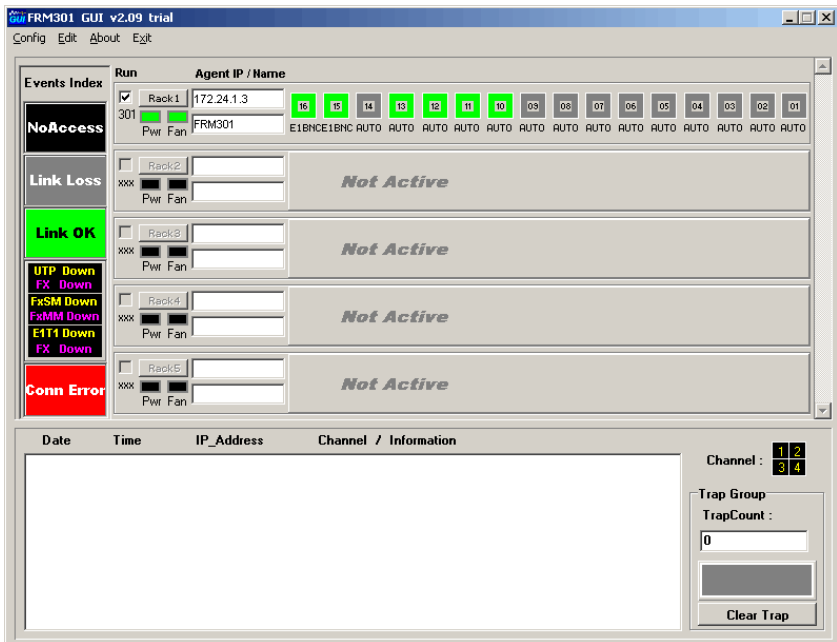# USER MANUAL

GUIMGR
Graphical User Interface Manager
for FRM301/FRM401 Media Racks

CTC Union Technologies Co.,Ltd.

ISO 9001

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center (Neihu Technology Park)
8F, No. 60 Zhouzi St.
Neihu, Taipei 114
Taiwan
Tel: +886-2-26591021
Fax: +886-2-27991355
Email: support@ctcu.com
URL: http://www.ctcu.com

GUIMGR User Manual

Graphical User Interface Manager, v1.0 June 2004

This manual applies to GUIMGR both Release and trial version 2.09 .

Table of Contents

1. Software Installation and Removal

1.1 Introduction

This brief manual will explain the installation / removal, configuration and operation of the FRM GUI (Graphical User Interface), a Windows® based program that uses SNMP protocol to monitor and configure the FRM301/401 fiber media converter racks. This first section will deal with the installation and removal of the GUIMGR software.

1.2 System Requirements

1.11 Operation System

The GUI program, hereafter called GUIMGR, is designed for installation in any Microsoft™ Windows® based computer. The program runs a standard Windows installer and is compatible on any 32bit OS (Windows 95/98/ME) or NT based OS (Win NT 4.0, Windows 2000, & Windows XP). Also highly recommended is the HyperTerminal program which is not installed by default in Windows 95/98.

1.12 Hardware

The minimum recommended hardware requirements for running GUIMGR are a Pentium™ class computer with 128MB memory, 5MB free disk space (the final installed software is less than 2MB), CDROM drive (for installing the software), VGA graphics display with 800x600 minimum resolution (1024x768 recommended), and a configured 10Base-T or 100Base-TX Network Interface Card (NIC). Our example will use a PC with the following static settings:

IP of 172.24.1.126
Subnet mask 255.255.0.0
Gateway of 172.24.190.254

The management station may be attached directly to the FRM301/401 SNMP card with an Ethernet crossover cable.

1.2 Installation

If you have only the trial version of GUIMGR, then it may not require normal installation. Simply un-zip the compressed transport file and place the executable file (GUI_trial.exe) and information file (agentIP.INI) in a convenient location. Create a shortcut to the "exe" file on the desktop, or place the executable file on the desktop itself. The "agentIP.INI" file must be in the same directory as the "exe" file to run properly.

GUI_trial.exe

If you have the full distribution version of the GUIMGR program, then please follow the procedure below for installation.

Place the GUIMGR installation CDROM in the computer's CDROM drive. Use "My Computer" or "Explorer" to browse to the CDROM's contents. Double click on the "Setup" icon to start the program installation.
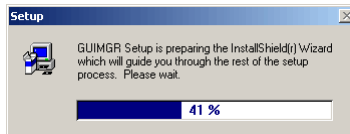
Figure 1.1 Setup started InstallShield Wizard
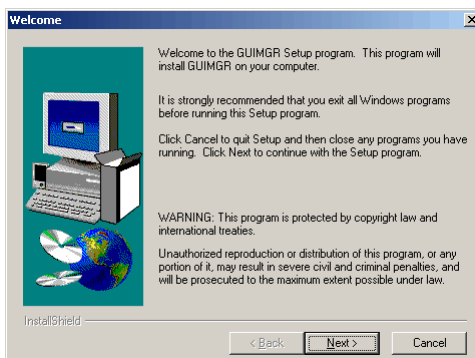
Figure 1.2 Setup welcome page, click "Next"
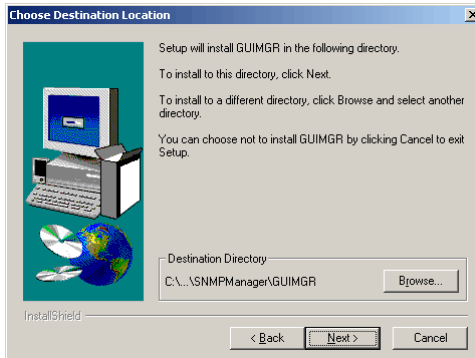
Figure 1.3 Choose program directory, click "Next" to use default.
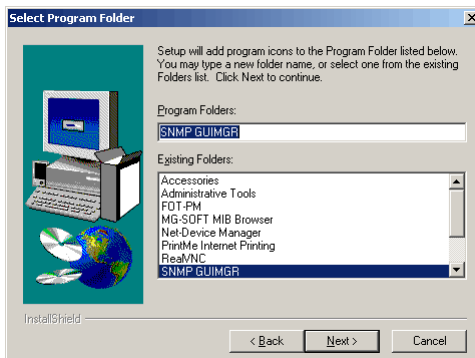
Figure 1.4 Select the Program Folder, click "Next" for default.
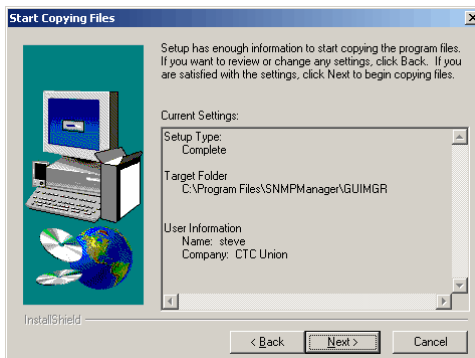
Figure 1.5. Start copying files, click "Next"
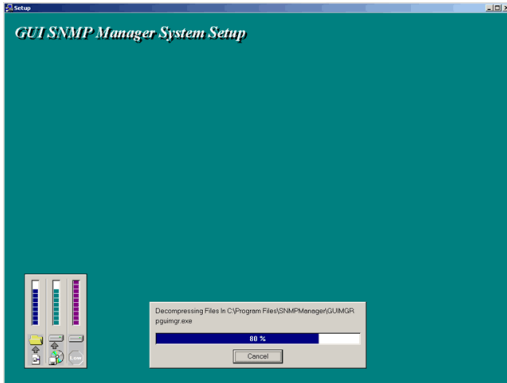
This completes the installation of the GUIMGR software program.

1.4 Remove GUIMGR

1.3.1 Control Panel Add/Remove programs

To open the control panel, click the Windows "Start" button and from the "Settings" icon, select "Control Panel".
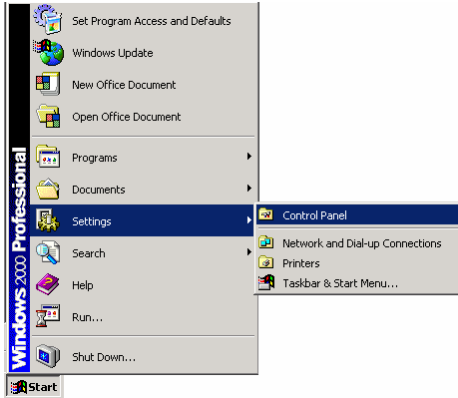
Figure 1.6 Opening the Control Panel in Windows 2000

In the Control Panel window, double click the "Add/Remove Program" icon. The following window will open. Find the GUIMGR icon as shown below.
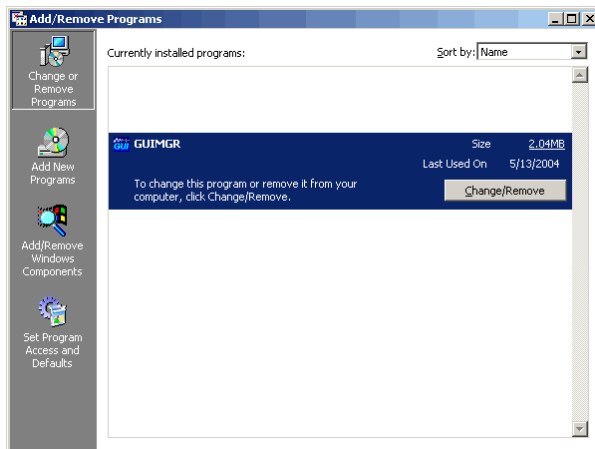
Figure 1.7 Add/Remove Programs window

Click the "Change/Remove" button.
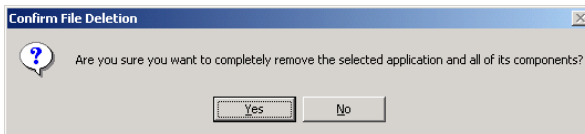
Figure 1.8 Confirm application removal, click "Yes" to continue uninstall.
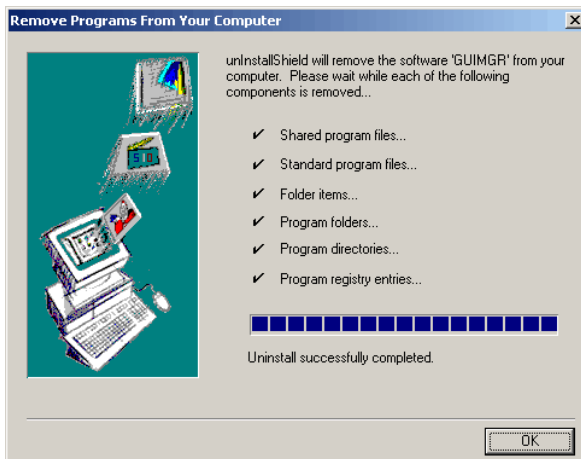
Figure 1.9 Uninstall completed successfully, then click "OK".

The GUIMGR computer program has now been completely uninstalled from your computer.

The registry entries created by the GUIMGR installation are not deleted. The password used to operate the GUI software is stored in the registry at:

HKEY_LOCAL_MACHINE/SOFTWARE/GUIMGR/config/Pass_word

The default password is "1021".

To remove all traces of the GUIMGR from the registry, delete <u>GUIMGR</u> under the HKEY_LOCAL_MACHINE/SOFTWARE location.

2. SNMP Card Configuration

2.1 Introduction

The FRM301/401 SNMP card is an optional component, installed in the FRM301/401 chassis, and provides Telnet and SNMP access. The setting of the SNMP card is performed through the terminal console port of the FRM301/401.

2.2 HyperTerminal™ settings

The settings for console port communication with the FRM301/401 are 38.4K baud, 8 bits, no parity, 1 stop bit and no flow control. In the HyperTerminal program terminal window click the "properties" icon and set the communication parameters as in the following graphics. Click the "Configure…" button in the properties window and set the port settings. When set properly, click "OK".
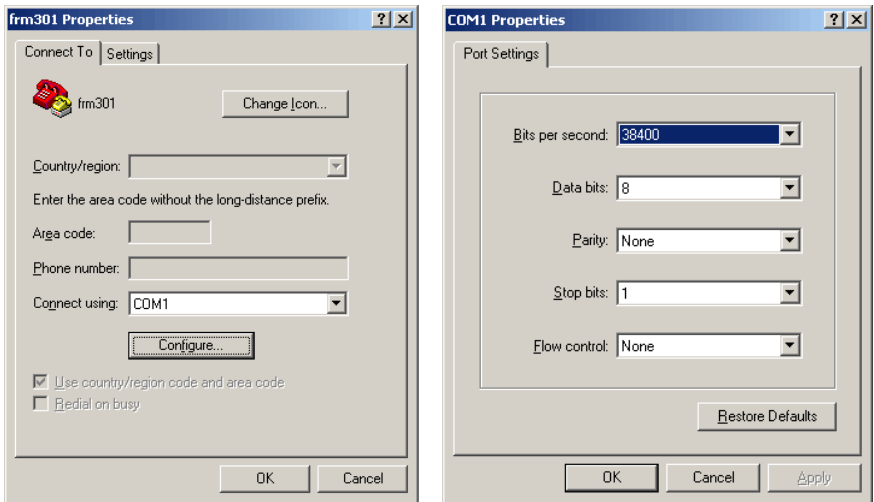
Figure 2.1 HyperTerminal port settings for FRM301/401

2.3 Connecting to the FRM301/401

The console port of the FRM301/401 is an RS-232 interface (DCE) that utilizes a DB9F connector. Use the configuration cable that is supplied with the FRM301/401 or prepare a three wire DB9(F) to DB9(M) cable with the following pinout:

DB9(M)	signal	DB9(F)
5	GND	5
2	TD	2
3	RD	3
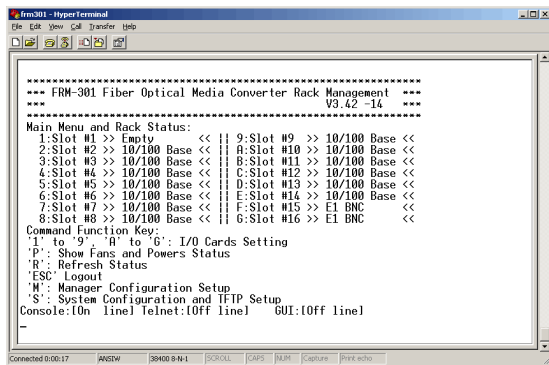
Figure 2.2 FRM301/401 main screen in console mode.

Connect the PC running HyperTerminal to the FRM301/401 that has an installed SNMP card option. The above screen indicates successful communication with the FRM301/401.

2.4 FRM301/401 menu system

Details of the menu system operation and meaning of menu items are described in detail in the FRM301/401 User's Manual. The following information is only for configuration of the SNMP option for use with a network management system.

From the main welcome screen, press "S" to enter the system configuration of the FRM301/401.

2.5 SNMP Card settings

```
**************************************************************
*** FRM-301 Fiber Optical Media Converter Rack Management  ***
***                              V3.42                     ***
**************************************************************
System Configuration and TFTP Setup Menu:
   MAC Address              : 0002AB025678
 1:IP Address               : 192.168.0.218
 2:Subnet Mask              : 255.255.255.0
 3:Gateway IP               : 192.168.0.254
 4:TFTP Server IP           : 192.168.0.45
 5:TFTP Server Path         :
   /300.bin

Command Function Key:
'1' to '5': Configure Setting
'R': Reset All Setting to Default
'S': Store Setting and Reboot
'T': TFTP and Flash
'ESC': Main Menu
```

2.5.1 SNMP Agent Configuration

The "agent" is the FRM301/401 SNMP. The IP address, subnet mask, default gateway, and TFTP server's IP address/path are all set within the System Configuration.

Select "1" IP Address

`IP Address->172.24.1.3`
Key-in the IP address for the SNMP agent in the FRM301/401. This IP address is also the Telnet IP address of the FRM301/401 rack.

Select "2" Subnet Mask

`Subnet Mask->255.255.0.0`
Key-in the subnet mask for the agent.

Select "3" Gateway IP

`Gateway IP->172.24.190.254`
Key-in the default gateway IP address.

Select "4" TFTP Server IP

`TFTP Server IP->172.24.1.126`
Key-in the IP address of a server running the TFTP protocol (trivial FTP) used for updating the SNMP firmware image in the SNMP card.

Select "5" TFTP Server Path

`TFTP Server Path->d:\342.bin`

Review the settings and make any necessary corrections. If all entries are correct press "S" to Store Settings and Reboot the SNMP agent.

2.5.2 Manager Configuration

From the SNMP main menu, select item "M", Manager Configuration Setup. Manager configuration is required to tell the agent (the SNMP card) who has authority to access the SNMP via "Get" commands (read) or "Set" commands (write) and where to send "trap" messages (unsolicited messages that are usually generated by alarms in the FRM301/401).

```
*************************************************************
*** FRM-301 Fiber Optical Media Converter Rack Management  ***
***                                   V3.42               ***
*************************************************************
Manager Configuration:
  Access Password: disable
  Community String #1 (Read/Write): public
  Community String #2 (Read Only) : *

    Access IP        SNMP Community Trap
    =============== ============== ====
  #1:*              public         Yes
  #2:*              *              *
  #3:*              *              *
  #4:*              *              *
Command Function Key:
'1': Edit Access IP#1        '3': Edit Access IP#3
'2': Edit Access IP#2        '4': Edit Access IP#4
'5': Edit Community#1 String (Read/Write)
'6': Edit Community#2 String (Read Only)
'7': User Password          '8': Manager Password
'9': Access Password ON/OFF
'R': Delete All Setting
'ESC': Main Menu
```

The manager configuration has the ability to setup access for up to four (4) different management workstations. The community strings act like passwords in dealing with the device via SNMP protocol. By changing the community strings for read / write ('public' in this case) and read only (undefined here) access, and assigning a community string to an access IP, an administrator can control access to the FRM301/401.

Enter the IP address of the management workstation that will be running the GUIMGR software, the access authority and whether or not it will be sent trap messages. Select "1":

```
IP('*':disable) ->172.24.1.126  #IP of manager
community '1' or '2'->1  #Manager has r/w privilege
trap 'y'es or 'n'o->y  #Manager will be sent trap messeges
```

Here are the results of our management configuration.

```
************************************************************
*** FRM-301 Fiber Optical Media Converter Rack Management  ***
***                                V3.42                 ***
************************************************************
Manager Configuration:
  Access Password: disable
  Community String #1 (Read/Write): public
  Community String #2 (Read Only) : *

     Access IP       SNMP Community Trap
     =============== ============== ====
  #1:172.24.1.126   public         Yes
  #2:*               *              *
  #3:*               *              *
  #4:*               *              *
Command Function Key:
'1': Edit Access IP#1        '3': Edit Access IP#3
'2': Edit Access IP#2        '4': Edit Access IP#4
'5': Edit Community#1 String (Read/Write)
'6': Edit Community#2 String (Read Only)
'7': User Password           '8': Manager Password
'9': Access Password ON/OFF
'R': Delete All Setting
'ESC': Main Menu
```

When leaving the Manager Configuration menu, the changes are automatically saved.

Note that in the above example, the management workstation with IP address 172.24.1.126 and using the community string 'public', has full read and write access and receives traps. If your management workstation has a different IP address, modify the above settings for your application. It is highly recommended that the read/write community string 'public' be changed using the menu selection '5'. Please also note that community strings are case sensitive. (public is not equal to Public)

3. GUIMGR Configuration and Operation

3.1 Introduction

This chapter assumes that the GUIMGR application has already been installed on the workstation as in Chapter 1 and that the SNMP agent has been correctly configured as in Chapter 2. This chapter will detail the GUIMGR configuration and the operation of the software in monitoring and controlling the FRM301/401 multiplexer.

3.2 Configuration

3.2.1 Start the GUIMGR application

Start the application by clicking the Windows "Start" button => Programs => SNMP GUIMGR => GUIMGR. A login password is required to enter the application. The password set from initial installation of the software is "1021". The user password may be changed via the "Config" pull down menu. Trial versions only need to click the "exe" file or shortcut and by default have no password set.
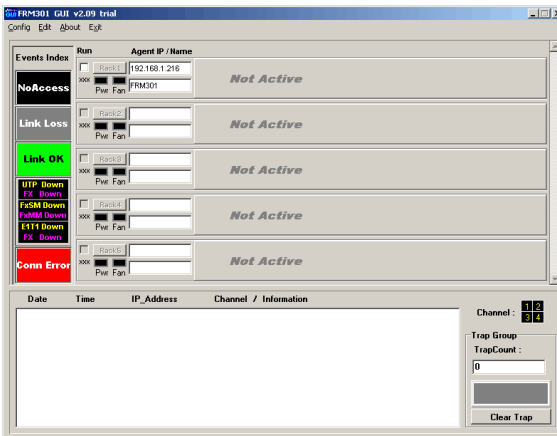

Figure 3.1 GUI manager login

Figure 3.2 GUIMGR first started

The GUIMGR behaves just like any other Windows® application. The following graphic shows all of the areas that may be clicked for further configuration. Some items are 'greyed' out until the application has connected with an actual FRM301/401 unit.
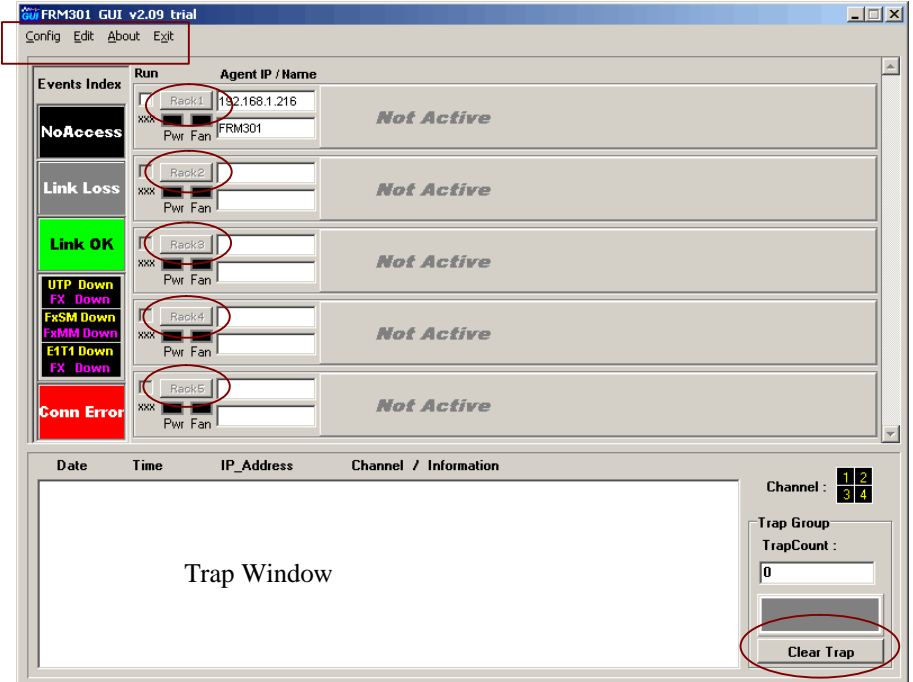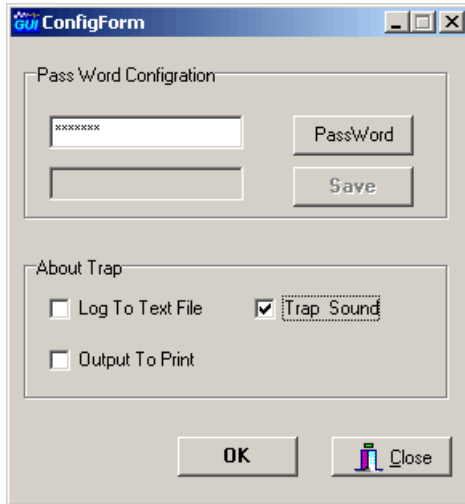

Figure 3.3 Selectable features of the Main GUIMGR

3.2.2 Configure user password

Click on "Config" from the window menu bar.

Figure 3.4 Configuration Form

Use this form to change the user password for the GUI. Note also that trap messages may be sent to a text file for logging, output to the default printer, and/or issue a warning beep on the PC.

3.2.3 Edit the SNMP Agent

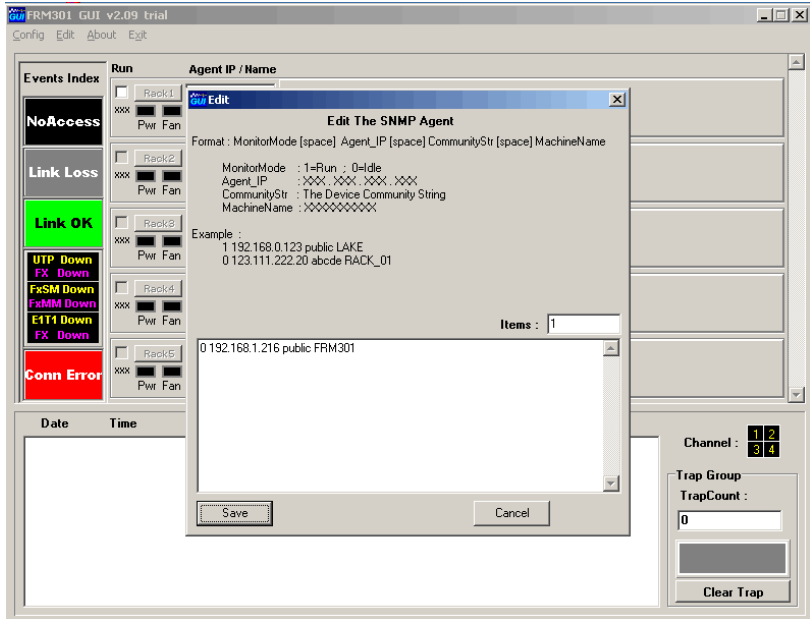Click on "Edit" from the window menu bar to enter the Edit SNMP Agent Window.

Figure 3.5 Edit the SNMP Agent

The entries already entered are there by default if the software was just installed. They are just for reference as examples of how the format should be entered into the window. If we continue with our example from the previous chapters, then the FRM301/401 unit which we wish to manage (the agent) is at IP address 172.24.1.3 and the r/w community string is 'public'. So we will click in the lower window (or select the already entered text) and backspace over it until the window is empty. Then we will enter our own format string:

1 172.24.1.3 public FRM301

Then click the "Save" button. Now the GUIMGR is set to manage a FRM301/401 at IP address 172.24.1.3 with a community string of 'public' and our manager will display the rack name as FRM301.

3.3 Operation

The interface for the GUIMGR program is a point and click Windows® application that requires little use of the keyboard.
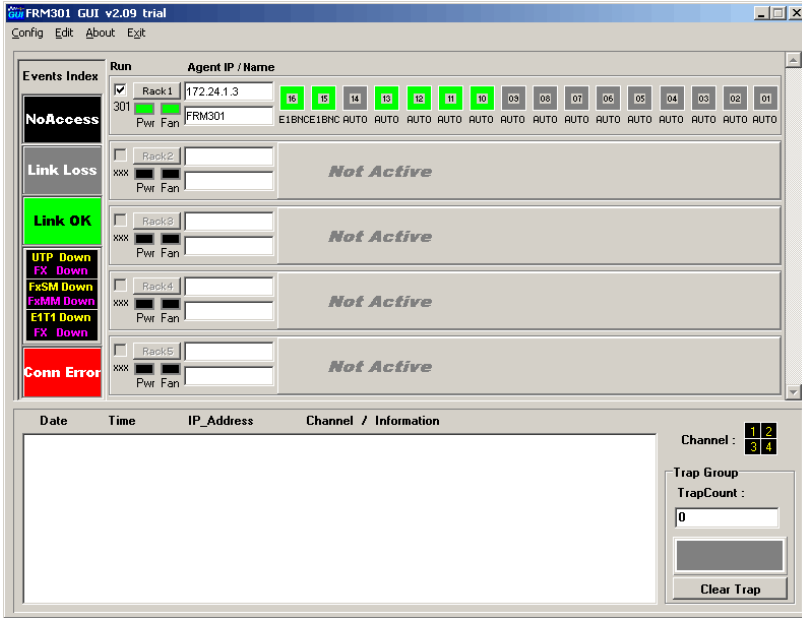

Figure 3.6 Operational GUIMGR screen

From the operational screen, the status of all rack units may be displayed. The Pwr and Fan indicators will display "green" when two power supplies are active and their fans are operating normally. Line card types are shown and link status displayed by color code:

"Green" status indicates that both the fiber and copper are linked.

"Yellow" indicates loss of link on the copper side.

"Magenta" indicates loss of link on fiber side.

"Grey" indicates neither copper nor fiber linked

"Black" color indicates an empty line card slot or un-identified card.

If all line cards are shown with "Red" color, it indicates a communication error. Possibly the configuration is not correct or there is a network error that prevents the manager from communicating with the agent.

The trap window at the bottom displays trap messages, indicating the source IP address, the time stamping of the trap and the trap message itself. New messages are displayed from the top, down. The "Clear Trap" button will erase all of the traps displayed and stored in memory.

3.3.1 Rack Detail

From this main display, we can view the details of any rack by clicking on the "Rack" button for that particular rack. Select the first device by clicking on the "Rack 1" button. A new window will open displaying the rack's front and rear panel details.
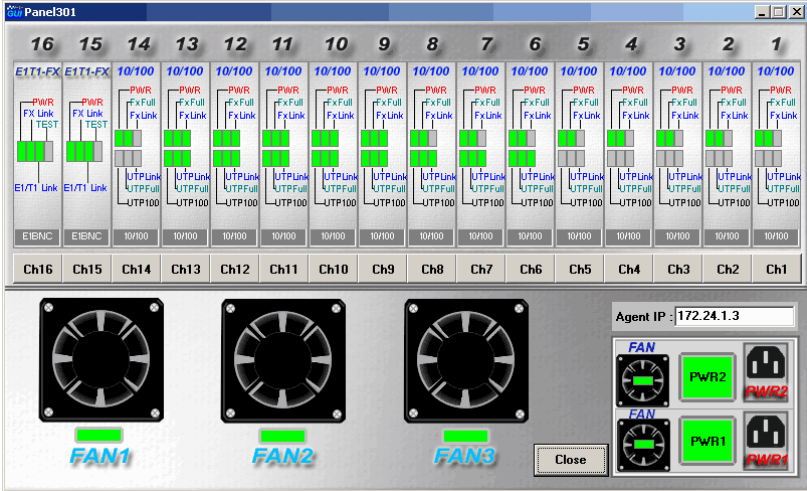

Figure 3.7 Rack 1's GUIMGR screen

The front panel graphic shows the operational state of all the installed line cards. The LED indications are shown in real time. Fan and power status are also displayed in "green". A "Red" indication on any of the fans, power supplies, or power supply fans indicates device or power failure.

3.3.2 Ethernet Line Card Settings

Click the button marked "Chx". From this window we can display the individual line card's status, setup the card's working status, configure the UTP and fiber modes, get the remote unit's status or do loop back functions. Use the "Get" button to read the card's status. Use the "Set" button to write new status to the card. (The operations are all preformed via SNMP protocol.)
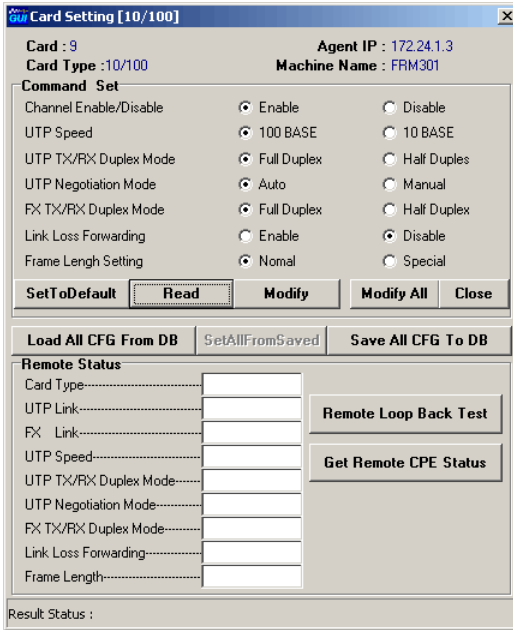
Figure 3.8 Ethernet Line Card Settings

The card slot, type, address of machine and machine type are shown in the header information. The 'Command Set' window is used for channel enable/disable, UTP mode setting, Fiber mode setting, LLF function enable/disable, and normal or extended packet frame length setting. The settings may be set to default, loaded from a configuration file previously saved on the PC, or saved to PC. The 'Read' button will get all the settings for this card. The 'Modify' button will set the settings selected to the card. The 'Modify All' button will take the displayed settings and write them to every card of the same type in the rack.

18

3.3.3 Remote Functions

The lower half of the window addresses the functions that can be performed when the fiber is connected to an FIB1-10/100 remote unit. Both of these functions are performed "in-band" and will cause a momentary loss of transmission in the link while they are being performed. The 'Remote Loop Back Test' button will test the fiber link by issuing a loopback code, sending pattern data, verifying the pattern data and then removing the loopback for normal transmissions.
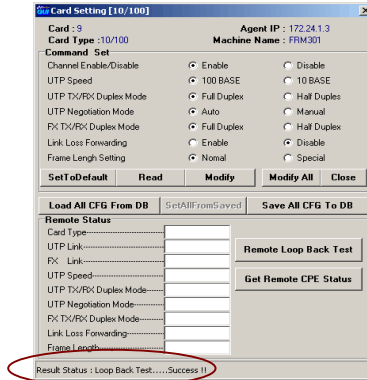

Figure 3.9 Loopback test with CPE

The 'Get Remote CPE Status' button will attempt to identify and read all the settings in the remote CPE unit.
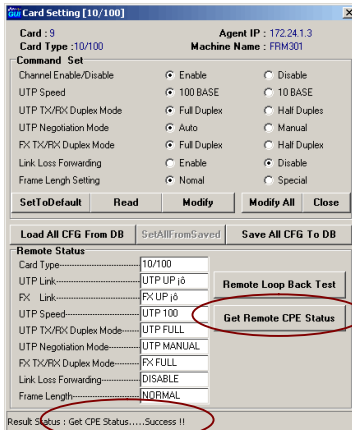

Figure 3.10 Remote Status for CPE

The card type, UTP and Fiber link status and other settings are all displayed for the remote side CPE.

Click the "Close" button to close the Card Setting window.

3.3.4 Gigabit Ethernet Line Card Settings

Click the button for a 1000Base line card to view and configure the local line card. Under the GUI, the card's status, Tx/Rx Duplex mode and LLF function may be read or modified.
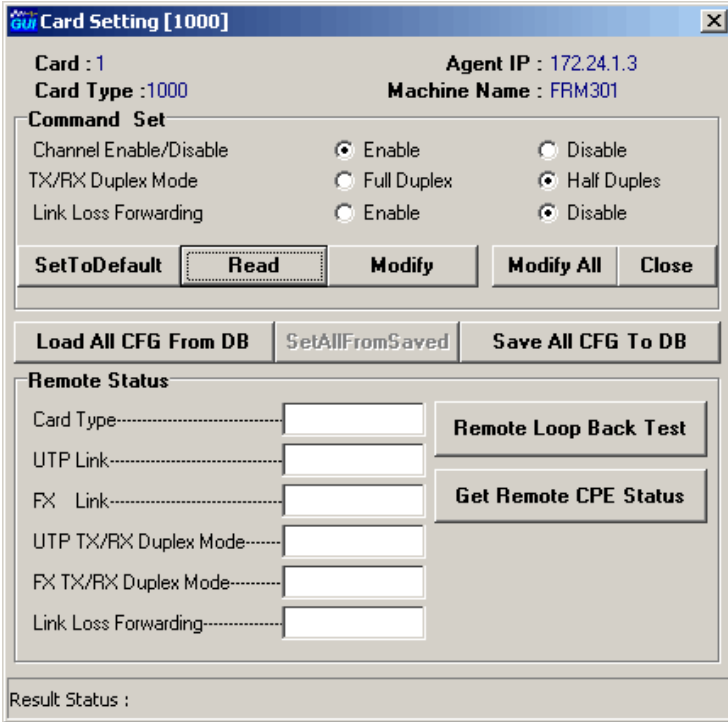

Figure 3.11 Gigabit Line Card Settings

The functions are very similar to those of the 10/100 Ethernet converter. When connected to an FIB1-1000, the loop back and get remote status functions may be used as well.

3.3.5 E1/T1 Line Card Settings

If an E1/T1 Line Card is installed in any slot, the status of the E1/T1 link, port settings and loop back functions may be viewed by clicking the channel button. Use the 'Get' button to read settings and the 'Set' button to send any modifications to the line card.
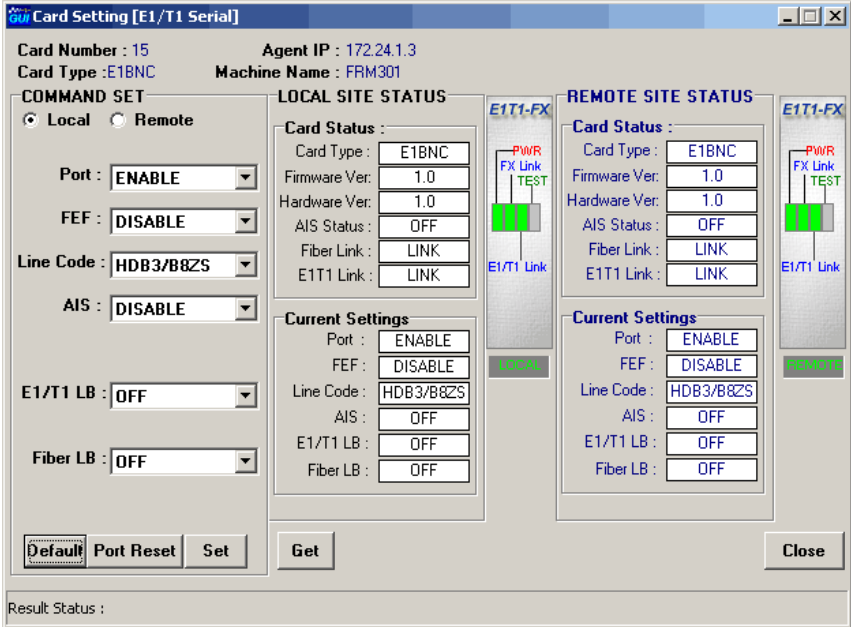

Figure 3.12 E1/T1 Line Card Settings

The command sets may be performed on the local converter in the rack or on the remote FIB1-E1/T1 fiber converter. The LEDs show the real time status of the card and remote converter. A full set of loop back functions are available.
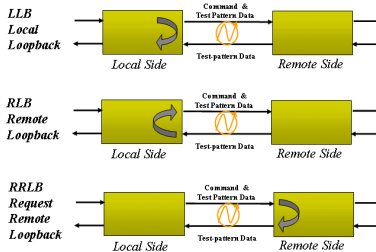

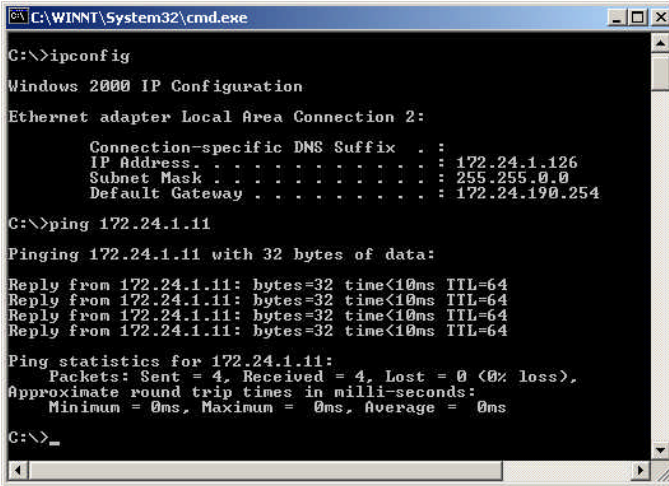**Figure 3.13 E1/T1 Loop Back Functions**

21

4 Troubleshooting

4.1 Network Settings

4.1.1 Review Agent Settings

During unit startup, the "SNMP" LED will light as the agent boots up, then it should blink at about one cycle per second after boot up and during normal operation. Refer to section 2.5.1 of the SNMP agent settings. Be sure you have a valid IP address for the attached network, that the subnet mask is properly set and that the default gateway is set if you wish to manage the FRM from a remote network.

Attach a network cable to the FRM's front panel LAN/SNMP connector using a straight cable if connecting to a HUB or a cross over cable if connecting directly to another MDI device, such as direct connection to a workstation. The Link LED should be on or flashing. No link LED means no link. From any PC on the network, confirm the agent can be pinged.


```
C:\WINNT\System32\cmd.exe

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 172.24.1.126
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 172.24.190.254

C:\>ping 172.24.1.11

Pinging 172.24.1.11 with 32 bytes of data:

Reply from 172.24.1.11: bytes=32 time<10ms TTL=64
Reply from 172.24.1.11: bytes=32 time<10ms TTL=64
Reply from 172.24.1.11: bytes=32 time<10ms TTL=64
Reply from 172.24.1.11: bytes=32 time<10ms TTL=64

Ping statistics for 172.24.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>_
```

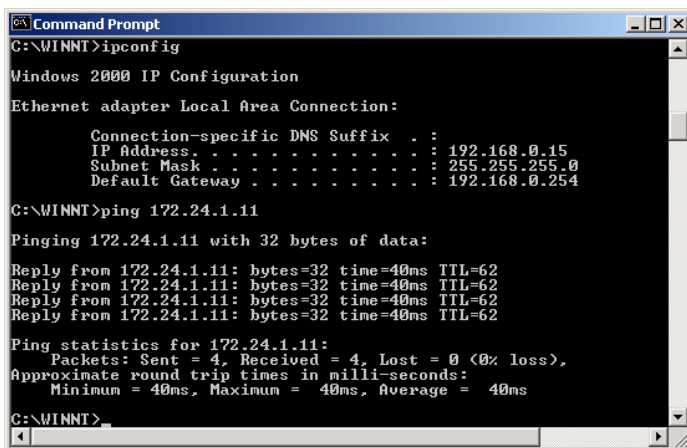**Figure 4.1 Ipconfig and Ping**

The "ipconfig" command from a command window in NT will display the workstation's IP, subnet and gateway settings. The "ping" command will send an ICMP protocol message to the agent, which in turn should reply. If no reply, double check all network connects, connect directly from a workstation to the FRM, or as a last resort replace the SNMP card of the FRM.

4.1.2 Review Manager Settings

For the GUIMGR to connect to the FRM for management, the FRM's SNMP must be properly configured with the manager's IP address and authorized for read/write (via community string setting) and trap messages. Review the settings explained in 2.5.2.

Review the "Edit" settings in 3.2.3 of the GUIMGR application, and confirm that the monitor mode is set to "1", IP address and community string for read/write match those as set from section 2.5.2.

If the management workstation is on a remote network, ensure it can also pass the ping test.

Figure 4.2 Ipconfig and Ping Remote Network

Check with your network administrator to ensure that any firewalls in place will allow passing of SNMP protocol in order to connect with an FRM on a remote network. By default SNMP uses port 161.

Always check all connections and double check all configurations. We have tested the FRM and GUIMGR extensively on local networks, on remote networks through bridges and routers and even over wireless links. You should not experience any problems if you follow each and every step in this guide. We hope you enjoy using the FRM with SNMP option and GUIMGR manager software.

Fiber Series Units

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technologies Center
(Neihu Technology Park)
8F, No. 60, Zhouzi St., Neihu, Taipei, Taiwan
Phone:(886) 2.2659.1021   Fax:(886) 2.2.799.1355
E-mail: info@ctcu.com http://www.ctcu.com