



RAS / IPL / SIG

SETUP GUIDE

The product family RAS, IPL et SIG are manufactured by

ETIC TELECOM
13 Chemin du vieux chêne
38240 MEYLAN
FRANCE

TEL : + (33) (0)4-76-04-20-05
E-mail : hotline@etictelcom.com
web : www.etictelcom.com

OVERVIEW.....	5
1 Purpose of this manual	5
2 Main functions of these Routeurs.....	5
PREPARING THE SETUP	9
1 Connecting a PC for configuration	9
1.1 Overview.....	9
1.2 First configuration	10
1.3 Changing the configuration later	10
2 Access to the administration server through the WAN interface	11
3 Working with HTTPS.....	11
4 Temporary return to the factory settings	12
5 Restoring the factory settings.....	12
6 Protecting the access to the administration server.....	13
7 Configuration steps	13
SETUP.....	15
1 Ethernet / WAN interface setup	15
2 ADSL interface setup	17
3 Cellular interface setup.....	19
3.1 SIM 1 or SIM 2 set-up	19
3.2 Using the SIM cards 1 and 2.....	20
3.3 Cellular connection control	21
4 Wi-Fi / WAN interface setup	22
5 LAN interface setup	23
5.1 Overview.....	23
5.2 Ethernet & IP menu	24
5.3 Wi-Fi access point set-up	25
5.4 Device list set-up.....	26
5.5 DHCP server menu	27
6 IPsec VPNs setup	28
6.1 Overview.....	28
6.2 IPsec VPN connection set-up	29
7 OpenVPN type VPN connection	33
7.1 Overview.....	33
7.2 Set-up principles	34
7.3 OpenVPN server set-up	35
7.4 Setting up an outgoing connection	37
7.5 Setting up an ingoing VPN connection.....	38
8 IP routing	39
8.1 Basic routing function	39
8.2 Static routes.....	39
8.3 RIP protocol	40
9 Substitution of addresses (NAT, Port forwarding, Advance NAT)	41
9.1 Network address translation (NAT).....	41

TABLE OF CONTENTS

9.2	Port forwarding	41
9.3	Advanced NAT	42
10	Publish the IP address of the router on the Internet	44
10.1	Overview	44
10.2	Set-up	44
11	Remote access connection	45
11.1	Advantages of a remote access connection	45
11.2	Types of remote access connections	46
11.3	OpenVPN remote user connection	47
11.4	OpenVPN connection for smartphones	47
11.5	PPTP connection	48
11.6	L2TP / IPSec connection	48
12	HTTPS connection and portal for smartphone, tablets or PCs	49
12.1	Overview	49
12.2	Set-up	50
12.3	Operation	50
13	M2Me_Connect connection setup	51
14	Users list	52
15	Assigning rights to remote users	54
16	Firewall setup	55
16.1	Overview	55
16.2	Main filter	56
17	Adding a certificate	58
18	Alarm email or SMS	59
19	Serial to Ip gateways	60
19.1	Overview	60
19.2	Modbus gateway	61
19.3	Raw TCP gateway	66
19.4	Raw UDP gateway	68
19.5	Raw multicast gateway	69
19.6	Unitelway gateway	70
19.7	Telnet gateway	71
19.8	USB gateway	72

DIAGNOSTICS AND MAINTENANCE 73

1	Visual diagnostic	73
2	« Ping » tool	73
3	« WiFi » scanner tool	73
4	Firmware update	73

OVERVIEW

1 Purpose of this manual

This manual describes how to set-up the RAS, IPL and SIG families of IP routers manufactured by ETIC TELECOM.

This manual applies in particular to the models listed below :

Machine Access Box with Ethernet	RAS-E
Machine Access Box with Cellular	RAS-EC, RAS-C
Machine Access Box with Wi-Fi	RAS-EW
Machine Access Box with Cellular and Wi-Fi	RAS-ECW
Router with Ethernet	IPL-E
Router with ADSL	IPL-A
Router with Cellular	IPL-C
Router with Wi-Fi	IPL-EW
Router with ADSL and Cellular	IPL-DAC
Router with Ethernet and Cellular	IPL-DEC
VPN Server with Ethernet	SIG-E
VPN Server with Cellular	SIG-EC
VPN Server with ADSL	SIG-A

In this document, the name "Router" refers to both RAS, IPL and SIG products.

2 Main functions of these Routers

IP router

The router provides powerful, flexible and comprehensive solutions to route IP packets from one network to other networks:

- Static routes, to reach nested networks,
- Network address translation d'adresse (NAT, DNAT, port forwarding),
- Routing protocol (RIP),
- Domain name management DNS et DynDNS.

IPSec & OpenVPN tunnels

The Router features IPSec and OpenVPN tunnels to provide a high level of security and also compatibility with existing devices.

The VPN connection guarantees a high level of performance and security

Transparency: The VPN interconnects the two networks so that any machine in one network can communicate with a machine on the other network.

Authentication: The router that establishes the VPN is authenticated by the one that accepts it and any other connection is rejected.

Confidentiality: Data traffic via the VPN is encrypted.

IPSec will be chosen when the Router needs to establish a VPN with an already installed IPSec VPN server.

OVERVIEW

OpenVPN will be preferred when VPN traffic is routed through intermediate routers to take advantage of the flexibility of this technique.

Remote access server for PCs, tablets and smartphones

The Router can also behave like a remote access server.

If he is registered in the user list, a remote user can access to particular devices of a machine network depending on his identity.

The new HTTPS portal make possible to access easily and safely to HMIs or PLCS web servers using a tablet, a PC or a smartphone.

Remote maintenance of machines using the M2Me_Connect service

The Router allows to connect easily and safely a machine to a remote PC, through the M2Me_Connect Internet cloud service, for operation like remote maintenance.

When the remote PC is connected, the remote user can exchange any kind of data with each device of the machine network as if his PC was directly connected to the machine network.

Firewall

The firewall protects against the sophisticated attacks coming from the Internet.

It is also able to filter IP frames between the WAN interface or any VPN interface on one hand, and the LAN interface on the other hand.

VRRP redundancy

VRRP makes possible to use two Routers shaping a redundant solution.

Automatic backup of an ADSL link over the cellular network

The IPL-DAC provides an ADSL interface and a cellular interface. It is designed for critical industrial remote SCADA systems.

In normal situation the data are transmitted via the main interface (usually the ADSL one).

In case of a failure the data are transmitted via the backup interface (usually the cellular one).

Automatic backup of a private VPN network over the cellular network

The IPL-DEC provides a WAN Ethernet interface and a cellular interface. It is designed for critical industrial remote SCADA systems.

In normal situation the data are transmitted via the main interface (usually the WAN Ethernet).

In case of a failure the data are transmitted via the backup interface (usually the cellular one).

Wi-Fi interface (optional)

The Router can be equipped with a Wi-Fi 2.4 and 5GHz interface able to behave like a client or an access point.

SNMP

The Router is an SNMP agent; it complies with the MIB2 standard and transmits an SNMP trap when configurable events occur.

DNS server

DNS makes it possible to assign Internet names to devices or organizations independently of their public IP address.

The Router behaves like a DNS server for the devices connected to the LAN.

DHCP server

On the LAN interface, the Router can behave like a DHCP server.

Configuration

The Router is configured using an HTML browser (HTTP or HTTPS).

EticFinder

The ETICFinder software can easily detect all ETIC branded products connected to an Ethernet network to display their MAC address and their IP address.

Serial gateway

Optionally, the Router provides 1 or 2 serial RS232, RS485, RS422 interfaces.

The serial gateway features the following modes :

- Raw TCP client or server

- Raw UDP

- Telnet

- Modbus master or slave

- Unitelway


PREPARING THE SETUP

1 Connecting a PC for configuration

1.1 Overview

The Router is configured using a PC with a web browser. No additional software is required.

Online help:

For most pages of the administration server an help page is available by clicking  located at the top right of the page.

Administration server address:

When the product is delivered, the IP address of the administration web server is 192.168.0.128.

First setup:

For the first configuration, we advise to connect the PC directly to the LAN interface of the Router. Subsequent changes can be made remotely.

Restoring the factory IP address:

The factory IP address 192.168.0.128 can be restored (see the User guide of the product).

Restricted access to the administration server:

If you do not have access to the administration server, it is probably that access has been restricted for security reasons or for other reasons.

Network IP address:

Later in the text, we often speak of "network IP address". We mean the lowest value of the addresses of the network.

For instance, if the netmask of a network is 255.255.255.0, the network IP address of that network is terminated by a zero (X.Y.Z.0.).

Characters allowed:

Accented characters are not supported.

PREPARING THE SETUP

1.2 First configuration

Step 1: Create or modify the PC TCP/IP connection

Assign to the PC an IP address different but consistent with the factory IP address of the Router.
For the first configuration, assign for instance 192.168.0.1 to the PC.

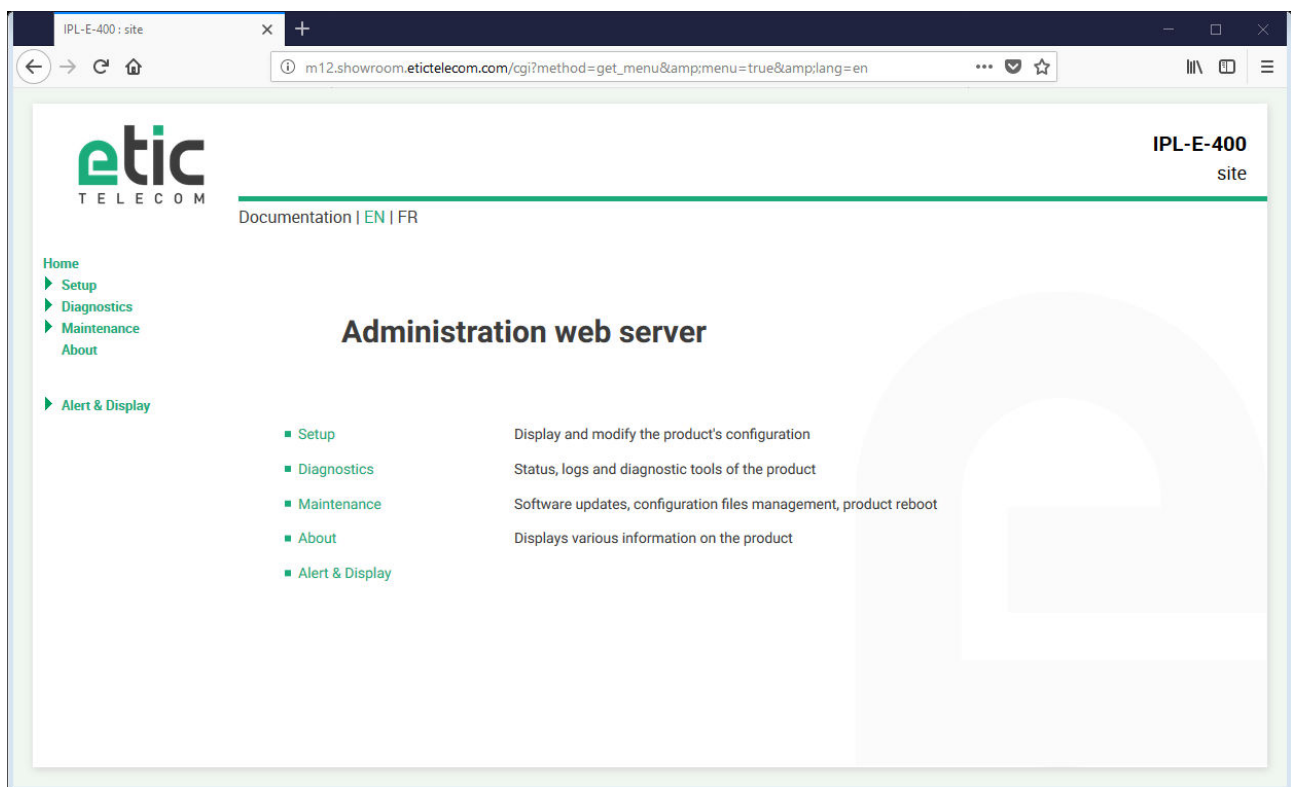
Step 2: Connect the PC to the Router

Connect the PC directly to the Router with any Ethernet cable (straight or cross-wired);

Step 3: Launch the web browser

Launch the web browser and then enter the IP address of the Router: 192.168.0.128

The Home page of the administration server is displayed.



Note: Access to the administration server is not protected when configuring the Router for the first time.

1.3 Changing the configuration later

Thereafter, the Router administration server is accessible from the local Ethernet interface or remotely through a remote connection at the IP address assigned to the product.

By default, the access to the administration web server is not allowed through the WAN interface.

2 Access to the administration server through the WAN interface

To allow the access to the administration server through the WAN interface:

- In the menu, choose **Setup > Security > Administration rights**.
- Enter the username and the password.
- Select the protocol to use for configuration **HTTPS only** or **HTTP and HTTPS**.
- Tick the **Enable access from the WAN(s)** checkbox.

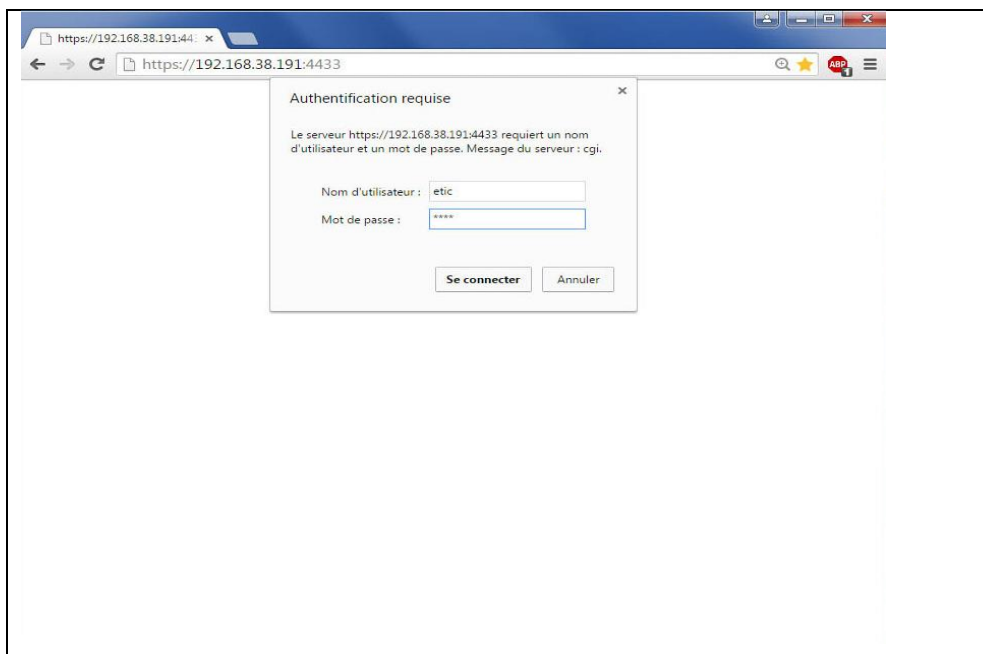
The administration server is accessible with HTTPS through the WAN or the LAN interface.

3 Working with HTTPS

Once HTTPS has been selected, proceed as follows:

The port 4433 is assigned to administration server.

- Open the web browser and enter the IP address of the Router administration server:
Example: <https://192.168.38.191:4433>.
- Click **Next** when a warning message is displayed
- Enter the user name and password that have been set to protect access to the administration server.




The home page of the administration server is displayed.

PREPARING THE SETUP

4 Temporary return to the factory settings

If the IP address of the Router could not be founded, or if it is impossible to access the administration server, for example, following a configuration error, it is possible to restore the factory settings without losing the current configuration.

- Press the push-button located on the back, for example with a small screwdriver
- Keep the push-button pressed for about 3 seconds;
- The LED  blinks red rapidly
- The administration server becomes accessible at the factory IP address (192.168.0.128), in HTTP without a password. The factory configuration is temporarily running. However, the current configuration is not lost and it is the one that is still displayed in the pages of the Administration Server.
- After reading the IP address or changing some parameters, press again the push button or reboot the product.
- The product can be reached at the registered IP address.

Note:

If the IP address of the Router is unknown, the software tool [EticFinder](#) can be used.


This software detects all ETIC branded products on a local network. After starting the software, click on the "Search" button, and when the product list is displayed, double-click on the product address to access the html server.

5 Restoring the factory settings

It is possible to restore the factory configuration permanently using the push button on the rear panel, or by using the administration server. In this case, the current configuration will be lost unless it has been saved to a file.

To restore the factory settings using the push button,

- Power off the Router,
- Press the push-button located on the back, for example with a small screwdriver,
- Power on the Router, while keeping the push-button pressed at least 10 s.

The LED  turns red; the Router boots and the factory configuration is restored.

Note: The factory configuration can also be restored via the menu [Maintenance > Configurations management](#) of the administration server.

6 Protecting the access to the administration server

- In the menu, choose **Setup > Security > Administration rights**
- Enter a user name and password to protect the administration server.
- Tick the **Password protect the web site access** checkbox

If the username and password to access the administration server are lost, you have to [temporarily return to the factory settings](#); access to the administration server is then free.

7 Configuration steps

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

- Set up the LAN interface
- Set up the WAN interface
- Set up the routing functions
- Set up VPNs
- Set up the remote access
- Set up the firewall
- Set up the serial gateways

SETUP

1 Ethernet / WAN interface setup

This section applies to the below routers:

IPL-E, IPL-EW, IPL-DEC, SIG-E, RAS-E, RAS-EC, RAS-EW, RAS-ECW.

Il s'applique aussi aux routeurs IPL-A ou IPL-C lorsque l'on souhaite utiliser l'interface RJ5 N°1 comme interface WAN au lieu de l'interface ADSL (IPL-A) ou l'interface cellulaire (IPL-C).

- Select the Set-up > WAN menu

« WAN type » list :

Select the "Ethernet" 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 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 Router.

Do not select PPOE except in the situation described above.

SETUP

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 path will 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 netmask and the default gateway address assigned to the 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 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

This section applies to the below routers:

IPL-A, IPL-DAC, SIG-A

- 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 paragraph).

SETUP

IP configuration of the ADSL line depending on the

	PPPoE	PPPoA	EoA	IPoA
“Priority” parameter Enter a medium value	●	●	●	●
« PPP login » & « PPP password »: Enter the ADSL account values	●	●		
« PPPoE service name » parameter : It is the name of the service provided by the operator It is usually not necessary to enter that parameter	●			
“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 provide those 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 for the devices of the LAN interface. Leave that checkbox unselected	●	●	●	●

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

3 Cellular interface setup

This section applies to the below routers:

IPL-C, IPL-DAC, SIG-C, RAS-C, RAS-EC, RAS-ECW

For some models, 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).

SETUP

« Cellular network » parameter :

The Router is supposed to connect to the best cellular relay available.

However, in particular situations, it may be useful to force the Router 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 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 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 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 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 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 Wi-Fi / WAN interface setup

This section applies to the below routers:

IPL-EW, IPL-AW, IPL-CW, RAS-EW, RAS-ECW

Remark :

The Wi-Fi scanner makes possible to detect the Wi-Fi networks around the Router.

To use the Wi-Fi scanner, select the Diagnostic > Tools > Wi-Fi scanner menu.

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

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

Wi-Fi 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.

« **Authentication** » 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.

Wi-Fi 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 netmask 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 on the LAN interface

A fixed IP address must be assigned to the LAN interface of the Router.

DHCP server

The 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 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 be allocated individually to the remote users.

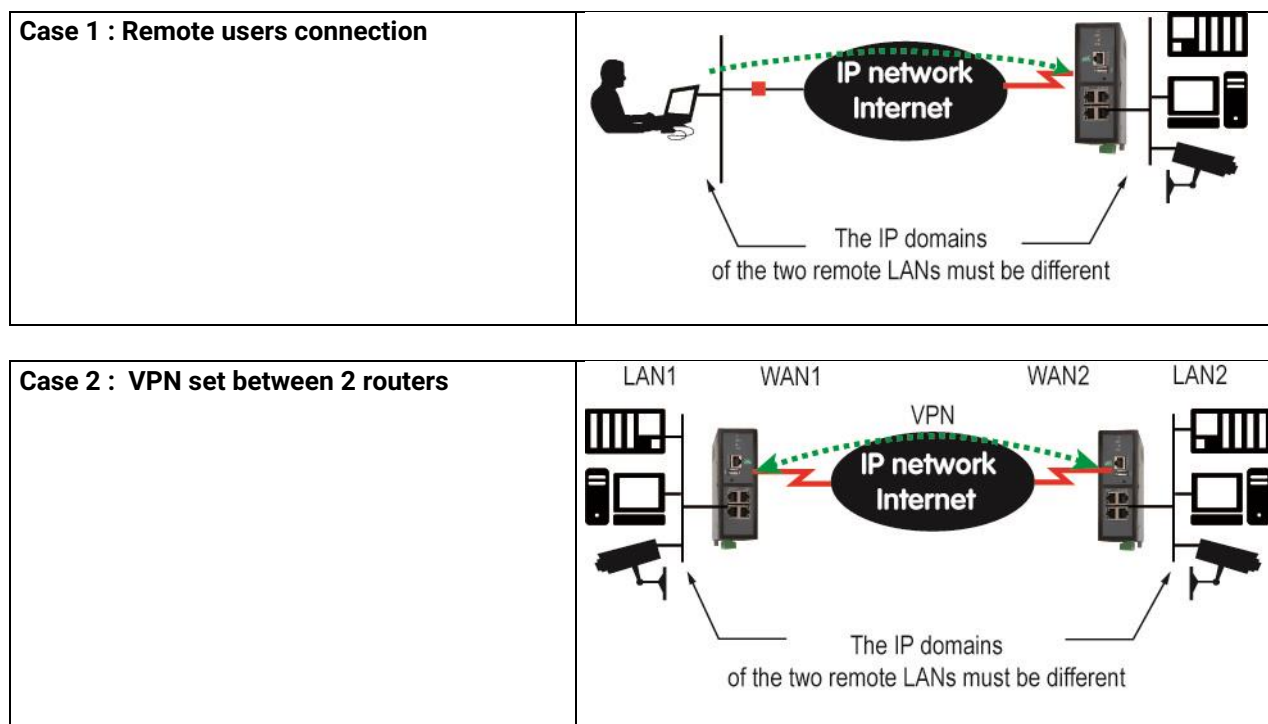
Wi-Fi access point

When the optional Wi-Fi interface is set-up as an access point, the devices connected to the Router through that Wi-Fi network belong to LAN network.

As a consequence, their IP address belong to the IP domain of the LAN network.

SETUP

IP addresses allocation



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 » & « netmask » 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, 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 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 Wi-Fi access point set-up

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

To set-up the Wi-Fi access point,

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

« 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.

« Preshared key » parameter :

Enter the WPA preshared key (at least 8 characters).

« Country code » parameter :

The RF channels allocated to the Wi-Fi 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.

« Wi-Fi Mode » parameter :

Select one of the possible Wi-Fi 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 Wi-Fi mode must be entered in each Wi-Fi client (tablet ...).

« RF channel » :

Select a traffic channel in the list.

SETUP

Remark :

It is preferable to select an unused channel at the location where the Router is installed.

Use the Wi-Fi scanner to display the channels used by the Wi-Fi 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

The screenshot shows the 'Devices list' configuration page in the etic RAS-ECW-220 web interface. The breadcrumb trail is 'Home > Setup > LAN interface > Devices list'. The left sidebar menu includes 'Setup' (with sub-items: WAN interfaces, LAN interface, Ethernet and IP, Wi-Fi access point, Devices list, DHCP Server), 'Remote access' (with sub-items: M2M_Connect, Users List, Access rights, Remote access servers), 'Network', 'Security', 'Serial gateways', 'Alarms', 'System', 'Diagnostics', and 'Maintenance' (with sub-item: Alarms). The main content area has a form for 'Site Name' (Bridge water station), 'Domain Name', and 'Show Web portal' (checked). Below this is a 'Devices list' table with columns 'Name' and 'IP Address'. The table contains three entries: 'Pump P/C' (192.168.38.10), 'Main P/C' (192.168.38.11), and 'WLS' (192.168.38.12). Below the table are buttons for 'Show', 'Edit', 'Delete', 'Add', 'Copy and edit', 'A', and 'V'. At the bottom are 'Save' and 'Cancel' buttons.

Name	IP Address
Pump P/C	192.168.38.10
Main P/C	192.168.38.11
WLS	192.168.38.12

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 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 Wi-Fi 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 » & « netmask » 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 ETIC Router, enter the address of the router.

6 IPSec VPNs setup

6.1 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.

10 IPSec connections can be set by one IPL or RAS router.

100 IPSec connections can be set by one SIG router.

500 IPSec connections can be set by one SIG VM 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 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 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 authentic 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.

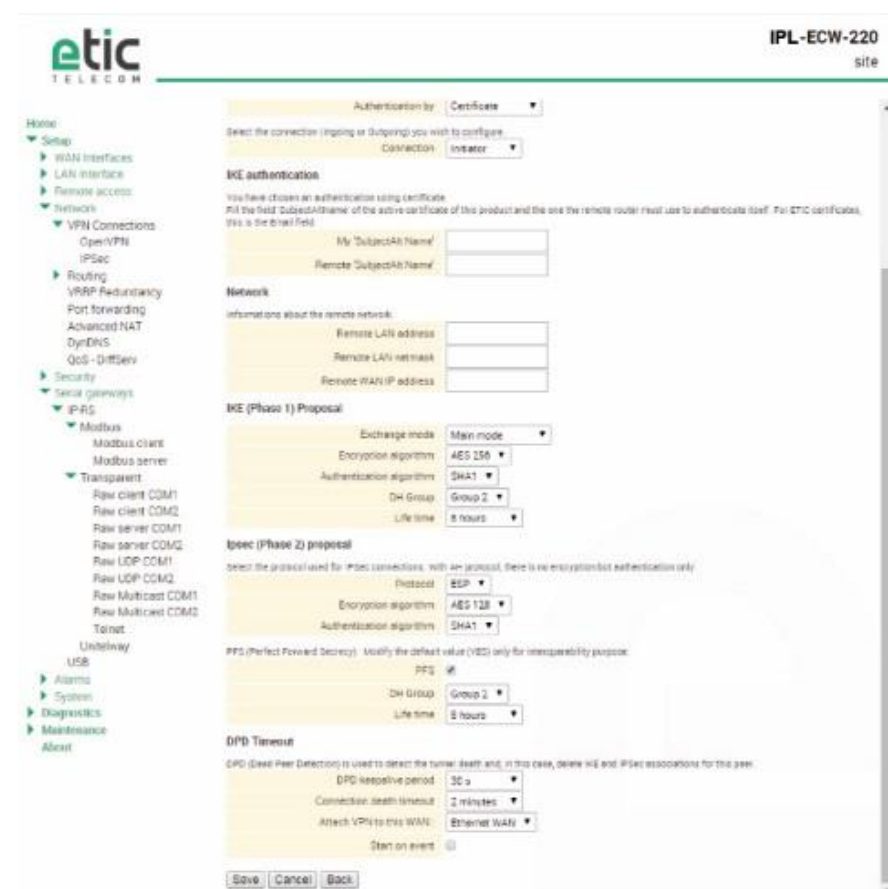
6.2 IPSec VPN connection set-up

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

The IPSec VPN home page is displayed.



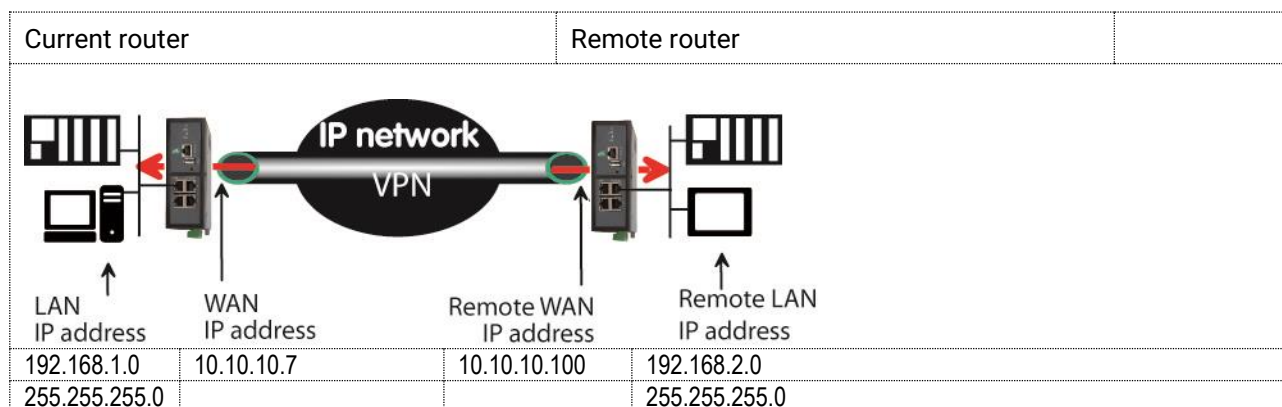
To add an IPSec VPN connection, click « Add». The set-up page of the new VPN connection is displayed.



SETUP

- 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.



« 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.

SETUP

«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.

7 OpenVPN type VPN connection

7.1 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.

10 OpenVPN connections can be set by one IPL or RAS router.

100 OpenVPN connections can be set by one SIG router.

500 OpenVPN connections can be set by one SIG VM 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.

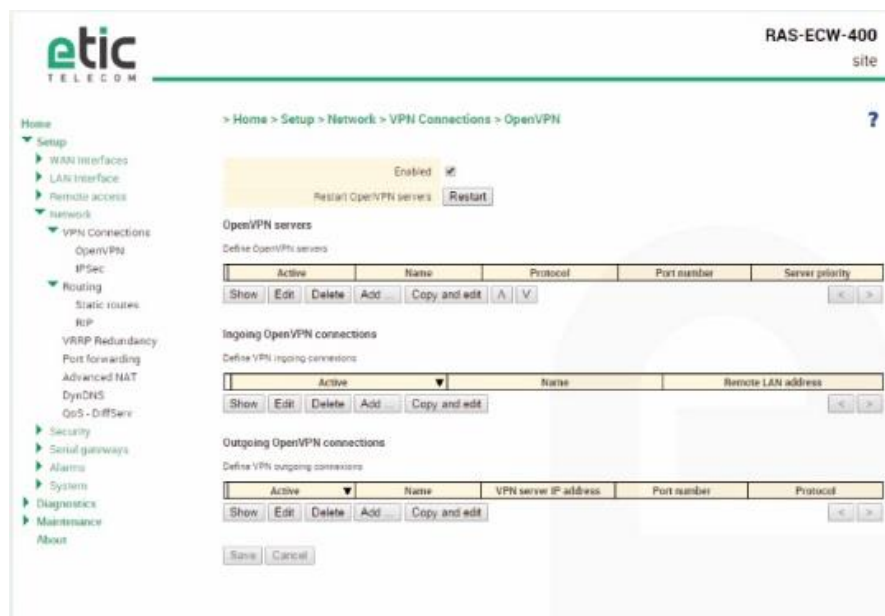
The reasons is the source IP address is not checked by OpenVPN to authenticate the remote router; OpenVPN authenticates the remote router with a Login password and certificate.

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.



7.2 Set-up principles

• VPN server set-up

If the Router behaves like a VPN server, it means that the 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 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 :

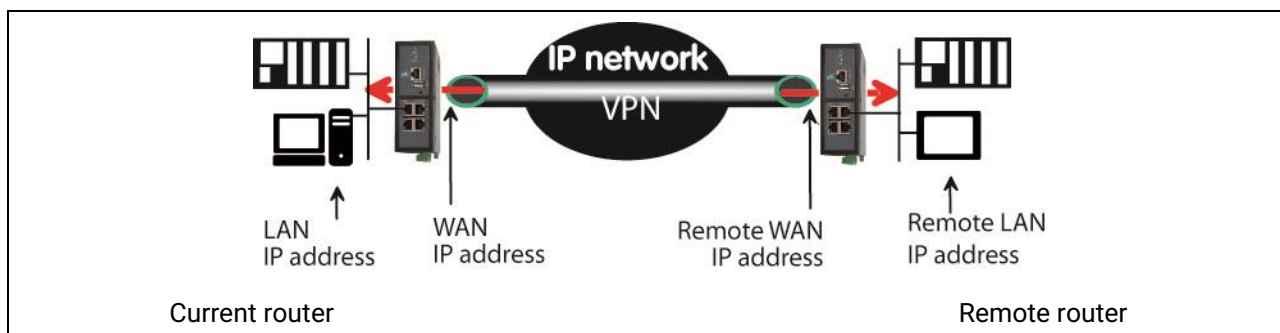
- Transport protocol (UDP or TCP) and port number.
- Encryption algorithm (Blowfish, AES 256, AES192, AES128, 3DES).
- Authentication (MD5, SHA1).

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



7.3 OpenVPN server set-up

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

Active ☒

name

Enter the port number used for Incoming and Outgoing connections.
Warning, this value must be different from the one used for remote user access.

Port number

Protocol

The VPN network address is a private network address used by routers to set the OpenVPN VPN, you can leave the default value except if one of your networks already uses it.

VPN network address

VPN network netmask

Enter the timeout to detect the death of the remote and

Connection death timeout

Packet retransmit timeout on OpenVPN control channel if no acknowledgment has been received from the remote party.

Packet retransmit timeout

Select the encryption algorithm and the authentication algorithm used for incoming and outgoing connections.

Encryption

Authentication

Enter the metric number used for all pushed routes.

Server priority (0 to 255, step 1)

Push routes parameters :

Push local route to VPN clients ☒

Push static routes to VPN clients ☒

Push clients routes ☐

First specific route to push:

IP address

Netmask

Second specific route to push:

IP address

Netmask

“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.

SETUP

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 parameter 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 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 Router.
If it is necessary static routes must be programmed in both routers.

« 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.

7.4 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 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 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 Router.

Select the interface to which the VPN must be attached.

SETUP

« 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

7.5 Setting up an incoming VPN connection

An incoming VPN connection is a connection received by the current Router acting as a VPN server.

- To create an incoming connection, select the « Add » button located just below the Incoming 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 Router.

If the active certificate of the remote Router is delivered by ETIC TELECOM, that field is the email field.

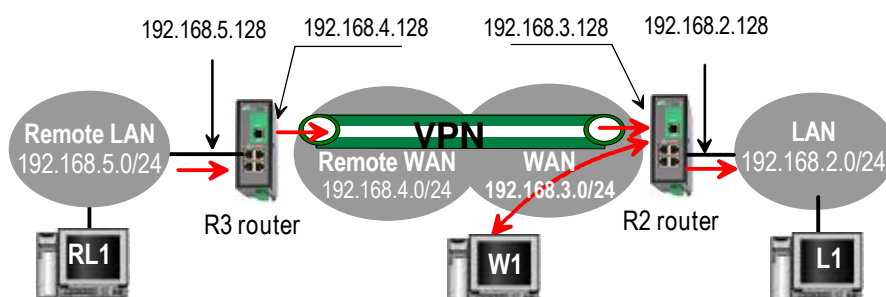
8 IP routing

8.1 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 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.

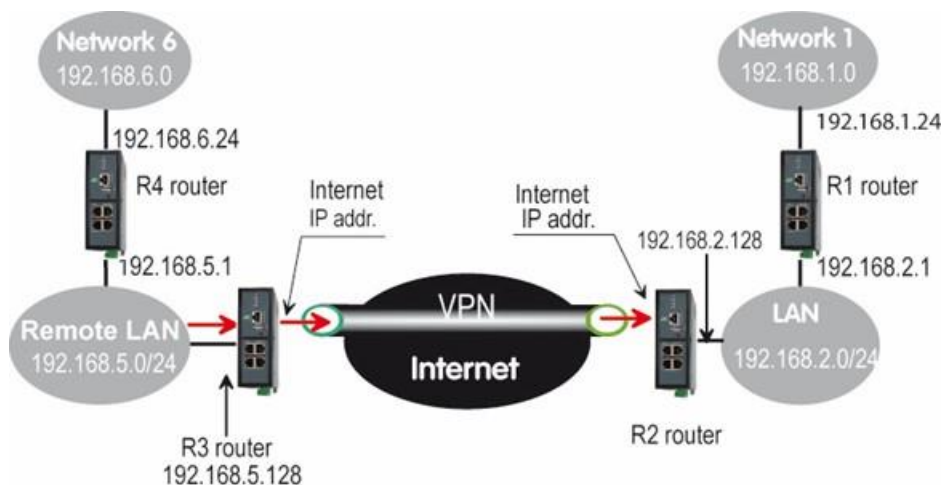
Remark 2 : A default gateway address must be entered in each device of the different networks.

8.2 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.



SETUP

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.

8.3 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.

9 Substitution of addresses (NAT, Port forwarding, Advance NAT)

9.1 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 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.

9.2 Port forwarding

9.2.1 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.

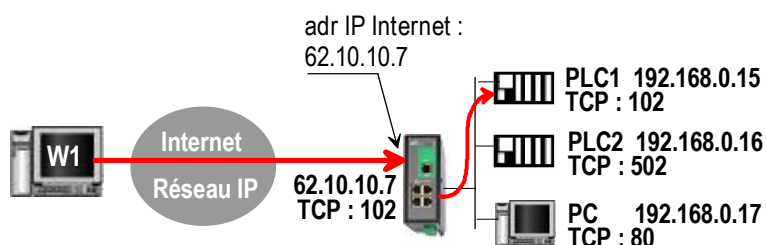
Example :

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 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 Router on a particular port number.

The 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.



SETUP

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

9.2.2 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)

9.3 Advanced NAT

9.3.1 Overview

The advanced NAT function consists in modifying the source or destination IP addresses and port number of the frames received by the 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	

9.3.2 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.

10 Publish the IP address of the router on the Internet

10.1 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.

10.2 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.

11 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.

11.1 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**

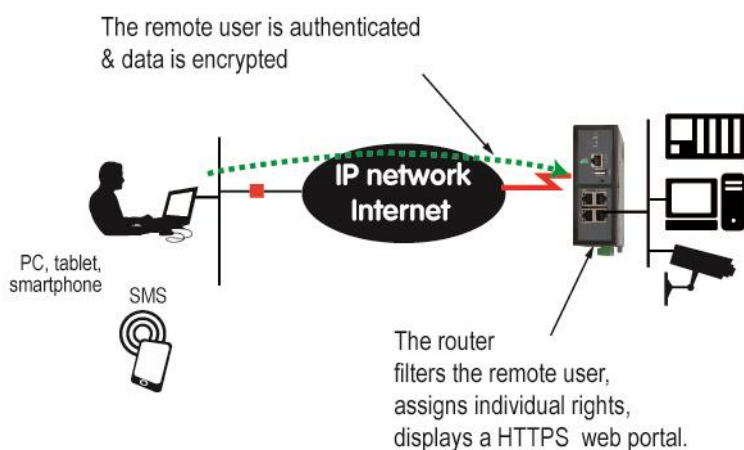
Once the remote connection has been launched, the PC receives automatically an IP address of the network. The user can access to each authorized device of the network.

- **Data encryption**

Data is encrypted from end to end.

- **PC, Tablet, smartphone**

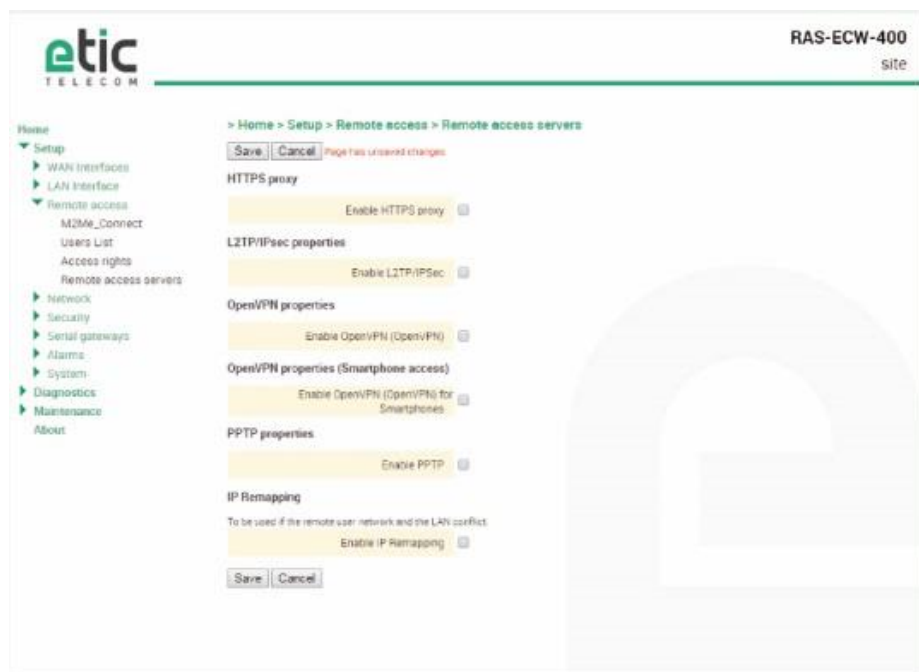
The solutions provided by the Router are suitable as well for Windows PCs or tablets or smartphones (Android or IOS).



To set-up a remote connection,

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

SETUP



11.2 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 <u>and</u> 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; It is described in the following chapter.

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

11.3 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 be 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 Router (see the table at the top of the page).

« Encryption Algorithm » & « Message digest algorithm » :

Leave the default values Blowfish & MD5.

11.4 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 be 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 Router (see the table at the top of the page).

SETUP

« Encryption Algorithm» & « Message digest algorithm» :

Leave the default values Blowfish & MD5.

11.5 PPTP connection

- Select the PPTP checkbox.

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

11.6 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 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).

12 HTTPS connection and portal for smartphone, tablets or PCs

12.1 Overview

The Router can behave like a HTTPS server for remote users.

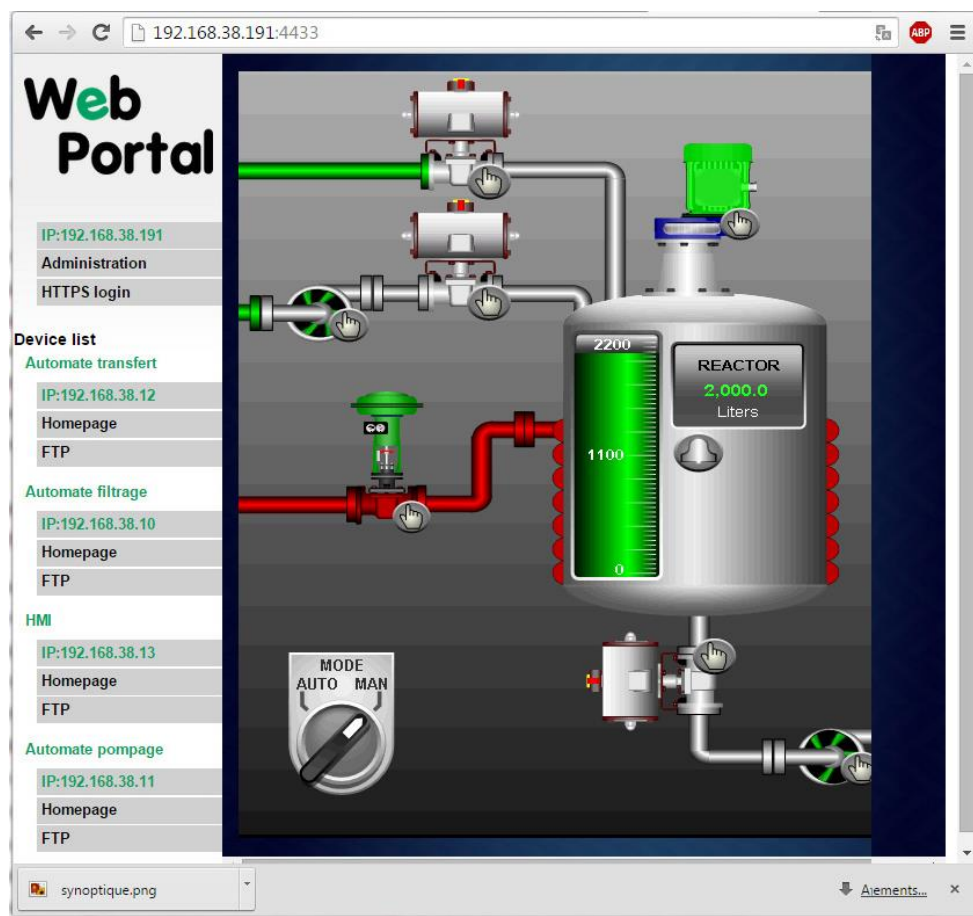
In addition, the HTTPS server can behave like a HTTPS to HTTP gateway to give a secure remote access to HTML / HTTP pages embedded in devices.

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 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.



12.2 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 organized 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

12.3 Operation

To access to the HTTPS internet portal from the Internet,

- Launch the browser
- Enter : <https://> « Internet IP address of the 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.

13 M2Me_Connect connection setup

That paragraph applies to all the models of RAS Routers. It also applies to all other Routers, 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 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 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 (ABOUT menu); it is required by the M2Me software of the remote PC when you will set-up the connection to the Router.

14 Users 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.

The screenshot shows the 'User Configuration' page for a user named 'Jane'. The page is part of the 'RAS-ECW-220 site' configuration. The breadcrumb trail is: Home > Setup > Remote access > Users List > User Configuration. The left sidebar contains a navigation menu with options: Home, Setup (expanded), WAN interfaces, LAN interface, Remote access (expanded), M2Me_Connect, Users List, Access rights, Remote access servers, Network, Security, Serial gateways, Alarms, System, Diagnostics, Maintenance, and About. The main content area displays a form for adding a new user. The form includes fields for: Active (checkbox), Full name (Jane), Company (etic telecom), Email address (jane@etictelecom.com), Phone number (33 7 98 65 41), User name (Jane), Password (password), and Password strength (medium). A 'Passwords match' checkbox is also present. Below the form, a security note states: 'For security reasons, choose a password longer than 8 characters with uppercase and lowercase letters, numbers and special characters'. At the bottom of the form are buttons for 'Save', 'Cancel', and 'Back'.

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

15 Assigning rights to remote users

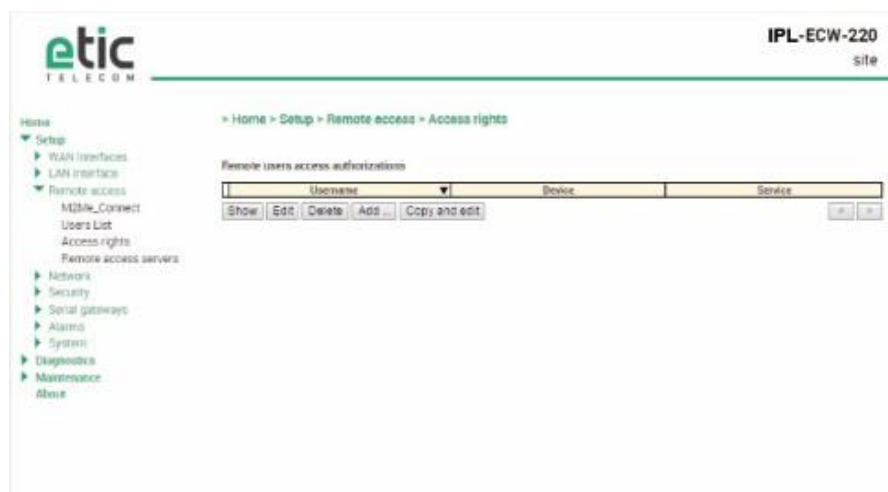
Individual access rights to the network can be assigned to each user.

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 can be a subnet or an IP address (refer to the Set-up > LAN interface > Device list).



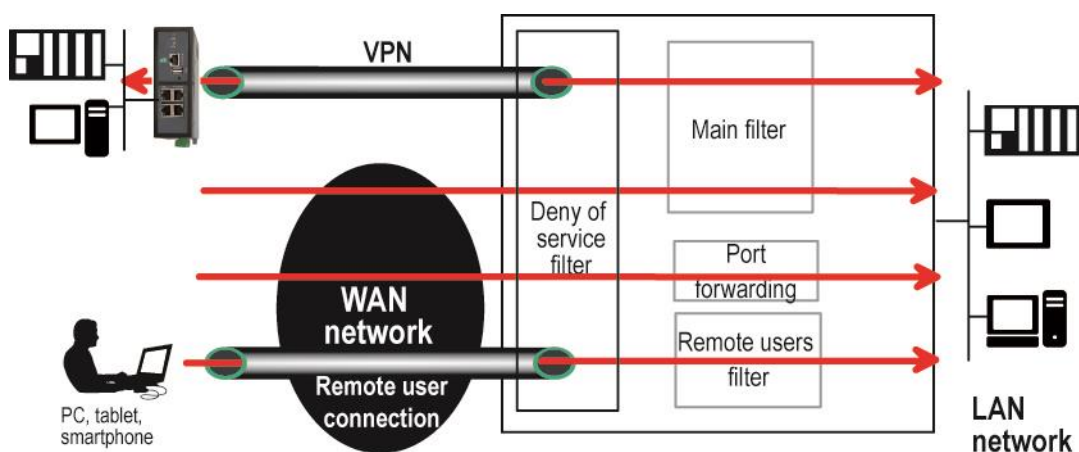
16 Firewall setup

16.1 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.



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 packets 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.

16.2 Main filter



16.2.1 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.

17 Adding a certificate

Coming from the factory, the 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 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 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 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.

18 Alarm email or SMS

All the models of Routers 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.

19 Serial to Ip gateways

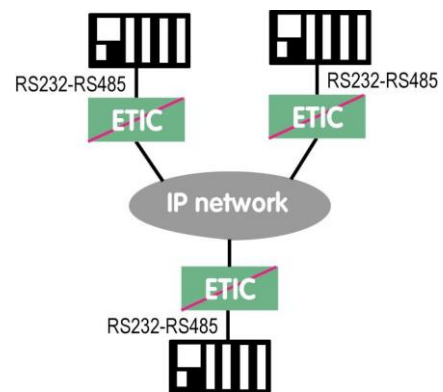
19.1 Overview

Depending on the model, the Router provides 2 serial ports : 2 RS232, or 1 RS232 and 1 RS485, or 1 RS422 isolated or 1 RS485 isolated.

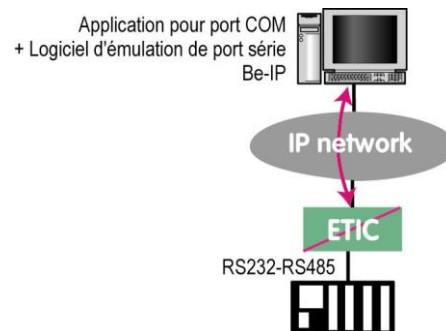
A gateway can be assigned to each serial port.

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.

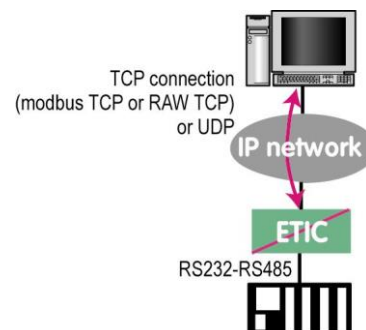
- Communication between serial devices



- Communication between a serial device and a PC via 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).



To perform the functions described above, several types of gateways are available.

19.2 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

19.2.1 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

.

19.2.2 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 product.

Select the Modbus Client gateway to connect a serial Master device to the serial port of the product.

19.2.3 Assigning a Modbus gateway to a serial port

The Modbus client gateway (respectively server) can be assigned to the serial port COM1 or COM2.

The Modbus client gateway can be assigned to a serial port (COM1 for ex.) while the Modbus server gateway is assigned to the other port (COM2 for ex.).

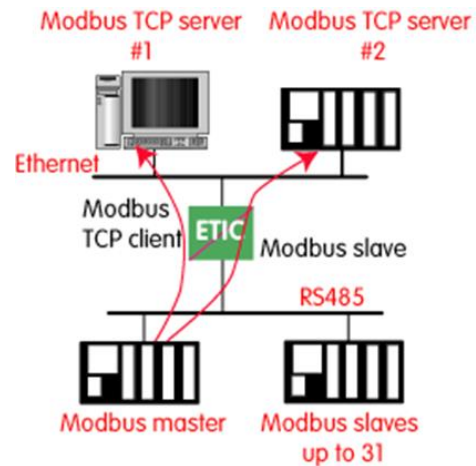
SETUP

19.2.4 Modbus client gateway

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

The gateway can be connected to several Modbus TCP servers on the IP network

Other slaves can be connected to the serial link.

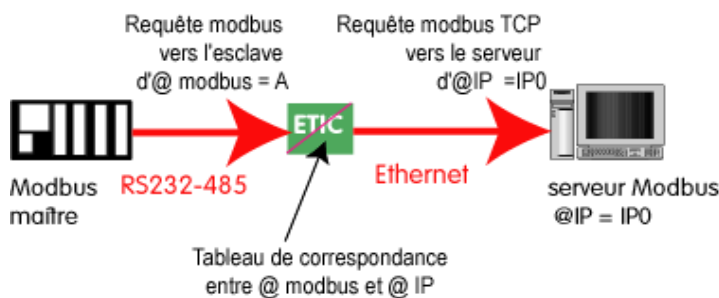


How the Modbus Client Gateway works :

In order to access a Modbus TCP server on the IP network, a mapping table between a Modbus slave address and an IP address is set ; so when the Modbus master sends a request to the Modbus slave at address A, the mapping table allow to transmit the request to the corresponding IP address.

In addition, the Modbus address field of the Modbus TCP frame is set to A.

The mapping table can contain 32 lines allowing a Modbus master to address 32 servers on the IP network.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Modbus > Modbus client**.
- Tick the **Enable Modbus client** checkbox.
- Configure the following parameters.

COM port

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Modbus protocol

Select RTU (hexa) or ASCII.

Inter-character time

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 idle Timeout

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

TCP port

Set the port number the gateway has to use. The default Modbus TCP port is 502.

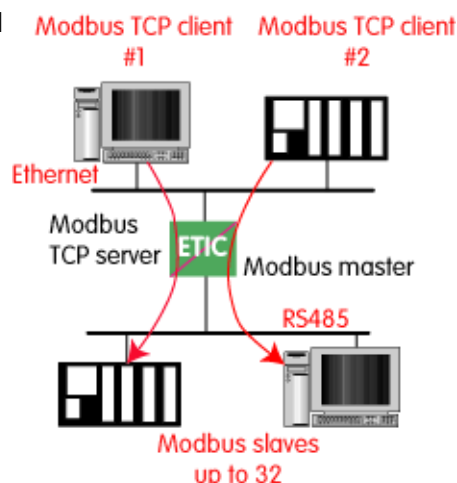
Modbus slaves

The table allow the mapping of a Modbus slave address to an IP address.

19.2.5 Modbus server gateway

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

Up to 32 slaves, can be connected to the RS485 port.



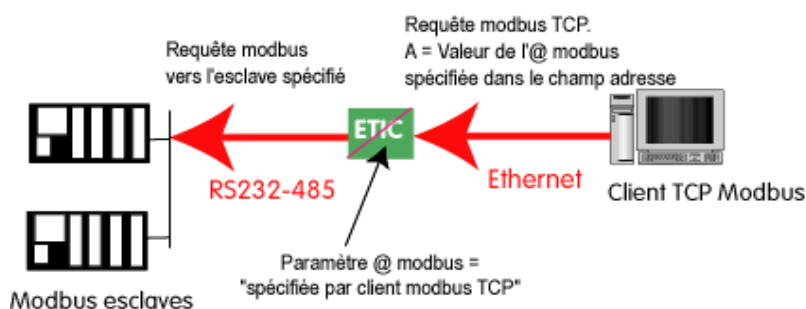
How the Modbus server Gateway works :

A Modbus TCP client send a Modbus TCP client to the gateway.

The gateway behave as a master on the serial link. It transcode and transmit the request on the serial link.

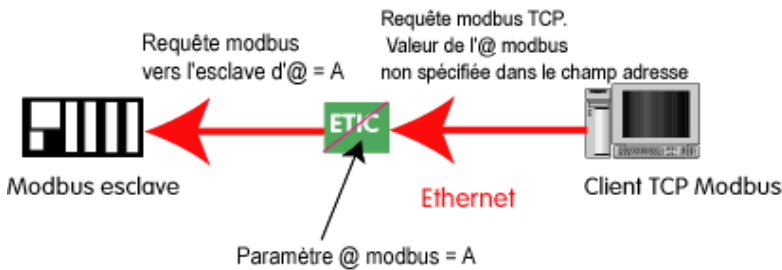
The Modbus slave address of the request is :

- Either the address contained in the Modbus TCP address field ; in this case, several slaves can be addressed on the serial link.



- Or a fixed address configured in the gateway (see below); in this case, only one slave can be addressed on the serial link.

SETUP



Warning : Several TCP Modbus client can send requests to the slaves on the serial link. Nevertheless, care must be taken not to saturate the serial link since its flow rate is much lower than the Ethernet one.

To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Modbus > Modbus server**.
- Tick the **Enable Modbus server** checkbox.
- Configure the following parameters.

COM port

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link..

Modbus protocol

Select RTU (hexa) or ASCII.

Enable proxy/cache function

If this function is active, a request is only sent to a slave if the same query has not been sent since the time set by the "cache refresh" parameter.

Cache refresh

Sets the minimum time between two identical requests to the same slave.

Inter-character time

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

If the value "0" is selected, the gateway uses the Modbus address specified by the Modbus TCP client to address the Modbus slave on the serial link ; up to 32 slaves can be addressed on the serial link.

If a particular value is selected (1 to 255), the gateway sends all requests to the selected slave ; only one slave can be addressed on the serial link.

TCP idle Timeout

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

Slave response timeout

Set the time the gateway will wait for a response from the slave.

TCP port

Set the port number the gateway has to use. The default Modbus TCP port is 502.

Local reiteration count

Set up the number of times the gateway will repeat a request in case of no response from the slave.

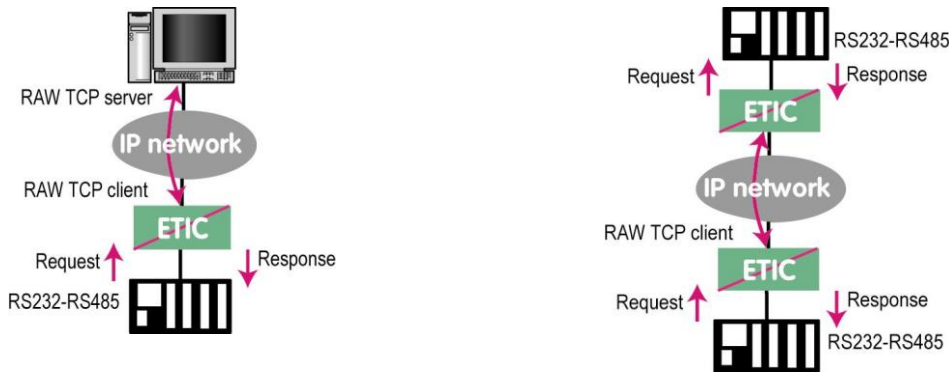
SETUP

19.3 Raw TCP gateway

19.3.1 Raw TCP client

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.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Transparent > Raw client COMx**
- Tick the **Enable** checkbox.
- Configure the following parameters.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Receive buffer size

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

RS end frame timeout

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 idle Timeout

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

TCP port

Set the port number the gateway has to use.

Warning : If two gateways of the same type are active on the two serial ports, they can not use the same TCP port number.

Server IP address

Set the IP address of the Raw server. The gateway will connect to that server and send it the data received on the serial link.

19.3.2 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).



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Transparent > Raw server COMx**
- Tick the **Enable** checkbox.
- Configure the following parameters.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Receive buffer size

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

RS end frame timeout

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 idle Timeout

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

TCP port

Set the port number the gateway has to use.

Warning : If two gateways of the same type are active on the two serial ports, they can not use the same TCP port number.

SETUP

19.4 Raw UDP gateway

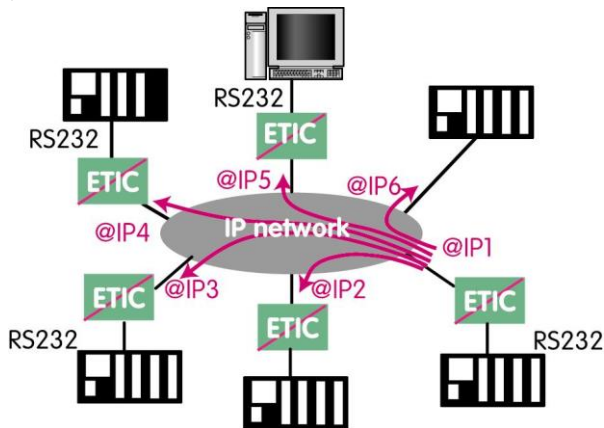
The RAW UDP gateway allows to connect together a group of serial or IP devices through an IP network. The group can include IP devices if they have the software pieces able to receive or transmit serial data inside UDP.

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.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Transparent > Raw UDP COMx**
- Tick the **Enable** checkbox.
- Configure the following parameters.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Receive buffer size

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

RS end frame timeout

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.

UDP port

Set the port number the gateway has to use.

Warning : If two gateways of the same type are active on the two serial ports, they can not use the same UDP port number.

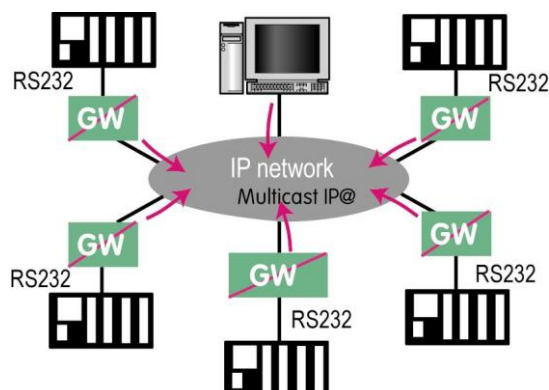
Destination

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.

19.5 Raw multicast gateway

This gateway is designed to connect a serial device to several devices on an IP network.

It uses the "multicast" protocol that can simultaneously deliver an IP frame to many devices without increasing the traffic: The RS232 data are transmitted in an IP frame with a particular IP address called multicast address; all subscribers to this address can receive the frame.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Transparent > Raw Multicast COMx**
- Tick the **Enable** checkbox.
- Configure the following parameters.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

Receive buffer size

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

RS end frame timeout

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.

UDP port

Set the port number the gateway has to use.

Warning : If two gateways of the same type are active on the two serial ports, they can not use the same UDP port number.

Multicast group IP address

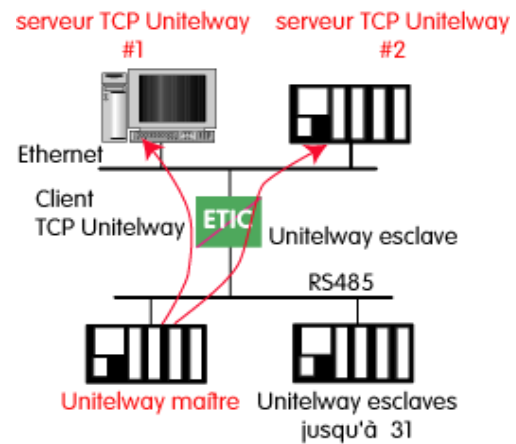
Set the IP address assigned to the multicast group in conformance with the IANA rules.

SETUP

19.6 Unitelway gateway

The Unitelway gateway is used to connect a Unitelway master PLC to an IP network.

In particular it is used to perform the remote maintenance of a Schneider Electric RS485 PLCs via an IP network.



To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Unitelway**
- Tick the **Enable** checkbox.
- Configure the following parameters.

COM port

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link..

Xway address

Gateway address in the Xway network.

TCP idle Timeout

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

Unitelway slaves

Mapping between the address of each Unitelway slave emulated by the gateway and the IP and XWAY addresses of the device on Ethernet.

19.7 Telnet gateway

This gateway allows a PC running a Telnet client software to connect to an equipment connected to the serial link of the Router.

The data rate and the format of the characters on the serial link can be controlled according to the RFC2217 standard.

To configure the gateway :

- In the menu, choose **Setup > IP-RS gateways > Telnet**
- Tick the **Enable** checkbox.
- Configure the following parameters.

COM port

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits

Allow to set the bitrate and the format of the asynchronous serial link.

TCP idle Timeout

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

TCP port

Set the port number the gateway has to use.

SETUP

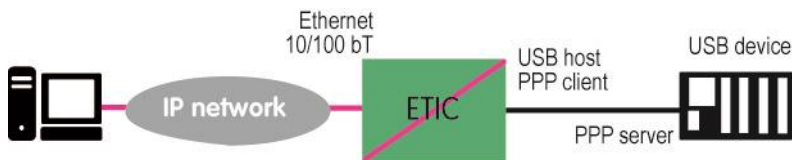
19.8 USB gateway

19.8.1 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 Router behaves like a USB host and a PPP client.

The USB device connected to the 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 Router (see the configuration below).

Destination IP address; Modbus case

If no specific IP address is assigned to the USB gateway (see below), the 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 Router.

19.8.2 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 to the Router. That address belongs to the network connected to the LAN interface of the Router. 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 if the PC is connected to the network through the Router the WAN interface.

It is not necessary to select that checkbox if the remote PC is connected to the Router through a VPN or through the LAN interface.

DIAGNOSTICS AND MAINTENANCE

1 Visual diagnostic

At power up, the RUN LED  is red for about 20 seconds during the initialization of the product.

Then the LED turns green and blinks for 30 seconds then becomes steady green when the product is ready.

If the LED remains red after that delay, the product is probably faulty ; please contact the hotline.

2 « Ping » tool

Select the Diagnostic > Tool > Ping menu.

Enter the PING destination IP address.

3 « 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.

4 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 Router restarts with the current firmware.

Once the firmware update has been carried-out, the 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.



13, Chemin du Vieux Chêne
38240 Meylan - France

Tel : +33 (0)4 76 04 20 00
contact@etictelecom.com

www.etictelecom.com