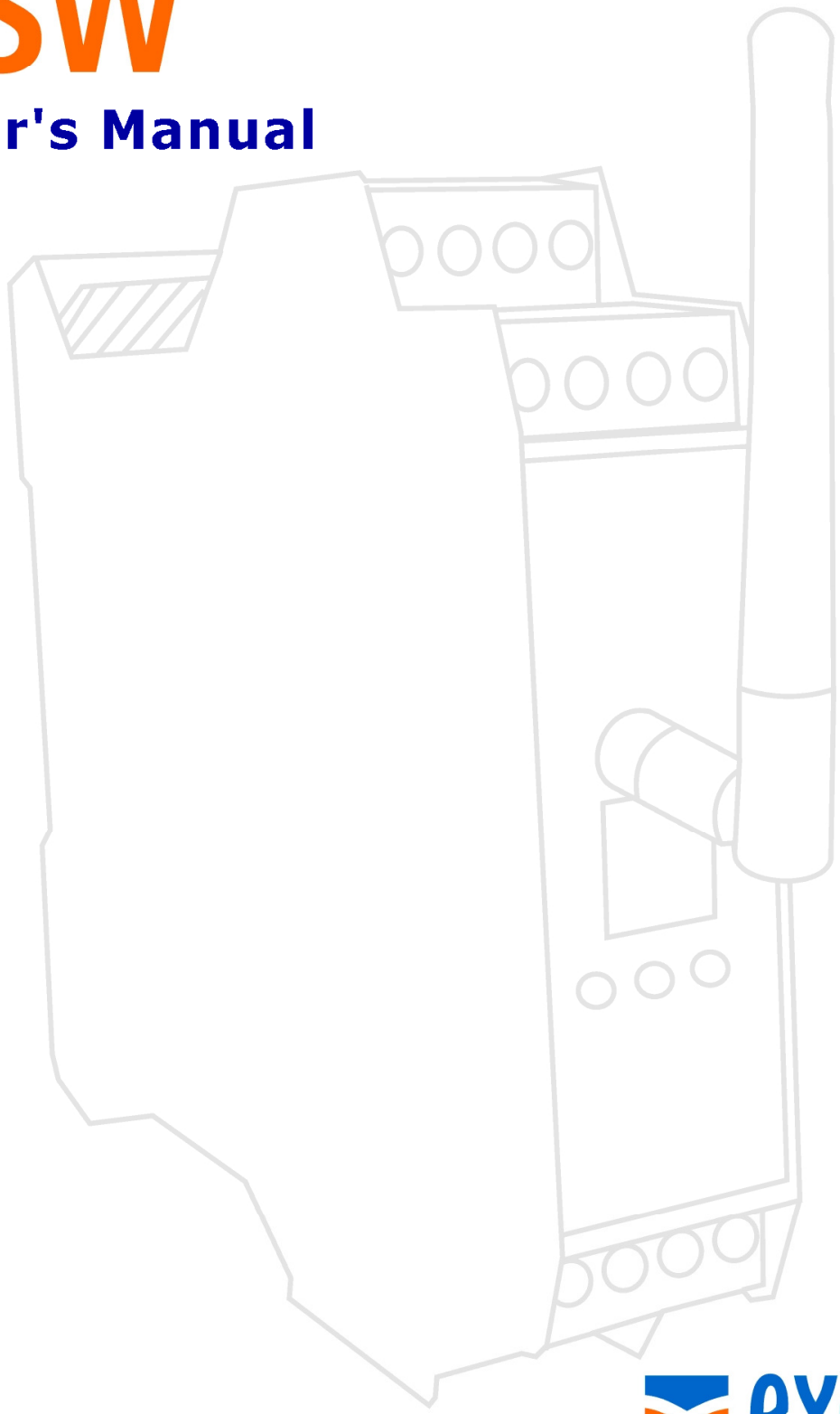
WI-FI SERIAL SERVER

SSW

User's Manual



exemys

www.exemys.com

SISTEMA DE GESTIÓN ISO 9001:2000

Exemys products are in permanent evolution to satisfy the needs of our clients. For this reason specifications and capacities are subject to change without previous notice.
Please find updated information at www.exemys.com

Rev. 1.0.0 – March 2009

Table of Contents

1. INTRODUCTION

1.1. About this manual

1.1.1. Purpose of this manual

The purpose of this manual is to provide the instructions to install, configure and operate the SSW in a simple and rapid manner.
The manual begins with a general description of the product followed by instructions for the correct installation of the hardware. Later, the configuration and operation are detailed.
To take advantage of the contents of this manual it is necessary to have sufficient knowledge about the Wi-Fi operation. If you do not have this knowledge, we recommend to first read Appendices C and D, which will give you a brief introduction to Wi-Fi.

1.1.2. Conventions, terms and abbreviations

Table 1 - Abbreviations

Abbreviation	Description
HTTP	HyperText Transfer Protocol
HTML	HyperText Markup Language
PC	Personal Computer
LAN	Local Area Network
MAC	Media Access Control
RTS	Request To Send
CTS	Clear To Send
IP	Internet Protocol
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
SNMP	Simple Network Management Protocol
MIB	Management Information Base
NMS	Network Management System
SSID	Service Set Identifier
WI-FI	Wireless Fidelity
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
AES	Advanced Encryption Standard
PSK	Pre-Shared Key
RC4	Rivest Cipher 4
MSDU	Mac Service Data Unit
BSS	Basic Service Set
IBSS	Independent Basic Service Set
ESS	Extended Service Set
STA	Wireless Station
DSS	Distribution System services
SS	Station Services
TKIP	Temporal Key Integrity Protocol
AP	Access Point
ISM	Industrial, Scientific, and Medical
GND	Ground (Voltage reference)

The following conventions are used in this manual:

Table 2 - Conventions

Convention	Description
n...m	A range of possible values. Any value can be selected within this range, including n and m.
<zz>	Indicates an ASCII character.
(text)	Any text, such as a server address.
aaa.bbb.ccc.ddd	An IP address.
<x – y>	Identifies a range of values between an initial value "x" and end value "y".

1.2. Why choose a Wi-Fi solution?

What are the benefits of a Wi-Fi network over the traditional wired network? What are the advantages regarding an application of an embedded system?
In principle the great advantage is the flexibility provided by a wireless network to an embedded application. It provides more options for monitoring, control and dissemination of information. It allows monitoring information in remote places at a low cost, where access is difficult through other means.
The following list summarizes some of the benefits of a Wi-Fi network:

- **Wireless Ethernet.** Wi-Fi is the replacement of Ethernet. Wi-Fi and Ethernet, both IEEE 802 networks, share the same elements of the protocol core.
- **Extended access.** The absence of cables extends access to locations where cables do not reach or is very expensive to do it.
- **Cost reduction.** As it was mentioned above, the absence of cables results in an important cost reduction. This is also accompanied by other factors like the low cost of wireless routers.
- **Mobility.** A wired connection restricts you physically to a particular place. A wireless connection gives us freedom to change places without losing the connection.
- **Flexibility.** Extended access, cost reduction and mobility, create opportunities for new applications also allowing new creative Solutions for old applications.

1.3. General Description of the Product

The SSW is a RS-232/485/422 to Wi-Fi (802.11b) converter and vice versa. This equipment adds network connectivity to serial devices that were not originally designed to work in networks. It allows access, through Wi-Fi (802.11b), to equipment such as alarm panels, data acquisition devices, PLC or any device with a serial interface.
The SSW extends serial communications distances without changing the interconnected equipment. This is a simple and easy way to incorporate the advantages of control and remote management of serial equipment not connected to the network. Using SSW, your equipments can be controlled, managed and monitored through the Internet. Additionally, SSW supports secure data communications, so it can be used in services requiring security.
The number of digital inputs/outputs and the number and type of serial ports provided by the SSW, depend on each particular model.

Model	Serial Port				I / O	
	COM A		COM B		Inputs	Outputs
	Type	Control	Type	Control		
SSW-1C0-42	RS232	RTS/CTS	-	-	4	2
	RS485	-	-	-		
	RS422	-	-	-		
SSW-200-42	RS232	RTS/CTS	RS232	RTS/CTS	4	2

Table 3 - Detail of I/O and Serial ports available for different models

The SSW is a complete solution for Wi-Fi (802.11b) connectivity of different types of devices, either through (RS-232/485/422) serial ports or through its digital inputs/outputs.

A typical connection example of SSW equipment within a Wi-Fi network is shown below, which gives network capacities to serial interface equipment that do not have them.

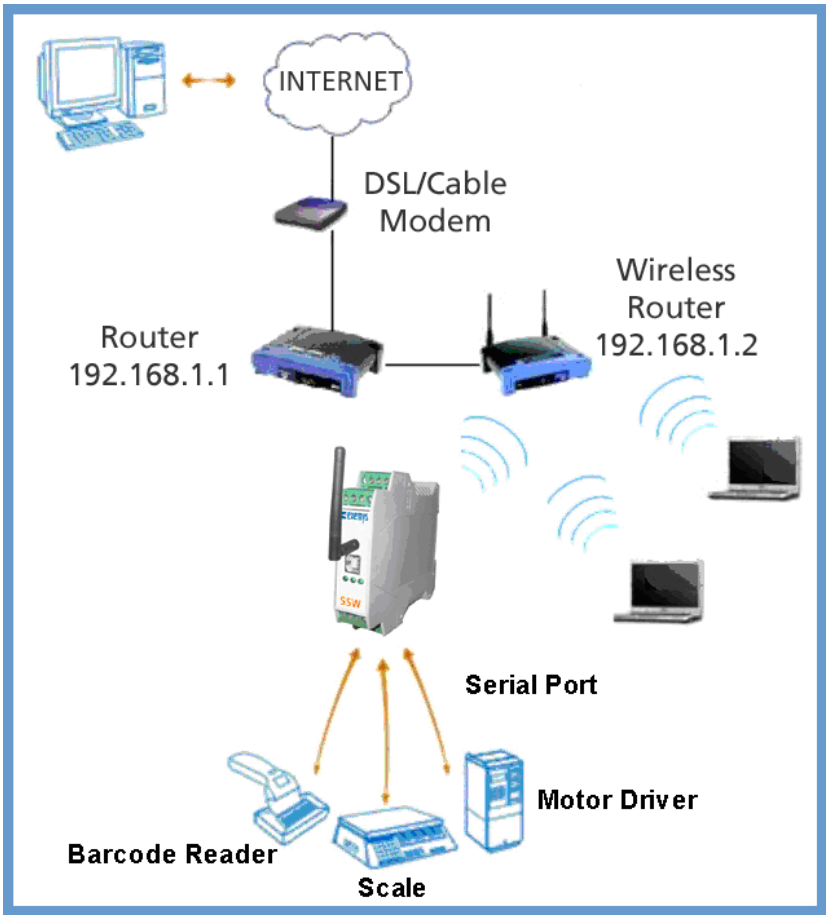


Figure 1 – Application example

2. INSTALLATION

2.1. Power Supply connection

The following figure shows the power supply input connection in terminals marked VIN(+) y GND(-). The SSW power supply has polarity and accepts the 10 to 30Vdc range.

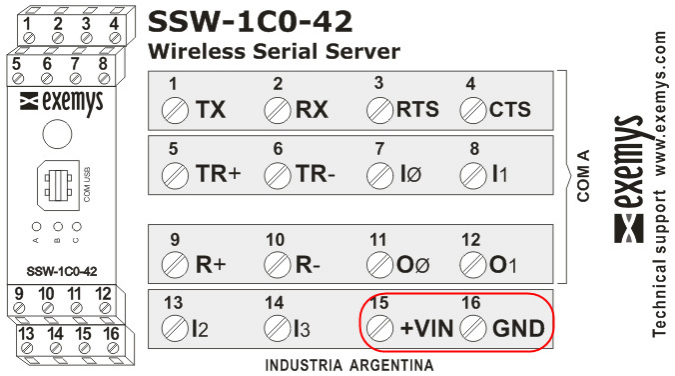


Figure 2 – Power supply connection

2.2. USB Port connection (only for configuration)

The SSW has a USB configuration port, which type B female USB connector is detailed in the figure.
This way, through a console, all the network parameters of the equipment con be configured, and the status of the Wi-Fi- Network can be checked. .
The USB Port configuration is available in all SSW models.

A USB cable can be used for configuration as shown in the figure.

Figure 3 –USB connection cable for the configuration console

2.3. LED Indicators

The SSW has three LEDs

- The POWER LED indicates that the equipment is ON.
- The LINK LED indicates connection and Wi-Fi activity.
- The COM LED indicates the status of Communications ports of the equipment.

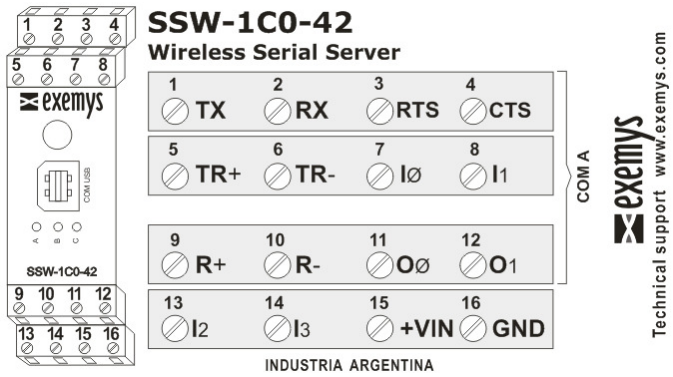
LEDs		Description
POWER	Continuously ON	The SSW is powered up.
LINK	Fast blinking	The SSW is trying to link with the Wi-Fi Access Point.
	Continuously ON	The SSW is effectively linked with the Wi-Fi Access Point.
COM	Continuously ON	A "connection" has been established (TCP or Virtual UDP) through some of the COM.
	Blinking	Data are being transmitted through one of the established connections.

2.4. Serial Ports connection

2.4.1. Serial Port connection in Model SSW-1C0-42

The SSW-1C0-42 has one serial port, that can be configured via WEB, to work in RS-232 (with or without flow control by hardware), RS-485 or RS-422.

Table 4 –SSW-1C0-42 Terminal board

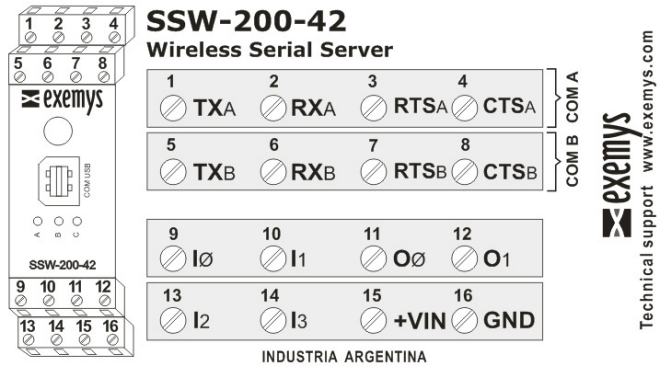


IMPORTANT NOTE:
This model has only one physical serial port and a connection to more than one Serial Port to the SSW simultaneously should not be attempted.

2.4.2. Serial Port connection in Model SSW-200-42

The SSW-200-42 has two RS-232 serial ports that can work with or without flow control by hardware (configurable through the Web).

Table 5 –Model SSW-200-42 terminal board



2.4.3. RS-485 and RS-422 connection

As you can see, the COMs in some models can be of the RS-485 or RS-422 type. The following figure shows how to connect a SSW-1C0-42 to a RS-485 network and to an RS-422 network.

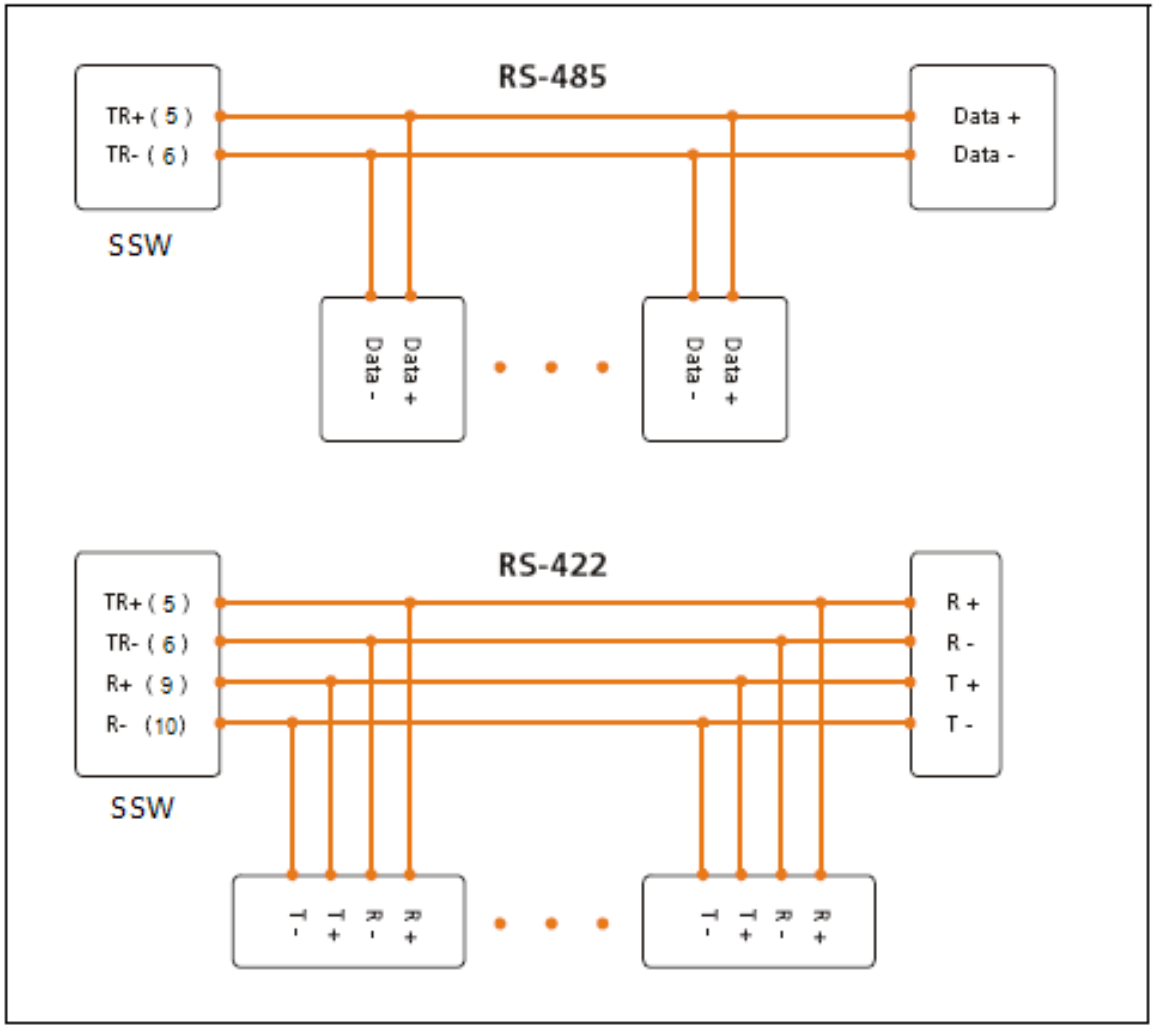


Figure 4- RS-485 / RS-422

2.5. Digital Inputs/Outputs

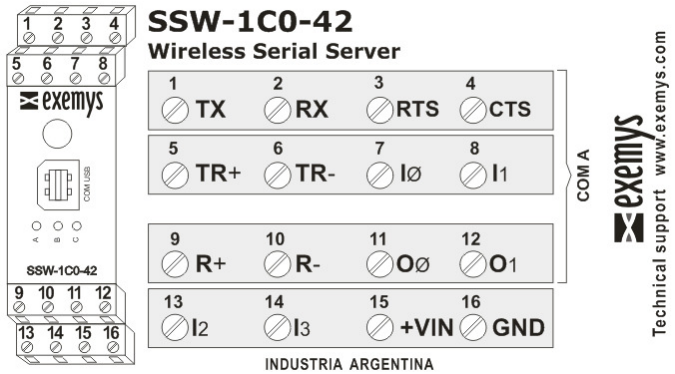
The number of inputs / outputs provided by the SSW are indicated in the last two digits of the product code. This can be observed in the following table:

Model	Inputs	Outputs
SSW-1C0-42	4	2
SSW-200-42	4	2

Table 6 – Inputs/Outputs for the different SSW models

The following figure shows the location of the inputs/outputs for all SSW models.
The inputs/outputs are numbered starting at 0. Consequently the first input will be I0 and the first output O0.

Model SSW-1C0-42



Model SSW-200-42

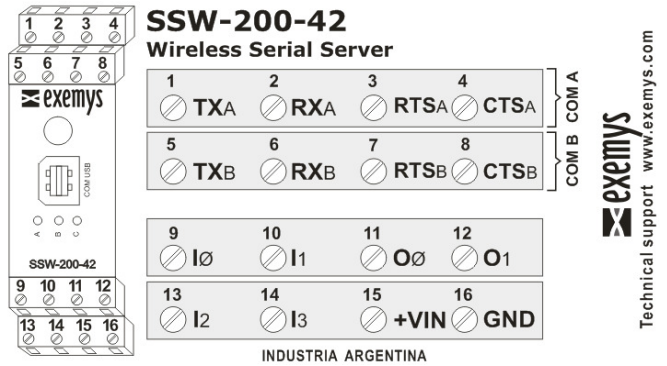


Figure 5 – View of the connection terminal boards for the different SSW models

Table 7 – Technical characteristics of inputs/outputs

Parameter	Minimum	Maximum	Unit
Output voltage	3	45	Vdc
Output current	--	50	mA
Voltage at input, Activated	3,5	28	Vdc
Voltage at input, Deactivated		1,5	Vdc
Impedance at input	2		Kohm

2.5.1. Digital input connection

To activate digital inputs an external continuous voltage must be applied. This voltage source has to share the GND terminal with the SSW power supply. If necessary, the same power supply used to power the SSW could be used. It is a sinking type input. It accepts sensors or PNP type sourcing devices.

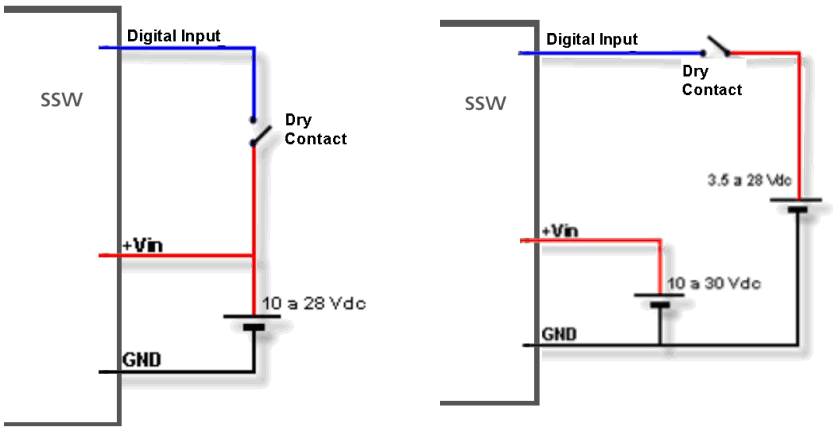


Figure 6 – Digital input with single and double power supply

2.5.2. Digital outputs connection

The digital outputs are of the "open collector" type. The load to be connected must be fed with an external power supply and it has to share the GND terminal with the SSW power supply. If necessary the same power supply to feed the equipment can be used. The output type is NPN Sinking (Open collector).

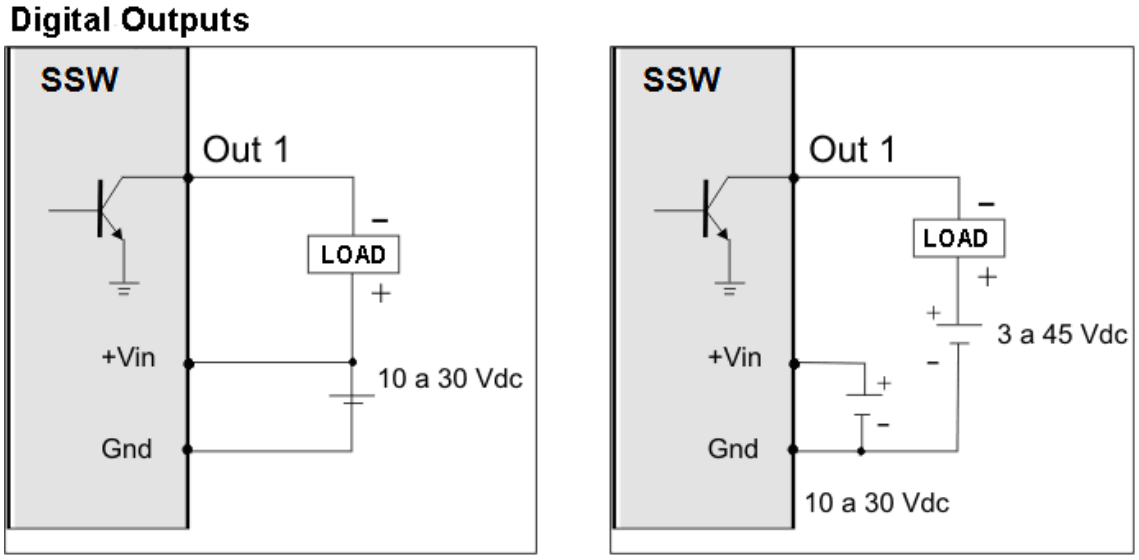


Figure 7 – Digital output connected with single and double power supply.

3. CONFIGURATION THROUGH THE USB PORT

3.1. Basic configuration

Before starting to work with the equipment, it must be configured loading all parameters related to the Wi-Fi connection and the network parameters. For them, the equipment has an embedded console, which operates through the USB port. This console performs the following functions:

- Searching for Wi-Fi available networks and joins them.
- Configure the name of the Wi-Fi network, channel and operation mode.
- Configure Wi-Fi security.
- Statically or dynamically assign IPs, load subnet mask and Default Gateway.
- List configuration.
- View the network status.
- List the configured region.
- Access equipment's help.

All configuration parameters are stored permanently and will remain stored even when the equipment is turned off.

INPORTANT NOTE:
It is assumed that there is an existing 802.11b or later network, configured in infrastructure mode, to which we will join.

3.2. List of console commands

The commands must be entered without intermediate spaces.

BASIC – Basic Wi-Fi configuration

Function:

It changes Wi-Fi basic configuration. It allows the configuration of the SSID network, the mode and the channel to be used.

Syntax:

BASIC:SSID,Mode,Channel

Parameters:

SSID: string <1 - 31> network identifier, Name.
Mode: Connection mode. It can be infrastructure or ad hoc (INF or ADH).
Channel: int <1 – 11> Communication channel. It depends on the country.

SECURITY – It configures the security of the Wi-Fi connection

Function:

It configures the type of encryption and authentication to be used. This command can have 1, 2 or 3 parameters depending on the type of encryption that is being passed as a parameter.
The parameters between [ ] depend on the type.

Syntax:

SECURITY: Type [,Reference [,Authentication]]

Parameters:

Type: Encryption type. (D, WEP, WPA)
Reference: for WEP <10 or 26 hexadecimal characters> only from (0 - 9) from (A - F) and from (a - f)

for WPA string <1 – 63 characters> only from (0 - 9) from (A - Z) and from (a - z) and space

Authentication: Open System or Shared Key. It can be (O or S).

As it has been mentioned, the SECURITY command admits a number of variable parameters according to the encryption type that wants to be configured. The following table clarifies this point:

Table 8 –SECURITY command according to the type of security

Security	Number of parameters of the SECURITY command
Security without encryption	1
WPA security	2
WEP security	3

Examples of the SECURITY command:

Security without encryption:

>**SECURITY**:D
Disabled security

WEP 104/128-bits (26 hexadecimal characters) security, with Open System authentication:

>**SECURITY**:WEP,0123456789ABCDF0123456789A,O
Enabled WEP security
Key: 0123456789ABCDF0123456789A
Authentication: Open System

WEP 40/64-bits (10 hexadecimal characters) security, with Shared Key authentication:

>**SECURITY**:WEP, C55EF0144D,S
Enabled WEP security
Key: C55EF0144D
Authentication: Shared Key

WPA security:

>**SECURITY**:WPA,my phrase
Enabled WPA security
Phrase: my phrase
Authentication: Pre-Shared Key

IMPORTANT NOTE:
For those cases in which the WPA encryption mode is configured, the SECURITY and BASIC commands will take a few seconds in responding and for the configuration to become effective. This applies to both commands, due to the fact that the SSW must calculate the WPA password based on the entered WPA phrase by the user and the configured SSID.

SCAN – It detects existing networks

Function:

Performs and active scan in each one of the channels to detect the existing networks.

Syntax:

SCAN

Parameters:

No parameters.

IMPORTANT NOTE:
During the scan for existing Wi-Fi available networks the connection is unavoidably lost.

SELECT – It selects one of the scanned networks

Function:

Of the scanned networks, one is selected by the identification number provided when the SCAN command is executed.

Syntax:

SELECT: Network number

Parameters:

Network number: Number provided at the moment the scan is made.

Examples of the SCAN and SELECT commands:

The sequence for scanning Wi-Fi networks is the following:

>**SCAN**
This action temporarily interrupts the Wi-Fi connection. To start scanning enter the command again.
>**SCAN**

```
0:  ExemysWIFI;INF;Ch 03;Excellent ;MAC 00:90:4C:91:00:01
1:  Studio    ;INF;Ch 06;Bad       ;MAC 00:21:29:69:CC:F0
```

The response of the SCAN command has the following format:

Number: SSID; Mode; Channel; Signal; MAC

Number: Correlative number identifying the network at that moment<1 – n>.
SSID: string <1 - 31> Network identifier or name.
Mode: string, can be INF or ADH.
Channel: int <1 - 14> Channel number .
Signal: string, Signal level detected for that network. It can be Bad, Regular, Good, Very Good or Excellent.
Mac: MAC address of Access Point or Wi-Fi router.

Once the SCAN has been completed, the network can be selected as follows:

>**SELECT**:0
SSID: ExemysWIFI
Mode: INF
Channel: 3

An out of range network number is entered; the SELECT command will give an error:

>**SELECT**: 3
The selected network does not exist.

NETWORK – Determines the network parameters

Function:

Configures the network parameters, the number of parameters depends of the selected IP assignment mode. It allows the assignment of static or dynamic IP modes. In case a static mode wants to be configured the static IP address must be entered manually, as well as the subnet mask and the Gateway.

Syntax:

(For assignment of dynamic IP)
NETWORK:DHCP
DHCP: Selects this operational mode.

(For assignment of static IP)
NETWORK:Ip, Netmask, Gateway

Parameters:

Ip: Static IP taken by the equipment disables DHCP.
Netmask:
Gateway:

LIST – Lists configured parameters

Function:

Shows on the screen the currently configured.

Syntax:

LIST

Parameters:

No parameters.

STATUS – Informs on the equipment status

Function:

Shows on the screen the equipment status regarding its connection. Indicates the Wi-Fi status, network status and the signal level.

Syntax:

STATUS

Parameters:

No parameters.

HELP – Command help

Function:

Shows a list of console commands and a brief description of their use.

Syntax:

HELP

Parameters:

No parameters.

3.3. Console configuration procedure

To begin with, the USB cable must be connected to the equipment and then execute the SSW Configuration application (provided with the equipment) in a PC or compatible.
For the detection of SSW devices, the Devices button is pressed. At this moment al SSW connected to the PC are detected (if they are not, press the Refresh button). The SSW to which we want to connect must be selected and then press the Connect button.

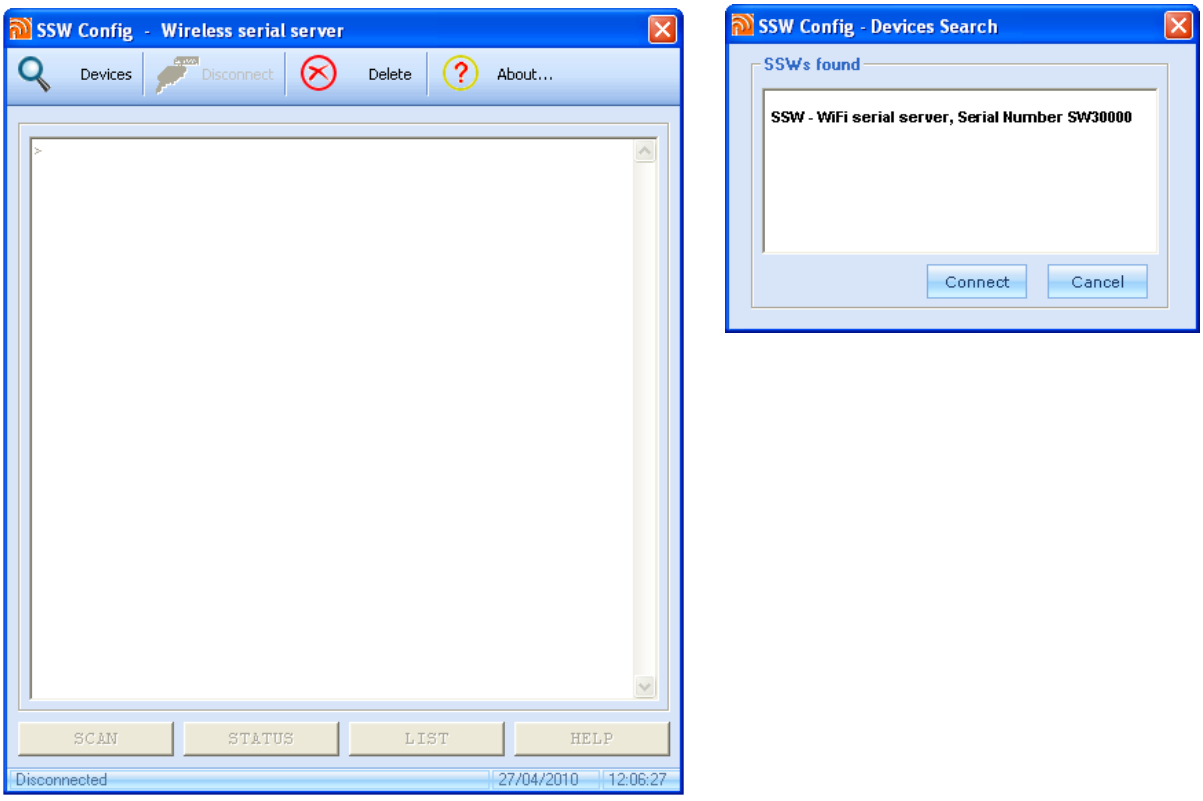


Figure 8 - Search for devices connected with SSW Config.
The status bar of the SSW Config window shows the connection status, the name of the device and its serial number. Once connected to the SSW, commands can be entered.

The minimum requirements for the SSW operation are the configuration of the Wi-Fi connection, security and network. There are three commands to perform these tasks. The commands are BASIC, SECURITY and NETWORK.
The following figure shows and example of how to do this:

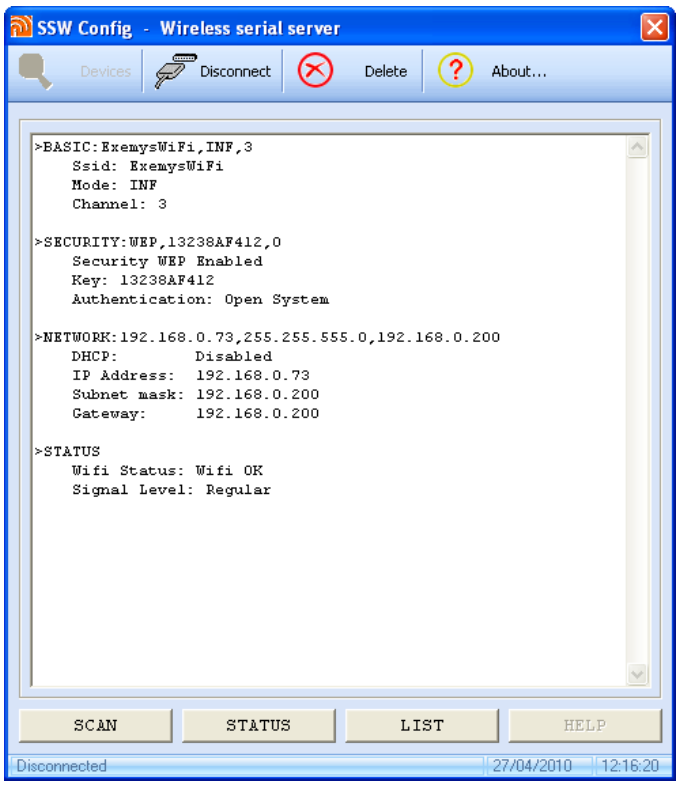


Figure 9 – Example of SSW configuration

The execution of the BASIC:ExemysWiFi,Inf,3 command specifies the SSID of the Wi-Fi network that is its name, which is ExemysWIFI, the operating mode, which is Infrastructure and the channel to be used, in this case is 3.

The first parameter of the SECURITY:WEP,13238AF412,O command you are configuring the encryption type, which is WEP 40/64-bits, with the second parameter the 10 hexadecimal character password is being entered and with the third one the Open System authentication is being enabled.
The NETWORK:192.168.0.73,255.255.255.0,192.168.0.200 command assigns the 192.168.0.76 static IP, the 255.255.255.0 subnet mask is set and the 192.168.0.200 IP address is specified as Default Gateway.

If the configured parameters are correct, in a few seconds the equipment should connect to the Wi-Fi network without problems. The previous figure shows that when the status command is executed (which shows the status of the equipment connection) the first time, the SSW has not yet joined the network, and after executing it again a few seconds later the SSW has entered the ExemysWiFi insfrastructure network and connected with a good signal.

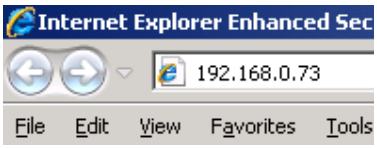
Once this is configured, the Web-Manager can be accessed through the IP address to the equipment.

IMPORTANT NOTE:
For the equipment to operate, the Access Point or WiFi Router must have been previously configured with the SAME PARAMETERS loaded in the SSW.

4. OPERATION WITH WEB-MANAGER

4.1. Access to the configuration Web page

Once the SSW has the Wi-Fi parameters configured and a valid IP, you will be able to access the Web page to configure the rest of the parameters. Use the Web browser with the JavaScript option activated allowing its use.



1. Enter the IP address of the SSW into the address field of the browser and press ENTER.
2. A dialog box will open where the SSW will ask you to enter the user/password to enter the page. Enter "admin" as user followed by the password to enter.
   The default password is "password", but this can be changed at any time.

3. You will be able to see in your browser the SSW configuration page. On the left there is a menu, while on the right the configuration page.

4.2. WEB configuration

In the SSW the COMs correspond to a socket that can be TCP or UDP depending on the configuration. This way, once communication is established in these sockets, data are transferred transparently from the corresponding COM to the socket and vice versa.

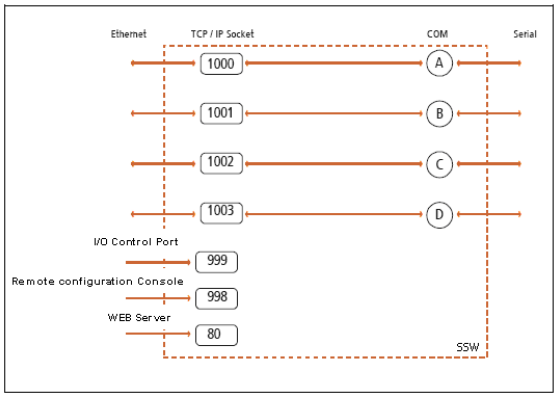


Figure 10 – Schematics of socket ports

The communication sockets correspond to the serial ports, they are flexible and completely configurable. SSW factory configuration in such a way that TCP 3000 and 2000 ports correspond to A and B COMs respectively, but this can be changed in the configuration of each COM.

As shown in the previous figure, the SSW has also 2 fixed TCP ports:
Supervision and control (Port 999) and HTTP Server (Port 80).
Through the Supervision and Control port (Port 999) the status of each channel can be supervised and also the management of SSW inputs/outputs.

4.2.1. Operational mode of channels

There are two available modes for data communication between the SSW and remote hosts. These modes are Server mode and Client mode.
The following table shows a brief description of the different operational modes of the channels.

Table 9 – Server or Client operational modes

Mode	Description
Server	If a COM-socket channel is configured to work in server mode in a port configured by the user, the SSW will be listening in this TCP port waiting for a client to establish a connection (each client will have to connect to the IP address and the server port). Once the connection is established, all data received in the socket will be transmitted to the corresponding serial port and vice versa.
Client	In the client mode, each COM-socket channel will have the IP address configured and the equipment port working as a server to which they must connect. This way, this channel will attempt to establish communication with the server, and once obtained, the received data in the socket will be transmitted by the corresponding serial port and vice versa.

Table 10 –Configurable parameters according to the operational mode of each channel

Server mode	Listening port
	Port type
	New connection priority
Client mode	Remote IP
	Remote port
	Port type

4.2.2. Access password to configuration

The configuration WEB page is protected with an access password. The equipment administrator can assign an access password to these resources, providing a secure access method to the SSW configuration.
To change the access password from the WEB-Manager:

- Select the "Configuration" option in the menu, and then click on the "Administrator" tab.
- Enter the new access password in the "Password" box, type again for confirmation.
- Finally press on "Save configuration" for the SSW to accept the changes.

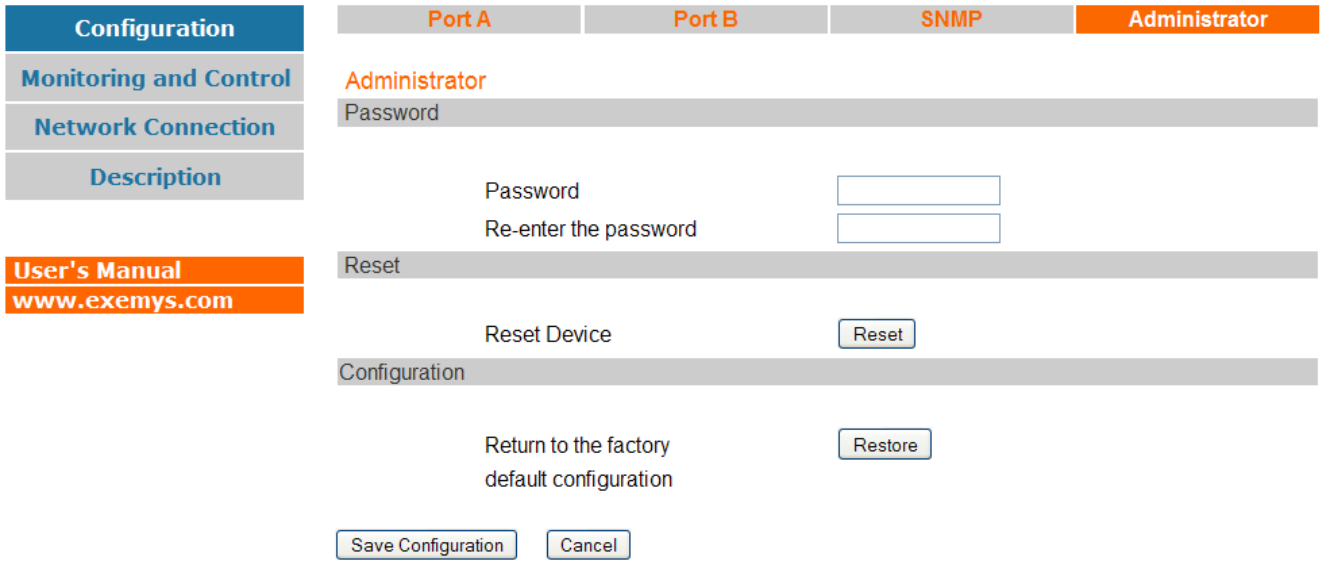


Figure 11 – Administrator Panel

4.2.3. How to return to factory configuration

The SSW administrator can at any time return the equipment configuration to the original factory configuration.

To return to the SSW original factory configuration from the Web-Manager:

- Select the "Configuration" option in the menu, and then click on the "Administrator" tab.
- Press the "Restore" button in the "Return to factory configuration" box. A message will appear asking you to confirm the action.
- Press "Accept" if you want to restart the SSW with the factory configurations.

IMPORTANT NOTE:
The Wi-Fi connection will probably be lost when the factory values are restored if the Access Point configuration is not updated with these values.

4.2.4. SSW reset

If necessary, the SSW can be reset, in this mode all connections will be closed and the SSW will return to its initial state.

To reset the SSW from the WEB-Manager:

- Select the "Configuration" option in the menu, and then click on the "Administrator" tab.
- Press the "Reset" button in the "Reset equipment" box. A message will appear asking for confirmation.
- Click on "Accept" if you want to reset the SSW.

4.2.5. Configuration of the COM-Socket channels

The COM-Socket channels of the SSW can be configured individually according to need. For this you must access to the "Port X" tab (that can be A, B, …, N according to the SSW model) in the "Configuration" menu of the WEB-Manager.

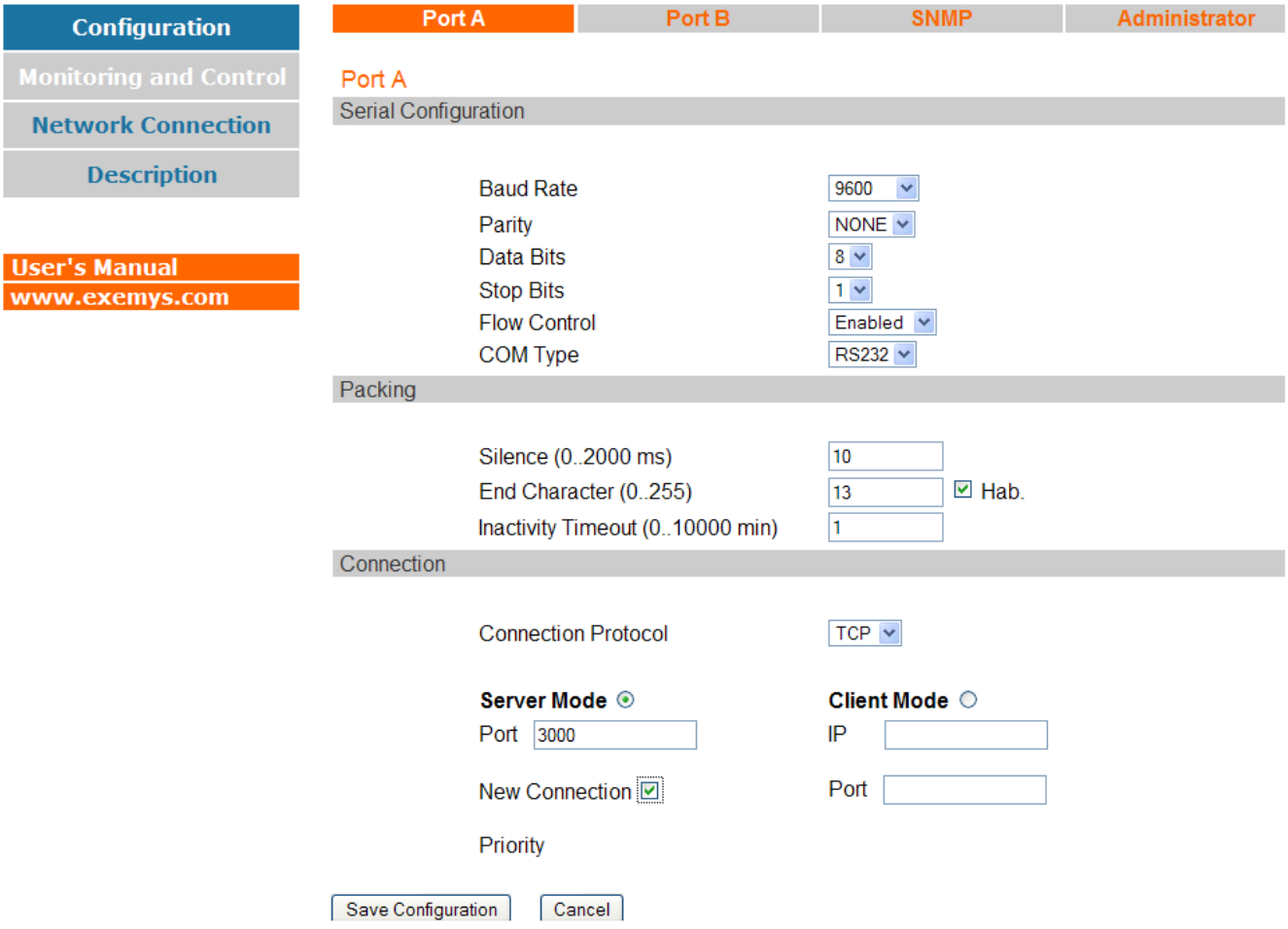


Figure 12 – Configuration of a COM-Socket

The configuration parameters of serial ports are:

Table 11 – Configuration parameters of the serial port.

Port setting

Baud Rate	Transfer rate in bits per second. Configurable speeds go from 300 bps to 115200 bps.

Parity	Error checking according to parity. Default value is NO (no error checking.).
Data bits	Indicate the number of bits used for characters. Default value is 8.
Stop bits	Indicates the number of stop bits. Default value is 1.
Flow control	Flow control by hardware (RTS/CTS). Manages the data flow between the devices to ensure an efficient process and avoid data loss. Available only in models with RS-232.
COM type (*)	Allows the selection of the serial port protocol. The available options are RS-232 with or without flow control by hardware, RS-485 (2-cable mode) and RS-422 (4-cable mode).

(*): The COM RS-485 and RS-422 types are only valid in models SSW-1C0-42 and SSW-2C0-42. Between these models the change is only the way of connecting and the COM connector layout of the SSW (see installation).

Packetizing are packet control criteria used to cut and transmit packets from the serial COM, to the socket (TCP or UDP). (In case none of the available packetizing options are enabled, the criteria for cutting and sending of packets used will be full buffer (the buffer size used in this communication sense is of 2000 characters).

Table 12 – Packetizing criteria.

Packetizing

Silence	This parameter is wait time or window time. Once last data are received in the COM, the SSW will wait this time before sending the packet on the Ethernet network through the corresponding socket. This manner there is a better use of the bandwidth of the 802.11 network, since it allows joining several received bytes through the serial port in one packet. On one side, it incorporates a delay in the transmission of the information, which has to be treated with special care according to the serial communication protocol being used. In case such protocol does not allow any delay, the configuration of the time window in 0 is recommended. Possible values for the time window can be in the range of 0 ms to 2000 ms.
End Character	Indicates which is the last character of the serial stream that makes up the TCP packet. When the arrival of that character is detected, the packet will be cut and will be transmitted through the socket. If a time window value different from 0 ms is used jointly, the condition occurring first, the arrival of the end character or the passing of the time window, has the priority. The criterion of the end character can be enabled or disabled by means of the Check Box indicated as "Hab".
Inactivity	This parameter if the maximum time of inactivity admissible by the equipment. After this time passes, the SSW considers that the connection has dropped and closes it. This option can also be disabled without closing the connection even if there is no data flow. If this value is 0, the connection will not be closed by inactivity in that channel, that is the option is disabled.

In case more than one packet control criterion is enabled at the same time, the condition that is fulfilled first will be executed.

As mentioned previously, the SSW channels can work in Server mode as well as in Client mode. The parameters that should be configured according to the operational mode selected for each channel are detailed below.

Connection

Server mode connection	**Connection type**	First select the transport protocol which can be TCP or UDP.
	Port	It is the port (TCP or UDP) to which the clients must connect when they want to send data that will go through the corresponding serial COM and vice versa.

	Priority new connection	It may happen that in Server mode, the client connection drops, if this client or another one attempts to connect to the SSW server channel that has the option. New connection priority enabled, the SSW will abort the previous connection allowing the new client to connect. If otherwise, the new connection Priority is not enabled in that server channel, the SSW will not allow the connection of the new client and in that case the server will be able to use the link closing option for inactivity time. If the server channel has the new connection Priority option enabled, if there is a connection established with a client and another client attempts to connect to the same server, the connection with the previous client will close and will allow the new client to establish the connection with the server. All in all, • Enabled new connection Priority: If a new client attempts to connect to an already open link (with the same client or not), it will abort the previous connection and will allow the new client to connect. • Disabled new connection Priority: It will not allow a new client to establish connection if there is already an open link in the server's port.
Client mode connection	**Connection type**	Allows the selection of the connection protocol that can be TCP or UDP.
	IP	IP address of the remote server to which that channel client will connect.
	Port	Port of remote server to which this channel client will connect.

Table 13 – Configuration parameters of the connection.

To configure these parameters you can do it from the Web-Manager:

- In the "Configuration" menu select the Port tab you want to configure.
- Among the necessary values. For the Termination parameter enter the ASCII value in the box and check to enable the option or do not check it to disable it.
- If you want the new connection Priority option enabled, check the respective box.
- Press the Save Configuration button so the SSW takes the new configuration.

4.2.6. Operation in SNMP mode

The SSW supports the SNMP supervision protocol. The SSW can be enabled to work as SNMP agent, this means that responds to queries under this protocol and is also capable of generating unsolicited messages (Traps) for the notification of certain events. General Enabling / Disabling of this service can be made by means of the equipment configuration Web page.
Though the SNMP is also possible to modify the status of digital outputs of the SSW.
With the SNMP service enabled, it is possible to enable or disable sending traps. UP to 2 Manager IP addresses can be configured (addresses to which the SNMP traps will be sent to) as a redundant security method and to configure the read, write and trap communities. It must be clear that if the same IP address is configured in both Manager IP fields, the alarms will arrive in duplicate. If what you want is to have one Manager IP address, the value 0.0.0.0 must be entered in the Manager IP address that you want to disable.
The "Reading Community" and "Writing Community" are keywords to access the equipment information with permission to read and write respectively. The "Trap Community" is the keyword received with each trap sent by this equipment.

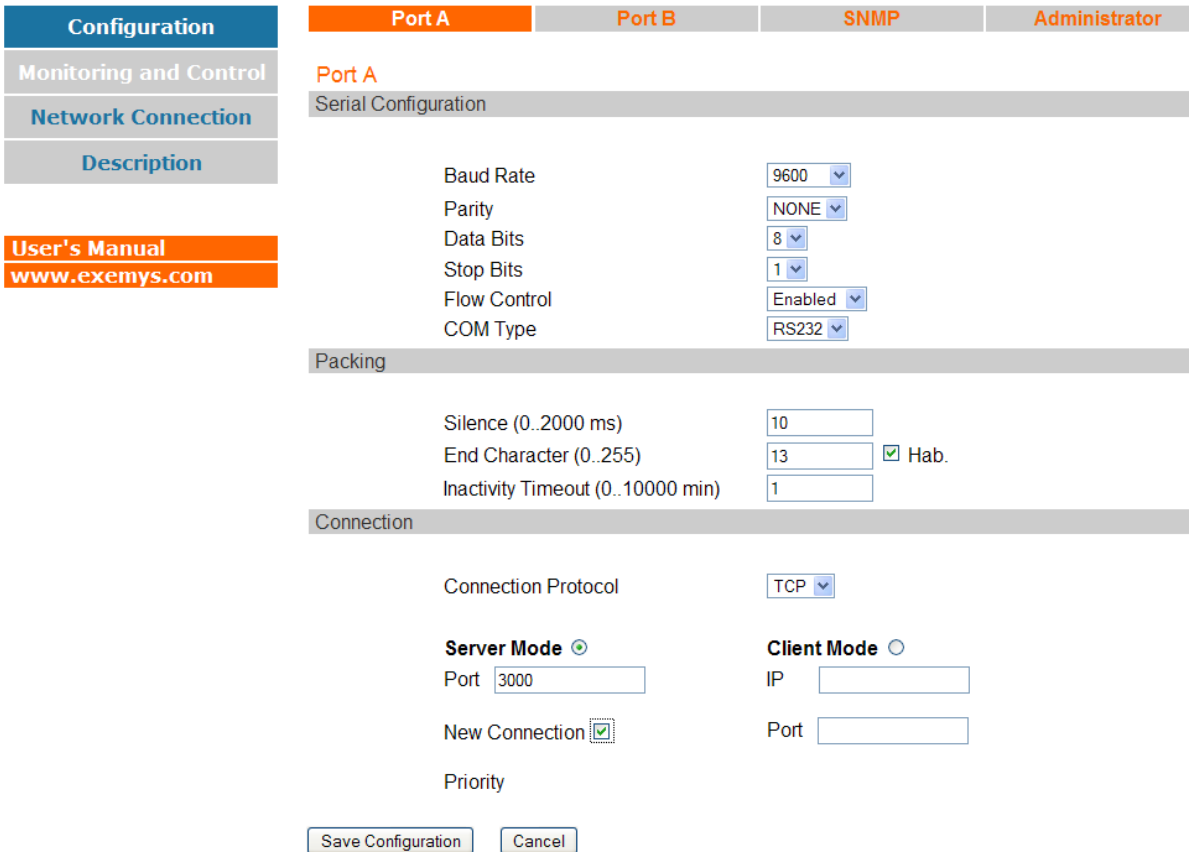


Figure 13 –SNMP configuration

IMPORTANT NOTE:
Community passwords can be up to 15 characters long.

4.2.6.1. SNMP Traps

When the status of any of the digital inputs or outputs of the equipment changes, the SSW notifies this event sending an SNMP Trap to the configured Manager IP address.
Details of traps sent by the SSW are shown below.

Table 14 – List of SNMP Traps

Trap	Description
Cold Start	This trap is sent every time the equipment is turned on.
Warm Start	This trap is sent every time the equipment makes a soft reset.
sswinputOn	This trap is sent every time a digital input is turned on. The input number and status are sent embedded in the trap.
sswinputOff	This trap is sent every time a digital input is turned off. The input number and status are sent embedded in the trap.
sswoutputOn	This trap is sent every time a digital output is turned on. The output number and status are sent embedded in the trap.
sswoutputOff	This trap is sent every time a digital output is turned off. The output number and status are sent embedded in the trap.

4.2.6.2. MIB

The MIB (Management Information Base) file described the number of objects or parameters of the SSW administered by the SNMP protocol. This file contains information about the type of object, level of access, etc.
The SSW.MIB file is included in the CD sent with the equipment.
This file must be loaded in the SNMP Manager for the correct administration of the different objects of the SSW.

4.2.6.3. Description of the SNMP tree

Table 15 – Variables of the SNMP tree.

Variable	OID	Description
	SYSTEM	
sysDescr	.1.3.6.1.2.1.1.1 .iso.org.dod.internet.mgmt.mib-2.system.sysDescr	Description of the device.
sysOID	.1.3.6.1.2.1.1.2 .iso.org.dod.internet.mgmt.mib-2.system.sysObjectID	It is the OID given by the company of the SNMP subsystem of this equipment.
sysUpTime	.1.3.6.1.2.1.1.3 .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime	It counts the time from system start up.
	NAME	
Name	.1.3.6.1.4.1.18284.1.2.2 *.serialServers.ssw	Configured name for this input.
	INPUTS / OUTPUTS	
Inputs	.1.3.6.1.4.1.18284.1.2.2.1.1.1 *.serialServers.ssw.iosTable.iosEntry.inputs	Status of Inputs.
Ouputs	.1.3.6.1.4.1.18284.1.2.2.1.1.2 *.serialServers.ssw.iosTable.iosEntry.outputs	Status of Outputs.
Index	.1.3.6.1.4.1.18284.1.2.2.1.1.100 *.serialServers.ssw.iosTable.iosEntry.iosIndex	Index of the inputs / outputs table (from 0 to 7).
	MANAGER	
IP Manager 1	.1.3.6.1.4.1.18284.1.2.2.10.1 *.serialServers.ssw.config.ipTraps1	IP address of first NMS.
IP Manager 2	.1.3.6.1.4.1.18284.1.2.2.10.2 *.serialServers.ssw.config.ipTraps2	IP address of second NMS.
IP aaddress	.1.3.6.1.4.1.18284.1.2.2.10.3 *.serialServers.ssw.config.ipConfigAddress	Equipment IP address.
Net mask	.1.3.6.1.4.1.18284.1.2.2.10.4 *.serialServers.ssw.config.ipConfigSubnetMask	Mask of equipment sub network.

Gateway	.1.3.6.1.4.1.18284.1.2.2.10.5 *.serialServers.ssw.config.ipConfigGateway	Equipment gateway.
STATISTICS		
Bytes TX through COM A	.1.3.6.1.4.1.18284.1.2.2.11.1.1.1 *.serialServers.ssw.stats.comA.portSerieA.transmittedBytes	Bytes transmitted by the Serial Port of channel A.
Bytes Rx through COM A	.1.3.6.1.4.1.18284.1.2.2.11.1.1.2 *.serialServers.ssw.stats.comA.portSerieA.receivedBytes	Bytes received by the Serial Port of channel A.
Status of A socket	.1.3.6.1.4.1.18284.1.2.2.11.1.2.1 *.serialServers.ssw.stats.comA.socketA.state	Status of channel A socket.
Tx Packets through socket A	.1.3.6.1.4.1.18284.1.2.2.11.1.2.2 *.serialServers.ssw.stats.comA.socketA.transmittedPackets	Packets transmitted through the channel A socket.
Rx Packets through A socket	.1.3.6.1.4.1.18284.1.2.2.11.1.2.3 *.serialServers.ssw.stats.comA.socketA.receivedPackets	Packets received through the channel A socket.
Openings A socket	.1.3.6.1.4.1.18284.1.2.2.11.1.2.4 *.serialServers.ssw.stats.comA.socketA.openings	Number of openings of the channel A socket.
CLosings for inactivity of the A socket	.1.3.6.1.4.1.18284.1.2.2.11.1.2.5 *.serialServers.ssw.stats.comA.socketA.inactivityClosure	Number of closings by inactivity time of the channel A socket.
Tx Bytes through COM B	.1.3.6.1.4.1.18284.1.2.2.11.2.1.1 *.serialServers.ssw.stats.comB.portSerieB.transmittedBytes	Bytes transmitted by the Serial Port of channel B.
Rx Bytes through COM B	.1.3.6.1.4.1.18284.1.2.2.11.2.1.2 *.serialServers.ssw.stats.comB.portSerieB.receivedBytes	Bytes received by the Serial Port of channel B.
Status of B socket	.1.3.6.1.4.1.18284.1.2.2.11.2.2.1 *.serialServers.ssw.stats.comB.socketB.state	Status of channel B socket.
Tx Packets through B socket	.1.3.6.1.4.1.18284.1.2.2.11.2.2.2 *.serialServers.ssw.stats.comB.socketB.transmittedPackets	Packets transmitted through the channel B socket.
Rx packets through B socket	.1.3.6.1.4.1.18284.1.2.2.11.2.2.3 *.serialServers.ssw.stats.comB.socketB.receivedPackets	Packets received through the channel B socket.
Opening through B socket	.1.3.6.1.4.1.18284.1.2.2.11.2.2.4 *.serialServers.ssw.stats.comB.socketB.openings	Number of openings of channel B socket.
Closing by inactivity of B socket	.1.3.6.1.4.1.18284.1.2.2.11.2.2.5 *.serialServers.ssw.stats.comB.socketB.inactivityClosure	Number of closings by inactivity time of channel B socket.
TRAPS		
sswinputOn	.1.3.6.1.4.1.18284.1.2.2.0.1 *.serialServers.ssw.ssw#.sswinputOn	Name of the trap sent each time an input passes from OFF status to ON status. Input number and status are sent embedded in the trap.
sswinputOff	.1.3.6.1.4.1.18284.1.2.2.0.2 *.serialServers.ssw.ssw#.sswinputOff	Name of the trap sent each time an in put passes from ON status to OFF status. Input number and status are sent embedded in the trap.
sswoutputOn	.1.3.6.1.4.1.18284.1.2.2.0.3 *.serialServers.ssw.ssw#.sswoutputOn	Name of the trap sent every time an output passes from OFF status to ON status. Output number and status are sent embedded in the trap.
sswoutputOff	.1.3.6.1.4.1.18284.1.2.2.0.4 *.serialServers.ssw.ssw#.sswoutputOff	Name of trap sent each time an output passes from the ON status to the OFF status. Output number and status are sent embedded in the trap.

*: OIDs in text format start with:**.iso.org.dod.internet.private.enterprises.exemys.exemysProducts**

4.3. UDP transport protocol

The transport protocol for the Wi-Fi interface can be selected. Possible products are: TCP and UDP.
An explanation about the UDP protocol in different operational modes follows.

4.3.1. Client channel with UDP Protocol

For a channel in Client mode, the IP address and Server port to which it will connect must be configured. When the transport protocol is UDP, this channel will transmit to that socket (IP-Port) the data received by the serial port and vice versa.
In the particular case in which the server IP address of that channel is the broadcast address (Remote server IP = 255.255.255.0), The SSW will transmit a UPD broadcast with everything received through the serial port. The serial port will transmit what has been received from the Wi_Fi side since it received it through a broadcast or a determined IP address.

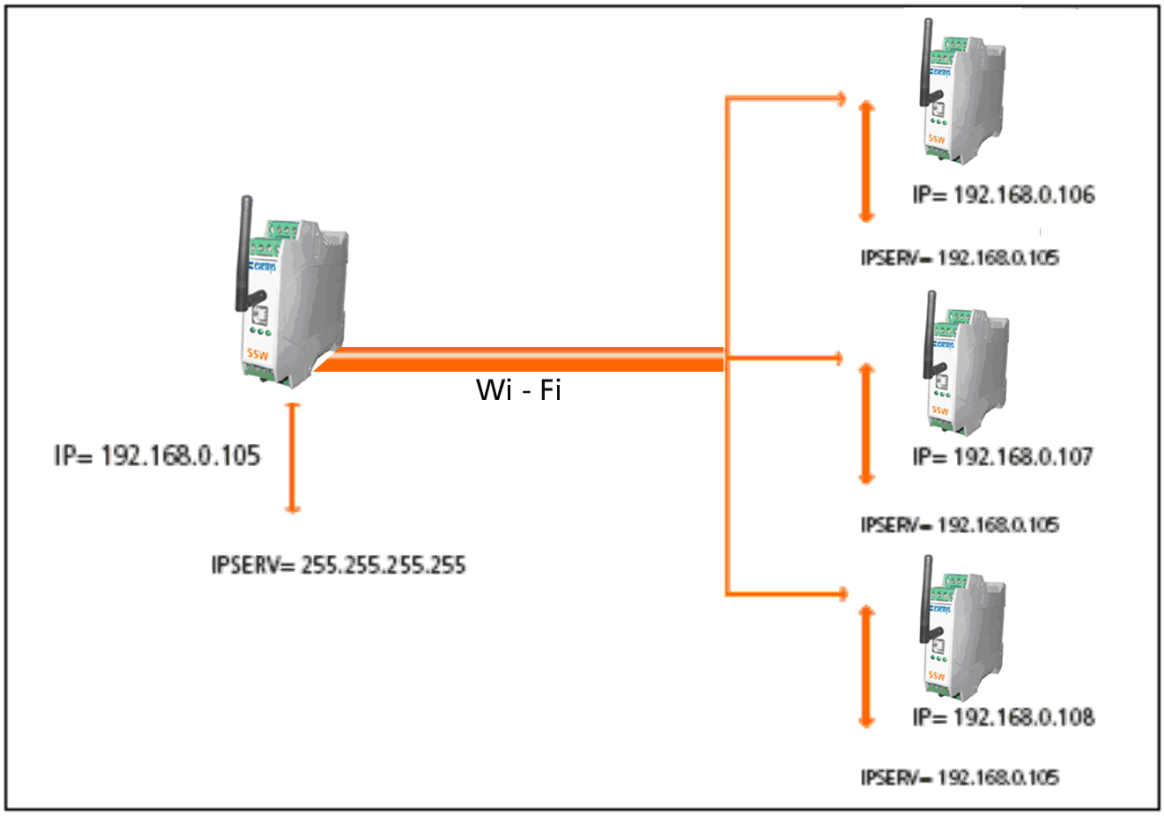


Figure 14 –UDP broadcast of the SSW in Client mode.

Canal de cliente UDP: UDP Client channel

4.3.2. Server channel with UDP Protocol

For a channel in Server mode only the port of this channel must be configured. When the transport protocol is UDP, the server channel will remain "linked" to the first IP address that sends a packet.
The Inactivity parameter must also be configured, which will work in a similar manner as in the TCP mode. It will simply lose the link with a determined IP address (the first one that sent a packet) after this time, allowing the other address to remain linked with the UDP Server channel.

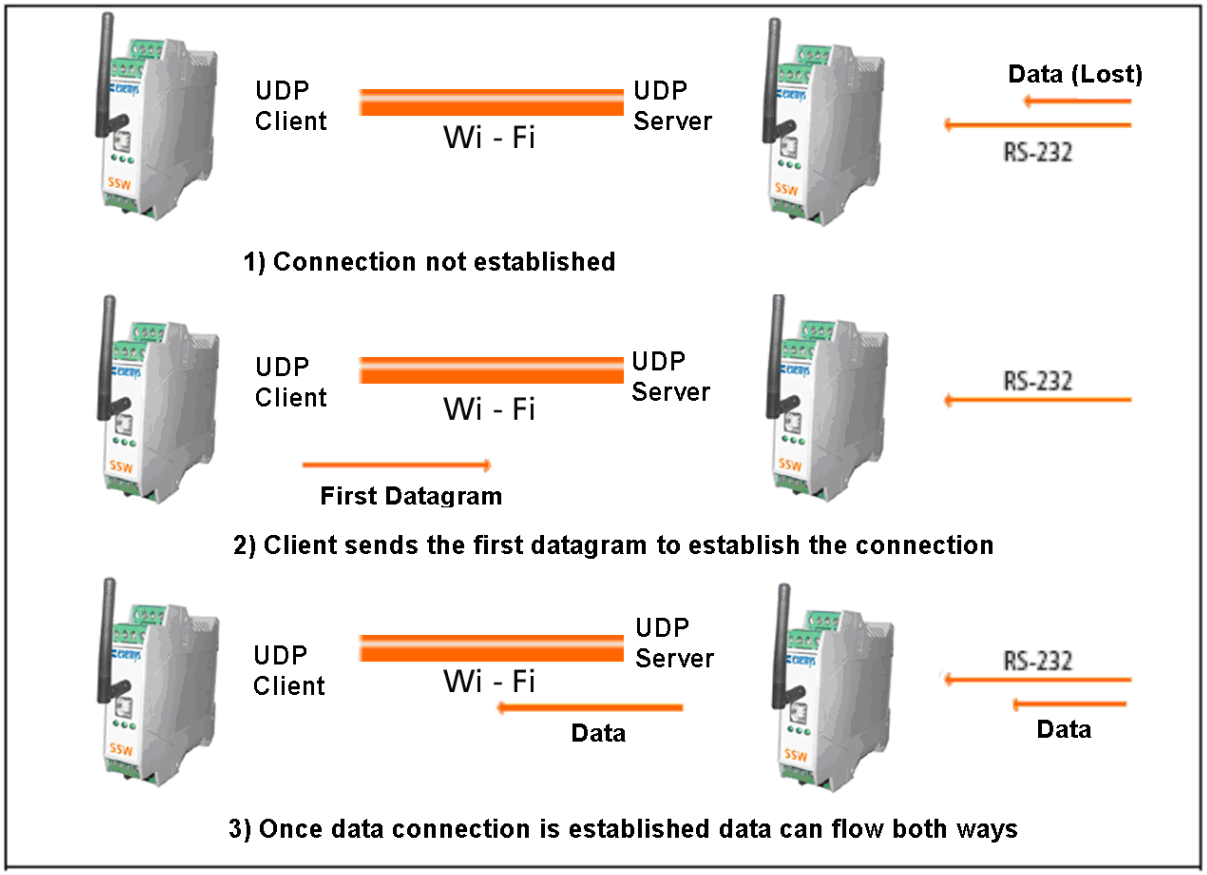


Figure 15 – Two SSW, one as client and the other one as server.

When two SSWs are connected with the UDP transport protocol, one of them in Client mode and the other one in Server mode, the SSW in Server mode will not send the received data through the serial port to the Client's IP unless the Client has previously sent a packet to establish communication. This means that the Server SSW will have to receive a UDP packet from the Client, and it will remain linked to that IP. Then all data received through the serial port will be transmitted to the Client IP.
If the Client does not send a packet to the server, the latter will not have established the link and the data received by the corresponding serial port will be lost.

4.3.3. Connection between two UDP clients

The UDP mode, different from the TCP, allows communication between two devices configured in Client Mode. This mode shows an advantage over the Client-server typology since the connection can be established both ways, regardless of which serial device sends the information first.
In this case, both devices must be configured in Client mode, and the IPs and ports of the Remote Server of the other device must be configured.

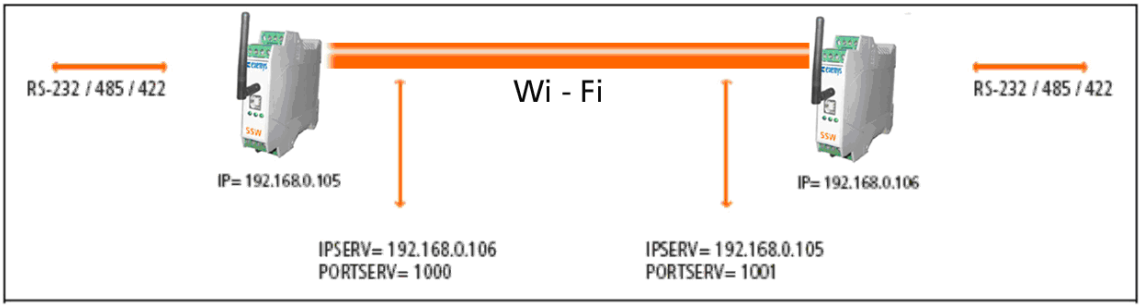


Figure 16 – Connection of two UDP clients

Canal de cliente UDP: UDP Client channel

4.4. *Monitoring and control*

If we select the "Monitoring and control" option of the Web-Manager menu, we will have access to 3 submenus that will let us perform the following actions:

- Monitor and control the status of inputs and outputs of the equipment.
- Monitor the statistics of all available COM-Sockets.
- See the network configurations, and monitor the reception level of the Wi-Fi signal.

4.4.1. Inputs / Outputs

If we select the "Inputs/Outputs" tab which is inside the "Monitoring and control" option if the WEB-Manager menu we can see the status of each one of the SSW inputs, through a green light that turns on an off. We can also turn on/off the outputs through buttons and see the status of them through yellow lights as we can see in the figure.

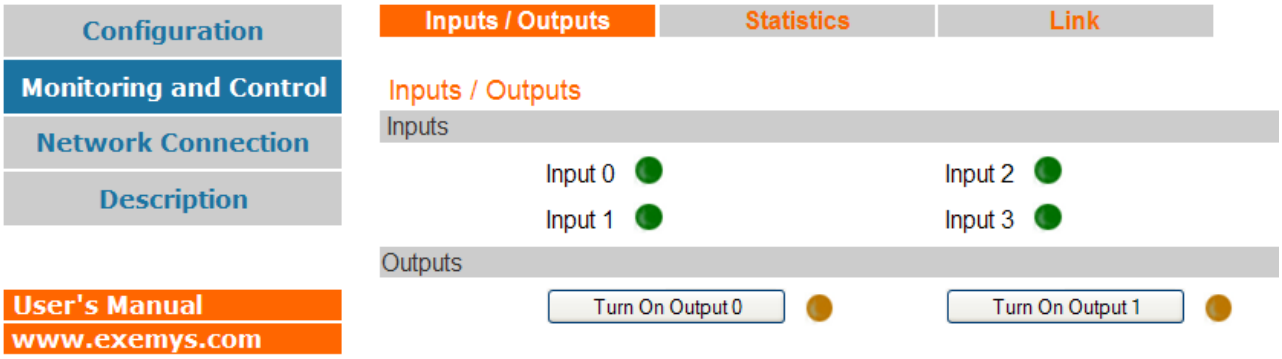


Figure 17 – Monitoring and Control of Inputs/Outputs via WEB-Manager.

In addition to this WEB resource, the equipment provides another alternative to monitor and control the status of inputs and outputs of the SSW, and is through the SNMP (See SNMP section in this manual).

4.4.2. Statistics

To gain access to equipment statistics the "Statistics" tab must be selected, within the "Monitoring and Control" menu. There, you will be able to see the number of transmitted and received bytes through the serial port, the number of packets transmitted and received by the socket, the number of socket openings, the number of closings by inactivity

and the socket status. As to the status of the socket, if these are not connected they will be attempting to connect to a server all the time if they were configured in client mode, or waiting for connection if they are in server mode.

The Reset Statistics button allows setting to zero all page counters.

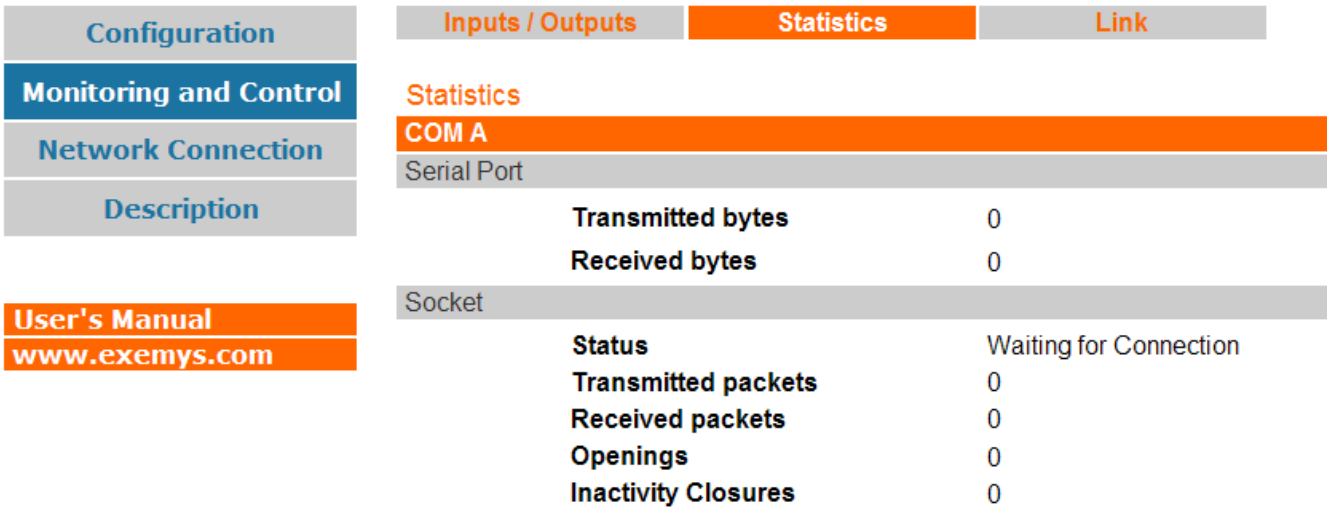


Figure 18 - Connection statistics

4.4.3. Link

Through the "Link" tab of the "Monitoring and Control" menu option, we can see the name of the Wi-Fi network, and the signal level.

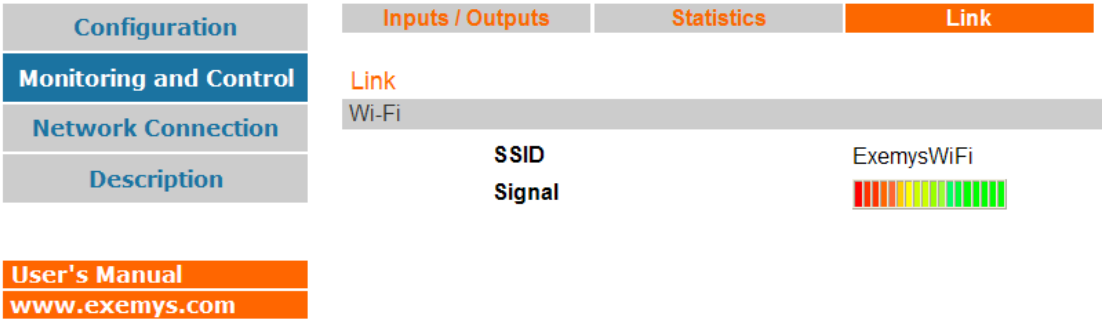


Figure 19 – Link page.

4.5. Network connection

The complete configuration status of the SSW can be seen gaining access to the "Network connection" option of the equipment menu.

4.5.1. Wi–Fi parameters

If you enter through the WEB-Manager to Network connection → Wi–Fi, we will be able to see all parameters relative to the Wi-Fi configuration, which are the basic parameters like network Name, mode and channel, and in reference to Wi-Fi security, the encryption type, password and authentication.

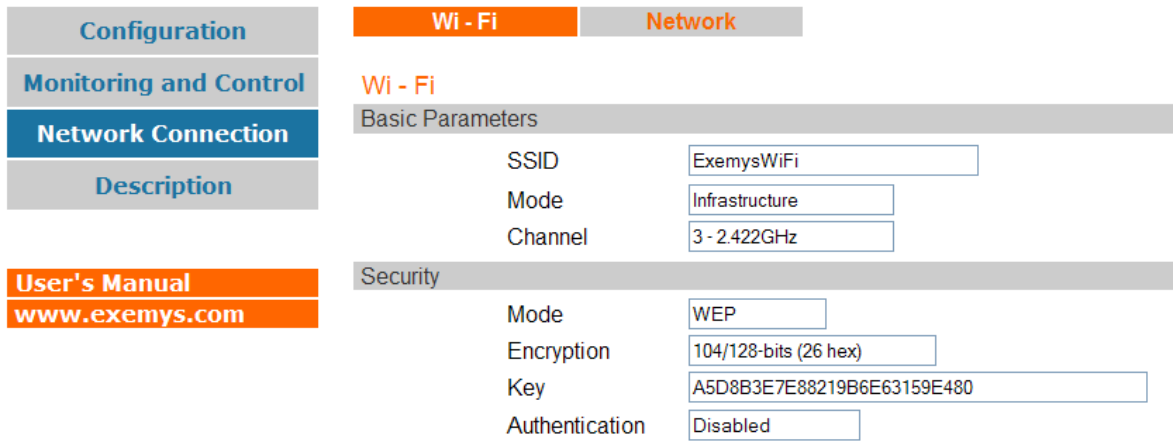


Figure 20 – Network connection: Basic parameters and Wi-Fi Security.

4.5.2. Network parameters

It lets you see if you are working with dynamic IP (DHCP enabled) or with static IP.

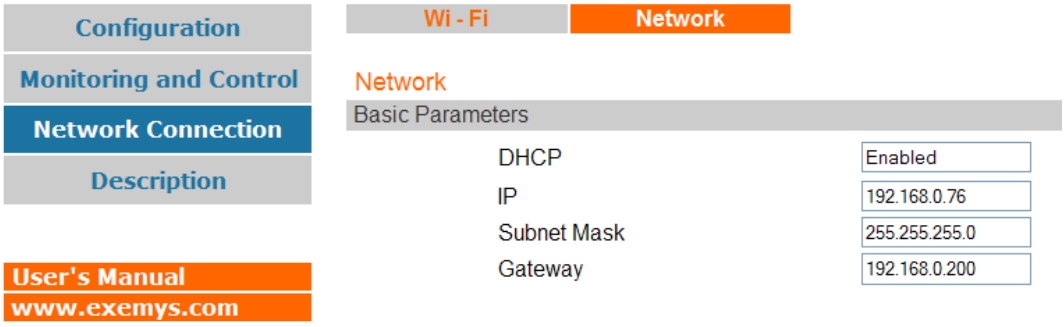


Figure 21 – Network connection: Basic network parameters.

4.6. SSW description

In the "Description" page we can see the SSW model, Hardware and Firmware versions, equipment MAC, and its serial number.

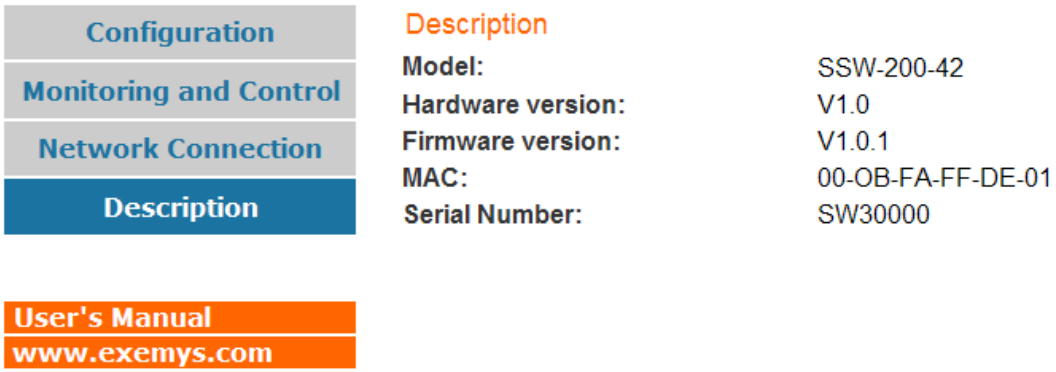


Figure 22 – SSW description through the WEB page.

5. SUPERVISION AND CONTROL PORT

The SSW incorporates the capacity of handling digital inputs and outputs and supervision of the status of connection sockets linked with each channel through simple commands.
The Supervision and Control port works through a TCP connection in port 999.
Each command must end with the CR character (ASCII 13).
For each executed command a response will be received confirming that the command has been executed, successfully or not.

5.1. Connection Supervision commands

For connection supervision of the SSW you have the commands **STA** and **RST**.
The **STA** command will inform on the connection status of sockets of each channel (Wi-Fi side), giving the response '1' (Connected) or '0' (Disconnected).
The **RST** command lets you restart the socket of a particular channel. If a socket of channel that is not available in this model is requested to reinitiate, it will respond with an error.

Table 16 – Connection Supervision commands.

Command	Description	Response
STA<CR>	Shows the status of the socket connection of all available channels (depending on the model).	**STA,ab<CR>** a..b: Status of sockets from 0..n-1 a, b: can be '1' o '0' Where n is the number of available sockets in each model. 1 = Connected 0 = Disconnected
RST:x<CR>	Resets the socket of channel x specified. The channel can be: A = COMA B = COMB (Depending on the number of available channels in the model)	*In case of success:* **RST:x,OK<CR>** Channel x reinitiated correctly. *In case of error:* **RST:x,ERROR<CR>** Channel x has not reinitiated or there is no channel in this model.

5.2. Automatic report of digital inputs (DIR)

In the Supervision and Control port the SSW informs the status of all inputs when a change is detected in any of them. The SSW will inform the status of all inputs when a client connects in the TCP 999 Port and each time a change is detected in any of the available inputs.

Table 17 – Automatic Report of digital inputs (DIR).

Report format	Description
DIR,abcdefgh<CR>	Will inform the status of all inputs when a client is connecting in the TCP 999 Port and each time a change is detected in any of the available inputs. a..h: Status of digital inputs (the number depends on the model). It can be 0 or 1.

5.3. Reading of inputs

For reading the status of inputs, the SSW incorporates the **INA** and **IN** commands.
To find out the general status of all available inputs in a particular SSW model, the equipment has the **INA** command.
On the other side, if we want to find out the status of only one input in particular of all the available inputs in the SSW model, we must use the **IN** command.
It should be noted that if the status of an input not available in this model is requested, it will respond with an error.

Table 18 – Input reading commands.

Command	Description	Response
INA<CR>	Returns the status of all available inputs in this SSW model.	**INA,abcdefgh<CR>** a..h: Status of inputs from 0..n-1 Where n is the number of available inputs in each model. 1 = In high status 0 = In low status
IN:i<CR>	Shows the status of input i, that must be available in this model. i = 0…n-1 (n is the number of available inputs in each model	*In case of success:* **IN:i,s<CR>** i = Read input (0..n-1) s = Status of input (0 or 1) *IN case of error:* **IN:i,ERROR<CR>** Input i is not available in this model.

5.4. Output handling

Output handling can be made through four supervision and control commands **OUT**, **OUR**, **PON** and **POF**.
Outputs must be handled individually.
The **OUT** command allows the change of status of a specific output individually. If this command is sent with an incorrect output number or that does not exist in this model, an error message will be returned.
The **OUR** command allow to know the real status of all digital available digital outputs in this SSW model. The outputs are listed in ascending order and their status is specified with "1" in case of high status, or "0" in case of low status.
The **PON** and **POFF** commands are used to generate high or low active pulses respectively, in a determined output during a specified time. These commands will return an error in case an inexistent output has been passed as a parameter or a time value out of the permitted range (from 0 to 100 seconds).

Table 19 – Output handling commands

Command	Description	Response
OUR<CR>	Returns the status of all available outputs in this SSW model.	**OUR,abcdefgh<CR>** a..h: Status of outputs from 0..m-1 Where m is the number of available outputs in each model. 1 = In high status 0 = In low status
		In case of success:

OUTo:s<CR>	Changes the status of output o. o = 0..m-1 (m is the number of available outputs in each model s = 0..1 is the new status of output o.	**OUTo:s,OK<CR>** Status of output o has been changed. *In case of error:* **OUTo:s,ERROR<CR>** Output o is not available in this model.
PONs:e<CR>	Generates a high active pulse in a specific output, during a specified time. s = 0..m-1 (m is the number of available outputs in each model). e = 0..100 is the time in seconds that the pulse is active.	*In case of success:* **PONs:e,OK<CR>** The pulse has been generated correctly. *In case of error:* **PONs:e,ERROR<CR>** No output is indicated, or the time for attempting a configuration was exceeded.
POFs:e<CR>	Generates a low active pulse in a specific output, during a specified time. s = 0..m-1 (m is the number of available outputs in each model. e = 0..100 is the time in seconds the pulse remains active.	*In case of success:* **POFs:e,OK<CR>** The pulse has been generated correctly. *In case of error:* **POFs:e,ERROR<CR>** No output indicated, or the time for attempting a configuration was exceeded.

A. TECHNICAL SPECIFICATIONS

Power

Voltage Input:	+10 a +30 VDC
Current:	250mA max.

WLAN

Standard:	IEEE 802.11b
Frecuencie:	2.4GHz
Band Widht:	11Mbps max.
TX Power:	16 dBm (40mW)
RX Sensibility RX:	-76 dBm
TX/RX Mode:	Half Duplex
Security:	WEP + WPA
TX Distance:	Up to 100 m in open areas
Modes:	Infraestructure + Ad-Hoc
Antenna Input type:	Reverse Polarity SMA male pin

Antenna

Gain:	+2dB
Antena Connector:	Reverse Polarity SMA female
Antenna dimensions:	11 cm lenght, 1 cm diameter

USB Port

Use:	Basic Configuration of Wi-Fi network
Connector:	Type "B" female
External cable:	Optional, USB type "A" Male, USB type "B" Male

Serial Ports

Quantity:	Up to 2 Serial ports RS232/485/422
Baud Rate:	300 / 115.200 bps
Flow Control:	Nothing / Hardware RTS-CTS
Signals:	RS232 (Tx, RX, RTS, CTS) RS485 (TR+, TR-) RS422 (TR+, TR-, R+, R-)
Connector:	Industrial pluggable terminal block

Inputs and Outputs

Inputs:	4, Voltage ON=3.5/28Vdc, Voltage OFF<0.5Vdc
Outputs:	2, Type=Open Collector NPN Sink., Voltage Max=3/45Vdc, 50mA
I/O Control:	SNMP traps - ASCII commands Internal Web page
Protocols:	TCP, UDP, IP/ICMP, DHCP Client, SNMP (Version 1), WEP, WPA, HTTP
Configuration:	InternalWeb page
Statistics:	InternalWeb page

Weigh and Dimensions

Dimensions:	120mm x 100mm x 22.5mm without antenna
Total Weigh:	150g

B. FACTORY DEFAULT CONFIGURATION

PARAMETER	DESCRIPTION	VALUE
Login		
User	User's name to initiate a session in the WEB-Manager	admin
Password	Password to initiate a session in the WEB-Manager	password
Wi-Fi connection		
SSID	Name of Wi-Fi network	ExemysWiFi
Mode	Wi-Fi connection mode	Infrastructure
Channel	Channel number used	3
Wi-Fi security		
Encryption	Type of encryption used	No encryption
Authentication	Type of authentication used	Open-system
WEP password	WEP password (in hexadecimal)	A5D8B3E7E88219B6E63159E480
WPA Passphrase	Phrase used to generate the WPA password	"now is the time"
Network connection		
IP address of the SSW	Static IP address assigned to the equipment	192.168.0.76
Netmask	Value of netmask	255.255.255.0
Gateway	Gateway Default address	192.168.0.200
DHCP	DHCP enable	Disabled
Serial configuration		
Baud Rate	Speed of communication	9600bps
Parity	Error checking	No parity
Data bits	Number of transmitted/received Data	8
Stop bits	Number of Stop Bits	1
COM type	There are three types: RS232/RS485/RS422	RS232
Flow control	Flow control of RS232 communication	Disabled
Packetized		
Silence	Time criteria for packetizing	2000
End character	End character criteria for packetizing	13
Inactivity time	Maximum inactivity time criteria in a connection	1
A Port connection		
Type of connection	Transport protocol used	TCP
Mode	Server or client	Server
Local port	Port used for listening connections	3000
Remote server IP	Server IP address to which equipment working in client mode will attempt to connect to	192.168.0.41
Remote server mode	Server port to which equipment working in client mode will attempt to connect to	1200
B Port connection		
Type of connection	Transport protocol used	TCP
Mode	Server or client	Client
Local port	Port used for listening to connections	2000
Remote server IP	Server IP address to which the equipment working in client mode will attempt to connect to	192.168.0.100
Remote server port	Server port to which the equipment working in client mode w ill attempt to connect to	1100