RAS/IPL/SIG Setup guide firmware 4.13.4

This documentation is also available in web version at
doc.etictelecom.com

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 Firewall 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

Enable ADSL	Permits to enable or disable the ADLS interface
Modulation	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	Range is `0 - 4095`. Leave the default value (8)
Virtual Channel Identifier	Range is `0 - 65535`. Leave the default value (35)
Multiplexing	Value `LLC` or `VC`. Leave the default value (LLC)
Encapsulation	• `PPPoE` : PPP over Ethernet • `PPPoA` : PPP over ATM • `EoA` : Ethernet over ATM, RFC1483/RFC2684 Bridged • `IPoA` : IP over ATM A set of IP parameters is associated with each of these encapsulation solutions (see the next paragraph).

ADSL WAN IP configuration

IP configuration of the ADSL line depends on

1.1. ADSL

	PPPoE	PPPoA	EoA	IPoA
ADSL WAN priority 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 & **PPP password**: Enter the ADSL account values.	✔	✔		
PPPoE service name 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, **IP address** & **Remote IP address** 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.	✔	✔	✔	✔
Obtain DNS servers addresses automatically, **Primary DNS IP address** & **secondary DNS IP address** 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 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 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

Enabled	Enable or disable cellular interface
Cellular interface priority	That parameter defines the priority of the path when more than one path is selected (Cellular & Ethernet WAN, for instance). The router will use first the interface having received the highest priority; the other interface will be used as a backup path.
SIM card	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
Interface MTU (Advanced parameters)	Maximum Transfer Unit, control the largest data packet that can be transferred without fragmentation

Cellular traffic counter

Reinit day	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***

Data sharing with Etic license server

SIMSend ICCID	Shares the ICCID of the SIM card to the Etic license server. This option must be activated if you wish to be able to view the data consumption of your EticSIM in your customer area.

SMS commands

Some SMS texts sent to the router act as commands and trigger actions on the router. Only users with their phone number registered in the router can trigger these commands.

These commands are listed in the table below.

`M2ME ON`	Enable the M2Me connection
`M2ME OFF`	Disable the M2Me connection
`CELL ON`	Connect cellular data
`CELL OFF`	Disconnect cellular data
`DOUT ON`	Set digital output to ON (1)
`DOUT OFF`	Set digital output to OFF (0)
`ACK XXXX`	Acknowledge the alarm with the identifier XXXX
`PING`	Sends back "PONG" to the emitter
`REBOOT`	Reboot the router

NOTE These commands are not case sensitive, i.e. `M2ME ON` will have the same effect as `m2me on`

Mobile service provider connection

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

SIM : Modem configuration

Access Point Name (APN)	Enter the label of the gateway (APN) to the Internet - or to other services - provided by the mobile service provider.
SIM PIN code	Enter the SIM card pin code. As long as the PIN code has not been correctly entered, the OPERATION LED indicator flashes (red colour).
Network type	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**:	Enter the login and password of the subscription. That parameters are generally not required.
Authentication with PAP only	Enable if you required PAP authentication
Obtain an IP address automatically	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.
Select an operator	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".

Paremeters shared with both SIM

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

Enable address translation (NAT)	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.

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.

Upon power-up, Network 1 is tested first.

If the Network 1 remains in failure during the period of time T1, the Router switches to the network 2.
If Network 2 functions correctly, the router uses this cellular network for at least period T3.
At the end of this period, the router returns to Network 1 and checks its availability. If it is unavailable, the router continues to use Network 2.
At any time, if Network 2 fails to function correctly during time period T2, the router switches back to Network 1.

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

The time periods T1, T2, and T3 can be configured.

We recommend not selecting small values for the T1, T2, and T3 parameters:

Example 1. Sim card switching timing

T1 - Max SIM1 disconnection time before switching = 20 mn
T2 - Max SIM2 disconnection time before switching = 20 mn
T3 - SIM2 connection time before retesting SIM1 = 12 hours

SIM backup timings

Max SIM1 unconnected time before switching	See above. Possible values: 5, 10, 20, 30, 60 mn
Max SIM2 unconnected time before switching	See above. Possible values: 5, 10, 20, 30, 60 mn
Try SIM1 again after	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 is able to check periodically 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.

Enable ping control	Enable or disable the PING control function
IP address or Hostname to ping:	IP address or the Hostname of the machine to which the Router will send a periodic ICMP message (PING)
Ping interval	Period between two consecutive pings
Ping retries	Enter the number of retries before resetting the PPP connection.

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 in Half or Full duplex. By default, the value `Autonegotiation` is used, which allows the interface to adapt the flow rate according to the equipment connected to this WAN.

IP configuration of the Ethernet WAN port

Connection type	• The `Ethernet` value is the default value. It must be selected when another router connected to the Ethernet/WAN interface of the Etic Telecom router is in charge of routing IP frames to the Internet • The[.etic-param-value]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. • The `Unused` value permits to disable this port.

WAN Interface

Choice	Ethernet	PPPoE
Ethernet WAN priority 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 and **PPP password** parameters: Enter the login and password of the PPP connection		✔
Obtain an IP address automatically, **IP address**, **Netmask** & **Gateway** 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.	✔	

Choice	Ethernet	PPPoE
Obtain the DNS server IP address automatically, **Primary DNS server** & **Secondary DNS server** 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 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.	✔	
Enable address translation NAT 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, ...)	✔	✔
Enable proxy ARP The router acts as an ARP proxy. Leave that checkbox unselected	✔	
Interface MTU Maximum Transfer Unit, controls the largest data packet that can be transferred without fragmentation, 1500 by default	✔	
Only 1 WAN connected at same time Checkboxto have only 1 WAN connected at same time	✔	✔

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 **Enable Wi-Fi WAN** checkbox.

Connection profiles

A board contains the different connection profiles to which the router can connect.

Enable	Permits to enable or disable a connection profile
Scan available networks	A `Scan`button allows you to obtain the list of SSIDs seen by the product as well as the signal level in dBm for each of them.
Network name (SSID)	Enter the name assigned to the Wi-Fi network to which the Router has to connect. **IMPORTANT** The SSID is case-sensitive
Authentification	Select WPA or WEP or None according to the access point configuration.
Key	Enter the WPA or WEP key according to the access point configuration.

Wi-Fi WAN IP configuration

WiFi WAN priority	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.

Obtain an IP address automatically, **IP address**, **Netmask** & **Gateway**	Leave this box checked 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 DNS servers addresses automatically, **Primary DNS server** & **Secondary DNS server**	Leave that checkbox selected if the DNS servers IP addresses are assigned by a DHCP server. Otherwise, Uncheck this box and enter the IP addresses of the DNS servers.
Enable address translation (NAT)	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** Check this box if a device on the LAN interface should establish a connection with a device connected to the Internet (FTP server, ...)
Enable proxy ARP	The router acts as an ARP proxy. Leave this option unselected
Enable only when the digital input is ON	Starts the Wi-Fi WAN when the Input is on rising edge (→ON).

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.

WARNING 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 & **IP 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	

IMPORTANT

Be careful with IP addresses used by the LAN interface when configuring VPNs.

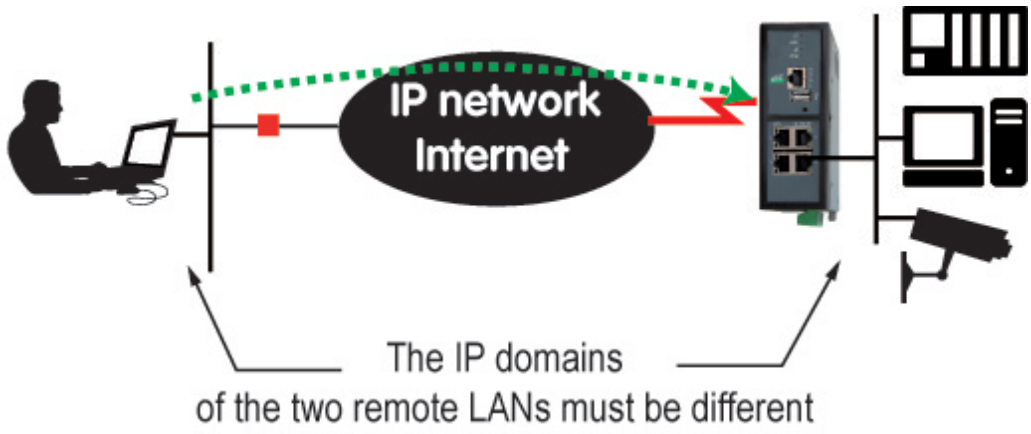


Figure 1. Case 1: Remote users connection

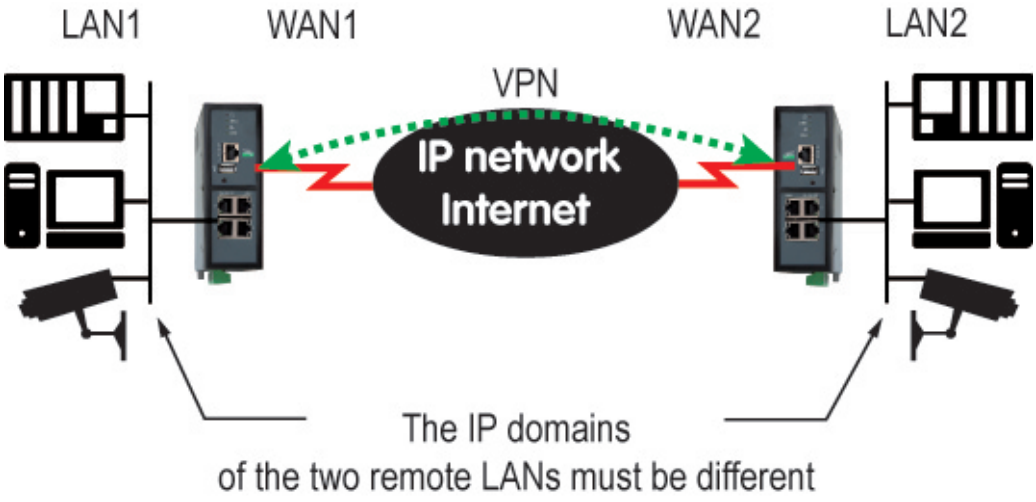


Figure 2. Case 2: VPN set between 2 routers

Advanced parameters

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 **NOTE** 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
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***

DHCP configuration

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

DHCP MAC-IP bindings

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. REMOTE ACCESS

Providing a secure remote access service requires three steps:

1. The remote connection setup
2. Create a user
3. Create an operator with its access rights

3.1. 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.

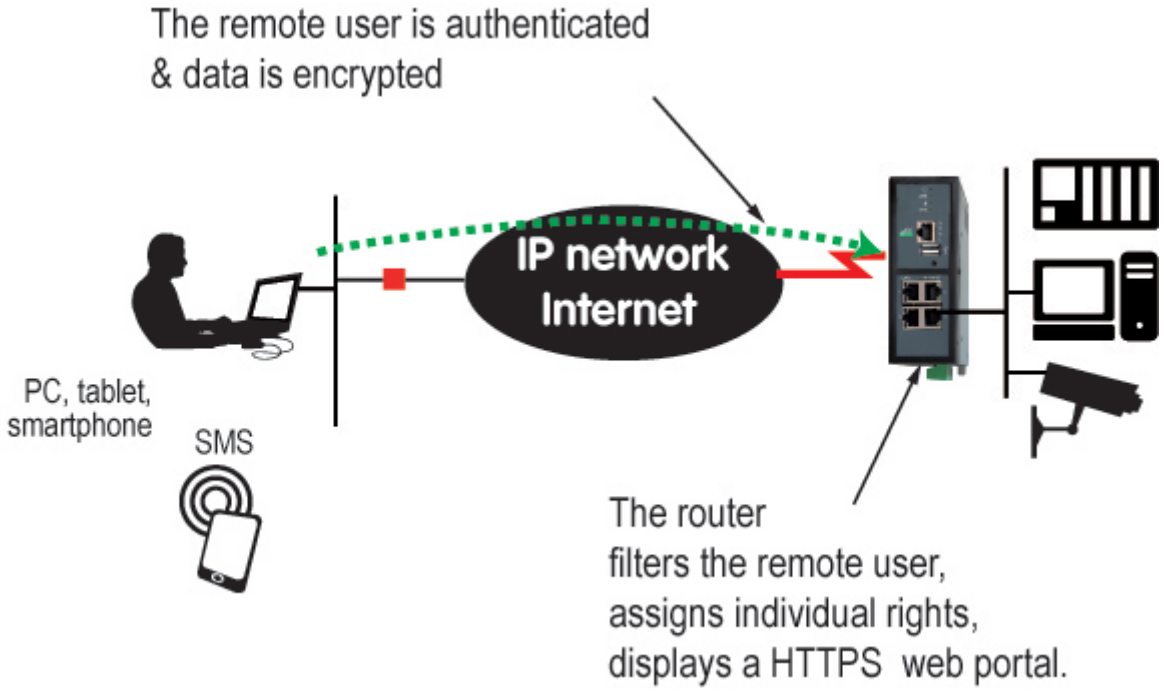


Figure 3. Remote access data encryption

PC, Tablet, smartphone

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

3.2. Remote access connections types

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

	Remote user Authentication	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, their identity is checked (Login/Password).

3.3. 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.

Purpose of M2Me_Connect

The M2Me_Connect service simplifies the connection of a remote PC to a machine through the Internet. It provides a solution when a direct PPTP or OpenVPN connection is impossible.

Let us take the example of a machine made of several devices forming a “machine network” and connected to a company network through a router. Suppose that an expert wishes to connect to one or several of these devices to help repairing them or to upgrade a firmware.

The simplest solution should be to set a remote connection between the remote PC and the router through the company network, the existing Internet access in the company, and the Internet.

Several reasons make that connection difficult or impossible, but the main one is a security reason: It is generally not allowed to set an ingoing connection from a PC connected to the Internet towards a device like a router connected inside a company network.

The M2Me_Connect service solves that difficulty:

- The PC does not connect directly to the router; both the PC and the router connect to the “M2Me_Connect” service.
- Once both parties have been authenticated by the M2Me_Connect service with their own certificate, a OpenVPN VPN is set from end to end from the PC to the router.
- The remote user identity is checked by the router to verify he or she belongs to the user list stored in the router.
- Finally, individual access rights are assigned to the remote user depending on their identity.

Figure 4. M2Me VPNs

The VPN can be transported in UDP or TCP.

NOTE	Once the M2Me connection is started, the M2Me LED flashes on the router.
IMPORTANT	The Product Key of the router is required by the M2Me software of the remote PC. Don’t forget to copy it from the menu ***About***.

Setup M2Me connection

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

1. Carry out the M2Me connection setup described below
2. Create at least one user in the menu ***Setup*** > ***Security*** > ***Users***
3. Register at least one operator in the menu ***Setup*** > ***Remote access*** > ***Operator list*** and assign access rights for the operator(s)

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

Connection to M2Me_Connect service

Check the **Enabled** parameter to activate the M2Me connection settings.

UDP and **TCP ports**	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.
Direct access to the Internet (no proxy)	If a proxy server filters outgoing connections, unselect the checkbox and enter the Proxy server parameters
Proxy type	Proxy type of the server (`HTTP`, `SOCKS5`)
Address and **Port**	Proxy IP address and port
Authentication	Type of Proxy authentication (`None`, `Basic`, `NTLM`) if the proxy is `HTTP`
Connect at power on	To connect automatically to M2Me network at power on
Connect when the digital input is ON	Connect to M2Me network only when digital input is ON
Connect now	If the router doesn't connect automatically, push this button to connect to M2Me network

End-to-end connection from M2Me PC client

Configuration used when the end user uses a computer.

Users authentication	`Login/Password` or `Login/Password + Certificate`, refer to Multi-factor authentication for more details
Use the factory certificate	Use the factory certificate for the end-to-end M2Me connection
Choose a custom certificate	Certificate used for the end-to-end M2Me connection

End-to-end connection from M2Me Smartphone client

Configuration used when the end user uses a smartphone or a tablet.

Users authentication	`Login/Password` or `Login/Password + Certificate`, refer to Multi-factor authentication for more details
Use the factory certificate	Use the factory certificate for the end-to-end M2Me connection

Choose a custom certificate	Certificate used for the end-to-end M2Me connection

3.4. 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 **WARNING** 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
Use TLSv1	Use TLS version 1. This version should only be used for compatibility with old devices. TLS version is 1.2 minimum if it's unchecked.
Users authentication	**Login/password** or **Login/password & certificate**, refer to Multi-factor authentication for more details
Use the factory certificate	Use the factory certificate
Choose a custom certificate	Use one of your custom certificates

3.5. 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 **WARNING** 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
Use TLSv1	Use TLS version 1. This version should only be used for compatibility with old devices. TLS version is 1.2 minimum if it's unchecked.
Users authentication	**Login/password** or **Login/password & certificate**, refer to Multi-factor authentication for more details
Use the factory certificate	Use the factory certificate
Choose a custom certificate	Use one of your custom certificates

3.6. 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.

3.7. Multi-factor authentication

When authenticating operators, the router checks login and password, but can also check other

parameters to have a multi-factor authentication (MFA).

Login / Password + Certificate

For the authentication with login, password and certificate, the certificate of the user is checked following these steps:

1. First, it checks if the operator has a certificate CN (common name) in its user description
2. If there is a CN specified for this operator, the incoming certificate must have the specified CN, otherwise the operator is rejected
3. If there is no CN specified for this operator, it will check in the `Authorized certificate list` (see chapter below), the incoming certificate CN must be present in the list, if it isn't, the operator is rejected

Authorized certificate list

In the screen ***Setup > Remote access > Operator list***

Active	Enable or disable a certificate
Authorized CN	Common name of a certificate owned by an operator *Example 5. Common name* my_cert_cn
Comment	Comment to know what this certificate corresponds to

4. USERS

Two types of users can access the router:

- `Operators` who needs access rights to the network
- `Administrators` who configures the Router

Both of them are linked to a `User`.

4.1. User management

The router has a user management mechanism. A user is a physical person who needs to access the device, regardless if it's to configure it, or to access through it.

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

4.2. Create a User

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

Active	Enable or disable a user
Full name	(Optional) Full name of the person
Company	(Optional) Company to which it belongs
E-mail address	(Optional) E-mail address, can be useful for Collect&Alert purposes
Phone number	(Optional) Phone number in international format, can be useful for Collect&Alert purposes *Example 6. Phone number* +33611223344
CN of the user certificate	(Optional) CN of the certificate with which this user must connect to be accepted for remote connections. Leave blank if none. Refer to Multi-factor authentication for more details
User name	Login of the user, used for authentication. It must be unique, no username can be used twice
Password	Password of the user, must have a valid strength.

4.3. Operators and access rights

An operator is an `User` who needs to access the LAN network via 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.

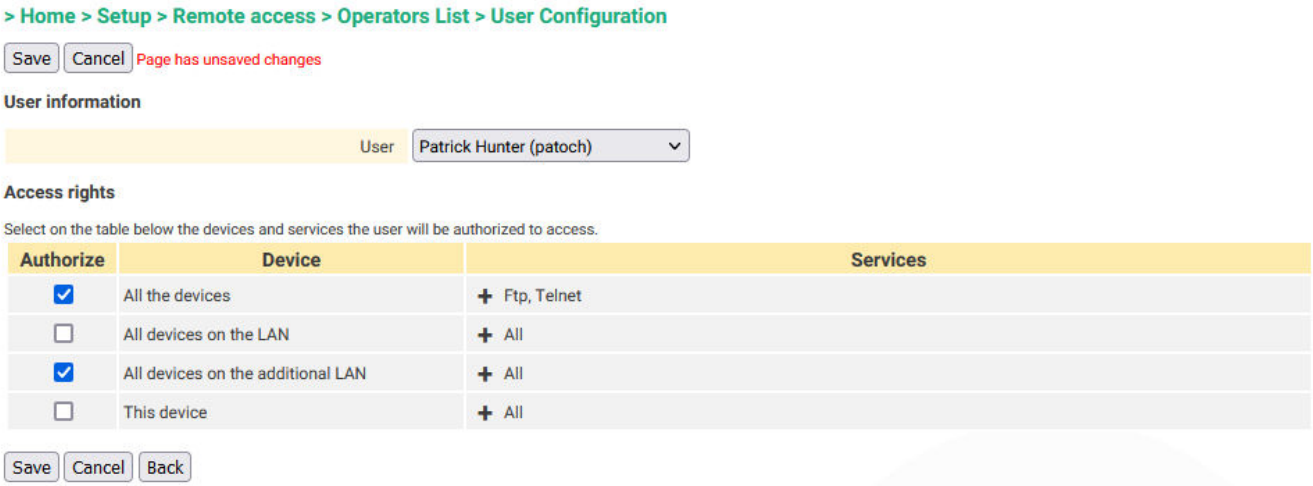


Figure 5. Operator creation screen

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

4.4. Administrators and roles

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

To protect the administration 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.

Figure 6. 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 administrator
- Remote management administrator
- Network administrator
- System administrator
- 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 administrator

- User management
- Remote access user list management
- Remote access rules management
- User creation
- Edition/deletion of users that are not linked to an administrator
- Can edit its own personal information, except the user name
- Network interfaces and M2Me connection diagnostic
- Save locally the current configuration

Remote management administrator

Same as Remote access administrator +

- Datalogger management
- Collect & Alert management

Network administrator

Same as Remote access administrator +

- Access all logs in read only except the audit trail
- Configuration and diagnostic network interfaces:
  - WAN
  - LAN
  - Remote access servers
  - VPNs (IPSec and OpenVPN)
  - Static routes
  - VRRP / RIP
  - Firewall / port forwarding / NAT / NAT 1:1
  - Dynamic DNS
  - Gateways
  - SMS / emails
- Certificate store
- Ping tool

System administrator

Same as Network administrator +

- Access and delete all logs (except the audit trail in read only)
- Configuration and diagnostic of:
  - Date/Time management
  - Periodical reboot
  - Remote Syslog
  - SNMP
  - ModBus / OPCUA server
  - GPS
- Software options
- Reboot
- Advanced diagnostics

Super administrator

Same as System administrator + Remote management administrator +

- Delegated authentication management
- Administrator and auditor management
- Full user list management
- Full configuration management: export, import, save, load, ...
- Update firmware

Auditor

- Access all logs in read only
- Can edit its own personal information, except the user name

5. USER INTERFACES

Several interfaces are available on the product to allow a user to interact with it.

These can be administrative interfaces to configure the product, or operations so that an operator can use certain features of the product.

5.1. Administration web page

The administration web page allows administrators to configure the product and its features.

Configuration

This web server can also be configured, go to page > ***Home*** > ***Setup*** > ***Security*** > ***Administration rights*** to configure it.

Password protect the configuration interface	Use an account with login/password to access the administration web page. `True` by default
Protocols to use for configuration	`HTTP only`, `HTTPS only` or `HTTP and HTTPS`. It is recommended to use `HTTPS only`
HTTPS port for administration (4433)	TCP port used for the administration web server. This is 4433 by default
Port TCP 80 redirects to Administration Area	When the WEB portal and application server are disabled, this checkbox allows you to redirect requests on port 80 to the HTTP or HTTPS administration port.
Use the factory self-signed certificate	Use a self-signed certificate for the web server. `True` by default
Choose a custom certificate	Use one of your custom certificates
Enable access via EticNet (HTTPS only)	Allows access to the web page via EticNet. `False` by default
Enable access from the WAN (HTTPS only)	Allows access to the web page from WAN interfaces. `False` by default

The web page works with sessions, if a logged in user remains inactive for 10 minutes, they are automatically logged out of the web page.

WARNING	When changing the administration web server certificate, your browser will likely block access and display a blank page. To apply the new certificate, please refresh the page and your browser's cache (kbd:[Ctrl+F5] in most browsers). If you are using the self-signed certificate, after a factory reset, the web server certificate will be renewed with a new one.

5.2. Operation web page

This HTTPS server can act as an HTTPS to HTTP gateway to provide secure remote access to HTML/HTTP(S) pages of devices on the LAN.

You must first create operators before you can access this page.

The operations web page allows operators to access the list of HTML servers they are authorized to access, as well as the Collect&Alert variables if the product is equipped with it. If the operator remains inactive for 10 minutes, they are automatically disconnected from the web page.

Configuration

This web server can also be configured, go to > ***Home*** > ***Setup*** > ***Remote Access*** > ***Remote access servers*** to configure it. The server runs on TCP port 443.

Enable HTTPS application server	Allows you to enable/disable the web server. `False` by default
Access HTTPS application server from the WAN	Allows access to the application server via WAN interfaces. `False` by default
HTTPS Application server accessible via EticNet	Allows access to the application server via EticNet. `True` by default **IMPORTANT** This option must be enabled to allow connection from the smartphone application.
Use the factory self-signed certificate	Use a self-signed certificate for the server. We recommend unchecking this box and using one of your own certificates. `True` by default
Choose a custom certificate	Use one of your custom certificates

WARNING

When changing the application web server certificate, your browser will likely block access and display a blank page. To apply the new certificate, please refresh the page and your browser's cache (kbd:[Ctrl+F5] in most browsers).

If you are using the self-signed certificate, after a factory reset, the web server certificate will be renewed with a new one.

Access the operating portal through M2Me by Smartphone

To facilitate access to equipment and other pages from the M2Me Smartphone application, it is possible to configure a list of links that will be directly available after connection.

Go to page > ***Home*** > ***Setup*** > ***LAN Interface*** > ***WEB portal***, and enable the option **Show web**

portal.

Then create links:

Nom	Name that will be displayed in the web portal
URL	URL associated with the link

By clicking on the link, you will be redirected directly to the configured URL.

For example, you can specify the Collect & Alert page. This way, on the smartphone application, you will have a link that will redirect you directly to the synaptics page, where you can read and write the variables of the configured PLCs.

5.3. SSH command line interface

The product provides an SSH server to allow administrators to manage the product and its features. To configure it, go to the page > ***Home*** > ***Setup*** > ***Security*** > ***Administration rights***

Enable SSH server	Enable/disable SSH server `True` by default
SSH public key (for passwordless login)	Public key for SSH authentication

The server allows multiple SSH sessions to be managed, each with session IDs and keys negotiated during the key exchange phase. These are deleted at the end of a session. A session can be closed by a user using the kbd:[Ctrl+D] keys.

The server uses strong and secure cipher suites for communications.

To copy files into the product, you can use `scp` into the directory `/tmp` which is the only directory with write access. Files copied on the SSH will see their execution capabilities removed for security reasons.

List of client SSH commands

A subset of Linux commands are available, plus a set of Etic Telecom commands which will help you configure and use your device.

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

Command	Description
shdsl_dotest	Call SHDSL socrates
shdsl_pmms	Read SHDSL pmms
get_external_ssh_users	Get the list of users who have already logged in once to the SSH interface from a delegated authentication server
clear_external_ssh_users	Clear the list of users who have already logged in once to the SSH interface from a delegated authentication server
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
unban_user	Unban a banned user from authentication by the protection mechanism
simplify_hotline_remote_access	Simplify hotline remote access for an amount of 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
set_params	Set parameters in the configuration
set_first_superadmin	Set first Super Administrator
reset_hotline_passwd	Reset hotline password
config_list	List saved configurations
config_load	Load a configuration
config_save	Save a 'User' configuration

Command	Description
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
get_log	Display a log

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
```

get_external_ssh_users

```
$ get_external_ssh_users --help
get_external_ssh_users : Get the list of users who have already logged in once to the
SSH interface from a delegated authentication server

usage : get_external_ssh_users
```

clear_external_ssh_users

```
$ clear_external_ssh_users --help
clear_external_ssh_users : Clear the list of users who have already logged in once to
the SSH interface from a delegated authentication server

usage : clear_external_ssh_users
```

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> [end_upgrade] [config_file]

    fw_path : Path of the firmware archive to upgrade to
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
```

unban_user

```
$ unban_user --help
unban_user : Unban a banned user from authentication by the protection mechanism

usage : unban_user <ip>

  user            : User to unban.
```

simplify_hotline_remote_access

```
$ simplify_hotline_remote_access --help
simplify_hotline_remote_access : Simplify hotline remote access for an amount of time.
This will disable hotline password requirement, and enable remote access VPN even if
you have not defined an operator for it

usage : simplify_hotline_remote_access [nb_minutes]

 nb_minutes       : (Optionnal - Default: 60 - Range [1 - 480]) Number of minutes to
simplify hotline remote access.
```

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

```
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_first_superadmin

```
$ set_first_superadmin --help
set_first_superadmin : Set first superadmin

usage : set_first_superadmin <login> <password>

     login     : Login of the Super Administrator.
  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> [common_name] [country] [organization]
[organizational_unit] [locality] [state]

  private_key : The private key to make the CSR for
  common_name : (Optionnal) Set Common Name (CN)
      country : (Optionnal) Set Country (C)
 organization : (Optionnal) Set Organization (O)
 organizational_unit : (Optionnal) Set Organizational Unit (OU)
     locality : (Optionnal) Set Locality (L)
        state : (Optionnal) Set State (S)

# If you don't want a specific field. Leave it empty with ""
```

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,
3072, 4096])
                 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`.

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
```

get_log

```
$ get_log --help
get_log : Get a specific log

usage : get_log <type> [display] [specific_log]

         type : Log type. Possible values : user / advanced_user / audit / firewall /
vpn / m2me / charon / gsm_ext_counter_log / gsm_ext_log / gsm_counter_log / gsm_log
      display : (Optionnal - Default : all) Display the whole log or output appended
data as the file grows: all / follow
 specific_log : (Optionnal - Only for type = vpn) A pair of param. Choose between
server/client log and a configuration. Ex : server 1
```

Get the OpenVPN server 0 example

```
$ get_log vpn follow server 0
```

6. 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.

6.1. 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.

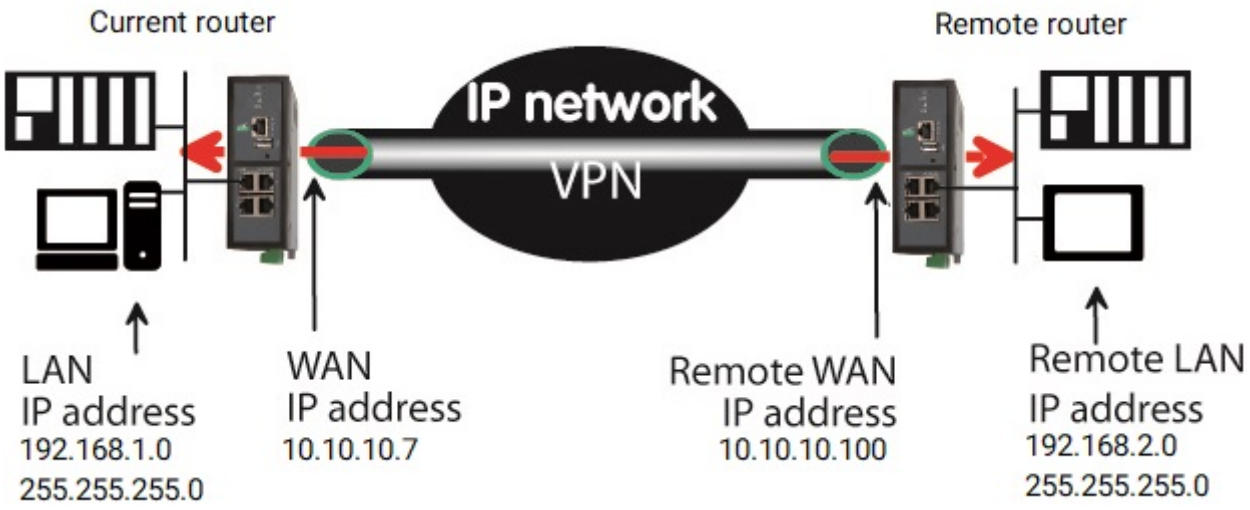


Figure 7. IPSec connection scheme

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**.

Parameter	Description
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: Static routes must be added in the Static Routes menu to go through the IPSec tunnel. The **Remote LAN Address** and **Remote LAN Netmask** fields must encompass the configured static routes.

Example 7. route-based

To associate the following 2 static routes with an IPSec node :

- 10.1.21.0/24
- 10.1.30.0/24

You can use the following IPSec configuration :

- Remote LAN address : 10.1.16.0
- Remote LAN mask : 255.255.240.0

NOTE

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

IKE Authentication - Case 1 : Use of a certificate

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

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

Parameter	Description
Use the factory certificate	Use the factory certificate
Choose a custom certificate	Use one of your custom certificates
Local IKE identity	The IKE identity must be contained in the certificate, either as the subject DN or as a subjectAltName. The identity will default to the certificate's subject DN if not specified **NOTE** IKE identity values are specified by `StrongSwan` documentation. https://docs.strongswan.org/docs/5.9/config/identityParsing.html
Remote IKE identity	The IKE identity must be contained in the remote certificate, either as the subject DN or as a subjectAltName **NOTE** IKE identity values are specified by `StrongSwan` documentation. https://docs.strongswan.org/docs/5.9/config/identityParsing.html
Certificate revocation policy	If no information about the incoming certificate revocation is available: `relaxed` will accept it, `strict` will refuse it.

IKE Authentication - Case 2 : Use of a pre-shared key

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.

Parameter	Description
Key value	Value of the key, it must be the same on the responder and initiator side.
Local IKE identity (Advanced parameters)	IKE identity to use for authentication round. Used to identify the current router **NOTE** IKE identity values are specified by `StrongSwan` documentation. https://docs.strongswan.org/docs/5.9/config/identityParsing.html
Remote IKE identity (Advanced parameters)	IKE identity to expect for authentication round. Used to identify the remote router **NOTE** IKE identity values are specified by `StrongSwan` documentation. https://docs.strongswan.org/docs/5.9/config/identityParsing.html

NOTE IKE ID type is specified by `StrongSwan` documentation. https://docs.strongswan.org/docs/5.9/config/identityParsing.html

Network section

Parameter	Description
Local LAN network (Advanced parameters)	IP address of the local LAN network. If empty, it's the LAN of the Router. This field is used for the local traffic selectors to include in the CHILD security association *Example 8. On IPSec connection scheme* 192.168.1.0

Parameter	Description
Local LAN netmask (Advanced parameters)	Netmask of the local LAN network. If empty, it's the LAN of the Router. This field is used for the local traffic selectors to include in the CHILD security association *Example 9. On IPSec connection scheme* 255.255.255.0
Remote LAN IP address	IP address of the remote LAN network. This field is used for the remote traffic selectors to include in the CHILD security association *Example 10. On IPSec connection scheme* 192.168.2.0
Remote LAN netmask	Netmask of the remote LAN network. This field is used for the remote traffic selectors to include in the CHILD security association *Example 11. 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 12. 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.

Parameter	Description
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	See the available values in the table Encryption algorithms

Parameter	Description
Authentication algorithm	See the available values in the table Authentication algorithms
DH group (Advanced parameters)	Diffie-Hellman group. See the available values in the table Diffie-Hellman groups
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.

Parameter	Description
Protocol	IPSec transport protocol. ESP ensures routers authentication and data encryption. ESP is now forced on ETIC Telecom products.
Encryption algorithm	See the available values in the table Encryption algorithms
Authentication algorithm	See the available values in the table Authentication algorithms
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. See the available values in the table Diffie-Hellman groups
Life time (Advanced parameters)	Phase 2 key lifetime

Table 1. Encryption algorithms

Algorithm	Description
Auto	AES-256-CBC and the default algorithms considered safe by `StrongSwan`
AES-256-GCM	256 bit AES-GCM with 128 bit ICV[1]
AES-256-CBC	256 bit AES-CBC
AES-192-CBC	192 bit AES-CBC
AES-128-CBC	128 bit AES-CBC

Table 2. Authentication algorithms

Algorithm	Description
Auto	SHA-256 and the default algorithms considered safe by StrongSwan
SHA-512	SHA2_512_256 HMAC (256 bit)
SHA-384	SHA2_384_192 HMAC (192 bit)
SHA-256	SHA2_256_128 HMAC (128 bit)
SHA1	SHA1 HMAC (96 bit)
MD5	MD5 HMAC (96 bit)

Table 3. Diffie-Hellman groups

Diffie-Hellman group	Description
Group 2	Modular Prime 1024 bits
Group 5	Modular Prime 1536 bits
Group 14	Modular Prime 2048 bits
Group 16	Modular Prime 4096 bits
Group 18	Modular Prime 8192 bits
Group 19	NIST Elliptic Curve 256 bits
Group 20	NIST Elliptic Curve 384 bits
Group 21	NIST Elliptic Curve 521 bits
Group 24	Modular Prime 2048 bits with Prime Order Subgroup 256 bits
Group 28	Brainpool Elliptic Curve 256 bits
Group 29	Brainpool Elliptic Curve 384 bits
Group 30	Brainpool Elliptic Curve 512 bits
Group 31	Modern Elliptic Curve 256 bits
Group 32	Modern Elliptic Curve 448 bits

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

Parameter	Description
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.

Parameter	Description
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 13. Possible values* Cellular WAN up, Cellular WAN down, Ethernet WAN up, Ethernet WAN down, TOR input ON, TOR input OFF, No VPN connected

6.2. 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

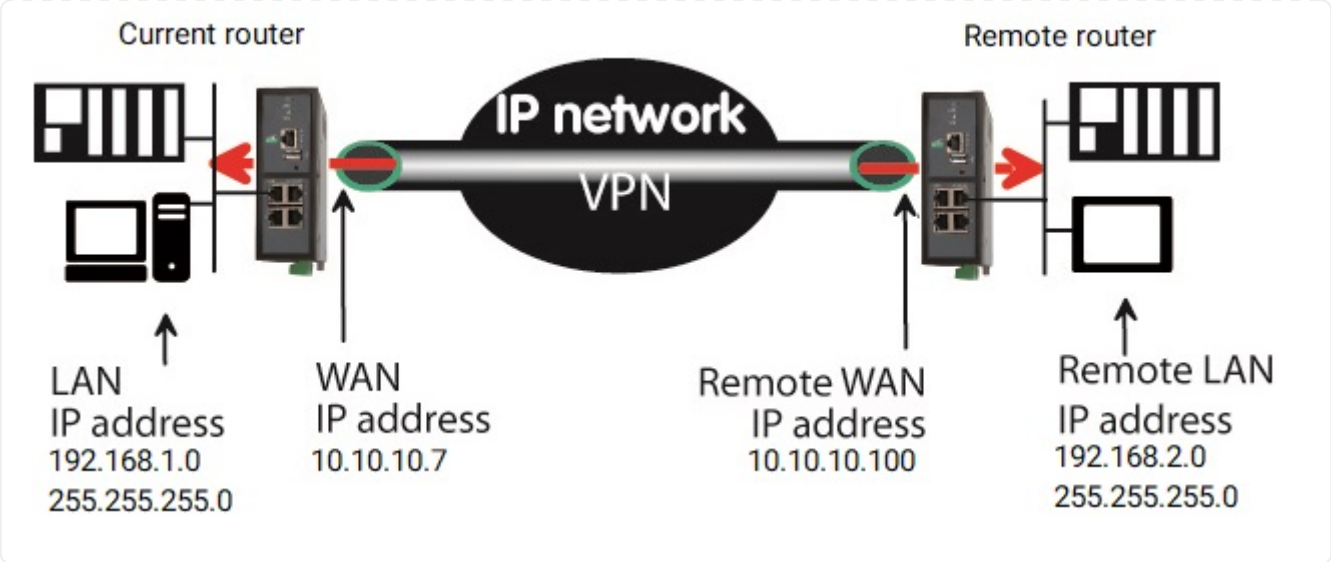
The router which initiates the connection is called the VPN client. It configures an outgoing connection.

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 14. 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).

Servers

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 **WARNING** The port number value must be different from the one used by remote access servers

Protocol	UDP or TCP
Virtual network device	TUN or TAP. **NOTE** • TUN: VPN data is sent over the network layer (L3) • TAP: VPN data is sent over the data link layer (L2)
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 **IMPORTANT** 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. **IMPORTANT** 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 15. Possible values* AES-256-GCM, AES-128-GCM, AES-256-CBC, AES-192-CBC, AES-128-CBC, Auto
Authentication	Algorithm for authentication *Example 16. 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. TLS version is 1.2 minimum if it's unchecked.
Disable compression	Disable compression
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
Enable tls-crypt-v2	Enable tls-crypt-v2, can't be used along with tls-crypt and tls-auth
tls-crypt-v2 key	Key value for tls-crypt-v2 server
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 (LAN IP address and LAN Additional IP address if there is one)
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
tun-mtu	Maximum Transmission Units
fragment	Enable internal datagram fragmentation so that no UDP datagrams are sent which are larger than this value in bytes.
mssfix	Announce to TCP sessions running over the tunnel that they should limit their send packet sizes such that after OpenVPN has encapsulated them, the resulting UDP packet size that OpenVPN sends to its peer will not exceed this value in bytes.

Outgoing connections

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 17. 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 **WARNING** The port number value must be different from the one used by remote access servers
Protocol	UDP or TCP
Virtual network device	TUN or TAP. **NOTE** • TUN: VPN data is sent over the network layer (L3) • TAP: VPN data is sent over the data link layer (L2)
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 18. Possible values* AES-256-GCM, AES-128-GCM, AES-256-CBC, AES-192-CBC, AES-128-CBC, Auto
Authentication	Algorithm for authentication *Example 19. 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.
Enable TLSv1 protocol (Only for compatibility)	Use TLS version 1. This version should only be used for compatibility with old devices. TLS version is 1.2 minimum if it's unchecked.
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 20. 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
Enable tls-crypt-v2	Enable tls-crypt-v2, can't be used along with tls-crypt and tls-auth
tls-crypt-v2 key	Key value for tls-crypt-v2 client
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 Ethernet

WAN section).

Ingoing connections

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 21. IP address* 192.168.2.0
Remote LAN netmask parameters	Netmask of the remote LAN *Example 22. 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.

[1] Valeur de Contrôle d'Intégrité

7. NETWORK

7.1. 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.

Here is an example where routing is used:

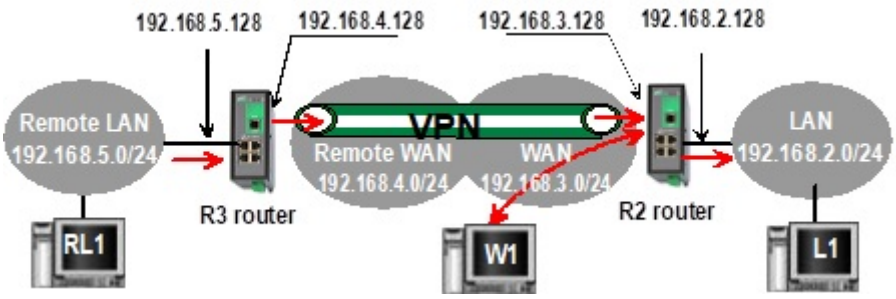


Figure 8. Basic routing

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

7.2. 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:

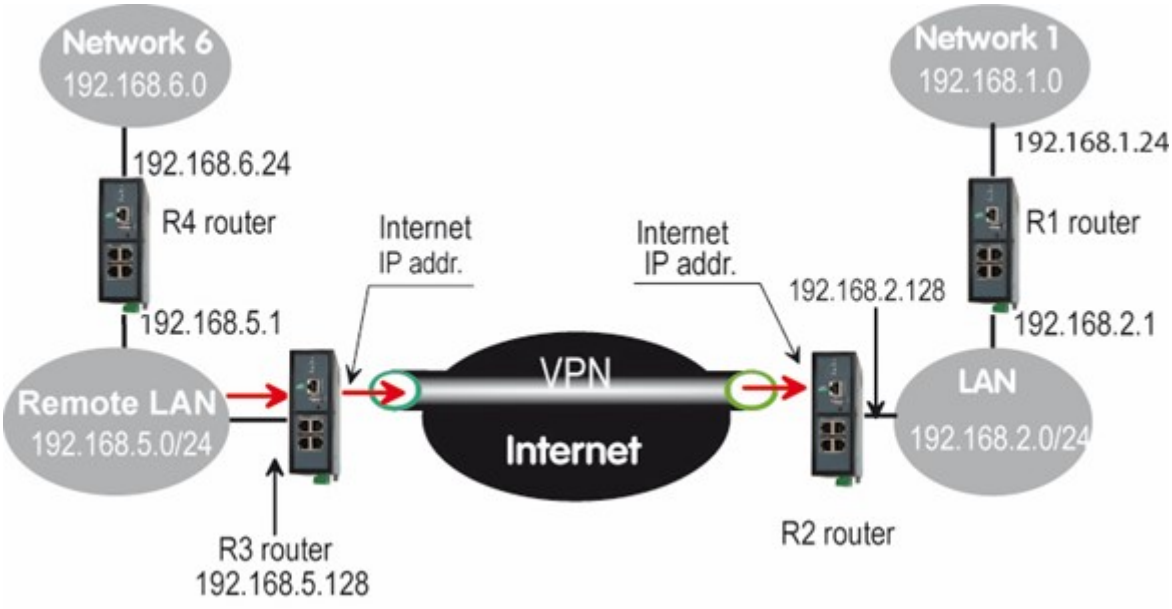


Figure 9. Static routes example

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 4. 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 connections)
OpenVPN outgoing node	OpenVPN node (see Outgoing connections)
IPSec node	IPSec node (see IPSec)

7.3. 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.

7.4. VRRP Redundancy

VRRP is a protocol that allows two or more routers on the same IP network to act redundantly with each other to increase the availability of the router function.

The mechanism is as follows: The routers placed in redundancy with each other each have different IP addresses, like any device on an IP network; but they also have a common IP address called virtual IP address.

This virtual and shared IP address is the IP address that should be registered in different network devices as the default router address.

In addition, a priority index (between 1 and 255) is assigned to each of the routers in the group. The routers in the group elect the master router; it is the one with the highest priority index, it will announce 255 as the priority index, while other routers, that we designate as backup routers, will remain silent.

The master router supports the router function; it responds to ARP requests sent by network devices. Additionally, it regularly broadcasts a presence message using the multicast address 224.0.0.18 with an IP protocol number 112. If the message is not received, a new master router is elected.

NOTE The Router manages this protocol as well on the WAN and LAN interface.

VRRP Configuration

Go to the view ***Setup > Network > VRRP Redundancy***

Enable VRRP on LAN	Check this box to enable VRRP on the LAN interface
Enable VRRP on WAN	Check this box to enable VRRP on the WAN interface
VRRP Id	Assign an identity code to the router group between `1` and `255`. All routers in the same group must have the same code. Two different groups cannot have the same code
Virtual IP address	Virtual IP address common to all routers in the group. Every redundant routers must have the same virtual IP address
Priority	Assign a priority index to the router between `1` and `255`. The highest index designates the highest priority router
Use a virtual MAC address	A virtual MAC address can be associated with the virtual IP address This way, when a network device transmits an ARP request, the master of the VRRP group always responds with the same MAC address. The MAC address used is an address intended for this purpose: 00-00-5E-00-01-XX, the last byte being the VRRP group number encoded in hexadecimal

7.5. 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 23. 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.

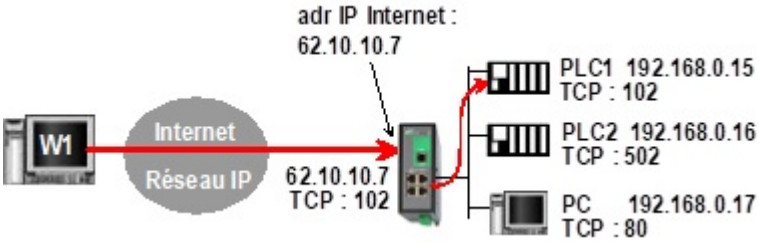


Figure 10. Port forwarding example

Table 5. 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)

7.6. Advanced NAT

Every incoming or outgoing frame from the router can be processed. NAT functions allow the IP addresses of the frames to be modified to reach devices located behind the router.

This function applies to IP frames emitted by devices belonging to the LAN and transmitted to the WAN.

The NAT function consists of replacing the source IP address of these frames with the source IP address of the Router on the WAN interface.

This function is required when a device belonging to the LAN network needs to connect to the Internet (for example, to transmit a file via FTP).

To enable the NAT function for Ethernet, for example, select the menu ***Home*** > ***Setup*** > ***WAN Interfaces*** > ***Ethernet***, then click on **Enable address translation (NAT)**.

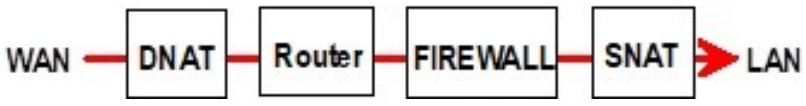
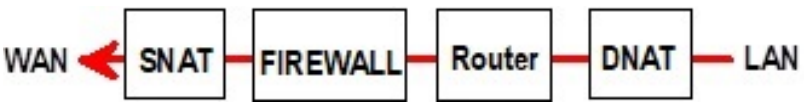
The advanced NAT function consists in modifying the source or destination IP addresses and port number of the frames received by the Router on its LAN or WAN interface.

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	
LAN to WAN	

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**.

7.7. NAT 1:1

NAT 1:1 (one-to-one) consists of mapping the IP address of a device on the LAN network to an IP address belonging to a WAN interface of the router.

It means that when a device on the WAN sends packets to that WAN IP, the router actually sends them back to the device on the LAN with its LAN IP address.

Select the ***Setup*** > ***Network*** > ***NAT 1:1*** menu.

Enabled	Enable or disable the NAT rule
WAN on which apply the rule	`Ethernet WAN` or `Wi-Fi WAN`
WAN IP to add	IP address added to the chosen WAN interface
LAN IP to map on WAN	IP address of the device on the LAN that needs to be reachable

WARNING	Firewall rules whose destination address is the WAN IP, or the LAN IP of a 1:1 NAT rule, are not taken into account

7.8. 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.

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.

Step 1: Domain name allocation

Reserve a domain name on your favorite Dynamic DNS website.

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 24. Domain name* mymachine.eticdns.com

7.9. ERSPAN Remote Mirroring

Mirroring principle

Mirroring allows you to copy traffic from one port to another port. This allows you to analyze network traffic with different analysis tools such as WireShark.

ERSPAN (Encapsulated Remote SPAN) allows you to transfer the network to a remote network. Network frames are encapsulated in a GRE (Generic Routing Encapsulation) tunnel. The analysis of the local network can therefore be done on a remote machine.

Configuration

- Mirroring is currently only available on products in the 100 range.
- ERSPAN is available in version 1.
- The mirrored network is the local network.

Go to ***Setup*** > ***Network*** > ***ERSPAN***

Source address	Source address to encapsulate data
Destination address	Destination address to forward LAN traffic to
GRE Key	GRE Tunnel Key
Tunnel ID	ERSPAN Tunnel ID
Maximum bitrate	Mirroring bitrate Limit

8. SECURITY

Router security functions and settings.

8.1. Authentication

Authentication protection

To protect the router from brute force attacks, there is a mechanism to ban users for Web, SSH and VPN authentication.

This mechanism is configurable, it is based on the number of failed attempts and makes all authentication attempts for a user invalid for a configurable time.

When an user successfully authenticates and has not yet been banned, its attempts counter resets to 0. After waiting for the ban duration, the attempts counter resets to 0.

Go to the view ***Setup > Security > Authentication***

Parameter	Description
Enabled	Enable this mechanism. `False` by default
Number of failed attempts before ban	Number of failed attempts for a user before they are banned. `10` by default
Ban duration (minutes)	Number of minutes the user will remain banned. `10` by default

A table is available in the view > ***Home > Setup > Security > Users*** summarizing the users banned from authentication, it is possible for a Super administrator to unban one or more user from this table using the **Unban user** button located just below the table.

Authentication warning

It is also possible to display a warning message regarding the use of the system to warn that access is restricted to authorized users only, that all activity may be monitored and recorded, and that unauthorized use is prohibited and subject to sanctions.

This message is displayed on the various authentication interfaces (Administration Area, Operation Area, SSH Interface)

Parameter	Description
Warning message before authentication	Message to be displayed on the various authentication interfaces to inform that access is reserved for authorized users only.

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 use remote access to the router or exploit Collect&Alert variables. So there are 2 sections in the configuration menu for delegated authentication, one for each user 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.

IMPORTANT	Authentication configuration is sensitive. It's easy to lock yourself out and lose access to the administration panel if it's misconfigured. The `Delegate + Local` mode is a good interim solution during configuration, as it allows you to continue logging in with your local users. Once authentication delegation is validated, you can change **Authentication Type** to a more restrictive option.
NOTE	Concerning delegated SSH administration, administrators from your delegated server will have to authenticate twice on the first connection.

Go to the view ***Setup > Security > Authentication***

Parameter	Description
Authentication type	• `Local` : Users who can authenticate are defined on the router. (By default) • `Delegated only`: Users can only authenticate on the delegated server. Users defined locally are ignored. • `Delegated with Local fallback`: Users who can authenticate are on the delegated server. If the server is unavailable, the router accepts local users. • `Delegate + Local`: Users who can authenticate are on the delegated server and on the router. It is recommended to keep only backup users locally.
Server type	Various server types supported for delegated authentication. Applies only if the authentication type is not `Local` • `EFM` • `LDAP` • `RADIUS` • `TACACS+`

You have the option to cache login credentials; this way, if your server goes down, users can still log in for a certain period of time.

Parameter	Description
Cache crendentials	Enable credential caching. `False` by default
Cache duration (minutes)	Cache validity period after authentication. `60` minutes by default.

The `Delegated with Local fallback` authentication type and credential caching can be enabled independently and simultaneously, resulting in the following authentication process:

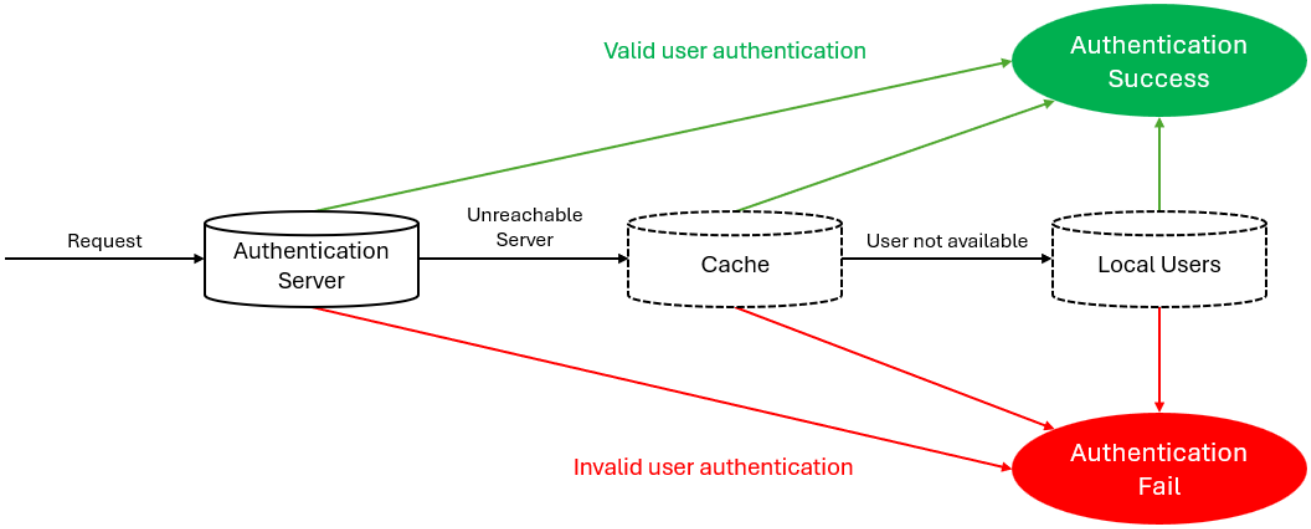


Figure 11. Authentication process taking into account the Cache and Local fallback

Configuring EFM authentication

Go to the view ***Setup > Security > Authentication***

The parameter **Authentication type** must be set to `EFM`.

The EFM values must be entered on the EFM page; see the section EFM for more details.

Configuring RADIUS/TACACS+ authentication

Go to the view ***Setup > Security > Authentication***

The parameter **Authentication type** must be set to `RADIUS` or `TACACS+`. Then fill the parameters for your server.

Parameter	Description
Server IP Address or Hostname	IP address or Hostname of your server. **IMPORTANT** 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.
Server port	Listening port of your TACACS+ server. Default port is 49.
Shared secret	Shared secret of TACACS+ server.

Configure access rights for Administrators

Administrators authenticated through RADIUS or TACACS+ have configurable access rights, Go to view ***Setup*** > ***Remote access*** > ***Administrator 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` for RADIUS and `TACACS_PLUS_ETIC_TELECOM` for TACACS+. 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 or TACACS+ 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` for RADIUS and `TACACS_PLUS_ETIC_TELECOM` for TACACS+. This group name is designed specifically for operators authenticating through RADIUS and by adding/editing this group, you can choose the access rights.

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.

NOTE You can check the LDAP authentication logs in the `Main` log

Parameter	Description
Server IP Address or Hostname	IP address or Hostname of your server. **IMPORTANT** • 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 25. 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 26. 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 27. 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 28. Root domain for group search* ou=groups,dc=mycompany,dc=com

Parameter	Description
Attribute used to identify users	LDAP attribute `used in DN` (distinguished names) to identify users. *Example 29. Attribute used to identify users* cn
Active Directory domain name	Domain name (used only if server type is Active Directory) *Example 30. 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.

Difference between Active Directory and Others

Active Directory

Logins of users who authenticate through Active Directory are their `userPrincipalName`.

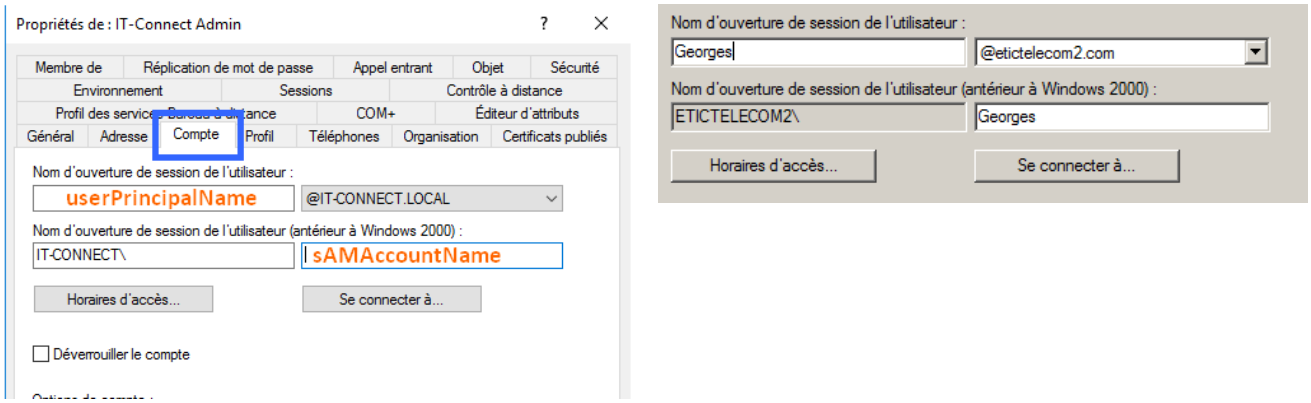


Figure 12. Active Directory server configuration

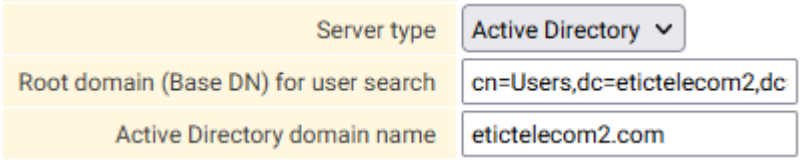


Figure 13. Active Directory router configuration

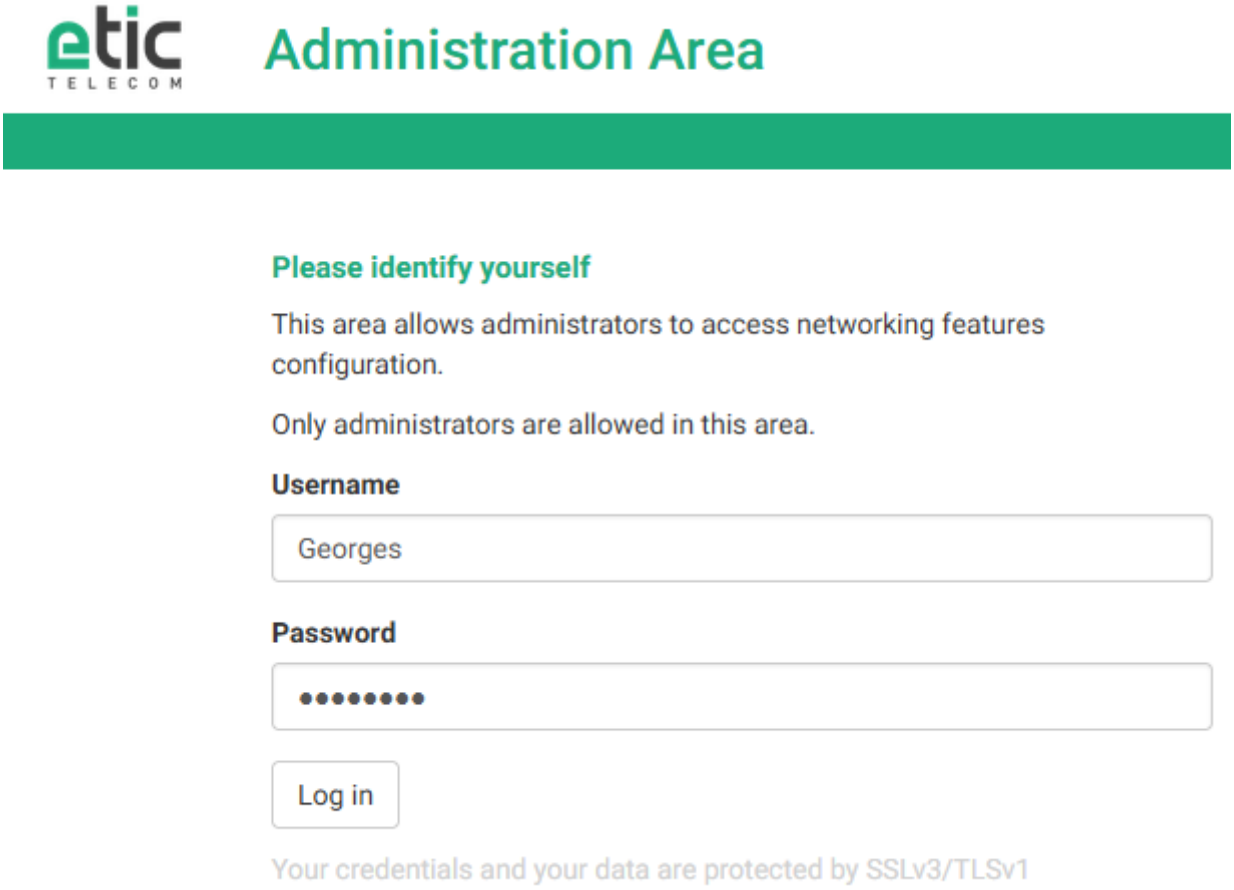


Figure 14. Web login with Active Directory

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`.

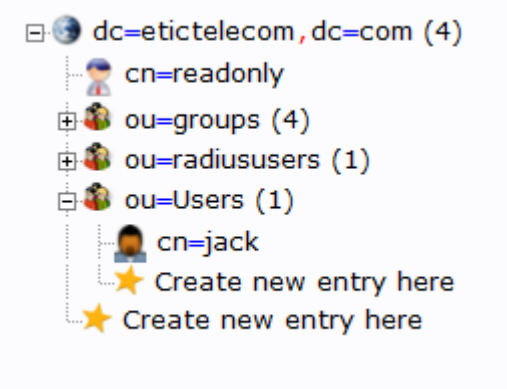


Figure 15. OpenLDAP server configuration

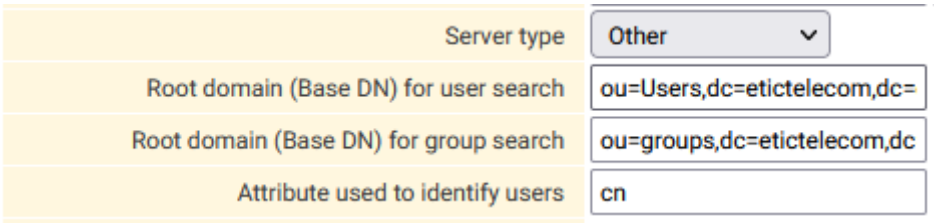


Figure 16. OpenLDAP router configuration

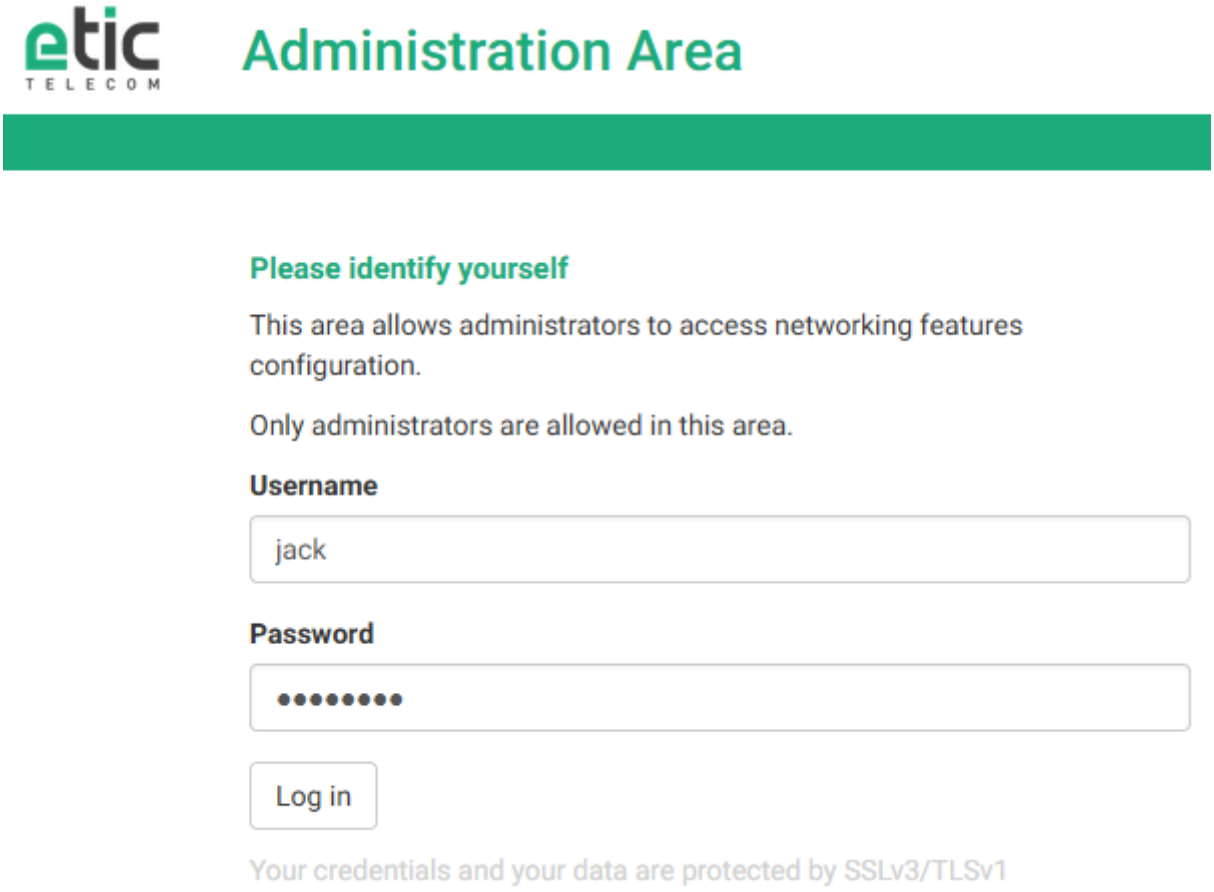


Figure 17. Web login with OpenLDAP

8.2. Firewall

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`).

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.

WARNING	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. `Deny` 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 31. 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***

8.3. Certificate store

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.

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.

IMPORTANT	Names given to certificates / private keys / CRL must follow some rules: 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, 3072, 4096 or ECDSA Prime256v1.

Certificate signing request

You can create a certificate signing request for a specific key. Select the key and click **Create CSR...**. A page will open allowing you to specify the fields for your CSR.

Next, click on **Save**, and your CSR will appear in PEM text format. This allows you to sign a certificate for a key with your custom certificate 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.

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.

NOTE	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.

NOTE	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 32. LDAPS needs client certificate, CA certificate and private key.

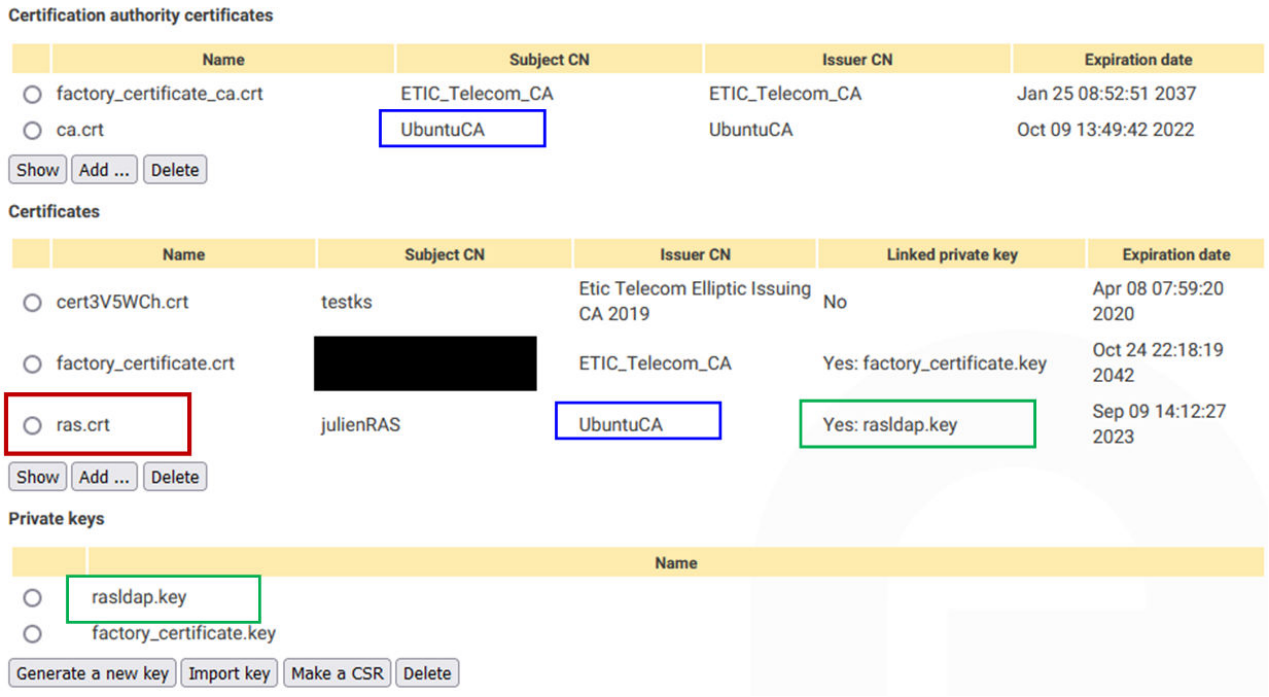


Figure 18. Certificate Store configuration

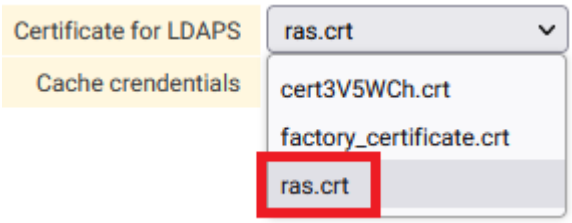


Figure 19. LDAP certificate configuration

Certificate revocation lists

Syslog, 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.

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

NOTE	For Syslog, it is necessary to reboot the router to take into account the CRL.

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

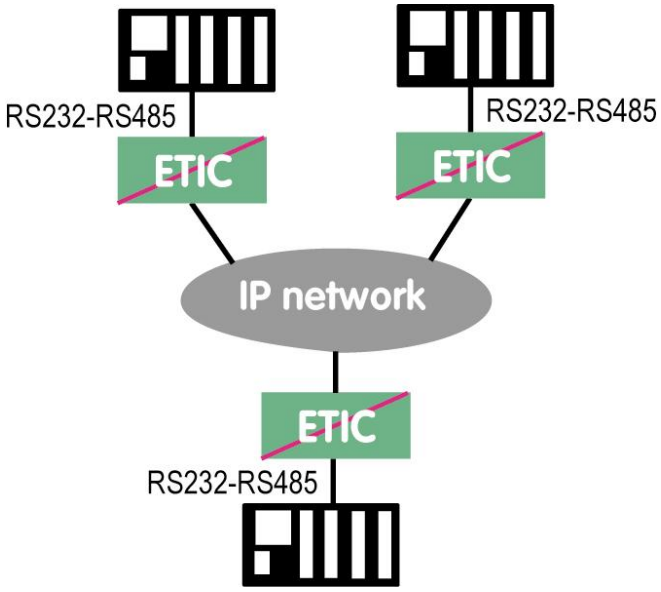
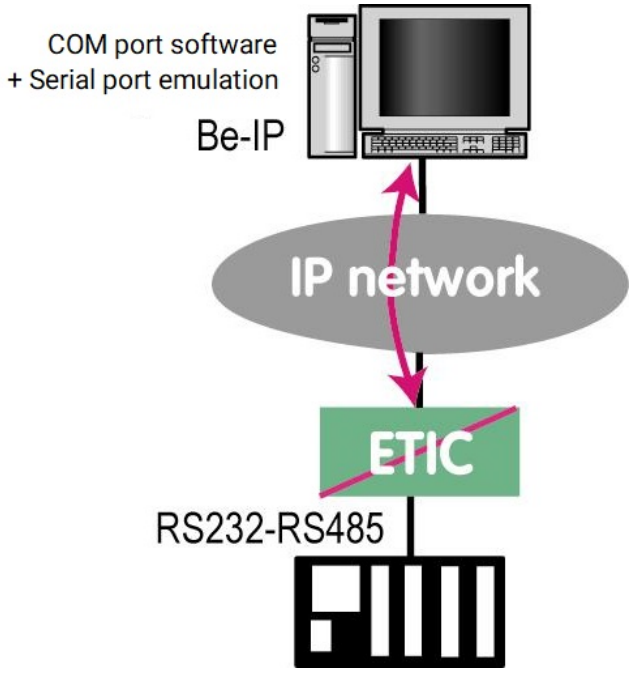
104. GTS_Root_R3.crt
105. GTS_Root_R4.crt
106. Hongkong_Post_Root_CA_3.crt
107. Microsoft_ECC_Root_Certificate_Authority_2017.crt
108. Microsoft_RSA_Root_Certificate_Authority_2017.crt
109. NAVER_Global_Root_Certification_Authority.crt
110. Trustwave_Global_Certification_Authority.crt
111. Trustwave_Global_ECC_P256_Certification_Authority.crt
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

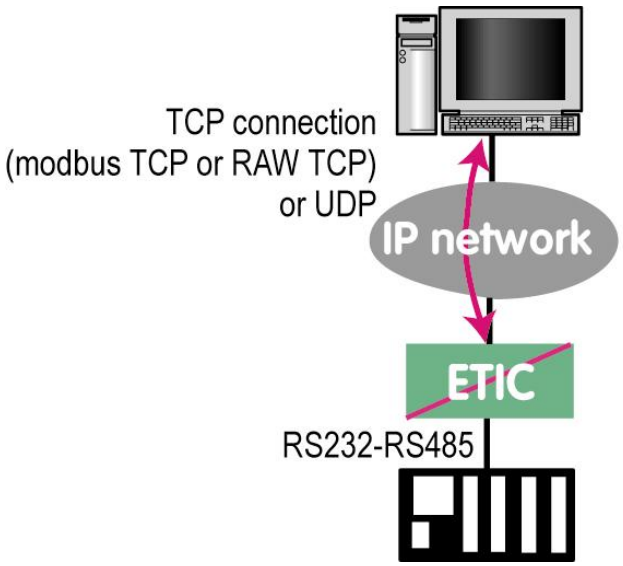
9. SERIAL TO IP GATEWAYS

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.

9.1. 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.

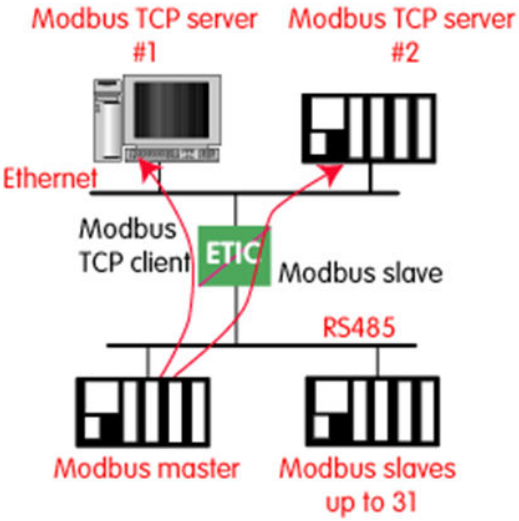
Select the Modbus Client gateway to connect a serial Master device to the serial port of the product.

Assigning a Modbus gateway to a serial port

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

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

Modbus client gateway

This gateway allows to connect a serial modbus master to the serial interface of the product. The gateway can be connected to several Modbus TCP servers on the IP network Other slaves can be connected to the serial link.	

How 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.

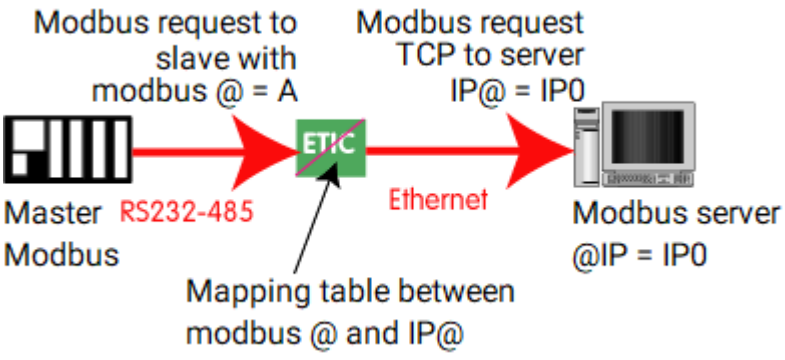


Figure 20. Modbus mapping table

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.

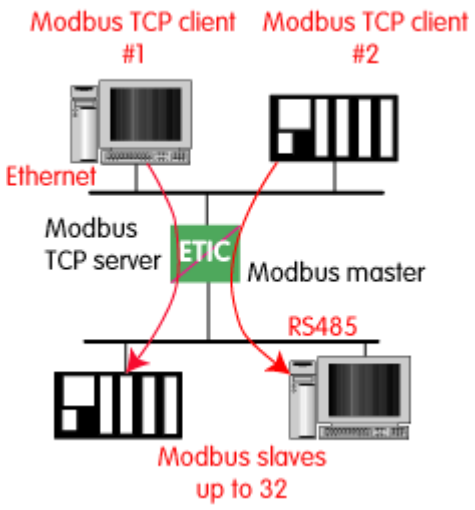
TCP port parameter:

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.

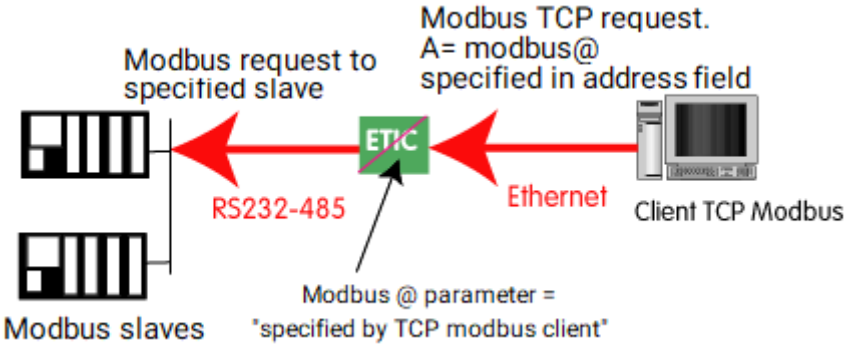
Modbus server gateway

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.	

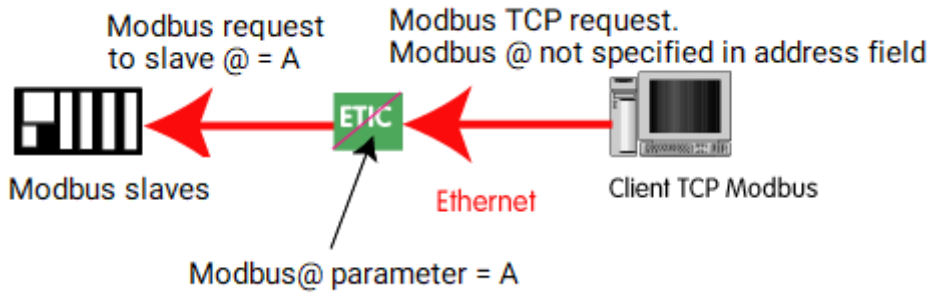
How Modbus server Gateway works

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.



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

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.

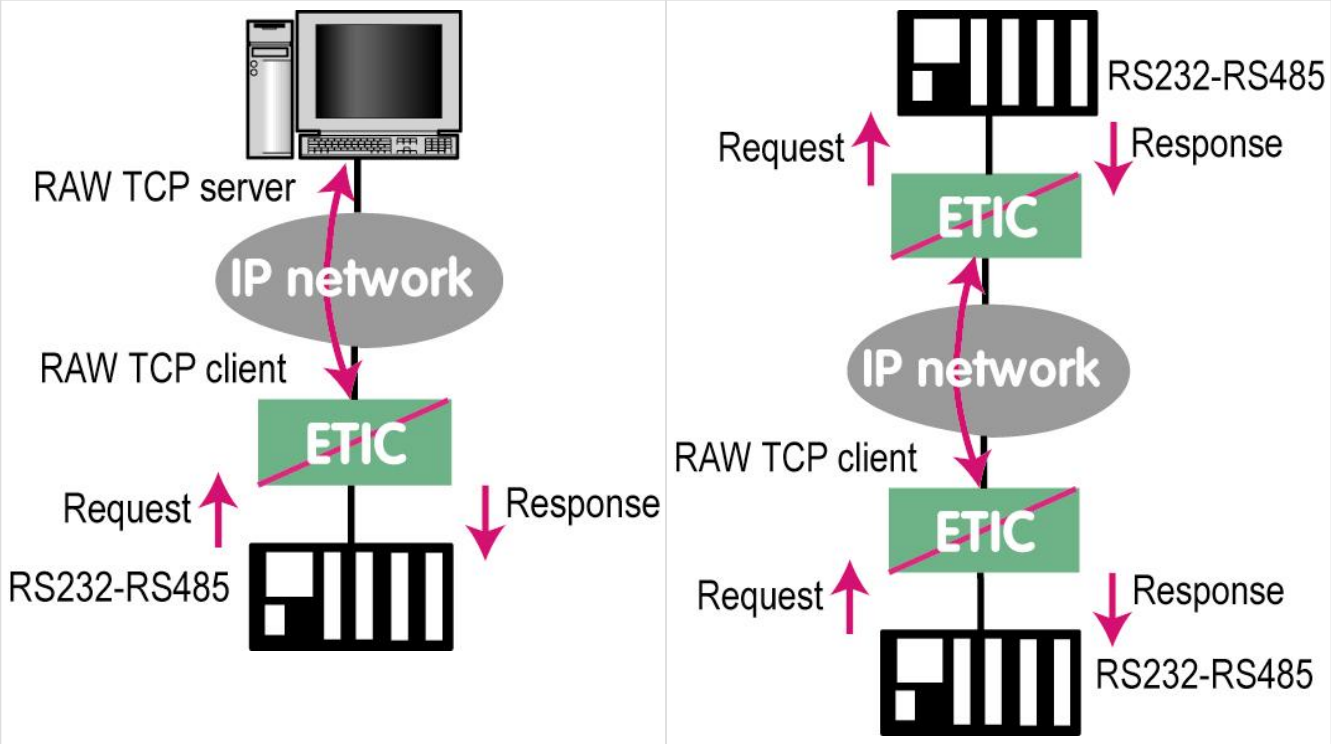
9.2. Raw TCP

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 6. 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.

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

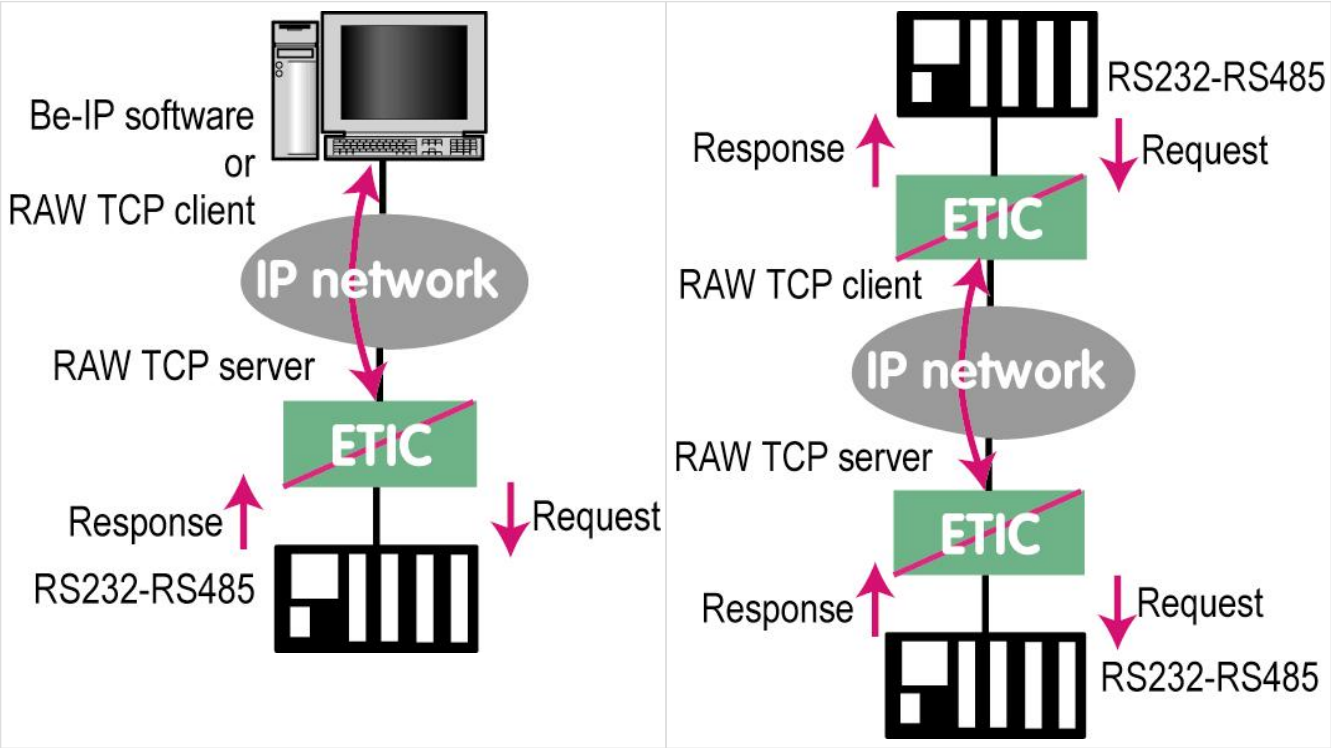
Server IP address parameter:

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 7. 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.

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

9.3. 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.

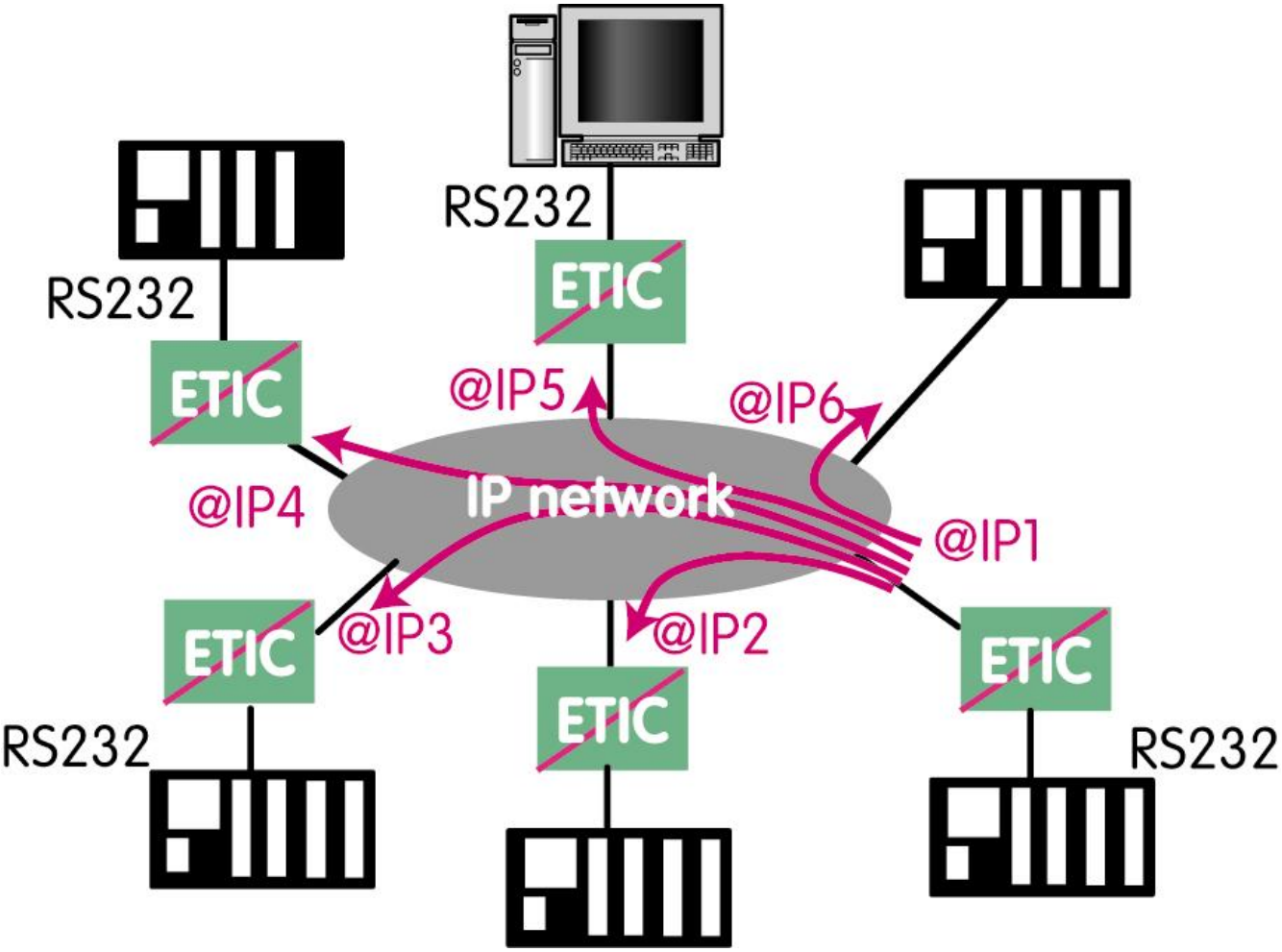


Figure 21. Raw UDP gateway

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.

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

Destination 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.

9.4. 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.

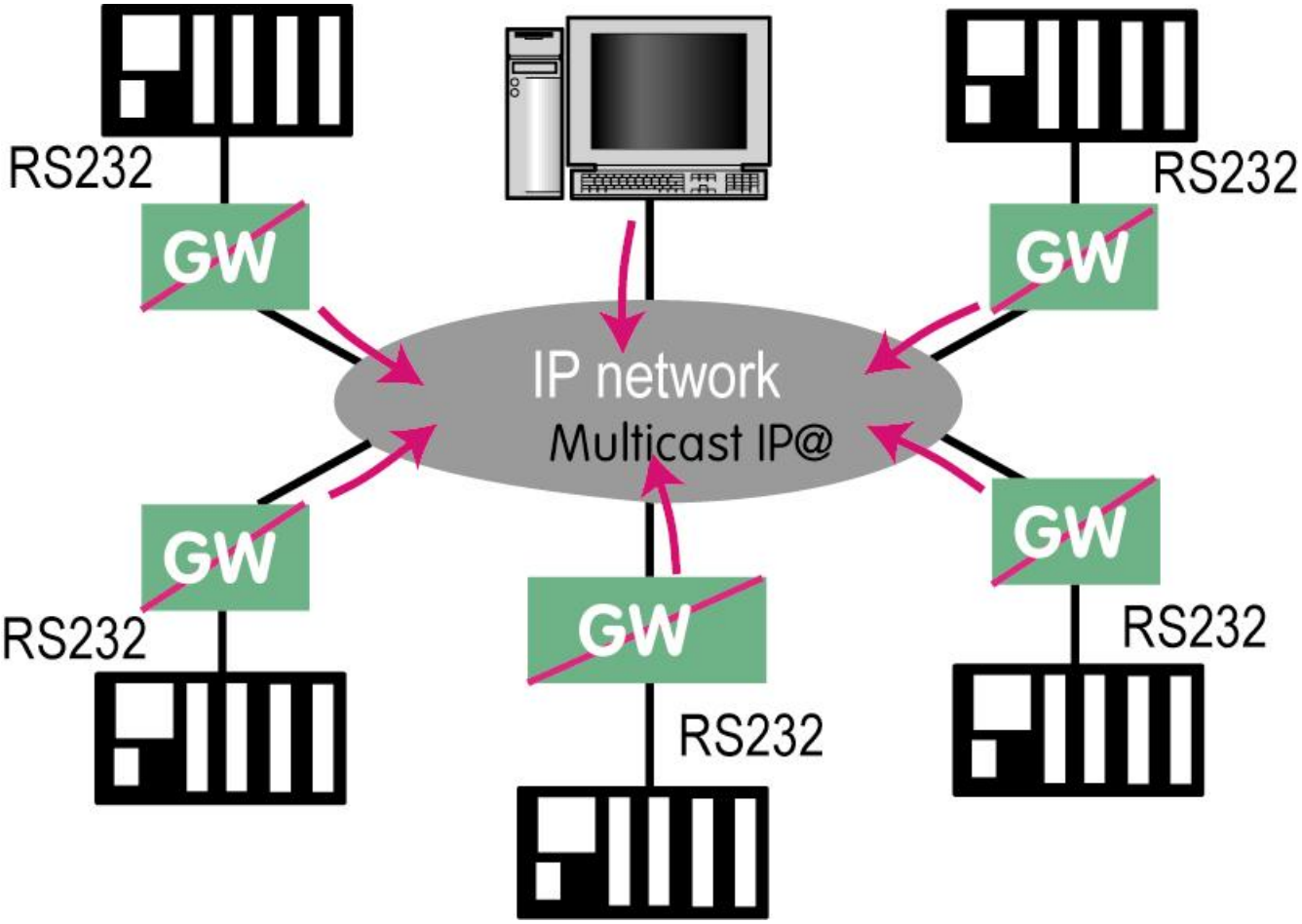


Figure 22. Raw multicast gateway

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.

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

Multicast group IP address parameter:

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

9.5. 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.

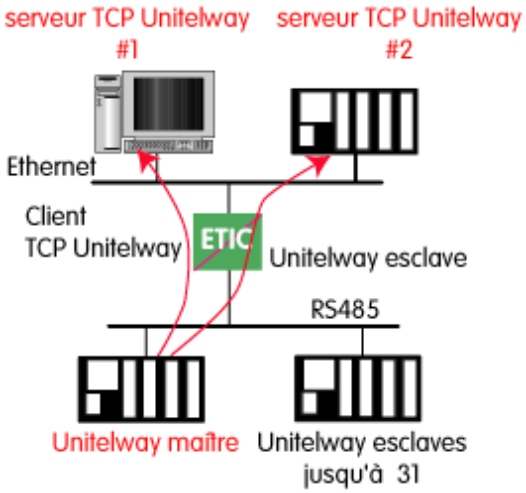


Figure 23. Unitelway gateway

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.

9.6. 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.

9.7. 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.

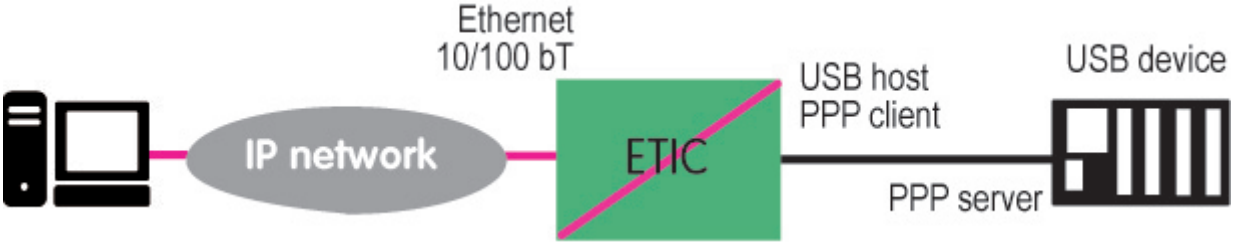


Figure 24. USB Gateway

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.

10. SYSTEM

These features allow for various adjustments to the router's system operation.

10.1. Email or SMS alerts

All the models of Routers are able to transmit e-mail or SMS alerts when one event occurs.

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

Every SMS or email sent is logged, along with the person/process that triggered it.

Message	Message type: SMS or e-mail
Alarm launched on event	Select the event: • `Input rising edge (¬ON)` • `Input falling edge (¬OFF)` • `Input rising or falling edge (¬ON or ¬OFF)` • `VPN connection/disconnection event`
Phone number (SMS choice):	Enter the phone number. If you use the M2Me server and the SMS pack, the number must have the country code. For example `0033` or `+33` for France. It is possible to enter several numbers separated by a comma.
Email sender (e-mail choice):	Enter the sender email address.
Email Destination (e-mail choice):	Enter the email recipients. It is possible to enter several e-mail adresses separated by a comma.
Subject (e-mail choice) :	Enter the subject of the alarm mail.
Text to send	Enter the alarm text.

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

10.2. Periodical reboot

It is possible to configure a periodic restart of the router.

Access the menu ***Setup*** > ***System*** > ***Periodical reboot***.

Enable periodical reboot	Enabling Periodic Restart
Reboot period	Restart time. Daily, Weekly, or Monthly
Reboot hour	Time to restart the product

NOTE

The periodic restart ensures that the router restarts regularly.

The weekly restart occurs on Sunday. The monthly restart occurs on the 1st of the month. If the router has already restarted that day, the periodic restart will not be triggered at the configured time.

10.3. 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.

Syslog remote server configuration

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

Transfer mode	• `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	Only if `Server authentication` or `Mutual authentication` Name of the syslog server. This field must correspond to the common name (CN) of the server certificate. **IMPORTANT** 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	Only if `Mutual authentication`. Chose a certificate in the `Certificate store` to sign logs. **IMPORTANT** The chosen certificate must be linked to a private key. Otherwise, logs can't be signed.

Format of logs sent to the remote server

Logs sent to a remote Syslog server are formatted as follows:

```
${ISODATE} ${UNIQID} ${PROGRAM} ${FACILITY} (${LEVEL}) | ${MSG}
```

Here is an example of the logs:

```
...
2025-07-04T16:15:51+02:00 9164560d@00000000000000dc   daemon_starter   local1
(info) |       NETWORK: LAN: lan4 is Down
2025-07-04T16:16:07+02:00 9164560d@00000000000000df   daemon_starter   local1
(info) |       NETWORK: LAN: lan2 Up 100Mb/s Full Duplex
2025-07-04T16:16:27+02:00 9164560d@00000000000000e0         dropbear authpriv
(info) | Child connection from 192.168.0.20:61448
2025-07-04T16:18:49+02:00 9164560d@00000000000000e1   gui_backend.py   local3
(info) | User 'admin' has authenticated to the Admin Web interface
2025-07-04T16:19:02+02:00 9164560d@00000000000000e2   gui_backend.py   local3
(info) | User 'admin' set params into the configuration
2025-07-04T16:19:04+02:00 9164560d@00000000000000e3        committer   local3
(info) | Changed parameters: {u'p_https_appserver_2_enable.0': u'false'}
```

```
...
```

The `FACILITY local1` corresponds to the `Main` log. `local3` corresponds to the `Audit Trail` log.

Remote Syslog Server Configuration

Depending on your server configuration, you may need to add `flags(no-parse)` to display the received raw text.

10.4. 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 33. 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 34. Possible values* AES-256-CBC, AES-192-CBC, AES-128-CBC, DES
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

10.5. OPC UA server

Configuring OPC UA server

Etic Telecom provides an OPC UA server that makes available different status and data collected by the product. The complete list of available data is presented in the section `Specification of OPC UA server nodes`.

Go to the menu ***Setup > System > OPC UA Server***.

Parameter	Description
Enabled	Enables the OPC UA server
Enable Anonymous logon	Autoriser les connexions anonymes
Enable Username/Password authentication	Requires username/password authentication
Username	Username used for authentication
Password	Password used for authentication
Security	
None	Disable security
Allow deprecated security policies	Allows the use of Basic128 and Basic256
Basic256Sha256	Checkbox to accept basic256sha256
Basic128	Checkbox to accept Basic128
Basic256	Checkbox to accept Basic256
Security check overrides	
Accept all client certificates	The server does not verify the client certificate
Client certificate	Certificate used by the client
Server certificate	Certificate used by the server

Reading OPC UA Nodes

To access to the OPC UA Server, we use UaExpert Client available from (https://www.unified-automation.com/downloads/opc-ua-clients.html). The OPC UA server can be reached on a specific URL. The URL is structured as follows:

- Protocol identifier `opc.tcp://`
- IP address of the device: `192.168.0.128`
- TCP Port number: `5040`

Example of URL: `opc.tcp://192.168.0.128:5040`

- After launching the UA Expert Client, to add a new connection to an OPC UA Server, click on the

+ button in the toolbar. A new dialog window will open. Double-click on < Double click to Add Server >.

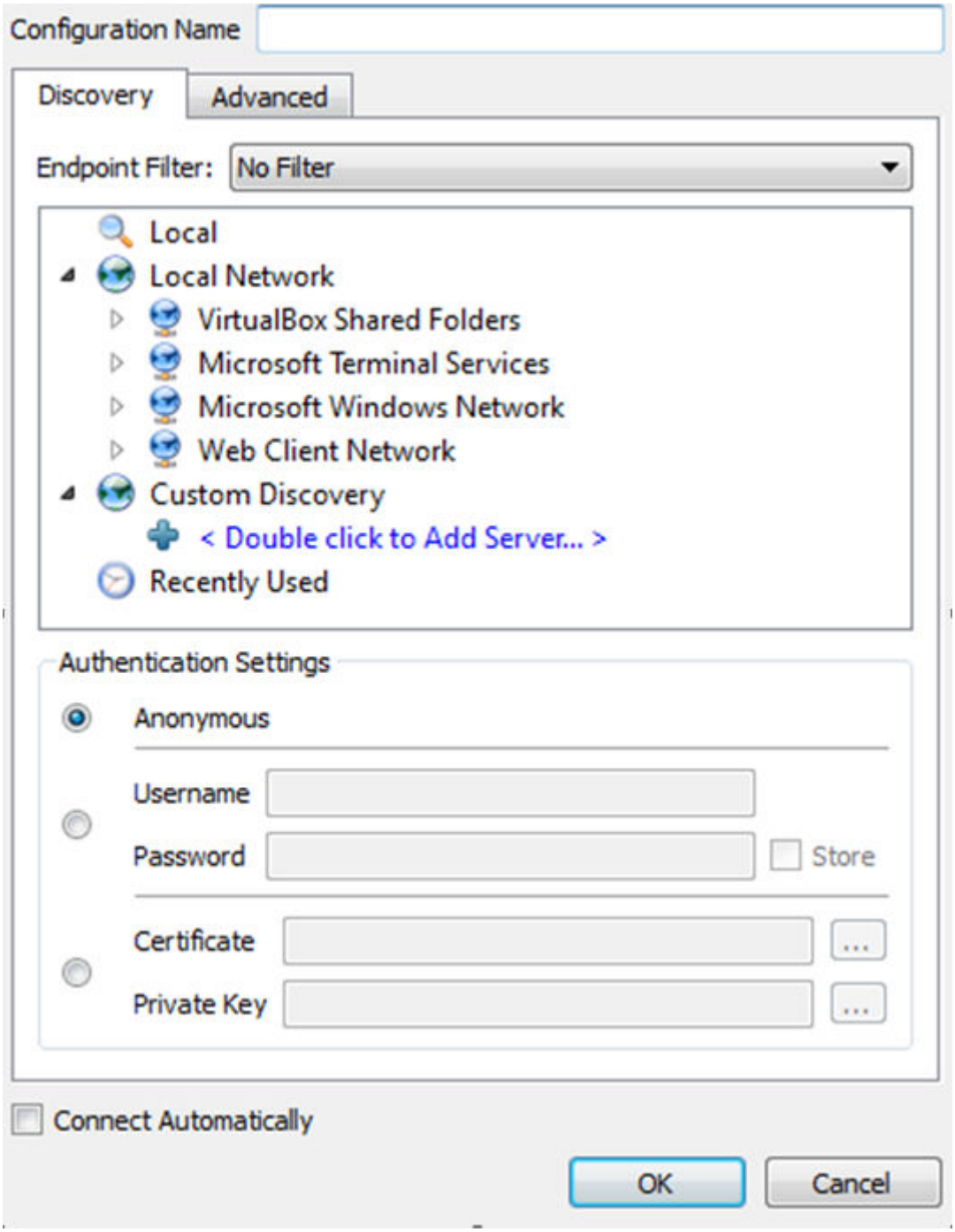


Figure 25. UA Expert Client menu to add new server

- Once the URL is added, the server and all endpoints it provides are shown.
- Choose an endpoint and confirm with OK. The Server is now listed in the Project Window and you can connect using the connector plug in the toolbar
- In the address space window, you can see the address space of the server which is currently selected in the project Window.

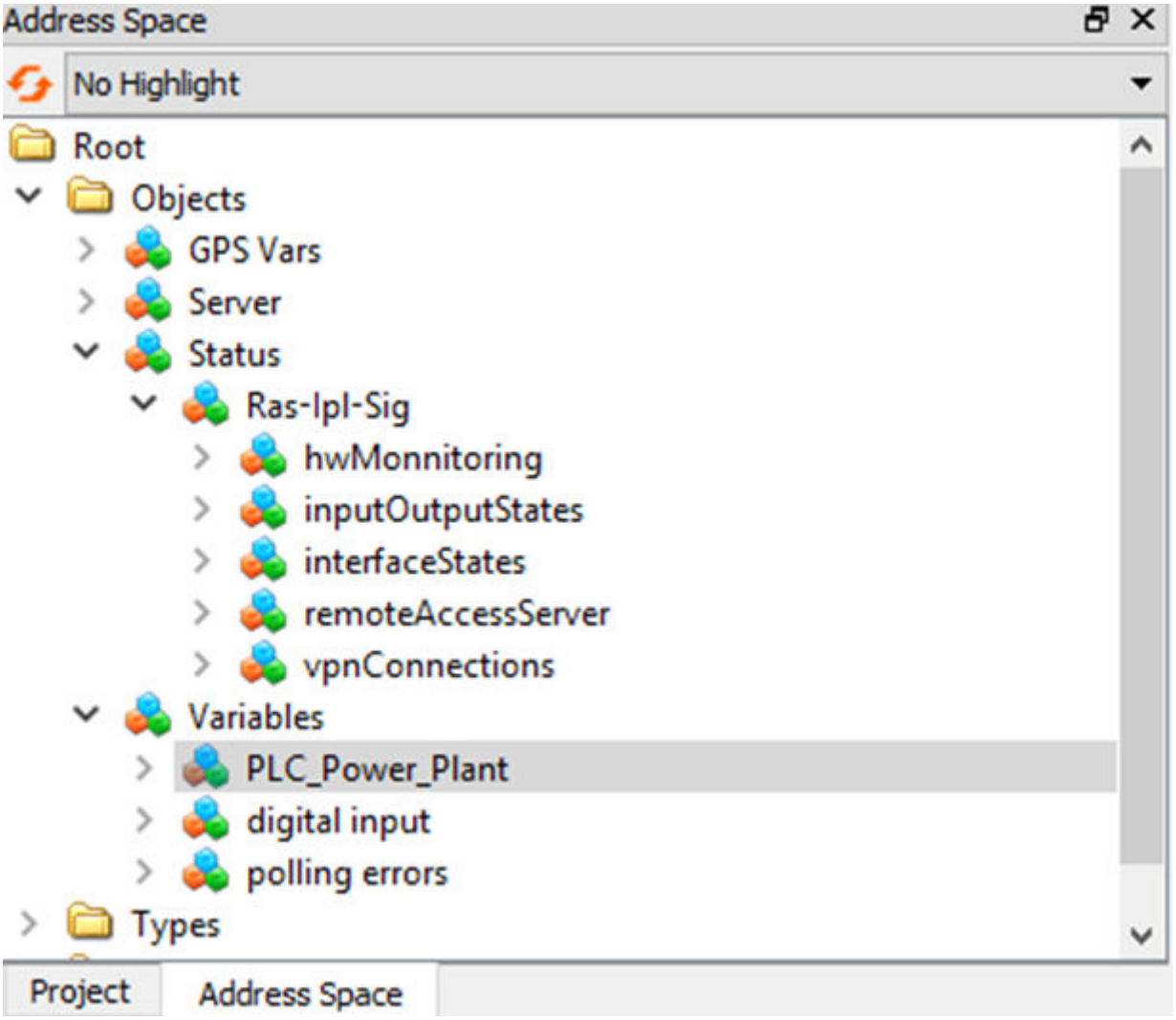


Figure 26. UA Expert Client adress space window

Specification of OPC UA server nodes

Status	NodeId
Hardware states	
Power supply 1	`ns=2;s=status_hwmon_alim1`
Power supply 2	`ns=2;s=status_hwmon_alim2`
Internal temperature	`ns=2;s=status_hwmon_temp`
Input/output states	
Input status	`ns=2;s=status_etor_state`
Output status	`ns=2;s=status_stor_state`
Network interfaces states	
Status of Ethernet LAN port (n)	`ns=2;s=status_lan(n)_state`
Wi-Fi LAN MAC address	`ns=2;s=status_wifi_lan_macaddr`
Wi-Fi WAN signal quality	`ns=2;s=status_wifi_lan_client_signal`

Status	NodeId
Wi-Fi LAN client authorized	ns=2;s=status_wifi_lan_client_authorized
ADSL WAN connected	ns=2;s=status_wan_adsl_is_connected
ADSL WAN modem status	ns=2;s=status_adsl_modem_state
ADSL WAN priority	ns=2;s=status_wan_adsl_priority
ADSL WAN IP address	ns=2;s=status_wan_adsl_ip_interface
ADSL WAN downstream attenuation	ns=2;s=status_adsl_dn_att
ADSL WAN downstream SNR margin	ns=2;s=status_adsl_dn_snrm
ADSL WAN upstream attenuation	ns=2;s=status_adsl_up_att
ADSL WAN upstream SNR margin	ns=2;s=status_adsl_up_snrm
GSM WAN connected	ns=2;s=status_wan_gsm_is_connected
GSM WAN priority	ns=2;s=status_wan_gsm_priority
GSM WAN operator	ns=2;s=status_wan_gsm_operator
GSM WAN cell ID	ns=2;s=status_wan_gsm_cid
GSM WAN Location Area Identity	ns=2;s=status_wan_gsm_lac
GSM WAN EC/IO	ns=2;s=status_wan_gsm_ecio
GSM WAN Bytes received	ns=2;s=status_wan_gsm_byte_trans
GSM WAN Bytes received	ns=2;s=status_wan_gsm_byte_recvd
Ethernet WAN connected	ns=2;s=status_wan_eth_is_connected
Ethernet WAN status	ns=2;s=status_wan_eth_state
Ethernet WAN status	ns=2;s=status_wan_eth_ip_interface
Wi-Fi WAN connected	ns=2;s=status_wan_wifi_is_connected
Wi-Fi WAN priority	ns=2;s=status_wan_wifi_priority
Wi-Fi WAN mode	ns=2;s=status_wan_wifi_mode
Wi-Fi WAN BSS	ns=2;s=status_wan_wifi_bss
Wi-Fi WAN Frequency (MHz)	ns=2;s=status_wan_wifi_freq
Wi-Fi WAN Signal	ns=2;s=status_wan_wifi_signal
Wi-Fi WAN SSID	ns=2;s=status_wan_wifi_ssid
WAN DNS 1 applied	ns=2;s=status_wan_applied_dns1
WAN DNS 2 applied	ns=2;s=status_wan_applied_dns2
WAN DNS 3 applied	ns=2;s=status_wan_applied_dns3
Remote Access Servers states	
M2Me connected	ns=2;s=status_m2me_connected
M2Me IP address	ns=2;s=status_m2me_ip

Status	NodeId
M2Me state	ns=2;s=status_m2me_state
M2Me port	ns=2;s=status_m2me_port
M2Me protocol	ns=2;s=status_m2me_protocol
Remote user name	ns=2;s=status_vpn_users_name0
Remote user connected	ns=2;s=status_vpn_users_connected0
Remote user IP address	ns=2;s=status_vpn_users_ipaddr0
Number of remote users connected	ns=2;s=status_nb_remote_users
VPN Connections	
IPsec VPN name	ns=2;s=status_vpn_ipsec_nodes_name0
IPsec VPN connected	ns=2;s=status_vpn_ipsec_nodes_connected0
IPsec VPN WAN address	ns=2;s=status_vpn_ipsec_nodes_wan_addr0
IPsec VPN LAN address	ns=2;s=status_vpn_ipsec_nodes_lan_addr0
OpenVPN VPN in name	ns=2;s=status_vpn_in_nodes_name0
OpenVPN VPN in connected	ns=2;s=status_vpn_in_nodes_connected0
OpenVPN VPN in WAN address	ns=2;s=status_vpn_in_nodes_wan_addr0
OpenVPN VPN in LAN address	ns=2;s=status_vpn_in_nodes_lan_addr0
OpenVPN VPN out name	ns=2;s=status_vpn_out_nodes_name0
OpenVPN VPN out state	ns=2;s=status_vpn_out_nodes_connected0
OpenVPN VPN out WAN address	ns=2;s=status_vpn_out_nodes_wan_addr0
OpenVPN VPN out LAN address	ns=2;s=status_vpn_out_nodes_lan_addr0
GPS location	
GPS Location Altitude	ns=0;i=11030
GPS Location Latitude	ns=0;i=11010
GPS Location Longitude	ns=0;i=11020

Variables Collect&Alert

Les variables définies dans Collect&Alert sont renseignées dans le serveur OPC UA. Leurs états et leurs valeurs peuvent être récupérés depuis un client OPC UA.

10.6. Modbus TCP server

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.

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 500-549:** Message sender
- **Registers 550-599:** Message destination
- **Registers 600-649:** Message subject
- **Registers 650-773:** Message text

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

Figure 27. Wireshark capture of a Modbus Request to write Message sender

Steps from PLC

1. Write characters (ASCII, Latin-1, UTF-8) 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.

Table 8. 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	500	501	502	503	504	505	506
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

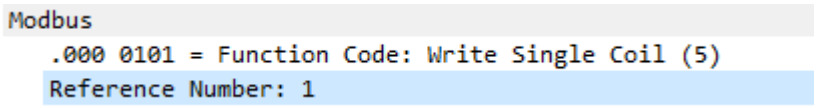


Figure 28. Wireshark capture showing a Modbus Request to trigger an E-Mail

Specification of registers and their contents

Register 10 Address: 40011

NodeID: 255

Register MAP

Register	Content	Type	Details
10-13	GPS Location latitude	LREAL (-1.79e+308 ... 1.79e+308)	Unit : ° • Register 10 - bit 0: LSB (Least Significant Bit • Register 13 - bit 15: MSB (Most Significant Bit)
14-17	GPS Location longitude	LREAL (-1.79e+308 ... 1.79e+308)	Unit : ° • Register 14 - bit 0: LSB • Register 17 - bit 15: MSB
18-19	GPS Location altitude	REAL (-3.40e+38 ... 3.40e+38)	Unit : meters • Register 18 - bit 0: LSB • Register 19 - bit 15: MSB
20-21	GPS Location speed	REAL (-3.40e+38 ... 3.40e+38)	Unit : m/s • Register 20 - bit 0: LSB • Register 21 - bit 15: MSB
22	GPS Location precision	UINT16 (0 ... 65535)	Unit : meters
...			

Register	Content	Type	Details
30	**Digital input status**	BITMAP	bit 0 - Status of input (0 disabled / 1 enabled)
31	**Digital output status**	BITMAP	bit 0 - Status of output (0 disabled / 1 enabled)
32	**Power supply 1**	UINT16 (0 ... 65535)	Unit : dV
33	**Power supply 2**	UINT16 (0 ... 65535)	Unit : dV
34	**Internal temperature**	INT16 (-32768 ... 32767)	Unit : °C
...			
40	**Main WAN Status**	UINT16 (0 ... 65535)	0: All Down / 1: ADSL / 2: Ethernet / 3: Cellular / 4: Wi-Fi
41	**ADSL WAN status**	BITMAP	• bit 0: ADSL WAN State (0 disabled / 1 enabled) • bit 1: ADSL WAN Connected (0 disconnected / 1 connected)
42	**Ethernet WAN status**	BITMAP	• bit 0: Ethernet WAN Status (0 disabled / 1 enabled) • bit 1: Ethernet WAN Connected (0 disconnected / 1 connected)
43	**Cellular WAN status**	BITMAP	• bit 0: Cellular WAN State (0 disabled / 1 enabled) • bit 1: Cellular WAN Connected (0 disconnected / 1 connected)
44	**Wi-Fi WAN status**	BITMAP	• 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)
...			
50	**ADSL WAN Down Rate**	UINT16 (0 ... 65535)	Unit : kbits/s
51	**ADSL WAN Up Rate**	UINT16 (0 ... 65535)	Unit : kbits/s
52-53	**ADSL WAN Down SNR Margin**	REAL (-3.40e+38 ... 3.40e+38)	Unit : dB
54-55	**ADSL WAN Up SNR Margin**	REAL (-3.40e+38 ... 3.40e+38)	Unit : dB
...			

Register	Content	Type	Details
70	**Cellular WAN Signal level**	INT16 (-32768 … 32767)	Unit : dBm
71-72	**Cellular WAN SNR**	REAL (-3.40e+38 … 3.40e+38)	Unit : dBm • Register 71 - bit 0: LSB • Register 72 - bit 15: MSB
73	**Cellular WAN Bytes Received**	UINT16 (0 … 65535)	Unit : Megabytes
74	**Cellular WAN Bytes Transmitted**	UINT16 (0 … 65535)	Unit : Megabytes
75-76	**Cellular WAN Total bytes**	UINT32 (0 … 4294967295)	Unit : Megabytes
…			
80	**Wi-Fi WAN Frequency**	UINT16 (0 … 65535)	Unit : MHz
81	**Wi-Fi WAN Signal level**	INT16 (-32768 … 32767)	Unit : dBm
…			
90	**LAN Interfaces states**	BITMAP	**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
91	**Wi-Fi LAN states**	BITMAP	• 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 Digital input (0 disabled / 1 enabled)
92	**M2Me remote access states**	BITMAP	• bit 0: M2Me Active (0 disabled / 1 enabled) • bit 1: M2Me Connected (0 disconnected / 1 connected) • bit 2: M2Me Proxy (0 disabled / 1 enabled)
93	**M2Me number of connected remote users**	UINT16 (0 … 65535)	
…			
100-109	**OpenVPN ingoing VPN states**	BITMAP[10]	bit X: VPN n° X Connected (0 disconnected-not created / 1 connected)

Register	Content	Type	Details
110-119	**OpenVPN outgoing VPN states**	BITMAP[10]	bit X: VPN n° X Connected (0 disconnected-not created / 1 connected)
120-129	**IPsec VPN states**	BITMAP[10]	bit X: VPN n° X Connected (0 disconnected-not created / 1 connected)
...			
500-549	**Message sender**	STRING[50]	50 registers made to write 99 characters (ASCII, Latin-1, UTF-8) - Not used for SMS
550-599	**Message destination**	STRING[50]	50 registers made to write 99 characters (ASCII, Latin-1, UTF-8) - Must be a valid phone number or E-mail
600-649	**Message subject**	STRING[50]	50 registers made to write 99 characters (ASCII, Latin-1, UTF-8) - Not used for SMS
650-773	**Text message to be sent**	STRING[123]	123 registers made to write 246 characters (ASCII, Latin-1, UTF-8)

10.7. Pairing with the EFM

Router Fleet Management

ETIC Telecom has a product called the **EFM** which allows you to manage a fleet of ETIC Telecom routers.

Pairing configuration

To be part of a fleet managed by a EFM, the router must be configured to specify which EFM it will be managed by. To do this, go to the menu ***Home*** > ***Setup*** > ***System*** > ***EFM*** and fill in the following parameters :

Enable	Enable router management by a EFM
Unique identifier of the organization	Unique identifier of the organization to which the router belongs
Your unique personal identifier	Your unique personal identifier
EFM IP Address or Hostname	IP address or Hostname of your EFM. By default, this is the hostname of ETIC Telecom's EFM SaaS **WARNING** Make sure the router is able to make the DNS resolution if you are using a hostname.

EFM Product key	EFM product key. By default, this is the ETIC Telecom EFM SaaS product key
Description	Router description for details on its use (Optional)
Latitude	Latitude of the router's GPS position (Optional)
Longitude	Longitude of the router's GPS position (Optional)

EFM authentication

It is possible to specify `EFM` as the authentication type for Administrators and Operators. See the EFM section of the Authentication page for more details.

11. 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.

11.1. Logs

See section Logs management

11.2. 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

11.3. 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

11.4. 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 Wi-Fi client (and not as a Wi-Fi access point)

11.5. 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

11.6. GPS

Access the menu ***Home > Diagnostics > GPS*** to obtain the available GPS information.

11.7. 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.

11.8. Advanced diagnostic

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

11.9. Logs

Multiples logs are available to help troubleshooting the router.

Go to the ***Diagnostics > Logs*** to access them.

All the logs pages have:

Filter	Accept a `regexp` to filter the content of the logs.
Clear log button	Clear the log. **WARNING** This action clear the logs `INSIDE` the router, this can't be undone.
Refresh button	Reload the current page with logs from the router

NOTE A log integrity mechanism has been implemented for the `Audit Log`. When it is displayed, a check is performed to ensure that this log has not been altered. If this is the case, a message is displayed indicating that the check failed.

Tags are placed in the logs to indicate in which log block the error was identified.

Main

This log contains main events of the router to ensure the system is running correctly.

Sections have been defined to help focus on specific part:

- SECURITY: Security like user authentication on the router
- CONFIGURATION: Eveything that concerns the configuration
- NETWORK: Network interfaces state or changes
- SYSTEM: Internal System events
- HWMON: Hardware monitoring
- GTW_RSIP: Gateway RSIP
- MESSAGING: SMS messaging and pagers
- DATALOGGER: Specific Datalogger logs
- REMOTE_ACCESS: Remote access events like M2Me connections

OpenVPN

Logs of every OpenVPN servers and clients. Each of them have its own tab.

IPSec

All logs from the IPSec internal tool.

Firewall

Logs from Firewall rules. The option **Log** as to be set to `Yes` in the screen ***Setup*** > ***Security*** > ***Firewall*** > ***WAN traffic filter rule*** for this rules to be logged in.

Audit trail

Are logged:

- User/Administrator connections and connections attempts
- All administrator actions (and attempts) that change the router configuration

This log records every action of every user. This is useful for analyzing what was done on the router and verifying non-repudiation of actions on the router.

Clear log button is not available for this log, as it serves a security purpose.

Advanced

Contains the Main log. But also more logs from internal components.

11.10. Visual diagnostic

At power up, the 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.

11.11. SSH commands

Useful commands

If you access SSH with a Super Administrator, you can access some useful linux commands for network diagnostics.

Some commands may be restricted to not interfere with firmware functionality and security. For example, `ifconfig eth0 192.168.0.128` will not work.

Command	Description
ifconfig	Show used ip addresses (You can't change ip addresses)
route	Show routes of the router (You can't add routes)

Command	Description
ping	Ping some devices
traceroute	Determine the path taken by packets
iperf	Test network performances
tcpdump	Analyze packets

12. MAINTENANCE

Configurations management	Save/restore a configuration, upload a configuration or return to factory configuration.
Firmware update	Check the available updates and update the firmware
Software options	Add software options to the router
Reboot	Force a router reboot
Parameters Errors	Summary of parameters errors on the current configuration

12.1. Configurations management

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

IMPORTANT	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.
Edition mode 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

12.2. 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**.

NOTE	The update file must be signed by Etic Telecom to be valid. Any other file will be rejected.

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.

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

13. COLLECT & ALERT

The Collect & Alert option available on RAS and IPL routers allows you to remotely monitor one or more PLCs. Modbus TCP and OPC UA PLCs can be addressed. When combined with serial-to-IP gateways, Modbus RTU can also be monitored.

The routers are capable of communicating with the PLCs and reading their registers. This allows you to:

- Display and write the current values of variables on the operating page
- Configure alarms to receive an email/text message if a threshold is exceeded
- Generate a report containing the evolution of variables

13.1. Variables and Synoptics

To view/write the PLC registers accessible from the router, it is necessary to configure the communication between the two.

The configuration is done through several steps:

- Data source: configure access to a data server (OPC UA or ModBus)
- Variables: attached to a data source, they correspond to one or more registers
- Synoptics: allows the display of variables to operators on the operations page

To assist with configuration, you can view the status of data sources and variables in the ***Collect&Alert*** > ***Server state*** page.

Data sources

Access the ***Collect&Alert*** > ***Data sources*** menu. You can configure new data sources there.

Enabled	Enable or disable the data source
Data source name	Name to identify the data source
Data source type	`ModBus` or `OPC UA`

The following parameters depend on the data source type.

ModBus

Sampling period (seconds)	Interval between two data source readings
Timeout (per variable)(seconds)	Timeout for reading a variable. Note that one reading is performed per variable.

IP adress of the ModBus server	ModBus Server IP Address
Server port	ModBus Server Port
Modbus Slave or Unit ID	ModBus Slave or Unit ID where to read registers on the server
Read bit op	Code to use for reading a PLC bit
Read word (16bit)	Code to use for reading a 16-bit word
Read double word (32 bits)	Code to use for reading a 32-bit word
Read float (32 bits)	Code to use for reading a 32-bit Float

OPC UA

Publishing interval (seconds)	Interval between two data source readings
IP adress of the OPC UA server	OPC UA Server IP Address
Server port	OPC UA Server Port
Username/Password Authentication	Allows you to configure a connection to the server with a login and password. If disabled, the server must accept anonymous connections.

The OPCUA connection security mode is `None`.

Variables

Access the ***Collect&Alert*** > ***Variables*** menu. You can create variables associated with data sources.

Name	Variable Name
Variable type	`ModBus`, `Digital Input` or `OPC UA`
Data source	(OPC UA, ModBus) Data source from which the variable will be read
NodeID Namespace Index	(OPC UA) Namespace in the OPC UA server where the variable can be found
NodeID ID Type	(OPC UA) Type of variable identifier
NodeID ID	(OPC UA) Variable identifier. String or numeric depending on the type
Register address	(ModBus) The variable's register. If the variable is on two registers (32 bits), the next register will also be used.

Variable Type

The variable can be of different types:

- Bit
- Bit in word (ModBus only)
- Unsigned 16bit integer
- Signed 16bit integer
- Unsigned 32bit integer
- Signed 32bit integer
- 32bit Float

Depending on the type, fields are available. The main ones are:

Decimal places	Number of decimal places to display
Gain	Multiplier of the value read from the register
Offset	Offset of the value read from the register. Applied after the gain
Unit	Corresponding unit
Value when 0	Value to display if the bit is at 0
Value when 1	Value to display if the bit is at 1

Trigger an alarm

An alarm can be associated with each variable. If the configured condition is met, an alarm is raised.

Alarm trigger	Configuring the alarm triggering condition
Acknowledge required	The alarm must be explicitly acknowledged even if the condition is no longer met
Failure description	Description that will be associated with the alarm

It is possible to associate an alert with these alarms to notify a recipient by email and/or SMS (see the Alert Cycles page).

Managing write permissions for a variable

Write permissions for a variable are managed using the Collect & Alert roles. See the Writing a variable page.

Synoptics

A synoptics groups a set of variables from one or more data sources. This allows you to view the variables on the operations page. This page is accessible to operators (see the Operations Web Page page).

Go to the ***Collect&Alert > Synoptics***] menu to create them.

13.2. Writing a Variable

Variables are associated with a data source and point to a register of it. See the Variables and Synoptics page for the configuration between a PLC's register and a variable.

Write permissions for a variable are managed through Collect & Alert Roles and Operators. Access the ***Collect&Alert > C&A Operator Rights*** menu to configure them.

NOTE	When writing an OPCUA variable, a new connection to the server is used. The OPCUA server must therefore accept at least 2 connections simultaneously to be able to read and write the variables.

Configuring write permissions for a variable

Collect & Alert roles

In the definition of a variable, it is possible to specify which role can write to it. A role can therefore have write permissions on a set of variables.

A role is defined by a unique identifier.

Role id	Role name

Collect & Alert operators

A Collect & Alert operator is the association between a user and a Collect & Alert role. A user can have multiple roles, which allows for fine-grained configuration of who can write variables.

An operator is therefore composed of a user and a role.

Collect & Alert role	Name of the role associated with the operator
User	User who will have write rights to the variables of this role

Writing a Variable

Once the roles and operators are configured, variables are written via the operations portal. The variable must be associated with a Synoptic to be visible in the operations portal.

To access the operations portal, the Collect & Alert operator must also be configured as an Operator. See the page Operators and access rights.

13.3. Alert cycles

Collect & Alerts alerts are associated with one or more variables.

If one of these variables reaches its alarm trigger condition, an alert is triggered and the recipients

are notified.

To add an alert, access the ***Collect&Alert > Alert cycles*** menu

Name	Alert Name
Variables triggering the alert cycle	The set of variables that trigger the alert
Recipients of the alert messages	Users to contact in the event of an alert
Type	Type of channel to use: Email and/or SMS
Reminder count	Number of reminders to send until the alert has been acknowledged
Reminder period (minutes)	Time Between Reminders

Alert Acknowledgement

Once triggered, an alert must be acknowledged if the variable is configured as such.

Acknowledgement can be done in several ways:

- Via digital input if the **Ack all alarms with digital input** option is enabled
- Via the administration page ***Collect&Alert > Alert status***
- Via the operations portal page ***Collect&Alert > Alarms***

14. HOTLINE SUPPORT AND VIRTUAL SHOWROOM

14.1. Hotline support

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

14.2. 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).

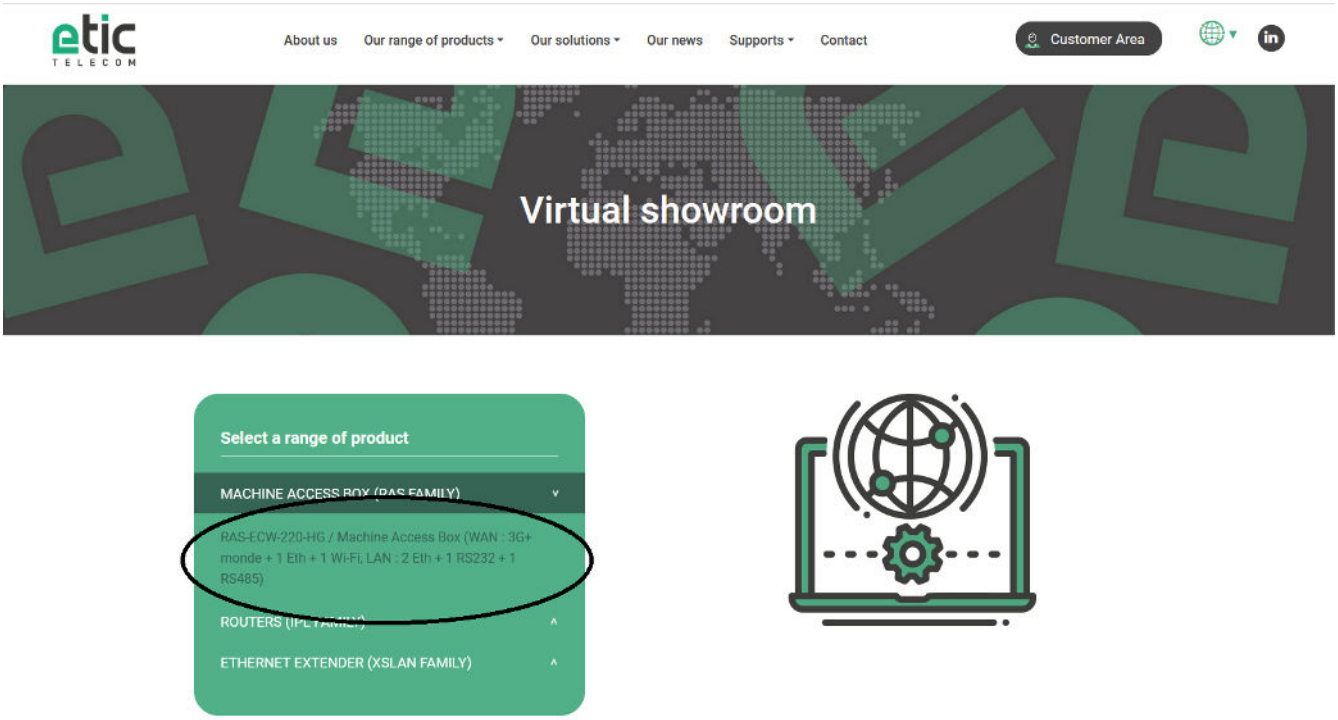


Figure 29. Access to Virtual showroom

14.3. 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 the hotline password generated from the administration page
- Disable the required hotline password by simplifying connection temporarily

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

Hotline 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.

Temporarily simplify Etic Telecom hotline connection to your router

Simplifying connection for Etic Telecom hotline will:

- enable remote access VPN even if you have not defined an operator for it
- make hotline password not required anymore. Remote users are still required to have a unique password that is exclusive to Etic Telecom for accessing your product.

You can perform it by one of these two actions:

- Holding the front button for 10seconds
- Clicking on the button ***Setup*** > ***Security*** > ***Administration rights*** menu and clicking **Simplify**.

The support team can now access your product for one hour, or until it restarts.

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