

# Operation Manual

# Remote-i Net





## Summary

Introduction.....	1
Installation.....	2
Operation.....	3
Normal operation steps.....	4
Basic Programming.....	5
Local Addressing of Remote-i Net.....	5
Searching for a DHCP server on the local network.....	5
Reconfiguring the Remote-i Net for use without a DHCP server.....	6
Remote-i Net Configuration Program.....	6
List of Remote-i Net devices found.....	8
Identification of the selected device.....	8
Remote-i Server addressing.....	10
Saving of information.....	11
Frequently Asked Questions.....	12
Technical Specifications.....	15
Technical Assistance.....	16



## Introduction

**Remote-i** is the generic denomination of a family of equipment manufactured by Contronics which allows communication (data downloading) between *Guardus* and a computer.

Contronics offers 4 different Remote-i models:

- Remote-i **Serial**
- Remote-i **Modem**
- Remote-i **ISP**
- Remote-i **Net**

The basic function of the family of *Remote-i* equipment is the same: to provide a means of communication between *Guardus* and a remote computer for the downloading of data. The difference between the models lies in the mechanism used to carry out this connection:

<i>Model</i>	<i>Method of Connection</i>
Remote-i <b>Serial</b>	Uses an external modem and a telephone line dial-up in order to connect directly with the remote computer.
Remote-i <b>Modem</b>	Evolution of the Serial model, bringing a built-in modem. The connection is carried out in the same way, using a telephone line dial-up.
Remote-i <b>ISP</b>	Evolution of the Modem model, designed specifically for use of the Internet (via a provider) through a telephone line dial-up. The remote computer also needs to be connected to the Internet in order to receive the downloads.
Remote-i <b>Net</b>	Variation of the ISP model, to deal with situations where the installation location already has a permanent connection to the Internet. The principal advantage is that it doesn't need to use a telephone line for connection to the remote computer.

In this manual only the ***Remote-i Net*** model will be dealt with.

## Installation

The installation of **Remote-i Net** is very simple, and it comes configured by the manufacturer to operate on the majority of local networks without any additional configuration being required.

Prior to starting the installation, verify that the location where the **Remote-i Net** will be installed fulfills the requirements necessary for physical connection:

- electrical AC socket supplying 110 or 220V
- local network access point

The power source provided with the **Remote-i Net** leaves the factory set to 220V. Verify that the voltage available at the socket is correct. If not, move the selection switch to the correct voltage (220 or 110).

The physical **Remote-i Net** connections will be made at the back of the equipment, as shown in the following figure:



Figure 1 - Back of Remote-i Net.

## Operation

The **Remote-i Net** operation is absolutely silent, and the signaling is carried out by 3 small colored lights (LEDs) on the front panel of the equipment.



Figure 2 - Front panel.

The visual signaling has the following set-up:

- **COMMUNICATION**, which indicates success or failure of the download process
- **LINE**, which shows the exchange of information between the Guardus and the remote computer
- **POWER**, which indicates that the equipment is switched on

During operation there may be a combined signaling, that is, depending on the situation the LEDs identified as **COMMUNICATION** and **LINE** can flash together, indicating a situation different to the basic information above. These situations will be dealt with in detail as follows.

## ***Normal operation steps***

The data download operation considered to be normal involves the following sequence of events:

1. after installation of the network cables and connection to the power source, the LED identified as POWER should light up in green, whenever the ***Remote-i Net*** is switched on;
2. immediately after the ***Remote-i Net*** is switched on, the three LEDs will be lit, indicating that the equipment is attempting to connect to the local network. After 3 seconds the LEDs identified as COMMUNICATION and LINE should turn off, and only the POWER will be lit. This indicates that the ***Remote-i Net*** is ready to operate on the local network;
3. the user places the *Guardus* on the metal receptacle mounted on the front of the ***Remote-i Net*** and this carries out a rapid reading of its content. This reading is signaled by a very brief flashing of LINE;
4. assuming that the data necessary for the download is correctly stored in the *Guardus*, the ***Remote-i Net*** will respond by lighting up COMMUNICATION in red. This indicator will remain unaltered during the entire download process, and the user shouldn't remove the *Guardus* from the metal receptacle as this will interrupt the operation;
5. when the remote computer is connected to the ***Remote-i Net***, the *Guardus* will immediately emit a sound and light signal, indicating that the two parts have been synchronized and download of data can commence;
6. the download process will proceed for a few seconds and may be accompanied by rapid flashing of LINE;
7. at the end of the download process, the *Guardus* will again emit a sound and light signal indicating that everything went well and the ***Remote-i Net*** will signal this with a color change of COMMUNICATION from red to green;
8. the user removes the *Guardus* from the metal receptacle and waits for the LED identified as COMMUNICATION to turn off, indicating the end of the download cycle.

The procedure described above assumes that everything occurred without problems. However, some difficulties may arise during this process which will be immediately signaled by ***Remote-i Net*** through a combined flashing of the COMMUNICATION and LINE LEDs.

In order to understand what ***Remote-i Net*** is trying to indicate with the light signals, read the section 'Frequently Asked Questions', on page 12.

## Basic Programming

The **Remote-i Net** comes configured by the factory ready to operate on most local networks without the need for reprogramming. However, there are some situations which require different programming to allow its connection to the user's local network.

### Local Addressing of Remote-i Net

The factory setting for **Remote-i Net** assumes the following conditions for the local network:

- TCP/IP network protocol
- twisted pair network cable with RJ-45 connector
- access point which accepts a standard 10base-T (10 Mbits/s in twisted pair)
- DHCP server

The DHCP (*Dynamic Host Control Protocol*) server is a component of the local network which is responsible for distributing IP addresses to the other machines. Each machine connected to the local network when turned on, searches for the DHCP server and requests an IP address to initiate the work. The DHCP server then verifies its list of available addresses, selects one of them and informs of the address which each machine must utilize in order to be identified by the other machines on the network.

This centralized control facilitates and disciplines the distribution of addresses when the quantity of machines connected to the same local network is very high (more than 10 machines).

Often, for small installations, a DHCP server is not required, and if that is the case for your installation, the **Remote-i Net** will need to be reconfigured.

### Searching for a DHCP server on the local network

The test to find out whether or not your local network has a DHCP server is very simple: it is just a matter of turning on the **Remote-i Net** with the factory configuration. The 3 LEDs of the **Remote-i Net** will light up while it searches for the DHCP server. If there is a DHCP server on the network, after 3 seconds two LEDs will go off (COMMUNICATION and LINE), and only the POWER LED will remain on.

Alternatively, should the 3 LEDs remain on after 5 seconds, this means that the **Remote-i Net** did not managed to find the DHCP server. The possible reasons are:

- faulty cable contact
- inappropriate network cable (it must be the same type used for computers)
- hub turned off
- DHCP server disconnected

After verifying the first three items and finding that the same signaling remains, one can assume with a high degree of certainty that your local network does not have a DHCP server available. In this case your **Remote-i Net** will need to be reconfigured.

## Reconfiguring the Remote-i Net for use without a DHCP server

The **Remote-i Net** leaves the factory programmed to find a DHCP server. If your network does not have a DHCP server, it will be necessary to reconfigure the **Remote-i Net**

Before reconfiguring the **Remote-i Net**, you should obtain the following information from the person responsible for your local network:

- free fixed IP address for the use of the **Remote-i Net**
- sub-network mask
- IP address of the local network router

Having obtained this information, use a “RiNetConfig” program to reconfigure your **Remote-i Net**. It is available on the same menu as the PROGuard program.

### Remote-i Net Configuration Program

The **Remote-i Net** configuration program is installed through the CommCenter installation procedure. The application is available in the following folder: ..\Program Files\Contronics\Common Files\Remote-i Net.

Once installed, the configuration program may be activated from the *Programs* menu, accessed by the Windows® *Start* button



Figure 3 - Start Menu / Programs.

As it starts, the program will display its main screen:

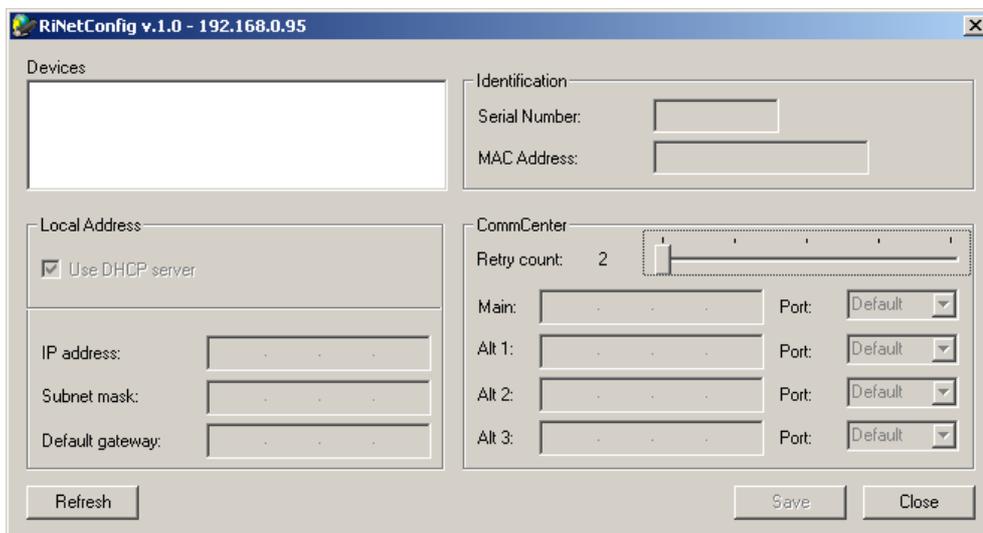


Figure 4 - Initial screen of the Remote-i Net configuration program.

Connect your **Remote-i Net** to the local network, turn on the power and the switch at the back of the equipment. The LED identified as POWER should remain on.

Returning to the configuration program, press the "Update" button in order to scan the local network in search of **Remote-i Net** devices. If a device of this type is found, it will appear on the list, as shown in the figure below.

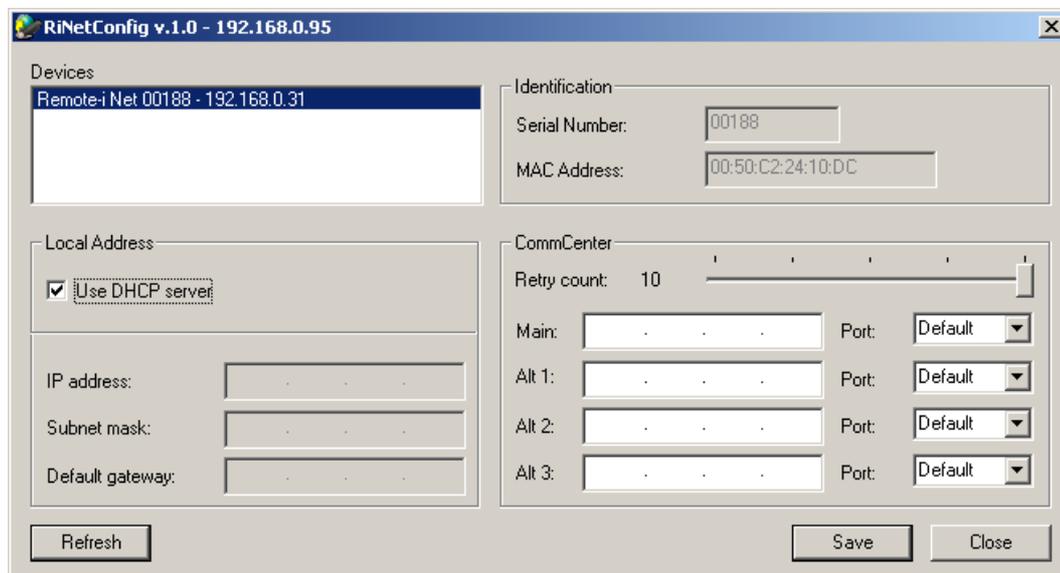


Figure 5 - Result of the scanning for a Remote-i Net.

If more than one **Remote-i Net** is connected at the same time, they will be listed on the upper left part, but only one of them may be programmed at a time.

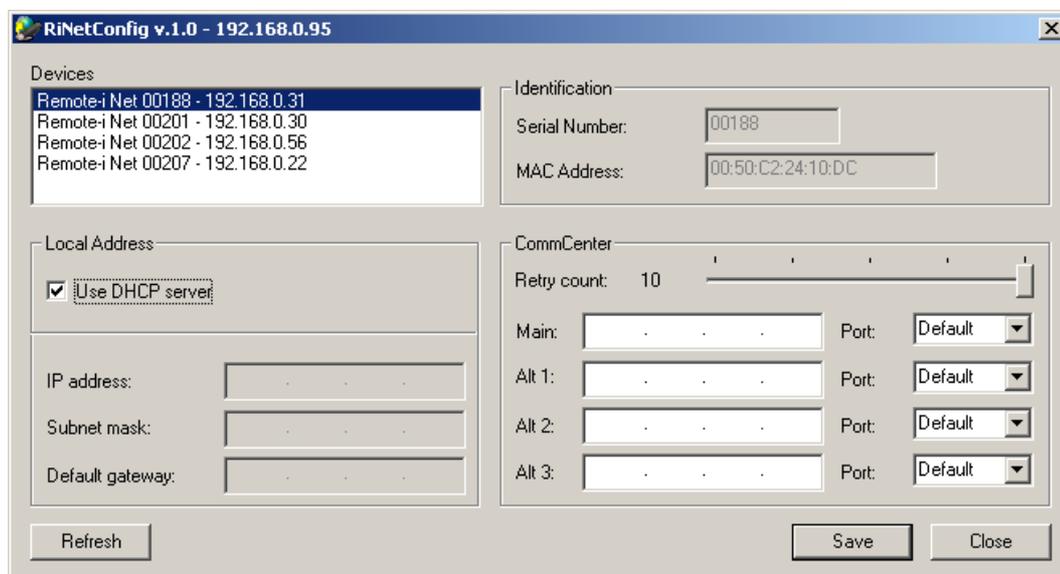
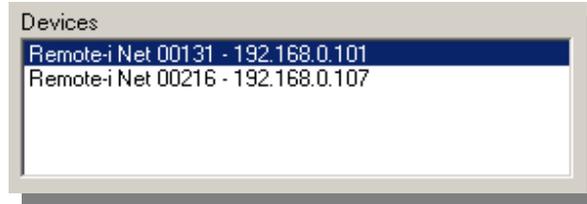


Figure 6 - Scanning with more than one Remote-i Net on the local network.

## List of Remote-i Net devices found

The list of devices found during the scanning of the local network appears on the upper left part of the main screen.



On each line of the list a **Remote-i Net** series number and the IP address which it is using at the time are shown.

## Identification of the selected device

When one of the devices listed is selected, the configuration data contained in its memory will be shown, grouped according to type of information. One of these groups is the unique identification of each device, which is shown on the upper right part of the main screen.



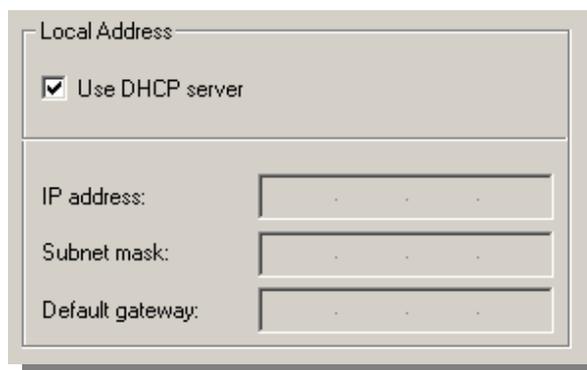
## Local addressing of the selected device

The selected device has a local network identification, composed of:

- IP address
- sub-network mask
- standard router address

These data may be obtained automatically by **Remote-i Net** when it is turned on (factory setting) or they can be set. The automatic obtention is carried out with the assistance of a DHCP server, which is normally available on medium and large local networks.

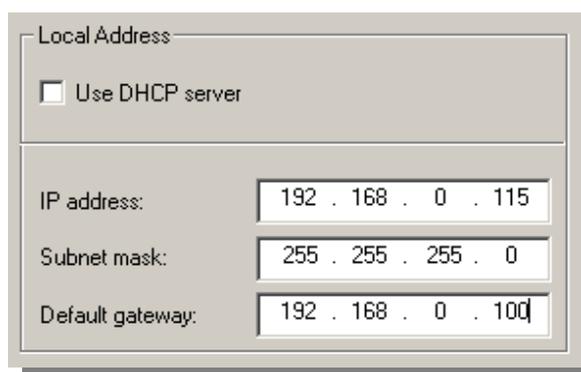
The automatic identification is always recommended when the local network, where the **Remote-i Net** is connected, has a DHCP server. For this, configure the **Remote-i Net** as shown in the following figure.



The screenshot shows a window titled "Local Address". At the top, there is a checkbox labeled "Use DHCP server" which is checked. Below this, there are three input fields: "IP address:", "Subnet mask:", and "Default gateway:". Each field is currently empty, showing only dots to indicate the expected format.

If your local network does not have a local DHCP server, find out from the person responsible for the local network, the data needed to fill in the fields “*IP address*”, “*Network mask*” and “*Standard router*”.

Example of the local fixed addressing (the numbers may vary):



The screenshot shows the same "Local Address" window. The "Use DHCP server" checkbox is now unchecked. The input fields are filled with the following values: "IP address:" is "192 . 168 . 0 . 115", "Subnet mask:" is "255 . 255 . 255 . 0", and "Default gateway:" is "192 . 168 . 0 . 100".

### Important Note

If the local network where the **Remote-i Net** will be installed doesn't have an active DHCP server, consult the person responsible before filling in the local addressing gaps.

If the numbers are not correct, the **Remote-i Net** will not be able to operate. If there is a conflict of IP addresses (same address for two machines on the local network) both the **Remote-i Net** and the other machine which has the same address will be affected.

## CommCenter addressing

The process of downloading the *Guardus* data involves not only the **Remote-i Net**, but also a program known as **CommCenter** which remains installed on a remote machine and is always ready to receive and process these data.

The **Remote-i Net** initially searches within the *Guardus* memory to check whether the computer address, where the *CommCenter* program is, is stored. If it is stored, the connection begins.

When the reading of the *Guardus* internal memory does not bring the necessary address information for the connection with the *CommCenter*, an option would be to use a program address in the memory of the **Remote-i Net** itself.

The **Remote-i Net** leaves the factory without any *CommCenter* address programmed, as shown in the following figure.

The screenshot shows the 'CommCenter' configuration window. At the top, there is a 'Retry count' slider set to 4. Below this, there are four rows for address configuration: 'Main', 'Alt 1', 'Alt 2', and 'Alt 3'. Each row consists of an IP address field (displaying four dots) and a 'Port' dropdown menu (displaying 'Default').

The **Remote-i Net** stores up to 4 different *CommCenter* addresses. The attempts to connect will always occur in the specified order starting with the primary address. The number of ports used by the *CommCenter* is normally 5120, referred to in the configuration program by the term "Standard".

To program one or more *CommCenter* address, enter with the information shown in the figure below:

The screenshot shows the 'CommCenter' configuration window with programmed addresses. The 'Retry count' slider is still at 4. The 'Main' address is '192 . 168 . 0 . 90' with 'Port: Default'. 'Alt 1' is '200 . 215 . 17 . 89' with 'Port: 19000'. 'Alt 2' and 'Alt 3' are empty IP fields with 'Port: Default'.

The number may vary for your particular installation. The above figure serves only to illustrate how the addresses may be formed.

The number of the ports may also be altered, although this is not recommended. If it is really necessary to change it, consult the person responsible for the *CommCenter* in your organization in order to find out the correct number to be used.

## **Saving of information**

All the information shown or edited on the main screen of the *Remote-i Net* configuration program remains stored only inside each specific device. No information is recorded on the computer which is being used for the configuration process.

The altered information will only be stored in the selected device when the button "*Save*" is pressed. Before confirming this operation, carry out a complete check to see whether the data are correct, mainly regarding the local addressing information.

## Frequently Asked Questions

The operation of **Remote-i Net** is very simple, but some difficulties may arise during the download process which will be signaled by the equipment in the form of a combination of flashes of the COMMUNICATION and LINE LEDs.

The following questions deal with such situations which do not follow the normal operation as described on page 4.

### 1. POWER LED does not light up. What should be done?

This situation suggests that the equipment has not been properly supplied with power.

Verify the following

- a. whether the electricity plug is firmly connected to the electricity socket
- b. whether the voltage selection switch for the electricity input is correct for the supply in your region (110V or 220V)
- c. a. whether the electricity source is firmly connected to the **Remote-i Net**
- d. whether the on-off switch is on (lever in upward position)

If these items are correct, and the electricity socket is receiving energy, and even so, the **Remote-i Net** POWER LED does not light up, call Technical Assistance (see contact information on page 19) and report the problem.

### 2. The Remote-i Net came on, but the 3 LEDs remained lit after the initial 3 seconds. What should be done?

This situation shows that your local network does not have an active DHCP at this time. The **Remote-i Net** leaves the factory configured to be used on a local network which has an active DHCP server, and when it does not find the server, it waits indefinitely for the server to return to operation. During this time the **Remote-i Net** remains inactive.

Proceed in the following way:

- a. verify with the person responsible for the local network whether there is at least one DHCP server available. Of there is, request verification that it is still active and whether the location where the **Remote-i Net** is connected, is attended by this DHCP server;
- b. if it is confirmed that the local network has no DHCP server available, ask the person responsible for a fixed IP address available for use with the **Remote-i Net**. The procedure to configure the **Remote-i Net** in order to use a fixed IP address, is described in the item "*Reconfiguring the Remote-i Net for use without a DHCP server*" on page 6.

**3. The Guardus starts emitting a series of “bips” without the COMMUNICATION LED lighting up. What has happened?**

This is not a *Remote-i Net* but a *Guardus* signal. What it is trying to tell you is that the position in which the *Guardus* was placed on the *Remote-i Net* metal receptacle caused a faulty contact. This situation is temporary and soon after the end of the 9 “bips” sequence the *Remote-i Net* will try again to connect with the *Guardus*. Just wait as everything will return to normal after a few seconds.

**4. The Guardus was placed on the Remote-i Net metal receptacle but the COMMUNICATION LED began to flash orange and nothing happened. What is the Remote-i Net trying to signal with this?**

The *Remote-i Net*, upon detecting that a *Guardus G* or *Guardus T* was placed on the metal receptacle, tries to read some internal information which gives the remote computer address which should receive the data download. If these data are not recorded on the *Guardus*, the *Remote-i Net* will try to find out whether they are programmed inside itself.

If the *Remote-i Net* still does not find sufficient information to attempt communication with the remote computer, the COMMUNICATION LED will signal this by flashing orange immediately after contact with *Guardus*. This signaling will remain while the *Guardus* is in contact with the metal receptacle.

What should be done:

- a. obtain the IP address and the number of the remote computer port which was programmed to receive the *Guardus* downloads of your company. If you do not know how to obtain this information, establish contact with the person responsible for your local network and give the name of the remote computer you wish to use;
- b. use this information (IP address and port number) to program the *Remote-i Net* as described in the item “CommCenter addressing” on page 10, or
- c. reprogram the *Guardus* so that it can start storing the IP address and the port number

To program *Guardus G* / *Guardus T*, use the application corresponding to each device. The *Guardus G*, for example, is reprogrammed through PROGuard.

**5. The COMMUNICATION LED remained red for some time without flashing and now it is flashing orange. What should be done?**

This is an indication that something has gone wrong in the process of connection between the *Remote-i Net* and the remote computer.

The most probably reasons for this signaling are:

- a. faulty contact of the *Remote-i Net* network cable
- b. the remote computer was switched off
- c. the remote computer is no longer accessible on the local network
- d. the *CommCenter* program, which waits for the remote computer downloads, was disconnected
- e. the connection between the *Remote-i Net* and the remote computer is experiencing traffic problems, possibly on the Internet

Carry out a verification of each one of these items. If it is a temporary problem, just remove the *Guardus* from the *Remote-i Net* metal receptacle until the COMMUNICATION LED goes off and try again. A new attempt will be started as soon as the *Guardus* is replaced on the metal receptacle.

If the problem remains, enter into contact with the person responsible for your local network, so that the source of the problem can be verified.

**6. The COMMUNICATION LED is red without flashing. Is it OK to remove the Guardus from the Remote-i Net metal receptacle?**

No. While the COMMUNICATION LED is lit in red the *Remote-i Net* will be processing the *Guardus* data download and should not be interrupted. Wait until this LED changes to green (without flashing) or to orange (flashing) before removing the *Guardus*.

**7. The COMMUNICATION LED is green without flashing. Is it OK to remove the Guardus from the Remote-i Net metal receptacle?**

Yes. When the COMMUNICATION LED remains green without flashing it means that the data which were stored on the *Guardus* were downloaded onto the remote computer successfully. This LED will only go off when the *Guardus* is removed from the metal receptacle.

**8. I will use Remote-i Net only on an internal network, where my PC which runs CommCenter is in the room next door. Which type of configuration do I need?**

You need to configure the (Guardus G or Guardus T) using the corresponding application for it to store the network address of the PC where the CommCenter program is running. If you do not know the PC address, ask your network administrator.

The steps to program the wand are as follows:

- a. Carry out a new download or open a previous download;

- b. In the 'Programing' guide, click on 'Reprogramming';
- c. In the 'Remote' guide fill in the field 'destination IP ' with the IP of the computer where the CommCenter will be installed;
- d. Click on 'OK' and place the wand in contact with the download interface for the programming to be saved. With this operation, every time that the wand is placed on the Remote-i Net the address of the PC which is running the CommCenter program will be read and automatically accessed through your local network.

**9. If my company uses several wands, do I need to program them one by one with the address of the PC which runs the CommCenter? Isn't there an easier way to do this?**

Yes, there is. You can use an alternative method which consists of programming the PC address in the actual Remote-i Net itself. So, when you place the wand on the Remote-i Net, it will try to read the PC address which is stored in the wand. If it finds it, it will use this address read from the wand. If not, it will use the address which is programmed inside itself. The steps to program the network address of the PC which is running the CommCenter in the Remote-i Net itself are the following:

- a. Open the program RiNet\_Config and click on 'Update';
- b. Deselect the option 'Use DHCP server' if it is selected;
- c. In "Devices" click on a Remote-i and fill in the fields 'IP Address', 'Network mask' and 'Standard Router' (this information can be obtained from the network administrator);
- d. Click on 'Save' to record these configurations.

**10. Our company provides security services for many clients spread around the city and even in other cities, but we want the data for all these clients to be concentrated at our company head office.**

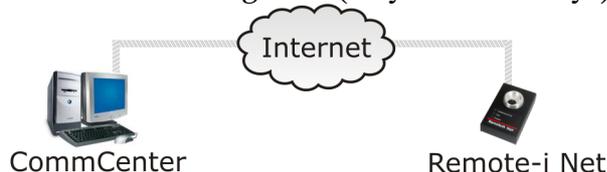
**How can the Remote-i Net be configured to do this?**

Remote-i Net does not distinguish between geographical locations in relation to the PC which is running the CommCenter, that is, as far as the Remote-i Net is concerned, it doesn't matter whether the PC is on an internal or external network, the procedure is exactly the same (see queries above).

**11. Do I need to carry out any special configuration at the head office of my company where the PC which runs the CommCenter is located?**

This depends on how the network where the PC is connected is organized. There are two distinct possibilities which reflect almost all of the field installations:

- a. Connection dedicated to the internet for a single PC (very rare nowadays)



- b. Company internal network connected to the Internet through a router or firewall (most installations).



In the first case, a special configuration will not be necessary. The Remote-i Net needs only to know the network (IP) address of your PC. In the second case, it will be necessary to open what is called the 'executive route' in your router/firewall so that all external connections which arrive at your Internet address via the 5120 port are directed only to the internal network address of the PC which is running the CommCenter program.

**12.If I open this 'executive route' of my router/firewall will I be compromising the security of my internal network.**

No, not all. The 'executive route' will work as if it were a direct connection between the Internet and the CommCenter program. Every connection which arrives at the 5120 port (standard port of the CommCenter program) will be diverted only to the PC which is running CommCenter, and to no other computer.

Only the PC which you designate to receive the connection via the 5120 port will receive messages, the rest of the network will not even be aware that there is an incoming connection.

**13.But if the CommCenter is offline, is my internal network at risk?**

No. The CommCenter uses only the 5120 port and should it be offline, for any reason, the connections which arrive at the 5120 port will simply be ignored, since there is no program 'receiving' that port. Since only the PC where the CommCenter is installed has been configured to receive connections which enter through the 5120 port, no computer on your internal network will be affected.

**14.So, that means that I can have 50 clients spread around the country sending wand data to my company without any of these clients needing to configure the router or firewall.**

Exactly. Only the network where the PC which runs the CommCenter is installed needs to have an 'executive route' in its router/firewall Internet access. Your clients do not need to be concerned about any of this, they just need to program the Internet address of your company head office so that the Remote-i Nets spread nationwide can operate.

**15.Can the Remote-i Net pose any threat to the security of the my client's internal network?**

No, not at all. Remote-i Net can only communicate with CommCenter. If it is programmed with the address of the PC which is running the CommCenter and the CommCenter is receiving at the 5120 port, the two can communicate, if not, Remote-i Net will indicate an error and will remain silent, without bothering anyone on your client's internal internet.

**16.I have just received my Remote-i Net. Is there any fixed internet address which I can use in the configuration of my Remote-i Net to check if it is really working?**

Yes, there is. Contronics has the address 200.247.154.87 which can be used to test your Remote-i Net. When a wand is placed on the Remote-i Net programmed with this address the wand download will be carried out at Contronics Head Office in Florianópolis, SC, Brazil. The data transferred to this address will be discarded, since Contronics has no interest in knowing the content of the data downloaded from its client's wands, but this is a simple and practical way to check whether your Remote-i Net is working properly.

**17.Can I use this address to test the Remote-i Net whenever it is installed at my client's facility's?**

Of course. Feel free to test it whenever you wish. Contronics has this address for that purpose, we only request that it be used moderately, since there are thousands of Remote-i Nets spread worldwide, which also use this address for tests.

**18.Is there an easy way to find out the internet address of my company?**

Yes, open the following address on your naverageator (Internet Explorer, Firefox or other):

*<http://www.myipaddress.com>* . The window which appears gives the address of your network when viewed on the internet.

## Technical Specifications

<i>Characteristics</i>	<i>Specifications</i>
Cabinet	aluminum body with black epoxy paint coating
Dimensions (H x W x L)	30 mm x 68 mm x 105 mm
Weight	315 g
Operation temperature	-5° à +70° celsius
Humidity tolerance	up to 95% without condensation
Power supply	external source of 9 V / 500 mA
Communication	Ethernet 10base-T, half-duplex
Signaling	3 LED indicators
Communication cable	twisted pair CAT-5 or CAT-3, RJ-45 connector

## Technical Assistance

Before entering into contact with Technical Assistance check the following items:

- whether your **Remote-i Net** has power (POWER LED on)
- whether the **Remote-i Net** local network cable is properly connected
- whether the COMMUNICATION and LINE LEDs are off (without *Guardus G* or *Guardus T*)
- whether your local network is operating
- whether the remote computer (where the *CommCenter* is) is active
- whether the *CommCenter* program is active
- whether the **Remote-i Net** local network and the remote computer local network are interconnected
- whether the situation observed is listed in the section "Frequently Asked Questions" (page 12)

If, even after verifying all of the items above, your **Remote-i Net** does not operate, establish contact with **Contronics Technical Assistance** by telephone, e-mail or fax and report your problem. The contact information is:

### Contronics Technical Assistance

Rua Lauro Linhares, 589 – 1º andar  
88.036-002 Florianópolis – SC

Telephone: +55 (48) 2106-2233

Fax: +55 (48) 2106-2211

E-mail: [support@contronics.com](mailto:support@contronics.com)