

The IPL-M156 and IPL-I1128 and IPL-L134 routers are manufactured by

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 : hotline@etictelecom.com
web : www.etictelecom.com

OVERVIEW

1	PRODUCTS IDENTIFICATION.....	6
2	SPECIFICATIONS.....	7
3	PRODUCT OVERVIEW.....	9

INSTALLATION

1	PRODUCT DESCRIPTION	13
1.1	Leds.....	13
1.2	Connectors	13
1.3	DIP-switches.....	16
2	VENTILATION.....	16
3	SUPPLY VOLTAGE.....	16
4	ETHERNET INTERFACE.....	16
5	RS232 INTERFACE	17
6	RS485 INTERFACE	17
7	INPUT & OUTPUT CONNECTION	17
8	PSTN LINE (IPL-M156).....	18
9	ISDN LINE (IPL-I1128).....	19
10	DEDICATED LINE (IPL-L134).....	19

CONFIGURATION

1	OVERVIEW	20
2	CONNECTING A PC TO THE ETHERNET INTERFACE.....	20
3	MODIFYING THE CONFIGURATION PARAMETERS THROUGH THE LAN	21
4	WRONG IP ADDRESS OR PASSWORD	21

../..

...CONFIGURATION

5	SAVING CONFIGURATION MODIFICATIONS.....	22
6	ASSIGNING AN IP ADDRESS TO THE LAN INTERFACE	22
7	MODEM CONFIGURATION	23
7.1	PSTN modem (IPL-M156).....	23
7.2	ISDN adapter (IPL-I1128)	23
7.3	Dedicated line modem (IPL-L134).....	23
8	CONFIGURING CONNECTIONS BETWEEN ROUTERS.....	24
8.1	Dial-up PSTN or ISDN connection.....	24
8.2	Dedicated line connection.....	27
9	CONFIGURING STATIC ROUTES	30
10	REMOTE USERS CONNECTION.....	31
10.1	Configuring the users list.....	32
11	RESTRICTING THE RIGHTS OF A REMOTE USER	33
11.1	Filter structure.....	33
11.2	Configuration.....	34
12	SERIAL TO IP GATEWAY	37
12.1	Modbus gateway	38
12.2	RAW TCP gateway	41
12.3	Multicast gateway	43
13	ADVANCED FUNCTIONS	45
13.1	Alarms	45
13.2	Configuring the web portal	47
13.3	Restricting access to the administration server	48

../..

MAINTENANCE

1	DIAGNOSTIC	49
2	SAVING THE PARAMETERS FILE.....	50
3	UPDATING THE FIRMWARE.....	50

APPENDIX 1 : HTML configuration server

1 Products identification

	IPL-M156	IPL-I1128	IPL-L134
Analog switched telephone line (PSTN)	•		
ISDN ETSI BRI interface (one B channel 64 kb/s)		•	
Dedicated, voice band, 2 wire line			•
RJ45 Ethernet 10 Mb/s	1	1	1
RS232-RS85	1	1	1
IP router	•	•	•
NAT – DNAT – Port forwarding	•	•	•
SNMP traps	•	•	•
DNS	•	•	•
DHCP client or server (LAN interface)	•	•	•
Firewall SPI	•	•	•
Remote access server (RAS)	•	•	•
VPN PPTP, IPSEC, SSL	•	•	•
Remote access server	•	•	•
Digital input for email alarms	3	3	3
Serial gateway : Raw TCP client and server, Telnet server, Multicast, Modbus client and server, Unitelway	•	•	•
Html Configuration	•	•	•
Option software IO Viewer	•	•	•

2 Specifications

General characteristics	
Dimensions	136 x 38 x 108 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 40 VDC - 170 mA at 24 VDC
Operating T°	-20°C / + 60°C Humidity 5 - 95 %

PSTN / ISDN / Dedicated line	
PSTN	Analog PSTN line (2 wires) V90 modem 56 kb/s DTMF and pulse dialling International and programmable line interface
ISDN	ETSI EURO-ISDN conform BRI interface 1 B channel management (64 kb/s)
Dedicated line	2 wires line V34 modem –33.4 kb/s Voice band 300-3400 Hz

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

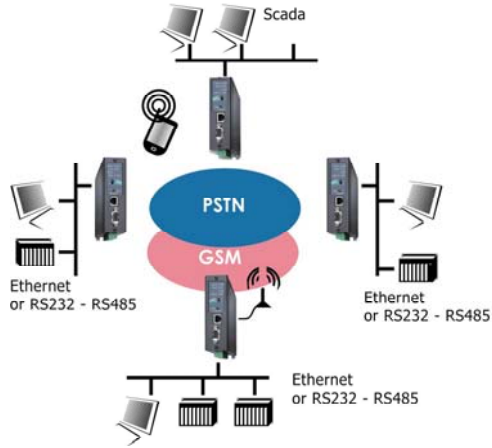
Remote access server (RAS)	
User list	25 users
Connection	PPP connection Login & password call-back
Alarms	3 inputs : emails

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

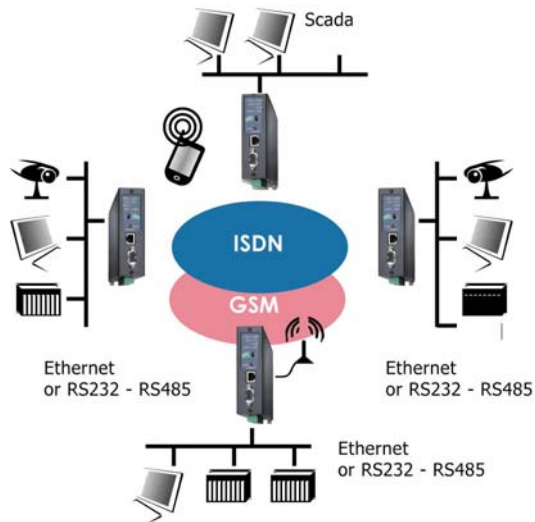
3 Product overview

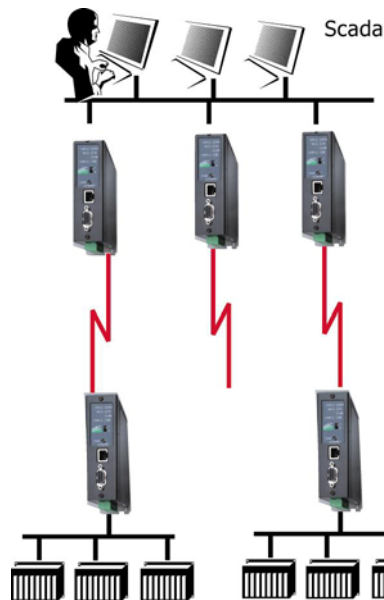
The IPL is designed to interconnect safely automated devices over the PSTN or ISDN or dedicated lines.

PSTN network



ISDN network



Dedicated line network**IP router**

The IPL 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 router is able to establish safe VPN tunnels.

Once a VPN is established between two IPL routers, 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 router, the remote user can access to the devices connected to the router.

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

SPI Firewall

The IPL incorporates a firewall.
The firewall controls the status of the sessions (TCP, UDP, ICMP) to avoid spoofing attacks.

DNS server

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

DynDNS client

The IPL router is compatible with the Dyn DNS service.

DHCP client or server

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

Emails – sms

An email can be sent each time one of the three digital inputs is opened or closed.

SNMP

The IPL router is an SNMP agent.

Html and DIP switches configuration

The IPL is configured with a web server .
Two DIP switches allow to set the method the products 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 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

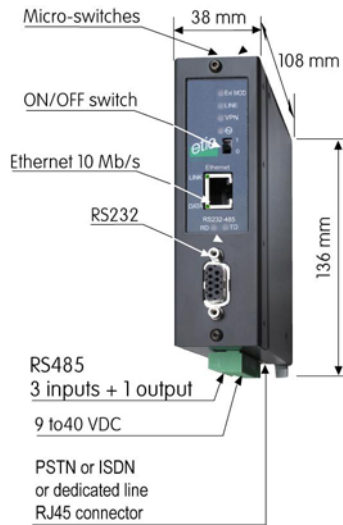
The product includes an up-to-date RS to IP gateway, enabling to connect serial devices safely to the GSM network and the Internet.

EticFinder software

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

1 Product description

IPL-M156 or IPL-I1128 or IPL-L134



1.1 Leds

	Function
Line /	Lit : Remote connection set Blinking : Remote connection in progress The number of blinks gives an indication of the signal level.
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)
	Lit : Operation Blinking : hardware defect

1.2 Connectors

pins screw-block : Supply voltage		
Pin	Signal	Function
1	+	9 to 30 V – 300 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	⇒

ISDN RJ45 connector IPL-I1128		
Pin	Polarity	
1		
2		
3	+	Emission to ISDN
4	+	Reception from ISDN
5	-	Reception from ISDN
6	-	Emission to ISDN
7		
8		

PSTN or dedicated line RJ45 connector IPL-M156 or IPL-L134		
Pin	Polarity	
1		
2		
3		
4		Telephone line wire 1
5		Telephone line wire 2
6		
7		
8		

Nota bene :
An RJ11 PSTN cable can be connected to the RJ45 connector of the IPL-M156 or IPL-L134.
The 2 wires of the PSTN or dedicated line must be present on wires 3 and 4 of the RJ11.



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	No IP @ is assigned to the product; DIP switch configuration

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 200 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 interface

The router provides an RS232 and an RS485 interface. Serial devices can thus be integrated to the IP network.

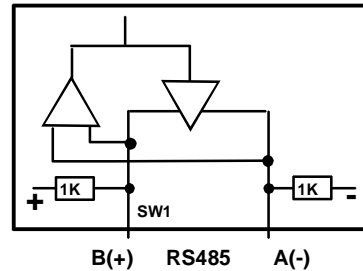
The RS232 cable must not be longer than 10 meters.

6 RS485 interface

The RS485 serial interface is provided on the 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.

7 Input & output connection

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.

8 PSTN line (IPL-M156)

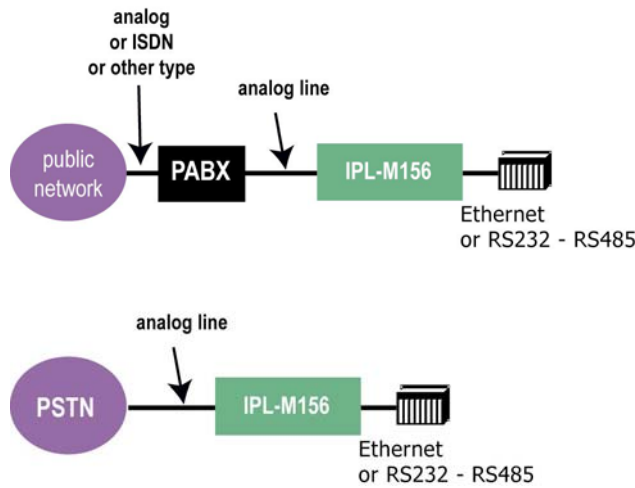
The IPL-M156 is designed to be connected to an analog telephone line.

That line can be an analog public line (PSTN subscriber line) or an analog line connected to a company telephone switch PABX (also called extension line).

The line connector located at the bottom of the router is an RJ45 8 points connector. But an RJ11 telephone cable can be used; The two active telephone wires are the wires number 4 and 5 located in the middle of the connector.

If the IPL line is an extension line, connected to a company PBX, it must be a Direct Inward Dialling line (DDI or DID) in such a way that the remote router can dial the IPL number and be connected directly to the IPL bypassing the operator.

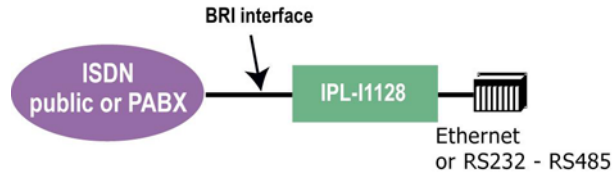
Important nota : The type of public lines connecting the company PABX to the public network does not matter; it can be PSTN but also ISDN, for instance.



9 ISDN line (IPL-I1128)

The IPL-I1128 is designed to be connected to a ISDN BRI interface (EURO-ISDN compliant).

It manages only one B channel providing 64 kb/s data rate.



10 Dedicated line (IPL-L134)

The IPL-L134 is designed to be connected to **a two wire dedicated line**.

The line must be a voice band line. It can be private or leased.

The line connector located at the bottom of the router is an RJ45 8 pins connector. The two telephone line wires are the wires number 4 and 5 located in the middle of the connector. An RJ11 telephone cable can be connected to the RJ45 connector. In the RJ11 connector, the telephone wires must be on pins 3 and 4

1 Overview

The IPL router is configured with a PC and an HTML browser.
2 DIP switches enable you to set the IP address : Factory address, stored address, BootP or DHCP client or server.

For the first configuration, we advise to connect the PC directly to the router Ethernet interface.

Modifications can be carried out through the LAN or remotely.

2 Connecting a PC to the Ethernet interface

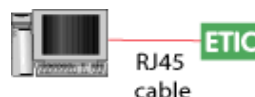
Step 1 : Check the DIP switches SW1 and SW2; they must be set to OFF and OFF to select the stored IP address, or, if necessary, to ON and OFF to restore the factory IP address.

Coming from factory, the DIP switches SW1 and SW2 are set OFF (ready for configuration); and the IP address of the IPL is 192.168.0.128.

Step 2 : Create or modify the PC TCP/IP connection

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

Step 3 : Connect the PC directly to an IPL Ethernet interface using a cross wired Ethernet cable.



Step 4 : Launch the navigator

Enter the IP @ of the IPL..

The Home page of the administration server is displayed



3 Modifying the configuration parameters through the LAN

- **If the IP @ of the IPL is assigned by a BOOTP - DHCP server**

Step 1 : Check the DIP switches SW1 is OFF and SW2 OFF to select DHCP / BOOTP operation.

Step 2 : Launch ETIC FINDER to detect the IPL over the LAN.

Click the product once detected.

The Home page of the administration server is displayed.

Note :

If the home page cannot be displayed, refer to paragraph 4 below.

- **If the IP @ of the IPL is fixed**

Launch the html browser and enter the IP address assigned to the router.

Or, launch the ETICFINDER utility.

- **Configuration modifications through the Internet**

Modifications can be also carried out through the Internet.

We advise to protect the access to the administration server with a password.

The modifications have to be carried out cautiously to avoid to loose the link with the router.

4 Wrong IP address or password

When launching the html browser, the homepage of the html server may not be displayed; the cause may be the IP address you entered or the password you used were wrong.

if the IP address you enter is wrong, you can recover the factory IP address by setting SW01 ON and SW2 OFF.

The factory IP address 192.168.0.128 will be restored as long as the SW01 micro switch will be left ON. Once, SW01 will be set OFF, the

stored IP address (the IP address which is displayed) will be used by the product.

Wrong Login to the administration server

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

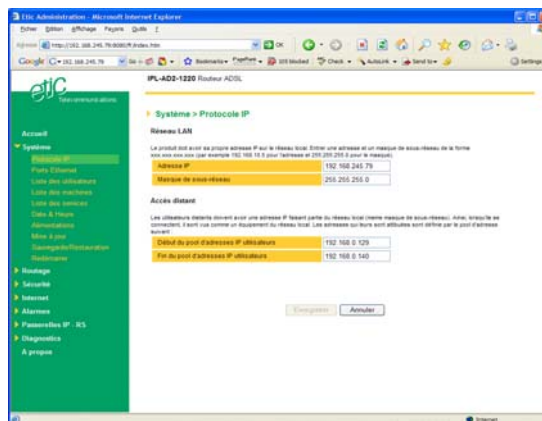
Careful : The factory IP address 192.168.0.128 will also automatically be assigned to the product as long as SW01 will remain ON and SW2 OFF.

5 Saving configuration modifications

- Once modifications of the parameters of one page have been carried out, click the « Save » button at the bottom of the screen.
- After some parameters changes, the IPL must restart. When the configuration has been completely carried out, click the « **Reboot** » red button in the green bar, if it is displayed.
- Once the product has restarted, check the red « **Reboot** » button has disappeared from the green bar.
- If you wish, save the configuration file using the “Save restore” menu.

6 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.

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.

7 Modem configuration

7.1 PSTN modem (IPL-M156)

- Select the "System" menu and then "Modem".
- Enter the prefix the router has to dial when the router is connected to a PABX line.
- Check that the "Use default initialisation string" option is selected.
- Check that the "Permanent link (Leased Line)" option is not selected.

7.2 ISDN adapter (IPL-I1128)

- Select the "System" menu and then "Modem".
- Enter the prefix the router has to dial when the router is connected to a PABX line.
- Check that the "Use default initialisation string" option is selected.
- Check that the "Permanent link (Leased Line)" option is not selected.

7.3 Dedicated line modem (IPL-L134)

- Select the "System" menu and then "Modem".

- Check that the “Use default initialisation string” option is selected.
- Select the “Permanent link (Leased Line)” option

8 Configuring connections between routers

All the remote routers with which an IPL router will have to communicate have to be declared as a remote node.

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

8.1 Dial-up PSTN or ISDN connection

The connection with a remote node 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 router dials towards the remote router when IP frames 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.



The table below explains the parameters in that three types of connection.

PSTN or ISDN switched connection			
Type of connection			Parameter description
OUT	IN	OUT & IN	
X	X	X	<u>“Enable” parameter :</u> Select the “yes” option.
X	X	X	<u>“Type” parameter :</u> Select the “switched” choice.
X	X	X	<u>“Node name” parameter :</u> Assign a name to the node.
X	X	X	<u>“call direction” parameter :</u> 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	<u>“Remote router IP @” and “Remote network netmask” parameter :</u> Enter the IP address and the netmask of the remote router Ethernet interface.
X		X	<u>“Modem” parameter :</u> Select the “built-in” choice.
X		X	<u>“Dial number” parameter :</u> Enter the number the router has to dial to connect to the remote router.
X		X	<u>“My login” and “My password” parameters :</u> Enter the login and the password the router has to transmit to the remote router to connect to it.
	X	X	<u>“Node login” and “Node password” parameters :</u> 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	<u>“Idle time-out” parameter (5 s to 60 mn) :</u> Set the time duration of the silence before the router will clear the call.
X		X	<u>“First packet time-out” parameter (5 s to 60 mn) :</u>



PSTN or ISDN switched connection / advanced parameters			
Click the “advanced conf.” button to configure advanced functions :			
Type of connection			Parameter
OUT	IN	OUT & IN	
	X	X	<p><u>“Verify calling number” and “calling number” parameters :</u> Select the option “yes” and Enter the telephone number of the remote router to force the router to check the calling number.</p>
X	X	X	<p><u>“Firewall filter” parameter :</u> Select the firewall filter assigned to the connection</p>
X	X	X	<p><u>“NAT” parameter :</u> 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.</p>
X	X	X	<p><u>“Router PPP IP address ” and “Remote router PPP IP address” parameters :</u> Enter the IP address assigned to the PPP interface. If no IP address is entered, the address of the Ethernet interface is assigned automatically.</p>

8.2 Dedicated line connection

The connection with a remote node can be an outgoing connection or an ingoing connection

If the connection is declared as an outgoing connection in a router, it must be declared as an ingoing connection in the remote router.



The table below explains the parameters to configure in both cases :

Dedicated line connection (IPL-L134)		
Type of connection		
OUT	IN	Parameter description
X	X	<u>“Enable” parameter :</u> Select the “yes” option.
X	X	<u>“Node name” parameter :</u> Assign a name to the node.
X	X	<u>“call direction” parameter :</u> 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.
X	X	<u>“Remote router IP @” and “Remote network netmask” parameter :</u> Enter the IP address and the netmask of the remote router Ethernet interface.
X		<u>“Modem” parameter :</u> Select the “built-in” choice.
X		<u>“My login” and “My password” parameters :</u> Enter the login and the password the router has to transmit to the remote router to connect to it.
	X	<u>“Node login” and “Node password” parameters :</u> Enter the login and the password of the remote router. These login and password are checked by the router when a call is incoming.

Dedicated line connection / advanced parameters		
Click the “advanced conf.” button to configure advanced functions :		
Type of connection		
OUT	IN	Parameter
X	X	<u>“Firewall filter” parameter :</u> Select the firewall filter assigned to the connection
X	X	<u>“NAT” parameter :</u> 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	<u>“Router PPP IP address ” and “Remote router PPP IP address” parameters :</u> Enter the IP address assigned to the PPP interface. If no IP address is entered, the address of the Ethernet interface is assigned automatically.

9 Configuring static routes

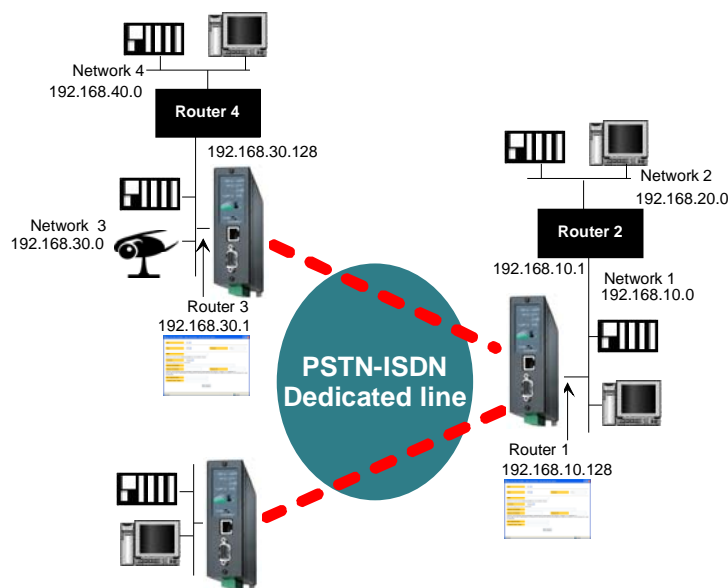
If the destination network is not connected to one of the remote routers linked to the router by a remote connection, the devices of that destination network cannot be reached.

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 :

Enter the destination network IP address and netmask.

Gateway IP address :

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

10 Remote users connection

10.1 Overview

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

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

- the remote user identity code and password is checked;
- individual access right are automatically allocated to the user in accordance with his or her identity;
- an IP address is automatically assigned to the remote PC;

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

Attention : Coming from factory, a default user is registered; his login is **admin** and the password is also **admin**.

10.2 Configuring the users list

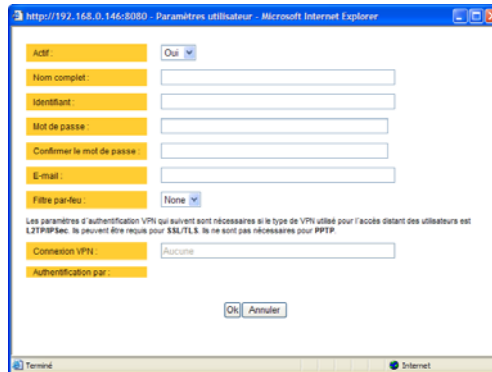
Select the “System” menu and then “User list”.

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 :

It is the name displayed in the user list.

Login & password

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

E-mail :

The IPL router will send an email to that address in two situations :
Alarm email : the router sends an alarm email to the defined user If the input 1 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. (See OPERATION chapter).

Firewall filter :

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

11 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.

11.1 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.

11.2 Configuration

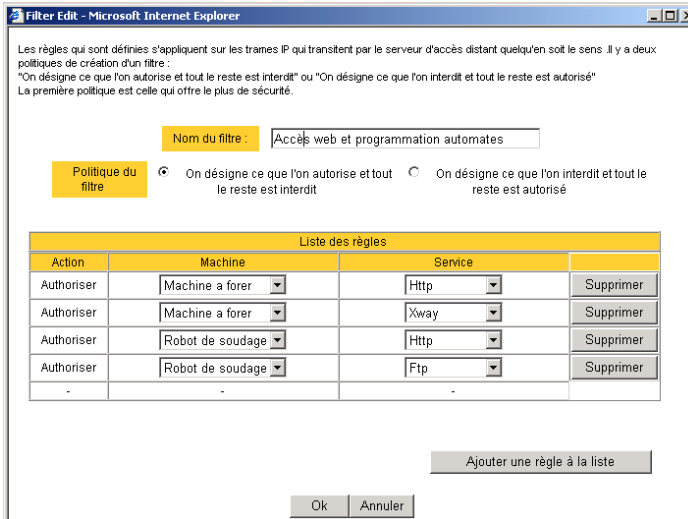
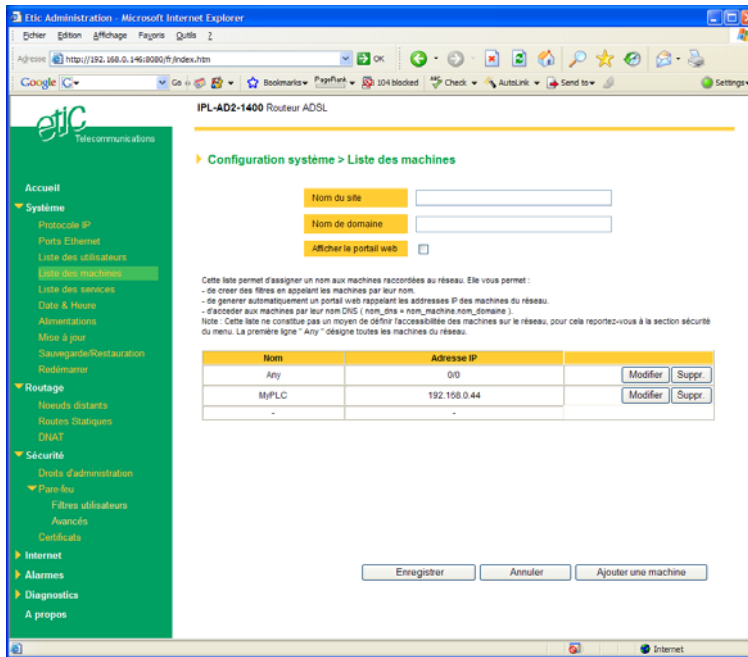
Step 1 : Complete, if necessary, the list of TCP ports.

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 : 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 3 : Assign a filter to each user

- Select the « System » menu and then « User list ».
- Among the users select a 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.

12 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.

Telnet :

To connect a Telnet terminal to the IPL.

RAW UDP :

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

Multicast :

To exchange serial data between a great number of serial and IP devices, through an IP network, using the multicast technology.

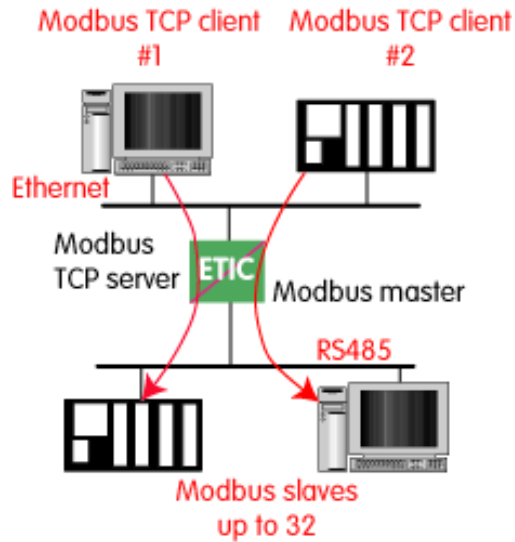
Unitelway slave :

To connect a serial unitelway master to an IP network.

12.1 Modbus gateway

12.1.1 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 :

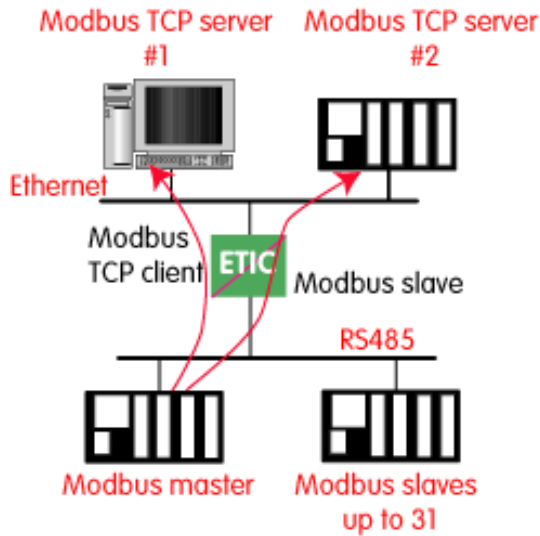
Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

TCP port number :

Set the port number the gateway has to use.

12.1.2 “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.

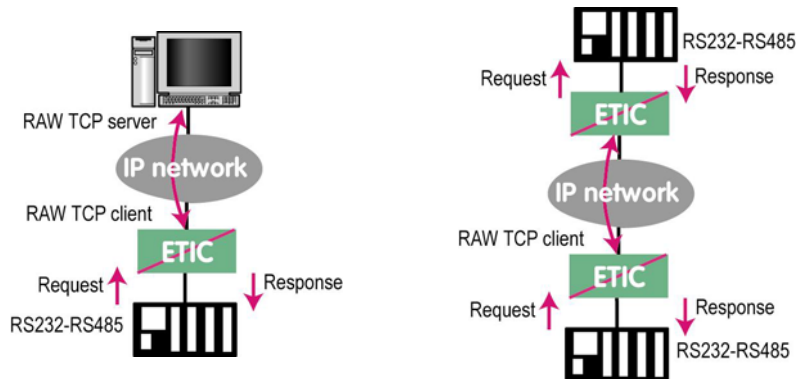
IP address :
The modbus client gateway allows to transmit modbus requests from the serial modbus master device to any modbus slave device, more precisely called “ modbus server”, located on the IP network.

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.

12.2 RAW TCP gateway

12.2.1 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.

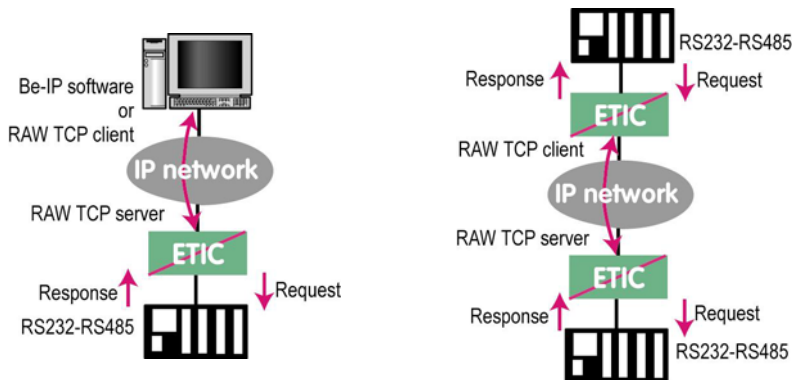
Raw server IP address :

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

Assign an IP address to define the destination gateway.

12.2.2 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.

12.3 Multicast gateway**12.3.1 Overview**

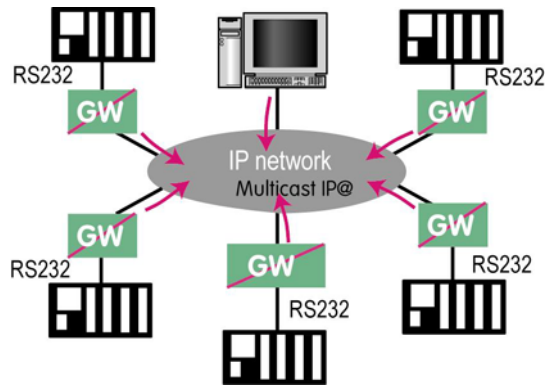
The multicast gateway permits to connect together a group of serial devices, and also Ethernet IP devices, through an IP network.

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.

12.3.2 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.

13 Advanced functions

13.1 Alarms

13.1.1 SNMP

The IPLA 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

13.1.2 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.

13.1.3 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.

13.2 Configuring the web portal

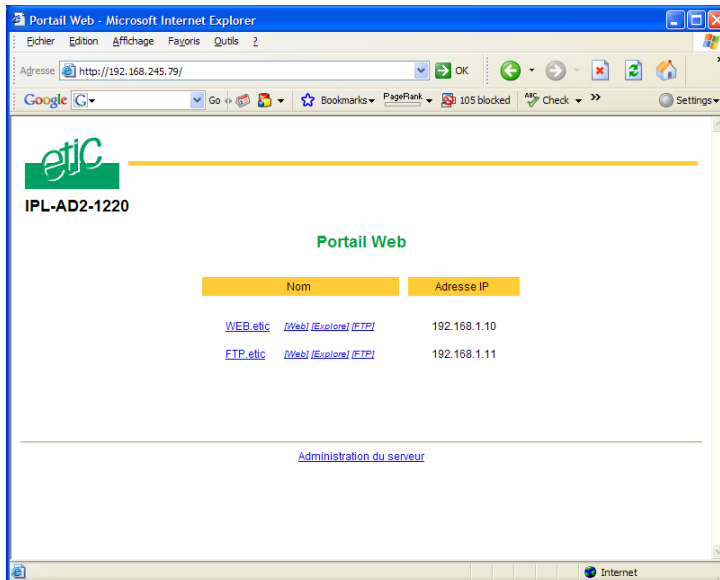
The web portal in an html page; it displays a list of devices connected to the LAN. Each line of the list is made of the device name, its IP address and three links :

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 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.

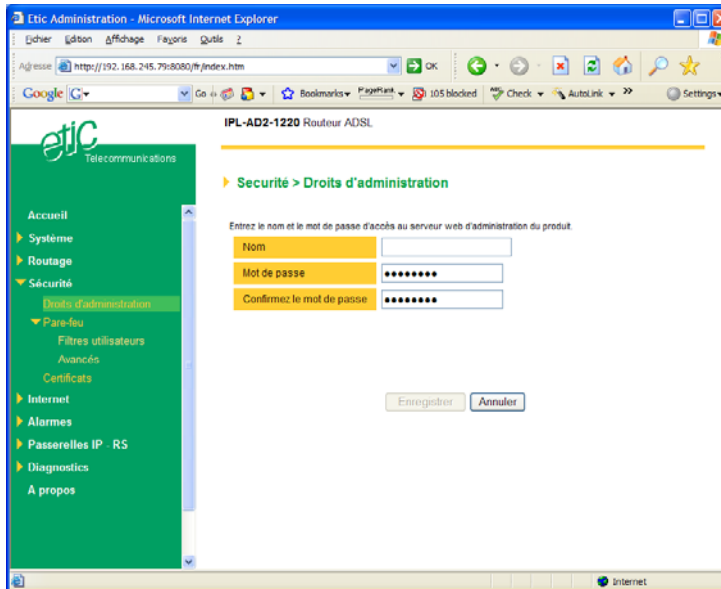


13.3 Restricting access to the administration server

The « administration rights » menu allows to restrict access to the administration server with a login and a password

If the login and or password have been forgotten, free access to the administration server can be recovered by setting the micro-switch 1 ON and the micro switch 2 OFF.

Attention : When the micro-switch 1 is set ON, and the micro-switches 2 is set OFF, the factory IP address 192.168.0.128 is restored.



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

Distribué par :

Contact :
hvssystem@hvssystem.com

Tél : 0326824929
Fax : 0326851908

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



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