IPL-E **IPL-A** **IPL-C**

Ethernet ADSL Cellular Routeur Firewall

SETUP GUIDE

Document reference : 9023409-01

The IPL family of IP routers is manufactured by

ETIC TELECOM

13 Chemin du vieux chêne
38240 MEYLAN
FRANCE

TEL : + 33 4-76-04-20-00
Hotline : + 33 4-76-04-20-05
FAX : + 33 4-76-04-20-01
E-mail : hotline@etictelecom.com
web : www.etictelecom.com

CONTENT

CONTENT

IPL ROUTER SETUP

CONTENT

… IPL ROUTER SETUP

CONTENT

1 Subject of the manual

This manual describes how to set-up the IPL family of routers manufactured by ETIC TELECOM

That manual applies in particular to the models listed below :

Ethernet interfaces IP router	IPL-E
ADSL router	IPL-A
Cellular LTE-UMTS-GPRS router	IPL-C
WiFi router	IPL-EW
ADSL & cellular router	IPL-DAC
Cellular backup router	IPL-DEC

2 Main features of the IPL routers

IP routing

The IPL family of routers provides an extended panel of routing functions among which :

- Static routes
- Source and destination address translation
- Port forwarding
- RIP and OSPF
- DynDNS.

IPSec & OpenVPN VPNs

The IPL routers are able to establish IPSec or OpenVPN VPNs.

IPSec will be preferred when it is the solution selected for a system for security reasons for instance or if the IPL ETIC TELECOM router must establish a VPN towards another router providing only IPSec.

OpenVPN will be preferred for its ease of use because it is transported by TCP or UDP.

Firewall

The IPL router incorporate an SPI firewall.
It is divided in three filters : The Deny of Service filter to prevent Internet attacks, the main filter to filter source & destination IP addresses, and the remote user filter.

OVERVIEW

Remote access server for PC, tablet or smartphone

The IPL routers provide a powerful and flexible remote access service.
PPTP, L2TP/IPSec, OpenVPN or HTTPS remote access connections can be set-up.

Remote users are authenticated, and particular access rights can be assigned to each remote user according to his identity.

The HTTPS web portal identifies each remote user and displays the list of the web servers o which he can access.

VRRP redundancy

VRRP is a short distance Ethernet protocol between two routers for instance.

It allows to replace one router when it fails by another one.

Optional WiFi interface

The IPL routers provide optionnaly a 2.4 & 5 GHz WiFi interface.
That WiFi interface can be used either as an access point or as a client.

SNMP

The IPL routers incorporate a MIB which make possible to collect the status of each router.

DHCP server

The IP can behave like a DHCP server on the LAN interface.

Emails – sms

The digital input allows to send an email or an SMS (cellular routers).

Serial gateway

The IPL routers provide optionally serial RS232, RS485, RS422 interfaces and gateway s.

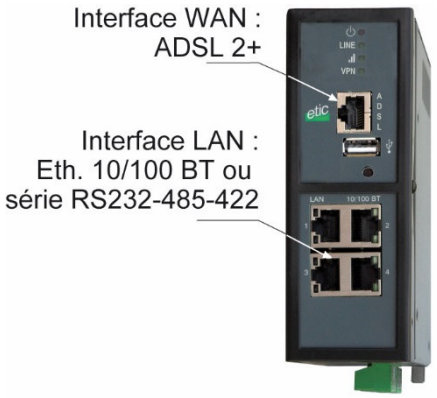
The following gateways solutions are provided :

- Raw TCP client or server.
- Raw UDP
- Telnet
- Modbus master or slave.
- Unitelway

3 IPL router organisation

The IPL router connects to the Internet or a private network on one hand (WAN interface), and to a machine network on the other hand (LAN interface).

ADSL router IPL-A



WAN interface
Depending on the model, the IPL routers provide the following WAN interfaces to reach te Internet or a company network :

WAN interface of the IPL routers						
	IPL-E	IPL-EW	IPL-A	IPL-AW	IPL-C	IPL-CW
Ethernet	●	●				
ADSL			●	●		
Cellular					●	●
WiFi		●		●		●

WAN interface of the IPL-D routers That models provide backup functions		
	IPL-DEC	IPL-DAC
Ethernet	●	
ADSL		●
Cellular	●	●

LAN interface
Depending on the model, the IPL routers provide 1 to 4 switched Ethernet ports to connect the devices of the machine.

That interface dedicated to connect a machine network is called the LAN interface.

Serial gateway location
The optional serial gateway is loacetd at the LAN IP address of the IPLrouter.

OVERVIEW

Remote access server location
The remote users can connect to the WAN interface of the router.

Firewall
The deny of service filter protects against Internet attacks.

The main filter filters IP frames between the LAN interface on one hand and the WAN interface or transmitted inside a VPN or transmitted inside a remote user connection on the other hand.

The remote users filter, identifies the remote users and assigns individual rights

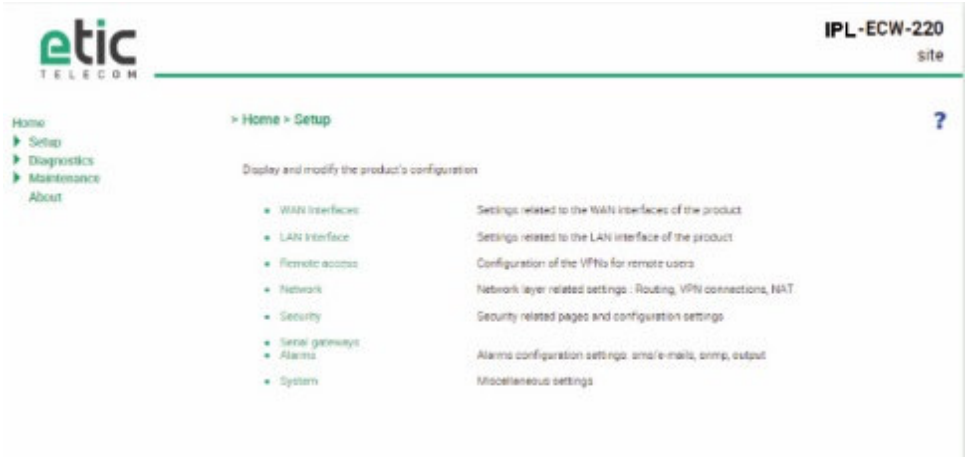
1 First setup

from factory, the IP address of the router is 192.168.0.128.

Step 1 : Create or modify the PC IP connection.
Assign to the PC an IP @ in accordance with the router RAS IP address.
For the first configuration, assign for instance 192.168.0.127 to the PC.

Step 2 : Connect the PC directly to the LAN interface of the router RAS.

Step 3 : Launch the HTML browser : http://192.168.0.128



2 Protecting the access to the administration web server

- Select Set-up > Security > Administration rights.
- Enter an administration identifier and password.

3 HTTPS set-up modifications through the WAN interface

The administration web server is located at the LAN IP address.
Coming from factory, access to the administration web server is not allowed through the WAN interface

To use HTTPS instead of HTTP to setup the product or to authorise access to the administration web server through the WAN interface,

- Select Configuration > Security > Administration rights.
- Enter an administration identifier and password.
- Check the “HTTPS configuration” box.
- Check the “WAN access“ box if you wish to access to the administration web server through the WAN interface.

Remark : the port Nr used to access to the administration web server with HTTPS is 4433.

Exemple : https://192.168.38.191:4433.

4 Recovering the factory LAN IP address

- Press the rear panel push-button ;

The OPERATION led indicator will flash.

The factory IP address 192.168.0.128 will be restored but the current configuration remains active.

5 Restoring the factory set-up

If firewall rules have been created finally preventing from reaching any IP address on the LAN interface including the router itself, it may be necessary to restore the factory configuration of the router.

To restore the factory configuration,

- Switch OFF the power supply of the router RAS.
- Press the rear panel push button and, switch-on the power supply.
- Keep the push button pressed until the operation led turns red.

Remark : The curent configuration is cleared and the factory IP address 192.168.0.128 is restored.

6 Saving or restoring a set of parameters

Once a product has been set-up, the current set of parameters can be stored inside the router.
In a second step, any set stored inside the router and displayed with the Configurations table can be saved as an editable file stored outside the ETIC router.

Inversely, a saved file can be loaded to the product Configurations table and then, if necessary, declared as the active set of parameters.

- Select the Maintenance > configuration management menu

To store the current configuration set of parameters in the configurations table,

- Assign a name for the current set of parameters ("configuration name" field) and click the Save button.

The updated Configurations table is displayed with an additional line.

To save a stored set of parameters as an editable file

- Select the set of parameters name in the Configurations table,
- Click the Export to the PC button.

The set_of_parameters.txt file is created.

To import an editable **.txt file

- Click the Select a file button,
- Browse the PC and select the file,
- Click the Import from PC button.

The updated Configurations table is displayed with an additional line.

To select a configuration set of parameters in the Configuration table, as the current configuration

- Select the set of parameters name in the Configurations table,
- Click the Load button.

The selected set of parameters is now the current set of parameters.

IPL ROUTER SET-UP

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

Function	Menu
WAN connection set-up Ethernet WAN ADSL setup Cellular network WiFi network (the router RAS is a WiFI client)	WAN interface
LAN interface set-up The Ethernete & IP setup of the router RAS LAN interface The IP adrresses of the devices of the machine	LAN Interface
Remote access set-up The M2Me connection The remote users Their access rights	Remote access
IP routing VPNs Static routes RIP Address translation Port forwarding DynDNS or NoIP	Network
Filtering the data-flow between the LAN interface on one hand and the WAN and VPN interfaces on the other hand	Security > Firewall
Serial gateway set-up	Serial gateway
Email or SM Alarm	Alarm
Administration web server access	Security > Administration rights

1 Ethernet / WAN interface setup

That section applies to the IPL-E router which provides a specialised Ethernet RJ45 WAN interface.

It applies also to the IPL-A ADSL router and to the IPL-C cellular router when one wishes to use the RJ45 Ethernet connector as the WAN interface instead of the ADSL interface (IPL-A) or the cellular interface (IPL-C).

- Select the Set-up > WAN menu

« WAN type » list :
Select the “Eternet” value.

Ethernet WAN port configuration

« Speed / Duplex» parameter :
Select 10 or 100 Mb/s & full or half duplex.

IP set-up of the Ethernet WAN port

« Connection type » list :

The Ethernet value is the default value.
It has to be selected when another router connected to the Ethernet/WAN interface of the ETIC router is in charge of routing the IP frames to the internet

The PPPOE value must be selected only in a particular situation :
When it is selected, the IPL router sets a PPP connection over Ethernet towards a service provider for instance.
It is useful when a modem, not supporting PPOE, is connected to the Ethernet WAN port of the IPL router.

Do not select PPOE except in the situation described above.

Choice	Ethernet	PPPoE
"Priority" parameter That parameter defines the priority of the path when more than one path is selected (Cellular & Ethernet WAN, for instance). The router will use as a priority the path to which the highest value is assigned; the other pat wil be used as a backup path.	●	●
« PPP login» et « PPP password » parameters Enter the login and password of the PPP connection		●
« Obtain an IP address automatically » checkbox: Leave that checkbox selected if the IP address on the WAN interface is assigned by a DHCP server. Otherwise unselect that checkbox and enter the IP address, the netwmask and the default gateway address assigned to the IPL router on the WAN interface.	●	
« Obtain the DNS server IP address automatically » checkbox: Leave that checkbox selected if the DNS servers IP address are assigned by a DHCP server. Otherwise unselect that checkbox and enter the IP addresses of the DNS servers.	●	●
« Enable address translation NAT» checkbox : If that option is selected, the source IP address of any IP frame coming from a device connected to the LAN interface and routed to the WAN interface , is replaced by the router WAN IP address. Remark : Select that checkbox if a device of the LAN interface needs to set a connection with a device connected to the Internet (FTP server …)	●	●
« Proxy-Arp » checkbox : Leave that checkbox unselected	●	●

Ping control

The IPL router is able to send periodically a PING message over the Ethernet WAN interface towards a particular machine.
If the PING receives a response, the Ethernet WAN interface is declared active with the declared priority.
If the PING message does not receive a response, the Ethernet WAN interface is disabled.

« Enable PING control" checkbox :
Select the checkbox to enable the PING control function.

"IP address" parameter
Enter the IP address of the machine to which the PING message has to be transmitted.

"PING interval" parameter
Enter the period of the PING message.

"PING retries" parameter
Enter the number of PING messages failures before disabling the Ethernet WAN interface.

2 ADSL interface setup

That section applies to the IPL-A ADSL router and to the IPL-DAC ADSL & cellular router.

- Select the Set-up > WAN menu

« WAN type » list :
Select the "ADSL" value.

ADSL modem configuration

"Modulation" parameter :
The default value is multi; the modem will adapt to the modulation of the FAI modem.
Otherwise, ask your provider the modulation which as to be used.

"VPI" parameter :
Range is 0 - 255
Leave the default value (8)

"Virtual Channel Identifier" parameters :
Range is 0 - 65535.
Leave the default value (35)

"Multiplexing" parameters :
Value LLC or VC
Leave the default value (LLC)

"Encapsulation" parameter :
PPPoE : PPP over Ethernet
PPPoA : PPP over ATM
EoA : Ethernet over ATM, RFC1483/RFC2684 Bridged
IPoA : Routed IP over ATM, RFC1483 Routed

A set of IP parameters is associated with each of these encapsulation solutions (see the next aragraph.

IP configuration of the ADSL line depending on the

	PPPoE	PPPoA	EoA	IPoA
"Priority" parameter Enter a medium value	●	●	●	●
« PPP login» & «PPP pasword»: Enter the ADSL account values	●	●		
«PPPoE service name » parameter : It is thename of the service provided by the operator It is usually not necessary to enter that paramater	●			
"Obtain an IP address automatically" checkbox : Leave that option selected if the provider is supposed to assign an IP address to the router through the line each time it connects to the Internet (default). Otherwise, unselect that option and enter the IP address assigned to the ADSL interface and the IP address of the remote router.	●	●	●	●
"Primary DNS IP address" & "secondary DNS IP address" parameters : Leave that option selected if the provider is supposed to provides that addresses automatically through the line (default). Otherwise, unselect that option and enter the IP of the primary and secondary DNS server.	●	●	●	●
« Enable address translation NAT» checkbox : If that option is selected, the source IP address of any IP frame coming from a device connected to the LAN interface and routed to the ADSL interface , is replaced by the router WAN IP address. Remark : Select that checkbox if a device of the LAN interface needs to set a connection with a device connected to the Internet (FTP server …)	●	●	●	●
Case à cocher « Activer le Proxy-Arp »: That function gives a direct access to the remote router (BRAS) for the devices of the LAN interface. Leave that checkbox unselected	●	●	●	●

The information entered in this page have to be provided by the Internet provider.

3 Cellular interface setup

Two SIM cards can be inserted in the router to allow the use of two different cellular networks .

The network corresponding o the SIM card Nr1 is the main network, while the other one is the backup network.

- To set-up the cellular network interface, select Set-up > WAN interface

« Connection type » list :
Select the « cellular" choice.

"Priority" parameter
That parameter defines the priority of the path when more than one path is selected (Cellular & Ethernet WAN, for instance).
The router will use first the interface having received the highest priority; the other interface will be used as a backup path.

"SIM card" parameter
It is possible to select the SIM card Nr1, or the SIM card Nr2 or both.

SIM card parameter	
Value	
SIM1	The SIM 1 is selected (default value)
SIM2	The SIM 2 is selected (default value)
SIM 1, backup to SIM2	The SIM 1 is used first ; the SIM 2 is used as backup

3.1 SIM 1 or SIM 2 set-up

Setting-up the SIM card 1 or the SIM card 2 is identical. We describe hereafter the SIM 1 set-up.

SIM 1 : Modem set-up
« Modem initialisation string » parameter :
Leave that field empty.

« APN » parameter :
Enter the label of the gateway (APN) to the Internet - or to other services - provided by the mobile service provider.

« PIN code » parameter :
Enter the SIM card pin code.
As long as the PIN code has not been correctly entered, the OPERATION led indicator flashes (red colour).

« Cellular network » parameter :
The router RAS is supposed to connect to the best cellular relay available.
However, in particular situations, it may be useful to force the router RAS to use a particular service.
That parameter gives the choice to select either the LTE 4G service, or the UMTS 3G service or the GPRS-EDGE service.
The default value is “AUTO”; in that case, the router RAS selects the best available connection.

Cellular IP interface set-up

«Login» & « Password» parameters :
Enter the login and password of the subscription.

Remark : That parameters are generally not required.

« Obtain an IP address automatically » checkbox :
The IP address of the cellular interface of the router RAS is usually assigned by the service provider over the air.
Otherwise, enter the IP address assigned to the cellular interface of the router.

« Obtain the DNS server IP address automatically » checkbox:
Leave that checkbox selected if the DNS servers IP address are assigned by a DHCP server.
Otherwise unselect that checkbox and enter the IP addresses of the DNS servers.

« NAT» checkbox :
If that option is selected, the source IP address of any IP frame coming from a device connected to the LAN interface and routed to the WAN interface , is replaced by the router WAN IP address.

Remark : Select that checkbox if a device of the LAN interface needs to set a connection with a device connected to the Internet (FTP server …).

3.2 Using the SIM cards 1 and 2

Each SIM card can be associated to two different mobiles data services.

In the subsequent text, the cellular service associated to the SIM card 1 is referred to as Network 1 and the cellular service associated to the SIM card 2 as the Network 2.

The network 1 is first service tested at power-up.

If the Network 1 remains in failure during the period of time T1, the router switches to the network 2.
If the Network 2 is functioning properly, the router uses that cellular network at least during the period of time T3.
On expiry of that period, the router switches back to the network 1 and checks if it is available. If it is not the router goes on using the Network 2.

At any time, if the network 2 does not work correctly during the period of time T2, the router switches to Network 1.

The periods of time T1, T2 and T3 can be selected.

We advise not to select too small values of the T1, T2 and T3 parameters. :

Example :
T1 Network 1 failure confirmation time = 20 mn
T1 Network 2 failure confirmation time = 20 mn
T3 Minimum connection time on network 2 = 12 hours

«Network 1 failure confirmation time » parameter
See above.
Value : 5, 10, 20, 30, 60 mn

«Network 2 failure confirmation time » parameter
See above.
Value : 5, 10, 20, 30, 60 mn

«Minimum connection time on Network 2» :
See above.
Value : 1, 12, 24 hours, 5 days, never.

3.3 Cellular connection control

The router RAS checks permanently that the cellular connection is properly set thanks to the PPP protocol established with the cellular infrastructure router.

However, with particular mobile service providers, or in particular situations, that PPP connection is declared active while the data transmission service is not provided by the mobile service provider.

It is why the router RAS is able to ping a particular server to check if the data service is really provided. If it is not, the PPP connection is reset.

That function must be enabled only if connection defects are noticed.

To implement that function, enter the parameters hereafter.

«IP address of the server» parameter :
Enter the IP address of the device to which the router RAS will send a periodic ICMP message (PING)

«PING Interval" parameter :
Enter the period of the PINGs
Value : 30 s, 1, 2, 5, 10, 20, 30, 60 mn

«Number of retries» parameter :
Enter the number of retries before resetting the PPP connection.
Value : 1, 2, 4, 8, 12

4 WiFi interface setup

Remark :
The WiFi scanner makes possible to detect the WiFi networks around the router RAS.
To use the WiFi scanner, select the Diagnostic > Tools > WiFi scanner menu.

To set-up the WiFi interface as a client to reach the Internet,

- Select Set-up > WAN interfaces > WiFi
- Select the « Enable » checkbox

WiFi modem set-up

« Network name (SSID) » parameter :
Enter the name assigned to the Wi-Fi network to which the router has to connect.

Attention : The SSID is case sensitive.

« Authentification » parameter :
Select WPA or WEP or None according to the access point set-up.

« Key » parameter :
Enter the WPA or WEP key according to the access point set-up.

WiFi WAN IP set-up

« WiFi WAN priority» parameter :
Enter a medium value.

« Obtain an IP address automatically » checkbox:
Leave that checkbox selected if the IP address on the WAN interface is assigned by a DHCP server.
Otherwise unselect that checkbox and enter the IP address, the netwmask and the default gateway address.

« Obtain the DNS server IP address automatically » checkbox:
Leave that checkbox selected if the DNS servers IP addresses are assigned by a DHCP server.
Otherwise unselect that checkbox and enter the IP addresses of the DNS servers.

« NAT» checkbox :
If that option is selected, the source IP address of any IP frame coming from a device connected to the LAN interface and routed to the WAN interface , is replaced by the router WAN IP address.
Remark: Select that checkbox if a device of the LAN interface needs to set a connection with a device connected to the Internet (FTP server …)

5 LAN interface setup

5.1 Overview

Ethernet switch or hub
The LAN interface consists of 1 to 4 switched Ethernet 10/100 BT RJ45 connectors.
An option enables to shape a hub instead of a switch for test purposes for instance.

IP address of the router RAS on the LAN interface
A fixed IP address must be assigned to the LAN interface of the IPL router.

DHCP server
The IPL router can also behave as a DHCP server for the devices on the LAN interface.

Remote users IP addresses allocation
If remote users PCs are supposed to connect to the devices of the LAN network, a pool of IP addresses belonging to the LAN network has to be reserved for them.

The addresses reserved for the remote users must not be allocated to other devices of the LAN network.

Example :

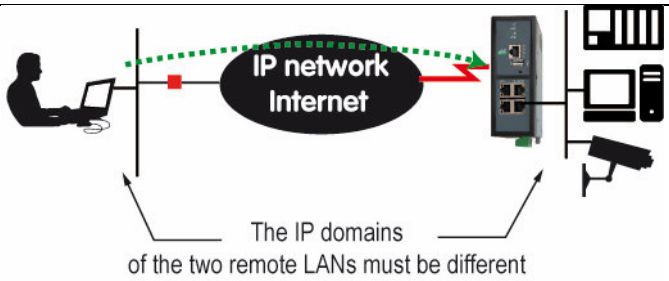
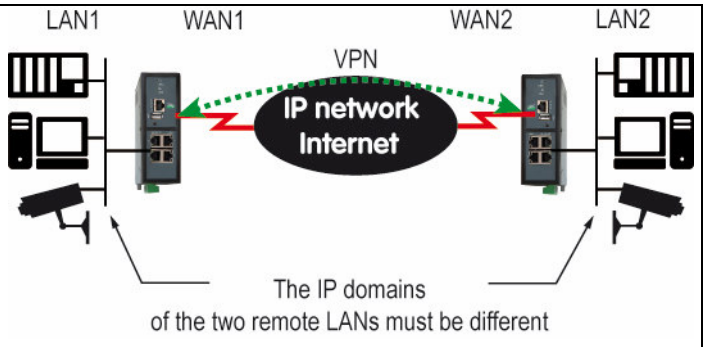
	IP address	Remark
LAN network	192.168.12.0 / 24	From 192.168.12.1 to 192.168.12.254
Netmask	255.255.255.0	
Router RAS IP addr.	192.168.12.1	
Remote users IP pool start	192.168.12.2	In this example, two remote users can simultaneously connect to the LAN network; one will receive the IP address 192.168.12.2 and the other 192.168.12.3.
Remote users IP pool end	192.168.12.3	
IP addresses available for the devices of the LAN network	192.168.12.4 to 192.168.12.254	

Identification of the devices connected to the LAN network
The identification of the devices connected to the LAN network can be stored into the router.

The access to an identified device can then e allocated individually to the remote users.

WiFi access point
When the optional WiFi interface is set-up as an access point, the devices connected to the router RAS through that WiFi network belong to LAN network.
As a consequence, their IP address belong to the IP domain of the LAN network.

IP adresses allocation

Case 1 : Remote users connection	
Case 2 : VPN set between 2 routers	

5.2 Ethernet & IP menu

- Select Set-up > LAN Interface > Ethernet & IP

Ethernet ports

« hub mode enable» checkbox :
If the checkbox is selected, the LAN ports behaves like a hub.

LAN network

« IP address » & « netsmask » parameters :
Enter the IP address assigned to the router over the LAN interface.
That IP address is also the IP address of the administration server of the router.

« Default gateway » parameter :
If another router is connected to the LAN network giving access to other networks, and acting as the default gateway for the router RAS, enter the address of the router.

Remark : leave that field empty, if no other router is connected to the LAN network.

Remote access menu

«Automatic management of the remote users» checkbox :
If that checkbox is selected, the router RAS allocates automatically an unused IP address of the LAN network to a remote user when he connects.

Unselect that checkbox to set-up the pool of fixed IP addresses which can be allocated to the remote users. That IP addresses must belong to the LAN domain.

Advanced parameters

5.3 WiFi access point set-up

Remark : The Wifi module can be set-up either like a client or like an access point.

To set-up the WiFi access point,

- Select the Set-up > LAN interface > WiFi access point menu
- Select the WiFi access point checkbox

« Network name (SSID) » parameter :
Enter the name assigned to the WiFi network to which the router RAS has to connect.

Attention : The SSID is case sensitive.

« Preshared key » parameter :
Enter the WPA preshared key (at least 8 characters).

« Country code» parameter :
The RF channels allocated to the WiFi service are not the same in all the countries.
It is why, the country code has to be entered carefully.

Click the help menu to display the list of the country codes.

« WiFi Mode» parameter :
Select one of the possible WiFi modes :

Mode 802.11a : 5 GHz OFDM
Mode 802.11.b : 2,4 GHz DSSS
Mode 802.11.g : 2,4 GHz OFDM

Remark : the selected WiFi mode must be entered in each WiFi client (tablet …).

« RF channel» :
Select a traffic channel in the list.

Remark :
It is preferable to select an unused channel at the location where the router RAS is installed.
Use the WiFi scanner to display the channels used by the WiFi networks active at the same location.

5.4 Device list set-up

To set-up the device list,

- Select the Set-up > LAN interface > device list menu

To add a device to the list,

- Click the « Add » button
- Assign a name and an IP address to the device

Remark : it is possible to enter a subnet and only a device.
Example : 192.168.38.8/29 = 192.168.38.8 to 192.168.38.15

5.5 DHCP server menu

The router RAS can behave like a DHCP server over the LAN interface.
In that case, a pool of addresses must be reserved ; the addresses of the pool are automatically distributed to the devices of the LAN acting as DHCP clients.

The addresses of the LAN domain which do not belong to that pool can be allocated as fixed IP addresses to particular devices.

Remark
Many WiFi office devices like tablets or smartphones do not support a fixed IP address.

- Select the Set-up > LAN interface > DHCP server

"IP address pool start" & "IP addresses pool end" parameters :
Enter the first and the last IP address reserved to the DHCP server.

« IP address » & « netsmask » parameters :
Enter the IP address assigned to the router over the LAN interface.
That IP address is also the IP address of the administration server of the router.

« Default gateway » parameter :
If another router is connected to the LAN network giving access to other networks, and acting as the default gateway for the router RAS, enter the address of the router.

6 M2Me_Connect connection set-up

That paragraph applies to all the models of IPL routers, but only if the M2Me option has been enabled.

Preliminary remark :
To provide access to a machine for remote users through the M2Me_Connect service, it is necessary to carry-out three steps :
1st step : carry-out the M2Me connection set-up described in this paragraph.
2nd step : Register a remote user (at least) in the user list; refer to a further paragraph in the manual.
3rd step : Assign access rights for the remote users.

The M2Me_Connect OpenVPN connection is set from the router RAS to the M2Me_Connect server.
The VPN can be transported in UDP or TCP.

- Select the Set-up > Remote access > M2Me_Connect menu.

« TCP port » & « UDP ports » parameters :
Enter the selected UDP and TCP ports the router will have to test to set the M2Me VPN.
The router RAS will try to set the M2Me connection successively with the selected UDP and TCP ports beginning with UDP.

- If a proxy server filters outgoing connections, unselect the No Proxy checkbox and enter the Proxy server parameters :

  the type of the proxy server (HTTP, SOCKS5)
  the proxy IP address and port number
  the type of required authentication (None, basic, NTLM) if the proxy is http

Once the M2Me connection has been set-up, the M2Me led flashes.

Attention :
Do not forget to copy the product key of the router RAS (ABOUT menu); it is required by the M2Me software of the remote PC when you will set-up the connection to the router RAS.

7 Remote access connection

Remark : Providing a secure remote access service requires three steps :

Step 1 : The remote connection set-up itself described in this paragraph.

Step 2 : The user list set-up described in the next paragraph.

Step 3 : The access rights definition described in the next paragraph.

7.1 Advantages of a remote access connection

Using a remote connection to access to a machine provides the following advantages :

- **Remote users identification**

The remote user login and password are registered in the user list.
When he connects, the login and password of the remote user, and optionally the certificate of his PC are checked.
The certificate can be delivered by ETIC TELECOM or by another authority.

- **Selective access rights**

Individual access rights can be assigned to each remote user according to his identity.

- **Transparent connection**

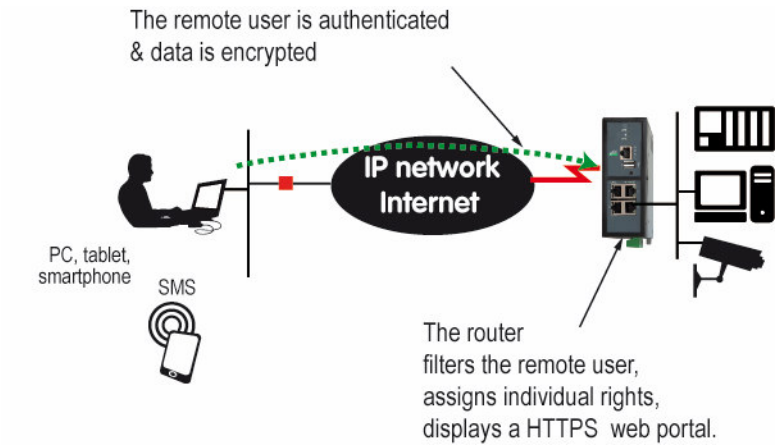
Once the remote connection has been launched, the PC receives automatically an IP address of the network.
The user can access to each authorized device of the network.

- **Data encryption**

  Data is encrypted from end to end.

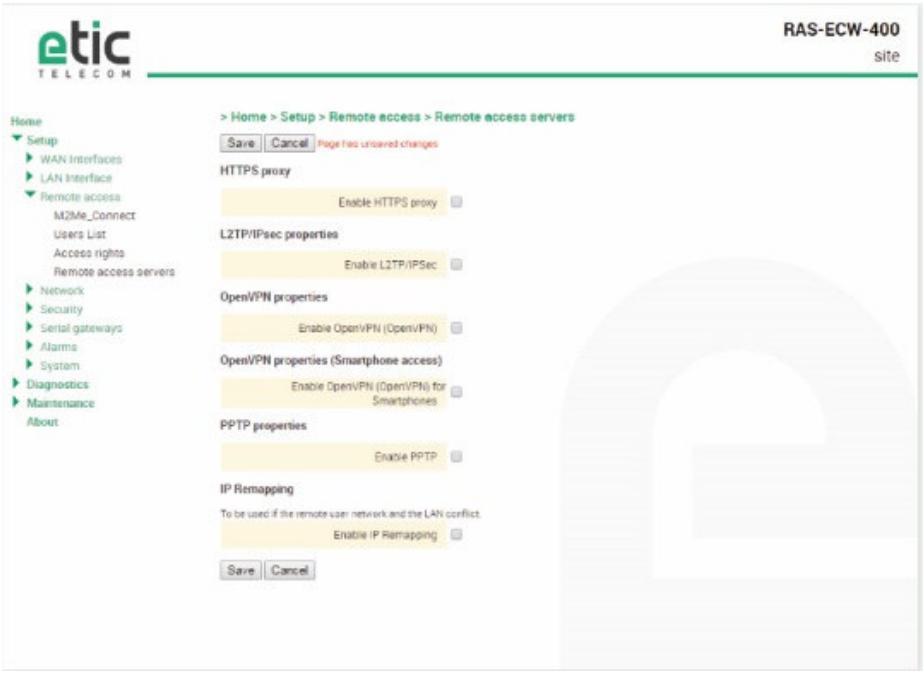
- **PC, Tablet, smartphone**

The solutions provided by the ETIC router are suitable as well for Windows PCs or tablets or smartphones (Androïd or IOS).



To set-up a remote connection,

- Select Set-up > Remote access > Remote access servers



7.2 Types of remote access connections

Four types of remote access connections can be set-up :

OpenVPN.,
PPTP,
L2TP/IPSec,
HTTPS.

	Remote user Identification	Authentication	Encryption
OpenVPN	Login	PWD Optionally a certificate	Yes
PPTP	Login	PWD	Yes
L2TP/IPSec	Login	PWD and Preshared Key or certificate	Yes
HTTPS	Login	PWD	Yes

That four types of connection can be implemented in PCs, tablets or smartphones.

They can be active at the same time.

The HTTPS connection is mainly dedicated to secure remote access to HTML pages embedded in supervision PCs, HMIs, or PLCs for instance;

When a remote user sets a remote user connection, whatever type, his identity is checked (Login / PWD).

7.3 HTTPS connection and portal for smartphones, tablets or PCs

7.3.1 Overview

The ETIC router can behave like a HTTPS server for remote users.

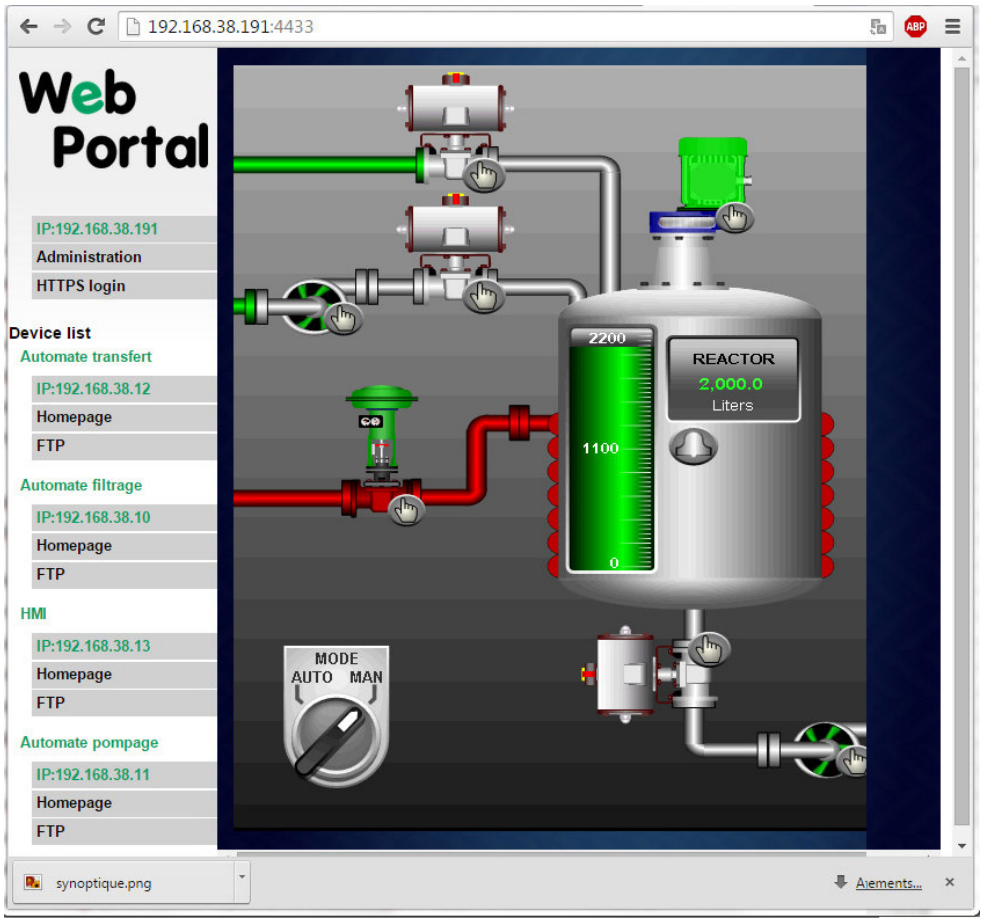
In addition, the HTTPS server can behave like a HTTPS to HTTP gateway to give a secure remote access to HTML / HHTP pages embedded in devices.

It means that a simple HTML / HTTP unsecure server can be used remotely through the internet in a safe way.

When a remote user connects to the ETIC router using an HTTPS secure connection, the portal displays the list of the html servers to which he has the right to access.

That list can include as well HTTPS native servers or HTTP unsecured server.

The remote user just has to select one server in the list.



7.3.2 Set-up

To enable the HTTPS portal through the LAN interface,

- Select Set-up > Remote access > Remote access server
- Select the «Enable the HTTPS proxy » menu

To give access to the HTTPS portal through the Internet (WAN),

- Select Set-up > Security > Administration rights
- Select the « Use HTTPS for set-up operation » checkbox

Important remark :

When the HTTPS portal is enabled, the access to the administration server and to the HTTPS portal from the LAN or from the WAN are organised according to the table below :

	From the Internet	From the LAN
HTTPS web portal	https:// Internet IP address	LAN IP address
Administration web server	https://Internet IP address: 4433	LAN IP address or https://adr. IP Internet : 4433

7.3.3 Operation

To access to the HTTPS internet portal from the Internet,

- Launch the browser
- Enter : https:// « Internet IP address of the ETIC router»
- Enter the login and password when the identification window is displayed.

The Web portal page displays the list of the web servers to which it is possible to connect according to the user identity.

7.4 OpenVPN remote user connection

The remote user can be authenticated with a password or with a password and a certificate.
The data is encrypted.
On the remote PC side, one can use a standard OpenVPN client or, if the PC is running Windows, the M2Me_Secure software which is simple to install, set-up and use.

To set-up the OpenVPN connection,

- Select the OpenVPN checkbox

« TCP port » & « UDP ports » parameters :
Select UDP or TCP and the port number.

Attention :
If OpenVPN VPNs between routers must also be set, the selected protocol (TCP or UDP) and port number of the OpenVPN VPN must different from the protocol and port number of the remote user connection.

«Remote users authentication» parameter :

Select the “Login / password” value or the “Login/password & certificate” value if the certificate of the remote PC must be checked.

In that case, the certificate of the remote PC must be stored in the ETIC router (see the table at the top of the page).

« Encryption Algorithm» & « Message digest algorithm» :

Leave the default values Blowfish & MD5.

7.5 OpenVPN connection for smartphones

It is possible to differentiate a remote user connection intended for PCs and another remote user connection intended for smartphones.

The protocol (TCP or UDP) or the port number of the smartphone connection must be different from the ones intended for PCs.

Select the smartphone remote user connection

« TCP port » & « UDP ports » parameters :
Select UDP or TCP and the port number.

Attention :
If VPN between routers must also be set, the selected protocol and port number of the OpenVPN VPN must different from the protocol and port number of the remote user connection.

«Remote users authentication» parameter :

Select the “Login / password” value or the “Login/password & certificate” value if the certificate of he remote PC must be checked.

In that case, the certificate of the remote PC must be stored in the ETIC router (see the table at the top of the page).

« Encryption Algorithm» & « Message digest algorithm» :

Leave the default values Blowfish & MD5.

7.6 PPTP connection

- Select the PPTP checkbox.

If the remote are PC running Windows, select only the MS-CHAP V2 checkbox.

7.7 L2TP / IPSec connection

- Select the L2TP/ IPSec checkbox.

«Remote users authentication» parameter :

Select the “Login / password” value or the “Login/password & certificate” value if the certificate of the remote PC must be checked.

In that case, the certificate of the remote PC must be stored in the ETIC router (see the table at the top of the User list page).

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

Leave the default values 3DES & MD5.

« Authentication method» parameter :

Select “preshared key” or “certificate”.

If the choice “Certificate” is selected, the remote PCs certificates must be stored in the ETIC router (User list menu).

8 User list

It is necessary to register at least one remote use in the user list.

The users list is able to register 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 his mobile telephone number to send alarm SMS to him.

To display the user list,

- select the Set-up> Remote access> User list menu

Remark : Coming from factory, the user list is empty.

To register a remote user in the user list,

- Click the « ADD » button located under the user list.

Enter the identity of the user (Login and password), his email address to send alarm emails.

9 Assigning rights to remote users

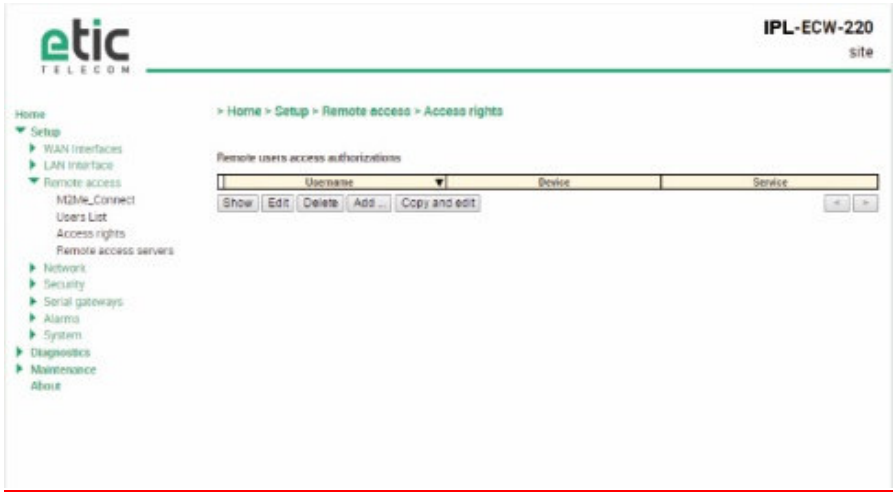
Individual access rights to the network can be assigned to each user.

The list of devices of the LAN network must have been registered previously (LAN interface menu).

To grant access rights to a remote user,

- Select the set-up, remote access, access rights menu.
- Click the « Add » button.
- Select a remote user in the list.
- Select a device in the list to authorise the remote user to access to that device.

  Remark : A device ca be a subnet or an IP address (refer to the Set-up> LAN interface > Device list).



10 IPSec VPNs set-up

10.1 Overview

An IPSec VPN tunnel allows to connect two networks in a safe and transparent way : Each device of the first network can exchange data with any device of the other network.

16 IPSec connections can be set by one ETIC router.

- **Glossary**

The router which initiates the IPSec VPN is called the initiator; the other one is called the responder.

- **Preshared key authentication**

Only one preshared key can be stored in one ETIC router; it is used by all the VPNs and also by the L2TP/IPSec remote user connection.

- **Certificate authentication**

The authentication of the two participants to the VPN connection can also be carried-out with certificates.
Coming from factory , a certificate produced by ETIC TELECOM is registered in the ETIC router.
Other kinds of X509 certificates can be added. (see the Set-up>Security>X509 certificate).
The certificate used by each participant to the VPN must be delivered by the same authority.

- **Setting-up an IPSec tunnel in the case where the source IP address is modified along the way from the initiator to the responder router.**

To provide a strong mutual authentication, each router checks the source IP address of the frames it receives is the authentical IP address.

It is why, the IPSec tunnel requires a particular setup when the IP address of the initiator or the responder is not fixed and / or when intermediate routers replace the source IP address by their own address (NAT).

It is what happens, in particular, in the case of cellular networks.

Two set-up solutions are possible :

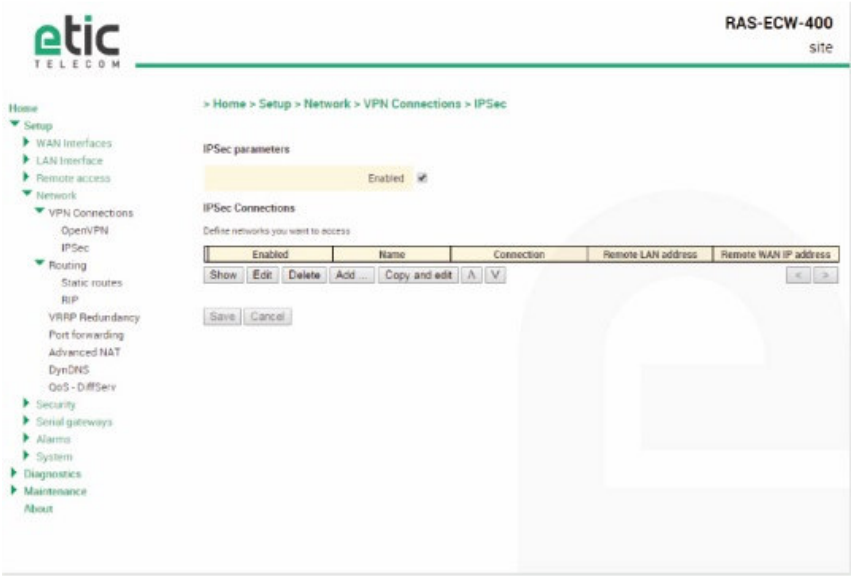
Solution 1 : Use a certificate for authentication instead of a preshared key

Solution 2 : if the preshared key authentication method is used, an IKE code (IKE ID) needs to be assigned to each router. See the IPSec set-up paragraph hereafter.

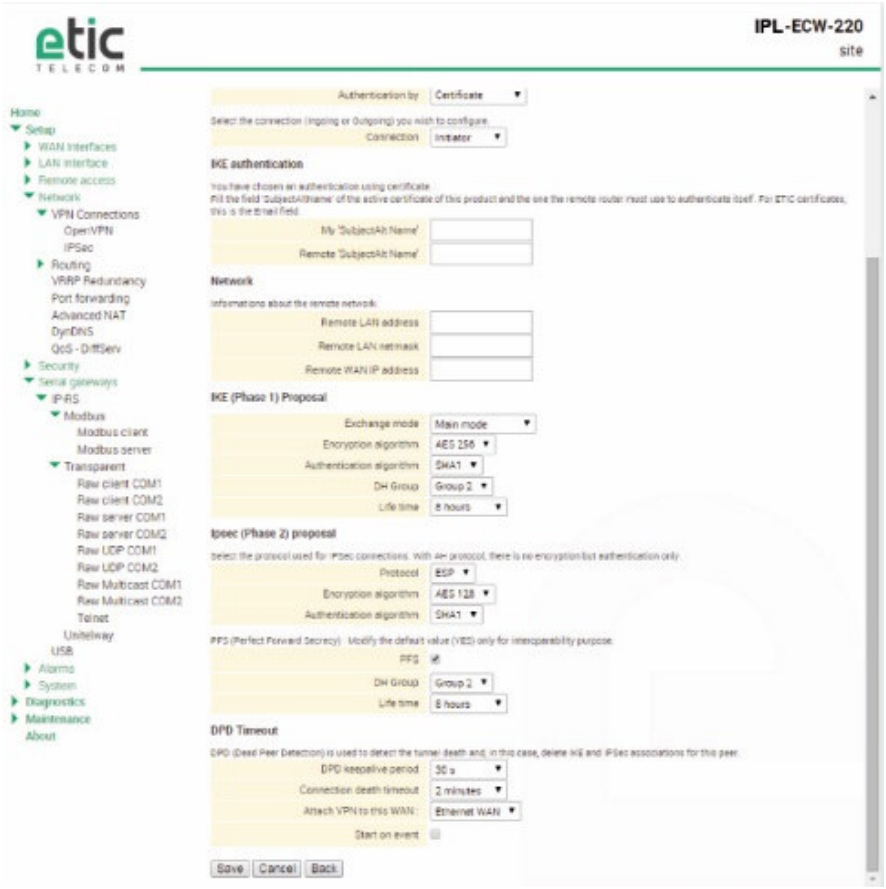
10.2 IPSec VPN connection set-up

- Select the Set-up> Network > IPSec VPN menu

The IPSec VPN home page is displayed.

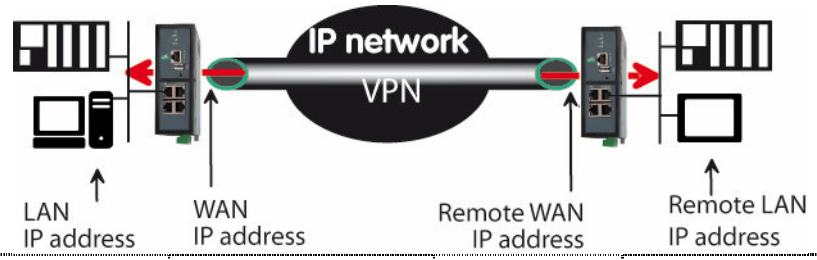


To add an IPSec VPN connection, click « Add». The set-up page of the new VPN connection is displayed.



- Select the Enable checkbox.
- Select the Advanced parameters checkbox if a preshared key is used and if intermediate routers translate the source P address.
- Assign a name to the connection.

The different IP addresses used during the set-up are described by the drawing below.

Current router		Remote router	
			
192.168.1.0	10.10.10.7	10.10.10.100	192.168.2.0
255.255.255.0			255.255.255.0

« Authentication » parameter :
Select preshared key or certificate.

« Connection » parameter :
Select Initiator if the current router is supposed to initiate the VPN.

Authentication section– Case 1 : Use of a certificate
Remark : Both certificates must be delivered by the same authority

« My SubjectAlt name » parameter:
Enter the 'SubjectAltName' value of the active certificate of the current router.
If the active certificate is an ETIC TELECOM certificate, that field is the email field.

Remote « SubjectAlt name » parameter :
Enter the 'SubjectAltName' value of the active certificate of the remote router.
If the active certificate is an ETIC TELECOM certificate, that field is the email field.

Authentication section– Case 2 : Use of a preshared key

« Preshared key » and « Passwords match » parameter :
Enter and confirm the preshared key.
The maximum length of the key is 40 characters.

« Local IKE ID» & « Peer IKE ID » parameters :
That identifiers make possible to set a preshared key VPN even if intermediate routers modify the source IP address.
The router receiving an IP frame checks the IKE ID of the remote router in place of its source IP address.

Network section
« Remote LAN IP address » & « Remote LAN Netmask" parameters :
Enter the IP address and netmask of the remote LAN network
192.168.2.0 & 255.255.255.0 of the drawing below

« Remote WAN IP address » & « Remote WAN Netmask" parameters (initiator only):
Enter the WAN IP address of the remote router

Remark :
This address is the address of the router towards which the VPN must be set.

IKE phase 1 section
IKE phase 1 performs mutual authentication between the two parties with the end result of having shared secret keys.

« Exchange Mode» parameter :
Select Main or Aggressive.

The « Aggressive » mode is simpler and faster than the « Main » mode.

«Encryption algorithm» parameter :
Recommended value : Auto

«Authentication algorithm» parameter :
The « Auto » choice is advised.
SHA1 provides a better security than MD5.

«DH group» parameter (only if the advanced parameters option has been selected) :
Recommended value : group 2.
The same value must be selected for the two routers.

«Life-time» parameter (only if the advanced parameters option has been selected) :
Enter the life-time of the IKE security association.
After that period of time, the IKE step 1 is carried-out again.

IKE phase 2 Section
The purpose of IKE phase two is to negotiate the IPSec parameters (general parameters, encryption, SA life-time…).
The result of the IKE phase 2 is the encrypted tunnel between the two routers.

«Protocol » parameter :
This parameter enables to set-up the IPSec transport protocol.
AH insures authentication only but does not encrypt the transported data.
ESP ensures routers authentication and data encryption.
ESP will be preferred.

«Data encryption algorithm » parameter :
Recommended value : AES

«Authentication algorithm» parameter :
SHA1 provides a better security than MD5.

«PFS» checkbox :
With PFS disabled, initial keying material is created during the key exchange in phase-1 of the IKE negotiation. In phase-2 of the IKE negotiation, encryption and authentication session keys will be extracted from this initial keying material. By using PFS, Perfect Forwarding Secrecy, completely new keying material will always be created upon re-key. Should one key be compromised, no other key can be derived using that information.

«DH group» parameter (only if the PFS option is enabled) :
Recommended value: Group 2.

«Life-time» parameter (only if the PFS option is enabled) :
Enter the phase 2 key life-time.

DPD section
DPD Keep-alive period" parameter : :
A DPD 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 keep-alive message are received from the remote point.

11 OpenVPN type VPN connection

11.1 Overview

An OpenVPN VPN tunnel allows to connect two networks in a safe and transparent way : Each device of the first network can exchange data with any device of the other network.

16 OpenVPN connections can be set by one ETIC router.

- **Glossary**

The router which initiates the OpenVPN VPN is called the VPN client the other one is called the VPN server.

The router which initiates the connection is called the VPN client
The connection is an outgoing connection

The router which receives the connection is called the VPN server
The connection is an ingoing connection

- **Login and password authentication**

Each OpenVPN connection can be authenticated using the Login & password of the VPN client.

- **Certificate authentication**

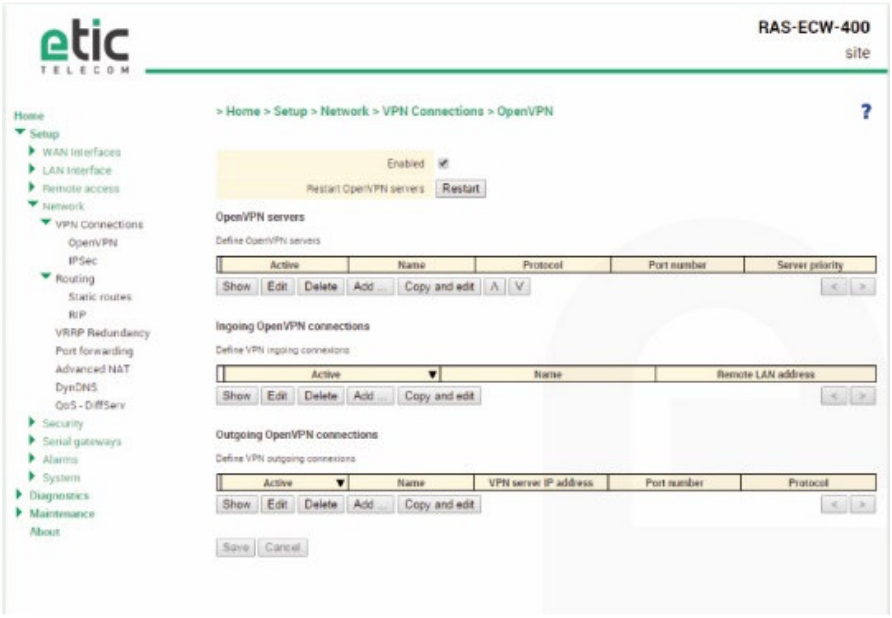
The authentication of the two participants to the VPN connection can also be carried-out using certificates in addition to a Login and password.
Coming from factory , a certificate produced by ETIC TELECOM is registered in the ETIC router.
Other kinds of X509 certificates can be added. (see the Set-up>Security>X509 certificate).
The certificate used by each participant to the VPN must be delivered by the same authority.

- **NAT translation insensitivity**

While IPSEC is sensitive to address translation of the source IP address by intermediate routers, OpenVPN is not.
The reasons is the source IP address is not checked by OpenVPN to authenticate the remote router; Open VPN authenticates the remote router with a Login password and certificate.
That characteristic makes OpenVPN very easy to implement in many situations and in particular when a cellular router is used.

- **Implementation easiness**

The transport level of OpenVPN is TCP or UDP; the port number can be selected
That characteristic makes OpenVPN very easy and reliable to implement in many situations and in particular when a cellular router is used.


etic
TELECOM
RAS-ECW-400
site
Home
Setup
WAN Interfaces
LAN Interface
Remote access
Network
VPN Connections
OpenVPN
IPSec
Routing
Static routes
RIP
VRRP Redundancy
Port forwarding
Advanced NAT
DynDNS
QoS - DiffServ
Security
Serial gateways
Alarms
System
Diagnostics
Maintenance
About
> Home > Setup > Network > VPN Connections > OpenVPN
?
Enabled
Restart OpenVPN servers
Restart
OpenVPN servers
Define OpenVPN servers
Active
Name
Protocol
Port number
Server priority
Show
Edit
Delete
Add ...
Copy and edit
Ingoing OpenVPN connections
Define VPN ingoing connections
Remote LAN address
Outgoing OpenVPN connections
Define VPN outgoing connections
VPN server IP address
Save
Cancel

11.2 Set-up principles

- **VPN server set-up**

If the ETIC router behaves like a VPN server, it means that the ETIC router has to receive at least one ingoing connection, the set-up has to be carried-out in two steps :

Step 1 : Configuration of the parameters of the OpenVPN server.
Only one server can be set-up.

Step 2 : Configuration of the ingoing, and possibly outgoing, connections.

The VPN server is unique; it can accept up to 16 ingoing connections from VPN clients.

- **VPN client set-up**

If the ETIC router behaves only like a VPN client, the set-up consists only of configuring the outgoing connection (one or several).

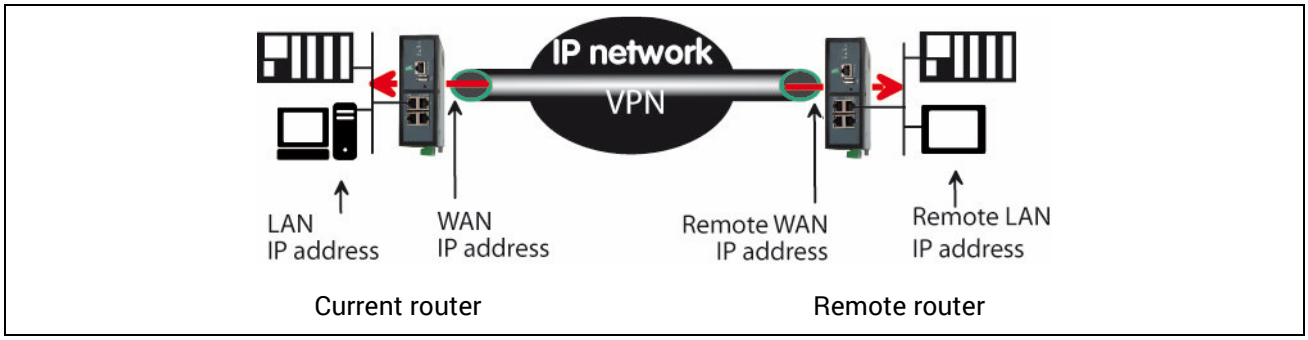
- **Set-up rules**

Common parameters
The following parameters are common for the server and for all the clients supposed to set a VPN to that server :

Transport protocol (UDP or TCP) and port number.
Encryption algorithm (Blowfish, AES 256, AES192, AES128, 3DES).
Authentication (MD5, SHA1).

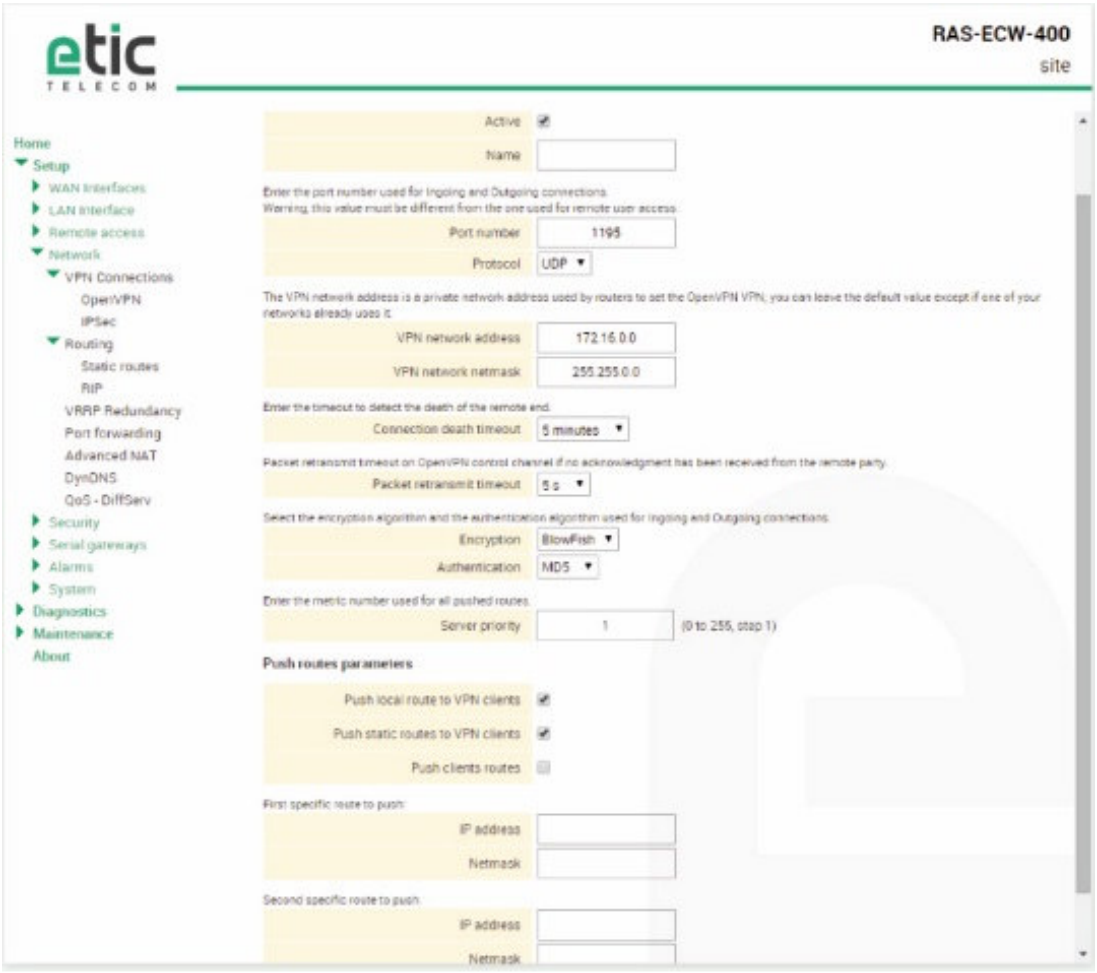
IP domains
The IP domain of the LAN and of the remote LAN must be different.

Example :
LAN network : 192.168.1.0 netmask 255.255.255.0
Remote LAN : 192.168.2.0 netmask 255.255.255.0



11.3 OpenVPN server set-up

- Select the « Add » button located just below the VPN server table



"Port number" & "protocol" parameters :
Select the port Nr and the type of level 3 protocol used to transport OpenVPN.

Attention : The port number value must be different from the one used by remote users.

"VPN network address" & "VPN network netmask" parameters :
The OpenVPN server router assigns automatically an IP address to the VPN client router.
That VPN IP address must not be confused with the WAN interface IP address.
Leave the default values 172.16.0.0 and 255.255.0.0

"Connection death time-out" parameter :
A control message (also called Keep-alive message) is sent periodically by the VPN server router to make sure that the VPN must be left active.
This parameter defines the period of the control messages.
As a consequence, it sets the maximum amount of time a VPN connection will stay established before being cleared if no response to the VPN control message is received from the remote router.

Remark :

The value of this parameter must be selected carefully; If the VPN has been cleared, for any reason, the router will wait during that period of time before launching the VPN again.

"Packet retransmit time-out" parameter:
This parameters sets the amount of time (in seconds) the server will wait for the response to the keep-alive control message before repeating it.

"Encryption algorithm" & "Authentication algorithm" parameter :
AES provides a better encryption than 3DES, and SHA-1 a better authentication than MD5.

« Priority » parameter :
Enter an intermediate value : 100 for instance.

« Push local route to VPN clients » parameter :
If that checkbox is selected, the server broadcasts to the clients the route to the IP domain of its local network.
Leave that checkbox selected.

«Push static routes to VPN clients » parameter :
If that checkbox is selected, the server broadcasts to the clients the static routes which have been set-up in the VPN server.
Leave that checkbox selected.

«Push client routes » checkbox :
Two solutions exist to enable a device connected to a VPN client router to exchange data with another device connected to another VPN client router.
The first one is to program a static route in both VPN client routers.
The second one is to select the "Push clients routes" option.

- If that option is selected, the VPN server broadcast to all the VPN clients the route to each of them. In that way, each device of the network can exchange data with each other device. Programming static routes is not necessary.

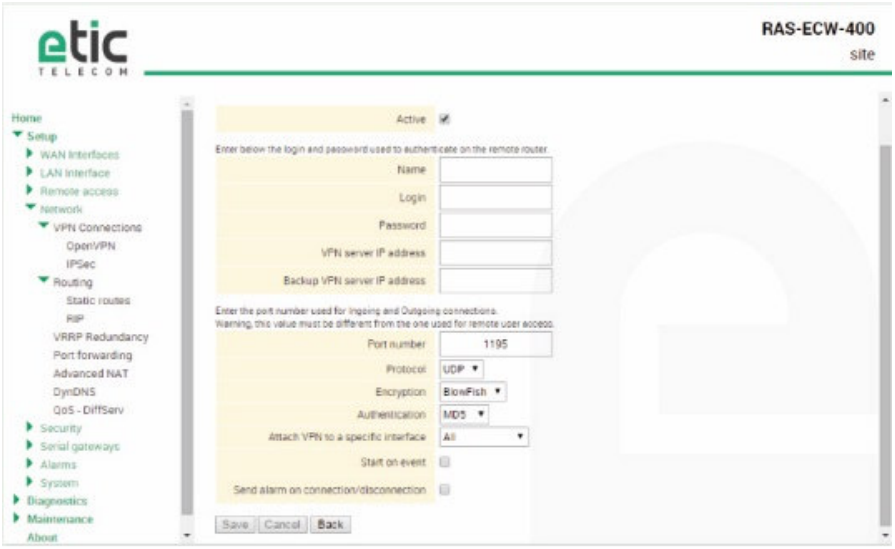
- If that option is not selected, a device connected to a VPN client ETIC router can exchange data with a device connected to the LAN network of the VPN server, but not with a device connected to one other VPN client ETIC router. If it is necessary static routes must be programmed in both routers RAS.

« 1st specific route to push» & « 2nd specific route to push» parameters :
These parameters allow to broadcast specific routes from the VPN server to the clients.

11.4 Setting up an outgoing connection

An outgoing connection is a connection initiated by the current router.

- Select the « Add » button located just below the Outgoing connection table.



- Select the « Enable » option and assign a name to the connection.

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

Remark : That login & password must be registered in the ingoing connection.

« VPN server IP address» parameter :
Enter the IP address of the VPN server.
That address can be a public IP address or a domain name or a DynDNS or NoIP address.

« Backup VPN server IP address» parameter :
The client VPN ETIC router is able to set a backup VPN if the main VPN fails.

“Port number” & “protocol” parameters :
Select the port Nr and the type of level 3 protocol used to transport OpenVPN.

Attention : The port number value must be different from the one used by remote users.

“Encryption algorithm” & “Authentication algorithm” parameter :
AES provides a better encryption than 3DES, and SHA-1 a better authentication than MD5.

«Attach the VPN to a specific interface» list :
An outgoing OpenVPN connection is normally attached to the main WAN interface of a ETIC router, for instance the cellular interface in the case of cellular router like IPL-C or RAS-EC.
However, it can be useful to attach the VPN to one other interface of the ETIC router.
Select the interface to which the VPN must be attached.

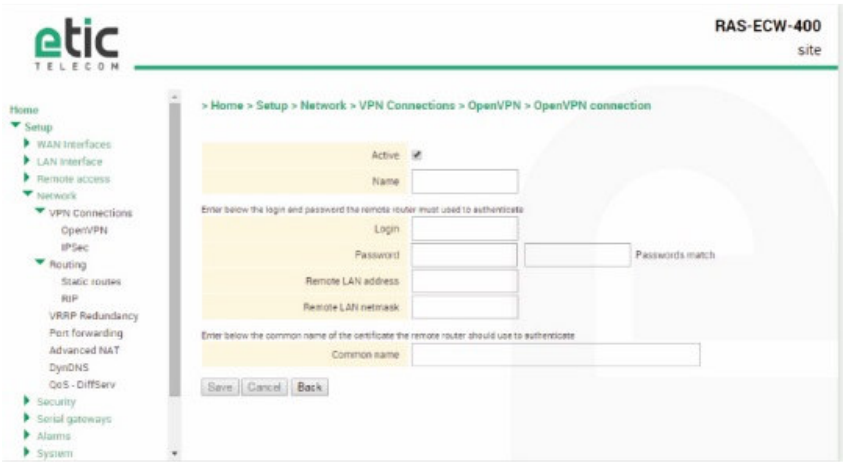
« Start on event » checkbox :

The VPN is usually established at power-up.
However, it can be useful to establish the VPN when a particular event occurs :
Cellular WAN up
Cellular WAN down
Ethernet WAN up
Ethernet WAN down
Digital input ON
Digital input OFF

11.5 Setting up an ingoing VPN connection

An ingoing VPN connection is a connection received by the current router acting as a VPN server.

- To create an ingoing connection, select the « Add » button located just below the Ingoing connection table.



- Select the « Enable » option and assign a name to the connection.

“Login & Password” parameter:
Enter the login and password of the remote router.

« Remote LAN IP address » & « Remote LAN netmask» parameters :
Enter the IP address and netmask of the remote LAN.
Ex : 192.168.2.0 / 255.255.255.0

« Common name» parameter :
Enter the value of the field 'SubjectAltName' of the active certificate of the remote ETIC router.
If the active certificate of the remote router is delivered by ETIC TELECOM, that field is the email field.

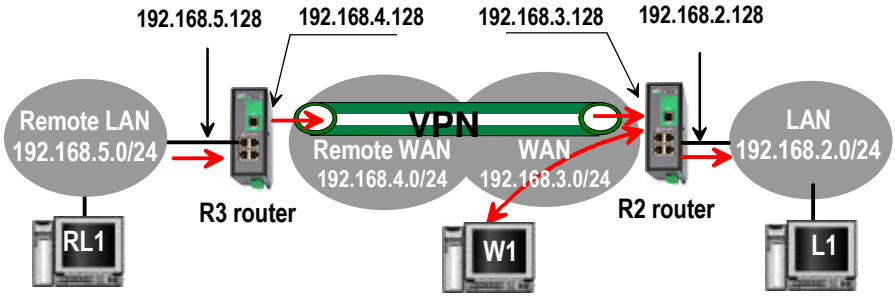
12 IP Routing

12.1 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 ETIC 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.

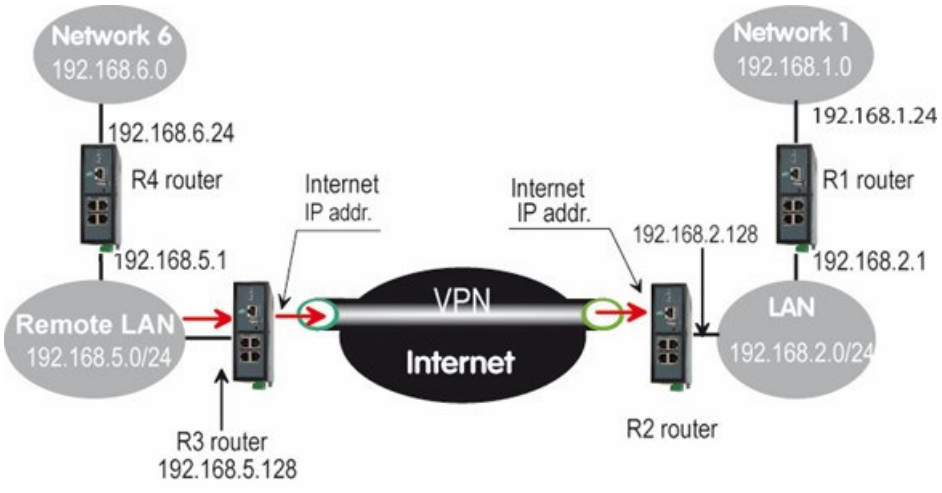
Remark 2 : A default gateway address must be entered in each device of the different networks.

12.2 Static routes

However, the router R2 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.



IPL ROUTER SET-UP

Router Nr2 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 in the router R2 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.

The same type of static routes must be entered in the other routers.

To set a static route,

- Select the "**Configuration**" menu, the "**network**" menu 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.

12.3 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 Setup>Network>Routing>RIP menu,
- Select the 'Enable RIP on LAN interface" and the "Enable RIP on WAN interface" options.

13 Network address translation (NAT)

That function applies to the IP frames issued by devices belonging to the LAN network and transmitted to the WAN network.

The NAT function consist in replacing the source IP address of that frames by the source IP address of the ETIC router on the WAN interface.

That function is required when a device belonging to the LAN network must connect to the internet (to transmit a file with FTP for instance).

To enable the NAT function,

- Select Set-up>WAN interface>
- Select the « Enable address translation » checkbox.

14 Port forwarding

14.1 Overview

Port forwarding consists in transferring IP frames intended for the IP router WAN interface to a particular device of the LAN interface using the destination port number.

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

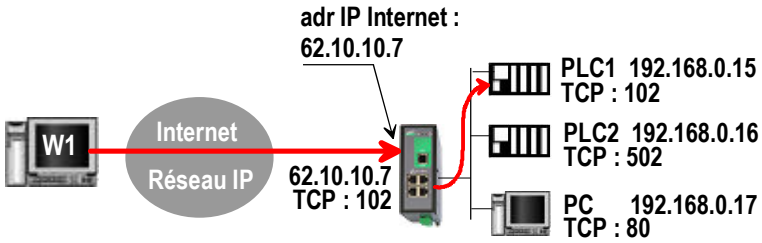
Example :

Let us suppose the PC named “W1” connected to the WAN network has to send frames to the device PLC1 connected to one Ethernet port of the ETIC router.

If routing tables cannot be registered nor a VPN, the solution can be to use the Port forwarding function :

When W1 needs to transmit frames to PLC1, it transits the frames to the ETIC router on a particular port number.

The ETIC router checks the frame, replaces the destination address by the IP address of the device on the LAN interface, and eventually changes the port number.



IN	OUT	
Service in	Device out	Service out
102	192.168.0.15	102
502	192.168.0.16	502
80	192.168.0.17	80

14.2 Set-up

To set-up a portforwarding rule,

- Select > Network> Routing > Port forwarding menu,
- Click the Add button,
- Enter the characteristics of the frames which must be forwarded :
  Source IP address,
  Port number (destination)

- Enter the characteristics of the device to which that IP frames must be forwarded.
  Destination IP address
  Port number (destination)

15 Advanced NAT

15.1 Overview

The advanced NAT function consists in modifying the source or destination IP addresses and port number of the frames received by the ETIC router on its LAN or WAN interface.

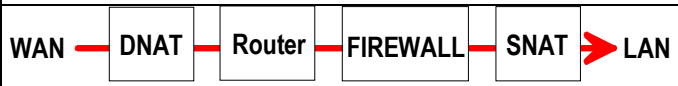
It applies to all the frames received by the router on any of its two interfaces except to the IP packets contained in a remote user connections.

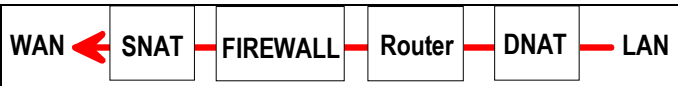
One brings out

the DNAT function which consists in replacing the destination port 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 RAS-3G 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	

LAN to WAN	

15.2 Set-up

To set the advanced address translation functions,

- select the setup >Network>Advanced NAT menu.

To create a new DNAT rule,

- click "Add a DNAT" rule.
- Select "Yes" to enable the rule.
- Enter the characteristics of the IP frames which must be modified by the DNAT rule.
  Source IP address & Destination IP address.
  Protocol (TCP, UDP, …)
  Source port & Destination port
- Enter the new destination port number and IP address.

To create a new SNAT rule,

- click "Add a SNAT" rule.
- Select "Yes" to enable the rule.
- Enter the characteristics of the IP frames which must be modified by the SNAT rule :
  Source & Destination IP address and transport protocol (TCP, UDP)
  Source & Destination port
- Enter the new source IP address.

16 DynDNS or NoIP set-up

16.1 Overview

The DynDNS or the NoIP services make possible to connect remotely to a device over the Internet even if the IP address of that device is dynamic.

The IP address of the device has to be a public IP address.

For instance, if a remote PC needs to connect to a RAS-EC or a IPL-C cellular router, DynDNS or NoIP solutions will help only if the IP address assigned by the mobile data service provider to the “antenna” of the router is a public IP address.

16.2 Set-up

Step 1 : Reserve a dynDNS domain name on the dyndns.org web site.
For instance mymachine.dyndns.org.

Step 2 : Router set-up

- Select the Set-up>Network>DynDNS menu
- Select the Enable option

« Dynamic DNS service provider » parameter :
Select DynDNS or NoIP

« DNS account login” parameter :
Enter the login assigned by dyndns.

« DNS account password” parameter :
Enter the password assigned by dyndns.

« Hostname» parameter :
Enter the DynDNS domain name (for instance mymachine.dyndns.org).

Remark :
If the IP address assigned to the antenna of the router on the 3G network is public but not fixed, it is possible to use the DynDNS service to set a connection from a device connected to the internet towards a device connected to the RAS-3G router.

To enable the DynDNS service proceed as follows :

- Reserve a dynDNS domain name on the dyndns.org web site.

For instance mymachine.dyndns.org.

- Select the« Set up » menu, and then WAN interface, and then “dynamic IP address” .

« Enable» checkbox :
Select that checkbox.

When you wish to set a connection toward the RAS-3G (PPTP, TLS, VPN …), enter the DynDNS host name instead of the antenna IP address of the RAS-3G router.

17 Firewall set-up

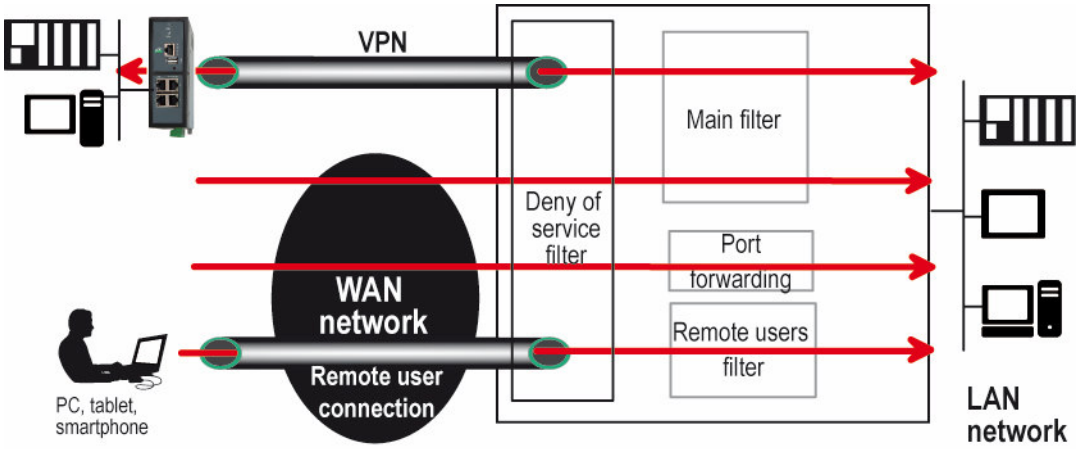
17.1 Overview

The firewall filters IP frames between the LAN interface on one hand and

- the WAN interface,
- or transmitted inside a VPN,
- or transmitted inside a remote user connection,

on the other hand.

The



It consists of three parts :

- **The « deny of service » filter**

That filter is active on the WAN interface only and protects against the Internet attacks.
It cannot be set-up.

- **The main filter**

The main filter is in charge of filtering IP frames between the LAN interface on one hand, and on the other hand, the WAN interface, or a VPN; see the drawing above.

The main filter checks source and destination IP addresses and the source and destination ports.

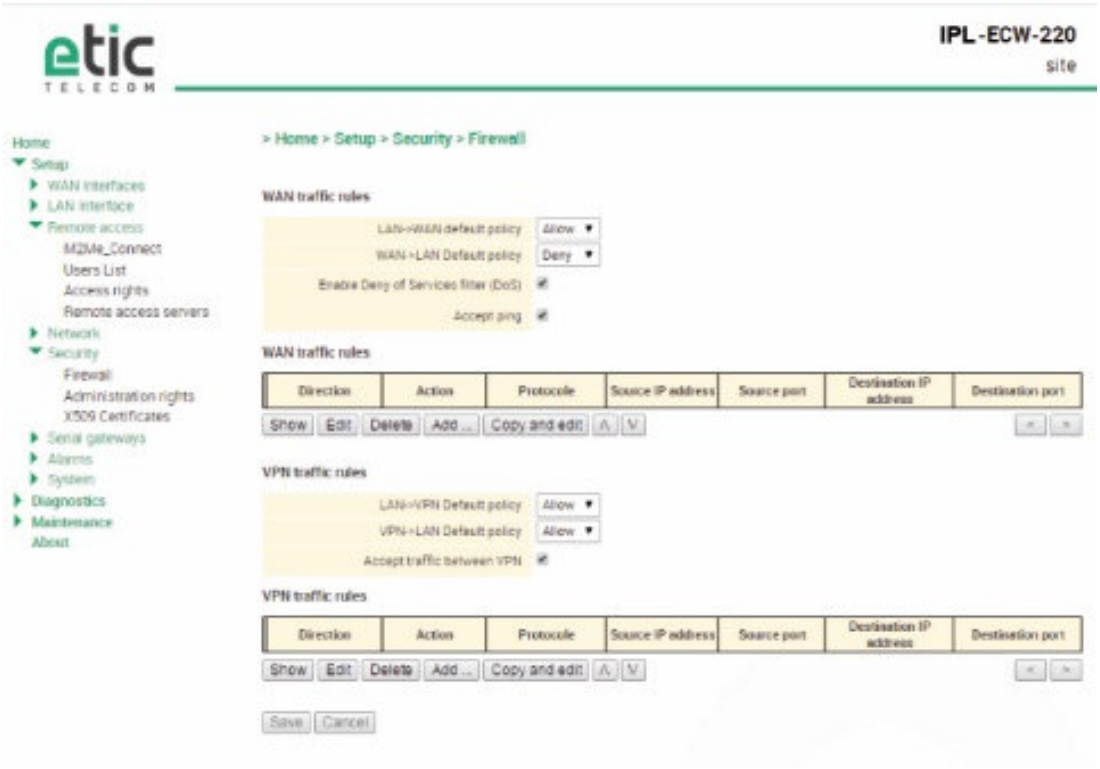
The main filter does not check the IP packets included in a remote user connection. That packets are checked by the remote users filter.

The main filter does not check the IP packets defined in the “Port forwarding” table. That packed are directly forwarded to the defined device (see Port forwarding).

- **The remote users filter**

The remote user filter filters the IP frames according to the identity or the remote user (Login & PWD).
Access rights to the devices of the LAN network are assigned to each user according to his identity.

17.2 Main filter



17.2.1 Main filter organisation

- **Main filter structure**

For a better organisation, the main filter is divided in two tables; both having the same structure.

The “VPN” filter : It filters the packets transmitted inside the VPNs.
The “WAN” filter : It filters the packets transmitted outside the VPNs

Each of that two filters is made of

a filter policy
and
a filter table each line of which is a filter rule

- **Main filter default policy**

The default policy is the decision which will be applied if a packet does not match any of the rules of the filter.

The WAN to LAN and the LAN to WAN traffic are regarded separately because the decision can be opposite for a packet coming from the WAN or coming from the LAN :

WAN to LAN : The default policy can be “Accept” or “drop”.

LAN to WAN : The default policy can also be “Accept” or “drop”.

For instance, if the default policy assigned the WAN to LAN traffic is “drop”, it means that an IP packet which does not match any of the rules of the main filter will be rejected.

- **Main filter table**

The main filter is a table, each line being a rule.

Each rule of the filter is composed a several fields which defines a particular data flow and another field which is called the action field.

The fields which define the data flow are :
Direction (« WAN to LAN » or « LAN to WAN »),
Protocol (TCP, UDP…),
IP@ & port number, source & destination.

The Action field can take two values
Accept : To authorize the data flow to be forwarded to the router interface.
Drop : To drop the packet which matches the rule.

- **How does the main filters works**

When the firewall receives a packet, it checks if it matches the first rule.
If it does, the decision is applied to the packet according to the "Action" field.

If it does not, the firewall checks if it matches the second rule; and so on.

If the packet does not match any of the rules of the table, the default policy is applied to the packet (Allow or Deny).

Remark :

Coming from factory, the main filter is set-up as follows :

The traffic carried inside the VPNs is authorized.

The traffic carried outside the VPNs is authorized when it is initiated by a device belonging to the LAN network.

The traffic carried outside the VPNs is denied when it is initiated by a device belonging to the WAN network.

18 Serial to IP gateway configuration

18.1 Overview

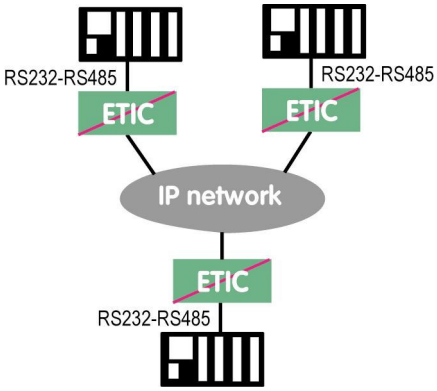
The ETIC router provides optionally 1 or 2 serial RS232, RS232, RS485 or RS422 ports.

A serial gateway can be assigned to each port .

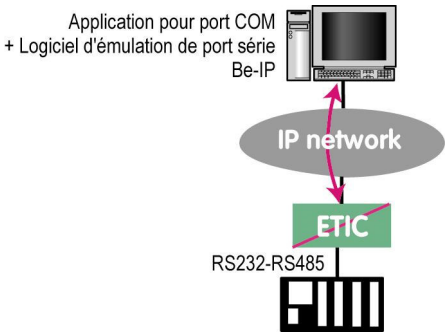
A serial gateway makes possible to use the IP network to transport serial data between two or several serial devices or directly with devices connected to the Ethernet network.

.

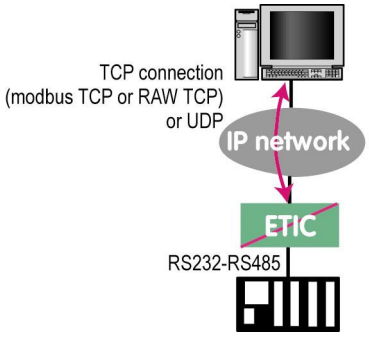
- Communication between serial devices



Communication between a serial deice and a COM port emulation software



- Communication between serial devices and a PC software application able to encapsulate the serial data into UDP or TCP (like a Modbus TCP software application for instance.



IPL ROUTER SET-UP

The gateways listed below are provided by the ETIC ROUTER router :

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 2 serial devices through an IP network.

Telnet :
To connect a Telnet terminal to the ETIC ROUTER.

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

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

Remark : If the same type of gateway is assigned to both serial ports, the UDP or TCP port numbers must be different.

18.2 Modbus gateway

The modbus gateway allows to connect serial RS232-RS485 master or slaves devices to one or several Modbus TCP devices connected to the IP network.

Remark :
Several ETIC router models provides two serial ports; one Modbus client gateway can be assigned to the port 1 and a Modbus client gateway to the port 2 using both the 502 TCP port.
But a Modbus client (resp. server) gateway can be assigned to both serial ports only if the gateways do not use the same TCP port number.

18.2.1 Glossary

A Modbus TCP client is a device connected to the Ethernet network and able to transmit Modbus requests to a Modbus TCP server device which will reply.

Several Modbus clients can send requests to the same Modbus TCP server.

A Modbus TCP server is a device connected to the Ethernet network and able to reply to Modbus requests to a coming from Modbus TCP client devices.

A TCP server can reply to several TCP clients.

A Modbus master device is a device connected to a serial asynchronous link and able to send requests to a Modbus slave device connected to the same serial network.

A Modbus slave device is a device connected to a serial asynchronous link and able to reply to Modbus requests connected to the same serial network.

Modbus address : An address between 0 and 254 assigned to each participant to a modbus network.

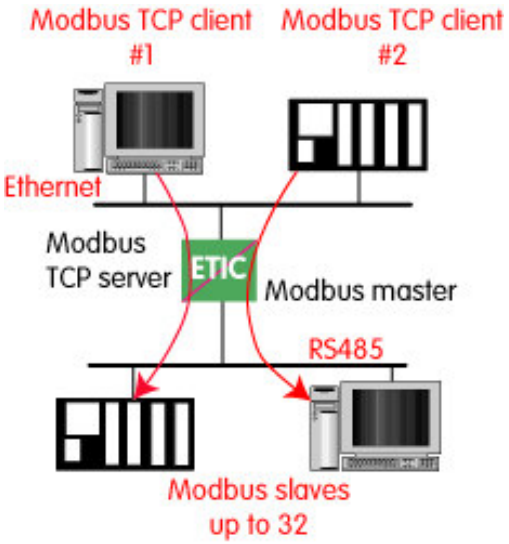
Remark the Modbus address must not be confused with the IP address of a Modbus device

18.2.2 Selecting a Modbus client or a Modbus server gateway

- Select the Modbus Server gateway to connect serial slave devices to the serial port of the ETIC router.
- Select the Modbus Client gateway to connect a serial Master device to the serial port of the ETIC router.

18.2.3 Modbus server gateway

This gateway allows to connect serial modbus slaves to the serial interface of the ETIC router.



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

"Port selection" parameter :
Select the serial port COM 1 or COM2.
If the modbus server gateway is assigned to one serial COM port, it cannot be assigned to the other one.

« ASCII / RTU protocol » parameter:
Select the right option

"Proxi" parameter:
Enable the proxi 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" parameter :
Set up the number of times the gateway will repeat a request before declaring a failure.

"Inter-character gap" parameter :
Set up the maximum delay the gateway will have to wait between a received character of a modbus answer packet and the following character of the same packet.

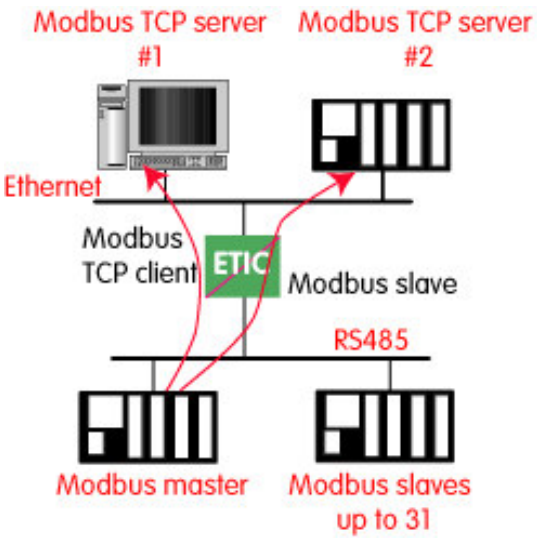
"Modbus slave address" parameter:
Choose "specified by the modbus TCP client" , if the address of the slave PLC must be decoded by the gateway from the modbus TCP packet coming from the client.
Otherwise, specify the modbus address of the slave PLC; in that case only one slave can be connected to the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

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

"TCP port number" parameter :
Set the port number the gateway has to use.
If the Raw TCP client gateway is assigned to both serial COM ports, the TCP port numbers must be different on each port.

18.2.4 Modbus client gateway

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



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

“Port selection” parameter :
Select the serial port COM 1 or COM2.
If the modbus server gateway is assigned to one serial COM port, it cannot be assigned to the other one.

« ASCII / RTU protocol » parameter :
Select the right option

“Inter-character gap” parameter :
Set up the maximum delay the gateway will have to wait between a received character of a modbus answer packet and the following character of the same packet.

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

“TCP port number” parameter :
Set the TCP port number the gateway has to use.

“IP address” parameter :
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.

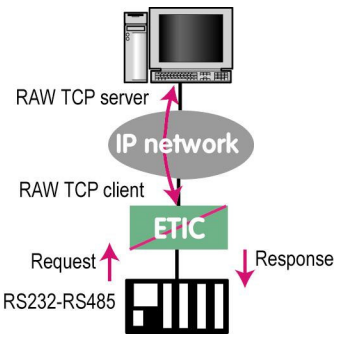
To assign an IP address to each modbus slave device with which the serial master device needs to communicate, click the “add a link” button; Assign an IP address in front of each modbus slave address with which the serial master device will have to communicate.

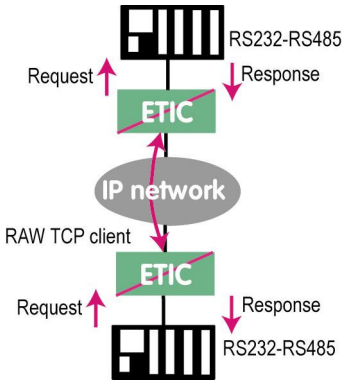
18.3 RAW TCP gateway

18.3.1 Raw client gateway

The RAW client gateway can be used if a serial “master” device has to send requests to one slave device (also called server) located on the IP network.

The server can be either an ETIC gateway or a PC including a software TCP server.





- Select the “transparent” and then the “raw client COM1” or the “raw client COM2” menu .
- Enable the raw client 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 packet” 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.

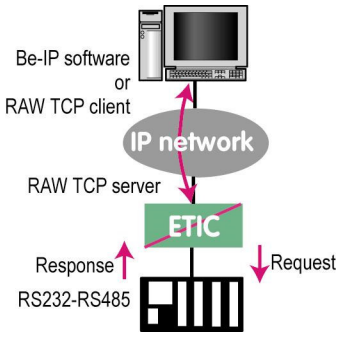
“TCP inactivity Timeout” parameter :
Set the time the gateway will wait before disconnecting the TCP link if no characters are detected.

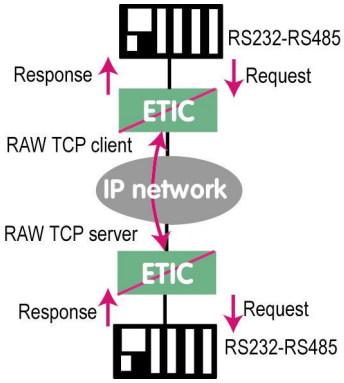
“TCP port number” parameter :
Set the port number the gateway has to use.
If the Raw TCP client gateway is assigned to both serial COM ports, the TCP port numbers must be different on each port.

“Raw server IP address” parameter :
The raw client gateway is able to communicate with a raw server gateway.
Assign an IP address to define the destination gateway.

18.3.2 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 COM1” or the “raw server COM2” menu.
- 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” parameters :
Set up the port number the gateway has to use.
If the Raw TCP server gateway is assigned to both serial COM ports, the TCP port numbers must be different on each port.

18.4 RAW UDP gateway

18.4.1 Overview

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

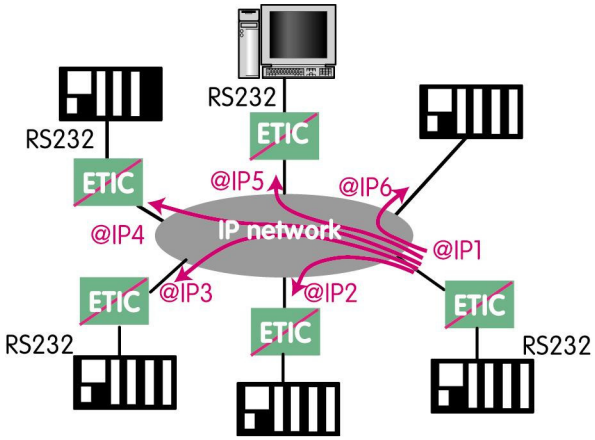
The group can include IP devices if they have the software pieces able to receive or transmit serial data inside UDP.

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

A table of IP addresses define the list of the devices belonging to the group.

The serial data is encapsulated in the UDP protocol.

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



18.4.2 Set-up

- 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 datagram.

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

«UDP port number» parameter :
Sets the UDP port number.
If the Raw UDP gateway is assigned to both serial COM ports, the UDP port numbers must be different on each port.

“IP addresses of the destination devices » table :

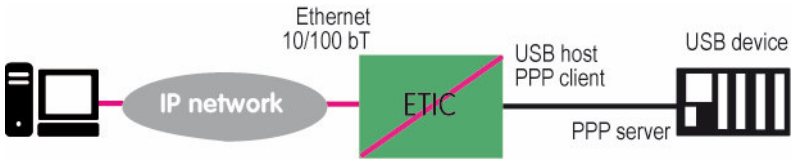
This table stores the IP addresses of the gateways to which the serial data, encapsulated inside UDP, have to be sent. A different UDP port number can be entered for each destination IP address.

19 USB gateway

19.1 Overview

The USB to IP gateway is able to forward IP traffic from devices connected to the Ethernet network to a USB device.

On the USB interface, the ETIC router behaves like a USB host and a PPP client.
The USB device connected to the ETIC router USB interface must behave like a PPP server.



Destination IP address; main case
When a device, connected to the Ethernet network, needs to transmit data to the USB device, the destination address of the IP frames which need to be transmitted to the USB device must be a specific IP address assigned to the USB gateway of the ETIC router (see the configuration below).

Destination IP address; Modbus case
If no specific IP address is assigned to the USB gateway (see below), the ETIC router forwards only modbus TCP traffic to the USB interface.
The destination IP address of the IP frames must be the LAN IP address of the ETIC router.

19.2 Set-up

Select the “Setup” menu and then the “USB” menu.

“Activate” checkbox :
Select the “Activate” checkbox.

“Use a specific IP address” checkbox :
If modbus TCP traffic only has to be forwarded to the USB device, that checkbox must not be selected.
If other kinds of traffic have to be forwarded, that checkbox has to be selected.

“Specific IP address” parameter :
If modbus TCP traffic only has to be forwarded to the USB interface, no IP address has to be entered.
If other kinds of traffic have to be forwarded to the USB device, an additional IP address must be assigned the RAS-3G.
That address belongs to the network connected to the LAN interface of the RAS-3G. It is the IP address of the USB gateway.
It will be used as the destination IP address of the IP frames which must be forwarded to the USB device.

“Accept WAN traffic” checkbox:
It is necessary to select that checkbox it the PC is connected to the network through the ETIC router the WAN interface.
It is not necessary to select that checkbox if the remote PC is connected to the RAS through a VPN or through the LAN interface.

20 Alarm email or a SMS

All the models of routers RAS are able to transmit an email when one events occurs.

- Select the Set-up > Alarms > SMS / Email menu
- Select the Enable option.

« Alarm launched on event » parameter :
Selects the event :
The digital input turns OFF
The digital input turns ON
The digital input turns OFF or ON
The VPN connects or disconnects

« Message » parameter :
Select Email or SMS

«Phone number » parameter (SMS choice):
Enter the mobile telephone number.

« Email sender » parameter (email choice):
Enter the sender email address.

"Email Destination" parameter (email choice) :
Enter the email destination address.

« Subject» parameter (email choice) :
Enter the subject of the alarm mail.

« Text» parameter :
Enter the alarm text.

SMTP client section

« Use the M2Mail service » parameter (email choice) :
ETIC TELECOM provides a SMTP service which can be used to send the alarm mail without additional set-up. Select that option to send the alarm mail through this service.

Otherwise, unselect that option and enter the SMTP server, the port number and the choice of level of security.

21 SNMP traps

- Select the Set-up > System > SNMP menu

"1st or 2nd SNMP network management IP address" parameter :
Enter the IP address of the main and possibly of the second management platform.

« SNMP version» parameter :
Select the version of the SNMP protocol used by the management server.

« Community name» parameter :
Enter the name of the SNMP community.

« System name» & system location parameter :
Enter a name and a location label to identify the ETIC router system.

22 Adding a certificate into the router

Coming from the factory, the ETIC 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.

An ETIC router can set a VPN with another one only if the certificates of both routers have been provided by the same authority.

Additional X509 certificates, provided by ETIC TEECOM or not, can be registered into the ETIC 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 ETIC router, only one certificate can be active.

To add a certificate,

- Select the Set-up > Security > Certificate menu.
- Click the « Add » button located below the certificate table.
- Select the type of certificate (PKC#12 or PEM).
- Select the certificate which must be added into the router.
- Enter the pass word which protects against the duplication of the certificate.

1 « Ping » tool

Select the Diagnostic > Tool > Ping menu.

Enter the PING destination IP address.

2 « WiFi » scanner tool

The Wifi scanner displays the main information about each WiFi network :

MAC address of the access point, SSID, reception level.

Remark : The WiFi interface of the ETIC router needs to be registered as a WiFi client interface.

3 Firmware update

The firmware update can be carried-out locally or remotely.

If the firmware update operation do not succeed, for instance if the connection fails, the ETIC router restarts with the current firmware.

Once the firmware update has been carried-out, the ETIC router restores the previous current set of parameters.

To update the firmware,

- Select Maintenance > Firmware update menu,
- Click the Select the firmware file button,
- Click Upgrade now.

When the firmware is updated, the product automatically reboots.

ETIC TELECOM
13 chemin du vieux Chêne
38240 Meylan
France
contact@eticTelecom.com