Distribué par :

Contact :
hvssystem@hvssystem.com

Tél : 0326824929
Fax : 0326851908

Siège social :
2 rue René Laennec
51500 Taissy
France
www.hvssystem.com

IPL-G12

3G - GPRS EDGE – GSM data router

User manual

Document reference : 9017009-02

The IPL-G12 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

INSTALLATION

../..

SETUP

../..

…SETUP

../..

… SETUP

DIAGNOSTIC AND MAINTENANCE

1 Products identification

	IPL-G12B	IPL-G12B-3G
UMTS HSDPA (3G)	-	•
GSM (GPRS-EDGE)	•	•
GSM data switched 9600 b/s	•	-
RJ45 Ethernet 10 Mb/s	1	1
RS232-RS85	1	1
IP router	•	•
NAT – DNAT – Port forwarding	•	•
SNMP	•	•
Dyn DNS	•	•
DHCP client or server (LAN interface)	•	•
Firewall SPI	•	•
VPN PPTP, IPSEC, TLS	•	•
Remote access server	•	•
Digital input for email alarms	3	3
Serial gateway : RAW UDP client & server multi-unicast Raw TCP client & server Modbus client and server Telnet server unitelway	•	•
Html Configuration	•	•
IO Viewer software option	•	•

• means the function is provided
- means the function is not provided

Important notice : In the manual hereafter, when we speak of “IPL-G12”, it means both the IPL-G12B and IPL-G12B-3G references

2 Technical data

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 30 VDC - 170 mA at 24 VDC
Operating T°	-20°C / + 60°C Humidity 5 - 95 %

3G & GPRS-EDGE & GSM data	
RF Frequencies	850/900/1800/1900 / 2100 MHz (see detailed table below)
RF power	EGSM850 EGSM900 : class 4 (2 W) GSM1800 GSM1900 : class 1 ((1 W)
RF connector	FME
UMTS *	HSDPA 384 kbps downlink / 384 kbps uplink
EDGE-GPRS **	Max data rate : 85,6 Kb/s downlink & 21,4 Kb/s uplink Multislot class 10
GPRS **	Multislot class 12
GSM data ***	9600 b/s

* IPL-G12B-3G only ** IPL-G12B-3G and IPL-G12B *** IPL-G12B only

UMTS Frequency range (3G)			
		Min	Max
Uplink (UE to Node B)	UMTS 850 Band V	824 MHz	849 MHz
	UMTS 1900 Band II	1850 MHz	1910 MHz
	UMTS 2100 Band I	1920 MHz	1980 MHz
Downlink (Node B to UE)	UMTS 850 Band V	869 MHz	894 MHz
	UMTS 1900 Band II	1930 MHz	1990 MHz
	UMTS 2100 Band I	2110 MHz	2170 MHz

GSM Frequency range (GPRS-EDGE)			
		Min	Max
Uplink (MS to BTS)	GSM 850	824 MHz	849 MHz
	E-GSM 900	880 MHz	915 MHz
	GSM 1800	1710 MHz	1785 MHz
	GSM 1900	1850 MHz	1910 MHz
Downlink (BTS to MS)	GSM 850	869 MHz	894 MHz
	E-GSM 900	925 MHz	960 MHz
	GSM 1800	1805 MHz	1880 MHz
	GSM 1900	1930 MHz	1990 MHz

Ethernet / IP router	
Ethernet	10BT
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	
VPN	Client or server IPSEC or TLS/SSL or PPTP Encryption 3DES Certificate 509
Firewall	Stateful packet inspection (50 rules)
Logs	Date and time stamped logs

Remote access server (RAS)	
User list	25 users
Connection	VPN PPTP / L2TP-IPSec / TLS Open VPN Login & password Certificate X509
M2Me	VPN Compliant with the M2Me_Secure VPN client Compliant with the M2Me_Connect mediation service
Alarms	3 inputs : emails

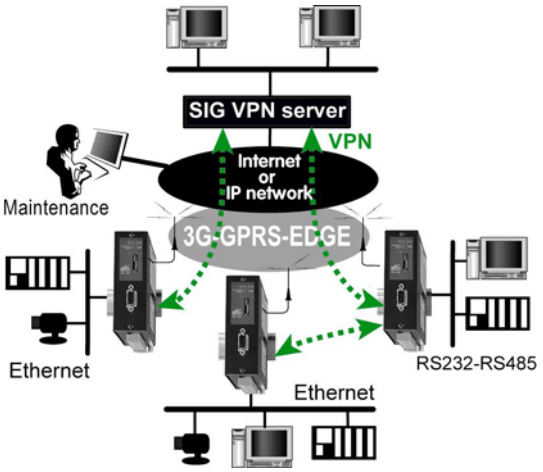
Serial interface	
RS232	1200 - 115200 b/s parity N / E / O
Serial to IP gateways	Serial gateway : RAW UDP client & server multi-unicast, Raw TCP client & server, Modbus client and server, Telnet server, unitelway

3 Product overview

IPL-G12B-3G router

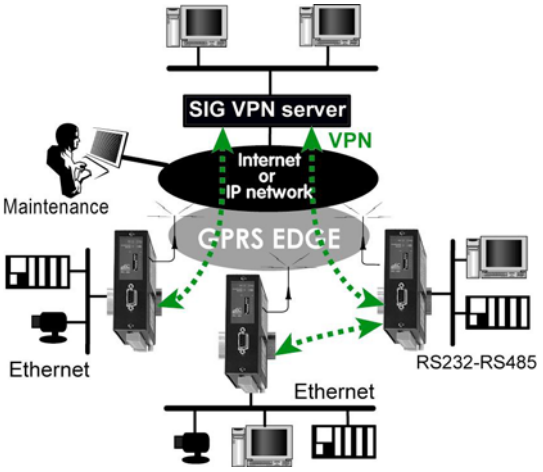
The IPL-G12B-3G router is designed to interconnect safely automated devices over the UMTS 3G or the GPRS-EDGE service.

The connection is permanent.



IPL-G12B router

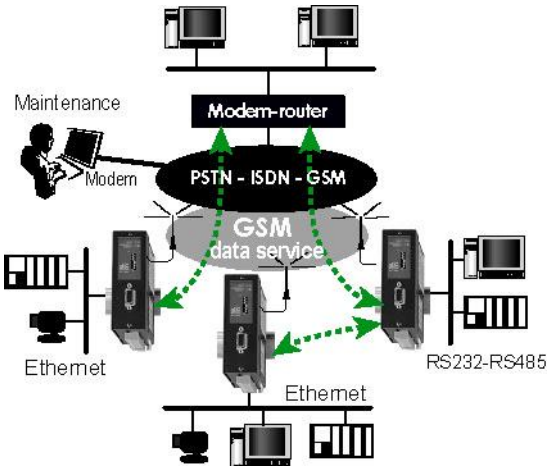
The IPL-G12B router provides the same function but over the GPRS-EDGE service (and not over the UMTS 3G service).



IPL-G12B router

The IPL-G12B router can set a 9600 b/s connection with another router also connected to the GSM or, if the service is provided, to the PSTN or the ISDN.

The connection is not permanent. One party must dial the other one.



IP router

The IPL-G12 router provides flexible and comprehensive solutions to route IP frames from one network to other networks.

The solutions include remote nodes description, static routes, RIP protocol and destination network address translation (DNAT).

Safe VPN links

The IPL-G12 router is able to establish safe VPN tunnels (TLS or IPSec and client or server).

Once a VPN is established between two IPL-G12 routers or between an IPL-G12 and an other compatible router , each IP device connected to the first LAN can exchange IP frames with any device connected to the other LAN as if they were linked with a private line.

If the VPN is established between a remote user PC and an IPL-G12 router, the remote user can access to the devices connected to the router.

The IPL-G12 router is able to establish up to 25 IPSec or TLS – SSL VPNs.

Authentication can be carried out with a pre-shared key or with certificates.

SPI Firewall

The IPL-G12 incorporates a firewall.
The firewall controls the status of the sessions (TCP, UDP, ICMP) to avoid sophisticated spoofing attacks.
Entering the product is not possible unless a DNAT rule or a VPN have been set.

DNS server

DNS makes it possible to assign Internet names to devices or organizations independently of their public IP address.
The IPL-G12 router behaves like a DNS server for the devices connected to the LAN.

DynDNS client

The IPL-G12 router is compatible with the Dyn DNS service.

DHCP client or server

Over the Ethernet LAN interface, the IPL-G12 can be a DHCP client or server.

Emails – sms

An email (or SMS) can be sent each time one of the three digital inputs are opened or closed.

SNMP

The IPL-G12 router is an SNMP agent.

Html and DIP switches configuration

The IPL-G12 is configured with a web server .
Two DIP switches allow to set the method the product receives its IP address over the LAN interface : From a DHCP client or server, factory IP address or stored IP address.

Remote access server

The IPL-G12 provides to authorized users a remote access to the devices connected either to the LAN or to a serial RS232-RS485 interface, as if his PC was directly connected to the LAN or to the RS232.

Serial gateway

The product includes an up-to-date RS to IP gateway, enabling to connect serial devices safely to the GSM network and the Internet.

EticFinder software

The ETICFinder software detects the ETIC products connected to an Ethernet interface and displays the MAC address and the iP address of each product.

M2Me_Secure ™ VPN client software

M2Me_Secure is a TLS client software (to order separately) edited by ETIC Telecommunications.
It is able to register up to 100 remote sites connection parameters the user can set on a click.

4 GSM services overview

3G service

The 3G service provides an IP permanent connection to the Internet at a high data rate (see the technical data table).

The connection can also be set towards a private network without using the Internet.

The 3G radio fixed infrastructure is not the same as the GSM mobile phone infrastructure; it why, the 3G service may be less available than the GPRS-EDGE service which uses the GSM mobile phone infrastructure.

GPRS-EDGE service

As the 3G service, the GPRS-EDGE service provides a permanent IP connection to the Internet but at a medium data rate (see the data-sheet).

The effective data rate depends of the operator and the reception quality.

The GPRS-EDGE service is provided over the usual GSM network. It is why the GPRS-EDGE service is usually available each time the GSM voice service is available.

GSM data service

The GSM data service is a 9600 b/s serial data transmission service.
It is a switched service; it means that one party has to dial the other party.

Most GSM service providers also provide the capability to dial from a PSTN modem or an ISDN adapter towards a GSM modem and reciprocally.
However, if that function is needed, please check it is provided by your GSM operator.

IP address

On a 3G or GPRS-EDGE network, the IP address assigned to the router's "antenna" interface by the wireless service provider can be public or private. It is generally dynamic.

Outgoing or ingoing VPN connection

The IPL-G12 can behave like a VPN client or a VPN server.

Outgoing VPN connections to the Internet or to a private network are generally easy to set..

The IPL-G12 can also behaves like a VPN server to accept ingoing VPN connections from the Internet for instance.

However, ingoing VPN connections from the Internet towards the IPL-G12 may not be possible if the IP address assigned to the router's "antenna" interface by the provider is a private IP address.

1 Product description

IPL-G12

1.1 Leds

	Function
Line /	• **If no SIM card is present :** Extinguished • **If the SIM card has been inserted :** Blinks to indicate the signal level - see table hereafter • **If the SIM card has been inserted ad if the id and password have been entered in the html server :** Blinking at power-on to indicate the signal level, Lit after 30 s, to indicate the router is connected to the GSM
VPN	Lit : One VPN at least has been established Blinking : VPN establishment in progress
LINK	Ethernet Interface connected
DATA	Data activity
RD	Bytes transmitted to the RS232 (from the IPL)
TD	Bytes received from the RS232 (to the IPL)
Operation	Blinks if the SIM cart has not been insterted Lit otherwise

the L / led	RF signal level indication at power-on
... briefly blinks 3 times	**The quality of the reception signal is fine**
... briefly blinks 2 times	**The quality of the reception signal is acceptable**
... briefly blinks 1 time	**The quality of the reception signal is poor**
... is turned off	**No reception** Is a GSM voice communication possible ? has the SIM card been correctly inserted ?

1.2 Connectors

2 pins screw-block : Supply voltage		
Pin	Signal	Function
1	+	9 to 30 V – 170 mA at 24 VDC (on line)
2	-	Ground

8 pins : Inputs / outputs		
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 fem. RS232 connector				
Pin	Circuit		Designation	IPL - Terminal
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
SW 3, 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 30 VDC and higher than 9 VDC. The consumption is 170 mA at 24 VDC.

Careful : The supply voltage module must be able to provide current peaks absorbed by the GSM RF transmitter.

4 Ethernet interface

The Ethernet interface is a 10 Mb/s interface.

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

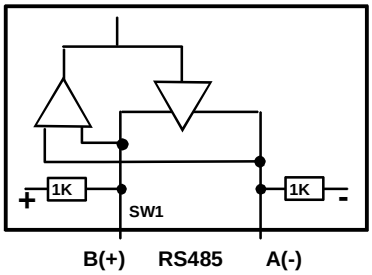
5 RS232 interface

The IPL-G12 router provides an RS232 and an RS485 interface. Asynchronous products can thus be integrated to the IP network.

The RS232 cable must not be longer than 10 meters.

6 RS485 interface

The RS485 serial interface is provided on the bottom on a 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.

7 Inputs & output

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 three digital inputs ; they are not isolated.
if the input 1 is opened, an SNMP trap will be sent to the SNMP server if that function has been enabled.

8 GSM connection

8.1 Checking the GSM reception signal level

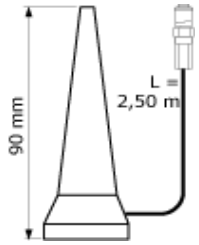
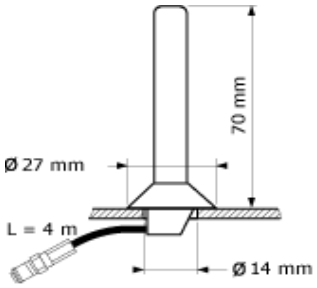
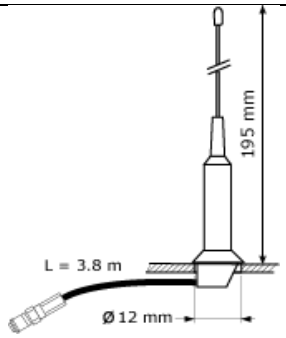
Before installing the product, check that the GSM reception signal level is good enough at the location you want to install the product.

That test can be carried out with a usual mobile phone using the same provider and the same service (either 3G or GPRS-EDGE).

The signal level must be good or excellent.

8.2 Antenna

If the cabinet in which the router has to be installed is made of metal, the antenna has to be installed outside the cabinet; for instance on its top.
The antenna must be ordered separately; the models below are available :

		
ANT200 0 db gain - magnetic	ANT200 0 db gain	ANT200 3 db gain

8.3 Installing the SIM card

Step 1 : Disable the PIN code of the SIM card

Before inserting the SIM card, the PIN code must be disabled.

That operation must be carried out with a mobile phone.
Once the PIN code has been disabled, no password is required when the mobile phone is powered on.

Step 2 : Insert the GSM SIM card

Before inserting the SIM card, the supply voltage must be disconnected.

The micro-sim card must be inserted in the slot located at the top of the product.

Step 3 : Check the reception signal level after installation

At power-on, the **L /** led gives an indication of the GSM signal quality :

the L / led	Signification
... briefly blinks 3 times	The quality of the reception signal is fine
... briefly blinks 2 times	The quality of the reception signal is acceptable
... briefly blinks 1 time	The quality of the reception signal is poor
... is turned off	No reception Is a GSM voice communication possible ? has the sim card been correctly inserted ?

Remark : The GSM signal level is also displayed in the administration server (menu “System” and then “Modem”).

1 Set up steps

To configure the router, we advise to proceed as follows :

- Connecting a PC to the router
- Setting up the LAN interface
- Setting up the router subscription to
  - the 3G GPRS EDGE service
  - or the GSM data service
- Setting up VPNs between routers
  - Case of the 3G GPRS EDGE service
  - Case of the GSM data service
- Setting up routing and IP address translation function
- Setting up remote users connections
  - Case of the 3G GPRS EDGE service
  - Case of 3G GPRS EDGE service using the M2Me_Connect connection service
  - Case of GSM data connections
- Setting up the remote users list
- Setting up the firewall
- Setting up alarm e-mails

2 Configuring the IPL-G12 router

2.1 Overview

Administration server address :
The administration html server is located at the LAN IP address of the router (The default address is192.168.0.128).

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-G12 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 o 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.

Router interfaces :
the rouetr feature two Ip nterfaces :
The Ethernet 10 BT interface which is called the LAN interface and the wireless interface which called the WAN interface.

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_iplg12_V241.bin”.

2.2 First configuration

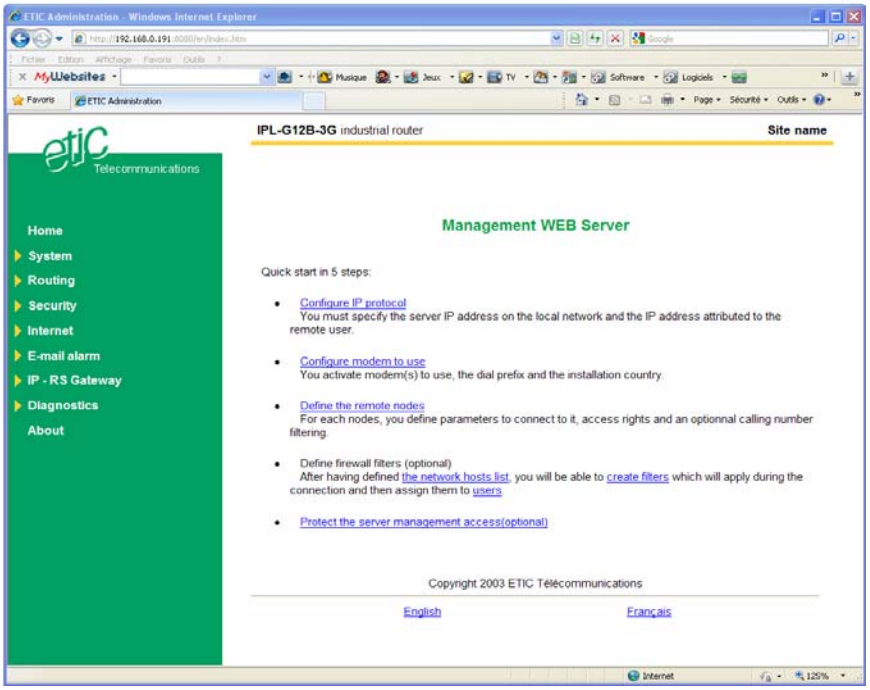
Step 1 : Check the DIP switches
Coming from factory, the DIP switches SW1 and SW2 are set OFF to select the stored IP address.
Coming from factory, the stored IP address is the factory IP address 192.168.0.128.

Step 2 : Create or modify the PC IP connection.
Assign to the PC an IP @ in accordance with the IPL-G12 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-G12 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-E 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.

T**o 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-G12 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-G12 factory configuration,

- Switch OFF the power supply of IPL-G12 router.
- Press the push-button on the top part of the IPL-G12 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 “Setup” 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 of the router

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

Local network parameters :

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

"**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" :
That parameters define the pool of addresses which will be assigned automatically to remote user's PCs when they will connect to the router.
Enter the start address and the end address.

9 3G or GPRS EDGE configuration

9.1 Configuring the 3G-GPRS-EDGE parameters

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

"Activate Internet connection" parameter :
Select the "by modem" choice.

"3G-GPRS mode" checkbox :
Select this option to enable the 3G-GPRS-EDGE mode.

"APN" parameter :
Enter the APN code assigned by the GSM operator.

"User name" & "password" parameters :
Enter the user name and password assigned by the GSM operator.

Careful : If no user name or password are assigned by the GSM operator, 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.

9.2 Internet connection control

The IPL-G12 can be connected on demand to the 3G GPRS EDGE network either by a local action or remotely.

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

«Connect to Internet after a phone call from » parameter :
When a call comes in from the phone number entered in this field, the IPL-G12 connects to the Internet.

« Allow Internet call-back» parameter :
If that option is selected, the router connects to the Internet after a remote user connects with the GSM data service and asks for the Internet call-back by entering the call-back number “0” (zero).

Connect to Internet at product power-on :
If that option is selected, the router connects to the Internet as soon it will be powered on.

Connect to Internet on a rising edge of the digital input 1 :
If that option is selected, the router connects to the Internet each time the digital input 1 is set closed.

Connect to Internet now :
The router connects to the Internet when the button “Connect” is clicked.

9.3 Controlling the 3G connection with a “Ping control”

In some situations, the wireless module and / or the wireless infrastructure may not indicate the wireless connection of the router to the service has failed.

It why, it is possible to enable the PING control feature.

If it is selected, the router periodically sends a PING to a selected IP address; if the ping does not receives a response, the wireless connection is restarted by the router.

- To enable the PING control function, select the “Internet “ menu and then “Ping control”.

“Activate Ping control” checkbox :
Select that checkbox to enable the pin control function.

“IP address to ping” parameter :
Enter the Ip address to PING.

“Ping interval” parameter :
Select the PING period.

“Ping retries” parameter :
Select the number of PING retries before restarting the router.

Attention : Enabling the PING control feature provokes a metered traffic .

10 GSM data configuration

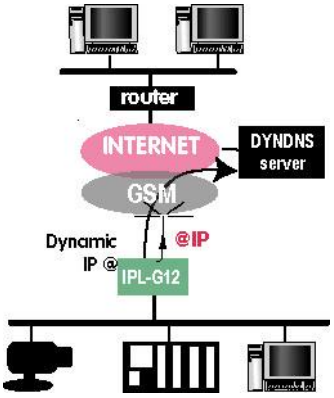
The GSM data connection capability is featured only by the IPL-G12B router.

- Select the “Internet” and “Modem” menu and check the 3G-GPRS checkbox is not selected.
- Select the “System” and then click “Modem” menu.
- The “Use default initialisation string” option must be selected unless particular communication difficulties.

11 Releasing a dynamic IP @ with the DYNDNS service

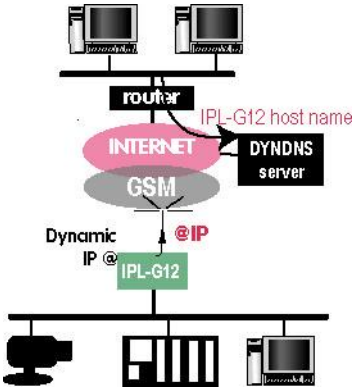
Dynamic DNS (DDNS) allows to create a hostname that points to a dynamic public IP.

If the IP address assigned to the IPL-G12 router over the Internet is public but not fixed, the router will contact the DYNDNS service each time it will change and update the hostname table with the new address.



Each time a device wishes to connect to the IPL-G12, it will use its host name and get its temporary IP address from the DYNDNS server.

It will then connect to the IPL-G12 as if its address was fixed.



To configure that function,

- **go to www.dyndns.org and create an account.**
- **Select the « Internet » menu and then click « remote control »**

  Enable the DYNDNS function
  Enter the account login and password provided by DYNDNS
  Enter the hostname you registered (Ex : iplG12grenoble2.dyndns.org).

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

12.1 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 f 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-G12 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-G12 router and another one must be the same.

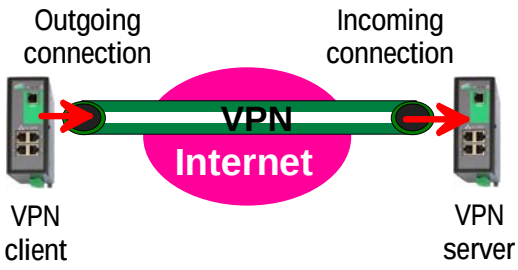
Two steps are necessary to configure the IPL-G12 to create VPN connections between routers :

1st step : Select and setup the VPN type parameters
Once a type of VPN has be selected, it applies to all the connections with remote routers.

2nd step : Create VPN connections

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

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

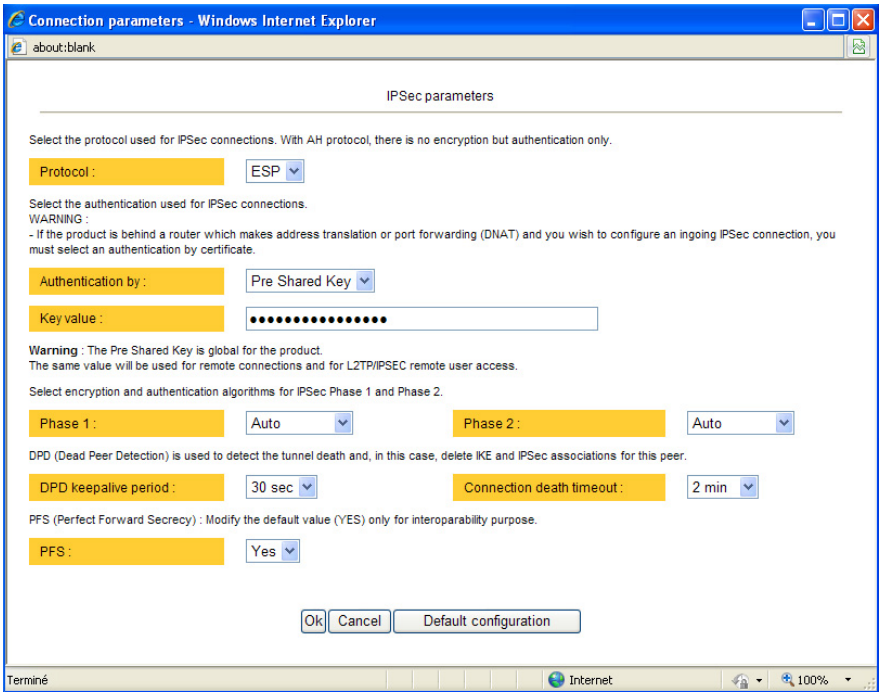


12.2 Configuring IPSec VPN connections

12.2.1 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” .



“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-G12 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).

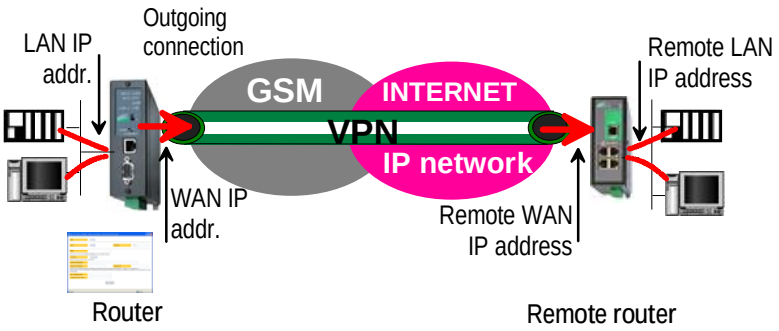
The default value is Auto; in that case both end-points will negotiate a common algorithm.

“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.

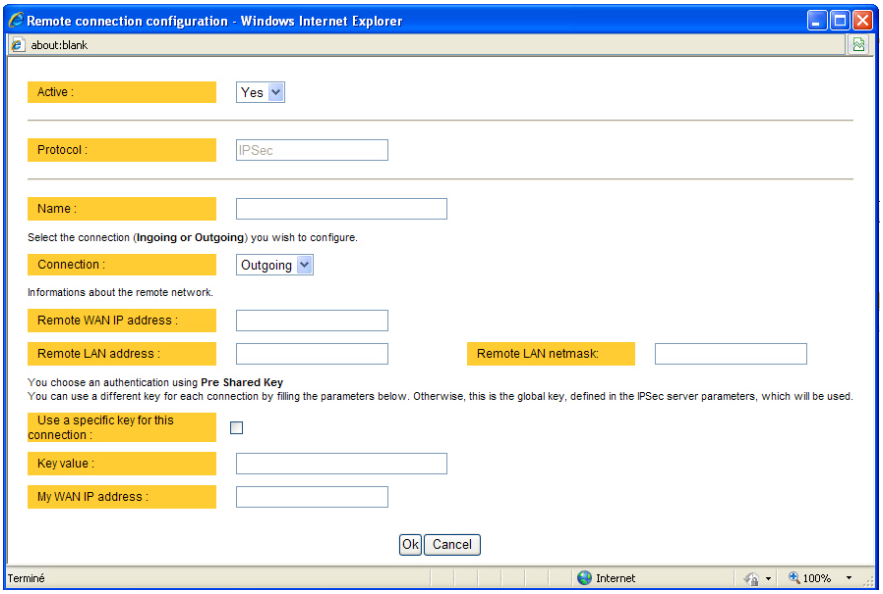
ATTENTION : Once the parameters of the IPSEC connection have been selected, click the OK button and then the Save button.

12.2.2 Configuring an outgoing IPSec connection



To set an ioutgoing 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.

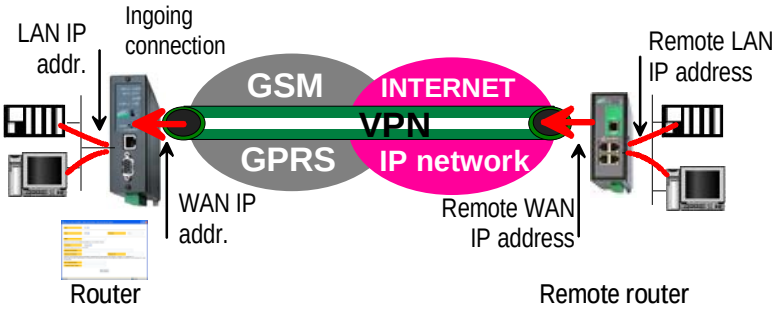
"My WAN address" parameter :
Enter the IP address of the router on the GPRS interface.

- **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.

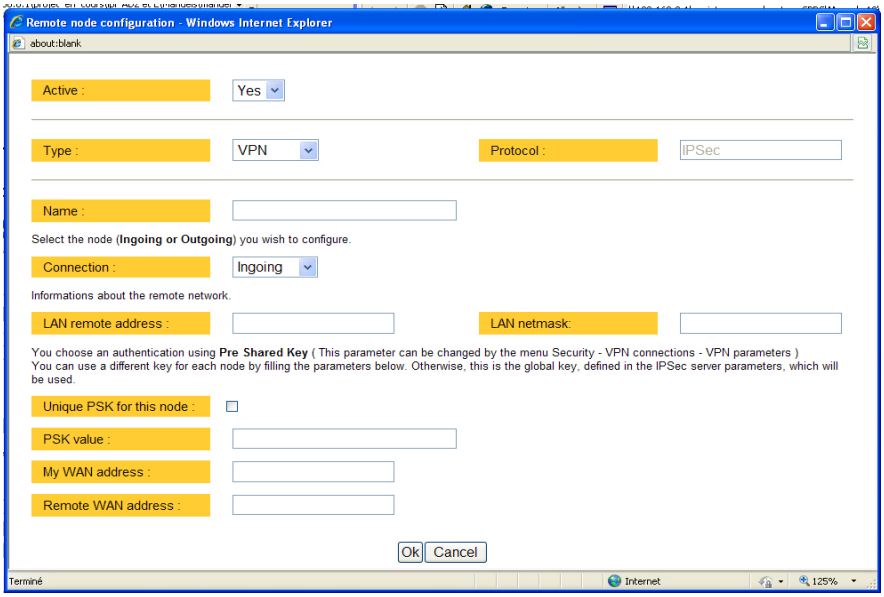
Attention : For ETIC certificates, this field is the Email field

12.2.3 Configuring an ingoing IPSec connection



To set an ingoing 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 “ingoing” 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-G12 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.

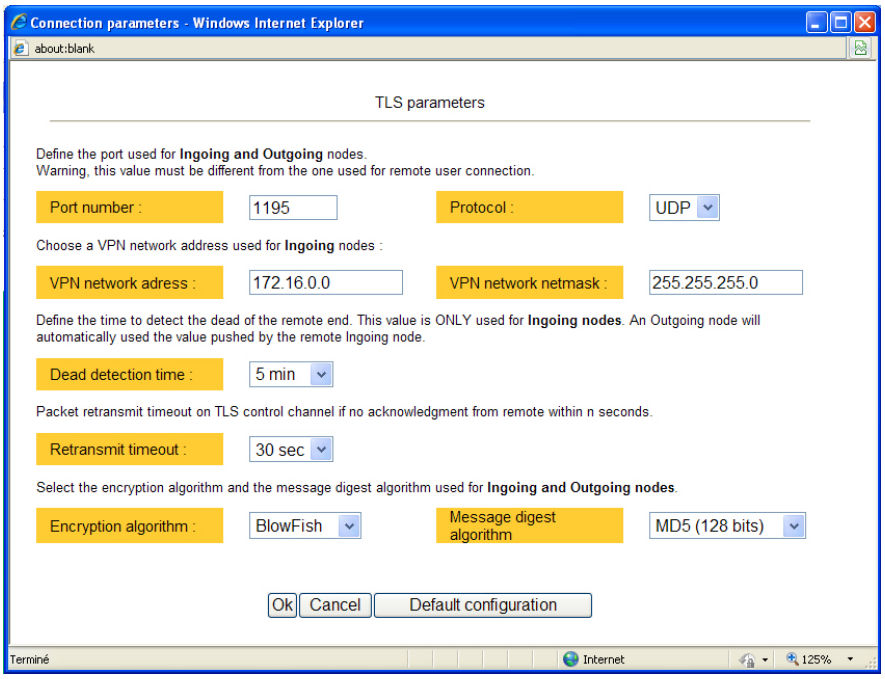
Attention : For ETIC certificates, this field is the Email field.

12.3 Configuring TLS VPN connections

12.3.1 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” .

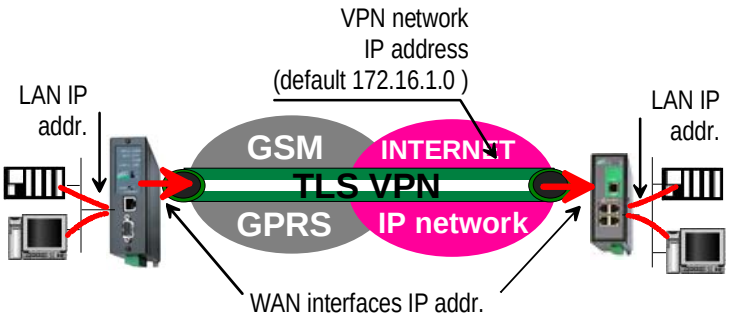


“Port number” & “protocol” parameters :
Select the port Nr and the type of protocol used to transport the TLS VPN; UDP will be preferred.

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.

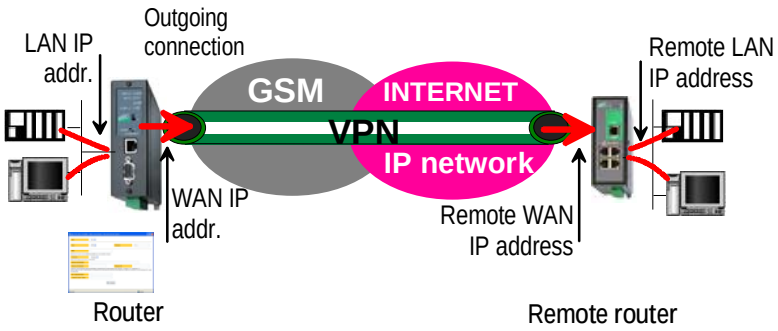
“Repetition time-out” parameter :

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 :

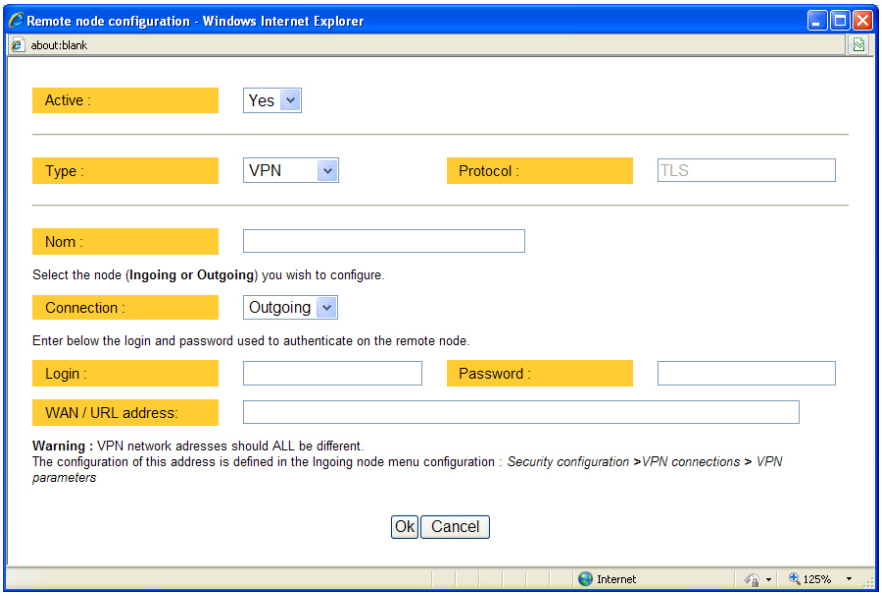
That parameters allow to define the encryption and hash algorithms in use.

12.3.2 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.

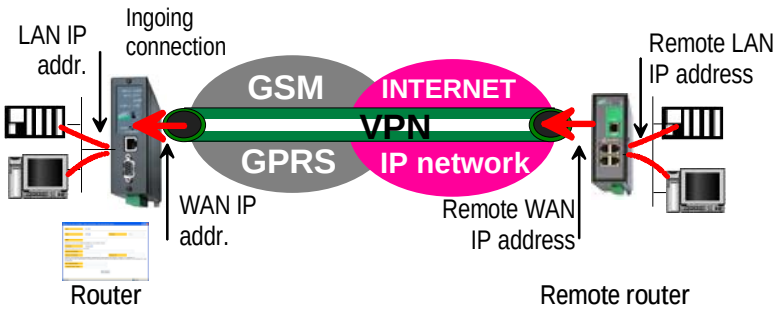


“Login” & “Password” parameters :
Enter the login and password, the router will have to use to authenticate.

“Remote WAN IP address / URL” parameter :
Enter the IP address of the remote router or its DNS name.

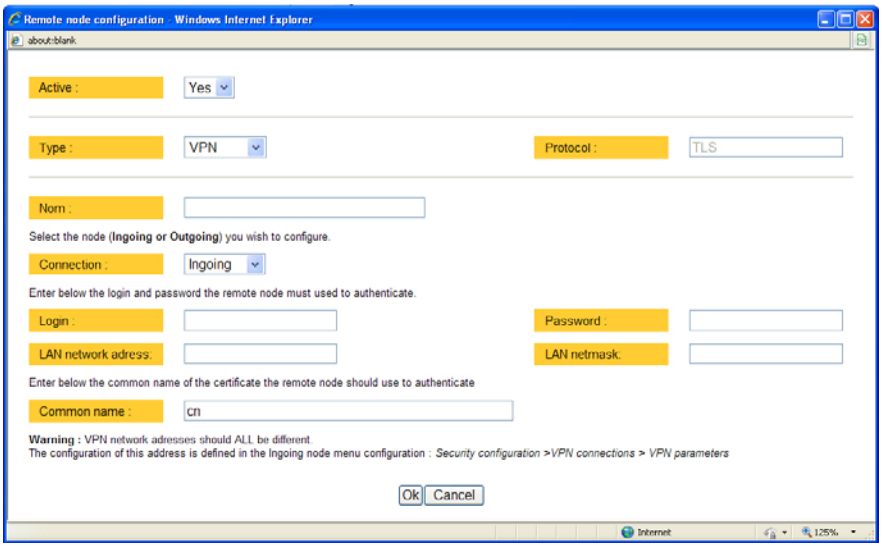
“Remote WAN IP address” parameter :
Enter the network IP address and netmask assigned to the remote router over the Internet (public IP address over Internet).

12.3.3 Configuring an ingoing TLS connection



To set an ingoing 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 "ingoing" 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.

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

13 Configuring connections between routers (9600 b/s GSM data)

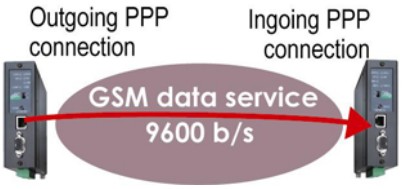
That function is provided only by the IPL-G12B router.

13.1 Principle

The GSM data service is a switched data service at a data rate of 9600 b/s.
It connects GSM routers together or with other routers connected to the PSTN or the ISDN.

A PPP switched connection must be set between routers. A PPP connection can be outgoing or ingoing or both.

Each remote routers with which an IPL-G12B router will have to communicate have to be registered as a remote node.



13.2 Configuration

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

The table below decribes the parameters depending on the PPP connection type (outgoing, ingoing, both).

PPP connection			
Type of connection			**Parameter description**
OUT	IN	OUT & IN	
X	X	X	**"Enable" parameter :** Select the "yes" option.
X	X	X	**"Type" parameter :** Select the "switched" choice.
X	X	X	**"Node name" parameter :** Assign a name to the node.
X	X	X	**"call direction" parameter :** Select "Outgoing" if the router sets that connection by dialling towards the remote router. Select "Ingoing" if the router waits from an incoming call from the remote router. Select "Outgoing and incoming" if the connection can be set either by dialling towards the remote router or by accepting an incoming call from the remote router.
X	X	X	**"Remote router IP @" and "Remote network netmask" parameter :** Enter the IP address and the netmask of the remote router Ethernet interface.
X		X	**"Modem" parameter :** Select the "built-in" choice.
X		X	**"Dial number" parameter :** Enter the number the router has to dial to connect to the remote router.
X		X	**"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.
	X	X	**"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.
X		X	**"Idle time-out" parameter (5 s to 60 mn) :** Set the time duration of the silence before the router will clear the call.
X		X	**"First packet time-out" parameter (5 s to 60 mn) :**

PPP connection / advanced parameters			
Click the "advanced conf." button to configure advanced functions :			
Type of connection			
OUT	IN	OUT & IN	**Parameter**
	X	**X**	**"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.
X	**X**	**X**	**"Firewall filter" parameter :** Select the firewall filter assigned to the connection
X	**X**	**X**	**"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 frames transmitted by a device towards the PSTN or ISDN. If no PPP IP address has been entered, it is replaced by the IP address of the router over the Ethernet interface.
X	**X**	**X**	**"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.

.

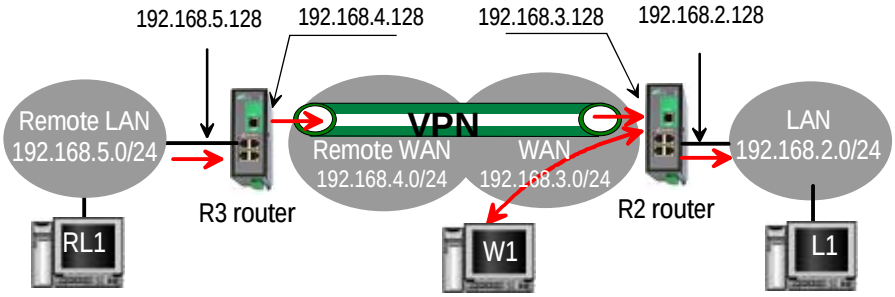
14 Routing functions

14.1 Basic routing function

Once an iP address has been assigned to the R2 router on the LAN interface and another one on the WAN interface (see drawing hereafter), the IPL-E R2 router is ready to route frames …

… between devices connected to the remote LAN network like RL1, and devices connected to the LAN network like L1 through a VPN;

… between devices connected to the WAN network like W1, and devices connected to the LAN network like L1

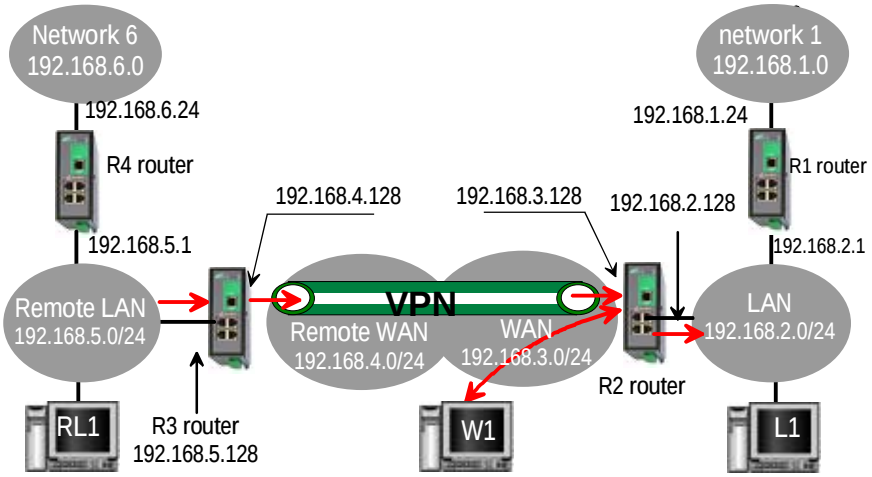


Remark 1 : Firewall rules must be set to authorize WAN to LAN transfer.

Remark 2 : A default gateway address must be entered in each device of the different networks.

14.2 Static routes

However, the R2 router is not able to route frames between a device like L1 belonging to the LAN network and a device connected to “network 6” (see the drawing hereafter).



In that case, it is necessary to enter the route to that hidden “network 6”; 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 neighbour router through which an IP packet to that destination must pass.

Router 2 static routes :

Active	Route name	Destination	Netmask	Gateway
Yes	Network 6	192.168.6.0	255.255.255.0	192.168.5.1
Yes	Network 1	192.168.1.0	255.255.255.0	192.168.2.1
Yes	Network Remote WAN	192.168.4.0	255.255.255.0	192.168.5.128

Remark :
It is not necessary to enter the static route to the WAN network nor to the remote LAN network, that routes have been automatically created by the router respectively when the WAN IP address has been entered and when the VPN has been configured.

To set a static route,

- Select the "**Routing**" menu and then "**Static routes**".
- click the "**Add a route**" button.

"Destination IP address" & "netmask" parameters :
Enter the destination network IP address and netmask.

"Gateway IP address" parameters :
Enter the Ip address of the gateway through which the IP packets intended for that network must pass.

14.3 RIP protocol

RIP (**Routing Information Protocol**) is a routing protocol which enables each router belonging to a network to acquire the routes to any subnet.

The principle is as follows :

Routing table
Each router holds a routing table.
Each entry of the table consists in the destination subnet address and the adjacent router address leading to that subnet.

Routing table broadcasting :
Each router broadcasts its table**.**

Routing table update :
Each router updates its own table using the tables received from the other ones.

To enable RIP,

- Select the "**Routing**" menu and then "**Static routes**".
- Select the 'Enable RIP on LAN interface" and the "Enable RIP on WAN interface" options.

15 Address and port translation

The IPL-G12 provides the capability to replace the original source IP address and the destination port and IP address in particular situations.

15.1 Port forwarding (DNAT)

The port forwarding function consists in transferring to a particular device connected to the LAN interface a particular data flow addressed to the IPL-G12 router on its wireless interface.

That function applies only to the IP frames sent to the wireless IP address of the router.

The transfer criteria is the port number used as an additional address field.

When a frame is addressed to the IPL-G12 router on a particular port, it is transferred to a particular device connected to the LAN interface.

Example : Suppose a remote device has to communicate with the devices PLC1 with TCP port 102, PLC2 with TCP port 502 and a PC port 80.

The DNAT rule will be

Internet / WAN	LAN translation	
Service	Device	Service
TCP-102	192.168.0.15	TCP-102
TCP-502	192.168.0.16	TCP-502
TCP-80	192.168.0.17	TCP-80

- To set the DNAT rules, select the “Internet” menu and then the “Routing” menu.

- Click “Add a DNAT rule”.

15.2 Advanced network address and port translation

15.2.1 Principle

That function consists in replacing the source IP address or/and the destination port and IP address of particular frames received by the router on its interfaces according to configured rules.

On the wireless interface, that function applies only to IP packets transported inside a PPTP or a TLS or an IPSec VPN connection.

On the LAN interface, that function applies to all the IP packets transmitted to the wireless network.

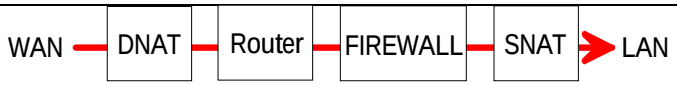
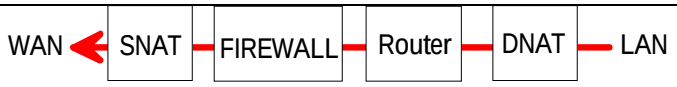
Remark : That function does not apply to IP frames included in a PPTP or TLS or L2TP remote user connection.

One brings out

the DNAT function which consists in replacing the destination port number and IP address.

the SNAT function which consists in replacing the source IP address.

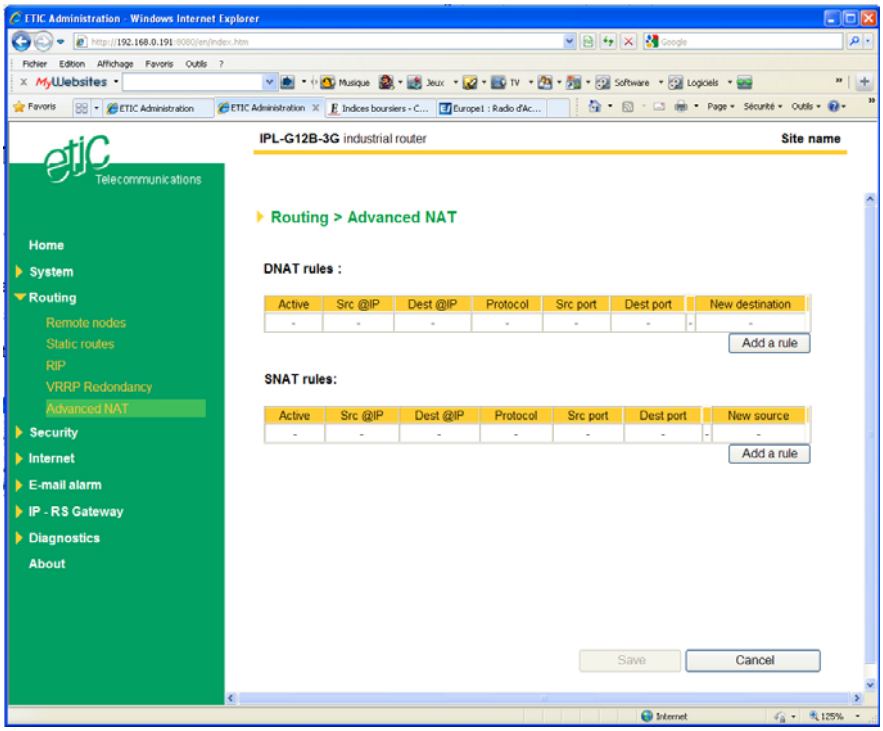
Because the DNAT and SNAT functions modify the IP addresses of the IP packets processed by the IPL-G12 router, and because the firewall filters that frames, it is very important to understand in which order that different functions are carried out :

Direction	
WAN to LAN (WAN=GSM)	
LAN to WAN (WAN=GSM)	

15.2.2 Configuration

To set the advanced address translation functions

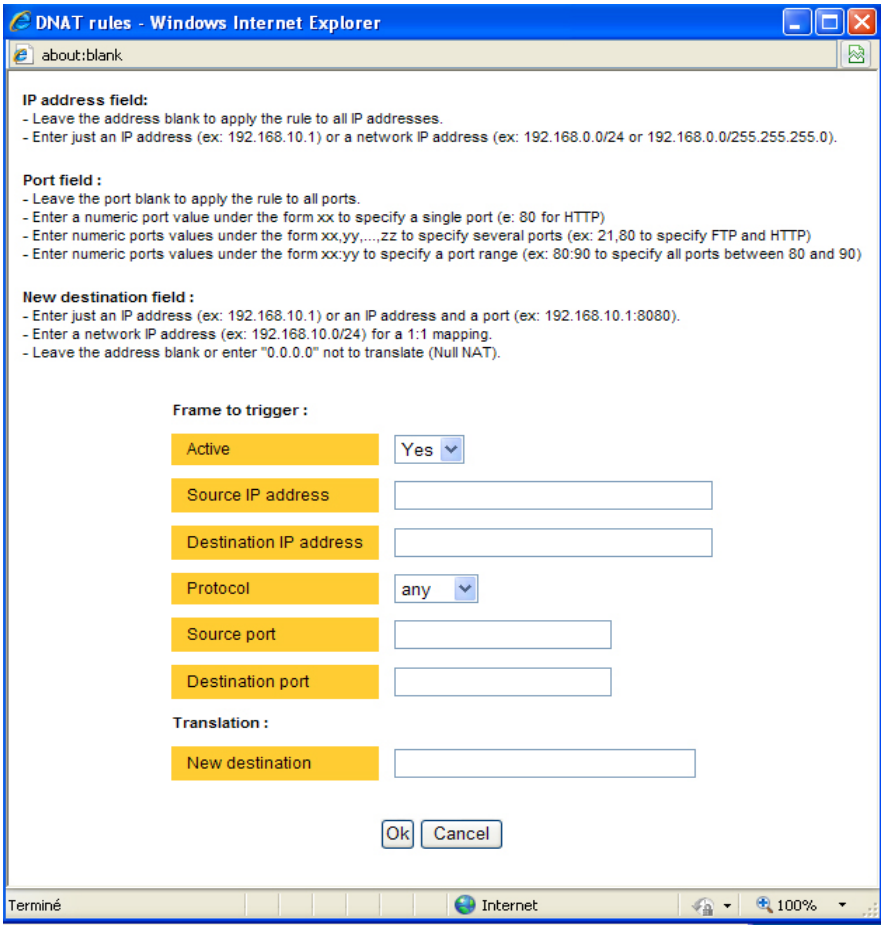
- select the "**Routing**" , and then the "**Advanced NAT**" menu.



To create a new DNAT rule

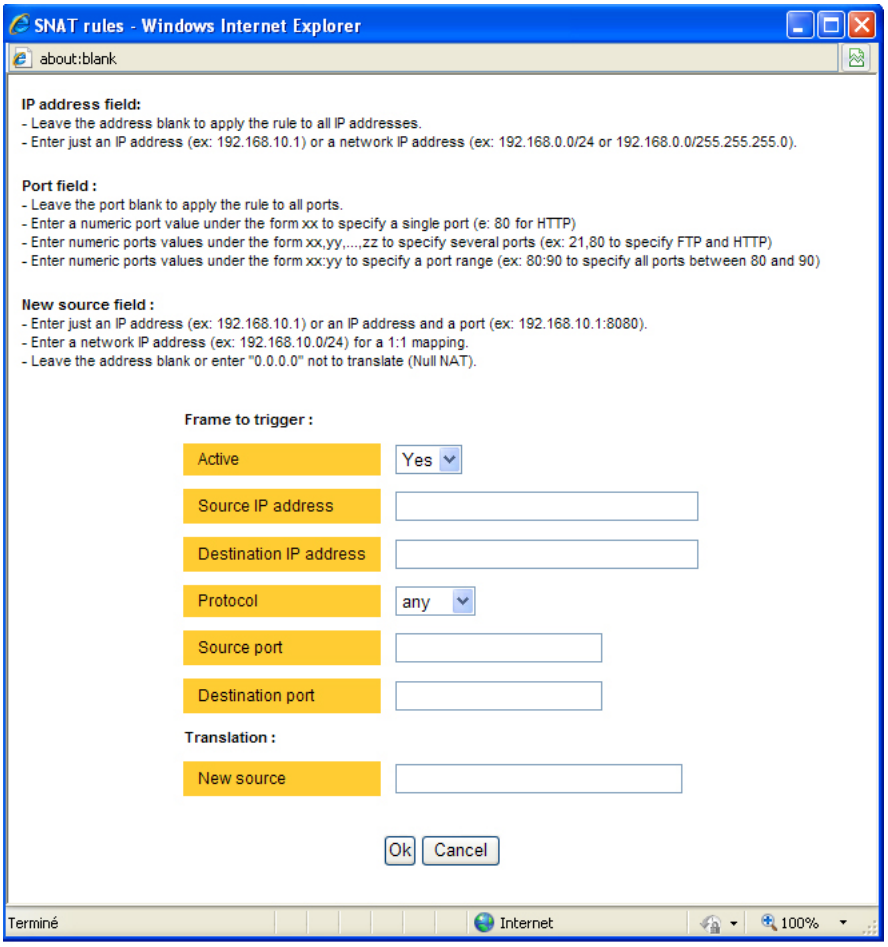
- Click "Add a DNAT" rule.
- Select "Yes" to enable the rule.
- Enter the replacement criterion :
  Source IP address & Destination IP address.
  Protocol (TCP, UDP, …)
  Source port & Destination port

- Enter the new destination port number and IP address.



To replace the source IP address & destination port

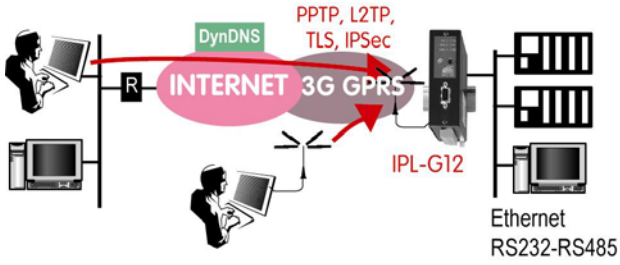
- Click "Add a SNAT" rule.
- Select "Yes" to enable the rule.
- Enter the replacement criterions :
  Source & Destination IP address.
  Protocol (TCP, UDP, …)
  Source & Destination port
- Enter the new source IP address.



16 Remote users connection (3G-GPRS-EDGE service)

16.1 Principles

RAS connection function
A remote user connection (RAS connection) is a tunnel set between a remote PC and the IPL-G12 router.



A remote user can set a RAS connection to the IPL-G12 router through the Internet.

The RAS connection gives access to all the devices connected the router.

Wireless interface IP address
The connection can be set only if a public (fixed or dynamic) IP address is assigned to the router on its wireless interface.

If the IP address is public but dynamic, the DYN DNS service can be used.

If the IP address is private, it is not possible to set a RAS connection towards the router through the Internet. In that case, the M2Me_Connect service is a suited solution.

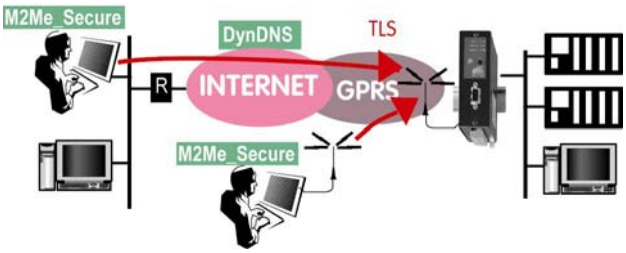
RAS connection safety
A remote user connection provides security and simplicity advantages :

- The remote user is identified with a login in and 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-G12 manages PPTP and TLS or L2TP remote connections.

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

16.2 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 an 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 theprotocol (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.

16.3 Configuring a PPTP VPN 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.

17 M2Me_Connect service

17.1 Overview

The M2Me_Connect service simplifies the connection of a remote PC to a machine through the Internet.

It provides a solution when a direct PPTP or TLS connection described before shows itself impossible.

Let us take the example of a machine made of several devices forming a “machine network” and connected to the Internet through an IPL-G12 router.

Suppose an expert wishes to connect to one or several of these devices to help repairing them or to upgrade a firmware.

The simplest solution should be to set a remote connection between the remote PC and the IPL-G12.

That solution is made impossible if, for instance, a private IP address is assigned by the wireless service provider to the router.

The M2Me_Connect service solves that difficulty :

The PC does not connect directly to the IPL-G12; both the PC and the router connect to the “M2Me_Connect” service.

Once both parties have been authenticated by the M2Me_Connect service with their own certificate, a TLS VPN is set from end to end from the PC to the IPL-G12 router.

The remote user identity is checked by the router to verify he or she belongs to the user list stored in the IPL-G12 router.

Finally, individual access rights are assigned to the remote user depending on his or her identity.

17.2 Configuring the M2Me_Connect connection

Step 1 : Router configuration

- Select the « Internet » menu and then « Connection ».

« M2Me_Connect » parameter:
Select “Activate”.

- Click “Properties” to tune the outgoing connection from the router to the M2Me_Connect” server.

“TCP ports” and “UDP ports” parameters :
Select the ports the router must check to set a connection to the M2Me_Connect service.

“Proxy” parameters :
Leave the proxy checkbox unselected.

- Test the connection

Click the “Control” menu, and press the “connect now” button.
Go to the ”Diagnostic” menu, “Network status” menu and then “M2Me”.
When the connection between the router and the M2Me_Connect service is established, the port number and protocol are displayed.

- Deselect the ports number needlessly selected

If too many ports have been selected, the connection delay may be long; it is why we advise to unselect all the ports except the one which has finally been successful.

Step 2 : Configuring 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 and the “M2Me_Connect” option.
  Enter the product key of the router; it can be pasted from the “About” menu of the router.

Attention : if you paste the product key, delete the last character and enter it again.

18 Remote users connection (GSM data service)

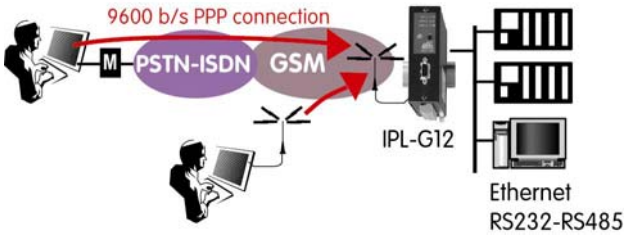
That feature is provided by the IPL-G12B router only.

18.1 Principe

If the GSM data service has been enabled, a remote PC, running a modem, can set a PPP switched connection to the IPL-G12 router.

The PPP remote connection can be set through the GSM network if the PC is equipped with a GSM data modem.

It can be set also through the telephone network (PSTN) if the PC is equipped with a V90 modem.



The login and password of the remote user is checked by the IPL-G12B router.

The default value of the login is admin and the default value of the password is admin.

An additional simultaneous remote connection can be set using a modem connected to the RS232 port of the IPL-G12B router.

The M2Me_Secure software makes the PPP conection easy.

18.2 Configuring the remote user connection

- Select the “Security” menu, click “VPN connections” and then “VPN parameters”;
- select the “Remote users connection VPN type” value : None

18.3 Configuring the remote user connection using an additional modem

- Select the “Security” menu, click “VPN connections” and then “VPN parameters”;
- select the “Remote users connection VPN type” value : None

- Select the “Modem” menu
- Select the “external modem activate” checkbox.
- Enter the initialisation string of the modem connected to the RS232 port of the router.

19 Configuring the users list

The user list registers 25 authorised remote users forms.

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.

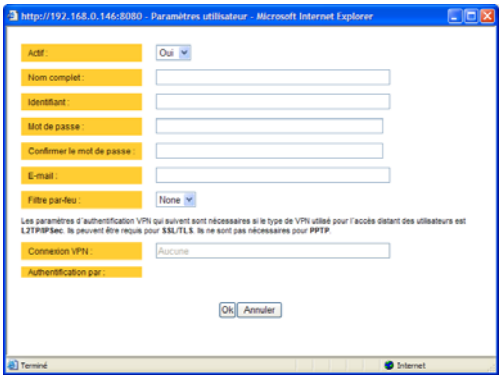
Select the “System” menu and then “User list”.

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-G12 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.

20 Configuring the firewall

20.1 Overview

The firewall of the IPL-G12 router is a stateful packet inspection firewall;

- it inspects the state of TCP or UDP or ICMP packet, to avoid spoofing.
- It includes a “deny of service” filter able to resist to saturation attacks;
- it checks the destination IP addresses and ports number of the remote users connections..

General filter
It cannot be configured.

It rejects all IP frames coming from the wireless network and sent to the IP address assigned to the router on the wireless network except :

The IP frames included in a VPN.

The IP frames sent to the IPL-G12 antenna IP address on particular ports if port forwarding rules has been created.

The IP frames included in a remote user connection, which are submitted to the remote user filter.

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

A remote user filter applies to the IP frames received inside a remote user connection (PPTP, TLS, L2TP/IPSec) from the wireless interface and towards the LAN interface. it checks the destination IP address and port number.

A filter can be assigned to a remote user (see User list).

According to his identity (Login and password, the remote user will thus only access to the IP domain defined by the filter.

20.2 Remote user filter

20.2.1 Filter structure

A filter is a table made of several lines; each line is called a rule.
A rule defines what decision has to be made when the firewall receives a particular IP frame from the wireless interface; the decision can be Reject or Allow.

Each rule of the filter is made of two fields which define a data flow :

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

Moreover, to describe the decision to carry out if a data flow matches a rule à filter policy has to be selected.

The policy can be

All is forbidden except what we specify.
Or
All is allowed except what we specify

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

Example :

Filter name : Access to the device PLC1 (html and modbus)		
Filter policy : All is forbidden except what we specify		
Rules list		
Action	Device	Service
Allow	PLC1 192.168.0.12	80
Allow	PLC1 192.168.0.12	Modbus 502

20.2.2 Configuration

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

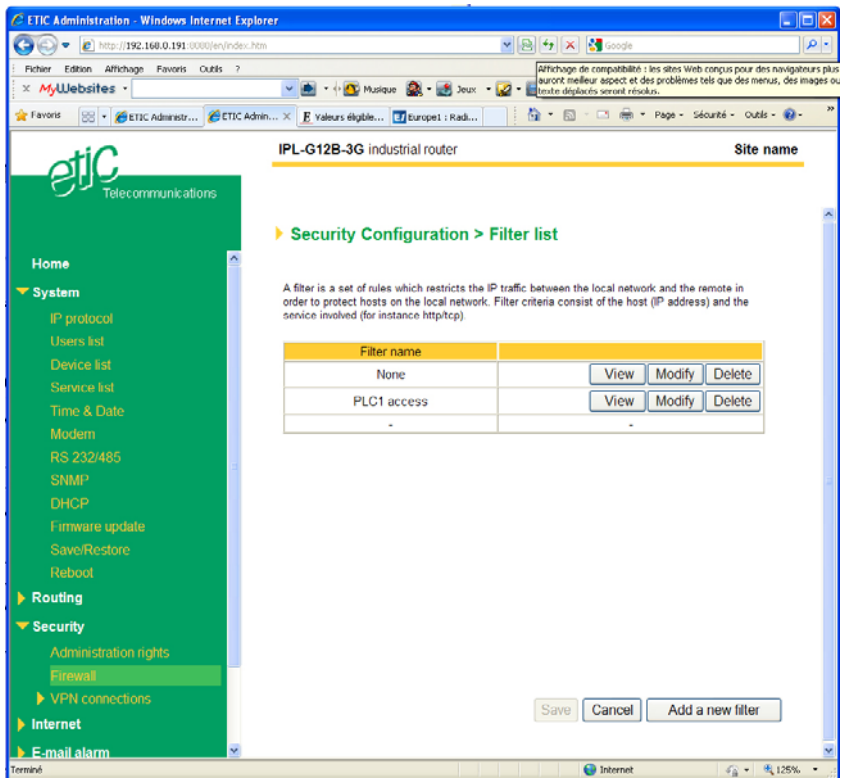
Important nota bene : The main services (html, ftp, modbus) are available from factory; for that reason, most of the time, that step can be skipped.

- 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.

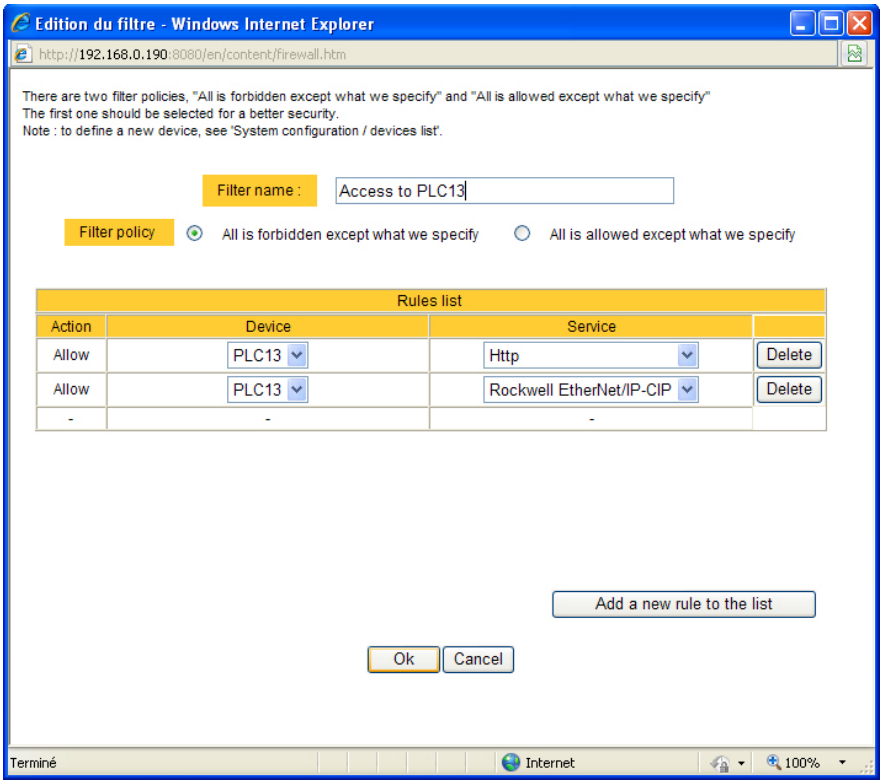
Step 2 : Enter the list of the devices connected to the LAN

- 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.

21 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 client or server :
To connect two serial devices, or one serial device and one TCP/IP device, through an IP network.

RAW UDP :
To exchange serial data between several serial or IP devices, through an IP network, using a table of IP addresses.

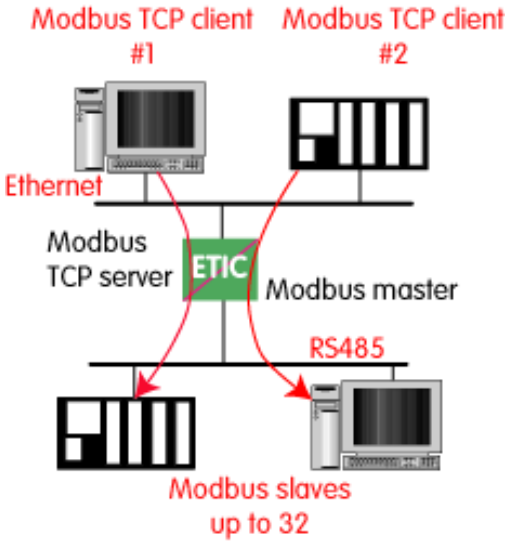
Telnet :
To connect a Telnet terminal to the IPL_G12 router.

Unitelway slave :
To connect a serial unitelway master to an IP network.

21.1 Modbus gateway

21.1.1 Modbus server gateway

This gateway allows to connect serial modbus slaves to the serial interface of the IPL-G12.



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

"Cache refreshment period" parameter :
Select the period at which the gateway will send request to the slaves PLC.

"Timeout waiting for the answer" parameter :
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.

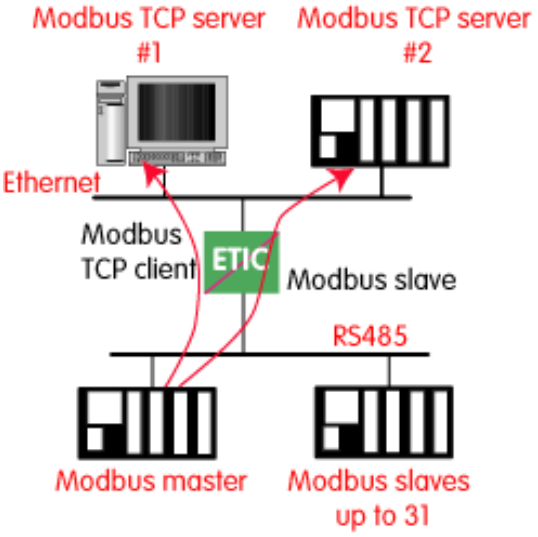
Modbus slave address :
Choose “specified by the modbus TCP client” , if the address of the slave PLC must be decoded by the gateway from the modbus TCP frame coming from the client.
Otherwise, specify the modbus address of the slave PLC; in that case only one slave can be connected to the RS232 serial 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.

21.1.2 “Modbus client” gateway

This gateway allows to connect a serial modbus master to the serial interface of the IPL-G12.



- 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.

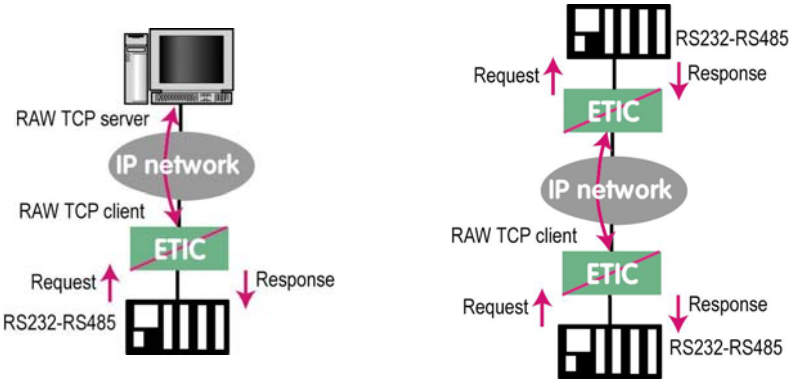
IP address :
The modbus client gateway allows to transmit modbus requests from the serial modbus master device to any modbus slave device, more precisely called “ modbus server”, located on the IP network.

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.

21.2 RAW TCP gateway

21.2.1 Raw TCP client gateway

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



The serial device must be for example a master device in half duplex protocols.

- 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.

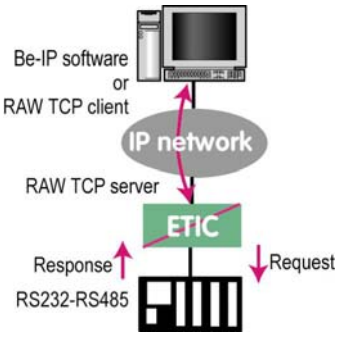
TCP inactivity Timeout :
Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

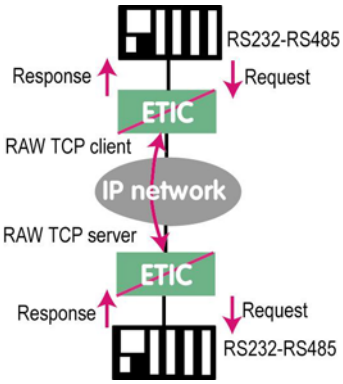
TCP port number :
Set the port number the gateway has to use.

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.

21.2.2 Raw TCP server gateway

That gateway can be used if a serial slave device has to answer requests coming from devices (client devices) located on the IP network.





- 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” parameter :
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 inactivity Timeout" parameter :
Set up the time the gateway will wait before disconnecting the TCP link if no characters are detected.

"TCP port number" parameter :
Set up the port number the gateway has to use.

21.3 RAW UDP gateway

21.3.1 Overview

The RAW UDP gateway permits to connect together a group of serial devices through an IP network.

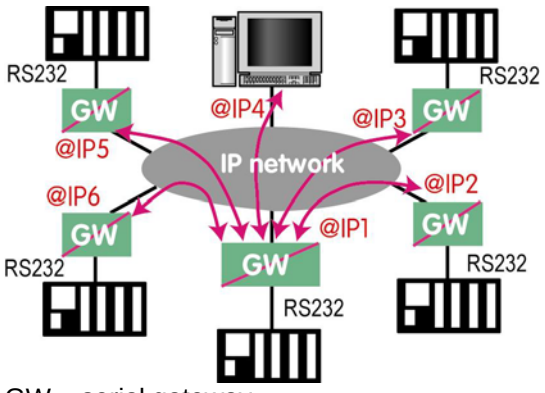
The group can also include IP devices if they have the software pieces able to receive or transmit serial data inside UDP.

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

A table of IP destination gateways is stored in each IPL-G12 belonging to the group.

The serial data is encapsulated in the UDP protocol.

The UDP frame is sent to each destination IP address stored in the table.



GW = serial gateway

21.3.2 Configuration

- Select the “gateway” menu and then the “Transparent” menu and then click “RAW UDP”.

- Select the “Activate” option.

« Serial input buffer size” **parameter** (value 1 to 1024) :
Sets the maximum size of an UDP frame.

“End of frame time-out” parameter (value 10 ms to 5 sec) :
Sets the delay the gateway will wait before sending the UDP frame towards the IP network when no characters are received from the serial interface.

«UDP port number» parameter :
Sets the UDP port number.

“IP addresses of the destination devices » table :
This table stores the IP addresses of the gateways to which the serial data, encapsulated inside UDP, have to be sent.
A different UDP port number can be entered for each destination IP address.

22 Advanced functions

22.1 Adding a certificate

Coming from the factory, the IPL-G12 router includes a certificate delivered by ETIC TELECOM acting as a certification authority.

That certificate can be used to set a VPN between two routers.

Two IPL-G12 routers can set a VPN with one another using certificates only if the certificates have been provided by the same authority.

Additional X509 certificates, provided by ETIC Telecommunications or not, can be downloaded into the router.

To import a new certificate, the file extension can be PKCS#12 with a password or PEM.

Even if more than one certificate have been downloaded into the IPL-G12 router, one certificate can be used for all the connections.

22.2 Alarms

22.2.1 SNMP

The IPL-G12A router is able to send snmp traps when alarms occur.

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

"SNMP network management IP address" parameters :
Enter the IP address of the management platform

"SysName" & "SysLocation" parameters :
That fields allow to identify the source device.
Example :
Sysname : etic
Syslocation : France

"Product start-up" parameter :
If that option is selected, the router will send an SNMP trap each time it will connect to the Internet

22.2.2 Digital output alarm

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

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

22.2.3 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 and click "email".

"Enable the alarm email" parameter :
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" parameter :
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" parameter :
Select the time the input has to stay in its alarm state to be taken into account.

"Alarm destination" parameter :
Select the user to whom the email must be sent.

"Text to send" :
Enter the email text.

22.3 Configuring the web portal

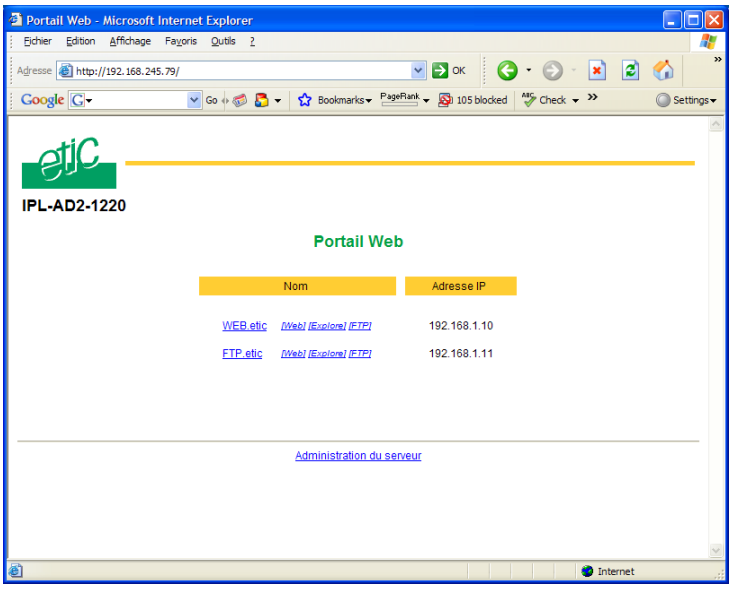
The web portal in an html page; it displays a list of devices connected to the LAN. Each line of the list is made of the device name, its IP address and three links :

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-G12 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.



22.4 Configuring the DNS server

For domain names resolution, the IPL-G12 can behave like a domain name server or a domain name relay.

DNS server :
A domain name server is a networking device which is able to associate a label (etictelecom.com for instance) with an IP address.

That function allows a client device to send a request to a network equipment referring to a domain name as if it was the actual IP address of the destination device.

The IPL-G12 router is able to resolve any domain name composed with the name of one of the devices entered in the devices list followed the site name which is entered at the top of the devices list.

DNS relay :

The IPL-G12 router behaves also like a DNS relay; any DNS request it receives from the LAN, which cannot be resolved because the device is not registered in the devices list, will be transferred to the internet to be resolved.

That function can be carried out only if the IPL-G12 IP address is pointed out as the main DNS server of the devices of the LAN.

That function is efficient in particular when a device connected to the LAN has to send emails through the Internet.

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 :

VPN and users connections and disconnections,
power on,
Serial gateway events.

- **Network status sub-menu :**

That page displays the current status of the LAN interfaces and of the GSM connection :

LAN interfaces :

That part of the page shows the data of the LAN interface :

MAC address,
Ethernet mode (10 /100, half or full),
IP address.

Modem :

That part of the page shows the data of the Internet interface :

GSM IP address,
DNS IP address.

The “View statistics” button gives access to the ADSL statistics windows; that windows shows

the reception signal attenuation,
the Signal to noise margin (SNR margin),
G821 error rates indicators.

- **VPN sub-menu**

That menu displays the table of the VPN (remote user connections and remote routers connections) which are established.

- **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 each 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 to a 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. 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_iplg12_V241.bin”.

3 Firmware update

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 uImage.

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
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
Advanced NAT	To substitute source or destination port and IP addresses

Security

Administration	To restrict access to the administration server
Firewall	To restrict access to devices of the LAN
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 raw TCP or UDP & telnet gateway
Unitelway	To configure the unitelway gateway

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

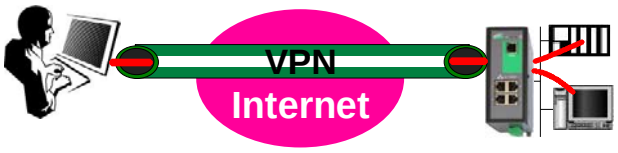
Alarms	To enter the conditions an email is transmitted to a user
About identification	To display the firmware and hardware

1 Overview

VPN is the acronym for « virtual private network » ; it is a mechanism which allows to connect safely 2 end-points, two routers for instance or one router and one PC, through a network not intrinsically safe.

Once a VPN has been set between two routers , any device of the first network can communicate with any device of the second one as if the two routers were directly connected with an Ethernet cable.

A VPN allows also to connect a remote user to the devices of a network.



2 Functions

A VPN provides the functions described hereafter :

Authentication
The VPN ensures that the party with which the communication is set is actually **the one it claims to be.**

Data integrity
The VPN mechanism ensures that information being transmitted over the public Internet is not altered in any way during transit

Confidentiality
A VPN protects the privacy of information being exchanged between communicating parties.

3 Operation

Authentication phase
The first operation the end-points carry out is authentication.

2 levels of authentication can be performed using a VPN :

Device level authentication
A code is stored in each end-point (i.e. router or PC); it can be a Key or a certificate delivered by a certification authority.
During the initial phase, the two end-point exchange their codes; each party checks that the other party code is valid.

User level authentication
The IPL-G12 router holds a user list; once a VPN has been set with the remote user PC, the remote user identification code and password is checked.

Encrypted tunnel transmission phase
Once the end-points have exchanged and checked each other identity code, they set the VPN tunnel.
It is an Ip frames exchange; the source and destination IP addresses are the end-points.
That tunnel encapsulates the encrypted IP data flow transmitted between any of the devices connected to each end-point.

VPN clearing
Periodically, each router (or at least the VPN server router) sends to the other one a control message to check the VPN must remain established.

If no response is received from the other party, the VPN is cleared.

Distribué par :

HVS.
PRECONISATEUR DE SOLUTIONS DEPUIS 1985

Contact :
hvssystem@hvssystem.com

Tél : 0326824929
Fax : 0326851908

Siège social :
2 rue René Laennec
51500 Taissy
France
www.hvssystem.com

etic TELECOMMUNICATIONS

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