RAS/IPL/SIG Setup guide firmware 4.9

TABLE OF CONTENTS

1. WAN INTERFACES

The WANs interfaces (Wide Area Network) are the interfaces exposed to the public network. These interfaces are protected by the firewall of the router. For more information about firewalling features see the <mark>Firewall</mark> section.

Next chapters will help you configure the WAN interfaces.

1.1. ADSL

This section applies to the below routers:

IPL-A, IPL-DAC, SIG-A

Go to the *Setup > WAN Interfaces > ADSL* menu

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).

IP configuration

IP configuration of the ADSL line depends on

	PPPoE	PPPoE	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. Usually, it is 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 that addresses automatically through the line (default). Otherwise, unselect that option and enter the IP of the primary and secondary DNS server.	✔	✔	✔	✔
Enable address translation NAT checkbox: If that option is selected, the source IP address of any IP frame coming from a device connected to the LAN interface and routed to the ADSL interface, is replaced by the router WAN IP address. **NOTE** Select that checkbox if a device of the LAN interface needs to set a connection with a device connected to the Internet (FTP server, …)	✔	✔	✔	✔
Enable proxy ARP checkbox: That function gives direct access to the remote router for the devices of the LAN interface. Leave that checkbox unselected	✔	✔	✔	✔

The information entered on this page must be provided by the Internet provider.

Ping control

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

Enable ping control	Enable or disable the PING control function
IP address to ping	IP address of the machine to which the PING message has to be transmitted
Ping interval	Period between two consecutive pings
Ping retries	Number of PING messages failures before disabling the WAN interface

1.2. Cellular

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 on the SIM card number 1 is the main network, while the other one is the backup network.

Cellular interface setup

Go to the *Setup > WAN Interfaces > Cellular* menu

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.

Priority parameter:

It is possible to select the SIM card number 1, or the SIM card number 2 or both:

- `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

<u>Cellular connection control</u>

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

Enable ping control	Enable or disable the PING control function
IP address to ping	IP address of the machine to which the PING message has to be transmitted
Ping interval	Period between two consecutive pings
Ping retries	Number of PING messages failures before disabling the WAN interface

<u>Mobile service provider connection</u>

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

SIM 1 : Modem configuration

Modem initialisation string parameter:

Leave that field empty.

APN parameter:

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

PIN code parameter:

Enter the SIM card pin code.

As long as the PIN code has not been correctly entered, the OPERATION LED indicator flashes (red colour).

Cellular network parameter:

The Router 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

Login & **Password** parameters:

Enter the login and password of the subscription. 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.

NOTE	Select that checkbox if a device of the LAN interface needs to set a connection with a device connected to the Internet.

Select an operator checkbox:

If that option is selected, a specific operator can be chosen. In some cases it could be interesting to force the cellular connection through a specific service provider. For instance to avoid roaming to foreign operator when installed in border area. An operator should be mentionned by its Mobile Country Code followed by the operator Mobile Network Code. For instance for Orange (MNC=01) in France (MCC=208), the field should be filled with the code "20801".

Cellular traffic counter

Reinit day parameter:

When this day of month is reached, the router resets its Cellular traffic counter. The cellular data counter value is logged every month on the log *Diagnostic>Statistics>Cellular datas*

SIM backup system

Each SIM card can be associated to a different mobile data service.

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 <mark>at least</mark> 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 1. Sim card switching timing

> T1 Max SIM1 unconnected time before switching = 20 mn
> T1 Max SIM2 unconnected time before switching = 20 mn
> T3 Time of SIM2 connection before retesting SIM1 = 12 hours

Max SIM1 unconnected time before switching parameter:

See above.
Possible values: 5, 10, 20, 30, 60 mn

Max SIM2 unconnected time before switching parameter:

See above.
Possible values: 5, 10, 20, 30, 60 mn

Time of SIM2 connection before retesting SIM1:

See above.
Possible values:1, 12, 24 hours, 5 days, never.

Cellular connection control

If connection faults are observed, it may be interesting to activate the cellular connection control option.

The Router checks permanently that the cellular connection is properly set.

However, with particular mobile service providers, or in particular situations, the connection can remain 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 cellular connection is reset.

To implement that function, enter the parameters hereafter.

IP address or Hostname of the server parameter:

Enter the IP address or the Hostname of the device to which the Router will send a periodic ICMP message (PING)

PING Interval parameter:

Enter the period of the PINGs.
Possible values: 30 s, 1, 2, 5, 10, 20, 30, 60 mn

Number of retries parameter:

Enter the number of retries before resetting the PPP connection.
Possible values: 1, 2, 4, 8, 12

NOTE	If the problems persist, it is possible to restart the power supply of the cellular module instead of restarting only the connection. To do this, modify the parameter `p_wan_gsm_ping_ctrl_power_reset` through SSH with the command `set_params`. *Command for activating the power reset* `$ set_params p_wan_gsm_ping_ctrl_power_reset.0 true`

1.3. Ethernet

This section applies to the below routers:

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

It also applies to IPL-A or IPL-C routers when you want to use the RJ5 N°1 interface as the WAN interface instead of the ADSL interface (IPL-A) or the cellular interface (IPL-C).

Go to the *Setup > WAN Interfaces > Ethernet* menu

Ethernet WAN port configuration

Speed / Duplex parameter:

Select 10 or 100 Mb/s & full or half duplex.

IP configuration of the Ethernet WAN port

Connection type list parameter:

The Ethernet value is the default value. It has to be selected when another router connected to the Ethernet/WAN interface of the Etic Telecom 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.

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.	✔	✔
Outgoing OpenVPN connections through a proxy checkbox: Select the checkbox to configure a proxy server. This proxy server will be used for Outgoing OpenVPN connections that are attached to the `Ethernet WAN` interface.	✔	

Choice	Ethernet	PPPoE
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. | NOTE	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 a WAN interface towards a particular machine. If the PING receives a response, this WAN interface is declared active with the declared priority. If the PING message does not receive a response, this WAN interface is disabled.

Enable ping control	Enable or disable the PING control function
IP address to ping	IP address of the machine to which the PING message has to be transmitted
Ping interval	Period between two consecutive pings
Ping retries	Number of PING messages failures before disabling the WAN interface

1.4. Wi-Fi

This section applies to the below routers:

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

NOTE	The Wi-Fi scanner makes possible to detect the Wi-Fi networks around the Router. To use the Wi-Fi scanner, select the *Diagnostics> Tools > Wi-Fi scanner* menu.

Configure the Wi-Fi interface as a client to reach the Internet

Select *Setup > WAN interfaces > Wi-Fi*. Then Enable the checkbox.

Wi-Fi modem

Network name (SSID) parameter:

Enter the name assigned to the Wi-Fi network to which the Router has to connect.

| CAUTION | The SSID is case-sensitive. |

Authentification parameter:

Select WPA or WEP or None according to the access point configuration.

Key parameter:

Enter the WPA or WEP key according to the access point configuration.

Wi-Fi WAN IP configuration

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.

| NOTE | Select that checkbox if a device of the LAN interface needs to set a connection with a device connected to the Internet (FTP server, …) |

2. LAN INTERFACES

The LANs interfaces (Local Area Network) are the interfaces that interconnects equipements within a limited area such as a factory, a machine, a building.

2.1. Ethernet switch

The LAN interface consists of 1 to 4 switched Ethernet 10/100 BT RJ45 connectors.

Next chapters will help you configure the LAN interface.

2.2. Ethernet & IP

Go to the screen *Setup > LAN Interface > Ethernet & IP*

LAN network

IP address & **Netmask**	A fixed IP address must be assigned to the LAN interface of the Router. It is `192.168.0.128` by default. **NOTE** — That IP address is also the IP address of the administration server of the Router
Default gateway	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. **NOTE** — Leave that field empty if no other router is connected to the LAN network

Remote access

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.

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

Automatic management of the remote users IP addresses	If checked, the Router allocates automatically an unused IP address of the LAN network to a remote user when he connects
IP address pool start & **Address pool end**	If addresses are not automatically allocated, these are the fixed IP addresses which can be allocated to the remote users. These IP addresses must belong to the LAN domain

Example 2. LAN configuration

	IP address	Remark
LAN network	192.168.12.0 / 24	From 192.168.12.1 to 192.168.12.254
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	

CAUTION

Be careful with IP addresses used by the LAN interface when configuring VPNs.
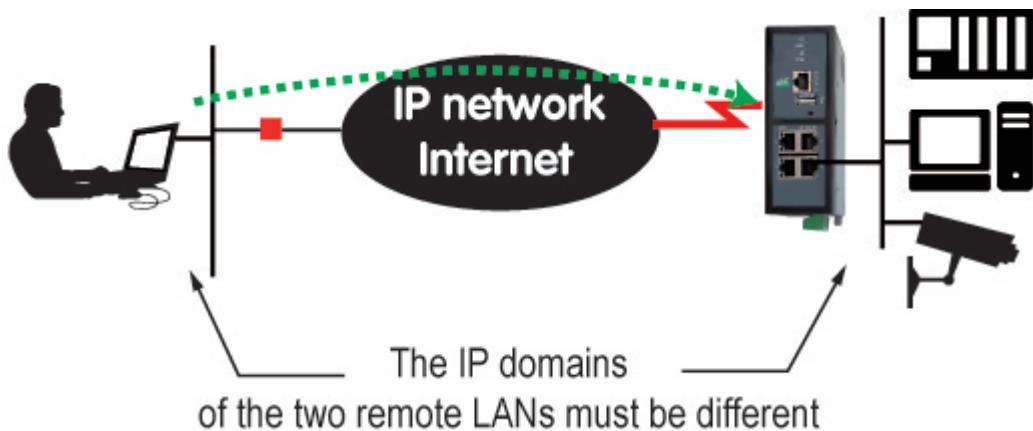
Figure 1. Case 1: Remote users connection
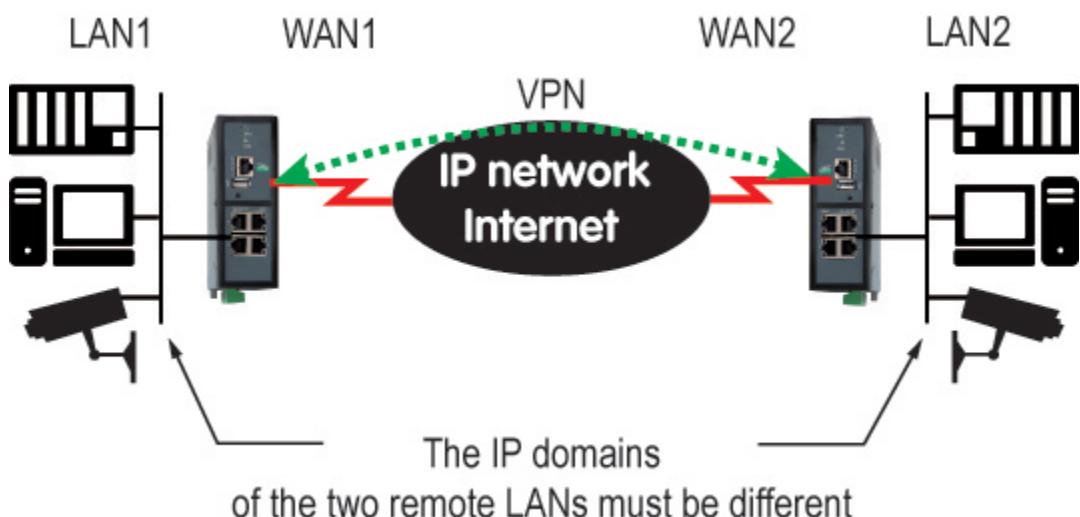
Figure 2. Case 2: VPN set between 2 routers

Advanced parameters

Show advanced parameters	Show advanced parameters
Port 1/2/3/4 configuration	Disable a LAN port or force a certain bit rate for this port, in Half or Full Duplex. `Auto-negotiation` by default
Enable DNS forwarder	The router acts as a DNS Forwarder. `True` by default
Primary DNS server & **Secondary DNS Server**	IP addresses of the DNS Servers to query
Enable proxy ARP	The router acts as a Proxy ARP. `False` by default
Additional IP address & **Additional subnet mask**	Add an IP address to the LAN interface, in addition to the main one
Disable ICMP redirect	ICMP redirect packets are ignored. `False` by default

2.3. Wi-Fi access point

Wi-Fi access point

When the optional Wi-Fi interface is configured as an access point, devices connected to the router via this Wi-Fi network belong to the LAN network.

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

The Wi-Fi module can be configured either like a client or like an access point.

Wi-Fi access point configuration

- Select the *Setup > LAN interface > Wi-Fi access point* menu

SSID	Enter the name assigned to the Wi-Fi network to which the Router has to connect. **IMPORTANT** │ The SSID is case-sensitive.
Pre-shared key	Enter the WPA pre-shared key (at least 8 characters)
Country code	The RF channels allocated to Wi-Fi service are not the same in all countries. See Country code. **WARNING** │ Unauthorized emission on restricted radio frequencies is liable to prosecution in many countries.

Mode	Select one of the possible Wi-Fi modes
	NOTE Selected Wi-Fi mode must be entered in each Wi-Fi client (tablet, …)
Enable IEEE 802.11n (High throughput)	Enable IEEE 802.11n High throughput. `False` by default
Channel	Enter a traffic channel number. It is preferable to select an unused channel at the location where the Router is installed
	TIP Use the Wi-Fi scanner to view channels used by Wi-Fi networks in a location (see Diagnostics Wi-Fi scanner section)
Enable only when the digital input is ON	Enable the Wi-Fi access point only when the digital input status is ON. `False` by default

Country code

AD	Andorra
AE	United Arab Emirates
AL	Albania
AM	Armenia
AR	Argentina
AT	Austria
AU	Australia
AW	Aruba
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BD	Bangladesh
BE	Belgium
BG	Bulgaria
BH	Bahrain
BL	Saint Barthélemy
BN	Brunei Darussalam
BO	Bolivia, Plurinational State of
BR	Brazil
BY	Belarus
BZ	Belize

CA	Canada
CH	Switzerland
CL	Chile
CN	China
CO	Colombia
CR	Costa Rica
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
DZ	Algeria
EC	Ecuador
EE	Estonia
EG	Egypt
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GD	Grenada
GE	Georgia
GL	Greenland
GR	Greece
GT	Guatemala
GU	Guam
HK	Hong Kong
HN	Honduras
HR	Croatia
HT	Haiti
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India

2.3. Wi-Fi access point

IR	Iran, Islamic Republic of
IS	Iceland
IT	Italy
JM	Jamaica
JO	Jordan
JP	Japan
KE	Kenya
KH	Cambodia
KP	Korea, Democratic People's Republic of
KR	Korea, Republic of
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania
LU	Luxembourg
LV	Latvia
MA	Morocco
MC	Monaco
MK	Macedonia, the former Yugoslav Republic of
MO	Macao
MT	Malta
MX	Mexico
MY	Malaysia
NL	Netherlands
NO	Norway
NP	Nepal
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PG	Papua New Guinea
PH	Philippines

PK	Pakistan
PL	Poland
PR	Puerto Rico
PT	Portugal
QA	Qatar
RO	Romania
RS	Serbia
RU	Russian Federation
RW	Rwanda
SA	Saudi Arabia
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SV	El Salvador
SY	Syrian Arab Republic
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad and Tobago
TW	Taiwan, Province of China
UA	Ukraine
US	United States
UY	Uruguay
UZ	Uzbekistan
VE	Venezuela, Bolivarian Republic of
VN	Viet Nam
YE	Yemen
ZA	South Africa
ZW	Zimbabwe

2.4. Device list

- Select the *Setup > LAN interface > Devices list* menu

Identification of the devices connected to the LAN network

The devices defined in the product are supposed to be reachable on the LAN side.

They consist of a name and an IP address to identify them, and are most often used to grant/restrict access to operators (remote users).

Add a device to the list

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

NOTE You can enter an IP address of a device or an IP address of a subnet of devices

Example 3. Device IP address configuration

192.168.8.8 or 192.168.8.8/29 (subnet)

Hostname and Domain name

This menu also permits to modify the hostname of the product. Two fields need to be filled for that:

- **Site Name**: Hostname of your product
- **Domain Name**: Name of the domain your product is supposed to be in

2.5. DHCP server

The Router can behave as a DHCP server for the devices on 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.

NOTE Many Wi-Fi office devices like tablets or smartphones do not support a fixed IP address.

Select the *Setup > LAN interface > DHCP server*

<u>DHCP configuration</u>

IP address pool start & **IP address pool end**	Enter the first and the last IP address reserved to the DHCP server.
Netmask	Netmask of allocated IP addresses
Default gateway	If another router is connected to the LAN network giving access to other networks, and acting as the default gateway for the Etic Telecom Router, enter the address of this router.
Primary DNS server & **Secondary DNS server**	IP addresses of the DNS Servers to query

<u>DHCP MAC-IP bindings</u>

You can bind an IP address to a MAC address, so that a device (identified by its MAC address) is always assigned the same IP address.

Client name	Name to identify client (optional)
Client MAC address	MAC address of the client *Example 4. MAC address* 12:34:56:78:9A:BC
Client IP address	IP address of the client

3. VPN CONNECTIONS

A VPN is a secured communication channel established between devices over a public or private network. VPN uses authentication and encryption techniques to secure the connection and protect it from eavesdropping or data manipulation. This is the best way to interconnect networks over an Internet connection.

This router proposes 2 VPN technologies: IPSec and OpenVPN.

3.1. IPSec

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.

- 15 IPSec connections can be set by one `IPL or RAS router`.
- 128 IPSec connections can be set by one `SIG router`.
- 100 IPSec connections can be set by one `SIG VM 100`.
- 1000 IPSec connections can be set by one `SIG VM 1000`.

IPSec principles

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

An example of the different IP addresses used during the configuration are described by the drawing below.
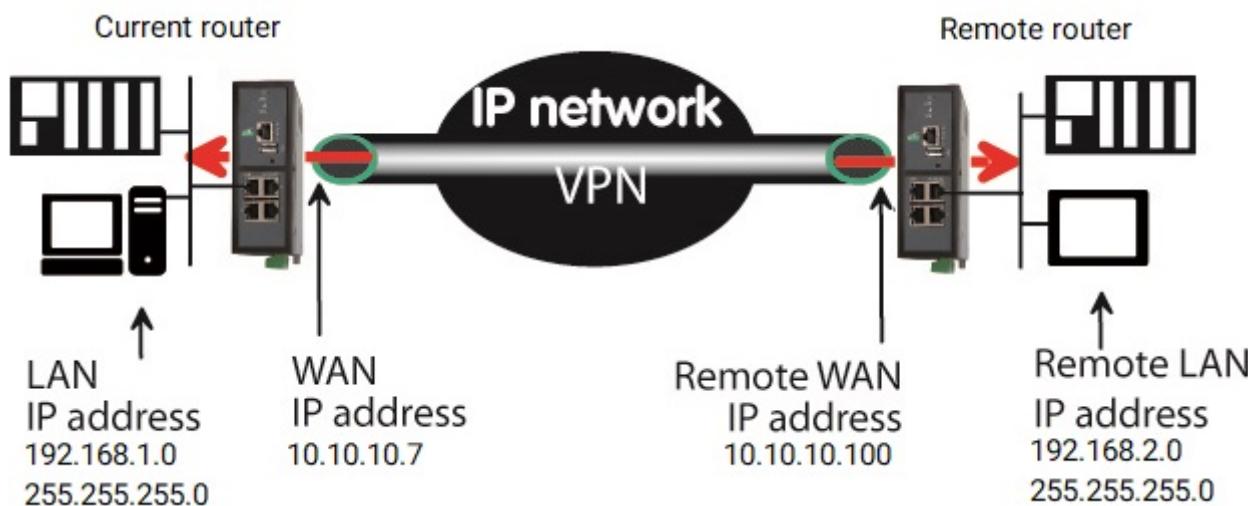
Figure 3. IPSec connection scheme

IPSec VPN connection setup

Select the *Setup > Network > VPN Connections > IPSec* menu

You must enable IPSec parameters to configure connections. The IPSec VPN home page displays information about configured connections.

To add an IPSec VPN connection, click **Add**.

Enabled	You can enable or disable a configured connection
Show advanced parameters	Checkbox if a pre-shared key is used and if intermediate routers translate the source IP address
Name	Assign a unique name to the connection
Authentication by	Pre-shared key or certificate
Connection	Initiator if the current router is supposed to initiate the VPN
Enable "Route-based" mode	`Route-based` if enabled / `Policy-based` if disabled. See **Policy-based VS Route-based** chapter for more explanations.

Policy-based VS Route-based

When using the `Policy-based` IPSec tunnel option, the IPSec daemon establishes a tunnel only for the configured remote networks. When established, all the traffic that match the policy is encrypted and sent to the remote router.

When using the `Route-based` IPSec tunnel option, the traffic sent to the remote router is managed by the networks routes. This option gives more flexibility to manage dynamically which networks are reachable through the tunnel.

For simple network to network tunnel it is easier to use the `Policy-based` mode (`Route-based` mode disabled)

IMPORTANT	In `Route-based` mode: a route to reach the **Remote LAN IP address** must be added in the Static routes menu
TIP	To send all router traffic over the tunnel (VPN as default gateway): 1. Enable the `Route-based` mode 2. Set **Remote LAN IP address** to 0.0.0.0/0 (should be the same as the peer router) 3. Set a static route to reach the peer (**Remote WAN IP address**/32 via the internet gateway or interface) 4. Set a default static route (0.0.0.0/0) via the IPSec VPN

<u>IKE Authentication - Case 1 : Use of a certificate</u>

IMPORTANT	Both certificates used by each participant must be delivered by the same authority

TIP	Check the menu *Setup > Security > Certificate store* to add custom certificates and CRL.

Use the factory certificate	Use the factory certificate
Choose a custom certificate	Use one of your custom certificates
My 'SubjectAlt name'	The 'SubjectAltName' value of the active certificate of the current router NOTE: If the active certificate is the factory certificate, that field is the email field
Remote 'SubjectAlt name'	The 'SubjectAltName' value of the active certificate of the remote router NOTE: If the active certificate is the factory certificate, that field is the email field
Certificate revocation policy	If no information about incoming certificate revocation: 'relaxed' will accept it, 'strict' will refuse it.

<u>IKE Authentication - Case 2 : Use of a pre-shared key</u>

Use a pre-shared key for authentication; it must be the same on the responder and initiator side.

These identifiers make possible to set a pre-shared 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.

Key value	Value of the key, it must be the same on the responder and initiator side.
Local IKE ID (Advanced parameters)	Used to identify the current router
Peer IKE ID (Advanced parameters)	Used to identify the remote router

<u>Network section</u>

Local LAN IP address (Advanced parameters)	IP address of the local LAN network. If empty, it's the LAN of the Router *Example 5. On IPSec connection scheme* 192.168.1.0
Local LAN netmask (Advanced parameters)	Netmask of the local LAN network. If empty, it's the LAN of the Router *Example 6. On IPSec connection scheme* 255.255.255.0
Remote LAN IP address	IP address of the remote LAN network *Example 7. On IPSec connection scheme* 192.168.2.0
Remote LAN netmask	Netmask of the remote LAN network *Example 8. On IPSec connection scheme* 255.255.255.0
Remote WAN IP address	IP address of the remote router towards which the VPN must be set *Example 9. On IPSec connection scheme* 10.10.10.100

IKE Phase 1 section

IKE phase 1 performs mutual authentication between the two parties with the end result of having shared secret keys. The same value must be selected for the two routers.

Use IKEv1 (Advanced parameters)	Use IKE version 1. This version should only be used for compatibility with devices that don't have IKEv2.
Exchange Mode (Advanced parameters)	Main or Aggressive. Aggressive mode should only be used for compatibility with devices that uses it. The aggressive mode is not considered as secure anymore.

Encryption algorithm	Algorithm used to encrypt data. Recommended value : Auto
	Example 10. Possible values
	Blowfish, AES 256 GCM, AES 128 GCM, AES 256 CBC, AES 192 CBC, AES 128 CBC, 3DES, Auto
Authentication algorithm	Algorithm for authentication, Recommended value : Auto
	Example 11. Possible values
	MD5, SHA1, SHA-256, SHA-384, SHA-512, Auto
DH group (Advanced parameters)	Diffie-Hellman group
Life time (Advanced parameters)	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 :	IPSec transport protocol. ESP ensures routers authentication and data encryption.
Encryption algorithm	Recommended value : Auto
Authentication algorithm	Recommended value : Auto
PFS	With PFS disabled, initial keying material is created during the key exchange in phase-1 of the IKE negotiation. In phase-2 of the IKE negotiation, encryption and authentication session keys will be extracted from this initial keying material. By using PFS, Perfect Forwarding Secrecy, completely new keying material will always be created upon re-key. Should one key be compromised, no other key can be derived using that information
DH group (Advanced parameters & PFS enabled)	Diffie-Hellman group
Life time (Advanced parameters)	Phase 2 key lifetime

DPD section

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

DPD Keep-alive period	Amount of time between two of these requests
Connection death time-out	Maximum amount of time a VPN connection will stay established if no traffic or no DPD keep-alive message are received from the remote point
Attach VPN to this WAN	Attach a VPN to a WAN so that the connection sets up only through this WAN. The option `All` may not work with IKEv1.
Start on event	The VPN starts on a specific event. If disabled, the VPN is established at power-up.
Start only when	Event that will start the VPN connection *Example 12. Possible values* Cellular WAN up, Cellular WAN down, Ethernet WAN up, Ethernet WAN down, TOR input ON, TOR input OFF, No VPN connected

3.2. OpenVPN

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.

- 15 in + 15 out OpenVPN connections + 2 servers can be set by one `IPL or RAS router`.
- 128 in + 128 out OpenVPN connections + 4 servers can be set by one `SIG router`.
- 100 in + 100 out OpenVPN connections + 4 servers can be set by one `SIG VM 100`.
- 1000 in + 1000 out OpenVPN connections + 4 servers can be set by one `SIG VM 1000`.

To configure OpenVPN connections go to menu *Setup > Network > OpenVPN*

OpenVPN principles

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

The router which receives the connection is called the VPN server. It configures ingoing connections.

The router can do both VPN client and VPN server at the same time.

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

Example 13. OpenVPN connection
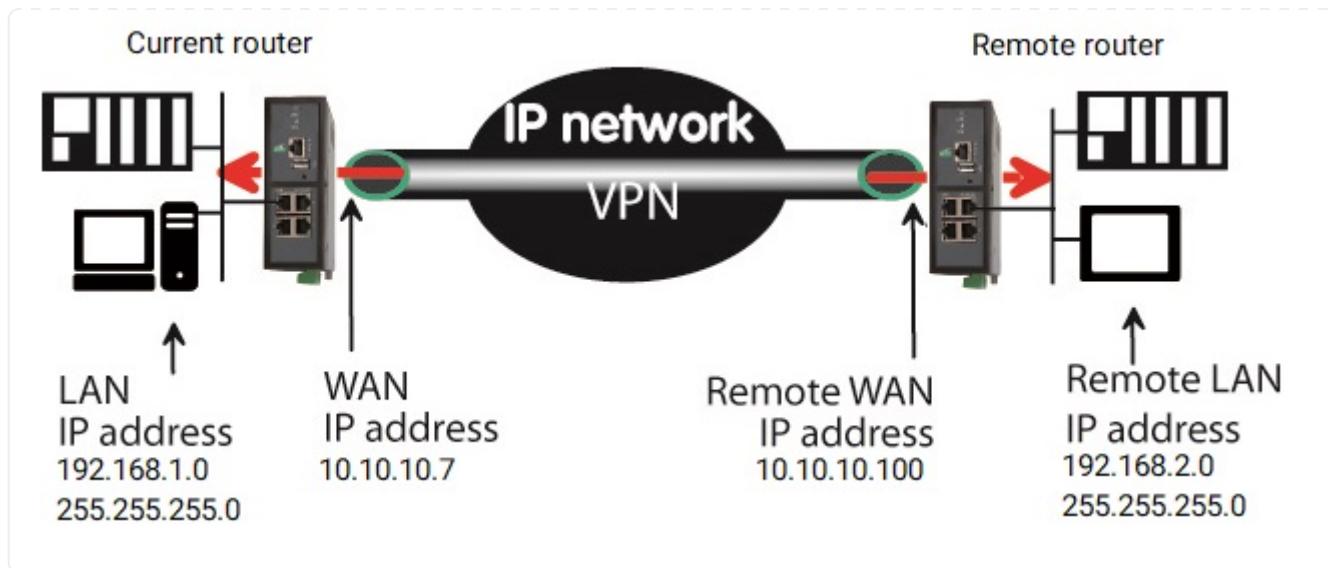
OpenVPN server

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

1. Configuration of the parameters of the OpenVPN servers
2. Configuration of the ingoing connections

OpenVPN client

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

Server

Select the **Add** button located just below the VPN server table

IMPORTANT	Both certificates used by each participant must be delivered by the same authority

Check the menu *Setup > Security > Certificate store* to add custom certificates and CRL.

Active	Enable or disable a connection
Name	Unique name of the connection
Port number	Port number of the transport protocol
	<table><tr><td>**CAUTION**</td><td>The port number value must be different from the one used by remote access servers</td></tr></table>

Protocol	UDP or TCP
Use the factory certificate	Use the factory certificate
Choose a custom certificate	Use one of your custom certificates
VPN network address & **VPN network netmask**	The OpenVPN server router assigns automatically an IP address to the VPN client router. Leave the default values 172.16.0.0 and 255.255.0.0 **CAUTION** That VPN IP address must not be confused with the WAN interface IP address.
Connection death time-out	Defines the period of the control messages 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. 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. **CAUTION** The value 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	Amount of time the server will wait for the response to the keep-alive control message before repeating it.
Encryption	Algorithm used to encrypt data *Example 14. Possible values* Blowfish, AES 256 GCM, AES 128 GCM, AES 256 CBC, AES 192 CBC, AES 128 CBC, 3DES, Auto
Authentication	Algorithm for authentication *Example 15. Possible values* MD5, SHA1, SHA-256, SHA-384, SHA-512
Diffie Hellman	Diffie Hellman group
Use TLSv1 protocol	Use TLS version 1. This version should only be used for compatibility with old devices.
Server priority	Metric used for all pushed routes
Push local route to VPN clients	If checked, the server broadcasts to the clients the route to the IP domain of its local network

Push static routes to VPN clients	If checked, the server broadcasts to the clients the static routes which have been configured in the VPN server
Push client routes	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. They must be programmed in both routers. 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. • The second one is to select the **Push clients routes** option. The VPN server broadcast to all the VPN clients the route to each of them. This way, each device of the network can exchange data with each other device. Programming static routes is not necessary.
First & second specific route to push	These parameters allow to broadcast specific routes from the VPN server to the clients.
Show advanced parameters	Show advanced parameters
Enable tls-auth	Enable tls-auth
tls-auth key	Key value for tls-auth
Enable tls-crypt	Enable tls-crypt
tls-crypt key	Key value for tls-crypt
Disable compression	Disable compression

<u>Outgoing connection</u>

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

• Select the **Add** button located just below the Outgoing connection table.

IMPORTANT	Both certificates used by each participant must be delivered by the same authority

Check the menu *Setup > Security > Certificate store* to add custom certificates and CRL.

Active	Enable or disable a connection
Name	Unique name of the connection
Login	Login configured on both sides of the connection
Password	Password configured on both sides of the connection

VPN server IP address	Public IP address or a domain name or a DynDNS or NoIP address. A list of addresses separated by character ';' can be used. If the port is not defined, the port entered in **Port number** field will be used *Example 16. List of addresses* 10.1.35.210;10.1.35.210:2194;10.6.66.102;10.6.66.102:1200
Backup VPN server IP address	Backup IP address if the main fails. Like in **VPN server IP address**, a list can be used
Port number	Port number of the transport protocol **CAUTION** The port number value must be different from the one used by remote access servers
Protocol	UDP or TCP
Use the factory certificate	Use the factory certificate
Choose a custom certificate	Use one of your custom certificates
Encryption	Algorithm used to encrypt data *Example 17. Possible values* Blowfish, AES 256 GCM, AES 128 GCM, AES 256 CBC, AES 192 CBC, AES 128 CBC, 3DES, Auto
Authentication	Algorithm for authentication *Example 18. Possible values* MD5, SHA1, SHA-256, SHA-384, SHA-512
Attach VPN to a specific interface	Attach a VPN to a WAN so that the connection sets up only through this WAN.
Use TLSv1	Use TLS version 1. This version should only be used for compatibility with old devices.
Start on event	The VPN starts on a specific event. If disabled, the VPN is established at power-up.
Start only when	Event that will start the VPN connection. *Example 19. Possible values* Cellular WAN up, Cellular WAN down, Ethernet WAN up, Ethernet WAN down, TOR input ON, TOR input OFF, No VPN connected

Send alarm on connection/disconnection	Send an alarm at each connection/disconnection
Show advanced parameters	Show advanced parameters
Enable tls-auth	Enable tls-auth
tls-auth key	Key value for tls-auth
Enable tls-crypt	Enable tls-crypt
tls-crypt key	Key value for tls-crypt
Disable compression	Disable compression

Getting through a proxy

If your router is behind a proxy on WAN Ethernet, you must attach the VPN to the `Ethernet WAN` interface.

Then configure the proxy settings in the page *Setup > WAN Interfaces > Ethernet* (see WAN Ethernet section).

Ingoing connection

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

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

Active	Enable or disable a connection
Name	Unique name of the connection
Login	Login configured on both sides of the connection
Password	Password configured on both sides of the connection
Remote LAN IP address	IP address of the remote LAN *Example 20. IP address* 192.168.2.0
Remote LAN netmask parameters	Netmask of the remote LAN *Example 21. Netmask* 255.255.255.0
Common name	'Common Name' of the active certificate of the remote router. **NOTE** You can retrieve the common name of the certificate in the Certificate store.

4. REMOTE ACCESS

Providing a secure remote access service requires three steps:

1. The remote connection setup

2. The operator list setup

3. The access rights definition

4.1. Advantages of a remote access connection

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

Remote users identification

The login, password and optionally the certificate of the remote user are checked when establishing the connection

Selective access rights

Individual access rights can be assigned to each remote user. The user can only access authorized devices of the network.

Transparent connection

Once the remote connection has been launched, the remote user receives automatically an IP address of the network.

Data encryption

Data is encrypted from end to end.

Figure 4. Remote access data encryption

PC, Tablet, smartphone

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

4.2. Remote access connections types

Four types of remote access connections can be configured. They can all be active at the same time.

	Remote users identification	Encryption
OpenVPN	Login/Password + Optionally a certificate	Yes
PPTP	Login/Password	Yes
L2TP/IPSec	Login/Password + Pre-shared Key or certificate	Yes
HTTPS	Login/Password	Yes

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/Password).

4.3. Remote user OpenVPN

- Select *Setup > Remote access > Remote access servers* menu

On the remote PC side, one can use a standard OpenVPN client or, if the PC is running Windows, the M2Me_Client software which is simple to install, configure and use.

Setup OpenVPN connection

Select the **Enable OpenVPN (OpenVPN)** checkbox

Port number	Port number used
Protocol	UDP or TCP **CAUTION** Make sure the combination Protocol + Port number is used only by this VPN. It must be different from the ones intended for PCs.
Encryption Algorithm	Algorithm used to encrypt data
Message digest algorithm	Algorithm for authentication
Users authentication	**Login/password** or **Login/password & certificate** In that case, the certificate of the remote PC must be entered in the Operator List menu.
Use the factory certificate	Use the factory certificate
Choose a custom certificate	Use one of your custom certificates

4.4. Smartphones OpenVPN

- Select *Setup > Remote access > Remote access servers* menu

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

Setup OpenVPN connection for smartphone

Select the **Enable OpenVPN (OpenVPN) for Smartphones** checkbox

Port number	Port number used
Protocol	UDP or TCP **CAUTION** Make sure the combination Protocol + Port number is used only by this VPN. It must be different from the ones intended for PCs.
Encryption Algorithm	Algorithm used to encrypt data
Message digest algorithm	Algorithm for authentication
Users authentication	**Login/password** or **Login/password & certificate** In that case, the certificate of the remote PC must be entered in the Operator List menu.
Use the factory certificate	Use the factory certificate

Choose a custom certificate	Use one of your custom certificates

4.5. PPTP and L2TP/IPSec

- Select *Setup > Remote access > Remote access servers* menu

PPTP connection

WARNING	Using PPTP is not recommended anymore due to fundamental security issues on the protocol.

Select the **Enable PPTP** checkbox

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

L2TP/IPSec connection

Select the **Enable L2TP/IPSec** checkbox

Cipher Algorithm	Algorithm used to encrypt data
Message digest algorithm	Algorithm for authentication
Authentication method	`Pre-shared key` or `Client certificate`, in that case, the certificate of the remote PC must be entered in the Operator List menu.

5. M2ME_CONNECT

All RAS routers are concerned by this section. It also applies to all other routers, only if the M2Me option has been enabled.

To provide access to a machine for remote users through the M2Me_Connect service, it is necessary to carry-out three steps:

1. Carry-out the M2Me connection setup
2. Register an operator (at least) in the menu *Setup > Remote access > Operator list*
3. Assign access rights for the operators

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

5.1. Setup M2Me connection

Select the *Setup > Remote access > M2Me_Connect* menu.

TCP & **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:

- **Proxy type** of the server (HTTP, SOCKS5)
- Proxy **IP address** and **Port number**
- Type of **Authentication** (None, Basic, NTLM) if the proxy is `HTTP`

Once the M2Me connection has started, the M2Me LED flashes.

| **CAUTION** | The <u>Product key</u> of the router is required by the M2Me software of the remote PC. Don't forget to copy it from the menu *About*. |

6. IP ROUTING

6.1. Routing function

Routing allows IP packets to be forwarded from one network to another. The destination of the packets and the **routing** table of the router make it possible to determine to which network it must be forwarded, in order to reach the final destination.

Let's see an example where routing is used:
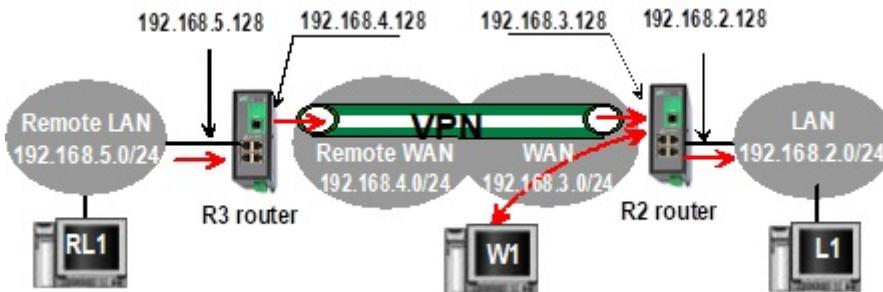
Figure 5. Basic routing

Once an IP address has been assigned to the R2 router on the LAN interface and another one on the WAN interface, the Router is ready to route packets:

- 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

| NOTE | • Firewall rules must be set to authorize WAN to LAN transfer |
| | • A default gateway address must be entered in each device of the different networks |

6.2. Static routes

A router dynamically learns the routes of networks connected directly to it. If you want your router to know how to forward a packet for a destination that isn't directly connected to it, you might need **Static routes**.

A static route consists of describing a destination network (IP address and network mask) and the IP address of the neighboring router through which IP packets intended for a destination must pass.

Example use case

Here is an example to illustrate the use of static routes:
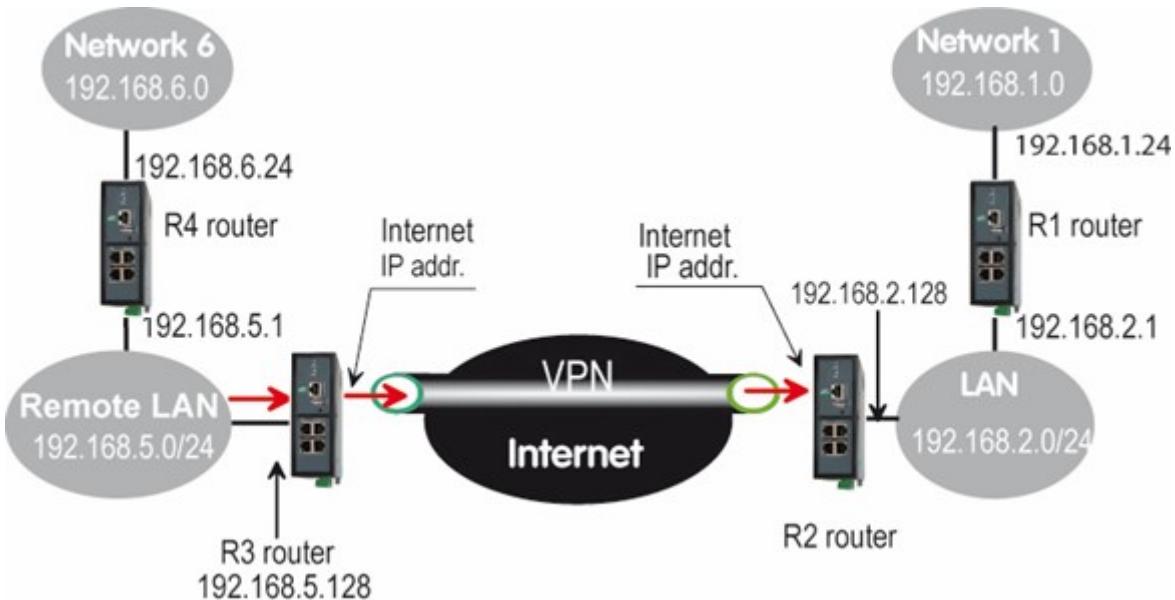
Figure 6. Static routes example

In this example, the router R2 is able to route packets coming from the `LAN` network to the `WAN` network of R2, or to the `Remote LAN` network, without any static routes. These routes have been automatically created by the router respectively when the WAN IP address has been entered and when the VPN has been configured.

But the router R2 is not able to route packets between a device belonging to the `LAN` network and a device connected to `Network 6`. In that case, it is necessary to manually enter the route to that `Network 6`; this route is called a static route.

Table 1. R2 static routes table, in order to be able to route to Network 1 and 6

Active	Route name	IP address	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

The same kind of static routes must be added in the other routers so that they know how to forward packets.

Static routes configuration

Select the *Setup > Network > Routing > Static routes* menu

This menu shows you a board summarizing static routes of the product, and if they are active or not.

Destination network

Route general parameters

Active	Enable or disable this route
Route name	Name for you to describe the usefulness of the route

Priority	Priority of the route (`1`:High - `255`:Low)
IP address & **Netmask**	Destination network IP address and netmask

Path

Path through which the IP packets intended for a network must pass.

IMPORTANT	Choose only one of these options and leave the others blank when creating a route

Gateway IP address	IP address of the gateway
Interface	Physical interface
OpenVPN ingoing node	OpenVPN node (see Ingoing connection)
OpenVPN outgoing node	OpenVPN node (see Outgoing connection)
IPSec node	IPSec node (see IPSec)

6.3. 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.

Setup RIP

Select the *Setup > Network > Routing > RIP* menu.
Select the **Enable RIP on LAN interface** and the **Enable RIP on WAN interface** options.

7. ADDRESSES SUBSTITUTION

Each frames comming in or out of the router can be processed. The NAT functions permit to work on the addresses of the IP frames to reach equipements that are placed behind the router.

7.1. 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 for Ethernet for example. Select the *Setup > WAN Interfaces > Ethernet* menu. Then click on **Enable address translation** checkbox.

7.2. Port forwarding

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 22. Port forwarding 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.
>
>
>
> *Figure 7. Port forwarding example*
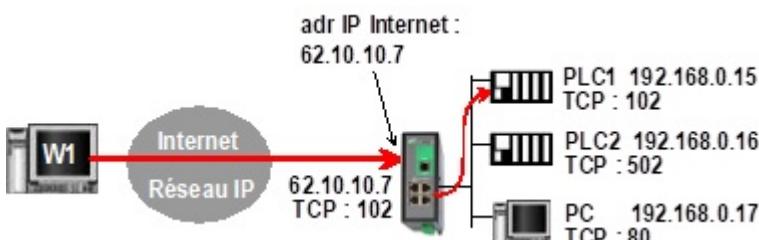
Table 2. Port forwarding example configuration

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

Setup port forwarding

To configure a port forwarding rule:

1. Select *Setup > Network > Routing > Port forwarding* menu

2. Click the **Add** button,

3. Enter the characteristics of the frames which must be forwarded:

   - **Source IP address**

   - **Port number** (destination)

4. Enter the characteristics of the device to which that IP frames must be forwarded:

   - **Destination IP address**

   - **Port number** (destination)

7.3. Advanced NAT

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	WAN — DNAT — Router — FIREWALL — SNAT ➤ LAN

Direction	
LAN to WAN	WAN ← SNAT — FIREWALL — Router — DNAT — LAN
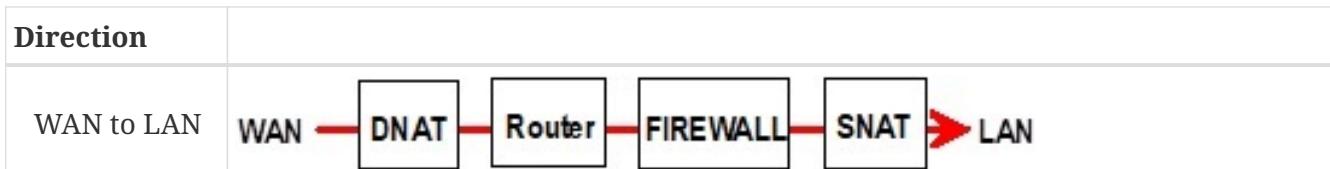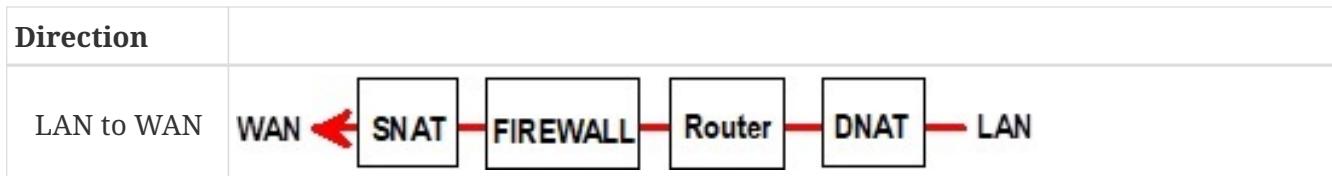
Setup

To set the advanced address translation functions, select the *Setup > Network > Advanced NAT* menu.

Create a DNAT rule

1. Click **Add** under the **DNAT rules** table.

2. Select **Active** to enable the rule.

3. 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**

4. Enter the new destination port number and IP address.

Create a SNAT rule

1. Click **Add** under the **SNAT rules** table.

2. Select **Active** to enable the rule.

3. Enter the characteristics of the IP frames which must be modified by the SNAT rule:

   ◦ **Source IP address** & **Destination IP address** and **Protocol** (TCP, UDP)

   ◦ **Source port** & **Destination port** (fields depending of the selected protocol)

4. Enter the **New source IP address**.

8. AUTHENTICATION DELEGATION

8.1. Delegated authentication

Etic Telecom provides a functionality allowing your router to retrieve users from authentication servers such as Active Directory, FreeRADIUS, or OpenLDAP.

In Etic Telecom routers, users are divided in 2 categories: `Administrators`, who are configuring parameters of the router, and `Operators`, who are reaching the router via M2Me. So there are 2 sections in the configuration menu for delegated authentication, one for each category.

This chapter describes the configuration to be carried out to use the users of your server on the router, with the correct rights and functions for each of them.

In each section, you have the possibility to cache credentials so that if your server is down, users can still log in for a certain time. Cache is cleared at reboot and shutdown of the router.

NOTE	If delegated authentication is activated for administrators, only local users with Super Administrator role have SSH access to the router. Administrators from your delegated server don't.

Case of local Super Administrators in delegated mode

Local users with Super Administrator role can still connect to the router with their local account.

If you wish to deny local Super Administrator to connect the router, you can disable the user account linked with the Super Administrator (see Users section).

8.2. Configuring RADIUS authentication

Go to the view *Setup > Security > Authentication*. The parameter **Authentication type** must be set to `RADIUS`. Then fill the parameters for your RADIUS server.

Server IP Address or Hostname	IP address or Hostname of your server. **CAUTION** — Make sure the router is able to do DNS resolution if you use hostname.
Backup server IP Address or Hostname	Backup address or hostname, in case the first one is not available. (Optional)
Authentication port	Listening port of your RADIUS server for authentication. Default port is 1812.
Shared secret	Shared secret of RADIUS server.

Configure access rights for Administrators

Administrators authenticated through RADIUS have configurable access rights, Go to view *Setup > Remote access > Operator groups*. You will find a board to add/delete/edit groups.

If you want to grant access to administrators to the router you will have to create one group called `RADIUS_ETIC_TELECOM`. This group name is designed specifically for administrators authenticating through RADIUS and by adding/editing this group, you can choose the role of radius administrators.

Configure access rights for Operators

Operators authenticated through RADIUS have configurable access rights, Go to view *Setup > Remote access > Operator groups*. You will find a board to add/delete/edit groups.

If you want to grant access to operators to the router you will have to create one group called `RADIUS_ETIC_TELECOM`. This group name is designed specifically for operators authenticating through RADIUS and by adding/editing this group, you can choose the access rights.

8.3. Configuring LDAP authentication

Go to the view *Setup > Security > Authentication*. The parameter **Authentication type** must be set to `LDAP`. Then fill the parameters that will be used for requests to your LDAP server.

| TIP | You can check the LDAP authentication logs in the `Main` log |

Server IP Address or Hostname	IP address or Hostname of your server.
	CAUTION • Make sure the router is able to do DNS resolution if you use hostname. • To use LDAPS, it may be necessary to fill in the hostname instead of the IP address. *Example 23. Server hostname* myserver.mycompany.com
Backup server IP Address or Hostname	Backup address or hostname, in case the first one is not available. (Optional)
Server port	Listening port of your LDAP server. Default port is 389.

Privileged account DN	Full distinguished name of the LDAP account used to perform requests. (Read-only rights to the necessary branches are sufficient) *Example 24. Privileged account DN* cn=admin, dc=mycompany,dc=com
Privileged account password	Password of the privileged account.
Server type	Either Active Directory or other (OpenLDAP, etc…)
Root domain (Base DN) for user search	Full distinguished name of the LDAP branch used to store users. (User leaves must be directly under) *Example 25. Root domain for user search* ou=users,dc=mycompany,dc=com
Root domain (Base DN) for group search	Full distinguished name of the LDAP branch used to store groups. (Group leaves must be directly under) *Example 26. Root domain for group search* ou=groups,dc=mycompany,dc=com
Attribute used to identify users	LDAP attribute `used in DN` (distinguished names) to identify users. *Example 27. Attribute used to identify users* cn
Active Directory domain name	Domain name (used only if server type is Active Directory) *Example 28. Domain name* mycompany.com
LDAP over SSL	Use LDAPS protocol or not **WARNING** LDAP without SSL means your passwords are visible on the network during authentication
Certificate type	Client certificate or CA certificate depending on whether the LDAP server needs mutual authentication or if only the router should authenticate it
CA Certificate for LDAPS	Choose a certificate on the list to use it

Certificate for LDAPS	Choose a certificate on the list to use it

Rights of users authenticating through LDAP are defined by their membership in groups.

IMPORTANT	A user that exists on the server, but has no groups giving him rights, will not be granted access to the router.

Some attributes are checked to know the user membership in groups. On the LDAP user object, the attribute checked is `memberOf`. On the LDAP group object, the attributes checked are `member`, `memberUid` and `uniqueMember`.

Configure access rights for Operators

Go to view *Setup > Remote access > Operator groups*. You will find a board to add/delete/edit groups. For each group, you can choose the access rights.

Configure functions for Administrators

Go to view *Setup > Security > Administrator groups*. You will find a board to add/delete/edit groups. You can add the same group multiple times if this group has multiple roles.

IMPORTANT	The parameter **Group name** is CASE-SENSITIVE and MUST match with the attribute `CN` of the group on the server.

8.4. Difference between Active Directory and Others

Active Directory

Logins of users who authenticate through Active Directory are their `userPrincipalName`.
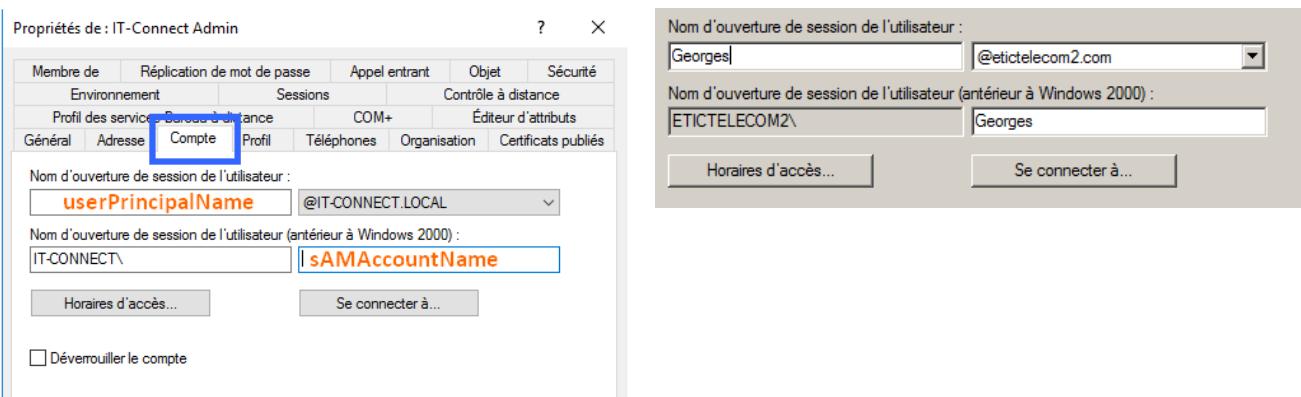
Figure 8. Active Directory server configuration

Server type	Active Directory ∨
Root domain (Base DN) for user search	cn=Users,dc=etictelecom2,dc
Active Directory domain name	etictelecom2.com

Figure 9. Active Directory router configuration
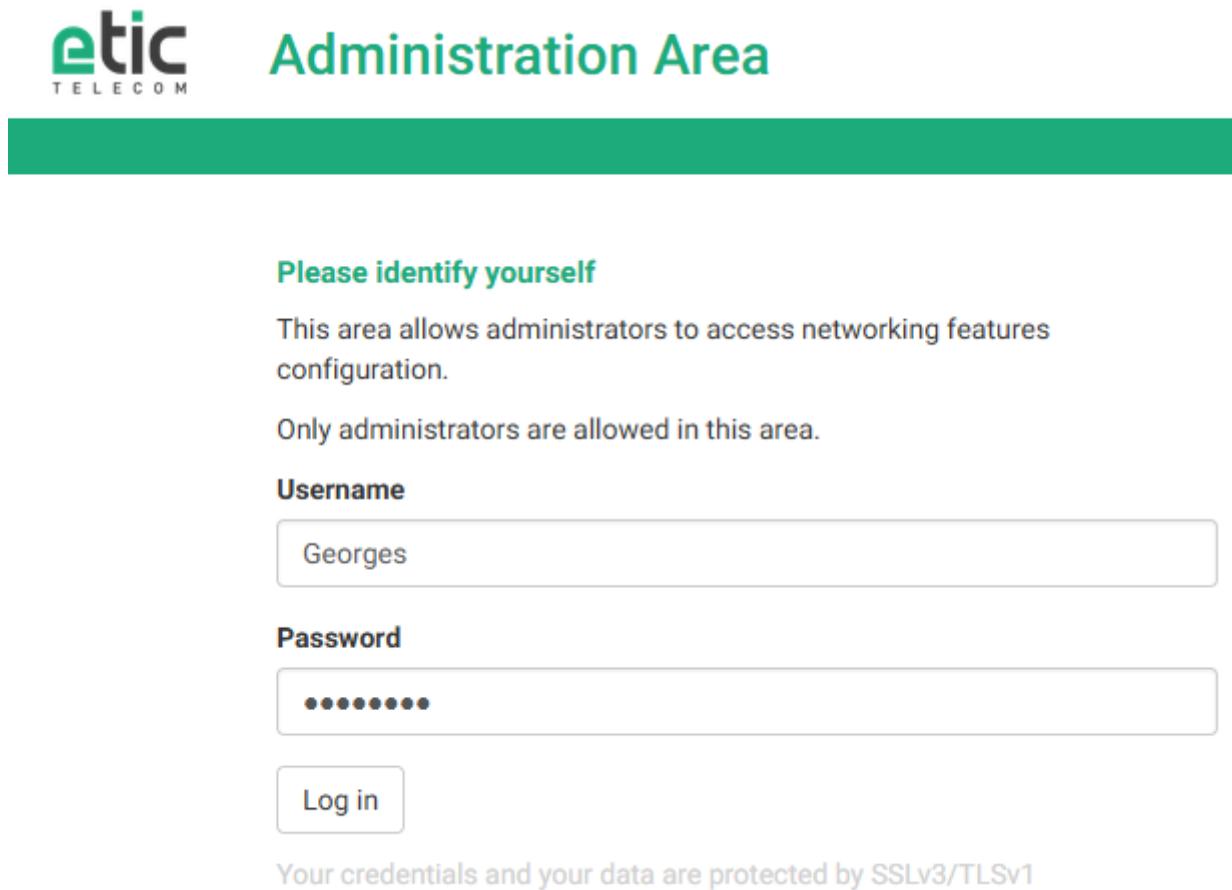
Figure 10. Web login with Active Directory

Others

Logins of users who authenticate through other types of servers, such as OpenLDAP, are the values of the attribute you defined in the configuration of the router, for example, the values of the attribute cn.
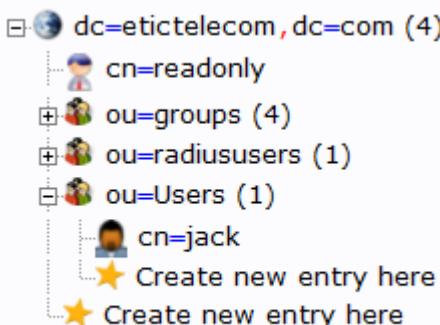
Figure 11. OpenLDAP server configuration

Server type	Other ▾
Root domain (Base DN) for user search	ou=Users,dc=etictelecom,dc=
Root domain (Base DN) for group search	ou=groups,dc=etictelecom,dc
Attribute used to identify users	cn

Figure 12. OpenLDAP router configuration
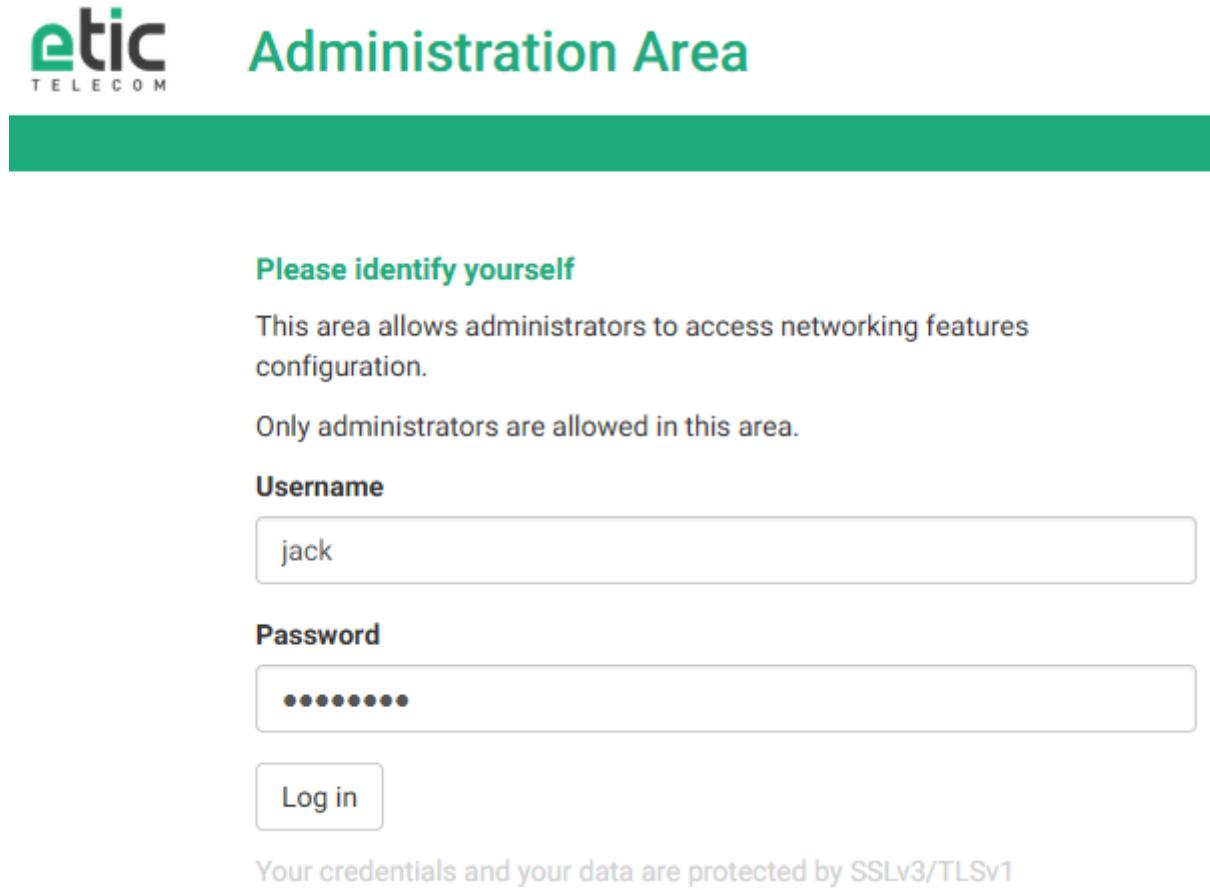
Administration Area

Please identify yourself

This area allows administrators to access networking features configuration.

Only administrators are allowed in this area.

Username

jack

Password

••••••••

Log in

Your credentials and your data are protected by SSLv3/TLSv1

Figure 13. Web login with OpenLDAP

9. CERTIFICATE STORE

9.1. Certificate store

Etic Telecom provides a certificate store, allowing you to manage client certificates, certificate authorities certificates, private keys and certificate revocation lists. Some programs that use information from this certificate store are OpenVPN, IPsec, LDAP, OPCUA, Syslog, FTP, MQTT, …

This chapter describes how to configure certificates and use them in the routers.

NOTE	The CA bundle, certificates, private keys and CRL are **never** stored in configuration files.

Factory settings

The certificate store always contains the certificates `factory_certificate_ca.crt` and `factory_certificate.crt` along with the private key `factory_certificate.key`, these are all created by Etic Telecom to identify your router on services offered by Etic Telecom. They can't be deleted.

9.2. Certificate Store view

The graphical user interface to configure this certificate store is on the view *Setup > Security > Certificate store*. This view is split into 4 boards: CA Certificates, Certificates, Private keys and CRL.

Adding/Deleting

On this webpage, there are buttons to add/delete x509 certificates, private keys and CRL. When adding one of them in the certificate store, you must specify a name for it, this name will then be used in other views to refer to it.

	Names given to certificates / private keys / CRL must follow some rules:
CAUTION	1. Be unique among its category
	2. Be suitable for a file name
	3. Not end with `.rsa`, `.info` or `.pub` for private keys
	4. Not be used by certificates, CA certificates and keys for p12 files

Adding can be done by importing the file in PEM format.

You also have the possibility to add the content of a p12 file by clicking on the **Add** button of the certificate board. The import format must be set to PKCS12 and you can choose your p12 file with its password.

Private keys

NOTE	Importing the PEM format of encrypted private keys isn't supported by the router.

Don't import private keys which size is too small for OpenSSL, most of the router features won't accept it for security reasons.

For private keys you can also generate it, the type of key you can generate is RSA length 2048 or ECDSA Prime256v1.

Certificate signing request

You can create a certificate signing request for a specific key, you can select the key and click on **Make a CSR**, it will show you the PEM text corresponding to it. It permits to sign a certificate for a key with your custom Certification Authority.

Certificate and CRL details

Each board shows you details about certificates, like the Subject Common Name, the Issuer Common Name, and the expiration date of the certificate. For client certificates it also shows you the fact that the certificate is linked with a private key or not.

There is also a **Show** button for certificates to show details for each certificate.

For each CRL, the GUI shows you the Issuer Common Name, the last update of the CRL and the next update of the CRL.

9.3. Usage of certificates

Some features require certificates to work. There will then be, in the interface of this functionality, a parameter which will allow you to choose the certificate to use.

If this functionality needs a mutual authentication, it will be necessary to choose a client certificate, if it is enough to authenticate the server there is the possibility of choosing only the CA certificate.

For client certificates, you will need to have a certificate with a private key and the CA certificate linked to it.

TIP	If a CA certificate isn't self-signed, you can concatenate every PEM from the intermediate CA to the root CA when importing the CA certificate. This way, the whole CA chain is available when using this certificate.

TIP	To troubleshoot, you can verify on the certificate store interface if your client certificate has a link to a private key, and if the client certificate issuer is in the list of CA certificates.

Example 29. LDAPS needs client certificate, CA certificate and private key.

Figure 14. Certificate Store configuration

Figure 15. LDAP certificate configuration

Certificate revocation lists

OpenVPN and IPsec VPN (StrongSwan) can check if an end entity certificate has been revoked with CRL files. For OpenVPN, we advise you to use one CRL for each CA.

CAUTION	Your CRL may need to have x509v3 extensions, like the subject key identifier, to work properly.

9.4. CA bundle

For data logger utilities and SMTP server, you must specify CA certificates that you trust, you can specify one of your custom certificates or choose the `Bundle of trusted CA Certificates`.

This bundle is a file containing a list of trusted CA certificates of big companies. It has been created by the Linux package `ca-certificates`; this package includes certificate authorities issued with Mozilla browsers to allow SSL-based applications to verify the authenticity of SSL connections.

Here is the list of all the trusted CA certificates included in this file:

1. ACCVRAIZ1.crt

2. AC_RAIZ_FNMT-RCM.crt

3. Actalis_Authentication_Root_CA.crt

4. AffirmTrust_Commercial.crt

5. AffirmTrust_Networking.crt

6. AffirmTrust_Premium.crt

7. AffirmTrust_Premium_ECC.crt

8. Amazon_Root_CA_1.crt

9. Amazon_Root_CA_2.crt

10. Amazon_Root_CA_3.crt

11. Amazon_Root_CA_4.crt

12. Atos_TrustedRoot_2011.crt

13. Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068.crt

14. Baltimore_CyberTrust_Root.crt

15. Buypass_Class_2_Root_CA.crt

16. Buypass_Class_3_Root_CA.crt

17. CA_Disig_Root_R2.crt

18. CFCA_EV_ROOT.crt

19. COMODO_Certification_Authority.crt

20. COMODO_ECC_Certification_Authority.crt

21. COMODO_RSA_Certification_Authority.crt

22. Certigna.crt

23. Certum_Trusted_Network_CA.crt

24. Certum_Trusted_Network_CA_2.crt

25. Comodo_AAA_Services_root.crt

26. Cybertrust_Global_Root.crt

27. D-TRUST_Root_Class_3_CA_2_2009.crt

28. D-TRUST_Root_Class_3_CA_2_EV_2009.crt

29. DigiCert_Assured_ID_Root_CA.crt

30. DigiCert_Assured_ID_Root_G2.crt

31. DigiCert_Assured_ID_Root_G3.crt

32. DigiCert_Global_Root_CA.crt

33. DigiCert_Global_Root_G2.crt

34. DigiCert_Global_Root_G3.crt

35. DigiCert_High_Assurance_EV_Root_CA.crt

36. DigiCert_Trusted_Root_G4.crt

37. E-Tugra_Certification_Authority.crt

38. EC-ACC.crt

39. Entrust.net_Premium_2048_Secure_Server_CA.crt

40. Entrust_Root_Certification_Authority.crt

41. Entrust_Root_Certification_Authority_-_EC1.crt

42. Entrust_Root_Certification_Authority_-_G2.crt

43. GDCA_TrustAUTH_R5_ROOT.crt

44. GlobalSign_ECC_Root_CA_-_R4.crt

45. GlobalSign_ECC_Root_CA_-_R5.crt

46. GlobalSign_Root_CA.crt

47. GlobalSign_Root_CA_-_R2.crt

48. GlobalSign_Root_CA_-_R3.crt

49. GlobalSign_Root_CA_-_R6.crt

50. Go_Daddy_Class_2_CA.crt

51. Go_Daddy_Root_Certificate_Authority_-_G2.crt

52. Hellenic_Academic_and_Research_Institutions_ECC_RootCA_2015.crt

53. Hellenic_Academic_and_Research_Institutions_RootCA_2011.crt

54. Hellenic_Academic_and_Research_Institutions_RootCA_2015.crt

55. Hongkong_Post_Root_CA_1.crt

56. ISRG_Root_X1.crt

57. IdenTrust_Commercial_Root_CA_1.crt

58. IdenTrust_Public_Sector_Root_CA_1.crt

59. Izenpe.com.crt

60. Microsec_e-Szigno_Root_CA_2009.crt

61. NetLock_Arany_=Class_Gold=_Főtanúsítvány.crt

62. Network_Solutions_Certificate_Authority.crt

63. OISTE_WISeKey_Global_Root_GB_CA.crt

64. OISTE_WISeKey_Global_Root_GC_CA.crt

65. QuoVadis_Root_CA_1_G3.crt

66. QuoVadis_Root_CA_2.crt

67. QuoVadis_Root_CA_2_G3.crt

68. QuoVadis_Root_CA_3.crt

69. QuoVadis_Root_CA_3_G3.crt

70. SSL.com_EV_Root_Certification_Authority_ECC.crt

71. SSL.com_EV_Root_Certification_Authority_RSA_R2.crt

72. SSL.com_Root_Certification_Authority_ECC.crt

73. SSL.com_Root_Certification_Authority_RSA.crt

74. SZAFIR_ROOT_CA2.crt

75. SecureSign_RootCA11.crt

76. SecureTrust_CA.crt

77. Secure_Global_CA.crt

78. Security_Communication_RootCA2.crt

79. Security_Communication_Root_CA.crt

80. Staat_der_Nederlanden_EV_Root_CA.crt

81. Starfield_Class_2_CA.crt

82. Starfield_Root_Certificate_Authority_-_G2.crt

83. Starfield_Services_Root_Certificate_Authority_-_G2.crt

84. SwissSign_Gold_CA_-_G2.crt

85. SwissSign_Silver_CA_-_G2.crt

86. T-TeleSec_GlobalRoot_Class_2.crt

87. T-TeleSec_GlobalRoot_Class_3.crt

88. TUBITAK_Kamu_SM_SSL_Kok_Sertifikasi_-_Surum_1.crt

89. TWCA_Global_Root_CA.crt

90. TWCA_Root_Certification_Authority.crt

91. TeliaSonera_Root_CA_v1.crt

92. TrustCor_ECA-1.crt

93. TrustCor_RootCert_CA-1.crt

94. TrustCor_RootCert_CA-2.crt

95. USERTrust_ECC_Certification_Authority.crt

96. USERTrust_RSA_Certification_Authority.crt

97. XRamp_Global_CA_Root.crt

98. certSIGN_ROOT_CA.crt

99. ePKI_Root_Certification_Authority.crt

100. Certigna_Root_CA.crt

101. Entrust_Root_Certification_Authority_-_G4.crt

102. GTS_Root_R1.crt

103. GTS_Root_R2.crt

104. GTS_Root_R3.crt

105. GTS_Root_R4.crt

106. Hongkong_Post_Root_CA_3.crt

107. Microsoft_ECC_Root_Certificate_Authority_2017.crt

108. Microsoft_RSA_Root_Certificate_Authority_2017.crt

109. NAVER_Global_Root_Certification_Authority.crt

110. Trustwave_Global_Certification_Authority.crt

111. Trustwave_Global_ECC_P256_Certification_Authority.crt

112. Trustwave_Global_ECC_P384_Certification_Authority.crt

113. UCA_Extended_Validation_Root.crt

114. UCA_Global_G2_Root.crt

115. certSIGN_Root_CA_G2.crt

116. e-Szigno_Root_CA_2017.crt

117. emSign_ECC_Root_CA_-_C3.crt

118. emSign_ECC_Root_CA_-_G3.crt

119. emSign_Root_CA_-_C1.crt

120. emSign_Root_CA_-_G1.crt

121. AC_RAIZ_FNMT-RCM_SERVIDORES_SEGUROS.crt

122. ANF_Secure_Server_Root_CA.crt

123. Certum_EC-384_CA.crt

124. Certum_Trusted_Root_CA.crt

125. GlobalSign_Root_E46.crt

126. GlobalSign_Root_R46.crt

127. GLOBALTRUST_2020.crt

10. FIREWALL

10.1. Firewall principles

A firewall filters IP packets according to a set of rules in a certain order:

1. When the firewall receives a packet, it checks if it matches the first rule.

2. If it does, the decision is applied to the packet to `Allow` it or to `Deny` it according to the rule.

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

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

10.2. WAN traffic rules & VPN traffic rules

To configure the rules, go to the *Setup > Security > Firewall* menu

This section helps you create firewall rules. For a better organisation, the rules are divided in two sections; both having the same structure.

The **WAN traffic rules** filters the packets transmitted outside the VPNs and the **VPN traffic rules** filters the packets transmitted inside the VPNs.

The firewall is in charge of filtering IP frames between Interfaces (LAN/WAN/VPN). Both of the section can filter incoming packets (From LAN/WAN/VPN).

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

CAUTION	Rules defined in the "Port forwarding" table aren't checked by rules in this section. These packets are directly forwarded to the defined device (see Port forwarding)

There are some default parameters in both section:

LAN→WAN default policy	`Allow` or `Deny`. Decision which will be applied if a packet does not match any of the rules of the filter. `Allow` by default
WAN→LAN default policy	`Allow` or `Deny`. Decision which will be applied if a packet does not match any of the rules of the filter. `Deny` by default
Enable Deny of service filter (DoS)	Enable rules to protect against Denial Of Service attacks. `True` by default

Enable conntrack helpers (Not recommended)	Connection tracking helpers are modules that provide support for tracking and manipulating certain application-layer protocols within the connection tracking subsystem (for example: FTP, H.323, SIP, PPTP, IRC). It is disabled by default for security reasons. `False` by default
Accept ping	Accept ping on the WAN interface. `True` by default
LAN→VPN default policy	`Allow` or `Deny`. Decision which will be applied if a packet does not match any of the rules of the filter. `Allow` by default
VPN→LAN default policy	`Allow` or `Deny`. Decision which will be applied if a packet does not match any of the rules of the filter. `Allow` by default
Accept traffic between VPN	Allow traffic coming from one VPN to be forwarded to another VPN. `True` by default

In these sections there are tables, 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.

Direction	The direction the packet is going *Example 30. Direction* ``` WAN ¬ LAN ```
Action	`Allow`: To authorize packets concerned or `Deny`: To drop packets concerned
Protocol	TCP, UDP, ICMP, AH, ESP, GRE, IGMP or All for all kinds of protocols
Source port & Destination port	Port number If TCP or UDP selected, leave blank if all ports are concerned
Source IP address & Destination IP address	Concerned IP addresses, leave blank if all addresses are concerned
Log	Packets matching this rule will be logged in the menu *Diagnostics > Logs > Firewall*

11. USERS

Two types of users can access the router:

- `Operators` that needs access rights to the network

- `Administratos` that configure the Router

Both of them are linked to a `User`.

11.1. User management

The router has a new user management mechanism. A user is a physical person who need to access the device regardless if it is to configure it or to access through it.

Users can be defined in the screen *Setup > Security > Users*.

Figure 16. User management screen

11.2. Create a User

To register a new user in the user list, click the **Add** button located under the user list.

Figure 17. User creation

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

11.3. Operators management

An operator is an `User` that need to access through the router.
Individual access rights to the network can be assigned to each `User`.

Create an Operator

In the screen ***Setup > Remote access > Operator list***, an administrator can define an operator, by associating an `User` with a set of firewall rules.

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

To grant access rights to a remote user:

1. Click the **Add** button.

2. Select a `User` in the list.

3. Select a device in the list to authorise the remote user to access to that device.

Figure 18. Operator creation screen

> **NOTE**   A device ca be a subnet or an IP address (refer to the ***Setup > LAN interface > Device list***).

11.4. Administrator and Role definition

An administrator is a user that will configure the router. It can access only screens allowed by its Role.

To protect the adminsitration section with authentication, select ***Setup > Security > Administration rights*** menu. Then check the **Password protect the configuration interface** checkbox.

Create an Admin

In the screen *Setup > Security > Administration Rights*, the Super Administrator can create an Administrator by associating a User with a Role.

> Home > Setup > Security > Administration rights > Add/Edit an administrator

Save   Cancel   Page has unsaved changes

Administration role

	Role	Network ⌄

Administration login

	User	Jean Michel Legellec (jeanmich) ⌄

Save   Cancel   Back

Figure 19. Admin creation screen

6 roles are defined and allow the user to access specific screens. They are defined in the section Role list:

- Remote access
- Remote management
- Network
- System
- Super Administrator
- Auditor

NOTE	At least one Super Administrator is required on the router. If there is no Super Administrator defined, the router will ask you to create one.

Role list

Remote access

- User management
- Remote access user list management
- Remote maintenance access rules management
- Network interfaces and M2Me connection diagnostic
- Current configuration backup
- Note creation

Remote management

Same as Remote access +

- Datalogger management

- Collect & Alert management

Network

Same as Remote management +

- WANs configuration

- LANs configuration

- Remote access servers configuration

- VPNs (IPSec and OpenVPN)

- Static routes

- VRRP / RIP

- Firewall / port forwarding / NAT / NAT 1:1

- Dynamic DNS

- Certificate store

- Gateways

- SMS / emails

- Ping tool

System

Same as Network +

- Network admin creation

- Remote access admin creation

- Operation admin creation

- Date/Time management

- Periodical reboot

- Remote Syslog

- SNMP

- ModBus / OPCUA server

- GPS

- Software options

- Reboot

- Advanced diagnostic

Super Administrator

Same as System + Operation +

- Delegated authentication management
- Complete user list management
- Configuration load

Auditor

- Read all parameters and status
- Internal status report generation

12. SYSLOG

To configure your product to send logs to a remote Syslog server of your choice.

Go to the *Setup > System > Syslog* menu and check the **Enable** option.

12.1. Syslog remote server configuration

Log server IP address & **Port number** parameters:

IP address and port of the Syslog server to send logs to

Transfert mode parameter:

- `Clear text`: logs are transferred in clear text form
- `Server authentication`: logs are encrypted with the server certificate
- `Mutual authentication`: logs are encrypted with the server certificate and signed with a private key

Server hostname parameter:

Only in `Server authentication` or `Mutual authentication`

Name of the syslog server. This field must match the server certificate common name.

CAUTION	Logs are encrypted with the server certificate. The CA that issued the server certificate must be present in the `Certification authority certificates` in the `Certificate store`.

Certificate parameter:

Only in `Mutual authentication`.

Chose a certificate from the `Certificate store` to sign logs.

CAUTION	The chosen certificate must be linked to a private key. Otherwise, logs cannot be signed.

13. HTTPS CONNECTION AND PORTAL FOR SMARTPHONE, TABLETS OR PCS

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

In addition, the HTTPS server can behave like an HTTPS to HTTP gateway to give 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.
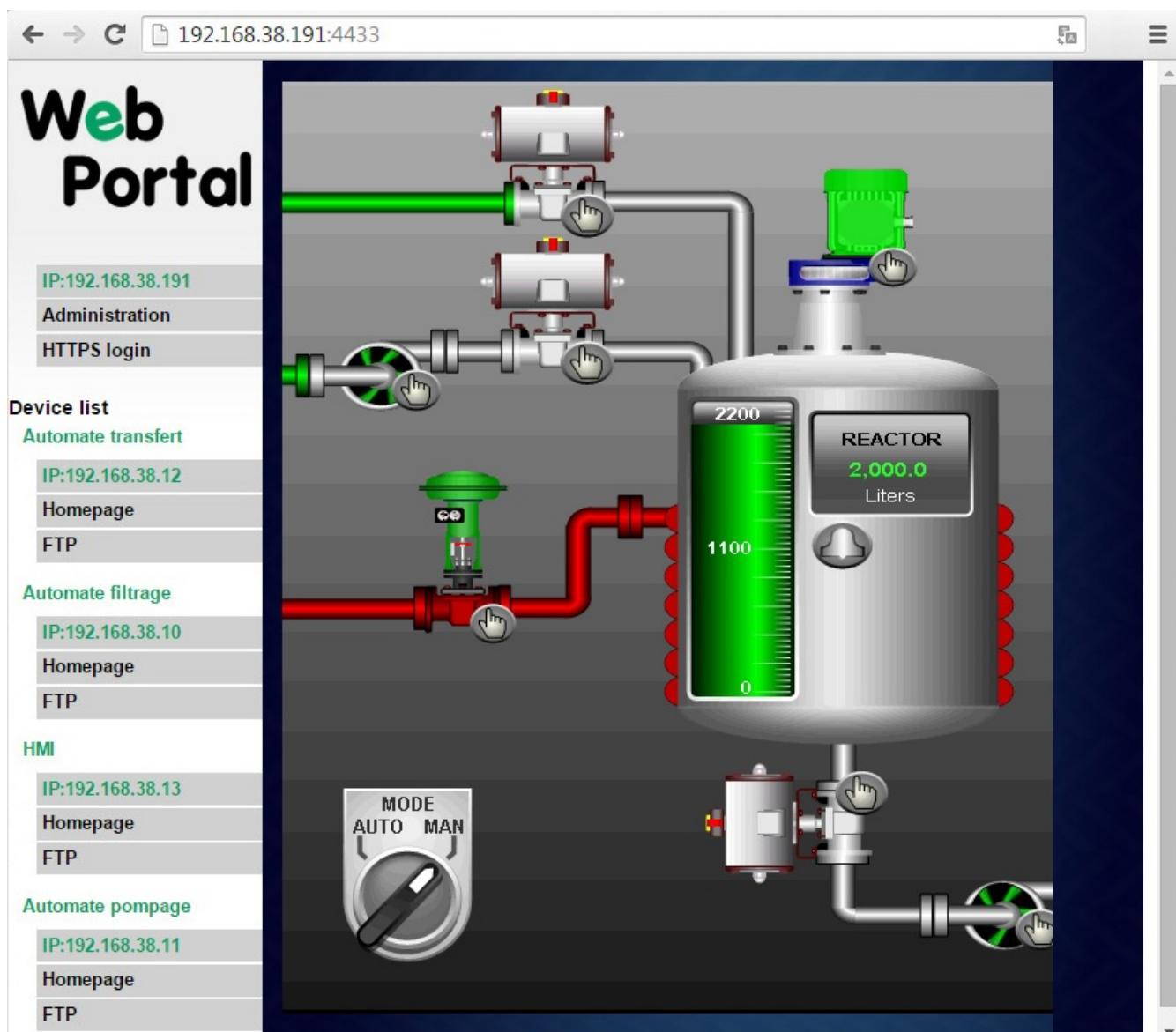
Figure 20. Embedded HTTP HTML page

13.1. Setup

Enable the HTTPS portal through the LAN interface

Select *Setup* > *Remote access* > *Remote access server* menu. Then check the **Enable HTTPS application server** checkbox.

Give access to the HTTPS portal through the Internet (WAN)

Select *Setup* > *Security* > *Administration rights* menu. Then check the **Enable access from the WAN (HTTPS only)** checkbox.

NOTE	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	Internet IP address	LAN IP address
Administration web server	Internet IP address: 4433	LAN IP address or https://adr.<IP Internet>: 4433

13.2. Operation

To access to the HTTPS internet portal from the Internet:

1. Launch the browser
2. Enter : https://« Internet IP address of the Router»
3. 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.

14. DYNAMIC DNS

The EticDNS, DynDNS or NoIP services make it possible to connect remotely to a router via the Internet even if the IP address of this router is dynamic.

The router's IP address must be a public IP address.

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

14.1. EticDNS

By creating an account on the Customer Area of the Etic Telecom website, you can manage your router and assign it a domain name for its Main WAN.

The router must be accessible via the Internet.

14.2. Step 1: Domain name allocation

Reserve a domain name on your favorite Dynamic DNS website.

14.3. Step 2: Router setup

Select the *Setup > Network > Dynamic DNS* menu. Then check the **Enable** checkbox.

Dynamic DNS service	Select `EticDNS`, `dyndns.org` or `NoIP`.
	NOTE — If you choose `EticDNS`, next parameters will be directly known by Etic Telecom
User account login	Login of your account assigned by your Dynamic DNS service
Password	Password of your account assigned by your Dynamic DNS service
Hostname	Domain name assigned by your Dynamic DNS service *Example 31. Domain name* mymachine.eticdns.com

15. ALARM EMAIL OR SMS

All the models of Routers are able to transmit an email when one event occurs.

Select the *Setup > System > SMS/e-mail* menu and check the **Enable** option.

Alarm launched on event parameter: Selects the event:

- `Input rising edge (¬ON)`
- `Input falling edge (¬OFF)`
- `Input rising or falling edge (¬ON or ¬OFF)`
- `The VPN connection/disconnection event`

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 to send parameter:

Enter the alarm text.

15.1. SMTP client section

Etic Telecom provides SMTP services which can be used to send alarm mails without additional setup.

Go to the menu *Setup > System > Messaging*.

Select **Use the M2Me server to send e-mail** option to send alarm mails through Etic Telecom service.

You can also use the SMTP server of your choice. Uncheck the previous box and configure the following parameters:

SMTP server	The destination SMTP server
Port	The port on which the SMTP server listens
Security	The encryption used: `None`, `StartTLS` or `TLS`
Use user certificate	Select the certificate from the certificate store that will be used to encrypt the connection
CA source	Whether the CA for server authentication is from the certificate store or the bundle provided with the router (see CA bundle)
SMTP server CA certificate	The CA from the certificate store for server authentication
Authentication	The way to authenticate on the server
Login and Password	Username and password for authentication on the server

15.2. SNMP

The Router is an SNMP agent; it complies with the MIB standard and transmits an SNMP trap when configurable events occur.
It can also send traps to an SNMP manager.

SNMP Configuration

Go to the menu *Setup > System > SNMP*

The following properties are used by both the SNMP agent and to identify the sending of traps.

System name	`syslocation` of the SNMP agent. Also allows the manager to identify the origin of traps.
System location	`sysname` of the SNMP agent. Also allows the manager to identify the origin of traps.

SNMP agent configuration

Enable	Enable the SNMP agent
SNMP protocol version	SNMP version to use. `SNMP version 1 and 2c` or `SNMP version 3`
Community name	This is the name shared between each agent and the SNMP manager. The SNMP agent only responds to requests from a manager who identifies himself by this name (only in `SNMP version 1 and 2c`)
Username	SNMP user username (only in `SNMP version 3`)

Authentication algorithm	Algorithm for authentication (only in `SNMP version 3`) *Example 32. Possible values* MD5, SHA1, SHA-224, SHA-256, SHA-384, SHA-512
Password	SNMP user password (only in `SNMP version 3`)
Cipher algorithm	Algorithm used to encrypt data (only in `SNMP version 3`) *Example 33. Possible values* AES-256-CBC, AES-192-CBC, AES-128-CBC, DES, Blowfish
Cipher key	Cipher key used to encrypt data (only in `SNMP version 3`)
Monitor the OpenVPN backup state	The VPN server can monitor the status of its clients' primary and backup VPNs via SNMP. It uses this data to display a summary table in the *Diagnostics > Network status > VPN Connections > OpenVPN* page
Name of the main VPN	Name of the first VPN to monitor
Name of the secondary VPN	Name of the second VPN to monitor

Trap sending configuration

Product startup - Cold start	Send SNMP trap Cold Start
Gateway restart - WarmStart	Send SNMP trap to gateway on reboot (router with serial link only)
RawTCP server gateway connected - LinkUp	Send SNMP trap on IP to serial link connection (router with serial link only)
RawTCP server gateway disconnected - LinkDown	Send SNMP trap on IP to serial link disconnection (router with serial link only)
First SNMP manager IP address	SNMP manager IP address to which SNMP traps will be sent
Second SNMP manager IP address	Second SNMP manager IP address to which SNMP traps will be sent
SNMP protocol version	Same as SNMP agent
Community name	Same as SNMP agent
Username	Same as SNMP agent
engineID	Specify `engineID` to define the SNMP entity. A hexadecimal between 5 and 32 bytes is expected. The parameter must start with `0x`.
Authentication algorithm	Same as SNMP agent
Password	Same as SNMP agent

Cipher algorithm	Same as SNMP agent
Cipher key	Same as SNMP agent

16. MODBUS TCP SERVER

16.1. Configuring Modbus TCP server

Etic Telecom provides a Modbus TCP server allowing you to make requests to retrieve various data collected by the product, but also to trigger product features. The complete list of available data is presented in the section `Specification of registers and their contents`.

Inside menu *Setup > System > Modbus Server*. Check the **Enable** box and enter a free TCP port number for the Modbus server. If you do not specify a port number, port 502 is used by default.

The machines connected to the product will be able to send Modbus TCP requests to previously specified port and thus retrieve the content of requested registers.

16.2. Reading and writing Modbus registers

Some registers are made to be read; they show statuses for the product. Others are made for you to write inside them for specific features. These registers are detailed in chapter `Specification of registers and their contents`.

- To read registers, send a Modbus Request `Read Holding Registers (FC=3)`.
- To write on registers, send a Modbus Request `Write Multiple Registers (FC=16)` or `Write Single Register (FC=6)`.
- To write on coils, send a Modbus Request `Write Single Coil (FC=5)` or `Force Multiple Coils (FC=15)`.

Sending SMS and E-Mail Functionality

Some registers are dedicated to message options:

- **Registers 490-539:** Message sender
- **Registers 540-589:** Message destination
- **Registers 590-639:** Message subject
- **Registers 640-763:** Message text

CAUTION

Here, registers numbers follow chapter `Specification of registers and their contents` but numbers used by Modbus client's requests are 10 registers higher.

```
Modbus
    .001 0000 = Function Code: Write Multiple Registers (16)
    Reference Number: 500
```

Figure 21. Wireshark capture of a Modbus Request to write Message sender

Steps from PLC

1. Write 8-bit ASCII characters starting from the first register of each option.

    ◦ Every option must be filled to send E-Mail, only Destination and Text for SMS.

    ◦ The Modbus Server will read registers until it finds a register with value 0x00, the Sender, Destination and Subject registers are therefore limited to 99 characters.

2. Write inside Modbus Coils to trigger the sending of the message.

    ◦ Setting Coil at address 0 to ON state will send an SMS.

    ◦ Setting Coil at address 1 to ON state will send an e-mail.

Example 34. Content of registers for the sender "ETIC Telecom": each register contains 2 characters; the first letter is on the LSB and the second on the MSB.

Register	490	491	492	493	494	495	496
Register @	40501	40502	40503	40504	40505	40506	40507
8-bit ASCII	TE	CI	T	le	ce	mo	
Hexadecimal	0x5445	0x4349	0x5420	0x6c65	0x6365	0x6d6f	0x0000
Decimal	21573	17225	21536	27749	25445	28015	0

```
Modbus
    .000 0101 = Function Code: Write Single Coil (5)
    Reference Number: 1
```

Figure 22. Wireshark capture showing a Modbus Request to trigger an E-Mail

16.3. Specification of registers and their contents

Register 0 Address: 40011

NodeID: 255

Register MAP

Register 0-3: GPS Location latitude: TYPE LREAL (-1.79e+308 … 1.79e+308) - °
- Register 0 - bit 0: LSB (Least Significant Bit)
- Register 3 - bit 15: MSB (Most Significant Bit)

Register 4-7: GPS Location longitude: TYPE LREAL (-1.79e+308 … 1.79e+308) - °
- Register 4 - bit 0: LSB
- Register 7 - bit 15: MSB

Register 8-9: GPS Location altitude: TYPE REAL (-3.40e+38 - 3.40e+38) - meters

- Register 8 - bit 0: LSB

- Register 9 - bit 15: MSB

Register 10-11: GPS Location speed: TYPE REAL (-3.40e+38 - 3.40e+38) - m/s

- Register 10 - bit 0: LSB

- Register 11 - bit 15: MSB

Register 12: GPS Location precision: TYPE UINT (0 ... 65535) - meters

...

Register 20: Input states Connected: TYPE WORD

- bit 0 - Status of input (0 disabled / 1 enabled)

Register 21: Output states Connected: TYPE WORD

- bit 0 - Status of output (0 disabled / 1 enabled)

Register 22: Power supply 1: TYPE UINT (0 ... 65535) - dV

Register 23: Power supply 2: TYPE UINT (0 ... 65535) - dV

Register 24: Internal temperature: TYPE INT (-32768 ... 32767) - °C

...

Register 30: Main WAN Status: TYPE UINT (0 ... 65535)

- 0: All Down / 1: ADSL / 2: Ethernet / 3: Cellular / 4: Wi-Fi

Register 31: ADSL WAN states: TYPE WORD

- bit 0: ADSL WAN State (0 disabled / 1 enabled)

- bit 1: ADSL WAN Connected (0 disconnected / 1 connected)

Register 32: Ethernet WAN states: TYPE WORD

- bit 0: Ethernet WAN State (0 disabled / 1 enabled)

- bit 1: Ethernet WAN Connected (0 disconnected / 1 connected)

Register 33: Cellular WAN states: TYPE WORD

- bit 0: Cellular WAN State (0 disabled / 1 enabled)

- bit 1: Cellular WAN Connected (0 disconnected / 1 connected)

Register 34: Wi-Fi WAN states: TYPE WORD

- bit 0: Wi-Fi WAN State (0 disabled / 1 enabled)

- bit 1: Wi-Fi WAN Connected (0 disabled / 1 enabled)

- bit 2: Wi-Fi WAN Auto-DNS (0 disabled / 1 enabled)

...

Register 40: ADSL WAN Down Rate: TYPE UINT (0 … 65535) - kbits/s

Register 41: ADSL WAN Up Rate: TYPE UINT (0 … 65535) - kbits/s

Register 42-43: ADSL WAN Down SNR Margin: TYPE REAL (-3.40e+38 - 3.40e+38) - dB

Register 44-45: ADSL WAN Up SNR Margin: TYPE REAL (-3.40e+38 - 3.40e+38) - dB

...

Register 60: Cellular WAN Signal level: TYPE INT (-32768 … 32767) - dBm

Register 61-62: Cellular WAN SNR: TYPE REAL (-3.40e+38 - 3.40e+38) - dBm

- Register 61 - bit 0: LSB

- Register 62 - bit 15: MSB

Register 63: Cellular WAN Bytes Received: TYPE UINT (0 … 65535) - Megabytes

Register 64: Cellular WAN Bytes Transmitted: TYPE UINT (0 … 65535) - Megabytes

...

Register 70: Wi-Fi WAN Frequency: TYPE UINT (0 … 65535) - MHz

Register 71: Wi-Fi WAN Signal level: TYPE INT (-32768 … 32767) - dBm

...

Register 80: LAN Interfaces states: TYPE WORD

- bit 0...1 - status of Ethernet LAN port 0

  ◦ 00 disabled

  ◦ 10 enabled/disconnected

  ◦ 11 enabled/connected

- bit 2...3 - status of Ethernet LAN port 1

- bit 4...5 - status of Ethernet LAN port 2

- bit 6...7 - status of Ethernet LAN port 3

Register 81: Wi-Fi LAN states: TYPE WORD

- bit 0: Wi-Fi LAN State (0 disabled / 1 enabled)

- bit 1: Wi-Fi LAN 802.11n (0 disabled / 1 enabled)

- bit 2: Wi-Fi LAN on Tor (0 disabled / 1 enabled)

Register 82: M2Me remote access states: TYPE WORD

- bit 0: M2Me Active (0 disabled / 1 enabled)

- bit 1: M2Me Connected (0 disconnected / 1 connected)

- bit 2: M2Me Proxy (0 disabled / 1 enabled)

Register 83: M2Me number of connected remote users: TYPE UINT (0 … 65535)

...

Register 90-99: Open VPN IN states: TYPE WORD

- bit X: VPN n° X Connected (0 disconnected-not created / 1 connected)

Register 100-109: Open VPN OUT states: TYPE WORD

- bit X: VPN n° X Connected (0 disconnected-not created / 1 connected)

Register 110-119: IPsec VPN states: TYPE WORD

- bit X: VPN n° X Connected (0 disconnected-not created / 1 connected)

...

Register 490-539: Message sender

- 50 registers made to write 99 8-bit ASCII characters (Not used for SMS)

Register 540-589: Message destination

- 50 registers made to write 99 8-bit ASCII characters - Must be a valid phone number or E-mail

Register 590-639: Message subject

- 50 registers made to write 99 8-bit ASCII characters (Not used for SMS)

Register 640-763: Text message to be sent

- 123 registers made to write 246 8-bit ASCII characters

17. CLIENT SSH COMMANDS

17.1. List of client SSH commands

You can manage your product through an SSH connection. A subset of Linux commands are available, plus a set of Etic Telecom commands which will help you configure and use your device.

To copy files into the product, you can use `scp` into the directory `/tmp` which is the only directory with write access.

All of these commands have a helper which you can access with argument `--help`.

Command	Description
m2me	Start or stop M2Me
test_smsemail	Proceed to the test of sending sms and email
stor	Change output to a specific state
test_ftpc	Test FTP client
shdsl_testmode	Test SHDSL mode
shdsl_dotest	Call SHDSL socrates
shdsl_pmms	Read SHDSL pmms
sw_upgrade	Upgrade software with a code
fw_upgrade	Upgrade firmware with an archive
get_upgrades_list	Get a list of available upgrades version online
upgrade_from_eticnet	Upgrade version from Eticnet server
set_date_time	Set the date and time
display_view	Display parameters descriptions used in views
delete_row	Delete a row in current configuration
add_row	Add a row in a group of parameters
edit_row	Edit a row in a group of parameters
swap_rows	Swap two rows in a group of parameters
get_groups_params	Get parameters of a group in the configuration
get_params	Get parameters in the configuration
get_status	Get statuses of the product
get_groups_status	Get statuses of a group of status

Command	Description
set_params	Set parameters in the configuration
set_superadmin_password	Set Super Administrator user password (login 'admin')
reset_hotline_passwd	Reset hotline password
config_list	List saved configurations
config_load	Load a configuration
config_save	Save a 'User' configuration
config_delete	Delete a 'User' configuration
config_upload	Upload a 'User' configuration
config_load_fac	Reload factory configuration
config_export	Export the configuration
make_csr_request	Make a CSR request for a specific private key
get_cert_infos	Get details of a certificate
generate_private_key	Generate a private key
import_private_key	Import a private key in x509 format
delete_private_key	Delete a private key
add_crl	Add a certificate revocation list in x509 format
delete_crl	Delete a certificate revocation list
add_cert	Add a certificate in x509 format
add_pkcs12	Add a PKCS12 file
delete_cert	Delete a certificate
role_add	Add administrator custom role(s)
role_list	List administrator roles or display their description
role_delete	Delete an administrator custom role

17.2. Commands helper

m2me

```
$ m2me --help
```

```
m2me : Start or stop M2Me

usage : m2me <expected_state>

  expected_state : START / STOP. start or stop the m2me on the device
```

test_smsemail

```
$ test_smsemail --help
test_smsemail : Proceed to the test of sending sms and email

usage : test_smsemail
```

stor

```
$ stor --help
stor : Change output to a specific state

usage : stor <expected_state>

  expected_state : ON / OFF. Switch ON or switch OFF the stor
```

test_ftpc

```
$ test_ftpc --help
test_ftpc : Test FTP client

usage : test_ftpc
```

shdsl_testmode

```
$ shdsl_testmode --help
shdsl_testmode : Test SHDSL mode

usage : shdsl_testmode
```

shdsl_dotest

```
$ shdsl_dotest --help
shdsl_dotest : Call SHDSL socrates

usage : shdsl_dotest <command>

  command   : Command to pass to socrates. help (without --) as command for more
information
```

shdsl_pmms

```
$ shdsl_pmms --help
shdsl_pmms : Read SHDSL pmms

usage : shdsl_pmms
```

sw_upgrade

```
$ sw_upgrade --help
sw_upgrade : Upgrade software with a code

usage : sw_upgrade <code>

        code : Code provided by Etic Telecom to upgrade your device
```

fw_upgrade

```
$ fw_upgrade --help
fw_upgrade : Upgrade firmware with an archive

usage : fw_upgrade <fw_path> [force] [end_upgrade] [config_file]

    fw_path : Path of the firmware archive to upgrade to
      force : (Optionnal - Default : False) Do not verify signature archive : True /
False
end_upgrade : (Optionnal - Default : True) End the action and clean the pending status
in database : True / False
config_file : (Optionnal - Default : '') Load a configuration file after the upgrade
```

get_upgrades_list

```
$ get_upgrades_list --help
get_upgrades_list : Get a list of available upgrades version online

usage : get_upgrades_list
```

upgrade_from_eticnet

```
$ upgrade_from_eticnet --help
upgrade_from_eticnet : Upgrade version from Eticnet server

usage : upgrade_from_eticnet <version> [config_file]

version_file : Version file to upgrade to. Use cmd 'get_upgrades_list' to get the
possible version files available
 config_file : (Optionnal - Default : '') Load a configuration file after the upgrade
```

set_date_time

```
$ set_date_time --help
set_date_time : Set the date and time

usage : set_date_time <date_time>

  date_time : Date/Time to set. Format shall be YYYY-MM-DD_HH:mm
```

display_view

```
$ display_view --help
display_view : Display parameters descriptions used in views

usage : display_view [view] ...

  views     : 0-N view(s) to display
```

delete_row

```
$ delete_row --help
delete_row : Delete a row in current configuration

usage : delete_row <group_name> <row_index>

  group_name  : Name of the group where to deleted the row
  row_index   : Index of the row to delete
```

add_row

```
$ add_row --help
add_row : Add a row in a group of parameters

usage : add_row <group_name> <param_name param_value> [param_name param_value] ...

  group_name              : Name of the group where to add rows
  param_name param_value  : 1-N couples of <param_name param_value> to add in a group
```

edit_row

```
$ edit_row --help
edit_row : Edit a row in a group of parameters

usage : edit_row <group_name> <row_index> <param_name param_value> [param_name
param_value] ...

  group_name              : Name of the group where to add rows
  row_index               : Index of the row to edit
  param_name param_value  : 1-N couples of <param_name param_value> to add in a group
```

swap_rows

```
$ swap_rows --help
swap_rows : Swap two rows in a group of parameters

usage : swap_rows <group_name> <row_index_1> <row_index_2>

  group_name        : Name of the group where to swap rows
```

```
    row_index_(1|2) : Indexes of the rows to swap
```

get_groups_params

```
$ get_groups_params --help
get_groups_params : Get parameters of a group in the configuration

usage : get_groups_params <group> ...

  group : 1-N group(s) to display
```

get_params

```
$ get_params --help
get_params : Get parameters in the configuration

usage : get_params <param> ...

  param : 1-N param(s) to display
```

get_status

```
$ get_status --help
get_status : Get statuses of the product

usage : get_status <status>.<index> ...

  status      : 1-N status to display
  index       : Index of the specified status to get (0-N)
```

get_groups_status

```
$ get_groups_status --help
get_groups_status : Get statuses of a group of status

usage : get_groups_status <group> ...

  group : 1-N group(s) to display
```

set_params

```
$ set_params --help
set_params : Set parameters in the configuration

usage : set_params <param_name param_value> [param_name param_value] ...

  param_name param_value  : 1-N couples of <param_name param_value> to add in the
configuration
```

set_superadmin_password

```
$ set_superadmin_password --help
set_superadmin_password : Set super admin user password (login 'admin')

usage : set_superadmin_password <password value> ...

  password     : Password of the Super Administrator. Password must follow the
following rules:
                 * One lowercase letter
                 * One uppercase letter
                 * One number
                 * One special character in the subset: &#{}[]@!?_ *+=~$%
                 * Minimum of 8 characters
Maximum of 50 characters
```

reset_hotline_passwd

```
$ reset_hotline_passwd --help
reset_hotline_passwd : Reset hotline password

usage : reset_hotline_passwd [password_length]

  password_length : (Optionnal - Default : 12) Length of the generated password.
```

config_list

```
$ config_list --help
config_list : List saved configurations

usage : config_list [config_types]
```

```
config_types    : types of configuration to display : Reference / User / Builder
```

config_load

```
$ config_load --help
config_load : Load a configuration

usage : config_load <conf_filename> [config_type] [edition_mode]

  conf_filename   : File name of the configuration to load
  config_type     : (Optionnal - Default : User) location of the configuration to load
: Reference / User / Builder
  edition_mode    : (Optionnal - Default : False) start edition mode : True / False
                       edition mode : Configuration has to be validated with option
<commit> to apply it
```

config_save

```
$ config_save --help
config_save : Save a 'User' configuration

usage : config_save <conf_name>

  conf_name       : Name of the saved configuration. Will be located in the User space
```

config_delete

```
$ config_delete --help
config_delete : Delete a 'User' configuration

usage : config_delete <conf_name>

  conf_name       : Name of the exported configuration. Will appear in the User space
```

config_upload

```
$ config_upload --help
config_upload : Upload a 'User' configuration
```

```
usage : config_upload <file_path> <conf_name> [force] [decryption_secret]


   file_path  : Path of the configuration file to upload
   conf_name  : Name of the configuration in User space
   force      : (Optionnal - Default : False) force upload file : True / False. Bypass
illformed configuration
   decryption_secret  : (Optionnal) Secret to decrypt password in the configuration
```

config_load_fac

```
$ config_load_fac --help
config_load_fac : Reload factory configuration

usage : config_load_fac
```

config_export

```
$ config_export --help
onfig_export : Export the configuration

usage : config_export <conf_filename> <destination_file> <secret_encryption>
[encryption_key] [config_type]

   conf_name         : Configuration name to export
   destination_file  : Output file destination
   secret_encryption : Encrypt or not the secrets : encrypt / no_encryption
   encryption_key    : (Only if <secret_encryption> is `encrypt`) Key to encrypt
configuration's secrets
   config_type       : (Optionnal - Default : User) location of the configuration :
Reference / User / Builder
```

make_csr_request

```
$ make_csr_request --help
make_csr_request : Make a CSR request for a specific private key

usage : make_csr_request <private_key>

   private_key : The private key to make the CSR for
```

get_cert_infos

```
$ get_cert_infos --help
get_cert_infos : Get details of a certificate

usage : get_cert_infos <certificate> [CA]

  certificate : Certificate to retrieve information
           CA : (Optionnal - Default : False) Look in Certification Authorities
certificates : True / False
```

generate_private_key

```
$ generate_private_key --help
generate_private_key : Generate a private key

usage : generate_private_key <pk_name> <algo> [algo_param]

    pk_name : Name of the private key
       algo : Private Key Algorithm (Possible value : rsa / ecdsa)
 algo_param : (Optionnal) Depending of the algorithm choosen
                 rsa   : (Default : 2048) length of the key (Possible value : 2048)
                 ecdsa : (Default : Prime256v1) curve to use (Possible value :
Prime256v1)
```

import_private_key

```
$ import_private_key --help
import_private_key : Import a private key in x509 format

usage : import_private_key <key_name> <key_path>

   key_name : Name of the private key
   key_path : Private key file path
```

delete_private_key

```
$ delete_private_key --help
delete_private_key : Delete a private key

usage : delete_private_key <private_key>
```

```
   private_key : The private key to delete
```

add_crl

```
$ add_crl --help
add_crl : Add a certificate revocation list in x509 format

usage : add_crl <crl_name> <crl_path>

   crl_name : Name of the certificate revocation list
   crl_path : CRL file path
```

delete_crl

```
$ delete_crl --help
delete_crl : Delete a certificate revocation list

usage : delete_crl <crl_name>

    crl_name : The CRL to delete
```

add_cert

```
$ add_cert --help
add_cert : Add a certificate in x509 format

usage : add_cert <cert_name> <cert_path> [CA]

  cert_name : Name of the certificate
  cert_path : Certificate file path
        CA : (Optionnal - Default : False) Insert in Certification Authorities
certificates : True / False
```

add_pkcs12

```
$ add_pkcs12 --help
add_pkcs12 : Add a PKCS12 file

usage : add_pkcs12 <pkcs12_name> <pkcs12_file> <pkcs12_password>
```

```
      pkcs12_name : Name of the Pkcs12
      pkcs12_file : PKCS12 file path
  pkcs12_password : password of the pkcs12
```

delete_cert

```
$ delete_cert --help
delete_cert : Delete a certificate

usage : delete_cert <cert_name> [CA]

  cert_name : The certificate to delete
         CA : (Optionnal - Default : False) Delete in Certification Authorities
certificates : True / False
```

role_add

```
$ role_add --help
role_add : Add administrator custom role(s)

usage : role_add <file_path>

  file_path  : Absolut path of the file with the customs roles to add
  overwrite  : (Optionnal - Default : False) Overwrite custom roles if it exists
already
```

Custom roles must be described in a `json` format.
This format is a `list` of role. Each role is a `dict` containing the following parameters:

role_name	Internal name of the role. 50 characters maxmimum, must be in lower case and starts with `p_custom_role_`
local_fr	Displayed text in french
local_en	Displayed text in english
func_permissions	Set a permission level for each functions: • `20`: read • `30`: write Functions `func_superadmin`, `func_admin`, `func_firmconf` can only be set to level `read`.

17.2. Commands helper

Custom role file example

```
[
    {
        "role_name": "p_custom_role_group_a",
        "local_fr": "Administrateur A",
        "local_en": "Administrator A",
        "func_permissions": {
            "func_generic": 30,
            "func_biwan": 20,
            "func_wan_eth": 20,
            "func_wan_br": 20,
            "func_wan_ip": 20,
            "func_diagnostics": 20,
            "func_logs": 20,
            "func_net_stat": 20,
            "func_diag_ifaces": 20,
            "func_vpn_node": 20,
            "func_tls_node": 20,
            "func_tools": 20,
            "func_firmconf": 20,
            "func_product_def": 20
        }
    },
    {
        "role_name": "p_custom_role_group_b",
        "local_fr": "Administrateur B",
        "local_en": "Administrator B",
        "func_permissions": {
            "func_generic": 30,
            "func_biwan": 30,
            "func_wan_eth": 30,
            "func_wan_gsm": 30,
            "func_wan_br": 30,
            "func_wan_ip": 30,
            "func_diagnostics": 30,
            "func_logs": 30,
            "func_net_stat": 30,
            "func_diag_ifaces": 30,
            "func_vpn_node": 30,
            "func_tls_node": 30,
            "func_tools": 30,
            "func_firmconf": 20,
            "func_product_def": 20
        }
    }
]
```

role_list

```
$ role_list --help
role_list : List administrator roles or display their description

usage : role_list [role_name]

    role_name : (Optionnal - Default : Empty) If empty, display role_name of all roles
                            If role_name is provided, display the role in a json
format
```

role_delete

```
$ role_delete --help
role_delete : Delete an administrator custom role

usage : role_delete <role_name>

    role_name  : Custom role to delete
        force  : (Optionnal - Default : False) Delete the role even if administrators
use it
```

18. SERIAL TO IP GATEWAYS

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.
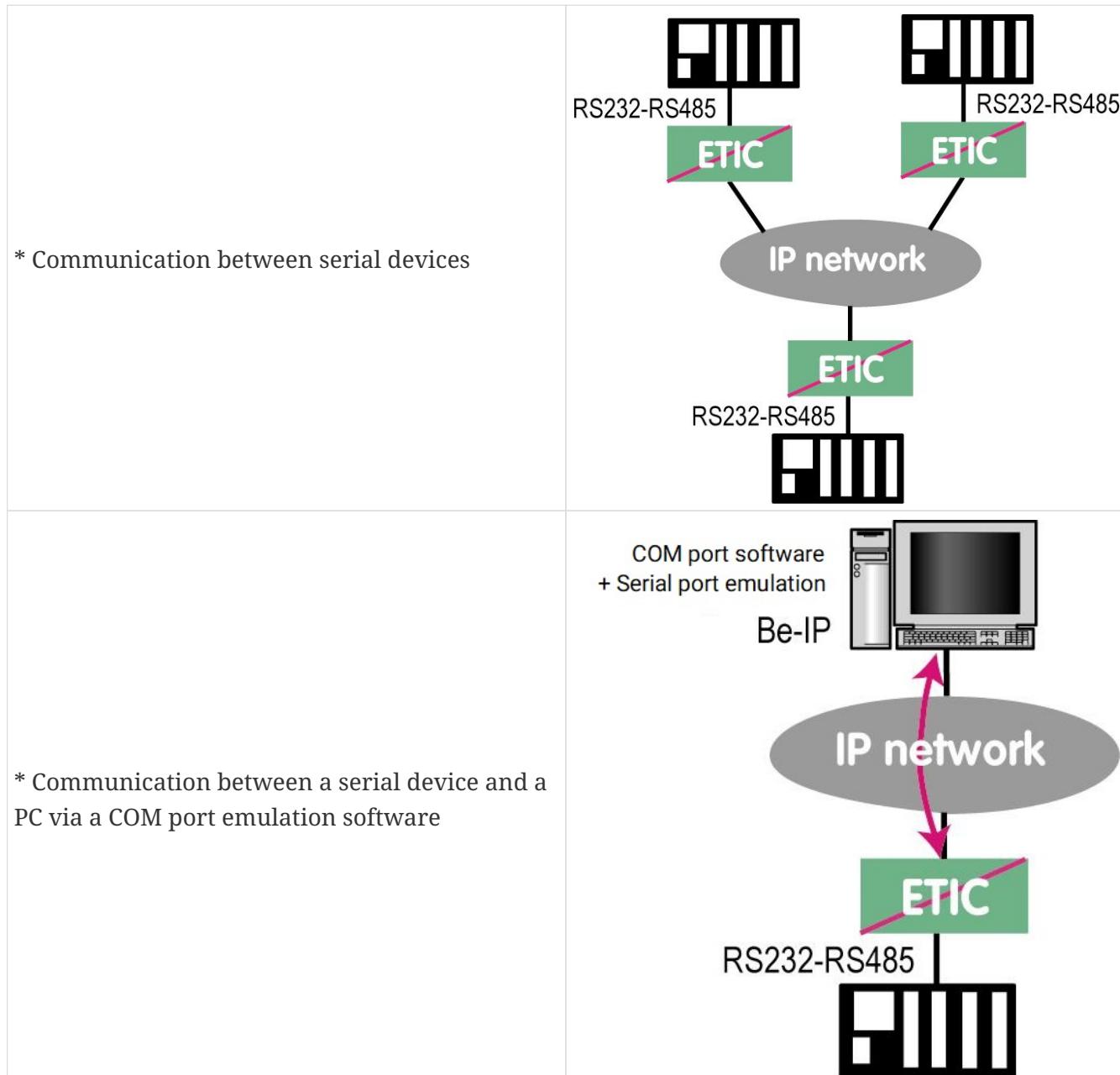
* Communication between serial devices	
* Communication between a serial device and a PC via a COM port emulation software	

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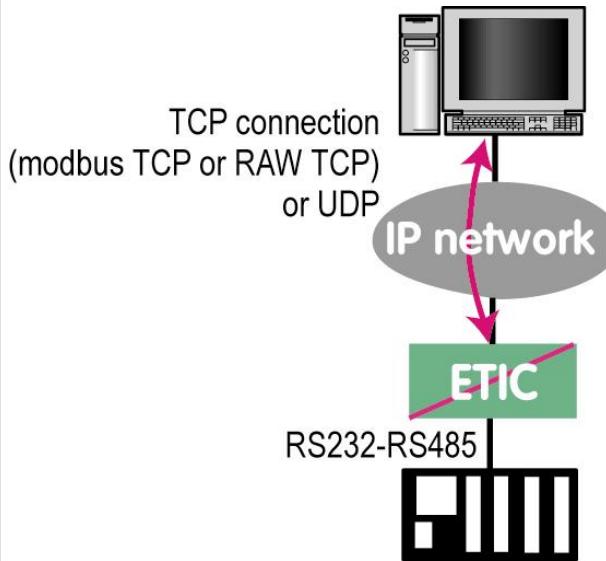
To perform the functions described above, several types of gateways are available.

18.1. Modbus

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

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.

NOTE   The Modbus address must not be confused with the IP address of a Modbus device.

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.

<u>Assigning a Modbus gateway to a serial port</u>

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).

<u>Modbus client gateway</u>

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.	
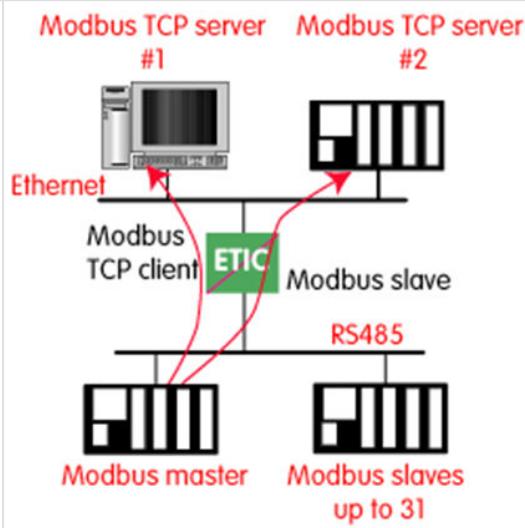
How works Modbus Client Gateway

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.
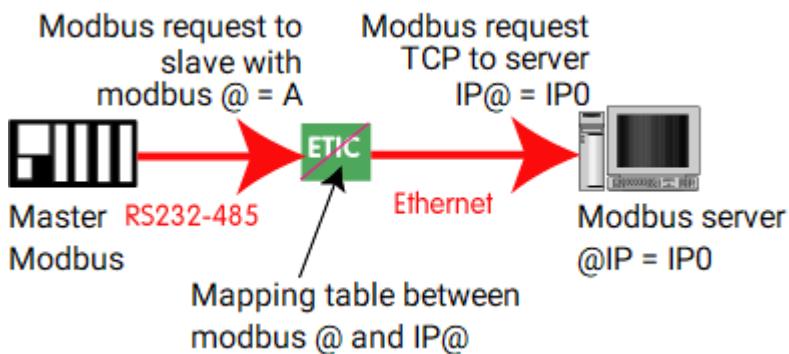

Figure 23. Modbus mapping table

Configure the gateway

Select *Setup > Gateways > IP-RS > Modbus > Modbus client*, then check the **Enable Modbus client** checkbox.

COM port parameter:

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits parameters:

Allow to set the bit rate and the format of the asynchronous serial link.

Modbus protocol parameter:

Select RTU (hexa) or ASCII

Inter-character time parameter:

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

TCP idle Timeout parameter:

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

TCP port parameter:

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

Modbus slaves parameter:

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

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.
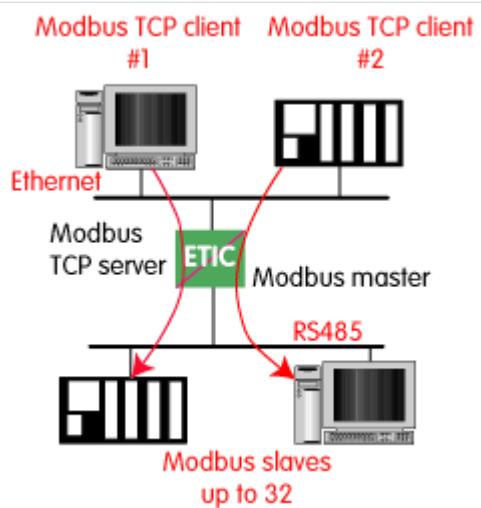
How Modbus server Gateway works

A Modbus TCP client send a Modbus TCP client to the gateway.
The gateway behave as a master on the serial link. It transcodes 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.
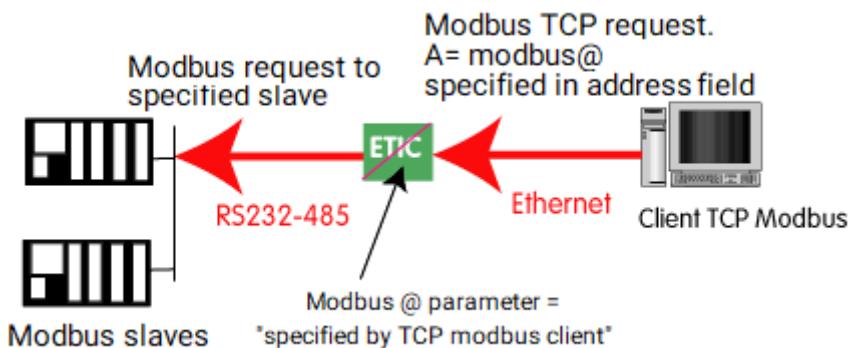
- Or a fixed address configured in the gateway (see below); in this case, only one slave can be addressed on the serial link.
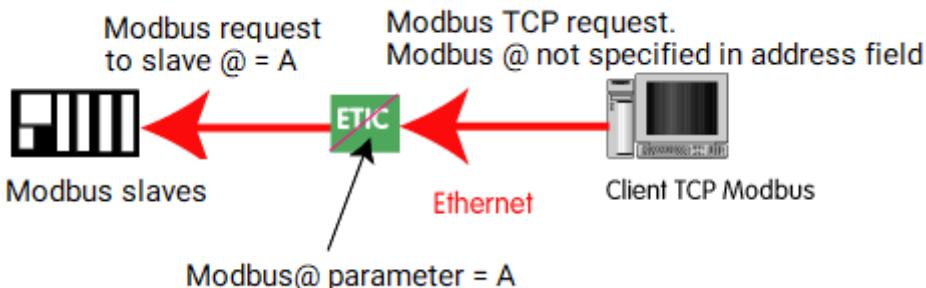
CAUTION	Several TCP Modbus client can send requests to the slaves on the serial link. Nevertheless, care must be taken not to saturate the serial link since its flow rate is much lower than the Ethernet one.

Configure the gateway

Select *Setup > IP-RS > Gateways > Modbus > Modbus server*, then check the **Enable Modbus server** checkbox.

COM port parameter:

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits parameters:

Allow to set the bit rate and the format of the asynchronous serial link.

Modbus protocol parameter:

Select RTU (hexa) or ASCII.

Enable proxy/cache function parameter:

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 parameter:

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

Inter-character time parameter:

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

Modbus slave address parameter:

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 parameter:

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

Slave response timeout parameter:

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

TCP port parameter:

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

Local reiteration count parameter:

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

18.2. Raw TCP

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 Telecom gateway or a PC including a software TCP server.

Table 3. Raw TCP client gateway
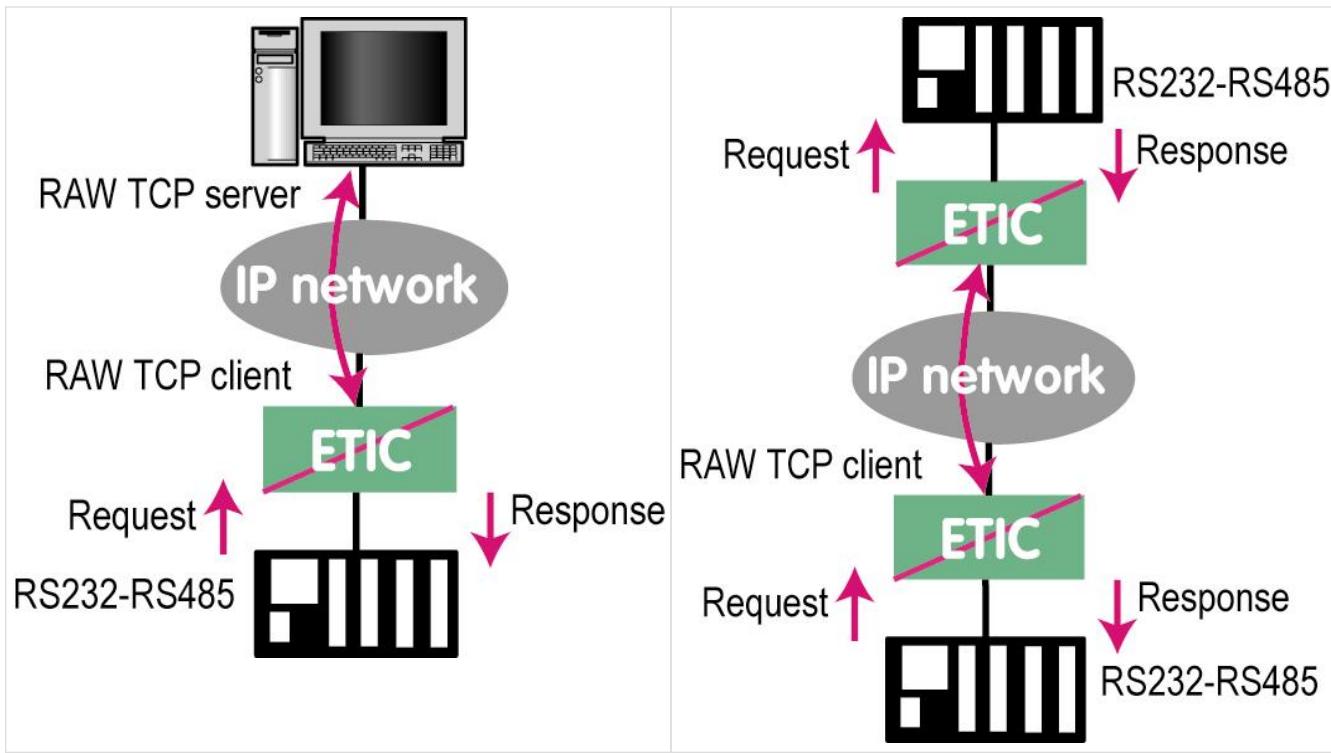
To configure the raw client gateway select *Setup > Gateways > IP-RS > Transparent > Raw client COMx*, then check the **Enable** checkbox.

Bitrate, Parity, Data, stop bits parameters:

Allow to set the bit rate and the format of the asynchronous serial link.

Receive buffer size parameter:

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

RS end frame timeout parameter:

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

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

TCP idle Timeout parameter:

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

TCP port parameter:

Set the port number the gateway has to use.

| CAUTION	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 parameter:

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.

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).

Table 4. Raw server gateway
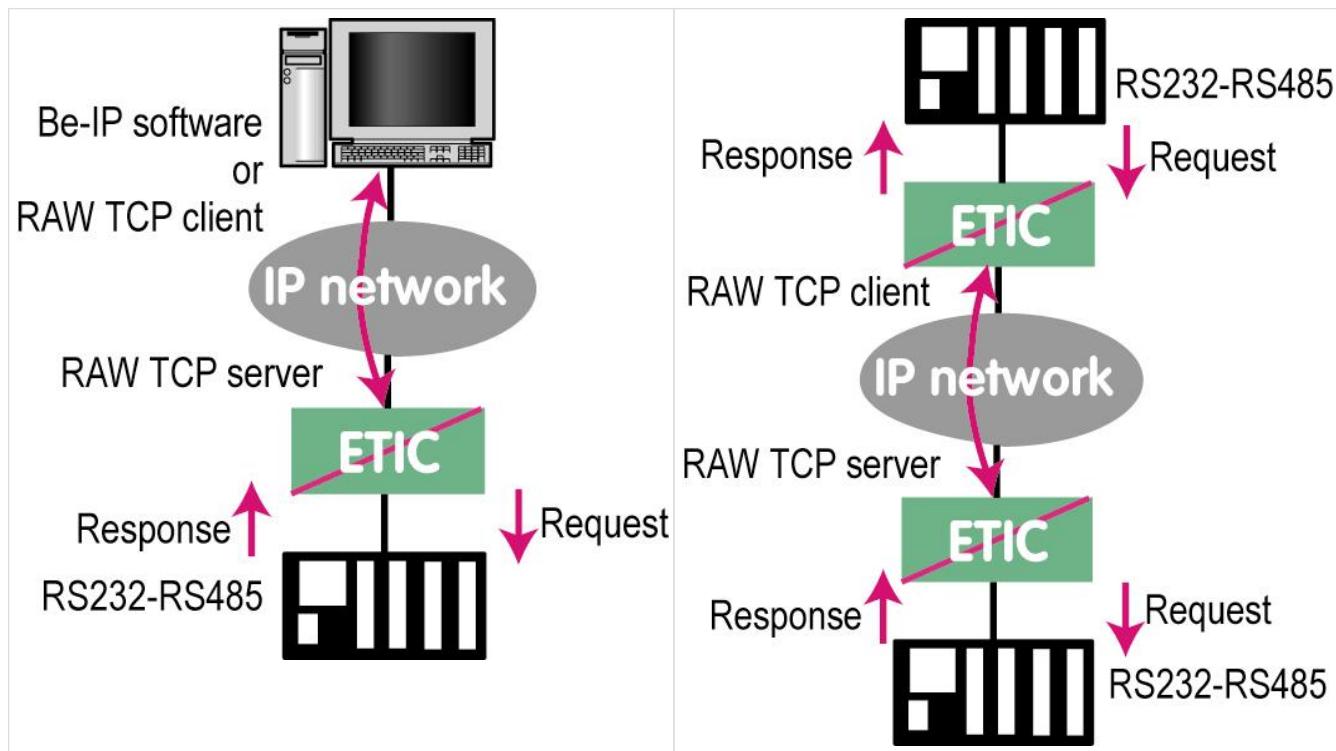
To configure the raw gateway server select *Setup > Gateways > IP-RS > Transparent > Raw server COMx*, then check the **Enable** checkbox.

Bitrate, Parity, Data, stop bits parameters:

Allow to set the bit rate and the format of the asynchronous serial link.

Receive buffer size parameter:

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

RS end frame timeout parameter:

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

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

TCP idle Timeout parameter:

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

TCP port parameter:

Set the port number the gateway has to use.

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

18.3. Raw UDP

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.
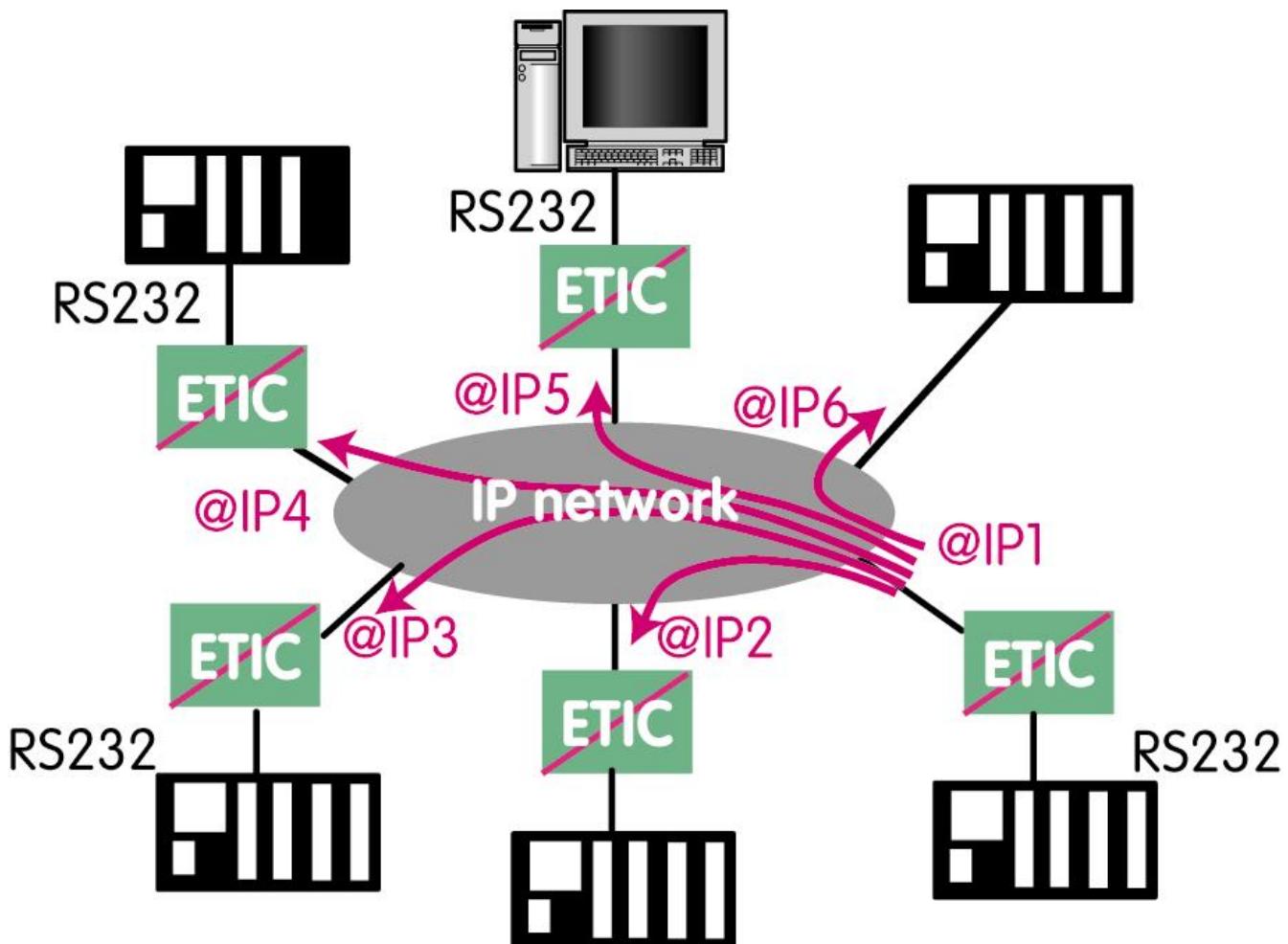

Figure 24. Raw UDP gateway

Select ***Setup > Gateways > IP-RS > Transparent > Raw UDP COMx***, then check the **Enable**

Modbus client checkbox.

Bitrate, Parity, Data, stop bits parameters:

Allow to set the bit rate and the format of the asynchronous serial link.

Receive buffer size parameter:

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

RS end frame timeout parameter:

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

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

UDP port parameter:

Set the port number the gateway has to use.

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

Destination parameter:

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.

18.4. Raw multicast

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.
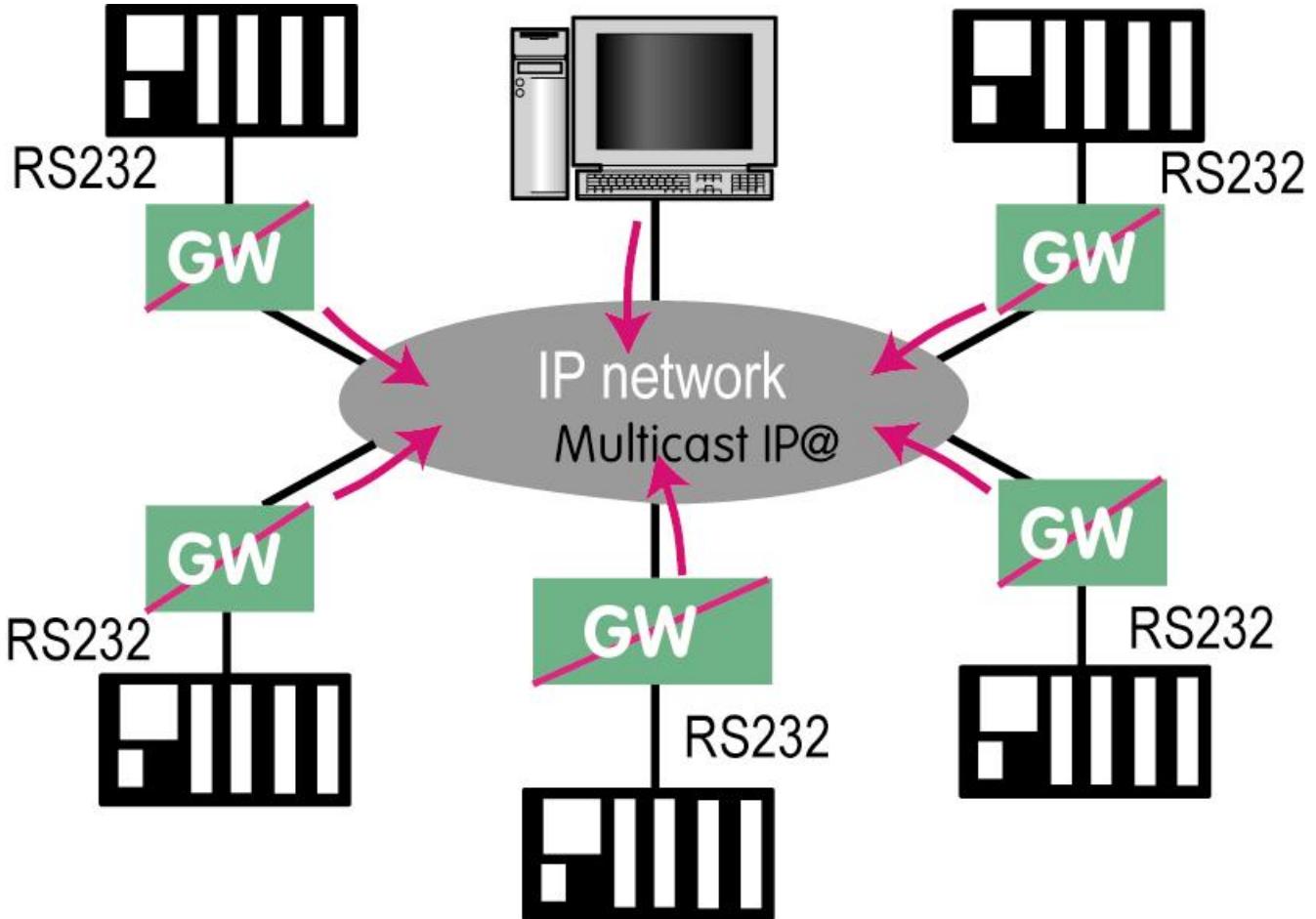
Figure 25. Raw multicast gateway

Configure the gateway

Select *Setup > Gateways > IP-RS > Transparent > Raw Multicast COMx*, then check the **Enable** checkbox.

Bitrate, Parity, Data, stop bits parameters:

Allow to set the bit rate and the format of the asynchronous serial link.

Receive buffer size parameter:

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

RS end frame timeout parameter:

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

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

UDP port parameter:

Set the port number the gateway has to use.

CAUTION	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 parameter:

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

18.5. Unitelway

The Unitelway gateway is used to connect an 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.
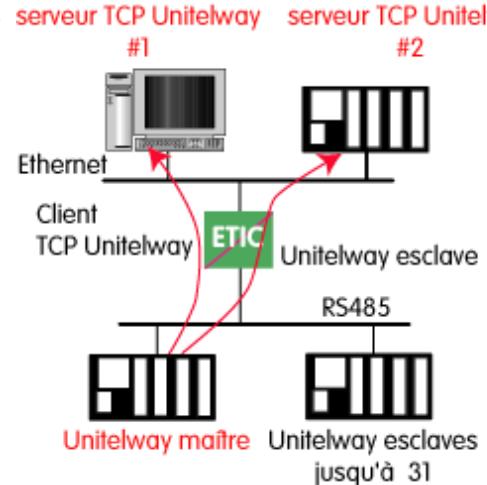
Figure 26. Unitelway gateway

Configure the gateway

Select *Setup > Gateways > IP-RS > Unitelway*, then check the **Enable** checkbox.

COM port parameter:

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits parameters:

Allow to set the bit rate and the format of the asynchronous serial link.

Xway address parameter:

Gateway address in the Xway network.

TCP idle Timeout parameter:

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

Unitelway slaves parameter:

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

18.6. Telnet

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.

Configure the gateway

Select *Setup > Gateways > IP-RS > Telnet*, then check the **Enable** checkbox.

COM port parameter:

Select the serial link 1 or 2 of the product.

Bitrate, Parity, Data, stop bits parameters:

Allow to set the bit rate and the format of the asynchronous serial link.

TCP idle Timeout parameter:

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

TCP port parameter:

Set the port number the gateway has to use.

18.7. USB

USB Gateway

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.
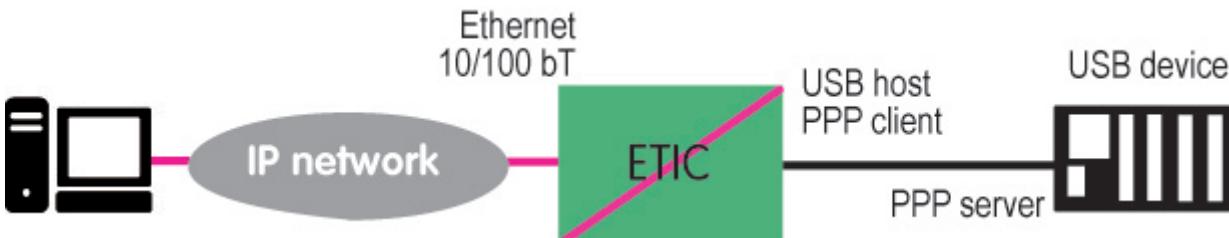

Figure 27. USB Gateway

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.

Setup

Select *Setup > Gateways > USB*, then check the **Enable** 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 it 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.

19. DIAGNOSTICS

While configuring your product, you might need to troubleshoot to be sure your configuration is working. Some tools are available in the administration interface to help you do that.

19.1. Logs

Select the menu *Diagnostics > Logs*

Main	Main events of the system, like the startup and connection/disconnection of users
OpenVPN & IPSec	Logs about VPNs to record details and timestamps of events relating VPN connections and disconnections
Firewall	Details of packets which are meant to be logged (see Firewall section)
Advanced	Permits to filter logs according to some functions to locate problems more easily

19.2. Network status

Select the menu *Diagnostics > Network status*

Interfaces	Status of your WAN/LAN interfaces and active DNS. You can get information about the different priorities, data rates, attenuation, delays, SNR, … of each interface when available ADSL Modem Status field: • Connected: The ADSL modem is connected • Showtime tc sync: ADSL modem is connected • Full init: Connection negotiation phase • Handshake: Contact made with ATU-C (DSLAM), ATU-C detected • Silent: No ATU-C detected • Idle: Modem ready, no ATU-C detected • Exception: The modem was connected, an error (cable unplugged in general) caused a disconnection
M2Me	Status of the connection of the router to the M2Me service
Remote Users	Currently connected operators list
VPN Connections	Status of your OpenVPN/IPSec VPN (Which are connected, since when…)
Routes	ARP table, the routing and extended routing table of your router
Active DHCP leases	A table that shows current DHCP leases. Each line corresponds to a lease: Client Hostname, MAC address, allocated IP address and the expiration date of the lease

19.3. Statistics

Select the menu *Diagnostics > Statistics*

ADSL bins	Usage of the bins of the ADSL modem
ADSL statistics	Get the upstream/downstream/connection error history of the ADSL connection
Cellular	Logs of Cell ID (CID) / Signal quality (SQ) / Signal Noise Ratio (SNR) / Bytes received / Bytes sent
Cellular datas	Logs of the Total of the bytes received and sent

19.4. Tools

Select the menu *Diagnostics > Tools*

Ping	Enter the ping destination IP address	
Wi-Fi scanning	The Wi-Fi scanner displays information about available Wi-Fi networks: MAC address of the access point / SSID / Reception level (dBm) / Channel number	
	NOTE	The Wi-Fi scanner can only work if the Wi-Fi interface is registered as a <u>Wi-Fi client</u> (and not as a Wi-Fi access point)

19.5. Hardware

Select the menu *Diagnostics > Hardware*

Input/Output	Check the status of the digital input/output. Control the status of the digital output
Hardware monitoring	Monitor power supplies voltage and internal temperature

19.6. GPS

Select the menu *Diagnostics > GPS*

Get the available GPS status and information.

19.7. Gateway status

Select the menu *Diagnostics > Gateway status*

This page is used to display the current status of the gateway settings, the number of bytes and frames exchanged and the number of error frames.

The **Serial data visualisation** menu allows you to display the RX and TX traffic on the serial link.

19.8. Advanced diagnostic

This section is intended for the Hotline service of Etic Telecom when problems are particularly difficult to analyze with other tools.

19.9. 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.

19.10. SSH commands

Useful commands

If you access SSH with the Super Administrator "*admin*", you can access some useful linux commands for network diagnostics.

Command	Description
ifconfig	Show used ip addresses (You can't change ip addresses)
route	Show routes of the router (You can't add routes)
ping	Ping some devices
traceroute	Determine the path taken by packets
iperf	Test network performances
tcpdump	Analyze packets

20. MAINTENANCE

Configurations management	Save/restore a configuration, upload a configuration or return to factory configuration.
Firmware updat	Check the available updates and update the firmware
Software option	Add software options to the router
Notepad	Keep track of changes that have been made on the router
Reboot	Force a router reboot
Parameters Error	Summary of parameters errors on the current configuration

20.1. Configurations management

Product configurations can be saved and loaded.
All parameters are concerned except the Certificate Store:

CAUTION	Values of certificates, private keys and CRLs aren't saved in configuration files, but parameters that point to them are still there. You need to add certificates and private keys in the product's certificate store before importing the configuration file.

Go to the *Maintenance > Configurations management* menu.

Save a configuration

To save a configuration, choose a name in the **Configuration name** field and click on **Save** button.

Load a configuration

NOTE	`Super Administrator` only

Select a configuration from the configuration list, then click on **Load**.
The product will apply the whole saved configuration. When the green LED stops to blink, the product is fully reconfigured.

Edition mode

This mode is useful to check what a configuration contains. Or to set a batch of parameters without having the product to reconfigure every parameter.

By clicking on **Edit** instead of **Load**, the configuration will be displayed, but not applied. <mark>Edition mode</mark> is enabled and modifications can be done to the configuration.

You can decide to **Apply** the configuration, or **Cancel** it.

Export a configuration

> **NOTE** | `Super Administrator` only

Select a configuration from the configuration list, then click on **Export to PC**.

The configuration may contain passwords that should be encrypted. Fill the popup with a password to encrypt these values. If left blank, passwords will be in clear text in the exported file.

> **WARNING** | Encryption password will be asked if you import that configuration later on

Import a configuration

> **NOTE** | `Super Administrator` only

To import a configuration from your computer:

1. Fill the **Configuration name** to be saved in the product
2. Provide the **Decryption key for secrets** if you encrypt passwords during the export phase
3. Select the file from your computer by clicking the **File to import** button

20.2. Firmware update

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

If the firmware update operation does 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. Unless you specified a specific configuration to apply.

Go to the *Maintenance > Firmware update* menu.

Upgrade using a local file

If the update file to update the firmware is located on your computer, you can:

1. Click the **Upgrade using an update file** button and select the firmware archive,
2. Click **Upgrade now**.

Internet update

Automatically search on internet for the latest firmware version of your product :

1. Click the **Get available updates** button,

2. Click **Upgrade** for the update you want to install.

Apply a configuration post-update

NOTE	`Super Administrator` only

In case of firmware downgrade, the actual configuration may not be valid with a previous version.

A configuration file can be specified to be applied after the product upgrade its firmware.
Available configuration files from the *Maintenance > Configurations management* menu are displayed in the list.
Version of the configuration is displayed for each of them.

CAUTION	Make sure you chose a configuration with a lower or equal version of the firmware you are installing.

21. HOTLINE SUPPORT AUTHENTICATION

The Etic Telecom hotline can not access your product without your consent.

When requiring assistance from the Etic Telecom hotline support, you have to perform one of these two operations to allow the team to access your product:

- Provide a password generated from the administration page

- Push a button on the rear side of your product

| WARNING | We highly recommend you to generate a remote access password in advance. |

21.1. Remote access password generation for Etic Telecom support

In the *Setup > Security > Administration rights* menu.

Generate new hotline password button:

Generate a new password and display it. It will be displayed only once, but you can reset a new password anytime.
If you communicate it with the Etic Telecom hotline team, we recommend you to reset a new password after they finished the support.

21.2. Front button

In case you did no save your password for Etic Telecom hotline team, you can allow the access by holding the front button for 10seconds.
The support team can now access your product for one hour, or until it restarts.

You can disable that functionality in *Setup > Security > Administration rights* menu and selecting **Disable push button for Etic Telecom hotline remote access**.

22. HOTLINE SUPPORT AND VIRTUAL SHOWROOM

22.1. Hotline support

Feel free to contact +33 4 76 04 20 05 or hotline@etictelecom.com

22.2. Virtual showroom

By surfing on our WEB site www.etictelecom.com (Support/Virtual Showroom) you can learn how to configure a Machine Access Box (namely a RAS product).
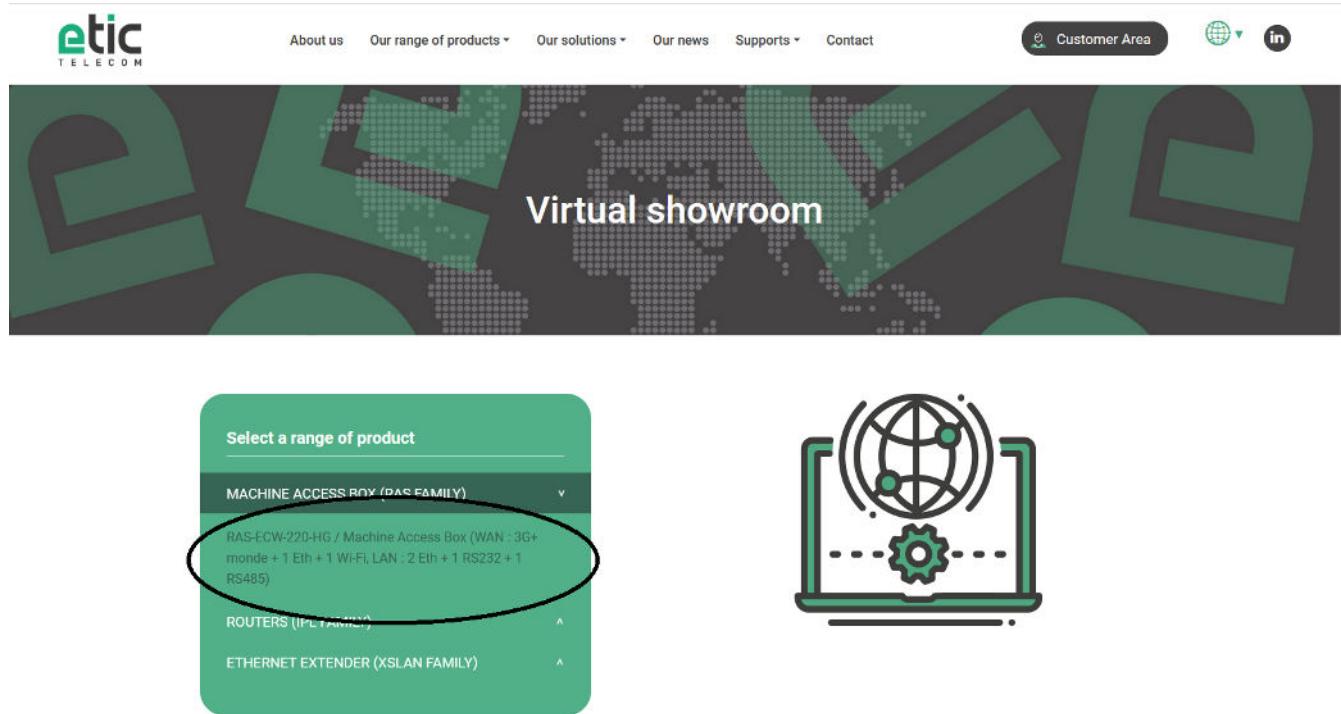
Figure 28. Access to Virtual showroom