etic
TELECOMMUNICATIONS

RAS-M156e   RAS-I1128e
RAS- G134e   RASG12e

Remote access server
_____

User's guide
Document reference: 9014509-02
_____

Content

./.. CONFIGURATION

OPERATION

1. Product identification

RAS-	M156e	I1128e	G134e	G12e
Built-in V90 PSTN modem	•			
ISDN 64 Kb/s (SO EURO-ISDN)		•		
Built-in GSM modem			•	
Built-in GSM-GPRS-EDGE modem				•
1 Ethernet + 1 RS232 / RS485	•	•	•	•
User list	•	•	•	•
Safety callback	•	•	•	•
On demand callback	•	•	•	•
Fire-wall	•	•	•	•
DYNDNS	•	•	•	•
Internet callback	•	•	•	•
VPN (PPTP, IPSEC, TSL) over Internet	•	•	•	•
DNAT	•	•	•	•
Alarm E-mail –SMS	•	•	•	•
Modbus master & slave gateway	•	•	•	•
Raw client and server gateway	•	•	•	•
Telnet gateway	•	•	•	•
Multicast gateway	•	•	•	•
Unitelway gateway	•	•	•	•
IO web server (3 inputs . 1 output)	•	•	•	•
Html Configuration	•	•	•	•
IO Viewer optional software module	•	•	•	•

2. Product overview

2.1. Product function

The RAS provides to authorized users a remote access to the machines connected either to an IP LAN or to a serial RS232-RS485 interface, as if his PC was directly connected to the LAN or to the RS232.

On the user PC side, the communication can be set either with a dial up modem or through an internet access.

Direct dial-up communication	Internet communication
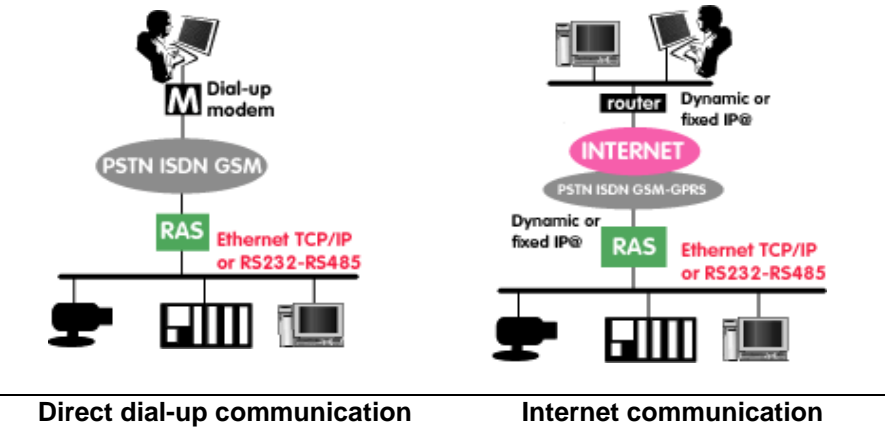
2.2. Remote PC to RAS communication capabilities

The communication between the remote user and the RAS can be either a dial-up communication or be established through the internet.

If the communication is established through the Internet, the public IP address assigned to the RAS can be dynamic or fixed (IP call back and DynDns functionalities).

The compatibility between the PC modem and line on one hand, and the RAS on the other hand, is summarized in the table below :

			M156e	I1128e	G134e	G12e
RAS reference ►			PSTN analog	ISDN BRI	GSM	GSM-GPRS
RAS line ►						
PC modem ▼	**PC line ▼**		▼	▼	▼	▼
PC + PSTN modem	PSTN analog	►	Yes	No	Yes	Yes
PC + ISDN adapter	ISDN	►	No	Yes	Yes	Yes
PC + ISDN modem / adapter	ISDN	►	Yes	Yes	Yes	Yes
PC + GSM modem	GSM	►	Yes	Yes	Yes	Yes
PC + GSM-GPRS-EDGE modem	GSM-GPRS	►	Yes	Yes	Yes	Yes
PC + Internet access	Any type (adsl …)	►	Yes	Yes	Yes	Yes

See Installation chapter for technical details.

2.3. Functions overview

Authorized users
The RAS prevents unauthorized access; it manages an authorized users list; a user name and a password is assigned to each of them.

Safety callback
If that option has been assigned to a user, the RAS calls the user back to its stored telephone number.

On demand callback
For economical reasons, and if that option has been authorized to a user, the RAS can callback the user to the telephone number he demands.

Fire-wall
The built-in firewall allows to limit the IP addresses and TCP ports to which each authorized user can connect.

Internet DynDns and IP callback
The RAS provides DynDns and IP callback functions; that functions allow to connect the user remote PC to the RAS through the internet even if the RAS public IP address is dynamic.

Secure connection over Internet (VPN)
The RAS is able to establish a secure connection (VPN) over the internet :
The VPN can be either PPTP for usual use, but also IPSEC or TLS.
With the VPN, a remote authorized user can connect to any machine of the LAN.

DNAT
If a VPN cannot be established through the internet, the DNAT function allows the user to access to some machines of the network.

RS to IP gateways
The product includes an up-to-date RS to IP gateway, allowing the user to connect remotely as well to IP as to asynchronous devices.

Emails – sms
A stored emails or sms can be transmitted each time the digital input is closed or opened.

The RAS can also transmit any email or SMS coming from an SMTP client connected to the IP network.

Html configuration
The RAS is configured with a PC and a web navigator. The configuration can be achieved through the ethernet interface or remotely.
For safety reasons, the remote configuration can be forbidden.

Specifications	
Dimensions	130 x 38 x 110 mm (h, l, p)
EMI	EN50082-2
Electrical safety	EN 60950
Thunder	EN61000-4 et -5 (2kW common & differential modes)
Supply voltage	RAS-M156e & RAS-I1128 : 9 to 40 VDC - 170 mA at 24 VDC
	RAS-G134e & RAS-G12e : 9 to 30 VDC - 300 mA at 24 VDC
Operating T°	0°/ + 60°C without condensation
PSTN Modem	V90 (56kb/s) compliant to E N CTR21 and US norms
ISDN adapter	BRI ETSI EURO-ISDN compliant
GSM-GPRS-EDGE	900-1800-1900 MHZ networks compliant
Ethernet	10 Mb/s
RS232-RS485	1200 to 115200 kb/s parity N / E / O
RS to IP gateway	Raw client and server Modbus master & slave Multicast – Telnet - unitelway
Safety protocols	PPP / PAP / CHAP Callback MS CB VPN : PPTP, IPSEC, TLS
Access control	User list (25 users) user name & password
Callback	Safety callback On demand callback
Fire-wall	IP and TCP ports limitation assigned to each user
Logs	Event logs (date and time)
Configuration	Using an html navigator Through the LAN or remotely

1   Product description

RAS-M156e / RAS-I1128e   RASG134e / RASG12e
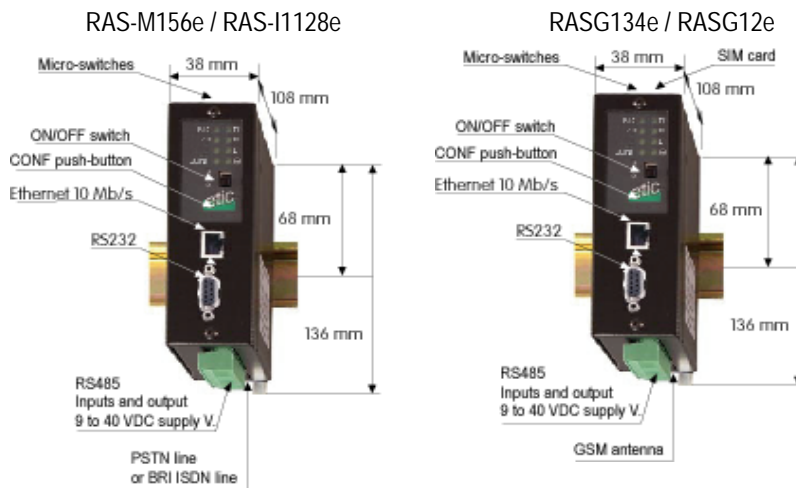
1.1   Leds

Led	Function
LINK	Ethernet connection OK
DATA	Ethernet network activity
RD	Characters received from the PSTN or ISDN or GSM
TD	Characters transmitted to the PSTN or ISDN or GSM
L **or** **L /**	Lit : remote connection established Blinking : GSM only : the number of blinks indicates the quality of the reception signal
CONF	The remote configuration has been authorized (the CONF push-button has been pressed)
⊛	Power led

1.2 Connectors

2 pins screw-block : Supply voltage		
Pin	Signal	Function
1	+	RAS-M156e RAS-I1128e :+ 9 to 40 V – 170 mA at 24 VDC RAS-G134e RAS-G12e :+ 9 to 30 V – 300 mA at 24 VDC (on line)
2	-	Ground

8 pins : Inputs / outputs		
Pin	Signal	Function
1	+	3 V DC provided by the RAS
2	IN1	Digital input Nr 1
3	IN2	Digital input Nr 2
4	IN3	Digital input Nr 3
5	OUT1	Relay output 1
6	OUT2	Relay output 2
7	B +	RS485 polarity B
8	A -	RS485 polarity A

Pin	Circuit		Designation	RAS - Terminal
1	CD	109	Carrier detect	⇒
2	RD	104	Data Reception	⇒
3	TD	103	Data Emission	⇐
4	DTR	108	Data terminal ready	⇐
5	GND	102	Ground	
6	DSR	107	Data set ready	⇒
7	RTS	105	Request to send	⇐
8	CTS	106	Clear to send	⇒
9	RI	125	Ring indicator	⇒

1.3 Micro-switches

Micro-switches		
SW 1	**SW 2**	
OFF	OFF	The current IP@ of the product is the stored IP @
ON	OFF	The active IP@ of the product is the factory IP@: 192.168.0.128 the IP@ automatically assigned the remote user is 192.168.0.129
OFF	ON	The active IP@ is the Ip @ provided by the BOOTP or DHCP server.
ON	ON	Reserved
SW3		
OFF		Access to the administration server is protected by the login and password which have been set.
ON		Access, from the LAN, to the administration server is not protected.
SW 4 to 8		Not used

2   Supply voltage

RAS-M156e or RAS-I1128e
The supply voltage must be strictly lower than 40 VDC and higher than 9 VDC. The consumption is 170 mA at 24 VDC.

RAS-G134e or RAS-G12e
The power supply module must be powerful enough to provide the peak current which occur during a GSM communication.

The supply voltage must be strictly lower than **30 VDC** and higher than 9 VDC. The consumption is 300 mA at 24 VDC when the product is on-line.

3   Fuse

The power input is protected with a 3A fuse.
!!! A replacement fuse is available on the board ; it is located over the leds.

4   Ethernet interface

The ethernet interface is a 10 Mb/s interface.

To connect a PC directly to the RAS, use the cross wired red cable provided with the product.

5   Fans

To avoid overheating when the ambient temperature is high, leave a 1 cm space on each side of the product.

6   Telephone line connection (RAS-M156e)

The RAS-M156e is designed to be connected to an analog telephone line.

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

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

Important nota : The type of public lines connecting the company PBX to the public network does not matter; it can be PSTN but also ISDN, for instance.
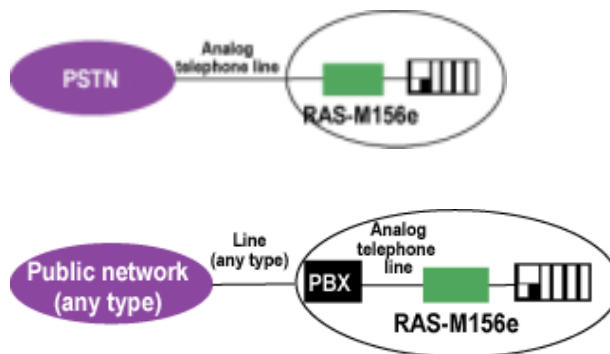
7　ISDN connection (RAS-I1128e)

The RAS-I1128e is designed to be connected to a ISDN BRI interface (EURO-ISDN compliant).
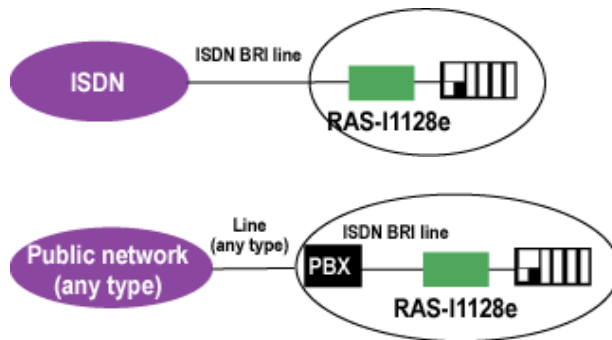
8　GSM products installation (RAS-G134e or RAS-G12e)

Checking the GSM reception signal level before installing
Before installing the product, check that the GSM reception signal level is good enough at the location you want to install the product; that test can be done with a usual mobile phone using the same provider.
The signal level must be good or excellent.

GSM subscription
The micro-sim card must be inserted in the slot located at the top of the product.

No password must be set.

Antenna
If the cabinet in which the RAS has to be installed is made of metal, the antenna has to be installed outside the cabinet; for instance on the top of the cabinet.

The antenna must be ordered separately; the models below are available :

ANT200	ANT200	ANT200
0 db gain - magnetic	0 db gain	3 db gain
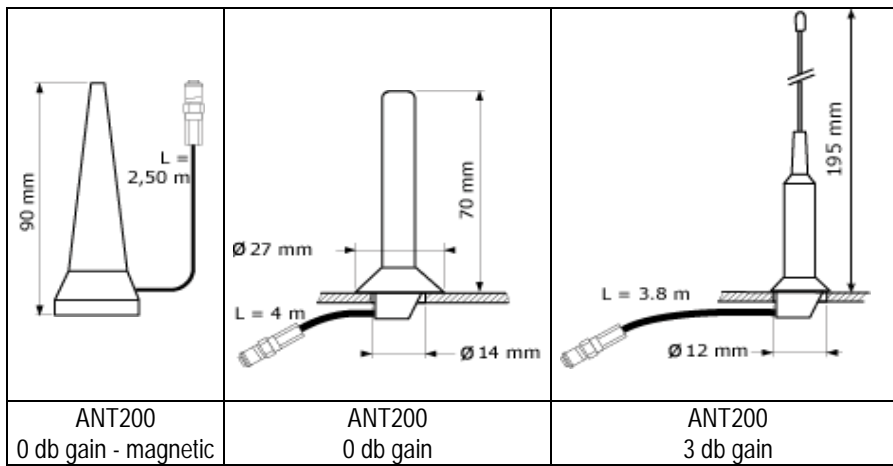
Checking the reception signal level after installation

When powering the product on, the **L /** led gives an indication of the GSM signal quality :

the L / led	Signification
... briefly blinks 3 times	**The quality of the reception signal is fine**
... briefly blinks 2 times	**The quality of the reception signal is acceptable**
... briefly blinks 1 time	**The quality of the reception signal is poor**
... is turned off	**No reception** Is a GSM voice communication possible ? has the sim card been correctly inserted ?

The Led must blink 3 times to ensure the transmission quality will be good.

9   GPRS service availability (RAS-G12e)

GPRS and GPRS-EDGE are services using the usual GSM network.

The GPRS service provides an IP permanent connection to the Internet at a medium data rate.

The GPRS-EDGE the same service as GPRS but at a higher data rate.

The effective data rate depends of the operator and the reception quality.

The GPRS or GPRS-EDGE services can be unavailable even if the GSM service is available. It is why, before installing, check with the provider if that services are available at the location you want to install the RAS.

Any way, if the GPRS is not available, the RAS-G12e RAS will automatically use the low speed GSM data service (9600 b/s).

10   RS232 / RS485 interface

The RAS provides an RS232 and an RS485 interface.
Asynchronous products can thus be integrated to the IP network.

RS232
The RS232 cable must not be longer than 10 meters.

RS485
If a product must be connected to the RS485 and if the distance is greater than 10 meters, a 10 KOhm termination resistor will have to be connected between the A and B signals.

11   Inputs / outputs connection

The input Nr 1 can be used to control the connection to the Internet or to send an email or a SMS (see configuration chapter).

The status of each input can be displayed with the web browser.

The digital output can be set off or on with the web browser.
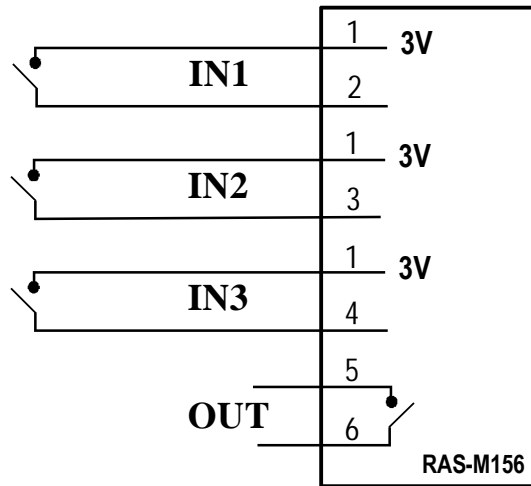
Relay output :   Max. voltage 50 VDC
                       max. current : 500 mA

Inputs: Not isolated
                       Maximum differential voltage : 20 VDC

12   Internet subscriptions

12.1 Remote user PC subscription

Any internet access is convenient.

A VPN can be set between the PC and the RAS; in that case, the internet access (router..) of the remote PC must be configured as follows :

- The TCP port # 1723 (VPN using PPTP) must be open.

- The IP protocol GRE 47 (Generic Routing Encapsulation) must be accepted.

Nota : If setting a VPN is not necessary or not possible, the link with the machines can be however established using the DNAT rules (see configuration chapter); in that case, the communication through Internet will not be protected.

12.2 RAS subscription

The provider must be a national provider (I.e. of same country as the country where the RAS is installed).

TCP Port 1723 must be open; and the IP47 "GRE" protocol must be authorized.
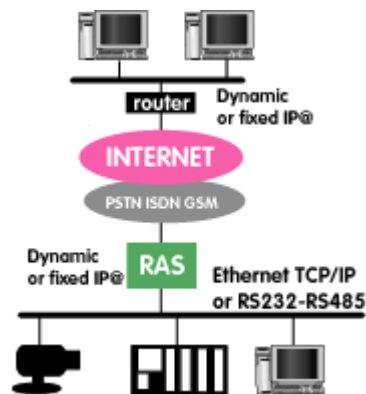
1   Overview

The RAS is configured using an html navigator.
The first configuration will be either carried out trough the ethernet interface or remotely through the PSTN or ISDN or GSM network.

2   Configuration through ethernet

2.1   Configuration with a PC directly connected to the RAS

Step 1 : Create or modify the PC TCP/IP connection
Assign to the PC an IP @ in accordance with the RAS IP address.

Note :
Coming from factory, the RAS IP address is 192.168.0.128. At the first configuration, assign 192.168.0.127 to the PC . (see appendix 1).

Any case, the factory IP address of the RAS can be restored by setting the micro-switches SW1 ON and SW2 OFF.

Step 2 : Connect the PC directly to the RAS ethernet interface
Using the red cross wired cable provided with the product.

Step 3 : Launch the navigator
Enter the IP @ of the RAS.

The Home page of the administration server is displayed

Note : The factory IP address of the RAS is **192.168.0.128**

2.2 Configuration through the LAN

Case of a LAN with a BOOTP or DHCP server

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

Step 2 : Launch ETIC FINDER to detect the RAS over the LAN.
Click the product once detected.

The Home page of the administration server is displayed.

Note :
If the identification window is displayed but not the Home page of the administration server, the Login or the password are wrong. See paragraph 4 and 5.4

Case of a LAN without BOOTP or DHCP server
Careful : If it is the first configuration of the product, it is advised to connect directly the PC to the RAS.

3   Remote configuration

The initial configuration can also be achieved remotely.

Step 1 : Create a « remote PPP connection» in your PC
(See appendix 2).

Step 2 : Complete the
remote connection windows

• Select the remote connection »
icon.

• Enter the user name and the
password (**admin** & **admin** are the
factory user name and Password).

• Enter the telephone number
assigned to the RAS line.

• Wait for the connection message
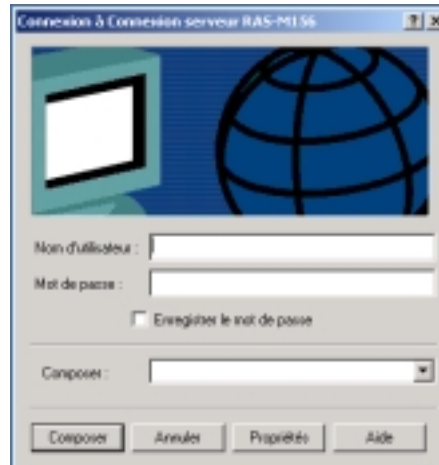
Step 3 : Connect to the RAS
html server
• Click the remote connection icon,
and then the "detail" button; the RAS
IP address is stated (the RAS factory
IP @ is **192.168.0.128**).

• Launch the html navigator and
enter the RAS IP address (don't enter
www).

The RAS server home page is
displayed.

Note :
If the home page is not displayed, See paragraph 5.
See paragraph 6.3.1 to protect access to the administration server

4   Wrong IP address or Login

if the RAS IP address you entered is wrong, you can recover the factory IP address by setting the SW01 ON.
The 192.168.0.128 IP address will be accepted by the RAS as long as the SW01 microswitch will be left ON.

Wrong Login to the administration server
The access to the administration server can be protected by a login and password; If the Login entered to access to the administration server is wrong, you can recover a free access, only from the LAN, by setting the SW03 microswitch ON.

5   Product configuration

5.1   Saving configuration modifications

•   **After every modification, click the « Save » button at the bottom of the screen.**

•   **When the configuration has been completely carried out, click the « restart » red button in the green bar.**

The RAS will restart; the telephone call will be cleared.

5.2   Administration server overview

System

IP protocol	To enter the IP @ of the RAS To enter the IP @ automatically assigned to the remote user
User list	To assign an ID and PWD to each user and define their rights.
Target	To define the machines which will have to be protected by the firewall
Date & time	
Modem	To change the initialization AT command sent to the built-in modem.
RS232/RS485	To set the RS232 – RS485 data rate and frame
SNMP	To define traps and SNMP server
Firmware upgrade	To upgrade the product firmware
Save	To download / upload the configuration file of the product
Restart	To restart the product

Security

Administration	To protect and limit access to the administration server.
Firewall	To build the filters
VPN	To set the VPN parameters

Internet

Account	To enter the internet account parameters
Routing	To enable internet routing and set parameters To set DNAT rules
Remote control	To set the conditions the RAS will connect to the internet
Dynamic IP address	To define the way the RAS will transmit its public IP address to the remote user or to the remote user PC

IP to RS gateway

Modbus	To configure the modbus gateway.
Transparent	To configure the raw, multicast & telnet gateway
Unitelway	To configure the unitelway gateway

Diagnostic

Logs	To display the Logs
Network status	To display all the parameters of the connection in use
Microswitch	To display the microswitches current position
Ping	To ping a machine
Syslog	

E-mail alarm   To define the conditions the RAS will send a mail or a SMS

About   To display the firmware and hardware identification

5.3 « System configuration » menu

5.3.1 « IP Protocol» menu
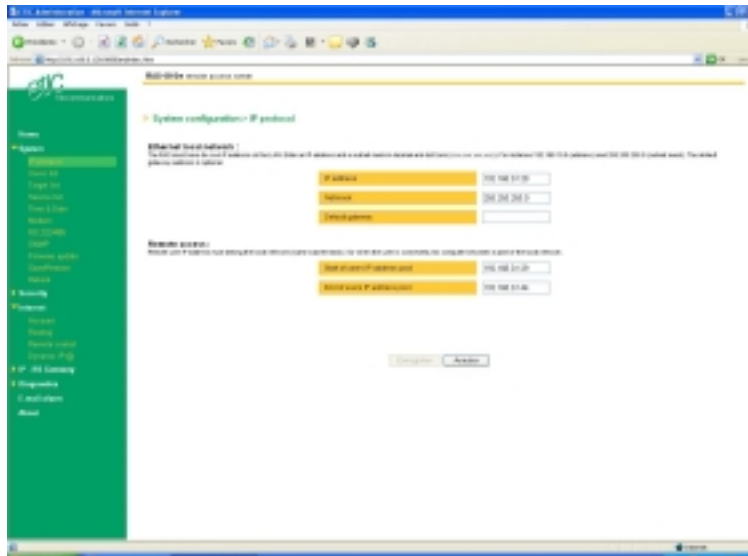
RAS IP @
It is the IP address of the product over the LAN

Netmask
To define the IP domain ; default is 255.255.255.0.

Default gateway :
The default gateway address must be entered only if other routers are connected to the LAN

Remote IP @
Enter the base address of the pool which will be automatically assigned by the RAS to the PC of a remote user.
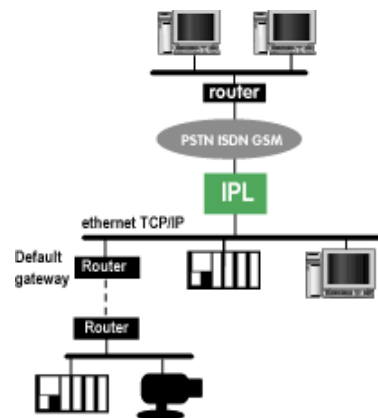
5.3.2 "User list" menu

Display the user list table

- Click the « System » menu and then «User ».
The user list will be displayed.
Each line of the user list comprises the user name and the filter name which is assigned to him.

Coming from factory, the user list includes only 1 user defined as follows

User name :   admin
Password :   admin

Display the parameters of a user

- Click « View »

Modify the parameters of a user

- Click « modify »

Add a user

- Click « add a user » at the bottom of the page.

Enter the user settings and save.

Users list

User form

Parameter « Active» (value Yes or NO)
Choose No if you want to prevent the user to access the network.
Choose yes to authorize the user to access to the network.

Parameter « Full name»
It is the name displayed in the user list.

Parameters « Login » & « password »
The login and the password have to be entered by each user at the beginning of the remote connection.

Parameter « Phone»
Enter the number of the telephone line from which the user usually calls.
That number will be used by the RAS in two cases :
*   To callback the user if the « Filter calling number » option has been set ;
*   to authorize access to that user only when he calls from that line if the callback « forced » option has been set.

Parameter « Filter calling number»
If that option is set, the user will access to the network only if he calls from the line number assigned to the parameter « phone » (see above).

Parameter « callback »

Callback = None : Once the Login and password of the calling user have been checked, he will be connected to the LAN.

Callback = Allowed : Once the login and password of the calling user have been checked, he is allowed to enter a telephone number to which the RAS will call back as soon the current connection will have been cleared.

Callback = Forced : Once the login and password of the calling user have been checked, the RAS clears the call and   automatically calls back using the telephone number stored as « Phone » (see above).

Parameter « e-mail »
The RAS will send an email to that address in 2 situations :
Alarm email : the RAS sends an alarm email to the defined user If the input 1 is closed or opened (if that option has been set).

Internet connection email : Once connected to the Internet, the RAS will send to the demanding user an email containing the dynamic IP @ assigned to the RAS by the provider. (See OPERATION chapter).

5.3.3 « Target list» menu

This menu allows to define the IP addresses of the machines belonging to the network.

The RAS will use these information to build the firewall filters.

5.3.4 « Date & time » menu

Check date and time to ensure the logs will be correctly dated.

5.3.5 « Modem » menu

Dial prefix :
It is the figure the RAS will add to each number to dial-out to the public network.

Default initialization string
This parameter defines the AT initialization sequence which is transmitted by the RAS to the built-in modem.
The default sequence must only be modified in case of difficulty and after discussion with ETIC hotline.

Product location
Select the country in which the RAS will be installed ; or leave
« international ».

5.3.6 « RS232 RS485 »

This menu allows to define the operating conditions of the RS232-RS485 serial interface.

5.3.7 « Save / restore » menu

That menu allows to store the configuration file in a PC hard disk or to download a stored file to the RAS.

5.3.8 « Reboot » Menu

To restart the unit.

5.4 "Security" menu

That menu allows to define the security policy :

- Access restriction to the administration server

- Access restriction to the machines (firewall)

- VPN over Internet

5.4.1 «Administration rights» menu

The « administration rights » menu allows

- to restrict access to the administration server from the LAN,

- to restrict or forbid remote access to the administration server.

Local management parameter

- **Local management = « Allowed »** : Any user can access the administration server from the ethernet interface or through the LAN. He will have to enter the login & password if that option has been set (see below).

- **Local management = « Allowed after local action »** : To access the administration server, the user must first press the CONF button of the front panel of the product.
He will have to enter the login & password if that option has been set (see below).

Remote management

Remote management = « Allowed » : Any user can access the administration server remotely. He will have to enter the particular login & password if that option has been set (see below).

- **Remote management = « Allowed after local action »** : To give access to the administration server remotely, the CONF button of the front panel of the product has first to be pressed.
The remote user will have to enter the login & password if that option has been set (see below).

- **Remote management = « forbidden »** : remote access to the administration server is forbidden.

- **Login & password**
  Enter the login & password which will have to be entered to access the administration server and confirm.

Attention : If you don't remember this login & or password, you can cancel the protection by setting the microswitch Nr 3 ON.

5.4.2 « Fire-wall » menu

5.4.2.1 Overview

One filter is a list of IP addresses and TCP ports.

2 policies can be applied to use one filter :

- **Cautious policy :** Access to the listed machines (IP address + TCP port) is allowed ; and the rest of the domain forbidden. This policy is cautious, because the authorized machines are precisely pointed out ; access to any other machine is forbidden.

- **Opened policy :** Access to the listed machines (IP address + TCP port) is forbidden and the rest of the field is authorized. This policy is opened, and not advised, because access to any machine, except the listed ones, is authorized.

25 different filters can be built.

Once the necessary filters have been built, any of them can be assigned to each user. In that way, a user will access only to an individually authorized area.

5.4.2.2 Building the firewall

Important nota bene : Before processing, check at least one machine (IP address + TCP port) has been created (menu « System » and then « target list »). :

Step 1 : Complete, if necessary, the list of declared TCP ports (also called « services »)

Step 2 : Build the filters.

Step 3 : Assign a filter to each user.

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

Important nota bene : The main services (html, ftp, modbus) are available from factory; for that reason, most of the time, that step can be skipped.

- Select the menu "system" and then "service list" The list of TCP ports is displayed.

- Click « add a service ».

- Enter the label of that the new service, assign a protocol (udp, tcp, icmp) and a port number.

- Save. The list is updated.
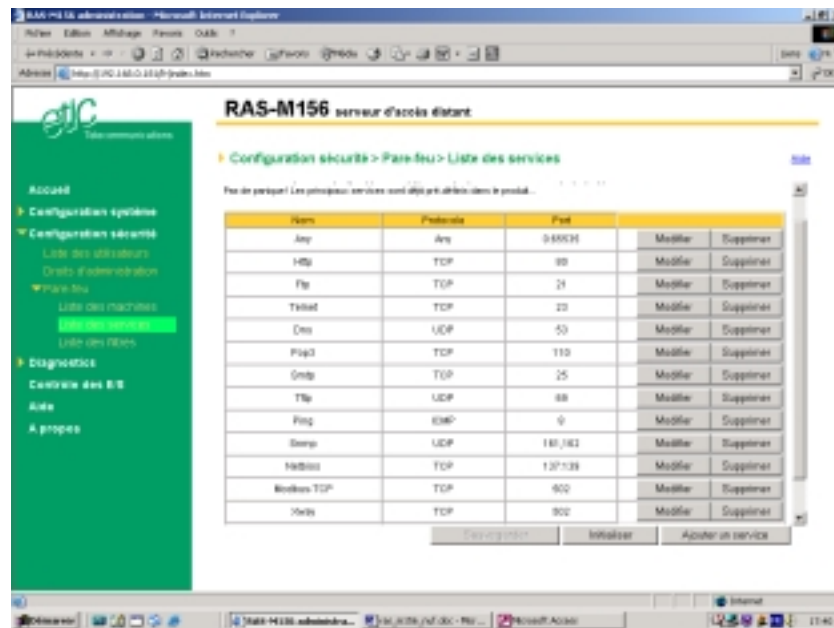
Step 2 : Build a filter

- Select the « security» menu, then « firewall» and then «Filter list» The list of the stored filters is displayed.

- Click « add a new filter »

- Assign a name to the new filter

- Choose the policy ; « All is forbidden except what we specify » is the advised policy.

- Click « add a new rule to the list ».

- Select a host (also called machine or IP address) among the ones which have been stored and a service (also called TCP port).

- Add other rules if necessary.

- Click OK when the filter is complete ; the updated filters list is displayed.

Step 3 : Assign a filter to each user

- Select the menu « Security» and then « User list ».

- Among the users select a user to which you want to assign a filter ; and click modify ; the user window is displayed.

- Assign a filter to the user ; click OK and save.

5.4.3 « VPN » menu

This menu allows to select which type of VPN will be used to protect the link between the remote user PC and the RAS over the internet.

For usual operation, select PPTP (no parameters have to be set in that case).

5.5 « Internet configuration » menu

5.5.1 "Account" menu

The information you have to enter her are provided by the internet provider ; see your subscription document.

Phone number
Enter the telephone number the RAS has to dial to connect to the Internet provider.

Login and password
Enter the Login and password which the RAS will have to transmit to the when connecting to the internet.

Outgoing mail server (SMTP)
 Ex : smtp.free.fr

Account E-Mail address
Enter the mail address associated to the internet account.

5.5.2 « Routing » menu

« Route LAN traffic to Internet » parameter :
If that option is selected, the RAS will route to the Internet the Ip frames the IP addresses of which are not in accordance with the LAN netmask.

Note :
1. The IP address of the RAS must be declared as the « default gateway » inside each machines of the LAN.

2. It is not necessary to select that option if the RAS just has to send an email when the digital input is active.

« Idle time before disconnecting from Internet » parameter:
Once connected to the Internet, the RAS will disconnect from the Internet after that delay if no IP frames have to be routed from the LAN.

Nota bene : The « Idle time before disconnecting from Internet » parameter applies only if the connection has been established by the routing process; it does not apply if the connection has been established on demand of a user or remote user.

"First packet time-out" parameter :
Once connected, and after that delay, the RAS will disconnect if a first IP frame has not been received from the Internet.

"Wait time for VPN connection" parameter :
Once connected to the Internet, and after that delay, the RAS will disconnect from the Internet if no authorized VPN client has been established.

DNAT rules table

Each line of the table defines a link between a service over the internet and a couple machine and service over the private LAN.

That rules can be used if a VPN secure connection cannot be set.

Let us assume that the remote user wishes to communicate with the PLC1 port 102 and also with the PLC2 port 502 and with the PC port 80.
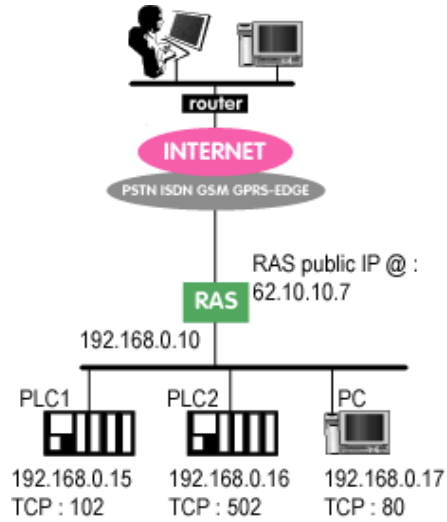
The following rules have to be entered :

Internet / WAN interface	LAN translation	
Service	Machine	Service
102	192.168.0.15	102
502	192.168.0.16	502
80	192.168.0.17	80

5.5.3 "Remote control" menu

This menu allows to define at which conditions the RAS will connect to the internet.

5 non exclusive possibilities are offered :

« Connect to Internet after an incoming phone call from … » :
If a telephone number is entered, the RAS will connect to the Internet each time it detects an incoming call from that line.
The line to which the RAS is connected must offer the caller ID function.
The * (star) character can be used to replace any numeric character;
For example,
If the number *042000 is entered, any caller id number finishing with the figures 042000 will cause the RAS to connect to the Internet.

«Allow Internet callback» :
If that option is selected , the RAS will connect to the Internet if the user requests an internet callback.
The user has first to call the RAS directly through the PSTN (or ISDN or GSM) and ask for an Internet callback by entering the figure « 0 » (zero) in the callback pop up displayed at the end of the calling process. The RAS will clear the call and will immediately connect back to the internet.

« Connect to Internet as soon as the RAS is on.»
If that option is selected, the RAS connects to the internet as soon as the OFF/ON switch of the front panel will have been set ON.

« Connect to Internet on a rising edge of input 1»
If that option is selected, the RAS connects to the internet as soon as the digital input #1 is active.

« Connect to Internet now»
Click the button to connect the RAS to the Internet.

5.5.4 "Dynamic IP address" menu

Once connected to the internet, the Internet provider assigns a public IP address to the RAS which remains valid during the duration of the connection.

The user remote PC has to know that address to be able to connect to the RAS through the internet.

3 possibilities are offered to communicate the RAS public IP address to the remote PC or to user of the remote PC.

- The RAS transmits its IP address to a well-known DynDns server.
- The RAS transmits its IP address to the remote user by email.
- The RAS transmits its IP address to a FTP server.

5.5.4.1 Transmission of the IP address to a DynDns server

Principle of DynDns operations :

Step 1 : DynDns account subscription
An account has to be subscribed to DynDns.org (web www.dyndns.org).
It consists in a login, password and in the host name assigned to the RAS.
Any host name you wish can be assigned; for example, "etic-ras" can be assigned, if it has not already been assigned.

Step 2 : RAS configuration
That host name, login and password have to be stored inside the RAS.

Step 3 : Operation

Each time the RAS connects to the internet (see remote control menu), it transmits its own IP address to the DynDns server in front of its hostname.
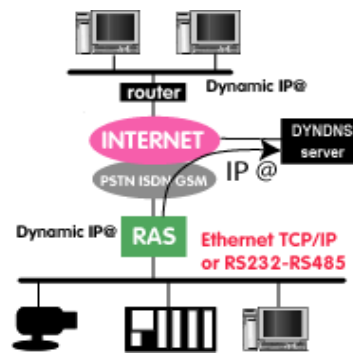
Each time he wants to connect to the RAS through the internet, the remote user will enter the RAS hostname (etic-ras.dyndns.org for instance) instead of the IP address which he does not know.

His PC will automatically go to the DynDns server, pick-up the RAS IP address …
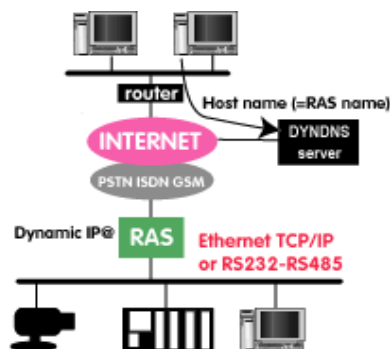
… and connects to the RAS
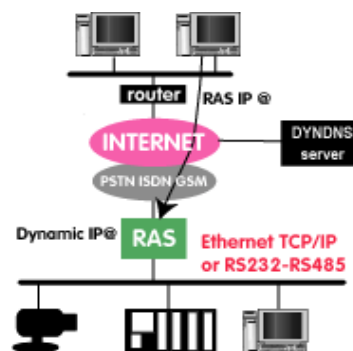
RAS configuration

- Enable the DNS option.

- Check the value of the "dynamic DNS provider" parameter is dyndns.org

- Enter the host name, login and password obtained from dyndns.org (www.dyndns.org web site)

- Enter the hostname assigned to the RAS.

5.5.4.2 Transmission of the IP address inside an email

When it connects to the Internet, a public IP address is assigned to the RAS by the provider.

That IP address has to be communicated to the remote user.

A mean to communicate that address to the remote user is to include it inside an email sent to the remote user.
The remote user will use that IP address to set a VPN and connect to the to the machines of the LAN.

To enable that method, a few parameters have to be set up.

« Inform of the IP address by email »
Select that option to enable the transmission of the public address to the remote user inside an email.

« HTML email with VPN launcher »
Select that option to include a VPN launcher inside the email to simplify the remote user procedure.

« Email default address »
Enter the email address the RAS will have to use to inform the remote user of its public IP address, once it will have got it from the provider.
That email address will be used only if the internet connection order is a local order : « connect » button or digital input nr 1 or OFF/ON switch.

Nota bene : If the order to connect to the internet comes from a remote user (Internet callback), the RAS will not use the default email address but

will refer to the email address assigned to the user to communicate its public IP address.

5.5.4.3   Transmission of the iP address of the RAS to a FTP server

instead of transmitting its public iP address by email to the remote user, the RAS can transmit an html page to a FTP server. That page will include the public IP address
The user will have to go to that FTP server to get the RAS public iP address.

Parameter « Transmit IP address to a FTP server»
Select that option if you want the RAS to transmit an HTML page to a FTP server.

Parameters « FTP server IP address» «Login name», « Password», « File path»
Enter the parameters of the FTP server.

5.6 «IP<>RS » gateway

That menu allows to configure the IP to asynchronous RS232-RS485 gateway included in the RAS.

The gateway can be used as well from the ethernet IP LAN as from a remote PC or both.
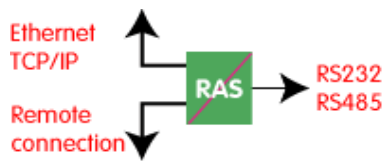
Using the gateway function does not prevent from transmitting from a remote IP machine to another machine connected to the IP LAN.

5.6.1 « Modbus » menu

The ETIC modbus gateway is made to link modbus devices connected to its serial interface to TCP modbus devices connected to the ethernet TCP/IP network or remotely.

5.6.1.1 Definitions

A **TCP Modbus client device** is a device connected to the ethernet TCP/IP network and able to send a modbus request to a modbus TCP server which is in charge of answering; A TCP modbus client is equivalent to a master.

A TCP Modbus server device is a device connected to the ethernet TCP/IP network and able to answer to a modbus request received from a TCP modbus client device. A TCP modbus server is equivalent to a slave.

A TCP modbus server can answer to any client of the Ethernet TCP/IP network.

5.6.1.2 ETIC modbus gateway capabilities

The ETIC modbus gateway can be configured

either

to link serial slaves to several TCP modbus clients devices connected to the ethernet network; in that case, select the modbus client gateway,

or

to connect a serial master to several TCP modbus servers devices connected to the ethernet network; in that case, select the modbus server gateway.

The modbus gateways can be used either by a device directly connected to the LAN or by a remote device, to communicate with the serial device.

5.6.1.3   Modbus server gateway

Modbus slaves devices are connected to the serial interface.

That gateway links asynchronous modbus slaves to modbus TCP clients connected to the ethernet network.

Each TCP client (i.e. modbus master) can send requests to any modbus slave device of the serial interface.
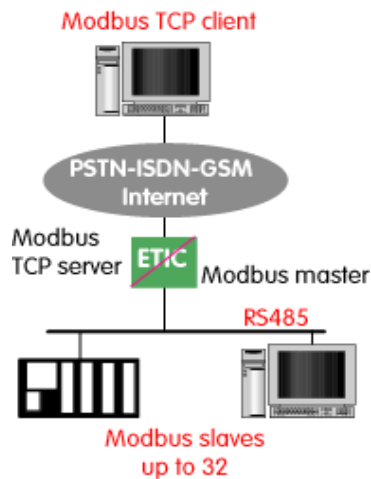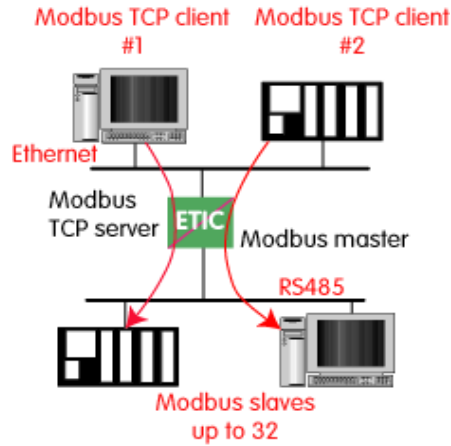
To configure the Modbus server gateway,

- select the modbus menu and then modbus server,

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

"Modbus protocol" parameter
Select the RTU or ASCII option

"Activate Proxi cache" parameter
Enable the proxi option if you wish to avoid to frequent requests on the serial interface.

"Cache refreshment period" parameter
the same request is received twice or more inside that delay, it will be sent only once to the slave on the serial interface.

"Timeout waiting for the answer" parameter
Set up the timeout the gateway has to wait for the answer of the modbus slave.

"Local retry" parameter
Set up the number of times the gateway will repeat a request to one of the modbus slaves on the serial interface before declaring a failure.

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

"Modbus slave address* parameter
  If only one modbus slave device is connected to the serial interface, set the modbus address of the device; any TCP modbus request received by the gateway will be sent on the serial interface using that modbus address.

  If several modbus slave devices are connected to the serial interface, select "specified by modbus TCP client";
  In that case, each request sent by the TCP/IP modbus client to one of the slaves connected to the serial interface must specify the modbus slave address value in the modbus address field.

"TCP inactivity Timeout" parameter
Set the time the gateway will wait before disconnecting the TCP link if no characters are received.
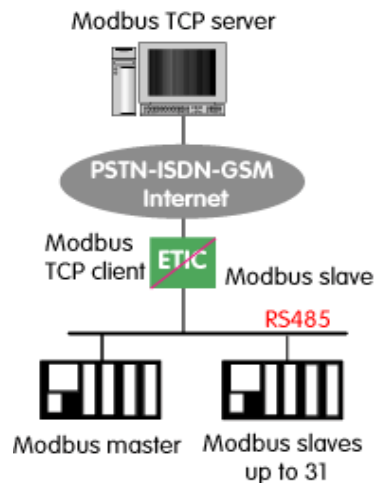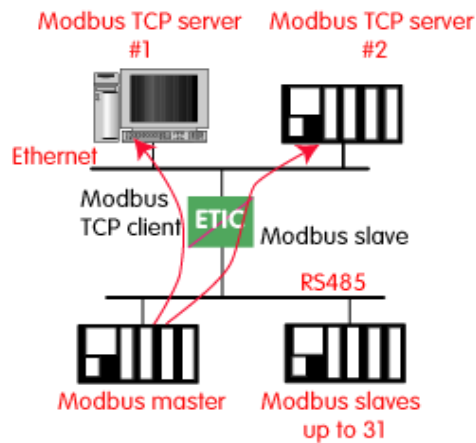
"TCP port number" parameter
Set the port number the gateway has to use.

5.6.1.4 "Modbus client" gateway

A Modbus master device is connected to the serial interface of the RAS.

That modbus master can send requests to slaves connected to the serial interface or to 256 modbus TCP servers maximum connected to the IP network (i.e. modbus slaves).

To configure the modbus client gateway,

- select the modbus menu and then "modbus client" menu;
- enable the "modbus client" gateway and set up the parameters as follows :

"ASCII / RTU protocol" parameter
Select the right option

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

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

"TCP port number" parameter
Set the TCP port number the gateway has to use.

"IP address table"
When the serial master sends a modbus request to a slave, it includes the modbus address of that slave.
If that slave is not a serial slave but a TCP modbus server on the ethernet network, the ETIC gateway needs to know what is its IP address.
That IP address table allows to assign an IP address to each modbus slave address.

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

5.6.2 "Transparent" menu

The RAS gateway provides solutions to connect serial devices to the IP network without interpreting the application protocol. That solutions are called transparent gateways.

4 transparent gateways are available : The raw client or server gateway, the multicast gateway or the telnet gateway.

5.6.2.1 "Raw client" gateway

That 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.
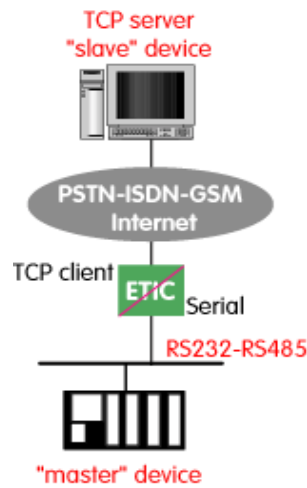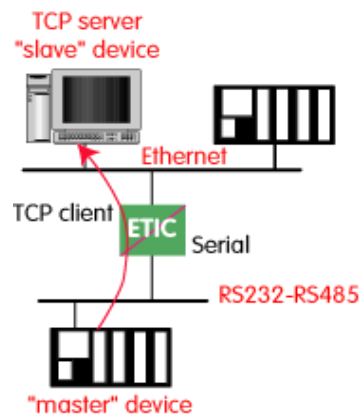
The serial device must be for example a master device in half duplex protocols.

To configure the "raw client" gateway,

- Select the "transparent" and then the "raw client" menus.

- Enable the raw client gateway; and set up the parameters as follows :

"RS232/485 input buffer size" parameter
Set up the maximum length of an asynchronous string the gateway will
store before transmitting it to the IP network.

"Timeout of RS232/485 end of frame" parameter
Set up the delay the gateway will wait before declaring complete a string
received from the asynchronous device.
Once declared complete, the gateway will transmit the string to the IP
network.

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

"TCP port number" parameter
Set the port number the gateway has to use.
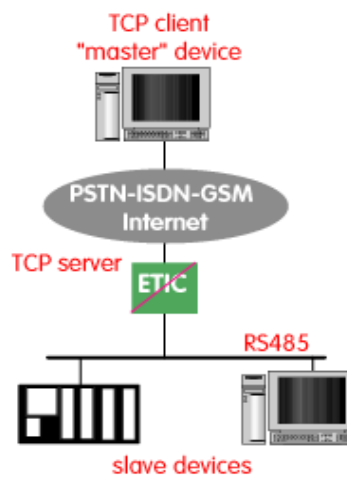
"Raw server IP address" parameter
The raw client gateway is able to communicate with a raw server gateway.
Assign an IP address to define the destination gateway.

5.6.2.2 "Raw server" gateway

That gateway can be used if a serial slave device has to answer requests coming from devices located on the IP network and acting like a master (also called TCP client).
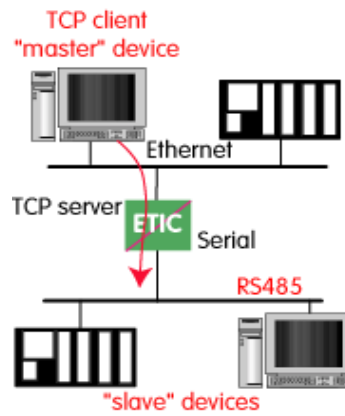
To configure the "raw server" gateway,

- Select the "transparent" and then the "raw server" menus.

- Enable the raw server gateway and set up the parameters as follows :

"RS232/485 input buffer size" parameter
Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

"Timeout of RS232/485 end of frame" parameter
Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.
Once declared complete, the gateway will transmit the string to the IP network.

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

"TCP port number" parameter
Set up the port number the gateway has to use.

5.6.2.3 "Multicast" menu

Internet Protocol multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients.

Thus, the multicast gateway must be used when

- a serial master device has to send requests to multiple slave devices; that devices can be IP or serial devices.
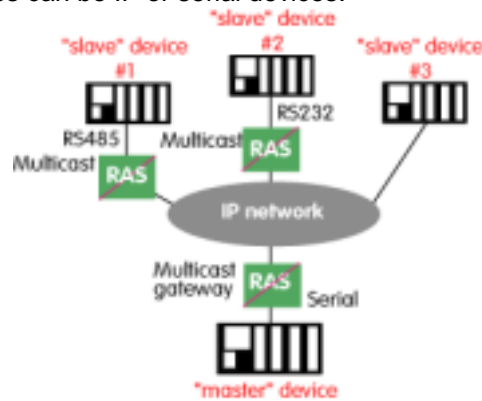
- Or when an IP master device (client) has to send requests to multiple slave devices; that devices can be IP or serial devices.
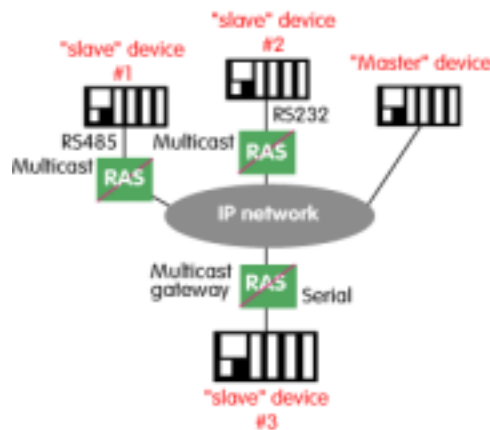
The *Internet Assigned Numbers Authority (IANA)* controls the assignment of IP multicast addresses.

The range of addresses from 224.0.1.0 through 238.255.255.255 are called "globally scoped addresses". They can be used to multicast data between organizations and across the Internet.
The range of addresses from 239.0.0.0 through 239.255.255.255 contains limited scope addresses or administratively scoped addresses. These are defined by RFC 2365 to be constrained to a local group or organization. Routers are typically configured with filters to prevent multicast traffic in this address range from flowing outside an autonomous system (AS) or any user-defined domain. Within an autonomous system or domain, the limited scope address range can be further subdivided so those local multicast boundaries can be defined. This also allows for address reuse among these smaller domains.

Note   This address range is only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.

To configure the multicast gateway,

- Select the "transparent" and then the "multicast" menus.

- Enable the multicast gateway and set up the parameters as follows :

"RS232/485 input buffer size" parameter
Set up the maximum length of an asynchronous string the gateway will store before transmitting it to the IP network.

"Timeout of RS232/485 end of frame" parameter
Set up the delay the gateway will wait before declaring complete a string received from the asynchronous device.
Once declared complete, the gateway will transmit the string to the IP network.

"TCP port" parameter
Set the port number the gateway has to use.

Multicast group IP address
Enter the multicast IP address assigned to the group with respect to the rules of the IANA authority.

5.6.3 « Unitelway » menu

The unitelway gateway is made to connect an RS232-RS485 unitelway master PLC to the RAS.

It allows to use the Schneider Electric program PL7 or Unity, or other Schneider programs, in order to maintain remotely a Schneider Electric PLC.
It can also be used to integrate an unitelway master PLC to an IP network.

- Select the Unitelway menu; select "enable the unitelway transceiver".

- Enter the XWAY address assigned to the asynchronous unitelway PLC on the IP network.

- Select « enable the IP-RS transceiver ».

- Enter the Xway address of the master PLC and, if they exist, the Xway addresses of the slave unitelway PLCs connected to the master PLC.

5.7 « Diagnostic» menu

4 diagnostic menus are proposed :

Logs :
Information about each connection to the administration server or to the LAN or RS232-RS485 are dated and stored.

Network status :
That screen gives detailed information about the status of each interface of the RAS (modem, ethernet, RS232-RS485).

Microswitches status :
That screen displays the status of the microswitches located on the top of the product.

Ping :
that screen enables to send a ping frame to any IP address.

Digital inputs & output (RAS-M156e, RAS-I1128e, RAS-G134e) :
That screen displays the status of the 3 digital inputs and allows to set ON or OFF the digital output.

5.8 « Alarm email» menu (RAS-M156e, RAS-I1128e, RAS-G134e).

« Enable the alarm email » option :
Select this option if you want an email to be sent to a user when the digital input 1 is set ON or OFF.

« Alarm launched on event » Parameter :
Choose if the email must be sent when the digital input 1 is closed or opened or both.

« Hold time » parameter :
Select the time the input has to stay in its alarm status to be taken into account.

« User to alert by e-mail” parameter :
Select in the list the user to whom the email must be sent.

"Text to send" :
Enter the email text.

1   Connect to the RAS through the PSTN or ISDN or GSM

1.1   Remote user PC modem

- **Case of a RAS with a built-in PSTN modem (RAS-M156 or RAS-M156e)**

The PC must be installed as follows :

PC + PSTN modem + subscriber PSTN line

PC + PSTN modem + analog line connected to a PBX

PC + "digital modem" * + ISDN line
* We call digital modem an ISDN adapter including a V34 or V90 modem.

PC + GSM modem
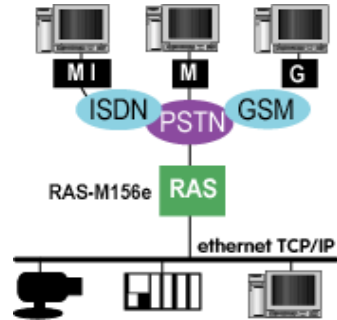
- **Case of a RAS with a built-in ISDN adapter**

The PC must be installed as follows :

PC + ISDN adapter + ISDN line
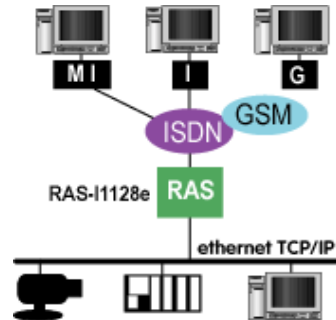
- **Case of a RAS with a built-in GSM or GSM-GPRS or GSM-GPRS-EDGE modem**

The PC must be installed as follows :

PC + PSTN modem + subscriber PSTN line

PC + GSM modem

PC + ISDN adapter + ISDN line
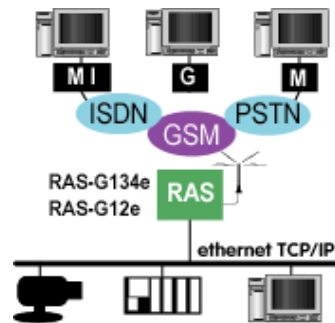
1.2   Setting the PC remote connection

A remote connection tool has to be created. It will be used each time you will have to connect the remote PC to the LAN through the RAS.

See appendix 2.

1.3 Connection without callback

- Double click the remote connection icon.

- Enter your user name and password.

- Enter the RAS telephone number and click "connect".

- When the "callback" popup is displayed, click "cancel"

The connection popup indicates your PC is now connected to the remote site; an icon appears is the PC toolbar; if you click it, you will get detailed information about the connection : In particular, RAS IP address.

You can get more detailed information about the connection in the diagnostic and then network status menu of the administration server of the RAS.

1.4   On demand callback

It is possible to ask the RAS to call you back at the telephone number you wish. That function is called "on-demand callback".

That function must have been previously authorized : See the "system" menu, and then "user list" and then callback option.

- Proceed as usually : Double click the remote connection icon; enter your user name, password and the RAS telephone number; click OK.

- Once the callback popup is displayed, enter the telephone number at which you wish to be called back and click OK.

- The RAS clears the call, and calls back.

After a few tens of seconds, once connected again, the connection icon in the tool bar indicates the PC is connected.

1.5   Safety callback

It is possible to ask the RAS to call you back at the telephone number you have stored in the user form. That function is called "safety callback".

That function must have been previously authorized : See the safety menu, and then "user list" and then callback option.

- Proceed as usually : Double click the remote connection icon; enter your user name, password and the RAS telephone number; click OK.

- Once connected, the RAS checks the user name and password, clears the call and calls back; it dials the telephone number stored in the user form.

After a few tens of seconds, once connected again, The connection icon in the tool bar indicates the PC is connected.

1.6   Connect your PC to the machines of the LAN

Once connected, the remote PC behaves like a machine of the network.

1.7   Web portal
The web portal function can help the user to identify the IP machines to which it is possible to connect.

The web portal can be enabled or disabled (go to the administration server « system configuration » and then "target list"; select the « Display the web portal » option).

The web portal screen displays the list of the machines which have been declared in the target list menu.

3 links are associated to each machine :

The html link : To go directly to the web server of the associated machine.

The « explore » link : To explore the HD of the associated machine, if it is a Windows machine.

The « ftp » link : To explore the files of the associated machine.

1.8   Clear the connection
•   Click the remote connection icon.

The remote connection window is displayed.

•   Click "disconnect".

2   Safe internet connection

A remote user can connect to the machines of the LAN through the Internet.

3 steps are necessary :

Step 1 : Connect the RAS to the internet

This operation can be carried out by several means (see drawing).

Step 2 : Get the IP address of the RAS, if it is a dynamic IP address.
You can get the IP address by using the DynDns function or also inside an email.

Step 3 : Set a VPN between the PC and the RAS; then connect the remote PC to the machines.

Note : If a VPN cannot be set, the DNAT function allows to connect to the machines.

RAS-M156e
RAS-I1128e
RAS-G134e
RAS-G12e
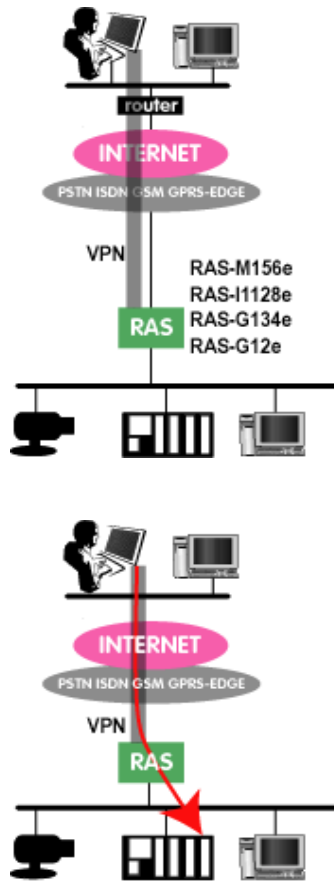
2.1   Step 1 : Connect the RAS to the Internet

4 possibilities are offered to order the RAS to connect to the Internet :

- **Internet callback type 1**

- **Internet callback type 2**

- **Internet connection when the digital input 1 is enabled**

- **Internet connection as soon as the RAS is ON**

- **Internet connection when the "Connection" button is pressed.**

That options are selected in the "Internet" menu and then "remote control"; they are not exclusive.

2.1.1   Internet callback type 1

No local action is necessary; the order can be given remotely by the user.

The "callback allowed" option must have been assigned to the user.
See the « System » menu and then «User».

- Connect to the RAS directly through the PSTN or ISDN or GSM.

- When the callback popup is displayed, enter "0" (figure zero) and OK;

The RAS clears the call and connects to the Internet.

2.1.2 Internet callback type 2

The "connect to the internet after a phone call from …" option must have been selected. See the « Internet » menu and then « Remote control ».

A phone Nr has to be entered in the associated field.

- Call the RAS from the telephone line number stored as indicated just above.

- The RAS identifies the caller; it checks if that number is the order to connect to the Internet.

If it is, the RAS connects to the Internet.

2.1.3 Internet connection as soon as the RAS is ON

The "connect to the Internet as soon as the RAS is ON" option must have been selected previously. see the "internet» menu and then « Remote control».

- Switch the RAS ON (front panel ON/OFF switch).

The RAS connects to the Internet.

The RAS will disconnect from the Internet as soon as the VPN will break.

2.1.4 Internet connection when the digital input 1 is enabled

The "connect to the Internet when the digital input 1 is active" option must have been selected previously. See the « Internet » menu and then « Remote control ».

- Close the digital input 1.

The RAS connects to the Internet.

The RAS will disconnect from the Internet as soon as the VPN will break or if the digital input is opened.

2.2   Step 2 : Get the RAS IP address (if dynamic)

If the RAS internet account is a "dynamic IP address" account, the provider provides a different IP address to the RAS at each connection, that address must be transmitted to the remote user through the Internet. The user will then use that address to connect to the machines.

4 possibilities are offered to transmit to the remote user the IP address assigned dynamically to the RAS.

- The IP address can be displayed in the administration server : "Diagnostic" and then "Network status".

- The IP address is automatically transmitted to a DynDns server (dyndns.org).

- The IP address can be received on the remote user inside an email.

- The IP address can be displayed as an html page of a FTP server

2.2.1 Send the IP address to a DynDns server

The « transmit the IP address to a DNS server" option must have been selected and a subscription at DynDns.org taken. See the " internet" menu and then the "Dynamic IP @".

Once connected to the Internet, the RAS automatically sends its own IP address to the DYNDNS server.
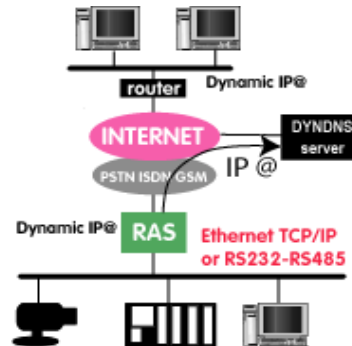
2.2.2 receive the RAS IP address inside an email

The « send the IP address inside an email" option must have been selected See the " internet" menu and then the "Dynamic IP @".

The RAS sends the IP address inside an email as shown below :

Hello admin, i am connected to internet.

IP: 62.147.75.153
MAC: 00:0A:B4:00:01:5F
SITE : FORD BRAZIL
DATE: Mon Nov 17 09:06:14 2005

2.2.3 Get the IP @ inside an Html page of a FTP server

- Create previously an FTP server :

Example :
FTP address   ftppero.free.fr
User name   etic1

Password   dwbbebfz
Path   test

- Launch your Internet browser

- Enter the FTP server address

Example : http://etic1.free.fr/test.htm.

The FTP server screen is displayed.

- Click "Launch VPN"

The VPN is automatically established. A popup window indicates "connected".

2.3   Step 3 : Connect to any remote machine

2.3.1   Connecting to the machines using a VPN

Once a VPN is set between the remote user PC and the RAS, the remote user PC will be as if it was directly connected to the remote LAN. Moreover the communication over internet is secure.

- Create a VPN connection (PPTP or IPSEC or TSL) in accordance with the option you selected in the RAS ("Internet" and then "VPN").

- Click the VPN connection icon.

- Enter the IP address assigned to the RAS over the Internet or the RAS host name (etic-ras.dydns.org, for instance) if you use dyndns, in the field « Destination IP address» and click OK.

- Wait until the VPN is established.

2.3.2   Connecting to the machines using Dnat

If a VPN cannot be set, for instance if a router does not accept PPTP or IPSEC or TSL protocols, it remains possible to connect to the machines using the Dnat Function (see the "Internet" menu and then "Routing").
That function must be used cautiously because the communication over internet is not secure. The machines are only protected by the firewall

running in the RAS.

We explain hereafter with an example how to use DNAT.

Suppose the situation described by the drawing aside :

The remote user wishes to communicate with the PLC1 port 102 and PLC2 port 502 and PC port 80 over a remote private LAN.

The RAS IP @ over internet is 62.10.10.7.
That IP address may be fixed or, if it is dynamic, the remote user got it by one of the means explained above.
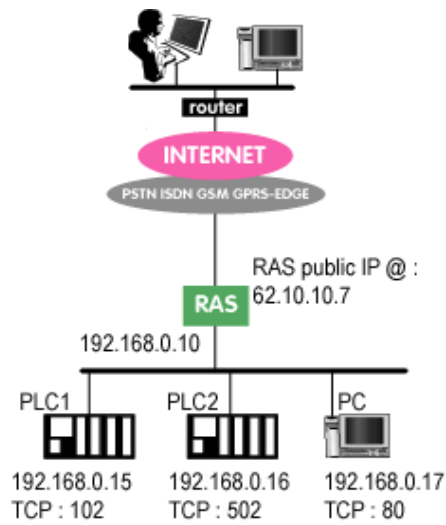
Principle of operations :
As the PLC1, PLC2 and PC IP addresses are not public, and as a VPN has not been set, the user will have to use a translating mean called DNAT.

Translation rules have to be stored inside the RAS in such a way that when the remote user sends an IP frame to the RAS public IP address with TCP = 102, the RAS will automatically route to the PLC1 port 102. the remote user will be then connected to the PLC1.
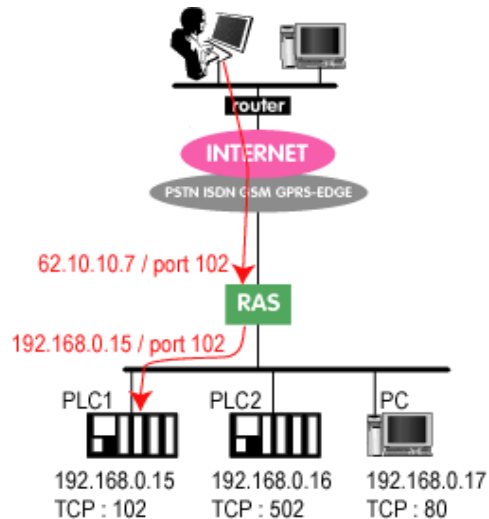
RAS configuration :

In our example, the remote user will have to go previously to the RAS web server and select the "Internet" menu and then "routing".

To be able to connect to the PLC1 and PLC2 and the PC, he will enter the DNAT rules hereafter :

If the RAS receives frames from internet to…		… it will send that frames over the LAN to	
IP destination	TCP	IP destination	TCP
62.10.10.7	102	192.168.0.15	102
62.10.10.7	502	192.168.0.16	102
62.10.10.7	8081	192.168.0.17	80

**Modifying an Ethernet connection so as to connect a PC directly to
the Ethernet interface of the RAS.
Windows 2000 case**

Not available yet

Set a remote connection
Windows 2000 case

Not available yet

Create a VPN connection
Windows 2000 case

Not available yet

Distribué par :

HVS.
PRECONISATEUR DE SOLUTIONS DEPUIS 1986

Contact :
hvssystem@hvssystem.com

Tél : 0326824929
Fax : 0326851908

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

etic
TELECOMMUNICATIONS

13, Chemin du Vieux Chêne

38240 Meylan France

Tel : 33 4 76 04 20 00

Fax : 33 4 76 04 20 01

E-mail : infos@etictelecom.com

Web : www.etictelecom.com