



IPL-RS232

IP router

User manual

Document reference : 9018009-01

The IPL-RS232 router is manufactured by

ETIC TELECOM
13 Chemin du vieux chêne
38240 MEYLAN
FRANCE

:

TEL : + 33 4-76-04-20-00
FAX : + 33 4-76-04-20-01
E-mail : hotline@etictelecom.com
web : www.etictelecom.com

OVERVIEW

1	PRODUCTS IDENTIFICATION.....	7
2	SPECIFICATIONS.....	8
3	PRODUCT OVERVIEW.....	10
3.1	Principles	10
3.2	Examples	11

INSTALLATION

1	PRODUCT DESCRIPTION	15
1.1	Leds	15
1.2	Connectors	16
1.3	DIP-switches	17
2	VENTILATION.....	17
3	SUPPLY VOLTAGE	17
4	ETHERNET INTERFACE.....	17
5	RS232 – RS485 INTERFACE	18
6	INPUT & OUTPUT	19

CONFIGURATION

1	SET UP STEPS	21
2	CONFIGURING THE IPL-RS232 ROUTER.....	21
2.1	Overview	21
2.2	First configuration	23
2.3	Modifying the configuration.....	24
3	REBOOTING THE ROUTER AFTER PARAMETERS CHANGES	24
4	RECOVERING THE IP ADDRESS OF THE ROUTER.....	24

../..

... CONFIGURATION

5	RECOVERING THE FACTORY CONFIGURATION	25
6	RESTRICTING ACCESS TO THE ADMINISTRATION SERVER	25
7	RECOVERING A FREE ACCESS TO THE ADMINISTRATION SERVER	25
8	ASSIGNING AN IP ADDRESS TO THE LAN INTERFACE	26
9	MODEM CONFIGURATION	26
10	CONFIGURING PPP CONNECTIONS BETWEEN IPL-RS232 ROUTERS	27
10.1	Principles	27
10.2	Outgoing PPP connection	30
10.3	Incoming PPP connection	32
10.4	Outgoing and ingoing PPP connection	34
11	SETTING UP A CONNECTION TO A 3G OR INTERNET OR TETRA NETWORK .	36
11.1	Step 1 : Step up the PPP connection	36
11.2	Step 2 : Adjusting routing parameters	36
12	CONFIGURING STATIC ROUTES	38
13	REMOTE USERS CONNECTION	40
13.1	Principle	40
13.2	Configuring a TLS remote user connection	41
13.3	Configuring a PPTP connection	42
13.4	Configuring the users list	43
14	RESTRICTING THE RIGHTS OF A REMOTE USER	45
14.1	Filter structure	45
14.2	Configuration	46

../..

... CONFIGURATION

15	CONFIGURING VPN CONNECTIONS BETWEEN ROUTERS (3G-GPRS-EDGE)	49
15.1	Principles	49
15.2	Configuring IPSec VPN connections	50
15.3	Configuring TLS VPN connections	56
16	SERIAL TO IP GATEWAY	62
16.1	Modbus gateway	63
16.2	RAW TCP gateway	66
16.3	Multicast gateway	68
17	ADVANCED FUNCTIONS	70
17.1	Alarms	70
17.2	Configuring the web portal	71

MAINTENANCE

1	DIAGNOSTIC	75
2	SAVING THE PARAMETERS FILE	76
3	UPDATING THE FIRMWARE	76

APPENDIX 1 : HTML configuration server

1 Products identification

	IPL-RS232	IPL-RS232-2
Ethernet 10 Mb/s	•	•
1 RS232-RS485	•	
1 RS232		•
1 digital output & 3 digital inputs	•	
PPP PAP & CHAP connection	•	•
PPP client or server	•	•
IP router (25 remote nodes)	•	•
Static routes s (30 routes)		
RAS server	•	•
Email Alarm-SMS	•	
HTML configuration	•	•

2 Specifications

General characteristics

Dimensions	128 x 38 x 107 mm (h, l, p)
Electrical safety	EN 60950- UL 1950
CEM	ESD : EN61000-4-2 : Discharge 6 KV RF field : EN61000-4-3 : 10V/m < 2 GHz Fast transient : EN61000-4-4 Surge voltage : EN61000-4-5 : 4KV line / earth
RoHS	2002/95/CE (RoHS)
Supply voltage	9 to 60 VDC - 125 mA at 24 VDC
Operating T°	-20°C / + 60°C Humidity 5 - 95 %

Ethernet / IP router

Ethernet	One Ethernet 10BT interface
IP router	Remote connections- static routes - RIP V2
Ip address translation	Source IP @ translation (NAT) Destination IP @ translation (DNAT) Port translation (Port forwarding)
DNS	Domain name
IP address assignment	Fixed IP @ or DHCP client or DHCP server

Security	
Connection	PPP connection Login & password Call-back
VPN	Client or server IPSEC or TLS/SSL or PPTP Encryption 3DES Certificate 509
Logs	Date and time stamped logs

Remote access server (RAS)	
User list	25 users
Connection	PPP connection Login & password call-back
Alarms	3 inputs : emails

Serial interface	
RS232	1200 - 115200 kb/s parity N / E / O
Serial to IP gateways	Modbus master and slave Raw client et server Telnet Multicast UDP multicast unitelway

3 Product overview

3.1 Principles

The IPL-RS232 is designed to interconnect safely automated devices through a telecom network.

A modem must be connected to the serial RS232 port of the IPL-RS232 router.

The connection is carried-out in two steps :

- 1st step : Modems connection
- 2nd step : PPP connection

1st step : Modems connection

The router controls the modem through the RS232 interface with AT commands.

If the network is a switched network like the PSTN or the ISDN the call command is sent to the modem each time IP packets have to be transmitted towards a remote router.

If the network is the 3G-GPRS service, or a TETRA radio network for instance, the modem connection is permanent as soon as the router is switched-on.

2nd step : PPP connection

Once the modem connection is set, a PPP connection is established.

If the telecom network is the PSTN or the ISDN or a leased line, the PPP connection is set with a remote IPL-RS232.

If the telecom network is the 3G-GPRS network or a radio network like TETRA, the PPP connection is set with a PPP server belonging to the infrastructure.

We present hereafter some examples of use of the IPL-RS232 router.

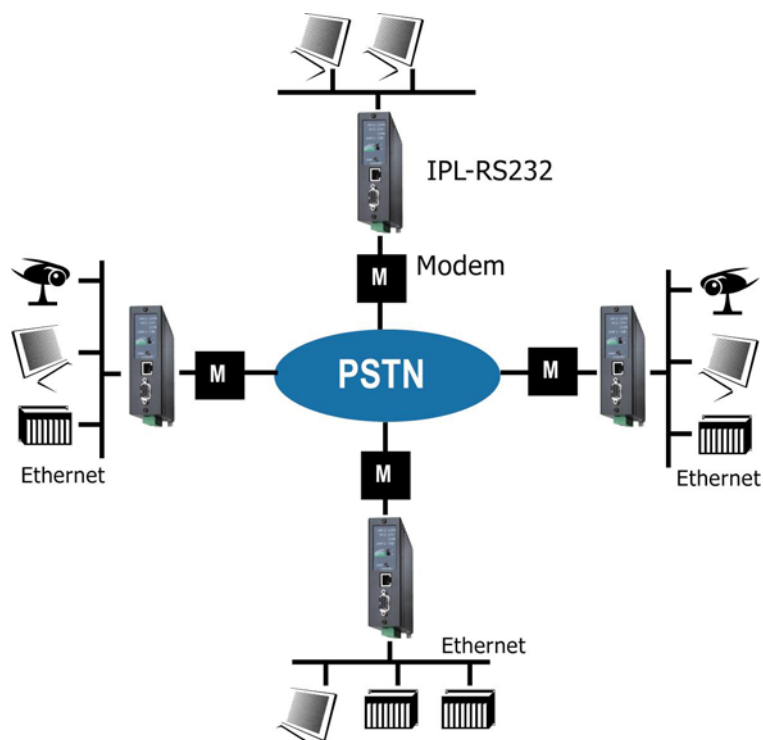
3.2 Examples

PSTN network :

Each router is connected to a PSTN modem (V34, V90 ...).

If the telecom provider offers the connection between the GSM network and the PSTN, some of the IPL-RS232 can also be connected to a GSM data modem instead of an ISDN adapter.

The PPP connection is set between IPL-RS22 routers.

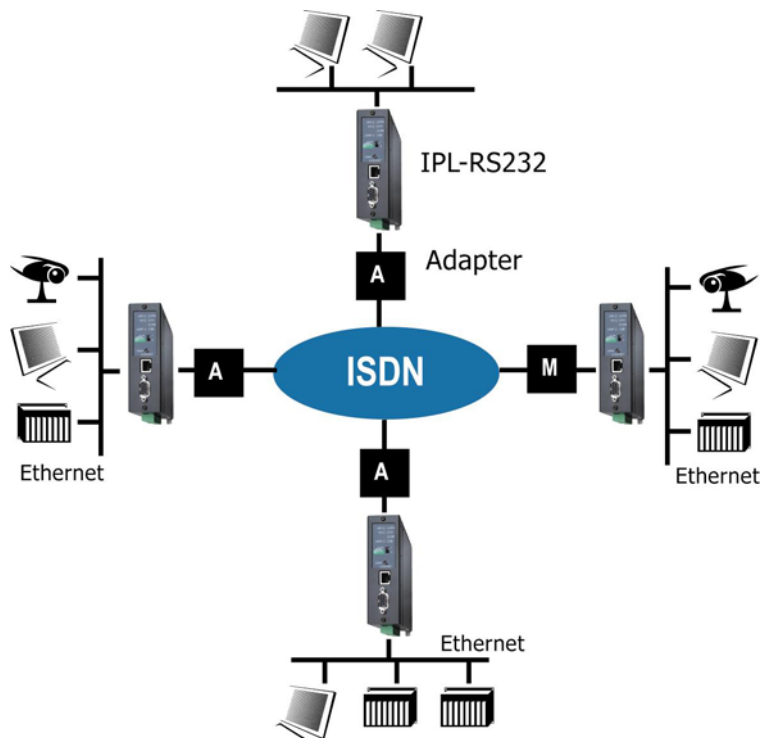


ISDN network :

Each router is connected to an ISDN adapter (V110 or V120).

If the telecom provider offers the connection between the GSM network and the ISDN, some of the IPL-RS232 can also be connected to a GSM data modem instead of an ISDN adapter.

The PPP connection is set between IPL-RS22 routers.

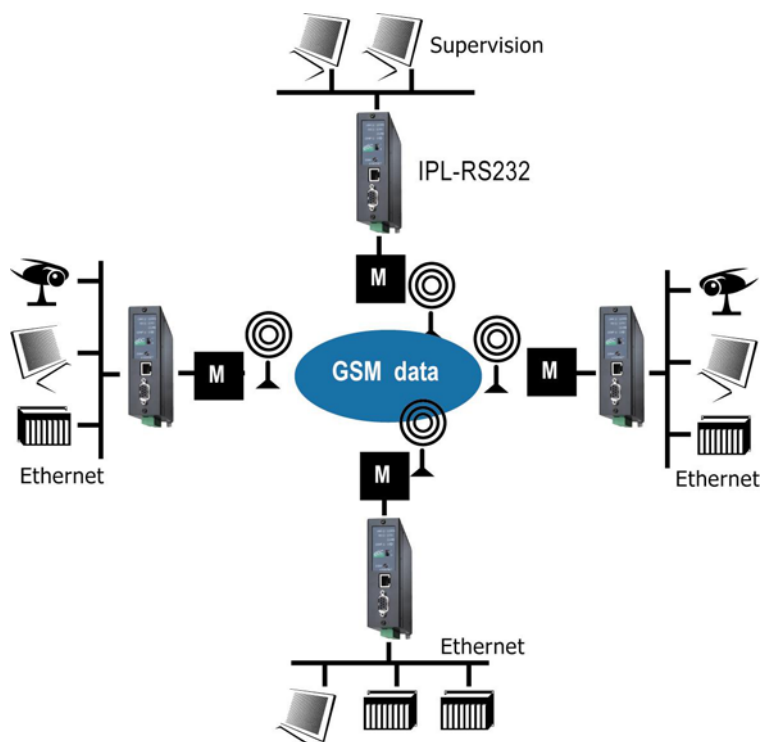


GSM-data service :

Each router is connected to a GSM-data modem.

If the telecom provider offers the connection between the GSM network and the PSTN, some of IPL-RS232 can also be connected to a PSTN modem instead of a GSM data modem.

The PPP connection is set between IPL-RS22 routers.



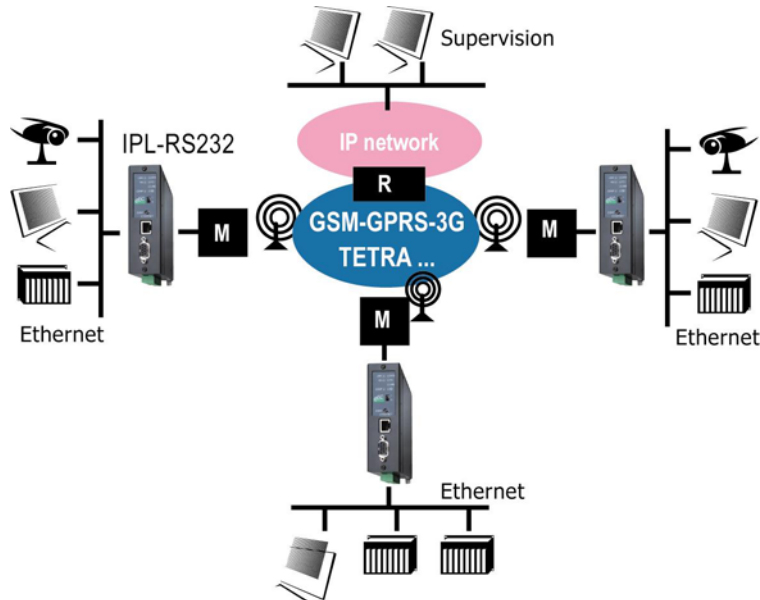
M = Modem GSM data

GPRS-EDGE or 3G or TETRA radio network :

Each IPL-RS232 router is connected to the appropriate modem (3G or TETRA...).

A PPP connection is set towards a PPP server belonging to the telecom infrastructure.

That PPP server is in charge of routing the IP packets towards its destination over a private IP network or the Internet.




M = GSM or TETRA modem

R = PPP server and IP router belonging to the telecom infrastructure.

1 Product description



1.1 Leds

	Function
Line	Lit : PPP Remote connection set Blinking : Remote connection in progress
VPN	Lit : One VPN at least has been established Blinking : VPN establishment in progress
LINK	Ethernet Interface connected
DATA	Data activity
RD	Bytes received from the modem
TD	Bytes transmitted to the modem
	Lit : Operation Blinking : Reset in progress or hardware defect

1.2 Connectors

pins screw-block : Supply voltage		
Pin	Signal	Function
1	+	9 to 40 VDC
2	-	Ground

8 pins : Inputs / outputs IPL-RS232 only		
Pin	Signal	Function
1	+	3 V DC provided by the IPL router
2	IN1	Digital input Nr 1
3	IN2	Digital input Nr 2
4	IN3	Digital input Nr 3
5	OUT1	Relay output 1
6	OUT2	Relay output 2
7	B +	RS485 polarity B
8	A -	RS485 polarity A

DB9 RS232 connector				
Pin	Circuit		Designation	IPL - Modem
1	CD	109	Carrier detect	⇒
2	RD	104	Data Reception	⇒
3	TD	103	Data Emission	⇐
4	DTR	108	Data terminal ready	⇐
5	GND	102	Ground	
6	DSR	107	Data set ready	⇒
7	RTS	105	Request to send	⇐
8	CTS	106	Clear to send	⇒
9	RI	125	Ring indicator	⇒

1.3 DIP-switches

DIP switches		
SW 1	SW 2	Management
OFF	OFF	The current IP@ of the product is the stored IP @
ON	OFF	The active IP@ of the product is the factory IP@ : 192.168.0.128 No login and password are required to access to the html server
OFF	ON	The active IP@ is provided by the BOOTP or DHCP server.
ON	ON	Reserved
SW3, SW 4		Not Used

Push-button : It enables to restore the factory profile.
To restore the factory profile, switch the power on while pressing the push-button until the RUN light turns green.

Attention : Once the factory profile has been restored, the stored configuration is lost.

2 Ventilation

To avoid overheating when the ambient temperature is high, leave a 1 cm (0.5 inch) space on each side of the product.

3 Supply voltage

The supply voltage must be strictly lower than 40 VDC and higher than 9 VDC. The consumption is 125 mA at 24 VDC.

4 Ethernet interface

The Ethernet interface is a 10 Mb/s interface.

To connect a PC directly to the router, use the cross wired red cable provided with the product.

5 RS232 – RS485 interface

The router provides a single serial interface made to connect a modem.

The modem is controlled by the IPL-RS232 using AT commands.

- **PL-RS232 model :**

The serial interface is at the same time RS232 and RS485 two wires.

The RS232 interface is available on a DB9 female connector.

The RS232 cable must not be longer than 10 meters.

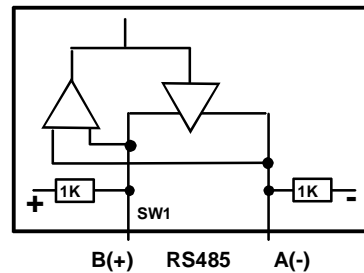
The RS485 serial interface is provided on the front panel 2 pins screw-block.

Polarisation resistors

1 Kohm bus polarisation resistors are included inside the product.

RS485 line adaptation

For a several meters long connection over the RS485 local interface, it is not necessary to adapt the RS485 line. For a longer distance, connect a 120 Ohm resistor at each end of the line.



- **IPL-RS232-2 model :**

The serial interface is an RS232 interface available on a DB9 male connector.

If the modem features a DB9 female connector, the cable between the IPL-RS232 router and the modem is a straight cable.

6 Input & output

The digital inputs and the output is featured by the IPL-RS232 model only.

Alarm output

1 relay output is provided to indicate an alarm.

The alarm condition can be selected using the html server.

The electrical characteristics of the output are :

Opto-isolated output

Maximum voltage : 50 VDC

Maximum current : 500 mA

Inputs

The product features one digital input ; it is not isolated.

if the input is opened, an SNMP trap will be sent to the SNMP server if that function has been enabled.



1 Set up steps

- Case the IPL-RS232 is used on a switched network like PSTN, ISDN, GSM data, private line

Step 1 : [Assign an IP address to the IPL-RS232 LAN interface](#)

Step 2 : [Set up the modem connection](#)

Step 3 : [Set up PPP connections with other routers](#)

:

- Case the IPL-RS232-2 is used on such networks as the 3G-GPRS network, the Internet or a radio TETRA network

Step 1 : [Assign an IP address to the IPL-RS232](#)

Step 2 : [Set up the modem connection](#)

Step 3 : [Set up the PPP connection](#) with the PPP server belonging to the infrastructure

Step 4 : [Set up VPNs](#) (if needed)

2 Configuring the IPL-RS232 router

2.1 Overview

Administration server address :

The administration html server is located at the LAN IP address of the router (The default address is 192.168.0.128).

Html browser :

We advise to use Internet Explorer version 8.

First configuration :

For the first configuration, we advise to connect the PC directly to the LAN interface of the IPL-RS232 router.

Modifications :

Modifications can be carried out from the LAN interface or remotely, using a RAS connection or through a VPN.

Restoring the factory IP address :

The factory IP address of the router on the LAN interface can be restored by setting the DIP switches SW01 ON and SW02 OFF.

In that position of the DIP switches, the stored configuration is not deleted.

Setting the DIP switches in that position gives also a free access to the administration server from the LAN interface.

During operations, the DIP switches must not be left in that position.

Network IP address :

Later in the text, we often speak of "network address".

We mean the lowest value of the addresses of the network.

For instance, if the netmask of a network is 255.255.255.0, the network address of that network is X.Y.Z.0.

Copy and paste :

Parameters must be entered with the keyboard; they cannot be pasted.

However, it can be useful to paste a string when it is long to avoid errors.

In that case, paste the string, delete the last character of the pasted string, and enter it again with the keyboard.

Saving and restoring the parameters file (see the maintenance chapter)

A parameters file can only be downloaded to a product having the same firmware version. It is why, we advise to assign a name to a parameter file including the product name and the software version like for instance "myrouterfile_ip1rs232_V241.bin".

DIP switches

Once the router has been set up, the DIP switches SW01 and SW02 must not be left in the "factory position" SW01=ON and SW02=OFF.

2.2 First configuration

Step 1 : Check the DIP switches

Coming from factory, the DIP switches SW1 and SW2 are set OFF to select the stored IP address.

Coming from factory, the stored IP address is the factory IP address 192.168.0.128.

Step 2 : Create or modify the PC IP connection.

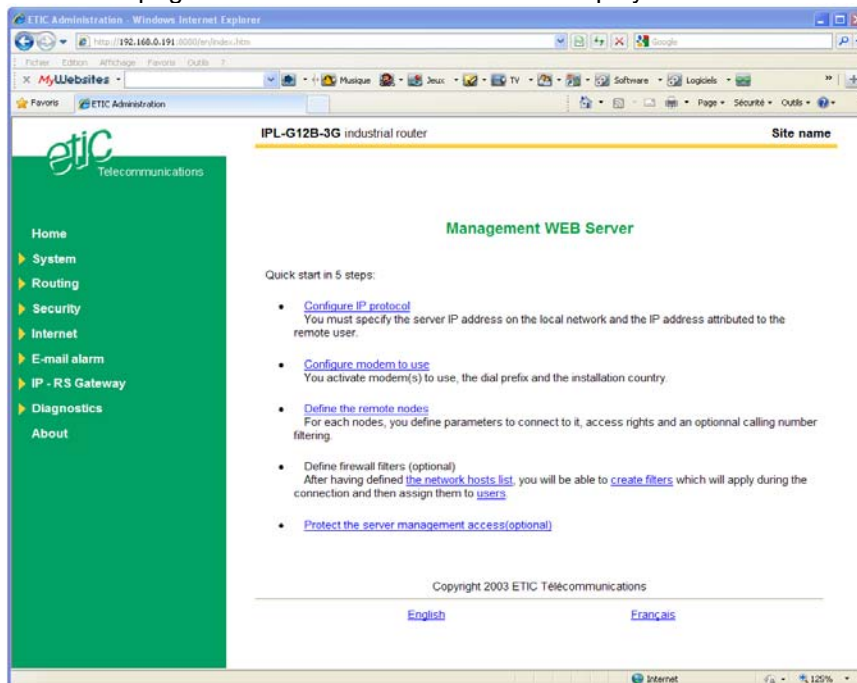
Assign to the PC an IP @ in accordance with the IPL-RS232 IP address. For the first configuration, assign or instance 192.168.0.127 to the PC.

Step 3 : Connect the PC directly to the LAN interface of the IPL-RS232 router using a cross wired Ethernet cable.

Step 4 : Launch the html browser

Enter the LAN IP @ of the router 192.168.0.128.

The Home page of the administration server is displayed



2.3 Modifying the configuration

From the local network :

- Launch the html browser and enter the IP address assigned to the router on the LAN
- Or, launch the ETICFINDER utility if you ignore the IP address assigned to the router.

Remotely :

- If no VPN is set with the router, set a RAS (PPTP, TLS, L2TP/IPSec) connection towards the router if a public Ip address is assigned to its "antenna" interface.
- Launch the html browser and enter the IP address assigned to the router on the LAN.

3 Rebooting the router after parameters changes

- After a page of parameters has been completed, click the « Save » button located at the bottom of the page.
- After some parameters changes, the IPL-RS232 must restart. When the configuration has been completely carried out, click the « **Reboot** » red button in the green bar, when displayed.
- Once the product has restarted, check the « **Reboot** » button has disappeared from the green bar.

To save the configuration file to a hard disk :

- Select the "maintenance" menu and then the "Save / restore" menu.
- Click the "Save current configuration to disk" button.

4 Recovering the IP address of the router

if the IP address you enter is wrong, it is possible to recover the factory IP address of the IPL-RS232 router by setting SW01 ON and SW2 OFF.
The factory IP address 192.168.0.128 will be restored as long as the SW01 and SW02 micro-switch will be left in that position.

Remark :

The SW01 and SW02 must not be left in that position during operations.

5 Recovering the factory configuration

It may be necessary to restore the factory configuration of the router.

To restore the IPL-RS232 factory configuration,

- Switch OFF the power supply of IPL-RS232 router.
- Press the push-button on the top part of the IPL-RS232 router and switch ON the power supply.
- Keep the push-button pressed until the Operation led turns red.

Remark : The stored configuration will be lost; the factory IP address 192.168.0.128 will be restored.

6 Restricting access to the administration server

The access to the administration server can be protected by a login and password.

To protect access to the administration server,

- Select the "Set up" menu, the "Security" menu and then the "Administration menu".

Remark : For more simplicity, we advise to chose the login and the password of one of the remote users stored in the user list.

7 Recovering a free access to the administration server

If the Login & or password entered to reach the administration server have been rejected, it is possible to recover a free access to the administration server from the LAN only, by setting SW01 ON and SW2 OFF.

Remark :

The factory IP address 192.168.0.128 will also automatically be restored as long as SW01 will remain ON and SW2 OFF.

During normal operations SW01 and SW02 must not be left in that position.

8 Assigning an IP address to the LAN interface

- Click « **System** » and then « **IP** protocol ».

Local network parameters :

IP address :

Enter the IP address assigned to the router over the Ethernet local network.

Remark : Different IP addresses must be assigned to each network connected through IPL-RS232 routers.

Netmask :

Enter the IP netmask assigned to the local network.

Remote access parameters :

Start of users IP address pool and end of users IP addresses pool :

These parameters define the pool of addresses which will be assigned automatically to remote user's PC when they will connect to the router. Enter the start address and the end address.

9 Modem configuration

- Select the “System” menu and then “Modem”.

« activate » parameter :

Select that checkbox if a modem is connected to the serial interface.

« Dial prefix » parameter :

If the modem is connected to a PBS, for instance, enter the prefix which it has to dial.

« Permanent link » parameter :

Select that checkbox if the modem connection is permanent, and if no number has to be dialed over the line.

« Use custom initialisation string » parameter :

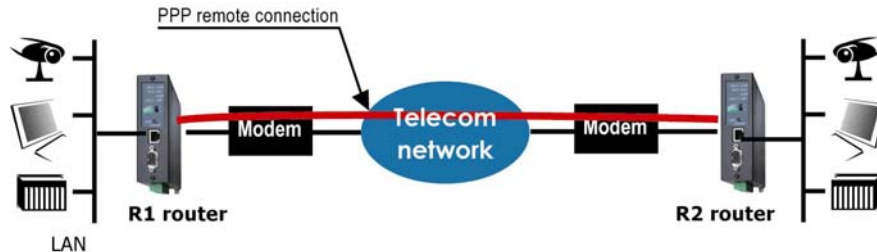
Enter the necessary initialisation string.

« Report connection state on the digital output. » :

If that checkbox is selected, the digital output is closed when the modem is connected.

10 Configuring PPP connections between IPL-RS232 routers**10.1 Principles**

An IPL-RS232 router must establish a PPP connection with each router it has to connect to.



In each router, PPP connections must be set up to register the parameters of each connection (Dial number, remote LAN IP address, password ...).

A PPP connection with a remote router can be an outgoing connection or an ingoing connection or an outgoing and ingoing connection.

If a connection is an outgoing connection, the local IPL-RS232 router dials towards the remote router when IP packets have to be transmitted.

If a connection is an ingoing connection, the local IPL router waits for a call from the remote router. It cannot dial towards that remote router.

If a connection is an outgoing and ingoing connection, the local IPL dials towards the remote router. It can also accept a call coming from that router.

When a connection has been registered as an outgoing connection inside a router, it has to be registered as an ingoing connection in the remote one.

The addresses of each network connected through the IPL-RS232 routers must be different IP networks.

For instance, referring to the diagram below, the following connections must be created :

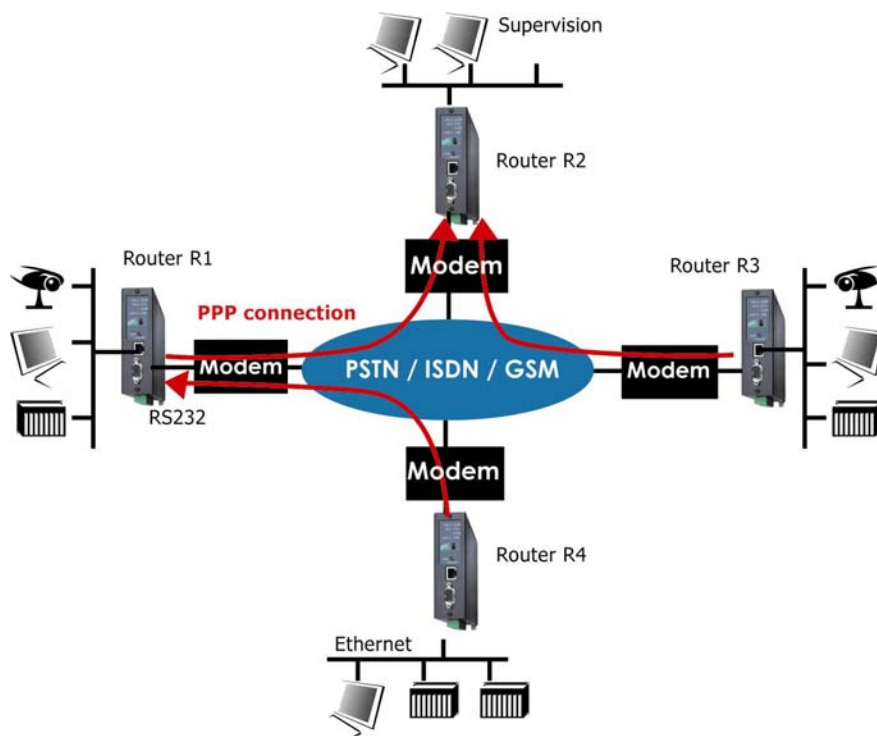
Router R1 : An outgoing connection to R2 and an incoming connection from R4

Router R2 : An ingoing connection from R1 and another one from R3

Router R3 : An outgoing connection to R2

Router R4 : An outgoing connection to R1

- To add and configure a remote node, select the “Routing” menu and then “Remote nodes”.
- Click the” Add a node” button.



10.2 Outgoing PPP connection

An outgoing connection is a connection set by the router itself towards a remote router.



- To add and configure a remote connection, select the “Routing” menu and then “Remote nodes”.
- Click the “Add a node” button.

“Enable” parameter :

Select the “yes” option.

“Type” parameter :

Select the “switched” choice.

“Node name” parameter :

Assign a name to the node.

“call direction” parameter :

Select “Outgoing” if the router must dial towards the remote router.

“Remote router IP @” and “Remote network netmask” parameter :

Enter the IP address and the netmask of the remote router Ethernet interface.

“Modem” parameter :

The “external” choice is the only possible.

“Dial number” parameter :

Enter the number the router has to dial to connect to the remote router.

“My login” and “My password” parameters :

Enter the login and the password the router has to transmit to the remote router to connect to it.

“Idle time-out” parameter (5 s to 60 mn) :

Set the time duration of the silence before the router will clear the call.

“First packet time-out” parameter (5 s to 60 mn)

Leave the default value.

Additional parameters :**“Firewall filter” parameter :**

Select the firewall filter assigned to the connection.

“NAT” parameter :

Select “yes” to enable source IP address translation.

In that case, the PPP the source address of any IP packet transmitted by a device towards the telecom network is replaced by the IP address of the router on the PPP connection.

If no PPP IP address has been entered, it is replaced by the IP address of the router over the Ethernet interface.

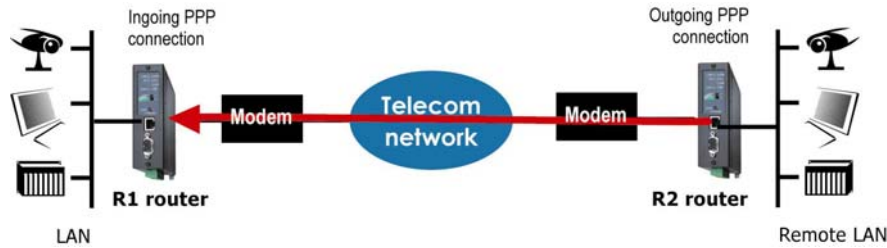
“Router PPP IP address ” and “Remote router PPP IP address” parameters :

Enter the IP address assigned to the PPP interface.

If no IP address is entered, the address of the Ethernet interface is assigned automatically.

10.3 Incoming PPP connection

An incoming connection is a connection established by the remote router.



- To add and configure an ingoing connection, select the “Routing” menu and then “Remote nodes”.
- Click the “Add a node” button.

“Enable” parameter :

Select the “yes” option.

“Node name” parameter :

Assign a name to the connection (for instance, the name of the remote site).

“call direction” parameter :

Select “Ingoing” if the router waits from an incoming call from the remote router.

“Remote router IP @” and “Remote network netmask” parameter :

Enter the IP address and the netmask of the remote router Ethernet interface.

“Node login” and “Node password” parameters :

Enter the login and the password of the remote router. These login and password are checked by the router when a call is incoming.

Additional parameters :

“Verify calling number” and “calling number” parameters :

Select the option “yes” and Enter the telephone number of the remote router to force the router to check the calling number.

“Firewall filter” parameter :

Select the firewall filter assigned to the connection

“NAT” parameter :

Select “yes” to enable the NAT function.

In that case, the PPP IP address of the router is assigned as the source address to all IP packets transmitted by a device towards the telecom network.

If no PPP IP address has been entered, it is replaced by the IP address of the router over the Ethernet interface.

“Router PPP IP address ” and “Remote router PPP IP address” parameters :

Enter the IP address assigned to the PPP interface.

If no IP address is entered, the address of the Ethernet interface is assigned automatically.

10.4 Outgoing and ingoing PPP connection

A connection must be set up as outgoing and ingoing if the router can dial to a remote router and receive a call from that remote router.

- To add and configure an ingoing and outgoing connection, select the "Routing" menu and then "Remote nodes".
- Click the "Add a node" button.

"Enable" parameter :

Select the "yes" option.

"Type" parameter :

Select the "switched" choice.

"Node name" parameter :

Assign a name to the node.

"call direction" parameter :

Select "Outgoing + ingoing" if the router must dial towards the remote router and receive calls from that remote router.

"Remote router IP @" and "Remote network netmask" parameter :

Enter the IP address and the netmask of the remote router Ethernet interface.

"Modem" parameter :

The "external" choice is the only possible.

"Dial number" parameter :

Enter the number the router has to dial to connect to the remote router.

"My login" and "My password" parameters :

Enter the login and the password the router has to transmit to the remote router to connect to it.

"Node login" and "Node password" parameters :

Enter the login and the password of the remote router. These login and password are checked by the router when a call is incoming.

"Idle time-out" parameter (5 s to 60 mn) :

Set the time duration of the silence before the router will clear the call.

“First packet time-out” parameter (5 s to 60 mn)

Leave the default value.

Additional parameters :

“Firewall filter” parameter :

Select the firewall filter assigned to the connection.

“NAT” parameter :

Select “yes” to enable source IP address translation.

In that case, the PPP the source address of any IP packet transmitted by a device towards the telecom network is replaced by the IP address of the router on the PPP connection.

If no PPP IP address has been entered, it is replaced by the IP address of the router over the Ethernet interface.

“Router PPP IP address ” and “Remote router PPP IP address” parameters :

Enter the IP address assigned to the PPP interface.

If no IP address is entered, the address of the Ethernet interface is assigned automatically.

11 Setting up a connection to a 3G or Internet or Tetra network

The IPL-RS232 router can be used to connect the devices of the LAN interface to a remote network through a telecom network like the 3G-GPRS network or the Internet or a radio network like a TETRA network.

The IPL-RS232 must set a PPP connection towards the PPP server belonging to the telecom infrastructure.

The configuration is carried-out in two steps :

- Step 1 : Setting up the PPP connection
- Step 2 : Setting up technical routing parameters

11.1 Step 1 : Set up the PPP connection

- Select the « **Internet** » menu and then click « **Account** ».

“Activate Internet connection” parameter :

Select the “by modem” choice.

“User name” & “password” parameters :

Enter the user name and password assigned to the Ipl-RS232 router by the telecom provider.

Careful : If no user name or password are assigned by the GSM operator, it may be necessary to enter at least an alphabetic character in each field.

“Authentication” parameter :

Unless particular difficulties, leave the default value “PAP/CHAP”.

“Outgoing mail server” and “account email address” parameters :

If emails have to be transmitted, enter the parameters.

11.2 Step 2 : Adjusting routing parameters

- Select the « **Internet** » menu and then click « **Routing** ».

“Route LAN traffic to Internet ” parameter :

Select that checkbox.

“Idle time-out” parameter (5 s to 60 mn) :

If no IP packets have to be transmitted, and after the idle time-out, the router clears the connection.

“First packet time-out” parameter (5 s to 60 mn) :

Leave the default value.

“Use modem” parameter :

Select “External”.

12 Configuring static routes

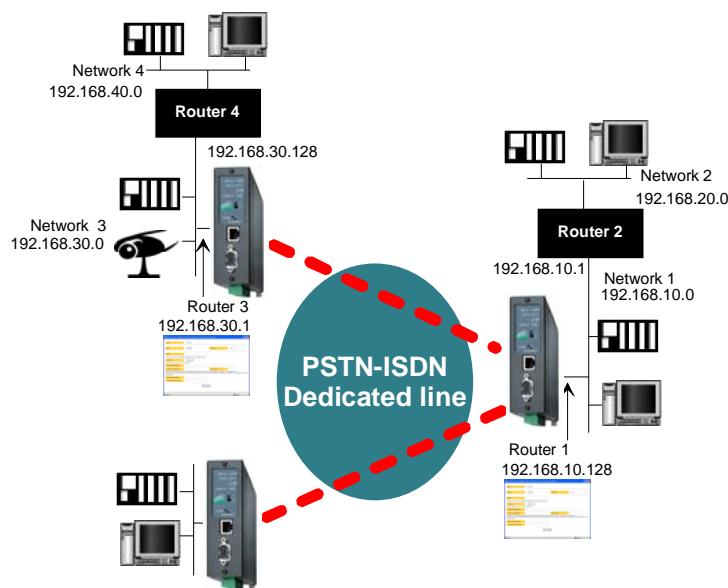
If the destination network is not connected to one of the remote routers linked to the router by a remote connection, the devices of that destination network cannot be reached.

In that case, it is necessary to enter the route to that hidden network; that route is called a static route.

A static route consists in a table which describes a destination network (IP address and netmask) and the IP address of the router through which an IP frame intended for that hidden network must pass.

That router can be one of the routers connected directly to the local network or a router connected to a remote network.

Example :



Router 1 static route :

Active	Route name	Destination	Netmask	Gateway
Yes	Network 2	192.168.20.0	255.255.255.0	192.168.10.1

Router 3 static routes :

Active	Route name	Destination	Netmask	Gateway
Yes	Network 4	192.168.40.0	255.255.255.0	192.168.30.128
Yes	Network 2	192.168.20.0	255.255.255.0	192.168.10.128

Select the "Routing" menu and click "Static routes"; click the "Add a route" button.

"Destination IP address" & "netmask" parameters :

Enter the destination network IP address and netmask.

"Gateway IP address" parameter :

Enter the Ip address of the gateway through which the IP frames intended for that network must pass.

13 Remote users connection

13.1 Principle

The IPL provides a remote user connection function called "RAS".

A RAS connection is a tunnel set between a remote PC and the IPL-RS232 router through the telecom network

RAS connection safety :

When a remote PC sets a RAS connection with the router,

- the remote user is identified with a login-in and a password or eventually a certificate.
- The data is encrypted.
- An IP address belonging to the local network is automatically assigned to the remote user's PC.

RAS connection types :

The IPL-RS232 manages PPTP and TLS or L2TP remote connections.

Only one type can be selected. It will apply to all the remote users connections.

13.2 Configuring a TLS remote user connection

- Select the "Security" menu, click "VPN connections" and then "VPN parameters";
- select the "Remote users connection VPN type" value : TLS;
- click the "Properties" Button and set the parameters.

Step 1 : Router configuration

"Port number" & "Protocol" parameters :

Select the port Nr and the type of protocol used to transport the TLS VPN; UDP will be preferred.

Attention :

The selected port number assigned to the remote users connections must be different from the one used for VPN connections between routers if such VPN connections have been configured.

"Users authentication" parameter:

Authentication and encryption can be carried-out with a pre-shared key or a certificate.

If the "Login/password" is selected, the remote user is authenticated with a login and a password.

If the "Login/password and Certificate" value is selected, the remote PC is authenticated with the certificate and the user with a login and password. In that case, the PC certificate must be stored in the user list.

«Encryption algorithm» & «Message digest algorithm» parameters:

Leave the default values

Step 2 : Configure the M2Me_Secure software

- Click « Menu » and then « New site ». The Site configuration window is displayed.
- Select the « General » tab and enter a site name.

- Select the « Connection » tab; select the option "That site can be reached through the Internet."
- In the field « Host name or IP address », select the router IP address or DynDNS name or DNS name.
- Select the « Advanced tab » ; select the protocol (UDP or TCP), the port number and the encryption algorithm.
The same values of that parameters must be assigned to the PC and to the router.

13.3 Configuring a PPTP connection

Step 1 : Router configuration

- select the "Security" menu, click "VPN connections" and then "VPN parameters";
- select the "Remote users connection VPN type" value : PPTP

Step 2 : Set a PPTP connection on the PC side.

13.4 Configuring the users list

The IPL router registers a users list; 25 remote users can be stored in the users list.

Each user form stores the identity of the user (Login and password), his email address to send alarm emails and the filter assigned to him.

To display the user list, select the “System” menu and then “User list”.

Attention :

Coming from factory, a default user is registered; his login is **admin** and the password is also **admin**. After the test phase, we advise to modify these login and password.

Select the “System” menu and then “User list”.

Display or modify a user entry

- Click the “View” or “modify” button

Add a user

- Click the “add a user” button.

Active (value Yes or NO) :

Choose No if you want to prevent the user to access the network.
Choose yes to authorize the user to access the network.

“Full name” parameter :

It is the name displayed in the user list.

“Login” & “password” parameters :

The login and the password will have to be entered by each user at the beginning of the remote connection.

“E-mail” parameter :

The IPL-RS232 router will send an email to that address in two situations :

Alarm email : the router sends an alarm email to the user's email address If the status of one of the three inputs is closed or opened (if that option has been set).

Internet connection email : Once connected to the Internet, the router will send to the demanding user an email containing the dynamic IP @ assigned to the router by the provider.

“Firewall filter” parameter :

Select the filter to assign to the user to restrict his access rights.

14 Restricting the rights of a remote user

A remote user filter applies to the IP frames received from an authenticated remote user.

Once the user has been authenticated and the PPP connection or the has been set, the router applies the filter assigned to the user who has been recognized; the remote user filter checks the destination IP address and port number.

25 remote user filters can be configured and assigned individually to each of the users declared in the user list.

14.1 Filter structure

A filter is a table made of several lines; each line is called a rule.

A rule defines what decision the filter has to make when it receives a particular IP frame from the Internet; the decision can be Reject or Authorize.

Each rule of the filter is composed a two fields which defines a data flow :

- Service : Protocol (telnet, http...),
- Host : destination IP@.

To avoid to be obliged to describe what the filter has to do with any possible data flow, the filter policy has to be selected.

The filter policy is the policy the firewall has to apply when it encounters an IP frame not described by one of the rules of the filter.

The policy can be

- "Drop all the IP frames not described by one of the rules";
- or
- "Accept all the IP frames not described by one of the rules".

The first policy is generally the right one because it is cautious.

14.2 Configuration

Step 1 : Complete, if necessary, the list of TCP ports.

Important nota bene : The main services (html, ftp, modbus) are available from factory; for that reason, most of the time, that step can be skipped.

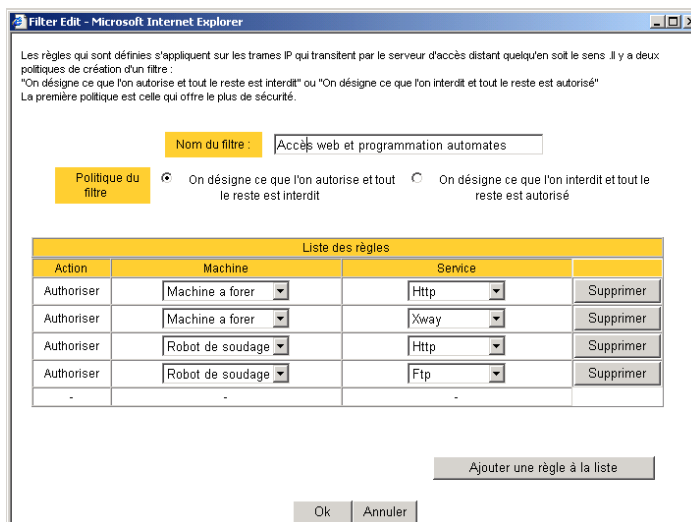
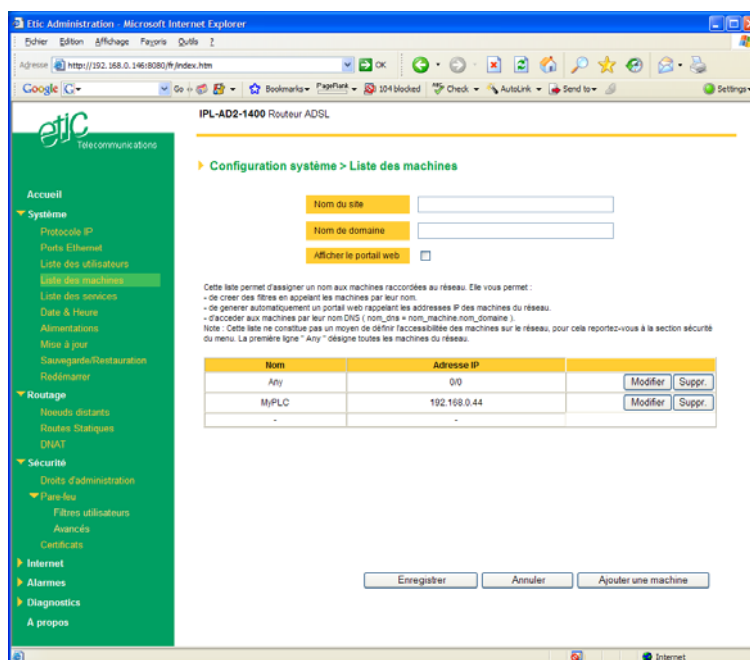
- Select the menu “system” and then “service list” The list of TCP ports is displayed.
- Click « add a service ».
- Enter the label of that the new service, assign a protocol (udp, tcp, icmp) and a port number.
- Save. The list is updated.

Step 2 : Enter the list of the devices connected to the LAN

- Select the «System» menu, then «Devices list». The list of the devices of the LAN network is displayed.
- Click « add a device ».
- Assign a label and an IP address to the device and click OK.

Step 3 : Build a filter

- Select the « security» menu, then « firewall» and then «Filter list» The list of the stored filters is displayed.
- Click « add a new filter ».
- Assign a name to the new filter.
- Choose the policy ; « All is forbidden except what we specify » is the advised policy.
- Click « add a new rule to the list ».
- Select a host (also called machine or IP address) among the ones which have been stored and a service (also called TCP port).
- Add other rules if necessary.
- Click OK when the filter is complete ; the updated filters list is displayed.



Step 4 : Assign a filter to each user

- Select the « System» menu and then « Users list ».
- Select the user to which you want to assign a filter ; and click modify ; the user window is displayed.
- Assign a filter to the user ; click OK and save.

15 Configuring VPN connections between routers (3G-GPRS-EDGE)

15.1 Principles

A VPN is a safe link set between two end-points over an IP network : Both routers authenticate, data are encrypted and each device of a LAN can exchange data with each device of the other one.

To get more explanations about how VPNs work, refer to appendix 2.

25 VPNs can be set on the WAN interface of the IPL-RS232 router.

Two types of VPN can be set : TLS VPN and IPSec VPN.

IPSec has the advantage to be a standard solution.

TLS is easier to employ because the transport layer is TCP or UDP; it is why, it can be easily used when the VPN must pass through several company routers.

Once a type of VPN (TLS or IPSec) has been selected, all the VPN set between the IPL-RS232 router and another one must be the same.

Two steps are necessary to configure the IPL-RS232 to create VPN connections between routers :

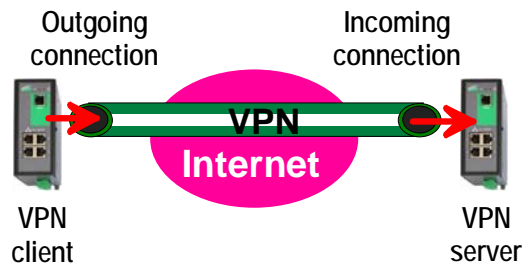
1st step : Select and set up the VPN type parameters

Once a type of VPN has been selected, it applies to all the connections with remote routers.

2nd step : Create VPN connections

A VPN connection can be an incoming connection or an outgoing connection.

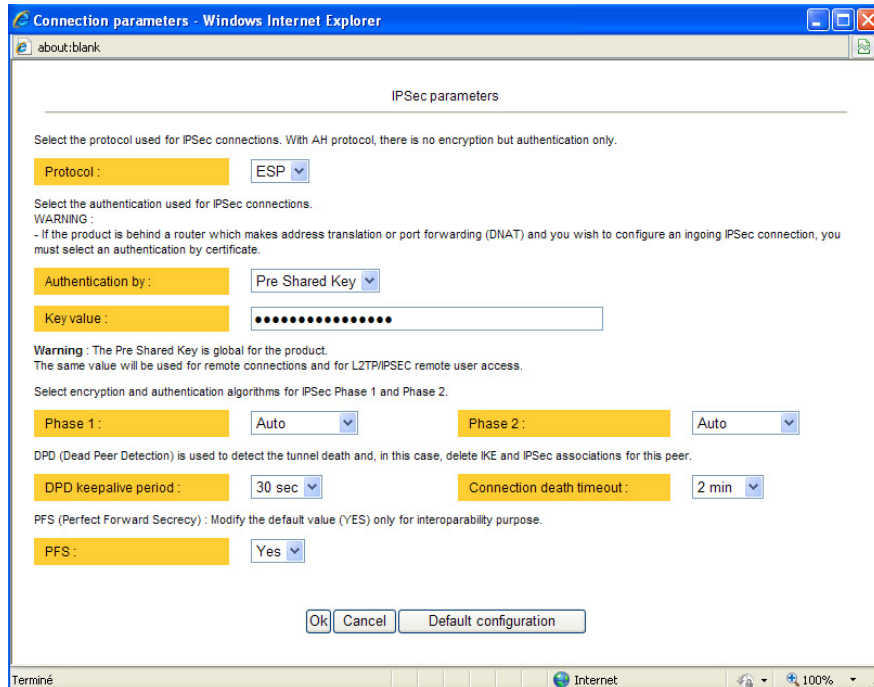
If a VPN connection is an incoming connection, the local router is named "VPN server" and the remote router is a "VPN client".



15.2 Configuring IPSec VPN connections

15.2.1 Configuring the IPSec protocol

- Select the “Security” menu, click ‘VPN connections’ and then “VPN parameters”.
- Select the “Remote nodes connections VPN type” value “IPSEC” and then click “Properties” .



Connection parameters - Windows Internet Explorer

about:blank

IPSec parameters

Select the protocol used for IPSec connections. With AH protocol, there is no encryption but authentication only.

Protocol : ESP

Select the authentication used for IPSec connections.

WARNING :

- If the product is behind a router which makes address translation or port forwarding (DNAT) and you wish to configure an incoming IPSec connection, you must select an authentication by certificate.

Authentication by : Pre Shared Key

Key value :

Warning : The Pre Shared Key is global for the product.
The same value will be used for remote connections and for L2TP/IPSEC remote user access.

Select encryption and authentication algorithms for IPSec Phase 1 and Phase 2.

Phase 1 : Auto Phase 2 : Auto

DPD (Dead Peer Detection) is used to detect the tunnel death and, in this case, delete IKE and IPSec associations for this peer.

DPD keepalive period : 30 sec Connection death timeout : 2 min

PFS (Perfect Forward Secrecy) : Modify the default value (YES) only for interoperability purpose.

PFS : Yes

Ok Cancel Default configuration

Terminé Internet 100%

“Encryption Protocol” parameter :

Select ESP to encrypt the data flow; select AH, if no encryption is required or if NAT traversal is required.

“Authentication” & “encryption key” parameters :

Authentication and encryption can be carried-out with a pre-shared key or a certificate.

“Pre-shared key” value :

The pre-shared key value applies to all the connections.

The maximum length of the key is 40 characters.

The same preshared key value will be used for remote users L2TP / IPSec connections.

“Certificate” value

The IPL- RS232 router is delivered with a certificate stored into the product in our factory.

To add a certificate, refer to the “Security” menu.

“Encryption and hash algorithm phase 1” & “Encryption and hash algorithm phase 2” parameters :

That parameters allow to define the encryption and hash algorithms in use during the phase 1 of the exchanges between the end-points (VPN set-up) and during the phase 2 (data exchange).

The default value is Auto; in that case both end-points will negotiate a common algorithm.

“DPD request period” parameter :

A DPD request (also called Keepalive message) is a message sent periodically by each end-point to the other one to make sure that the VPN must be left active.

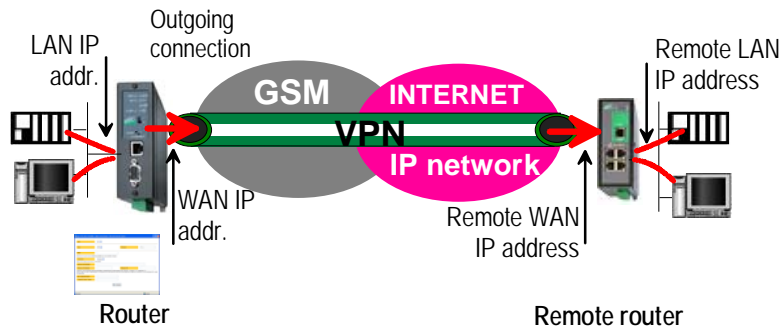
This parameters sets the amount of time (in seconds) between two of these requests.

“Connection death time-out” parameter :

This parameter defines the maximum amount of time (in seconds) a VPN connection will stay established if no traffic or no DPD request message are received from the remote point.

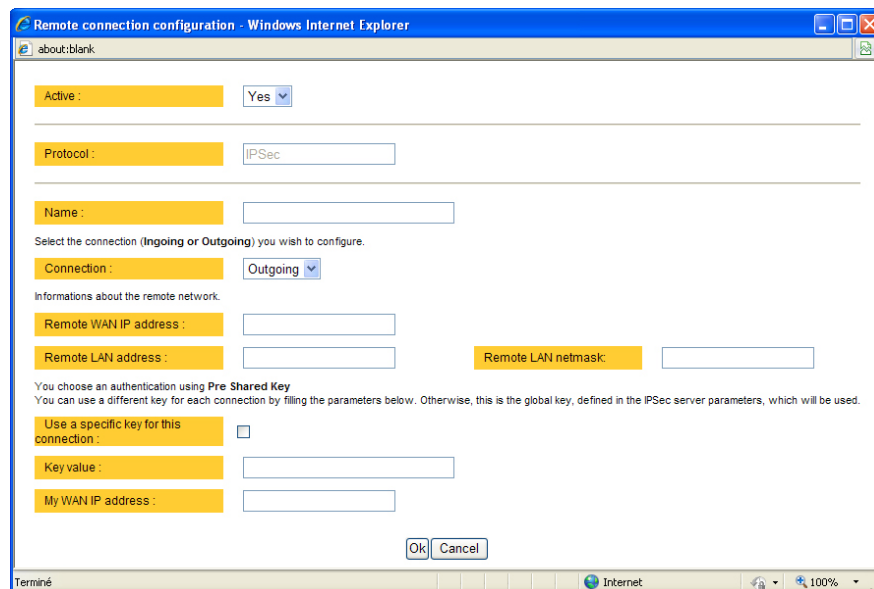
ATTENTION : Once the parameters of the IPSEC connection have been selected, click the OK button and then the Save button.

15.2.2 Configuring an outgoing IPSec connection



To set an outgoing IPSec VPN connection,

- Select the “Routing” and then the “Remote nodes” menu.
- Click the “add a node” button.
- Give a name to the connection and select the **“Outgoing”** option.



‘Remote WAN IP address’ parameter :

Enter the network IP address and the netmask assigned to the remote router over the internet.

“Remote LAN address” & “Remote LAN netmask” parameters :

Enter the network IP address and the netmask assigned to the remote LAN.

- **Case a Preshared key (PSK) is used for authentication**

If the preshared key used by the connection is the general PSK entered in the “VPN” menu, no additional parameter has to be entered.

If a particular PSK must be used, complete the configuration of the connection as explained below.

“Unique PSK for this node” parameter :

Select that option if a particular PSK key has to be used for this connection.

“PSK value” parameter :

Enter the value of the PSK.

“My WAN address” parameter :

Enter the IP address of the router on the GPRS interface.

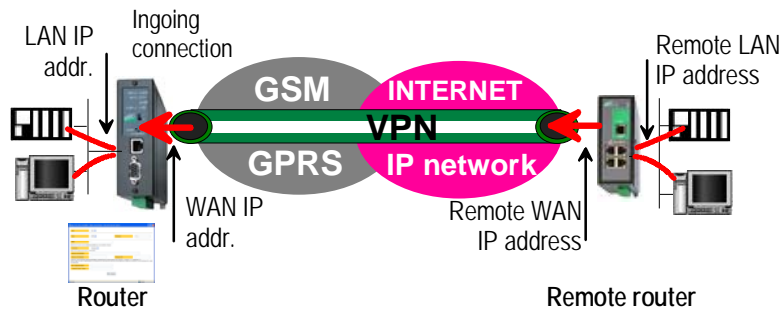
- **Case a certificate is used for authentication**

“My subjectAlt name” & “Remote subjectAlt name” parameters :

Paste the field "SubjectAltName" of the active certificate of the router you are configuring and the one the remote router.

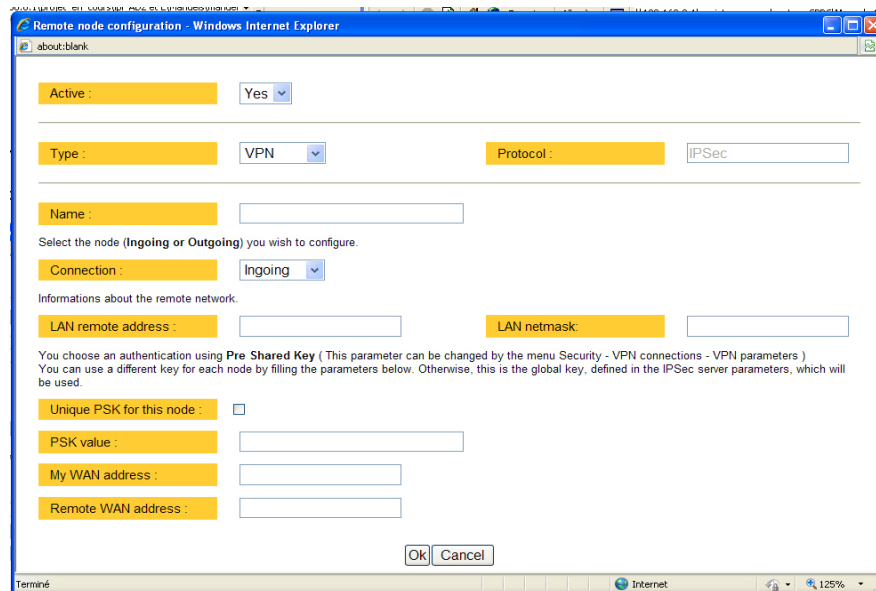
Attention : For ETIC certificates, this field is the Email field

15.2.3 Configuring an incoming IPSec connection



To set an incoming IPSec VPN connection,

- Select the “Routing” and then the “Remote nodes” menu.
- Click the “add a node” button.
- Give a name to the connection and select the **“incoming” connection direction option**.



“Remote WAN IP address” parameter :

Enter the IP network address and netmask assigned to the remote router over the Internet (public IP address over Internet).

“Remote LAN address” & “Remote LAN netmask” parameter :

Enter the IP network address and netmask assigned to the remote LAN.

- **Case a preshared key is used**

If the key used by the connection is the general PSK entered in the VPN menu, no additional parameter has to be entered.

If a particular PSK must be used, complete the configuration of the connection as explained below.

“Unique PSK for this node” parameter :

If that option is not selected, the preshared key entered in the VPN configuration screen will be used by the router.

If that option is selected, enter the specific key.

“My WAN address” & “Remote WAN address” parameters :

Enter the WAN IP address of the IPL- RS232 router (public IP address over Internet) and the WAN IP address of the remote router.

- **Case a certificate is used for authentication**

“My subjectAlt name” & “Remote subjectAlt name” parameter :

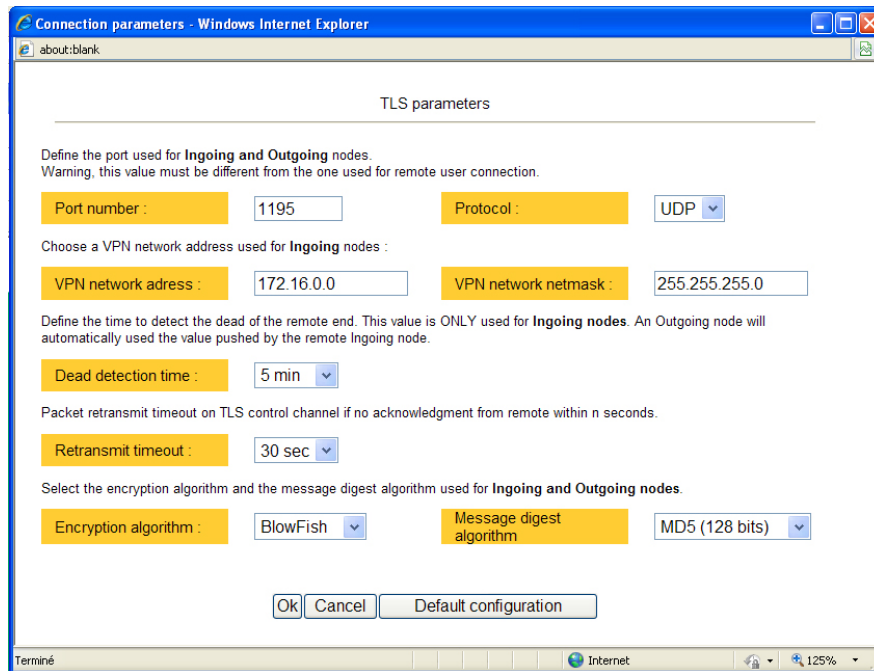
Paste the field "SubjectAltName" of the active certificate of the router you are configuring and the one the remote router.

Attention : For ETIC certificates, this field is the Email field.

15.3 Configuring TLS VPN connections

15.3.1 Configuring the TLS protocol

- Select the “Security” menu, click ‘VPN connections and then “VPN parameters”.
- Select the “Remote nodes connections VPN type” value “TLS” and then click “Properties” .



Connection parameters - Windows Internet Explorer

about:blank

TLS parameters

Define the port used for **Ingoing and Outgoing** nodes.
Warning, this value must be different from the one used for remote user connection.

Port number : 1195 Protocol : UDP

Choose a VPN network address used for **Ingoing** nodes :

VPN network address : 172.16.0.0 VPN network netmask : 255.255.255.0

Define the time to detect the dead of the remote end. This value is **ONLY** used for **Ingoing nodes**. An Outgoing node will automatically used the value pushed by the remote Ingoing node.

Dead detection time : 5 min

Packet retransmit timeout on TLS control channel if no acknowledgment from remote within n seconds.

Retransmit timeout : 30 sec

Select the encryption algorithm and the message digest algorithm used for **Ingoing and Outgoing** nodes.

Encryption algorithm : BlowFish Message digest algorithm : MD5 (128 bits)

Ok Cancel Default configuration

Terminé Internet 125%

“Port number” & “protocol” parameters :

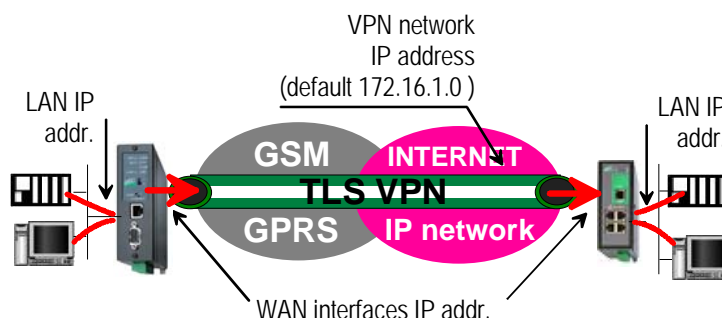
Select the port Nr and the type of protocol used to transport the TLS VPN; UDP will be preferred.

Attention : The port number value must be different from one used by remote users; to configure the **VPN dedicated to remote users** select the “Security” and then VPN menu.

“VPN network address” & “VPN network netmask” :

The TLS VPN server router assigns automatically an IP address to the VPN client router.

That VPN network IP address must not be confused with the WAN IP address (the public IP address assigned to the routers over the Internet) nor with the LAN IP addresses.



Attention :

The VPN network IP address field must be different from LAN IP address field.

The number of VPN addresses cannot be greater than 255; the netmask cannot exceed 255.255.255.0.

“Connection death time-out” parameters :

This parameter defines the maximum amount of time (in seconds) a VPN connection will stay established before being cleared if no response to the VPN control message has been received from the remote router.

“Repetition time-out” parameter :

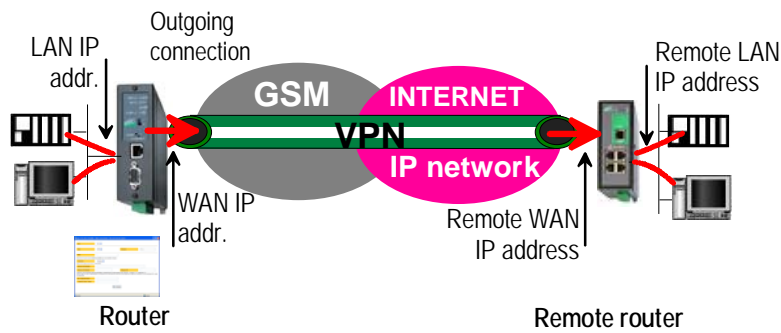
A control message (also called Keepalive message) is sent periodically by the VPN server router to make sure that the VPN must be left active.

This parameters sets the amount of time (in seconds) the server will wait for the response before repeating it.

“Encryption algorithm” & “Message digest algorithm” parameter :

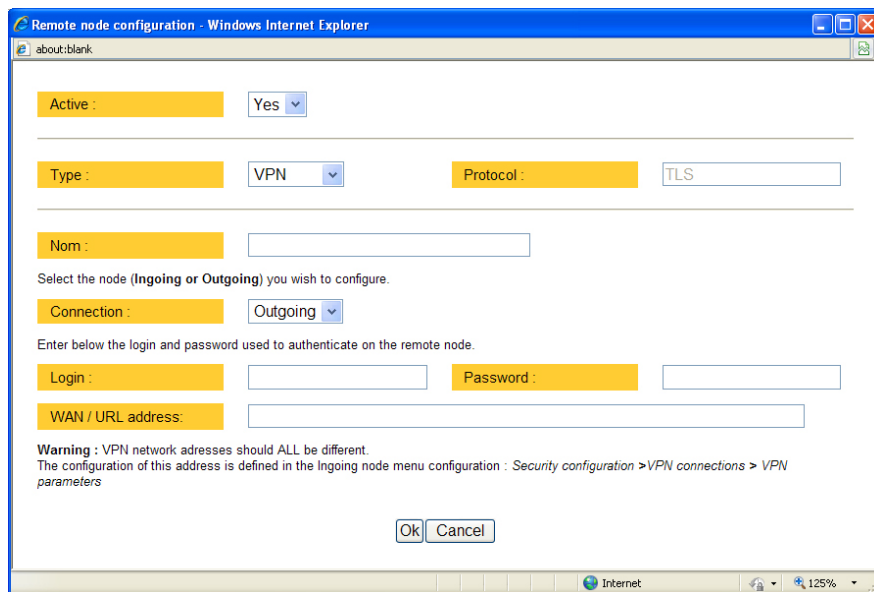
That parameters allow to define the encryption and hash algorithms in use.

15.3.2 Configuring an outgoing TLS connection



To set an outgoing TLS VPN connection,

- Select the “Routing” and then the “Remote nodes” menu.
- Click the “add a node” button.
- Give a name to the connection and select the **“Outgoing” connection direction** option.



Remote node configuration - Windows Internet Explorer

about:blank

Active : Yes

Type : VPN Protocol : TLS

Nom :

Select the node (Ingoing or Outgoing) you wish to configure.

Connection : Outgoing

Enter below the login and password used to authenticate on the remote node.

Login : Password :

WAN / URL address :

Warning : VPN network addresses should ALL be different.
The configuration of this address is defined in the Ingoing node menu configuration : Security configuration > VPN connections > VPN parameters

Ok Cancel

“Login” & “Password” parameters :

Enter the login and password, the router will have to use to authenticate.

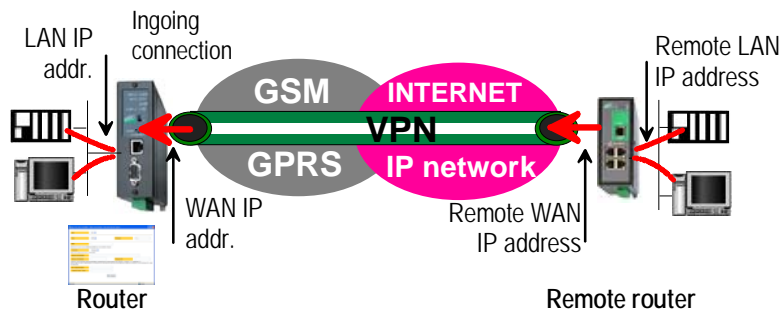
“Remote WAN IP address / URL” parameter :

Enter the IP address of the remote router or its DNS name.

“Remote WAN IP address” parameter :

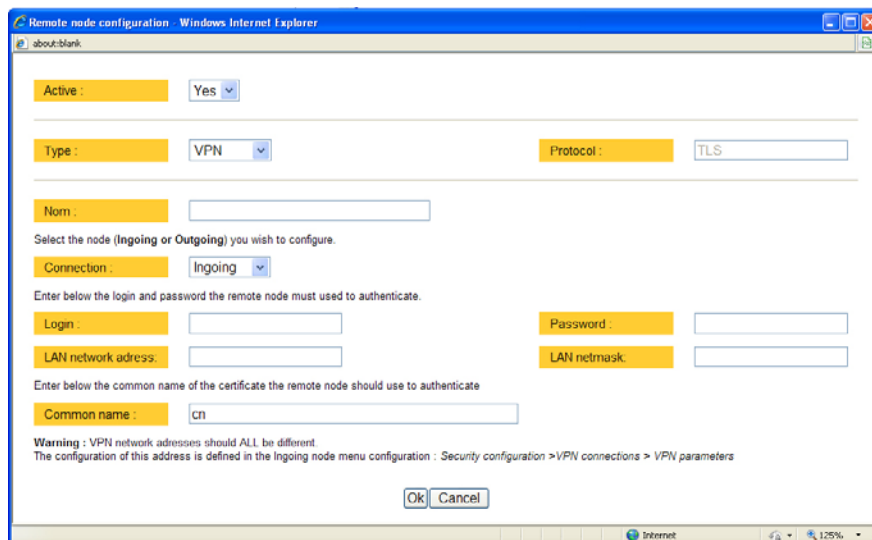
Enter the network IP address and netmask assigned to the remote router over the Internet (public IP address over Internet).

15.3.3 Configuring an incoming TLS connection



To set an incoming TLS VPN connection,

- Come back to the “**VPN connections**” screen,
- Click the “add a connection” button.
- Give a name to the connection and select the “**incoming**” connection direction option.



“Remote router Login” & “Remote router password” parameter :

Enter the login and password of the remote router

The remote router has to use that login and password to authenticate.

“Remote LAN address” & “Remote LAN netmask” parameters :

Enter the network IP address and netmask assigned to the remote LAN.

“Common name” parameter :

Enter the remote router certificate common name.

16 Serial to IP gateway

The gateways listed below are provided :

Modbus client or server (i.e. master or slave)

To connect several serial modbus slaves to several IP modbus clients.
Or to connect a serial modbus master to an IP modbus server.

RAW TCP server or client :

To connect two serial devices through an IP network.

RAW UDP :

To exchange serial data between several serial and IP devices, through an IP network, using a table of IP addresses..

Telnet :

To connect a Telnet terminal to the IPL.

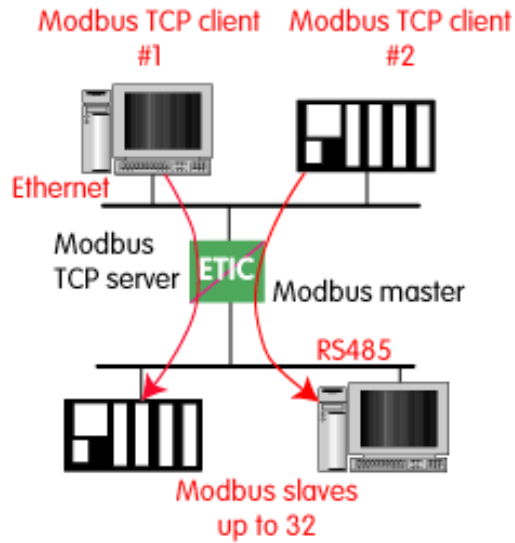
Unitelway slave :

To connect a serial unitelway master to an IP network.

16.1 Modbus gateway

16.1.1 Modbus server gateway

This gateway allows to connect asynchronous modbus slaves to the serial interface of the IPRS.



- Select the modbus menu and then modbus server and enable the modbus server gateway and set the parameters as follows :

ASCII / RTU protocol :

Select the right option

Proxy :

Enable the proxy option if you wish to avoid to frequent requests on the RS232-RS485 interface.

Cache refreshment period :

Select the period at which the gateway will send request to the slaves PLC.

Timeout waiting for the answer :

Set up the timeout the gateway has to wait for the answer of the modbus slave answer.

Local retry :

Set up the number of times the gateway will repeat a request before declaring a failure.

Inter-character gap :

Set up the maximum delay the gateway will have to wait between a received character of a modbus answer frame and the following character of the same frame.

Modbus slave address :

Choose "specified by the modbus TCP client" , if the address of the slave PLC must be decoded by the gateway from the modbus TCP frame coming from the client.

Otherwise, specify the modbus address of the slave PLC; in that case only one slave can be connected to the RS232 serial interface.

TCP inactivity Timeout :

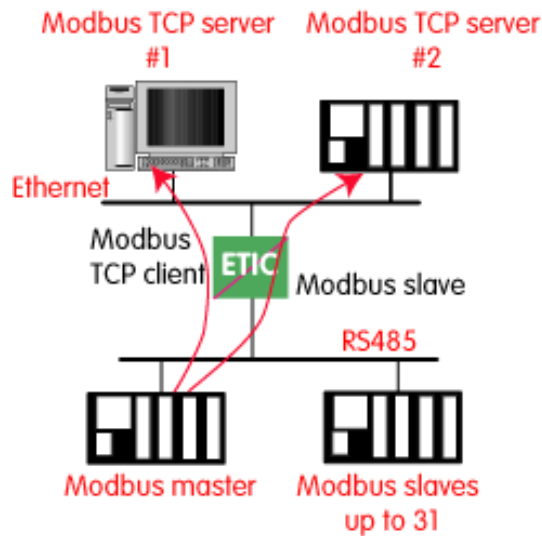
Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

TCP port number :

Set the port number the gateway has to use.

16.1.2 “Modbus client” gateway

This gateway allows to connect a serial modbus master to the serial interface of the IPRS.



- Select the modbus menu and then “modbus client” menu; enable the “modbus client” gateway and set up the parameters as follows :

ASCII / RTU protocol :

Select the right option

Inter-character gap :

Set up the maximum delay the gateway will have to wait between a received character of a modbus answer frame and the following character of the same frame.

TCP inactivity Timeout :

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

TCP port number :

Set the TCP port number the gateway has to use.

IP address :

The modbus client gateway allows to transmit modbus requests from the

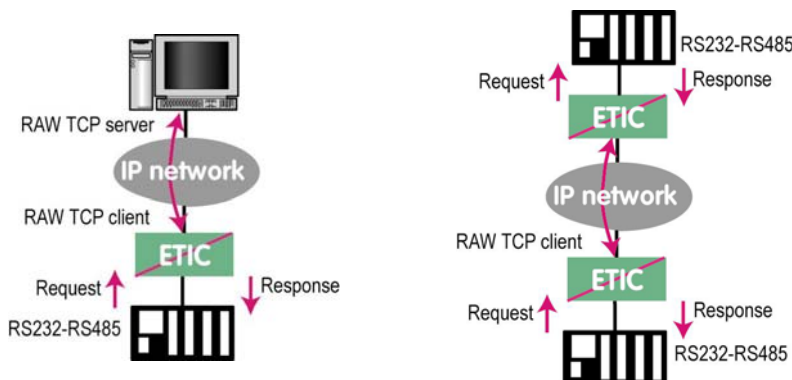
serial modbus master device to any modbus slave device, more precisely called “ modbus server”, located on the IP network.

To assign an IP address to each modbus slave device with which the serial master device needs to communicate, click the “add a link” button; Assign an IP address in front of each modbus slave address with which the serial master device will have to communicate.

16.2 RAW TCP gateway

16.2.1 Raw TCP client gateway

That gateway can be used if a serial master device has to send requests to one or several slave devices (also called server) located on the IP network.



The serial device must be for example a master device.

- Select the “transparent” and then the “raw client” menus.
- Enable the raw client gateway; and set up the parameters as follows :

RS232/485 input buffer size :

Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

Timeout of RS232/485 end of frame :

Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.

Once declared complete, the gateway will transmit the string to the IP network.

TCP inactivity Timeout :

Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

TCP port number :

Set the port number the gateway has to use.

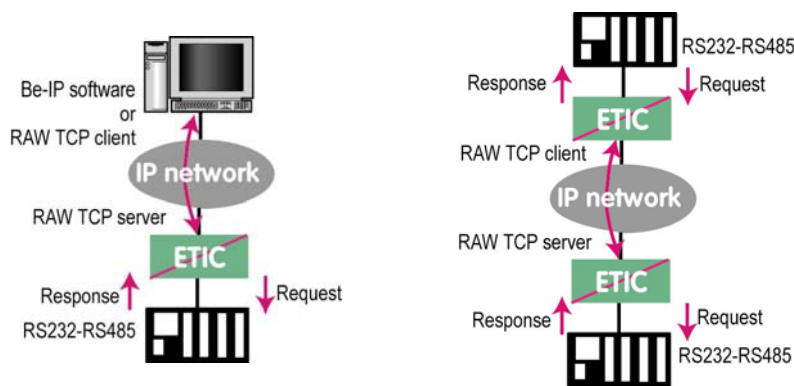
Raw server IP address :

The raw client gateway is able to communicate with a raw server gateway.

Assign an IP address to define the destination gateway.

16.2.2 Raw server gateway

That gateway can be used if a serial slave device has to answer requests coming from devices located on the IP network and acting like a master (also called TCP client).



- Select the “transparent” and then the “raw server” menus.
- Enable the raw server gateway and set up the parameters as follows :

RS232/485 input buffer size :

Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

Timeout of RS232/485 end of frame :

Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.

Once declared complete, the gateway will transmit the string to the IP network.

TCP inactivity Timeout :

Set up the time the gateway will wait before disconnecting the TCP link if no characters are detected.

TCP port number :

Set up the port number the gateway has to use.

16.3 Multicast gateway

16.3.1 Overview

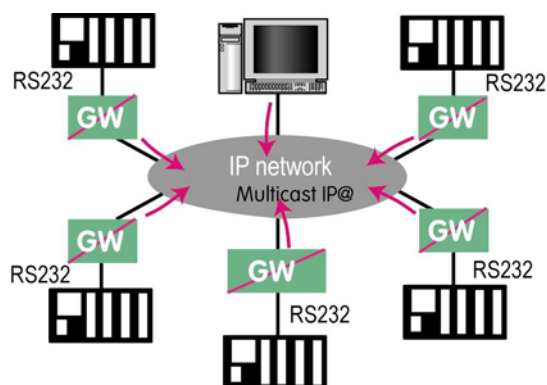
The multicast gateway permits to connect together a group of serial devices, and also Ethernet IP devices, through an IP network.

The serial multicast gateway can be used, for instance, when a serial master device has to send requests to many slave serial devices (also called server) located on the IP network.

Serial data is transmitted by each serial device to all other serial devices through the IP network.

But at the opposite of the RAW UDP technology described previously, that Multicast gateway does not send an IP frame to each destination IP gateway.

Serial data is encapsulated in a unique IP frame **transmitted to a multicast address** received by all the gateways or IP devices.



The *Internet Assigned Numbers Authority (IANA)* controls the assignment of IP multicast addresses.

The range of addresses from 224.0.1.0 through 238.255.255.255 are called globally scoped addresses. They can be used to multicast data between organizations and across the Internet.

The range of addresses from 239.0.0.0 through 239.255.255.255 contains limited scope addresses or administratively scoped addresses. These are defined by RFC 2365 to be constrained to a local group or organization. Routers are typically configured with filters to prevent multicast traffic in this address range from flowing outside an autonomous system (AS) or any user-defined domain. Within an autonomous system or domain, the limited scope address range can be further subdivided so those local multicast boundaries can be defined. This also allows for address reuse among these smaller domains.

Nota bene :

1/ This address range is the destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.

2/ The multicast gateway can be used through an Ethernet LAN; but it is not easy to send across routers.

16.3.2 Configuration

To configure the multicast gateway,

- Select the “transparent” and then the “multicast” menus.
- Enable the multicast gateway and set up the parameters as follows :

RS232/485 input buffer size :

Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

Timeout of RS232/485 end of frame parameter :

Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.

Once declared complete, the gateway will transmit the string to the IP network.

TCP port” parameter :

Set the port number the gateway has to use.

Multicast group IP address :

Enter the multicast IP address assigned to the group with respect to the rules of the IANA authority.

17 Advanced functions

17.1 Alarms

17.1.1 SNMP

The IPL- RS232 router is able to send snmp traps when alarms occur.

Activation :

If that option is selected, the router will send an SNMP trap if an alarm is detected.

SNMP network management IP address :

Enter the IP address of the management platform

SysName & SysLocation :

That fields allow to identify the source device.

Example :

Sysname : etic

Syslocation : France

Product start-up :

If that option is selected, the router will send an SNMP trap each time it will connect to the Internet

17.1.2 Digital output alarm

If an alarm occurs, the router will open the digital output..

The causes which make the output to open can be either the ADSL disconnection, power input 1 failure, power input 2 failure.

17.1.3 E-mail alarm

When the digital input is closed or opened, an email can be transmitted to one of the users of the users list.

To set that function select the "Alarm" menu.

Enable the alarm email :

Select this option if you want an email to be sent to a user when the digital input 1 is set ON or OFF.

Alarm launched on event :

If the option OPEN is selected, the alarm will be sent each time the digital input will be opened.

If the option CLOSED is selected, the alarm will be sent each time the digital input will be opened.

If the option BOTH is selected, the alarm will be sent each time the digital input will be opened or closed.

Hold time :

Select the time the input has to stay in its alarm state to be taken into account.

Alarm destination :

Select the user to whom the email must be sent.

Text to send :

Enter the email text.

17.2 Configuring the web portal

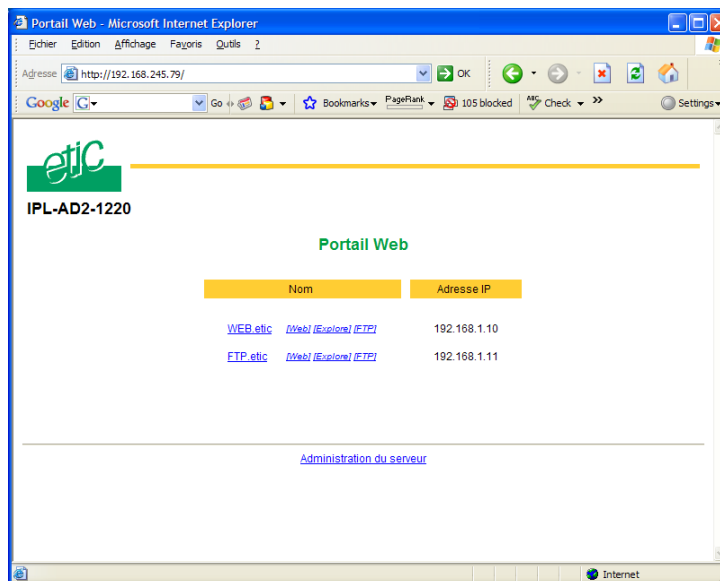
The web portal is an html page; it displays a list of devices connected to the LAN. Each line of the list is made of the device name, its IP address and three links :

The html link : To go directly to the web server of the associated machine.

The « explore » link : To explore the HD of the associated machine, if it is a Windows machine.

The « ftp » link : To explore the files of the associated device.

If the we portal option has been selected (see below), the web portal page is displayed when the remote user launches the navigator and enters the Ip address assigned to the IPL-RS232 router. In that case, the administration server, usually can be displayed at the same address but at the port number 8080 instead of 80 when the web portal page option is not selected.



1 Diagnostic

The html server provides extended diagnostic functions.

Select the Diagnostic menu and then the appropriate sub-menu.

- **Log sub-menu:**

The log displays the last 300 dated events :

Remote routers and users connections and disconnections,
power on,
Serial gateway events.

- **Network status sub-menu and then status sub-menu :**

That screen displays the current status of the LAN interface and of the modem :

LAN :MAC address, Ethernet mode (half or full), IP address.

Modem : Built-in or external modem status.

- **Serial gateway :**

That page displays the current status of the serial gateways :

Type of the gateway(Modbus, RAW, Telnet ...),
serial port set-up (data rate etc...),
number of characters received or sent,
Number of TCP frames or UDP datagrams received or sent,
Number of TCP connections enabled.

The View link displays a window which shows the hexadecimal received and transmitted traffic over the serial COM port.

- **Ping :**

That screen enables to send a ping frame to an IP address.

- **IO control**

That screen displays the status of the digital input and output and allows to set ON or OFF the alarm digital output.

2 Saving the parameters file

Once a product has been configured, the parameters file can be stored and restored when necessary.

To save the parameters file,

Select the "System" menu and then "Save restore",

Click the "Save" button

Select the location to store the file and give a name to the file.

The file suffix is ".bin".

To restore a parameters file

Select the "System" menu and then "Save restore",

Click the "browse" button and select the parameters file,

Click the "Load" button and confirm to restart the product.

Attention : A parameters file can only be restored towards a product having the same firmware version.

3 Updating the firmware

Step 1 : Before starting, you need,

A PC with a Web browser.

An Ethernet cable or a switch

The FTP server software which can be downloaded from the « firmware page » of the ETIC « download area » web server.

Step 2 : Download the release of the firmware from our download area to your PC

Step 3 : Prepare the PC

Check the Ip address of the PC is compatible with the one of the router.

Connect the router to the PC.

Launch the TFTP server (tftp32.exe) software and select the new release (L026xxx/img) by using the "Browser" button.

Click on "Show dir" to check the files of the directory : rfsmini.tgz, rootfs.bin, u-boot.bin and ulmage.

Step 4 : Update the firmware

Launch the web browser

Enter the IP address of the ETIC product ; the home page of the ETIC configuration server is displayed.

Select the "System" menu and then " firmware Update". In the field "IP address of the TFTP server", enter the IP address of your PC.

Note : The IP address of the PC is written in the field "Server Interface" in the TFTP server windows.

Click "Save" and then "Update".

The first file should begin to be downloaded from the PC to the router.

During the operation, the led blinks

When the download is finished, the product automatically reboots.

To be sure the new release has been installed, go to "About" in the administration web page of the IP product.

System

IP protocol	To enter the IP @ of the router over the LAN interface To enter the IP @ assigned to the remote users
Users list	To assign an ID and PWD to each authorized user and set their rights
Devices	To store the IP @ of the devices connected to the LAN
Service list	To define the protocol and port (TCP or others) list
Date & time	To set date and time of the day.
Modem	To set the initialisation string of the modem
RS232-RS485	To set the parameters of the serial interface
SNMP	To set the SNMP traps
DHCP	To set the DHCP server function over the Ethernet interface
Firmware update	Update the product firmware
Save / restore	To download / upload the configuration file of the product.
Reboot	To restart the product

Routing

Remote nodes	To describe remote routers
Static routes	To describe the routes to reach hidden devices
RIP	To enable the RIP protocol

Security

Administration	To restrict access to the administration server
Firewall	To restrict access to devices of the LAN To restrict access to the Internet
VPN	To set the VPNs parameters and register certificates

Internet

Account	To register the Internet subscription parameters
Remote control	To set the conditions the router will connect to the Internet
Routing	To set routing parameters and DNAT rules
Remote control	To define the conditions the router connects to the Internet
Dynamic IP @	To set the conditions the router will publish its temporary IP @ over the Internet

RS to iP gateway

Modbus	To configure the modbus gateway.
Transparent	To configure the rawTCP, multicast & telnet gateway
Unitelway	To configure the unitelway gateway

Alarms	To enter the conditions an email is transmitted to a user
---------------	---

Diagnostic

Logs	To display logs
Network status	To display all the parameters of the connection in use MAC & IP @, SHDSL connection : data rate, error rate, statistics
Gateway status	To display the status of the gateway
Micro switch	To display the micro switches current position
Table of routes	To display the table of routes
Ping	To ping a machine
IO control	To display the IOs status
Resume	To display the connections

About	To display the firmware and hardware identification
--------------	---



ETIC TELECOM

13, Chemin du Vieux Chêne

38240 Meylan France

Tel : 33 4 76 04 20 00

Fax : 33 4 76 04 20 01

E-mail : contact@etictelecom.com

Web : www.etictelecom.com