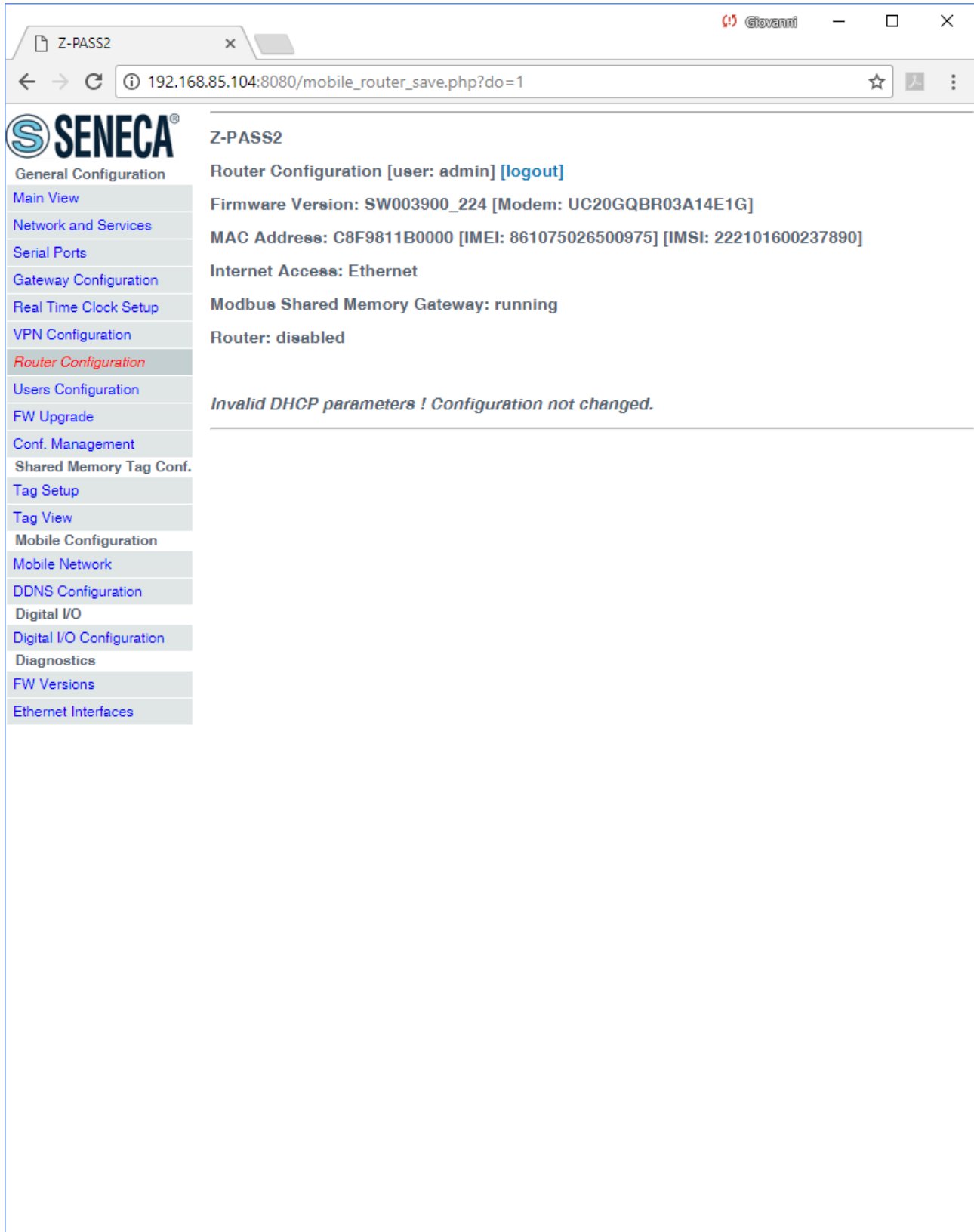
Finally, there are 5 sections which let you define up to 5 “Port Mapping” rules (also known as “Virtual Servers”); for each section, the available parameters are the following:

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	<i>Empty</i>
Server IP Address	IP address which the received packet is forwarded to	<i>Empty</i>
Internal Port	TCP or UDP port which the received packet is forwarded to	<i>Empty</i>

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



If you try to enable the DHCP server functionality (DHCP 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:



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-PASS2

Router Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861076026600976] [IMSI: 222101600237890]

Internet Access: Ethernet

Modbus Shared Memory Gateway: 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	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	ON	ON ▼
Mobile Network Firewall		
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	192.168.85.103	192.168.85.103
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		

APPLY

In this example, 2 rules have been set:

- the first rule tells Z-PASS 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 Z-PASS configuration web site on the standard HTTP port;

- the second rule tells Z-PASS that any TCP or UDP packet received on the 502 port (which is often used for Modbus TCP protocol) shall be forwarded to the 192.168.85.103 IP address (which corresponds to another device) on the same (502) destination port.

Another important aspect of “Port Mapping / Virtual Server” rules is that they let define which ports are open in the “Mobile Network Firewall”; for example, if you want to connect to the web configuration site and to the SSH console, through the public IP address assigned to the 3G interface, the 8080 and 22 TCP ports shall be open; this can be done as shown in the following figure.

Z-PASS2

192.168.85.104:8080/mobile_router.php

General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces

Z-PASS2

Router Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861076026600976] [IMSI: 222101600237890]

Internet Access: Ethernet

Modbus Shared Memory Gateway: 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	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 ▼
Mobile Network Firewall		
Enable	ON	ON ▼
Port Mapping / Virtual Server 1		
Protocol	TCP	TCP ▼
External Port	8080	8080
Server IP Address		
Internal Port	8080	8080
Port Mapping / Virtual Server 2		
Protocol	TCP	TCP ▼
External Port	22	22
Server IP Address		
Internal Port	22	22
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		

APPLY

19.9 Users Configuration

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

SENECA®

General Configuration

Main View

Network and Services

Serial Ports

Gateway Configuration

Real Time Clock Setup

VPN Configuration

Router Configuration

Users Configuration

FW Upgrade

Conf. Management

Shared Memory Tag Conf.

Tag Setup

Tag View

Mobile Configuration

Mobile Network

DDNS Configuration

Digital I/O

Digital I/O Configuration

Diagnostics

FW Versions

Ethernet Interfaces

Z-PASS2

Users Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

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

APPLY

In this page, you can change the “Web Administrator”, “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 GUEST/Username	Username to access the web configuration site, in “view-only mode” (see paragraph 19.19)	guest
WEB GUEST/Password	Password to access the web configuration site, in “view-only mode” (see paragraph 19.19)	guest
FTP USER/Username	Username to access the Device FTP/SFTP site	user
FTP USER/Password	Password to access the Device FTP/SFTP site	123456

For all the fields in this page, the following characters are allowed:

a-zA-Z0-9- _ | ! @ \$ % ^ & * ? + { } < > ; , : .

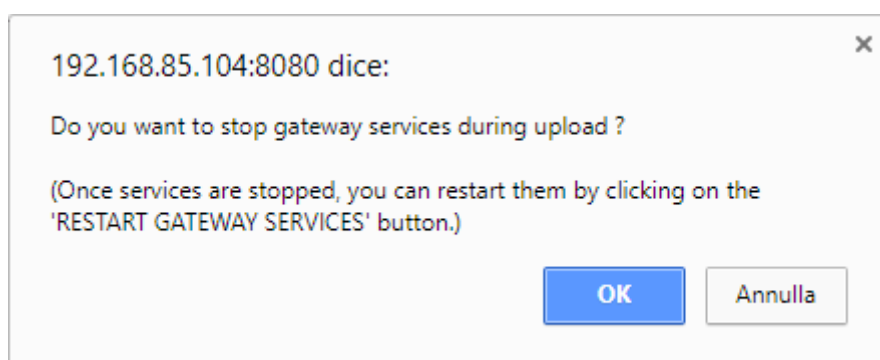
each field can contain up to 100 characters.

The same rules apply to the other “Username” and “Password” fields of the web pages and to the “Tag Name” field of the “VPN Configuration” page.

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

19.10 FW Upgrade

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



If you click on the “OK” button, Modbus Ethernet to Serial/Transparent/Modbus Shared Memory Gateway Services are stopped and you come to the “FW Upgrade” page, shown in the following figure.



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

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



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

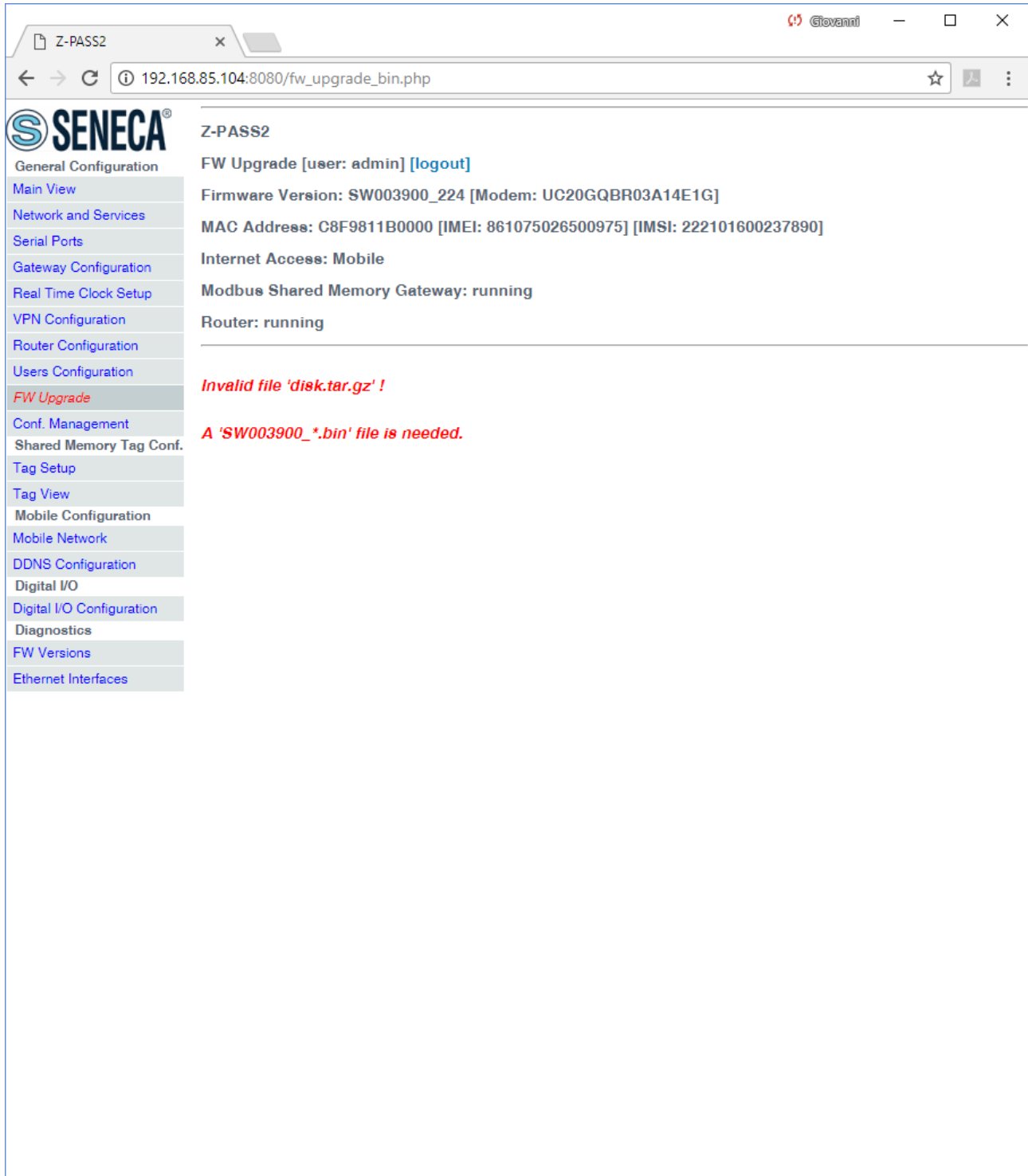
Since an erroneous use of the FW Upgrade functionality might compromise the proper Z-PASS operation, use this page only to apply upgrades provided by Seneca, with the support of Seneca personnel.

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

*SW003900_xxx.bin*¹⁸

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.

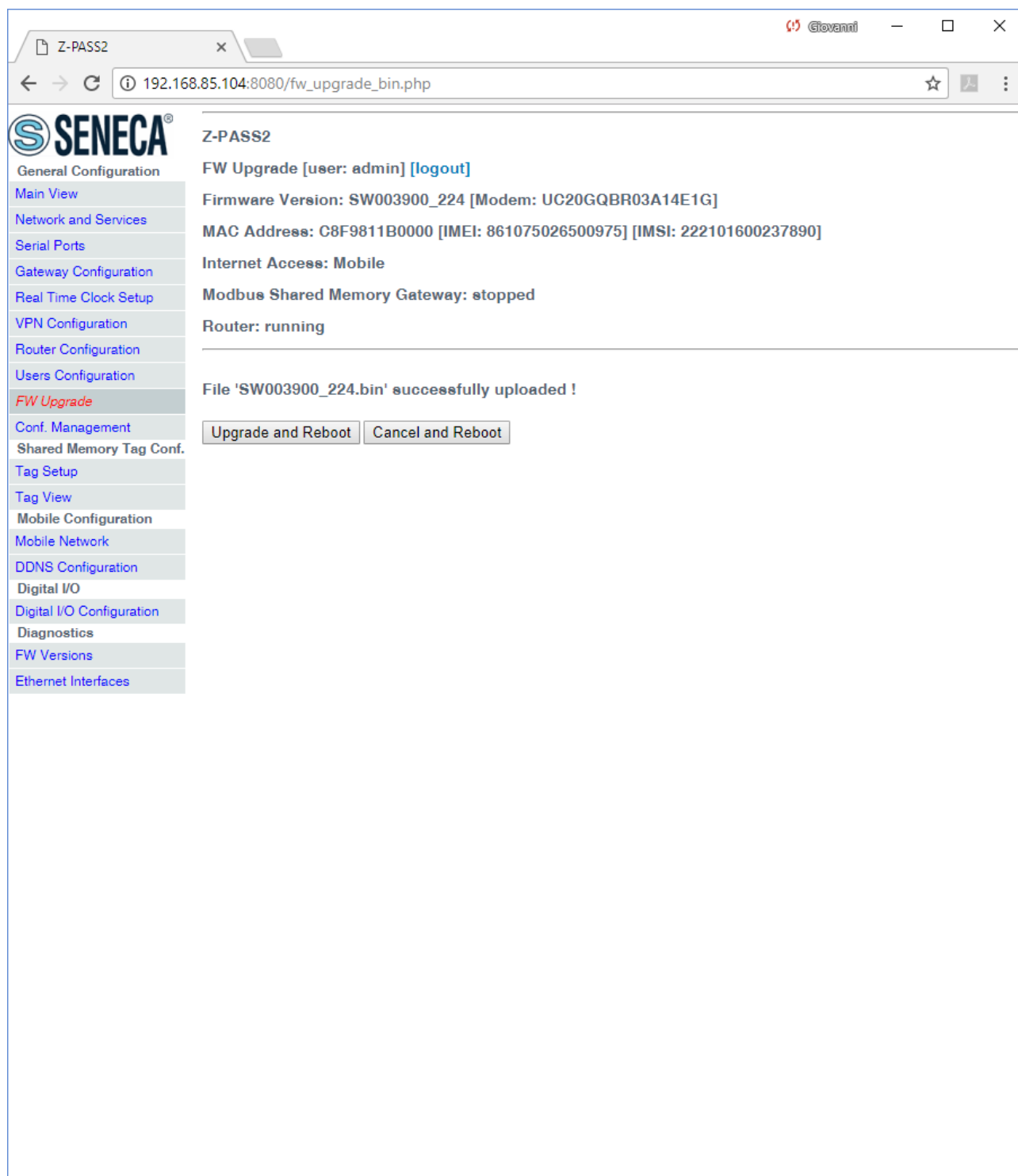
¹⁸ The FW file can be downloaded from Seneca web site (see chapter “Upgrading the firmware by USB pen”).



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



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



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 Z-PASS MUST NOT be switched off; during the

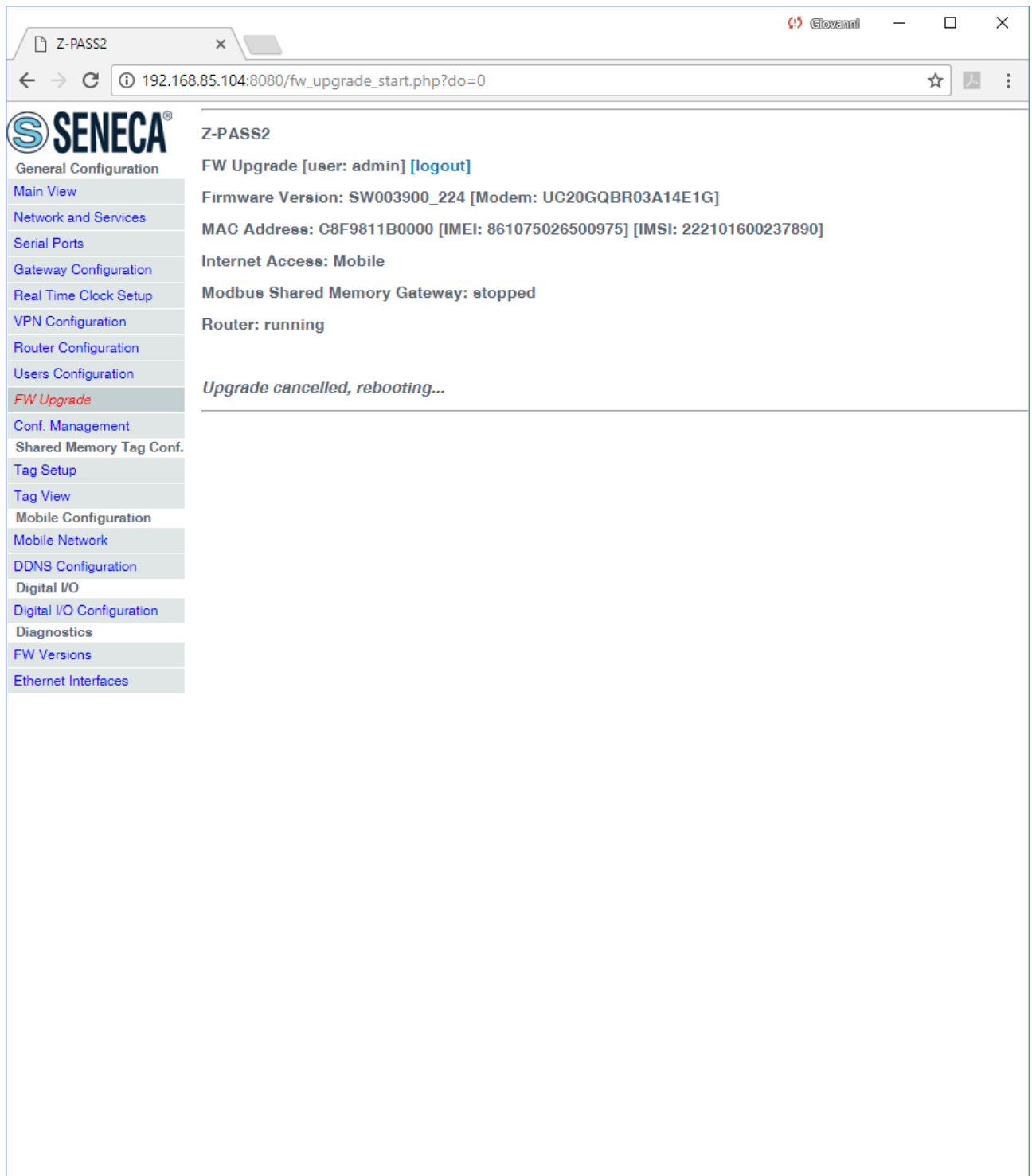
procedure, the Z-PASS will be rebooted several times; also, during the procedure, several LEDs will blink simultaneously¹⁹; the upgrade procedure is ended when only the LED “RUN” is blinking²⁰;



¹⁹ This applies only to products with HW revisions IO and R01; in details: for IO HW revision, all LEDs will blink simultaneously, except for Power, LAN/WAN, COM and modem LEDs; for R01 HW revision, RUN, VPN and SERV LEDs will blink.

²⁰ Also SERV and VPN LEDs might blink, depending on the Device configuration and status.

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



19.11 Configuration Management

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



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 *SW003900_conf.tar.gz* and carries:

- files containing all configuration parameter values;
- files containing the Modbus Shared Memory Gateway tags, if present;
- 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 Z-PASS by means of a USB pen is the following:

- copy the *SW003900_conf.tar.gz* file into the root folder of the USB pen;
- switch off the Device;
- insert the USB pen into the USB#1 port of the Z-PASS;
- switch on the Z-PASS; the procedure will take some minutes to be completed; during this time, the Z-PASS MUST NOT be switched off; during the procedure, the Z-PASS will be rebooted;
- after the reboot, wait until you see the “RUN” LED blinking;
- remove the USB pen;
- the configuration has been applied to the Z-PASS.

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-R01 into a Z-PASS2.

This page lets you load also the configuration archive as a zip file (*SW003900_conf.zip*).

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 *SW003900_logs.tar.gz* is downloaded, which contains the debug logs stored by the CPU during its operation.



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

19.11.1 Factory reset by USB pen

A USB pen can be used also to reset the Z-PASS to its factory state; the procedure is the following:

- create an empty file named *SW003900_reset_cmd* into the root of the USB pen;
- switch off the Z-PASS;
- insert the USB pen into the USB#1 port of the Z-PASS;

- switch on the Z-PASS; the procedure will take some minutes to be completed; during this time, the Z-PASS MUST NOT be switched off; during the procedure, the Z-PASS will be rebooted;
- after the reboot, wait until you see the “RUN” LED blinking;
- remove the USB pen;
- the factory reset has been performed.

19.12 Mobile Network

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

SENECA®

General Configuration

- Main View
- Network and Services
- Serial Ports
- Gateway Configuration
- Real Time Clock Setup
- VPN Configuration
- Router Configuration
- Users Configuration
- FW Upgrade
- Conf. Management
- Shared Memory Tag Conf.
- Tag Setup
- Tag View
- Mobile Configuration
- Mobile Network**
- DDNS Configuration
- Digital I/O
- Digital I/O Configuration
- Diagnostics
- FW Versions
- Ethernet Interfaces

Z-PASS2

Mobile Network [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Ethernet

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
SIM		
PIN (if required by SIM)	8342	8342
Operator Selection		
Mode	Automatic	Automatic
Operator	[22201] I TIM (UMTS)	Operator list not available
Data Connection		
Enable	OFF	OFF
APN Mode	Automatic	Automatic
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None
Username	user	user
Password	pass	pass
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

The above figure shows the “Mobile Network” page for Z-PASS2-IO.

For Z-PASS2-R01 and Z-PASS2, the “Operator Selection” section and the “GET OPERATOR LIST” button are not available, so the page is as shown in the following figure.

Z-PASS2

Mobile Network [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: 1231B02SIM5350E]

MAC Address: C8FA81160002 [IMEI: 862264020406715] [IMSI: 222101600237889]

Internet Access: Ethernet

Modbus Ethernet to Serial Gateway: running

Router: disabled

	CURRENT	UPDATED
SIM		
PIN (if required by SIM)	8342	8342
Data Connection		
Enable	OFF	OFF
APN Mode	Automatic	Automatic
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None
Username	user	user
Password	pass	pass
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
SIM/PIN (if required by SIM)	PIN needed to unlock the SIM card, if PIN locking functionality is enabled	1234

	on it ²¹	
Operator Selection/Mode (only on Z-PASS2-IO)	This parameter tells if the modem shall select the Mobile Network Operator: - automatically (Mode=Automatic) - as selected by the user (Mode=Manual) - reverting to “automatic” mode, if “manual” selection fails (Mode = Manual/ Automatic)	Automatic
Operator Selection/Operator (only on Z-PASS2-IO)	This parameter contains the list of the Mobile Network Operators currently available, that is detected by the modem. The list items are strings with the following format: - the MCC+MNC²² code in square brackets (e.g.: “[22201]”) - the string identifying the operator (e.g.: “I TIM”) - the access technology, that is “GSM” or “UMTS”, in brackets This list is initially empty: it shall be filled by clicking on the “GET OPERATOR LIST” button.	“[22201] I TIM (UMTS)”
Data Connection/Enable	Flag to enable/disable the Mobile Network connectivity	OFF
Data Connection/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 (Mode=Manual). When APN Mode = Automatic, APN, Authentication Type, Username and Password parameters are disabled.	Automatic
Data Connection/APN	Access Point Name, as given by the Mobile Network Operator	ibox.tim.it
Data Connection/Authentication Type	Type of authentication required; possible values are: “None”,	None

²¹ Please note that the procedure to enable/disable the PIN locking functionality on the SIM is not performed by the Device.

²² MCC = Mobile Country Code, MNC = Mobile Network Code

	"CHAP/PAP", "CHAP only", "PAP only"	
Data Connection/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
Data Connection/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
Data Connection/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 left empty, the check is not performed. It is important to note that the FQDN or IP address specified must be reachable from the Z-PASS mobile network, otherwise the Z-PASS will detect that the mobile connection is not working and will drop it.	www.google.com

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

- the SIM/PIN Status; if an error in PIN setting has occurred or PUK/PUK2 setting is needed, this status is shown in red color
- the number of remaining attempts for PIN setting; when this value is less than 3 (shown in red color), it means that PIN setting has failed, that is the configured PIN value is wrong
- the radio "Signal Level", in the range [0..7]
- the selected operator (only for Z-PASS2-IO)
- 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

192.168.85.104:8080/mobile_network.php?showinfo=1

General Configuration

- Main View
- Network and Services
- Serial Ports
- Gateway Configuration
- Real Time Clock Setup
- VPN Configuration
- Router Configuration
- Users Configuration
- FW Upgrade
- Conf. Management
- Shared Memory Tag Conf.
- Tag Setup
- Tag View
- Mobile Configuration
- Mobile Network**
- DDNS Configuration
- Digital I/O
- Digital I/O Configuration
- Diagnostics
- FW Versions
- Ethernet Interfaces

Z-PASS2

Mobile Network [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Ethernet

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
SIM		
PIN (if required by SIM)	8342	8342
Operator Selection		
Mode	Automatic	Automatic
Operator	[22201] I TIM (UMTS)	Operator list not available
Data Connection		
Enable	OFF	OFF
APN Mode	Automatic	Automatic
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None
Username	user	user
Password	pass	pass
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

Mobile Status

SIM/PIN Status	PIN required
PIN Remaining Attempts	3
Signal Level [0..7]	5
Selected Operator	"vodafone IT" (UMTS)
Registration Status	Registered (home network)
Connection Status	Disconnected
IP Address	0.0.0.0
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0
GPS Location	45.37421,11.94562 [Map]

SENECA®

General Configuration

- Main View
- Network and Services
- Serial Ports
- Gateway Configuration
- Real Time Clock Setup
- VPN Configuration
- Router Configuration
- Users Configuration
- FW Upgrade
- Conf. Management
- Shared Memory Tag Conf.
- Tag Setup
- Tag View
- Mobile Configuration
- Mobile Network**
- DDNS Configuration
- Digital I/O
- Digital I/O Configuration
- Diagnostics
- FW Versions
- Ethernet Interfaces

Z-PASS2

Mobile Network [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

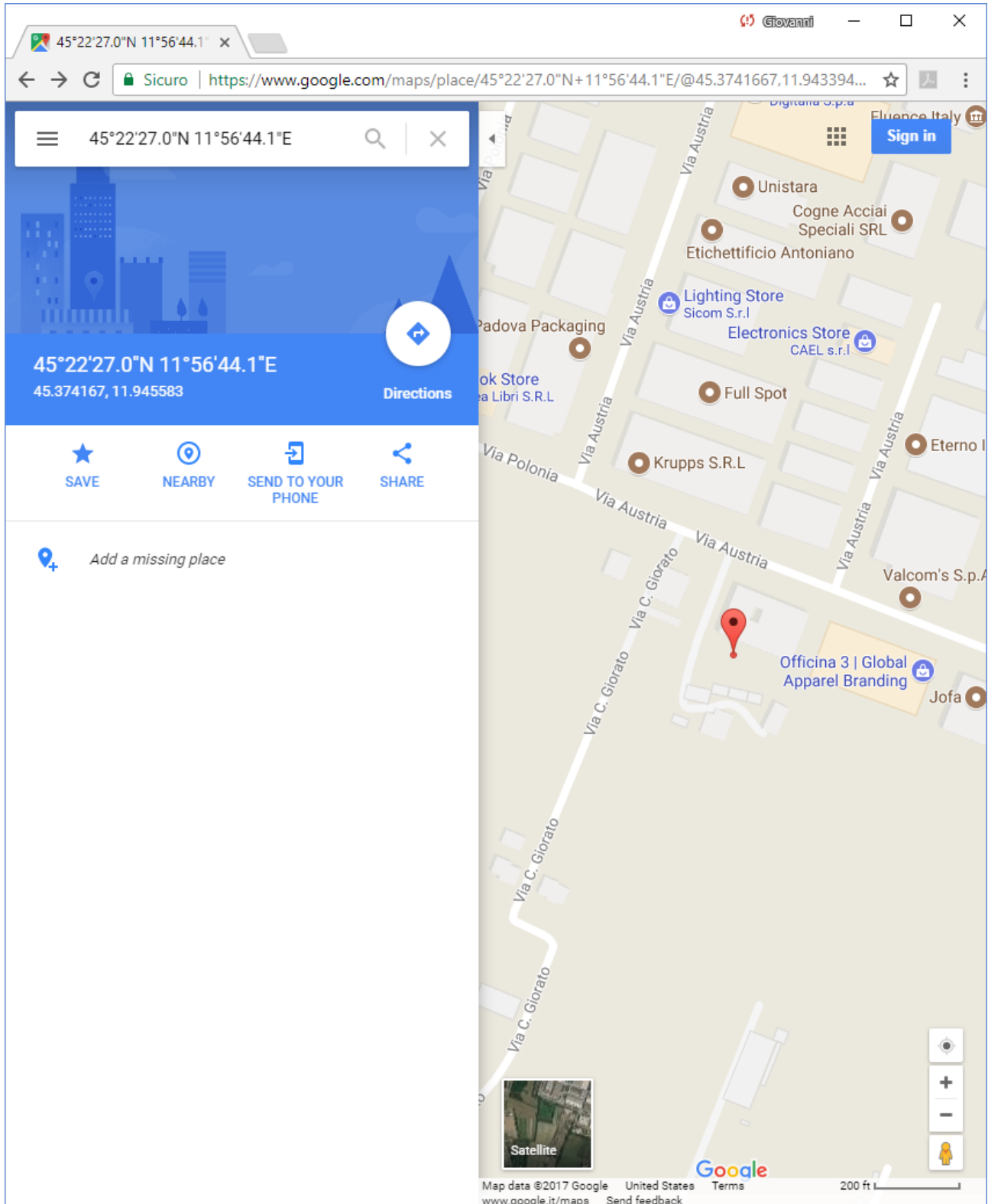
	CURRENT	UPDATED
SIM		
PIN (if required by SIM)	8342	8342
Operator Selection		
Mode	Automatic	Automatic
Operator	[22201] I TIM (UMTS)	Operator list not available
Data Connection		
Enable	ON	ON
APN Mode	Automatic	Automatic
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None
Username	user	user
Password	pass	pass
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

APPLY HIDE MOBILE STATUS GET OPERATOR LIST

Mobile Status	
SIM/PIN Status	PIN required
PIN Remaining Attempts	3
Signal Level [0..7]	5
Selected Operator	"vodafone IT" (UMTS)
Registration Status	Registered (home network)
Connection Status	Connected
IP Address	10.211.101.167
RX Packets / Bytes	6 / 65
TX Packets / Bytes	6 / 98
GPS Location	45.37421,11.94562 [Map]

REFRESH

As shown in the above figures, only for Z-PASS2-IO, the last row of the “Mobile Status” gives the “GPS Location” as Latitude, Longitude values; clicking on the [Map](#) link, the Google Maps™ on the current position are shown.



If the GPS signal is not available, the “GPS Location” row contains the string “Not fixed” and the [Map](#) link is not shown.

The following figure shows the situation when an error in PIN setting has occurred, due to a wrong value of the PIN parameter.

The screenshot displays the Z-PASS2 web interface in a browser window. The address bar shows the URL `192.168.85.104:8080/mobile_network.php?showinfo=1`. The interface includes a sidebar with navigation links such as General Configuration, Main View, Network and Services, Serial Ports, Gateway Configuration, Real Time Clock Setup, VPN Configuration, Router Configuration, Users Configuration, FW Upgrade, Conf. Management, Shared Memory Tag Conf., Tag Setup, Tag View, Mobile Configuration, Mobile Network (highlighted), DDNS Configuration, Digital I/O, Digital I/O Configuration, Diagnostics, FW Versions, and Ethernet Interfaces.

The main content area is titled "Z-PASS2" and shows the "Mobile Network" configuration page. It includes fields for Firmware Version (SW003900_224), MAC Address (C8F9811B0000), Internet Access (Ethernet), Modbus Shared Memory Gateway (running), and Router (running). Below these are configuration options for SIM, Operator Selection, Data Connection, and Ping Connection Testing IP Address.

	CURRENT	UPDATED
SIM		
PIN (if required by SIM)	1234	1234
Operator Selection		
Mode	Automatic	Automatic
Operator	[22201] I TIM (UMTS)	Operator list not available
Data Connection		
Enable	OFF	OFF
APN Mode	Automatic	Automatic
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None
Username	user	user
Password	pass	pass
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

Buttons: APPLY, HIDE MOBILE STATUS, GET OPERATOR LIST

Mobile Status

SIM/PIN Status	PIN error
PIN Remaining Attempts	2
Signal Level [0..7]	4
Selected Operator	No operator
Registration Status	Searching for network
Connection Status	Disconnected
IP Address	0.0.0.0
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0
GPS Location	Not fixed

REFRESH button

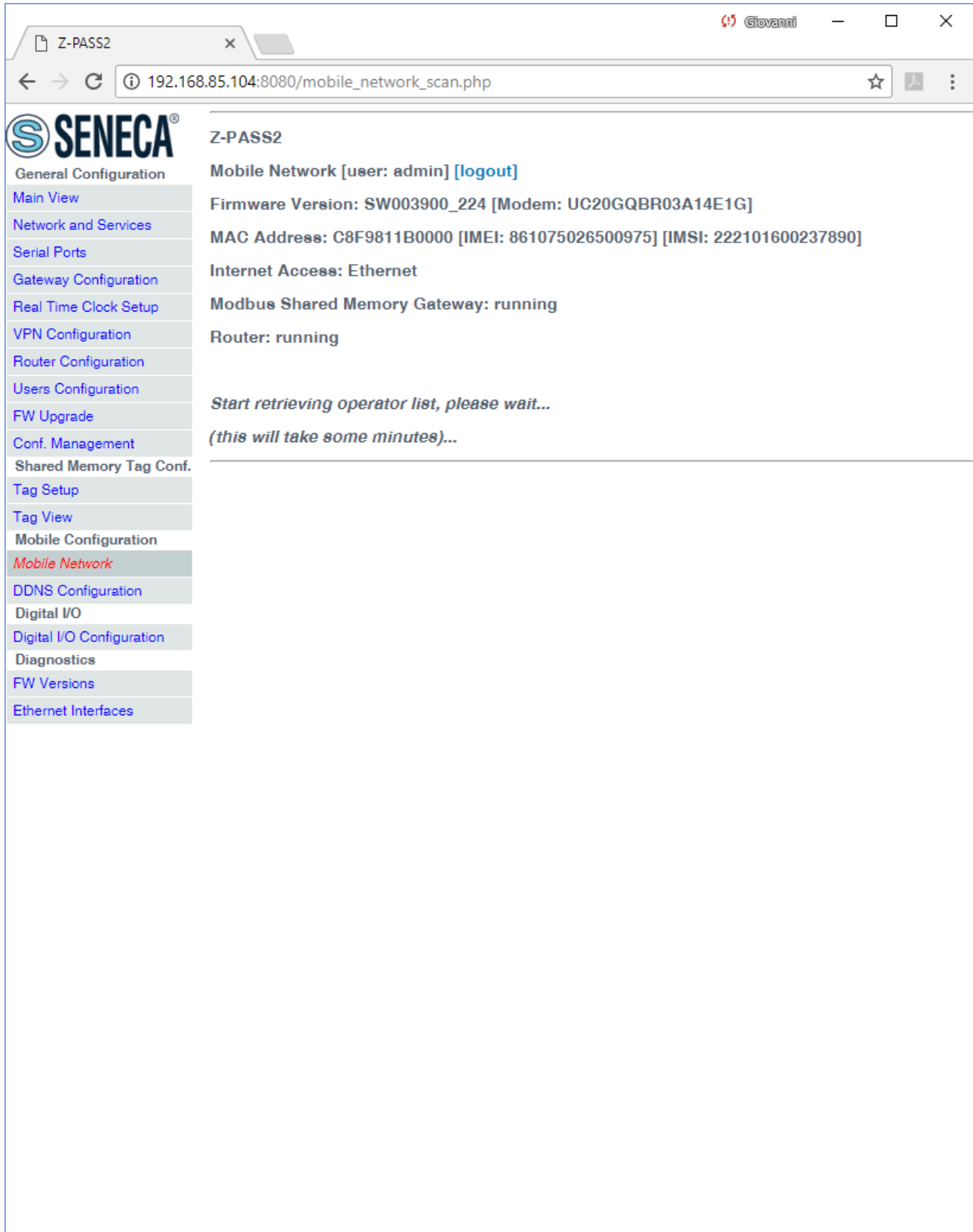
It should be noted that, when the PIN is set during procedures automatically performed by the Z-PASS firmware, if the number of remaining attempts is 1, no more attempt is done to avoid blocking the SIM.

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

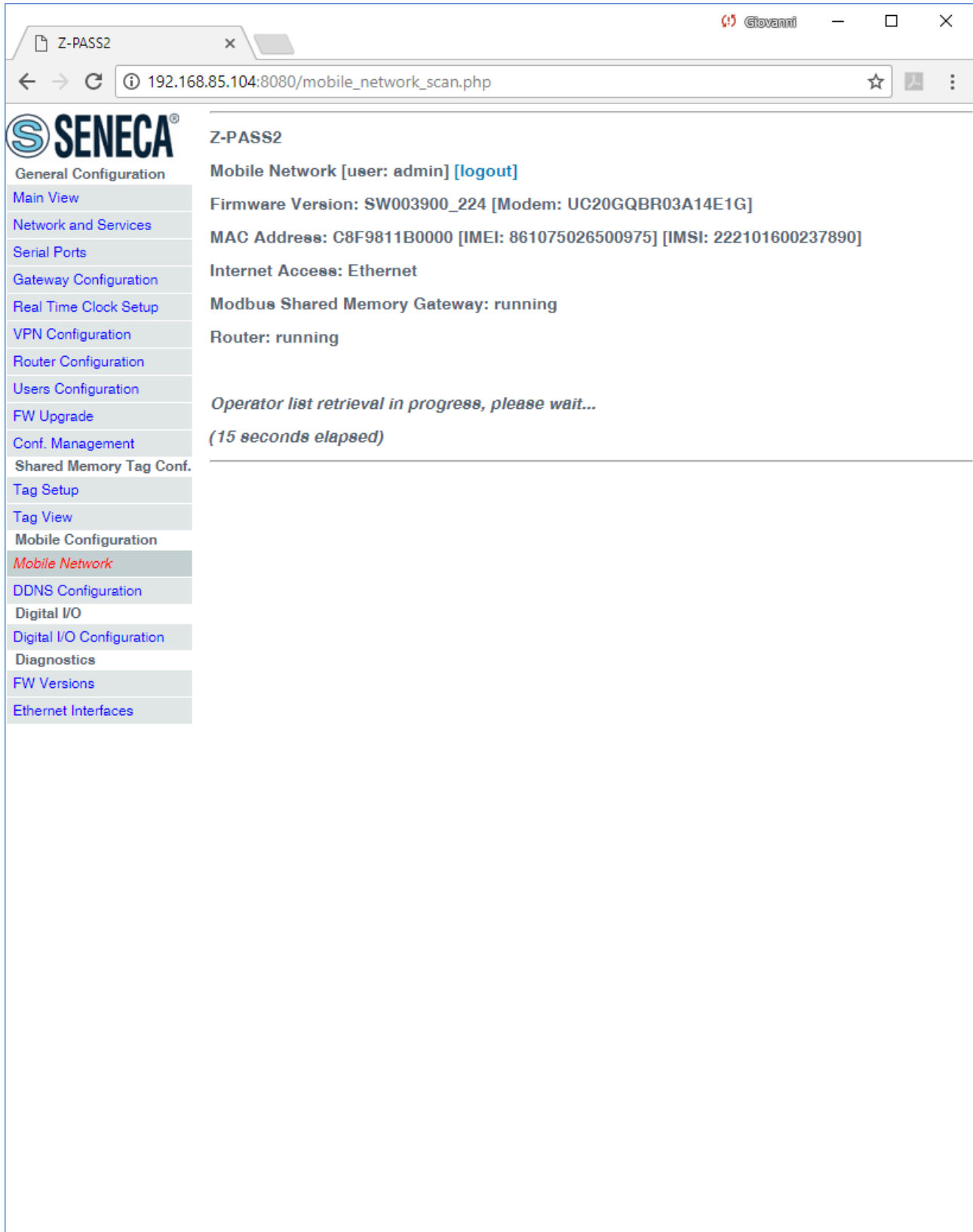
You can hide the “Mobile Status” section, by clicking on the “HIDE MOBILE STATUS” button.

As already told above, the “GET OPERATOR LIST” button lets you retrieve the list of the operators currently available, that is detected by the modem (only on Z-PASS2-IO).

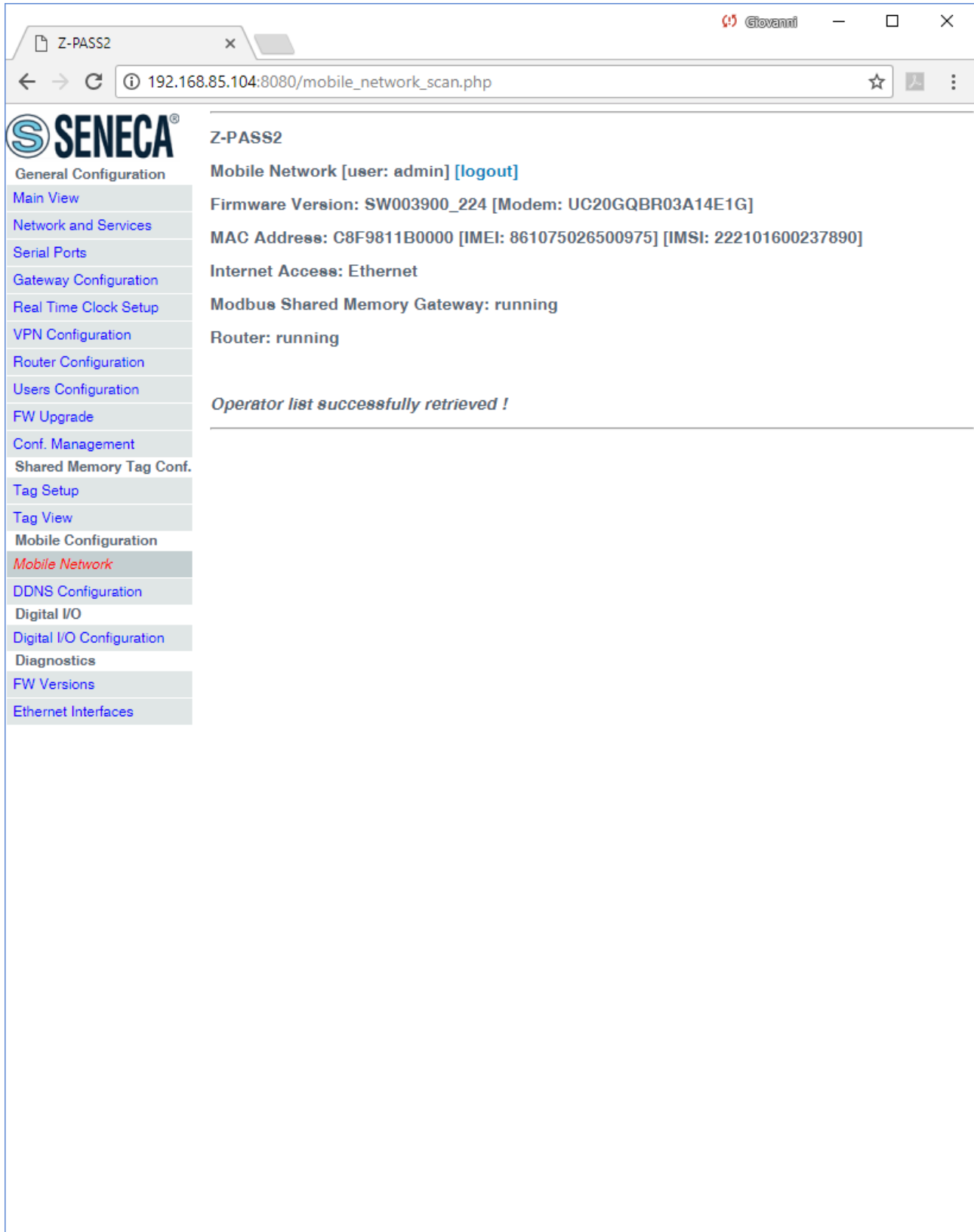
When you click on the button, the following page is shown.



Typically, it takes about 1 minute to get the list, so the page shows the number of seconds elapsed.



When the procedure is completed, the following page is shown.



After some seconds, the page automatically evolves to the “Mobile Network” page, with the operator list filled, as shown in the following figure.

Z-PASS2

192.168.85.104:8080/mobile_network.php

General Configuration
Main View
Network and Services
Serial Ports
Gateway Configuration
Real Time Clock Setup
VPN Configuration
Router Configuration
Users Configuration
FW Upgrade
Conf. Management
Shared Memory Tag Conf.
Tag Setup
Tag View
Mobile Configuration
Mobile Network
DDNS Configuration
Digital I/O
Digital I/O Configuration
Diagnostics
FW Versions
Ethernet Interfaces

Z-PASS2

Mobile Network [user: admin] [logout]
Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]
MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
Internet Access: Ethernet
Modbus Shared Memory Gateway: running
Router: running

	CURRENT	UPDATED
SIM		
PIN (if required by SIM)	8342	8342
Operator Selection		
Mode	Automatic	Automatic
Operator	[22201] I TIM (UMTS)	[22210] Vodafone IT (GSM) [22210] Vodafone IT (GSM) [22210] Vodafone IT (UMTS) [22201] I TIM (GSM) [22250] unknown (UMTS) [22288] I WIND (UMTS) [22288] I WIND (GSM) [22299] 3 ITA (UMTS) [22201] I TIM (UMTS)
Data Connection		
Enable	OFF	
APN Mode	Automatic	
APN	ibox.tim.it	ibox.tim.it
Authentication Type	None	None
Username	user	user
Password	pass	pass
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

You can choose an operator from the list, to perform “Manual” or “Manual/Automatic” selection.

19.13 DDNS Configuration

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

Z-PASS2

DDNS Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Ethernet

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
<i>DDNS Configuration</i>		
Type	None	None ▼
Hostname		
Username		
Password		
APPLY		
<i>DDNS Update Status</i>		
Status		---
IP Address		---

In this page, you can set the parameters related to the Dynamic DNS service, as listed in the following table:

Field	Meaning	Default value
Type	Type of Dynamic DNS service; possible values are: - None - dyndns.it - dyndns.org - no-ip.com	None
Hostname	The hostname provided with the service subscription	empty
Username	The username provided with the service subscription	empty
Password	The password provided with the service subscription	empty

The parameters shall be set according to the DDNS service subscription; an example is given in the following figure.

Z-PASS2

DDNS Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Ethernet

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
DDNS Configuration		
Type	dyndns.it	dyndns.it ▼
Hostname	zpasstest1.ns0.it	zpasstest1.ns0.it
Username	gsp-seneca	gsp-seneca
Password	123456	123456

APPLY

DDNS Update Status	
Status	---
IP Address	---

When an IP address assigned to the Mobile Network Interface has been bound with the hostname, the “DDNS Update Status” section appears like in the following figure.

Z-PASS2

192.168.85.104:8080/ddns_conf.php

General Configuration

- Main View
- Network and Services
- Serial Ports
- Gateway Configuration
- Real Time Clock Setup
- VPN Configuration
- Router Configuration
- Users Configuration
- FW Upgrade
- Conf. Management
- Shared Memory Tag Conf.
- Tag Setup
- Tag View
- Mobile Configuration
- Mobile Network
- DDNS Configuration**
- Digital I/O
- Digital I/O Configuration
- Diagnostics
- FW Versions
- Ethernet Interfaces

Z-PASS2

DDNS Configuration [user: admin] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
DDNS Configuration		
Type	dyndns.it	dyndns.it
Hostname	zpasstest1.ns0.it	zpasstest1.ns0.it
Username	gsp-seneca	gsp-seneca
Password	egdirba!	egdirba!
DDNS Update Status		
Status	good	
IP Address	91.80.5.100	

19.14 Digital I/O Configuration

By clicking on the “Digital I/O Configuration” link, in the “Digital I/O” menu, you come to the page described in the following sub-paragraphs²³; the page differs between Z-PASS1-IO and Z-PASS2-IO:

19.14.1.1 Z-PASS2-IO

In this page, you can configure the operating modes of the Digital I/Os and the security level applied by the “Remote Connection Disable” feature (see chapter 16).

Field	Meaning	Default value
Input 1 Mode	This parameter represents the	Remote connection disable

²³ This page is available only for Z-PASS1-IO and Z-PASS2-IO products.

	operating mode of the Digital Input 1 (DI 1). Since this is the digital input used for “Remote Connection Disable” feature, its value (“Remote connection disable”) cannot be changed.	
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 connection, 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”.	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”²⁴.	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: “VPN Connection” “VPN Service” “Internet Connection” “SMS	VPN Connection

²⁴ “Remote toggle” function is still to be defined.

	Service". See chapter 16, 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.

From this page, you can also change the status of the digital outputs working as “General Output”; the procedure is the following:

- when you move the mouse over one of the rectangles containing the digital I/O label (in the following figure, “DO 2”), the rectangle becomes red:

The screenshot shows the SENECA Z-PASS2 web interface. The top navigation bar includes links for General Configuration, Main View, Network and Services, Serial Ports, Gateway Configuration, Real Time Clock Setup, VPN Configuration, Router Configuration, Users Configuration, FW Upgrade, Conf. Management, Shared Memory Tag Conf., Tag Setup, Tag View, Mobile Configuration, Mobile Network, DDNS Configuration, Digital I/O, Digital I/O Configuration (highlighted), Diagnostics, FW Versions, and Ethernet Interfaces.

The main configuration area displays the following settings:

- Z-PASS2**
- Digital I/O Configuration** [user: admin] [logout]
- Firmware Version:** SW003900_224 [Modem: UC20GQBR03A14E1G]
- MAC Address:** C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
- Internet Access:** Mobile
- Modbus Shared Memory Gateway:** running
- Router:** running

The **Digital I/O Configuration** section contains a table with the following columns: CURRENT and UPDATED.

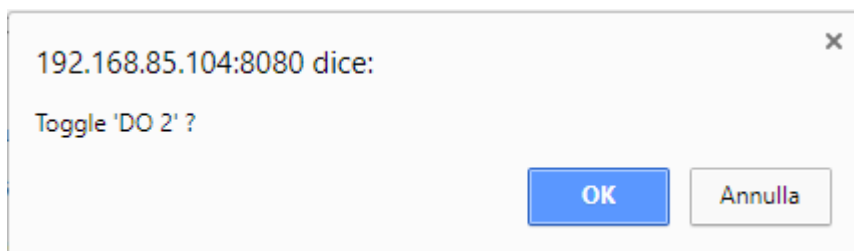
	CURRENT	UPDATED
Input 1 Mode	Remote connection disable	Remote connection disable ▼
Output 1 Mode	Remote connection active	Remote connection active ▼
Input 2 Mode	General input	General input ▼
Output 2 Mode	General output	General output ▼
Input/Output 1 Mode	General input	General input ▼
Input/Output 2 Mode	General output	General output ▼
Service Disable	VPN Connection	VPN Connection ▼

Below the configuration table is an **APPLY** button.

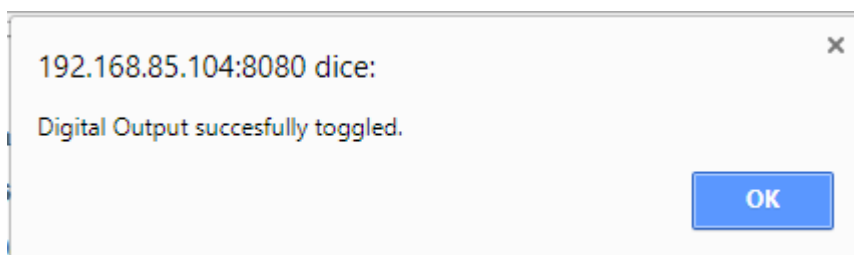
The **Digital I/O Status** section displays the current status of the digital I/Os:

DI 1	DO 1	DI 2	DO 2	DDO 1	DDO 2
LOW	LOW	LOW	LOW	LOW	LOW

- when you click on the rectangle (only when I/O mode is “General Output”), a confirm pop-up is shown:



- if you click on “Cancel” button, no action is performed; if you click on “OK” button, the digital output status is toggled and a new pop-up is shown:



Please note that the above procedure applies also to Z-PASS1-IO.

The status of the digital input configured as “Local Alarm” is reported in the “ALARM” column in the “Devices” tab of the “Seneca VPN Box Manager” and “Seneca VPN Client Communicator” applications.

VPN Box Manager - 3.2.0.8

VPN BOX SingleLan (tlc.seneca.it)
Single Lan, Utente Connesso SUPERVISOR

Status Dispositivi SENECA Accessi VPN

7 Dispositivo/i, 2 nuovi, 0 in aggiornamento, 5 configurati, 0 in allarme

	TAG	MAC	IMEI	STATUS	ALARM	SIGNAL	UPTIME	
	zpass1_C8F981160066	C8:F9:81:16:00:66	MODEM NON INSTALLA...	SERVICE OFF - VPN DO...	●	-	-	Reset
	ELTECO	C8:F9:81:18:00:06	861075026509463	SERVICE OFF - VPN DO...	●	-	-	Reset
	GREEN_METHANE2	C8:F9:81:02:01:D6	862264020120993	SERVICE ON - VPN UP	●	6/7	Last 06/10/2017 11.43.5...	Reset
	Demo	C8:F9:81:16:00:9E	862264020393319	SERVICE OFF - VPN DO...	●	-	-	Reset
	zpass2s_C8F981160017	C8:F9:81:16:00:17	862264020382288	SERVICE OFF - VPN DO...	●	-	-	Reset
	ZEUS001	C8:F9:81:15:00:94	MODEM NON INSTALLA...	SERVICE OFF - VPN DO...	●	-	-	Reset
	TOPCO	C8:F9:81:11:00:6D	862264020400825	SERVICE OFF - VPN DO...	●	-	-	Reset

Configurazione CONFIGURED, ultimo refresh 27/09/2017 14.17.08

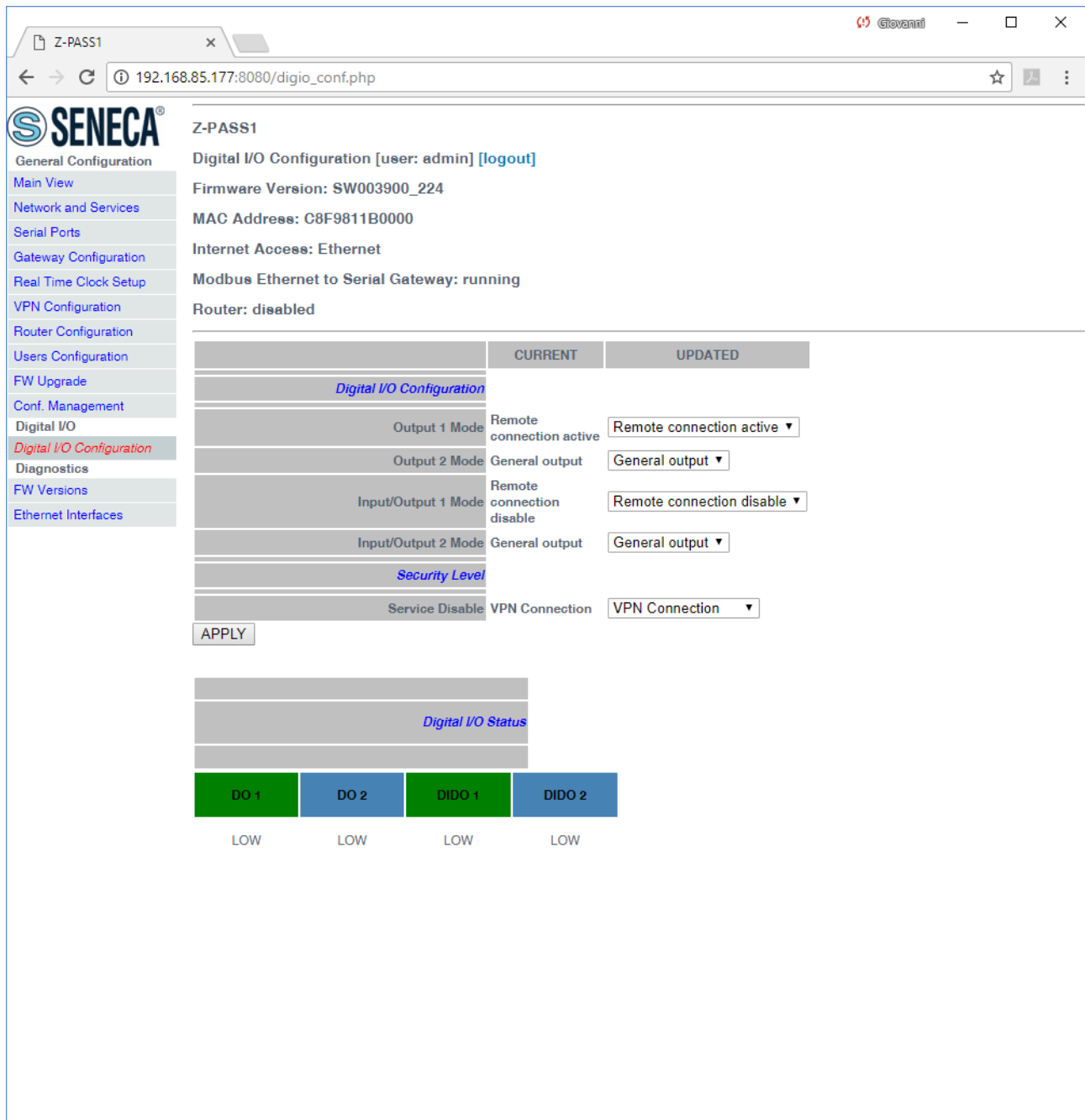
Connessione Network 192.168.96.0/255.255.255.0 (VPN 10.9.1.133)

Versione ver. SW002940_331, hw Z-PASS1-R02, mode LAN/WAN

DI1 NA OFF DIO1 CONNECTION DISAE
ON DO1 VPN STATUS OFF DIO2 INPUT
DI2 NA
OFF DO2 OUTPUT

Configura
Elimina

19.14.1.2 Z-PASS1-IO



SENECA®

General Configuration

Main View

Network and Services

Serial Ports

Gateway Configuration

Real Time Clock Setup

VPN Configuration

Router Configuration

Users Configuration

FW Upgrade

Conf. Management

Digital I/O

Digital I/O Configuration

Diagnostics

FW Versions

Ethernet Interfaces

Z-PASS1

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

Firmware Version: SW003900_224

MAC Address: C8F9811B0000

Internet Access: Ethernet

Modbus Ethernet to Serial Gateway: running

Router: disabled

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

APPLY

Digital I/O Status

DO 1	DO 2	DIDO 1	DIDO 2
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 Connection Disable” feature (see chapter 16).

Field	Meaning	Default value
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 connection, its value (“Remote connection active”)	Remote connection active

	cannot be changed.	
Output 2 Mode	This parameter represents the operating mode of the Digital Output 2 (DO 2). Possible modes are: “General output” “Remote toggle” ²⁵ .	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). Since this is used as an input for “Remote Connection Disable” feature, its value (“Remote connection disable”) cannot be changed.	Remote connection disable
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” “Local alarm”.	General output
Service Disable	This parameter determines which access services are disabled when “Remote Connection Disable” digital input is HIGH. Possible values are: “VPN Connection” “VPN Service” “Internet Connection” “SMS Service”. See chapter 16, for a detailed description of these values.	VPN Connection

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

19.15 SMS Configuration

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

²⁵ “Remote toggle” function is still to be defined.

Z-PASS2
SMS Configuration [user: admin] [logout]

Firmware Version: SW003900_226 [Modem: UC20GQBR03A14E1G]
 MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237893]
 Internet Access: Ethernet
 Gateway: running
 Router: disabled

	CURRENT	UPDATED
SMS Configuration		
SMS Commands Enable	ON	ON ▼
SMS Acknowledge	ON	ON ▼
SMS Relay to Admin	ON	ON ▼
Startup SMS	OFF	OFF ▼
SMS Send Attempts	1	1
Send Delay Between Attempts (s)	10	10
Service Centre		

APPLY

In this page, you can set the parameters related to the “SMS Commands” functionality (see chapter 18), as listed in the following table:

Field	Meaning	Default value
SMS Commands Enable	Flag to enable/disable the SMS commands functionality	ON
SMS Acknowledge	Flag to enable/disable the sending of a response (“acknowledge”) to “set” commands (while “get” commands always have a response) (see chapter 18)	ON
SMS Relay To Admin	Flag to enable/disable the relaying	ON

	of rejected or unrecognized commands to the “admin” user	
Startup SMS	Flag to enable/disable the sending of a “startup” message to the “admin” user	OFF
SMS Send Attempts	Number of attempts to send an SMS	1
Send Delay Between Attempts (s)	Delay, in seconds, between attempts to send an SMS	10
Service Centre	SMS Service Centre (SMS-SC) number Typically, this parameter can be left empty, since SMS-SC number is already configured on the SIM	empty

The “Startup SMS”, controlled by the corresponding parameter, has the following format:

```
Z-PASS2<hwrev> '<vpnbox tag name>' (IMEI:<modem IMEI>) STARTED
```

as in the following example:

```
Z-PASS2-IO 'zpass' (IMEI:861108030033046) STARTED
```

19.16 Phonebook

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

Z-PASS2
 Phonebook [user: admin] [logout]
 Firmware Version: SW003900_226 [Modem: UC20GQBR03A14E1G]
 MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237893]
 Internet Access: Ethernet
 Gateway: running
 Router: disabled

IMPORT FROM CSV Scegli file Nessun file selezionato EXPORT TO CSV

ADD MODIFY DELETE

#	User Type	Group	Phone Number	Email Address
1	admin	0	+390123456789	admin@seneca.it
2	manager	0	+391234567890	mgr@seneca.it
3	user	0	+399876543210	

In this page, the list of the Phonebook “users” is shown.

By clicking on the “ADD” button, a new user can be inserted into the Phonebook, as in the following figure.

The screenshot shows the Z-PASS2 web interface. The browser address bar displays '192.168.85.104:8080/phonebook_mod.php?id=0'. The page title is 'Z-PASS2'. The top status bar shows 'Phonebook [user: admin] [logout]'. The main configuration area displays the following information:

- Firmware Version: SW003900_226 [Modem: UC20GQBR03A14E1G]
- MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237893]
- Internet Access: Ethernet
- Gateway: running
- Router: disabled

Below this information is a table for Phonebook Users:

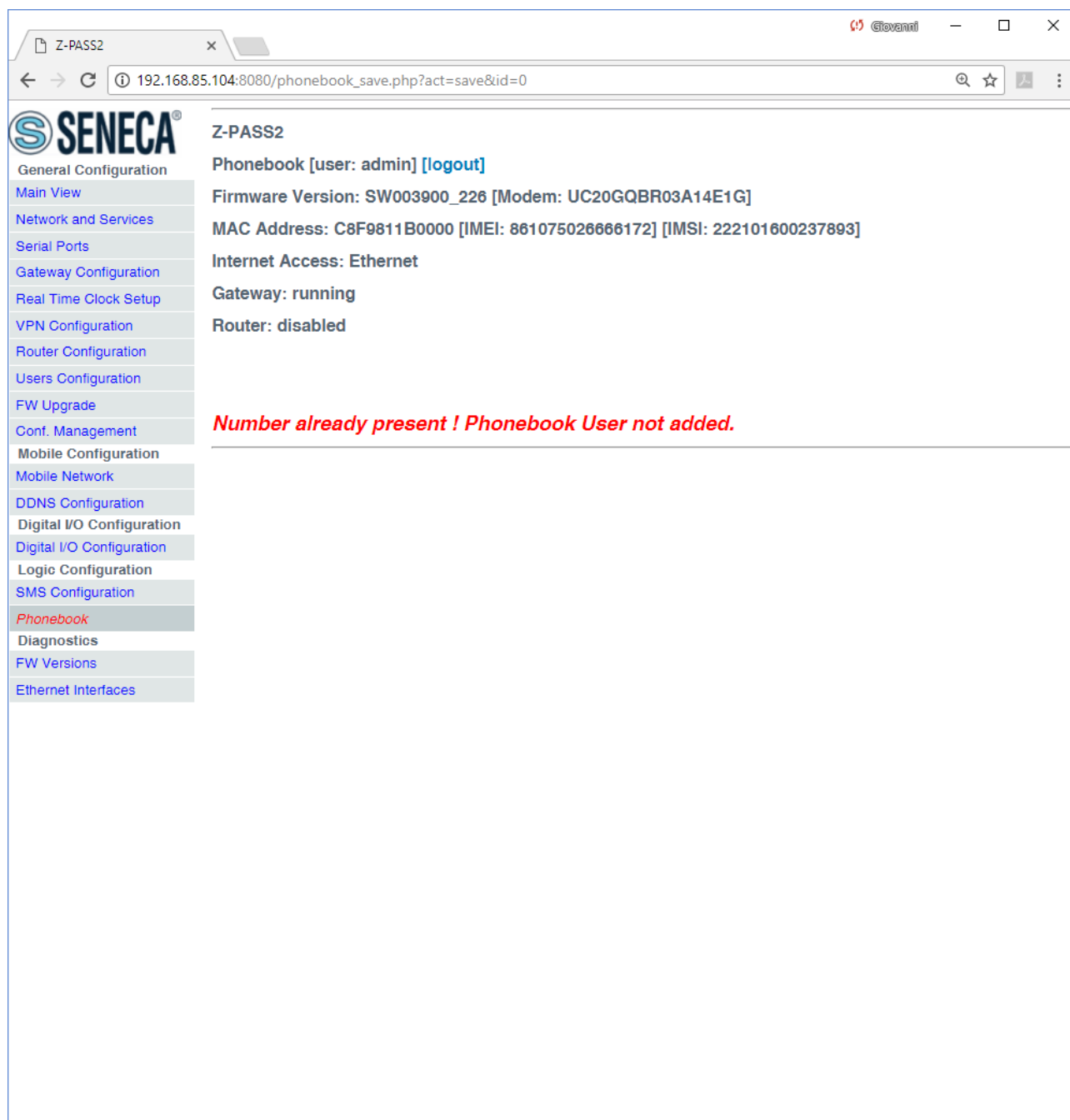
	CURRENT	UPDATED
Phonebook User		
User Type	user	user
User Group (*)	0	0
Phone Number		
Email Address (*)		
NOTE: fields marked with * will be used in a future release.		
APPLY		

The following table explains the meaning of the parameters related to a Phonebook user.

Field	Meaning	Default value
User Type	Possible user types: - “admin”: this is the user with receives all the rejected or unrecognized SMS commands, if the “SMS Relay to Admin” parameter is set to ON and the “Startup SMS” messages, if the “Startup SMS” parameter is set to ON; this user can send SMS commands to the device	ON

	- “manager”: this user can send SMS commands to the device - “user”: currently, this type of user does not have any role (to be developed in a future FW release)	
User Group	Currently this parameter has no use (to be developed in a future FW release)	0
Phone Number	Phone Number in “international format”; the initial ‘+’ character shall be present	Empty
Email Address	Currently this parameter has no use (to be developed in a future FW release)	Empty

Two users with the same phone number cannot be present in the Phonebook; so, when trying to add a new user with an already existing phone number, the following error is given.



It is possible to insert more than one “admin” user into the Phonebook; just note that only the most recently inserted “admin” user will receive “relayed” SMS commands and “Startup SMS” messages.

Conversely, if no “admin” user is present in the Phonebook, rejected and unrecognized SMS commands won’t be relayed and “Startup SMS” messages won’t be sent, even if the corresponding enable parameters are set to ON.

Selecting a user in the list and clicking on the “MODIFY” button, you can modify the user’s parameters, as in the following figures.

Z-PASS2

Phonebook [user: admin] [logout]

Firmware Version: SW003900_226 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237893]

Internet Access: Ethernet

Gateway: running

Router: disabled

IMPORT FROM CSV Scegli file Nessun file selezionato EXPORT TO CSV

ADD MODIFY DELETE

#	User Type	Group	Phone Number	Email Address
1	admin	0	+390123456789	admin@seneca.it
2	manager	0	+391234567890	mgr@seneca.it
3	user	0	+399876543210	

Z-PASS2

Phonebook [user: admin] [logout]

Firmware Version: SW003900_226 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026666172] [IMSI: 222101600237893]

Internet Access: Ethernet

Gateway: running

Router: disabled

	CURRENT	UPDATED
Phonebook User		
User Type	manager	manager
User Group (*)	0	0
Phone Number	+391234567890	+391234567890
Email Address (*)	mgr@seneca.it	mgr@seneca.it

NOTE: fields marked with * will be used in a future release.

Selecting a user in the list and clicking on the “DELETE” button, you can remove a user from the Phonebook.

Finally, the “EXPORT TO CSV” and “IMPORT FROM CVS” buttons let you export/import the Phonebook to/from a “.csv” file (the separator character is “;”).

Please note that, when importing the Phonebook from a .csv file, the previous Phonebook contents are deleted; so, a fast way to “clean” the Phonebook, if it contains many users, is to import an empty .csv file.

19.17 FW Versions

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

The screenshot shows the Z-PASS2 web interface. The browser address bar indicates the URL is 192.168.85.104:8080/fwver_full.php. The page title is Z-PASS2. The left sidebar contains a menu with options like General Configuration, Main View, Network and Services, Serial Ports, Gateway Configuration, Real Time Clock Setup, VPN Configuration, Router Configuration, Users Configuration, FW Upgrade, Conf. Management, Shared Memory Tag Conf., Tag Setup, Tag View, Mobile Configuration, Mobile Network, DDNS Configuration, Digital I/O, Digital I/O Configuration, Diagnostics, FW Versions (highlighted), and Ethernet Interfaces.

The main content area displays the following information:

- Z-PASS2**
- FW Versions** [user: admin] [logout]
- Firmware Version:** SW003900_224 [Modem: UC20GQBR03A14E1G]
- MAC Address:** C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
- Internet Access:** Mobile
- Modbus Shared Memory Gateway:** running
- Router:** running

Below this information is a table titled **FW Components Versions**:

HW Version	
HW Revision	Z-PASS2-IO
FW Components Versions	
Linux Kernel	2.6.28 #137 PREEMPT Tue Jun 20 10:46:10 CEST 2017
Initial RAM Disk	Jun 1 13:55:29 2017
Root File System	227_20171201
Default Disk File System	SW003900_224
Disk File System	SW003900_224

In this page, the following information are shown:

- the product name along with its HW revision (in the above figure: “Z-PASS2-R01”)
- the version strings of all the FW components, which are:
 - o Linux Kernel (*kernel*)
 - o Initial RAM Disk (*initrd*)
 - o Root File System (*rootfs*)
 - o Default Disk File System (*diskdfl*)
 - o Disk File System (*disk*)

19.18 Ethernet Interfaces

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

The screenshot shows the Z-PASS2 web interface. The browser address bar indicates the URL is 192.168.85.104:8080/eth_stats.php. The page title is Z-PASS2. The left sidebar contains a menu with options like General Configuration, Main View, Network and Services, Serial Ports, Gateway Configuration, Real Time Clock Setup, VPN Configuration, Router Configuration, Users Configuration, FW Upgrade, Conf. Management, Shared Memory Tag Conf., Tag Setup, Tag View, Mobile Configuration, Mobile Network, DDNS Configuration, Digital I/O, Digital I/O Configuration, Diagnostics, FW Versions, and Ethernet Interfaces. The main content area shows the Ethernet Status for user admin. It includes fields for Ethernet Status, Firmware Version (SW003900_224), MAC Address (C8F9811B0000), Internet Access (Mobile), Modbus Shared Memory Gateway (running), and Router (running). Below this, there are two sections for LAN and WAN Ethernet. The LAN section shows Link Status as Down, RX Packets / Bytes as 0 / 0, and TX Packets / Bytes as 0 / 0. The WAN section shows Link Status as Up, RX Packets / Bytes as 195612 / 16.6M, and TX Packets / Bytes as 14664 / 2.6M. A REFRESH button is located below the WAN section.

LAN ETHERNET	
Link Status	Down
RX Packets / Bytes	0 / 0
TX Packets / Bytes	0 / 0

WAN ETHERNET	
Link Status	Up
RX Packets / Bytes	195612 / 16.6M
TX Packets / Bytes	14664 / 2.6M

REFRESH

The above figure applies to a Z-PASS2-R01/Z-PASS2-IO, when the “Ethernet Mode” is “LAN/WAN”; a similar page also applies to a Z-PASS1-R01/Z-PASS1-IO.

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-PASS1, Z-PASS2 and for Z-PASS1-R01/Z-PASS1-IO, Z-PASS2-R01/Z-PASS2-IO when the “Ethernet Mode” is “Switch”, the “Ethernet Interfaces” page is similar to the one shown in the following figure.

The screenshot shows a web browser window with the URL `192.168.85.104:8080/eth_stats.php`. The page title is "Z-PASS2". On the left, there is a navigation menu with the "SENECA" logo and various configuration options. The main content area shows the "Ethernet Status" page, which includes the following information:

- Ethernet Status** [user: admin] [logout]
- Firmware Version:** SW003900_224 [Modem: UC20GQBR03A14E1G]
- MAC Address:** C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]
- Internet Access:** Mobile
- Modbus Shared Memory Gateway:** running
- Router:** running

Below this information, there is a table showing network statistics for the Ethernet interface:

ETHERNET	
RX Packets / Bytes	60470 / 4.6M
TX Packets / Bytes	1086 / 227.2K

A "REFRESH" button is located below the table.

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.

19.19 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” page, 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.



Note that, as told above, the “FACTORY DEFAULT” and “RESTART” buttons are disabled.

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

Z-PASS2

Mobile Network [user: guest] [logout]

Firmware Version: SW003900_224 [Modem: UC20GQBR03A14E1G]

MAC Address: C8F9811B0000 [IMEI: 861075026500975] [IMSI: 222101600237890]

Internet Access: Mobile

Modbus Shared Memory Gateway: running

Router: running

	CURRENT	UPDATED
SIM		
PIN (if required by SIM)	8342	8342
Operator Selection		
Mode	Automatic	Automatic
Operator	[22210] vodafone IT (GSM)	Operator list not available
Data Connection		
Enable	ON	ON
APN Mode	Manual	Manual
APN	m2mbis.vodafone.it	m2mbis.vodafone.it
Authentication Type	None	None
Username	user	user
Password	pass	pass
Ping Connection Testing IP Address (if empty, testing is disabled)	www.google.com	www.google.com

Mobile Status	
SIM/PIN Status	PIN required
PIN Remaining Attempts	3
Signal Level [0..7]	6
Selected Operator	"vodafone IT" (UMTS)
Registration Status	Registered (home network)
Connection Status	Connected
IP Address	91.80.15.232
RX Packets / Bytes	738 / 57.9K
TX Packets / Bytes	698 / 51.1K
GPS Location	45.37421,11.94561 [Map]

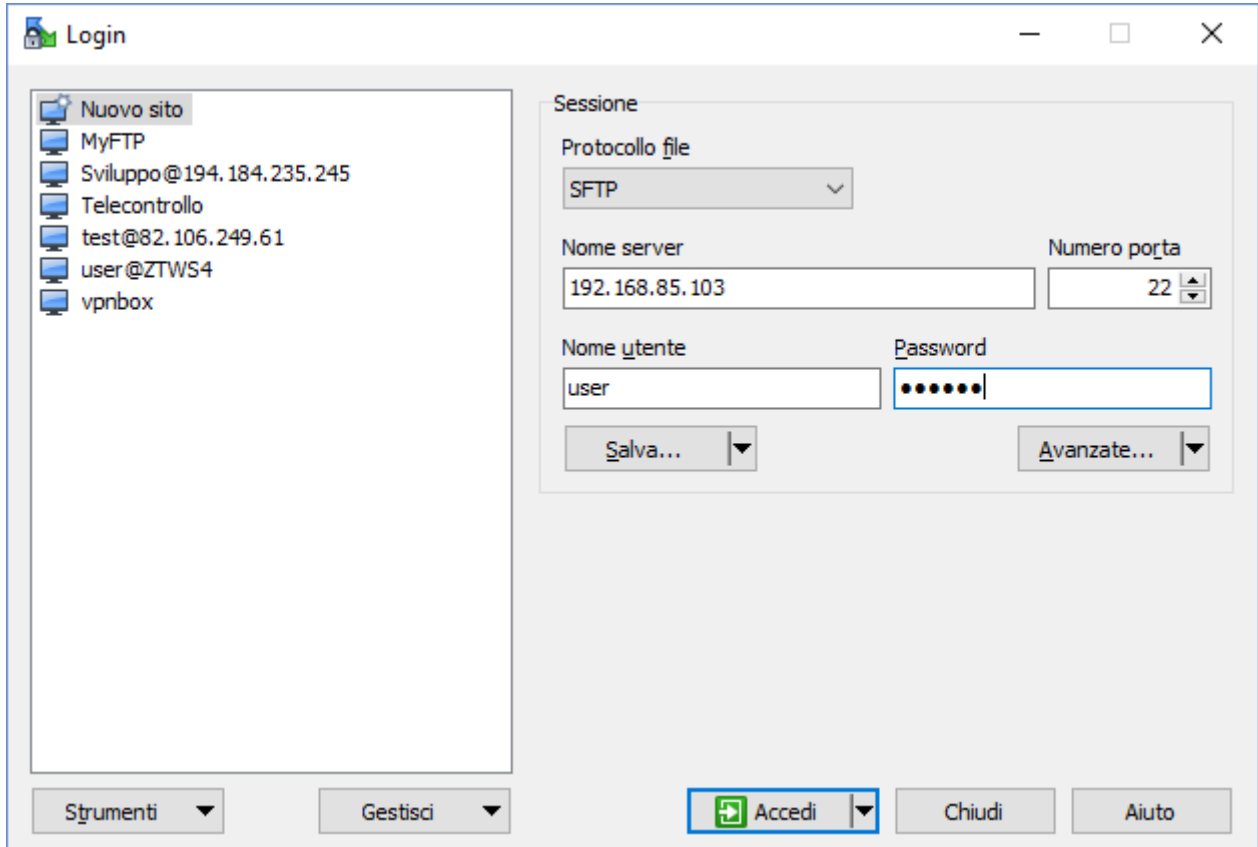
In the “Mobile Network” page, the “APPLY” and “GET OPERATOR LIST” buttons are disabled, whereas the “SHOW MOBILE STATUS”/“HIDE MOBILE STATUS” and “REFRESH” buttons are enabled, letting the “guest” user view the Mobile Status.

20 FTP/SFTP access

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

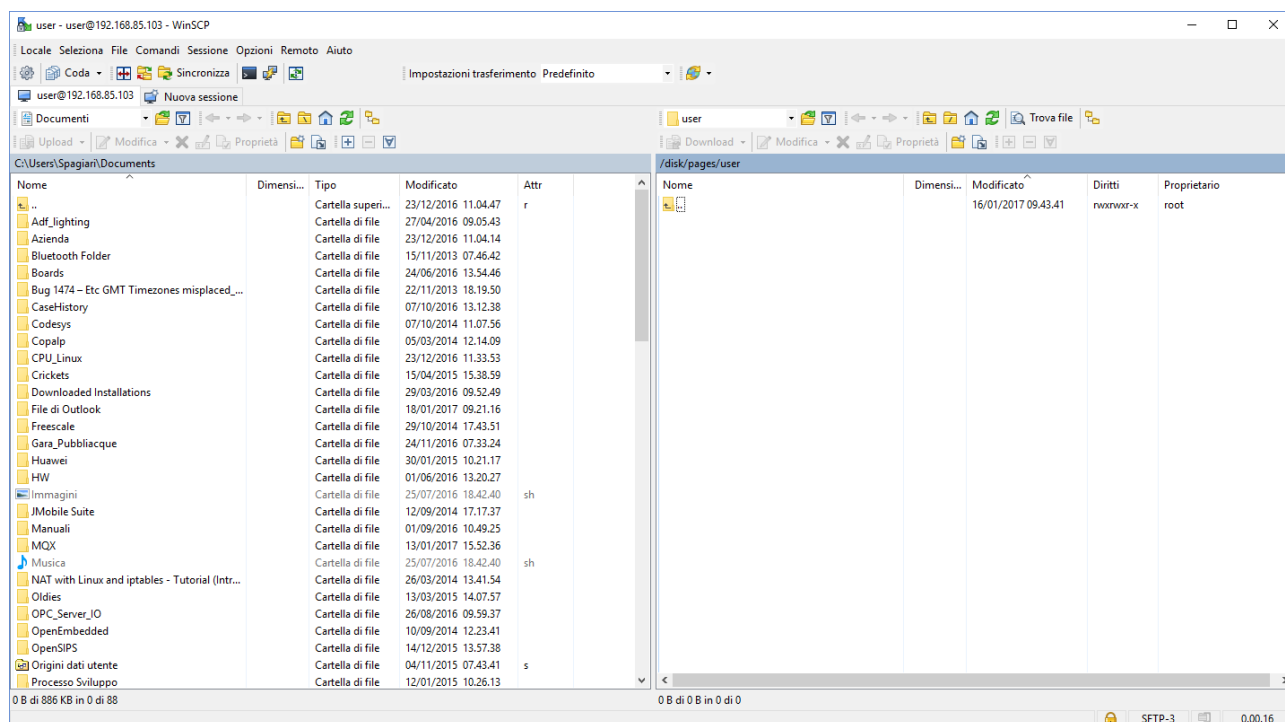
<http://winscp.net/eng/download.php>

You must set the connection as in the following figure (the screenshot shows a connection to the 192.168.85.103 IP address):



The credentials (username and password) are those (“user”, “123456”) set for the “FTP USER” (see “Users Configuration” web page in paragraph 0).

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.



The WinSCP program can be used both as an FTP or SFTP client to transfer files to/from the Z-PASS; 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.

21 Glossary

Bridge: a device that translates from one communications protocol into another.

Gateway: a device that acts as a portal between two programs allowing them to share information by communicating between different protocols.

Serial Device Server: a device that enables devices with an RS-232, RS-422 or RS-485 serial interface to connect to a local area network (LAN) or, more generally, an IP network.

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.

Tunnel Point-to-Point: an IP tunnel between a single Master device and a single Slave device.

Tunnel Point-to-Multipoint: an IP tunnel between a single Master device and multiple Slave devices.