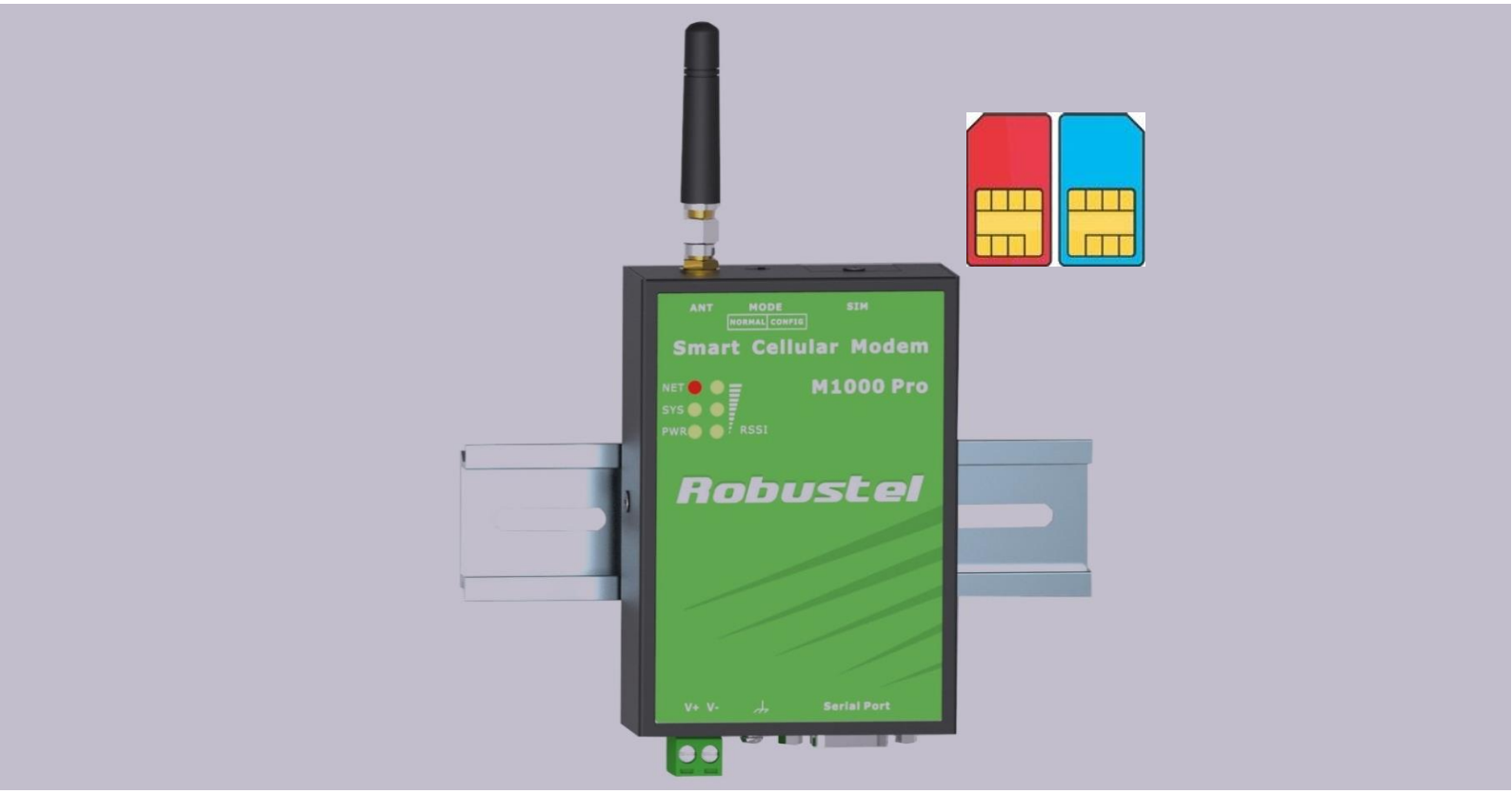
Robustel GoRugged M1000 Pro V2

Dual SIM Industrial Serial to Cellular Gateway

For GSM/GPRS/EDGE/UMTS Networks

User Guide

Document Name:	**User Guide**
Firmware:	**2.22.0**
M1000 Pro V2 Configurator:	**2.22.0**
Date:	**2015-05-13**
Status:	**Confidential**
Doc ID:	**RT_UG_M1000 Pro V2_v.2.1.0**



Robustel

www.robustel.com

About This Document

This document describes the hardware and software of the *Robustel M1000 Pro V2 Dual SIM Industrial Serial to Cellular Gateway*.

Trademarks and Permissions

Robustel are trademark of Guangzhou Robustel Technologies Co., Limited.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the use of this document.

Technical Support Contact Information

Tel: +86-20-23354618
Fax: +86-20-82321505
E-mail: support@robustel.com
Web: www.robustel.com

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the gateway is used in a normal manner with a well-constructed network, the gateway should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Robustel accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the gateway, or for failure of the gateway to transmit or receive such data.

Safety Precautions

General

- The gateway generates radio frequency (RF) power. When using the gateway, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your gateway in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Be sure that the gateway will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the gateway should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the gateway for proper operation. Only uses approved antenna with the gateway. Please contact authorized distributor on finding an approved antenna.
- Always keep the antenna with minimum safety distance of 20 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.

***Note**: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Gateway may be used at this time.*

Using the gateway in vehicle

- Check for any regulation or law authorizing the use of GSM devices in vehicle in your country before installing the gateway.
- The driver or operator of any vehicle should not operate the gateway while driving.
- Install the gateway by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the gateway.
- The gateway should be connected to the vehicle's supply system by using a fuse-protected terminal in the vehicle's fuse box.
- Be careful when the gateway is powered by the vehicle's main battery. The battery may be drained after extended period.

Protecting your gateway

- To ensure error-free usage, please install and operate your gateway with care. Do remember the following:
- Do not expose the gateway to extreme conditions such as high humidity / rain, high temperature, direct sunlight, caustic / harsh chemicals, dust, or water.
- Do not try to disassemble or modify the gateway. There is no user serviceable part inside and the warranty would be void.

- Do not drop, hit or shake the gateway. Do not use the gateway under extreme vibrating conditions.
- Do not pull the antenna or power supply cable. Attach/detach by holding the connector.
- Connect the gateway only according to the instruction manual. Failure to do it will void the warranty.
- In case of problem, please contact authorized distributor.

Regulatory and Type Approval Information

Table 1: Directives

2011/65/EC	Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS)	
2012/19/EU	Directive 2012/19/EU the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE)	

Table 2: Standards of the Ministry of Information Industry of the People's Republic of China

SJ/T 11363-2006	"Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products" (2006-06).
SJ/T 11364-2006	"Marking for Control of Pollution Caused by Electronic Information Products" (2006-06). According to the "Chinese Administration on the Control of Pollution caused by Electronic Information Products" (ACPEIP) the EPUP, i.e., Environmental Protection Use Period, of this product is 20 years as per the symbol shown here, unless otherwise marked. The EPUP is valid only as long as the product is operated within the operating limits described in the Hardware Interface Description. Please see **Table 3** for an overview of toxic or hazardous substances or elements that might be contained in product parts in concentrations above the limits defined by SJ/T 11363-2006. 

Table 3: Toxic or hazardous substances or elements with defined concentration limits

Name of the part	Hazardous substances					
	(Pb)	(Hg)	(Cd)	(Cr (VI))	(PBB)	(PBDE)
Metal Parts	o	o	o	o	o	o
Circuit Modules	x	o	o	o	o	o
Cables and Cable Assemblies	o	o	o	o	o	o
Plastic and Polymeric parts	o	o	o	o	o	o

o:

Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

x:

Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in SJ/T11363-2006.

Revision History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Release Date	Firmware Version	Doc Version	Details
2013-11-19	2.5.0	V2.0.0	Update User Guide to firmware version 2.5.0
2015-05-13	2.22.0	V2.1.0	Update Section: Packing List, Install SIM Card, Power Supply, Firmware version, Connection, Dual SIM, Safety Precautions, Regulatory and Type Approval Information, mount the Gateway, PIN assignment, file format, Sentence Revision, Regulatory and Type Approval Information

Contents

Chapter 1 Product Concept

1.1 Overview

Robustel GoRugged M1000 Pro V2 is a rugged serial to cellular gateway with dual SIM offering state-of-the-art 2G/3G connectivity for machine to machine (M2M) applications.

- Dual SIM redundancy for continuous cellular connection.
- Various SIM backup polices: PING/Monthly data traffic/Roaming.
- Auto GPRS/UMTS connection (no AT commands required).
- Support CSD communication (only receive CSD call).
- Transparent TCP and UDP socket connections.
- Supports Virtual COM (COM port redirector).
- Supports ICMP, DDNS, Telnet.
- Supports RobustLink (Centralized M2M management platform).
- Supports Modbus gateway (Modbus RTU to Modbus TCP).
- Supports Modbus master polling, collects data at preset interval and sends to RobustLink.
- Various reboot policies: SMS/Caller ID/Timing.
- Various dial-up policies: Always Online/Connect On Demand.
- Remote configuration via RobustLink/TCP/SMS.
- Remote firmware upgrade via RobustLink/TCP.
- RS232/RS485 selectable by software.
- Six LED indicators provide signal strength and running status.
- Watchdog for reliable communications.
- Wide range input voltages from 9 to 36 VDC and extreme operating temperature.
- The metal enclosure can be mounted on a DIN-rail or on the wall, also with extra ground screw.

1.2 Packing List

Check your package to make certain it contains the following items:

- Robustel GoRugged M1000 Pro V2 gatewayx1

- 2-pin pluggable terminal block for power connector x1

- CD with user guide and configuration utility x1

***Note**: Please notify your sales representative if any of the above items are missing or damaged.*

Optional accessories (can be purchased separately):

- SMA antenna (Stubby antenna or Magnet antenna optional) x1

Stubby antenna ***Magnet antenna***

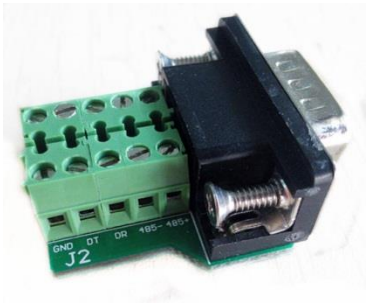
- Serial cable for RS232 (DB9 Female to DB9 Male, 1 meter) x1

- Wall Mounting Kit

- 35mm Din-Rail mounting kit

- AC/DC Power Supply Adapter (12VDC, 1A) x1

- DB9 Male to terminal block for serial port
  The detail about the PIN assignment is showed in the 2.3 PIN assignment section.



1.3 Specifications

Cellular Interface

- Standards: GSM/GPRS/EDGE/UMTS
- GPRS: max. 86 kbps (DL & UL), class 10
- EDGE: max. 236.8 kbps (DL & UL), class 12
- UMTS: max. 384 kbps (DL & UL)
- Frequency: 850/900/1800/1900 MHz for GPRS/EDGE, 850/900/1800/1900/2100 MHz for UMTS/HSPA+
- CSD: Up to 14.4 kbps

- SIM: 2 x (3V & 1.8V)
- Antenna Interface: SMA Female

Serial Interface

- Number of Ports: 1 x DB9 Female
- Serial Standards: RS232 and RS485
- ESD Protection: ±15KV
- Baudrate: 1200bps to 115200bps
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B)

System

- LED Indicators: PWR, RUN, NET and 3 level RSSI
- Real Time Clock: Built-in RTC with button battery
- Watchdog and Timer: Built-in watchdog and timer

Software

- IP protocols: PPP, TCP, UDP, ICMP, DDNS, Telnet
- Serial Port: TCP client/server, UDP, Modbus RTU to Modbus TCP, Virtual COM (COM port redirector)
- RobustLink: Centralized M2M management platform

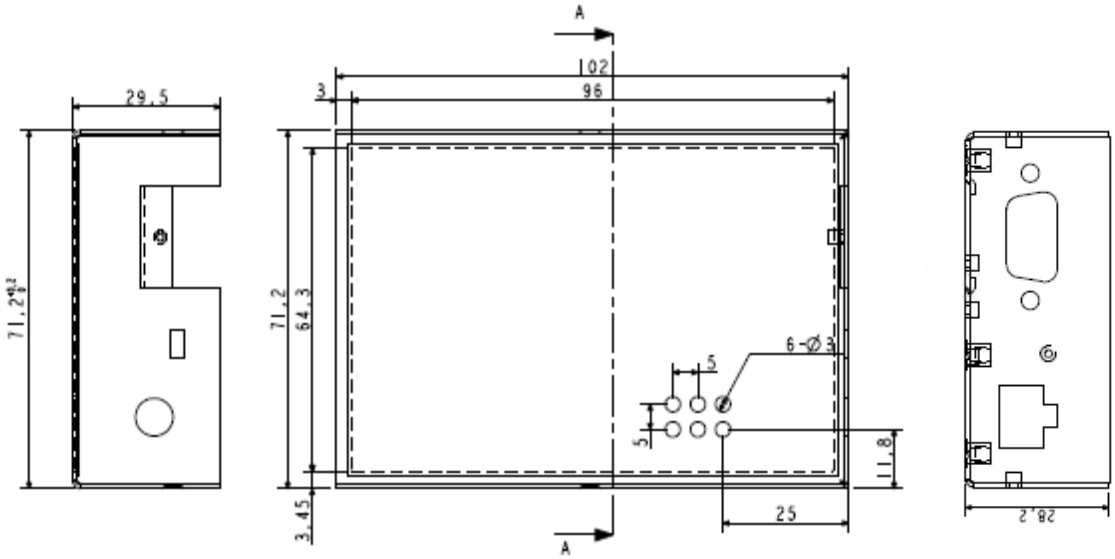
Power Supply and Consumption

- Power Supply Interface: 2-pin 5mm pluggable terminal block
- Input Voltage: 9 to 36 VDC
- Power Consumption: Idle: 50-60 mA@12 V
  Data Link: 100 to 200 mA (peak)@12 V

Physical Characteristics

- Housing & Weight: Metal, 300g
- Dimension(L x W x H): 102 x 71 x 29 mm
- Installation: 35mm Din-Rail or wall mounting or desktop

1.4 Dimensions

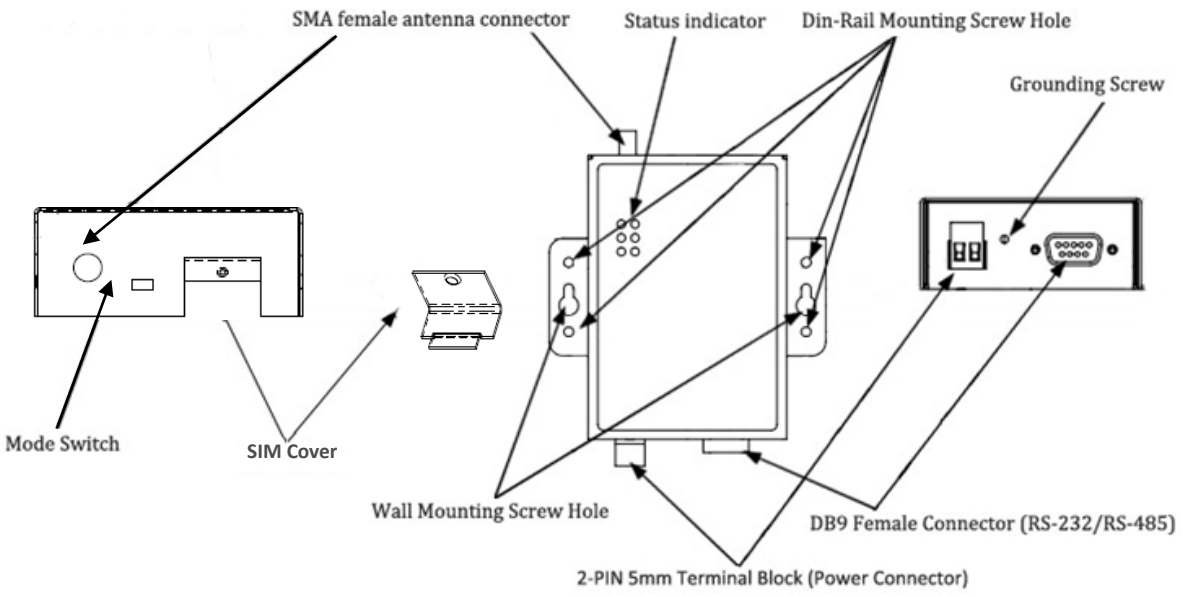


1.5 Selection and Ordering Data

Model No.	Description	Operating Environment
M1000-PGPRSA	1-port RS232, GPRS Class 10	-40 to 85°C/5 to 95% RH
M1000-PGPRSB	1-port RS232/RS485, GPRS Class 10	-40 to 85°C/5 to 95% RH
M1000-PUMTSA	1-port RS232, GPRS/EDGE/UMTS	-40 to 85°C/5 to 95% RH
M1000-PUMTSB	1-port RS232/RS485, GPRS/EDGE/UMTS	-40 to 85°C/5 to 95% RH

Chapter 2 Installation

2.1 Overview

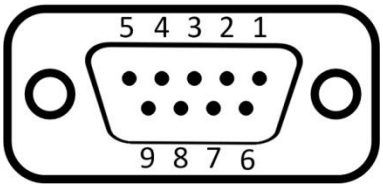


2.2 LED Indicators

Name	Color	Function
RSSI (3 LEDs)	Green	Cellular signal strength level
NET	Red	Indicating the GPRS/UMTS connection status. Register to network: blinking every 3s Device running error alarm: always on Wireless module rebooting and searching GPRS/UMTS network: blinking every 1s ***Note**: RSSI LEDs which will be explained later show the specific error info.*
SYS	Green	Indicating the system status. System is booting: blinking every 0.5s System is running normally but without any GPRS/UMTS connection: blinking every 1s System is running normally and GPRS/UMTS connection established: blinking every 3s System is running abnormally: 2.5s on and 0.5s out during every 3s
PWR	Green	On when DC power connected

RSSI LEDs	Function
None	No signal or SIM card not installed properly
1 bar (Only the first LED is on)	Weak or insufficient signal (SMS only)
2 bars (The first and the second LED are on)	Average signal (GSM/GPRS/UMTS connections)
3 bars (All the RSSI LEDs are on)	Exceptional signal (GSM/GPRS/UMTS connections)
The first and the second LED are blinking every 1 second	PIN code error
The third LED is blinking every 1 second	PIN code error and need to use PUK code to unlock it
The second LED is blinking every 1 second	No SIM card or SIM card not installed properly
The third LED is blinking every 1 seconds	Wireless module communication error, no AT command response.
The first and the third LED are blinking every 1 second	Cannot register to network or SIM card is unavailable

2.3 PIN assignment



Terminal block

PIN	RS232	RS485 (2-wire)	Terminal block	Direction
1		Data+ (A)	485+	-
2	RXD		RXD	M1000 Pro V2 → Device
3	TXD		TXD	Device → M1000 Pro V2
4			DT	-
5	GND		GND x2	-
6		Data- (B)	485-	-
7	RTS		RTS	Device → M1000 Pro V2
8	CTS		CTS	M1000 Pro V2 → Device
9			DR	-

2.4 Install SIM Card

Be sure to insert a SIM card before you use the gateway.

***Note**: A SIM card set with PIN code cannot be used normally in the gateway without the correct PIN code.*

Make sure to disconnect the adapter and switch off your gateway before inserting or removing your SIM/USIM card.

- **Inserting SIM Card**

1. Make sure your adapter is disconnected.
2. Use a screwdriver to unscrew the screw on the cover, and then remove the cover, you could find the SIM Card slot.
3. Insert the SIM card, and you need press the SIM card with your fingers until you hear “a cracking sound”. Then use a screwdriver to screw the cover.

- **Removing SIM card**

1. Make sure your adapter is disconnected.
2. Press the SIM card until you hear “a cracking sound”, then the SIM card will pop up to be pulled out.

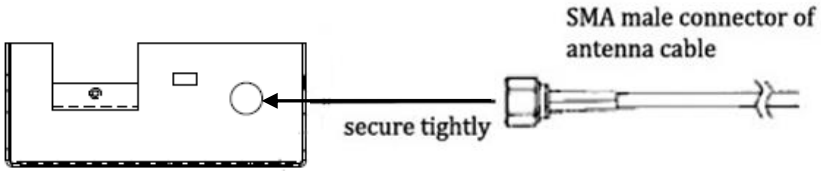
Note:

1. *Don’t forget screw the cover for again-theft.*
2. *Don’t touch the metal surface of the SIM card in case information in the card is lost or destroyed.*
3. *Don’t bend or scratch your SIM card. Keep the card away from electricity and magnetism.*
4. *Make sure to disconnect the power source from your gateway before inserting and removing your SIM card.*

5. *Please use the specific M2M SIM card when the device works in extreme temperature (temperature exceeding 0-40 ℃), because the long-time working of regular SIM card in harsh environment(temperature exceeding 0-40 ℃)may increase the possibility of SIM card failure.*

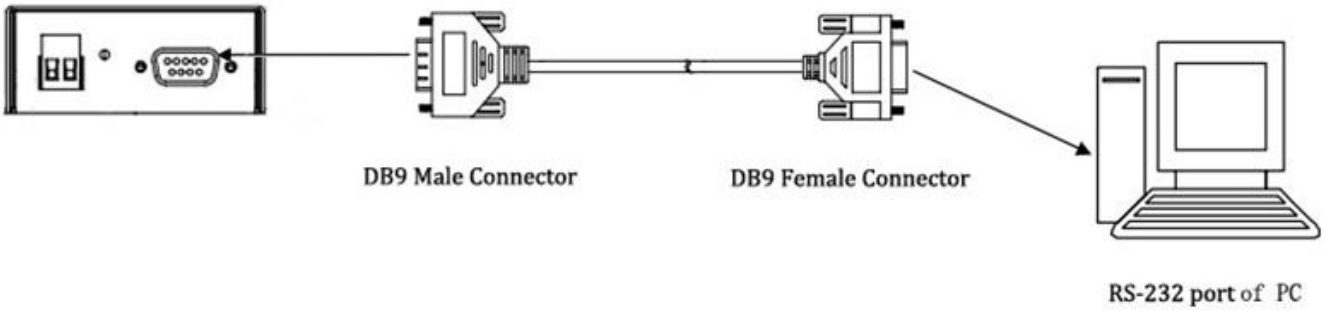
2.5 Connect the External Antenna (SMA Type)

Connect this to an external antenna with SMA male connector. Make sure the antenna is within correct frequency range as your GSM operator with impedance of 50ohm, and connector is secured tightly.



2.6 Connect the Gateway to External Device

User can use the serial cable to connect the gateway's DB9 female connector to external controller / computer.

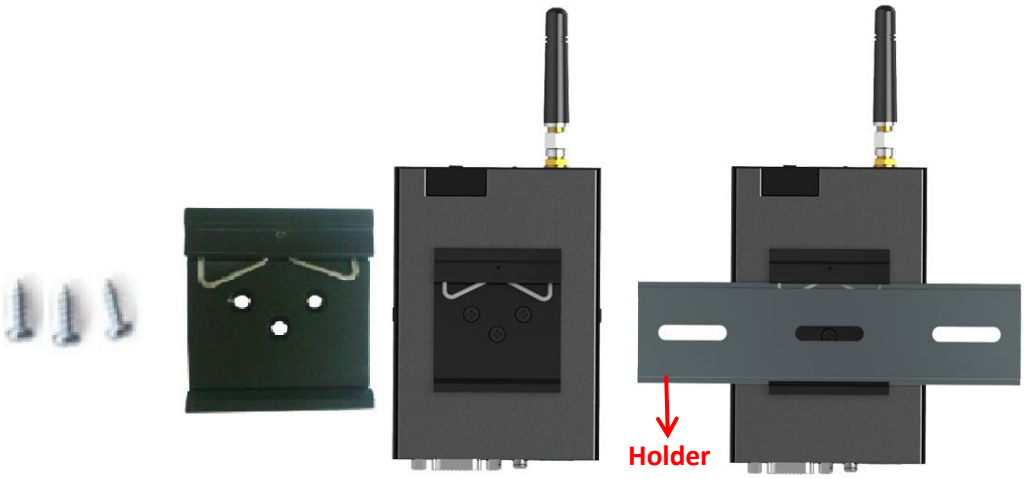


2.7 Mount the Gateway

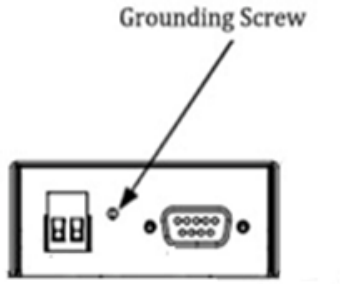
- **Two ways of mounting the Gateway**

1. Use 3 pcs of M3 screw to mount the Gateway on the Wall mounting Kit.
   And then use 2 pcs of M3 screw to mount the Wall mounting Kit on the wall.

2. Mount the Gateway on a DIN rail with 3 pcs of M3 screws, and then hang the DIN-Rail on the holder.
   You need to choose a standard holder.



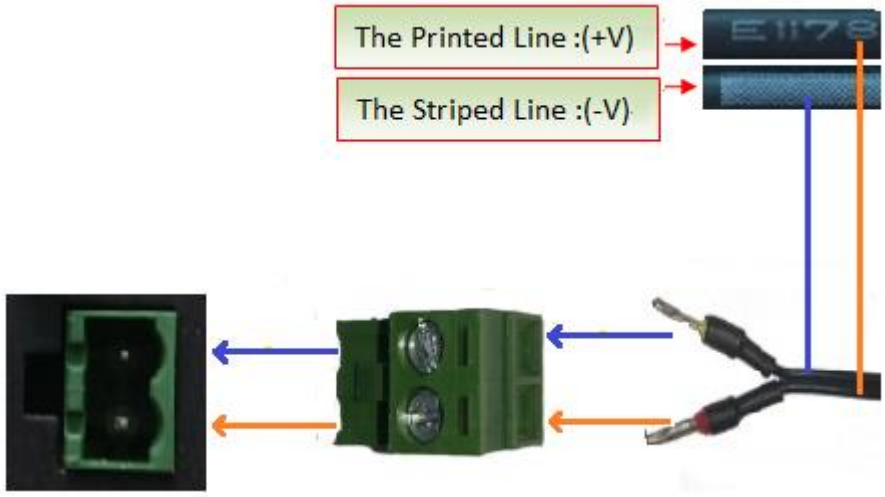
2.8 Ground the Gateway



Grounding and wire router helps limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground by screwing to the grounding surface before connecting devices.

***Note**: This product is intended to be mounted to a well-grounded mounting surface, such as a metal panel.*

2.9 Power Supply

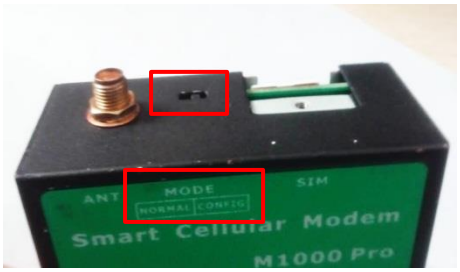


The power supply range is 9 to 36VDC.

***Note**: Please take care about the polarity, and do not make reverse connection. There are two lines connecting to the power supply adapter, as it illustrates on the power supply adapter label, the line printed with letters needs to be connected with the positive polarity, and the striped line needs to be connected with the negative polarity.*

Chapter 3 Operate the Gateway

3.1 Working Mode Overview



There are two working modes available in the gateway, please check carefully:

Mode	Description
Config Mode	When DIP switches to **Config Mode**, user could use follow functions: 1. Configure gateway via **M1000 Pro V2 Configurator** ; 2. Upgrade firmware. **Serial port parameters is fixed as 115200, 8, None, 1**
Normal Mode	When DIP switches to **Normal Mode**, user could use follow functions: 1. Automatic GPRS/UMTS connection (no AT commands required); 2. Wakeup by Timing/Periodical/Call/SMS/Serial Data; 3. Transparent data communication or become a Modbus gateway; 4. CSD communication. 5. Remote configuration or firmware updating. **Serial port default parameters: 115200, 8, None, 1**

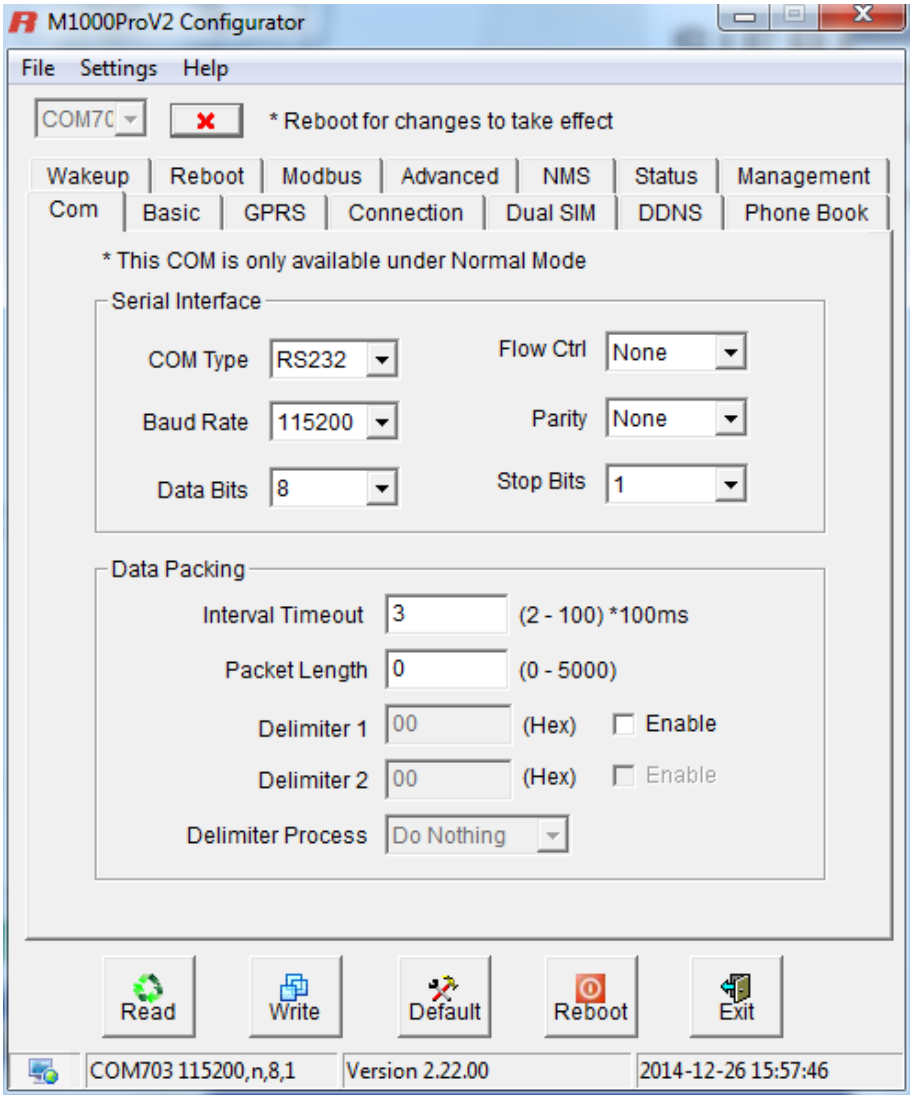
3.2 M1000 Pro V2 Configurator Overview

M1000 Pro V2 Configurator is a PC-based configuration software tool for managing and configuring Robustel M1000 Pro V2 gateway. With a full graphics mode and Windows-based environment, even first time users will find it easy to learn how to use this new software tool.

M1000 Pro V2 Configurator not only makes configuration easily, but also makes it convenient to carry out “mass deployment” and “pre-configuration”. The most important benefits of using the “M1000 Pro V2 Configurator” utility are:

1. Green software, no need installation;
2. Full graphics mode, easy to learn how to configure the M1000 Pro V2;
3. Configuration profile can be easily stored, and then replicated to other M1000 Pro V2;
4. Easy to upgrade gateway firmware.

***Note**: M1000 Pro V2 Configurator can be used with Windows 2000/XP/Vista/7 32/64-bit operation systems. If there is any running issue, for example, the Configurator run normally in Win 7 system but fail to run in Windows XP system, please search "Microsoft Visual C++ 2008 Redistributable Package" to download relevant patch and then install the patch.*

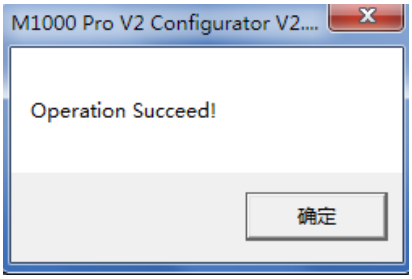


3.2.1 Management via RS-232 port

1. Switch the gateway to "Config Mode", connect the RS-232 port of the gateway to a host PC, and then power on the gateway.

2. Double click "M1000 Pro V2 Configurator.exe" to start the software.

3. Select correct COM port, then click  button. After that you can see the popup windows "Operation Succeed".

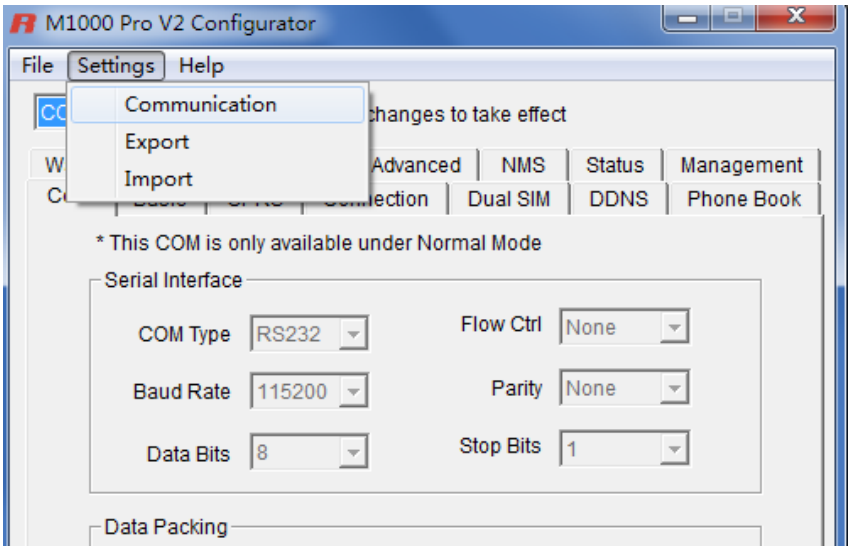


***Note**: The RS-232 connector uses standard PINOUT. A direct male DB9 to female DB9 cable can be used to connect to a PC's serial port.*

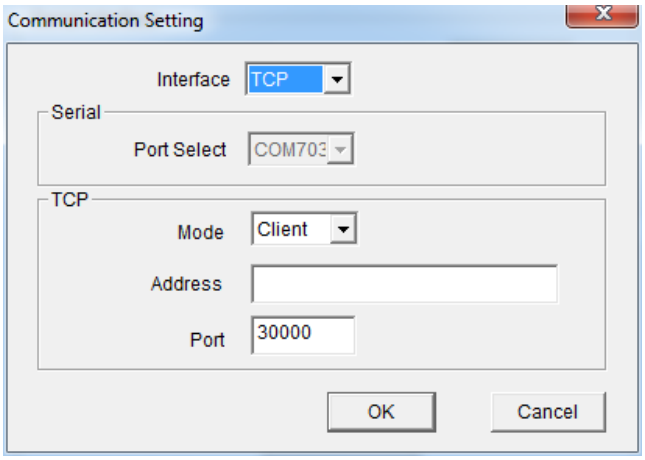
3.2.2 Management via TCP connection

1. Double click "M1000 Pro V2 Configurator.exe" to start the software.

4. Go to tab "Settings" -> "Communication".



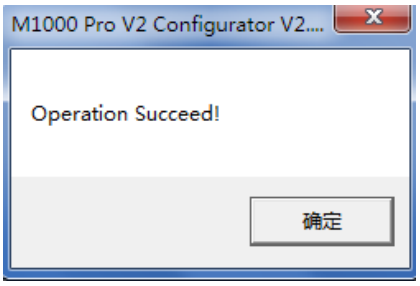
2. Select “TCP” interface and the correct mode in the drop down boxes, and enter the local TCP port. If you choose client mode, you need to enter the remote gateway’s IP address. Then click “OK”.



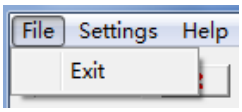
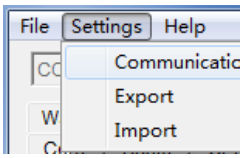
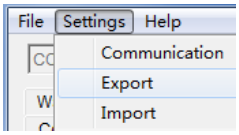
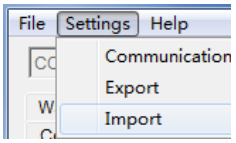
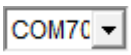
***Note**:*

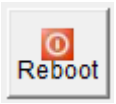
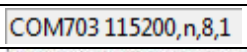
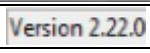
- *If you choose TCP client mode, the configurator will establish a TCP connection to the remote gateway which works as TCP server.*
- *If you choose TCP server mode, the configurator will be in listening status. Then you need to send an SMS to the remote gateway to trigger it to establish a TCP connection with configurator. The form of SMS is “0009, configurator’s IP address or domain name, configurator’s TCP port”. Please refer to section **Chapter 1.5.2 SMS Command for Remote Control***
- *The NMS function of gateway must have been enabled. Please refer to section **3.2.16 NMS.***
- *The cell phone’s number must be included in gateway’s phonebook.*

3. Click  button. After that you can see the popup windows “Operation Succeed”.



3.2.3 Operation Area Introduction

Menu	Icon	Description
File->Exit		Exit the M1000 Pro V2 Configurator.
Settings->Communication		Set the communication ways of configurator: Serial or TCP.
Settings->Export		Export the gateway’s current configuration file to your local PC.
Settings->Import		Import the gateway’s configuration file from local PC to the gateway.
Help->Help		Show some notices about this configurator.
Help->About		Manufacturer’s information and Gateway Configuratior version.
Port No.		Select the local RS-232 port to communicate with the gateway.
Connect		Connect the M1000 Pro V2 Configurator to the gateway.
Disconnect		Disconnect the M1000 Pro V2 Configurator to the gateway, and release the PC’s RS-232 port.

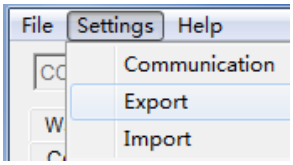
Read		Read gateway's current settings.
Write		Save changes into gateway. ***Note**: Some parameters changes need to reboot to take effect.*
Default		Set gateway to default factory settings.
Reboot		Reboot the gateway.
Exit		Exit the M1000 Pro V2 Configurator.
Disconnecting		Gateway is not communicating with M1000 Pro V2 Configurator.
Connecting		Gateway is communicating with M1000 Pro V2 Configurator.
Serial Management Settings		Show current RS232 communication parameter.
TCP Management Settings		Show current TCP management communication status
Versions		Show current firmware version

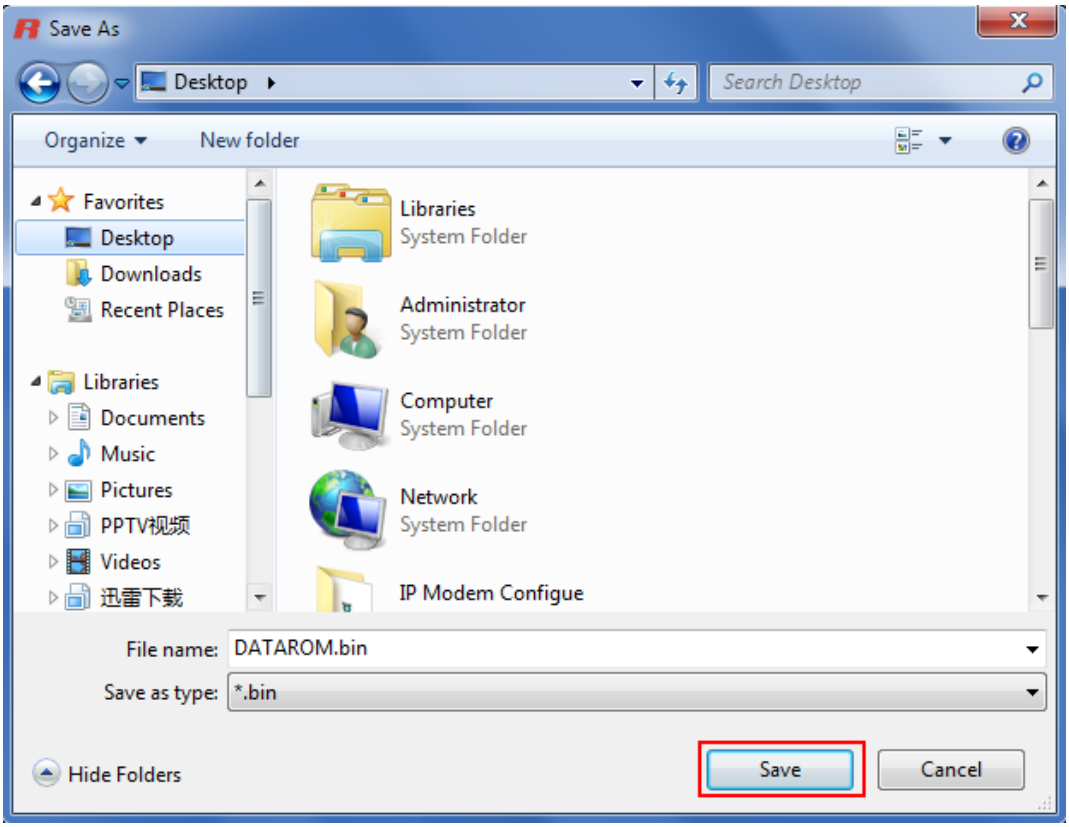
Important Notice:
You must save your parameter changes by clicking "Write" button and then reboot M1000 Pro V2 by clicking "Reboot" button to activate the configuration changes.

3.2.4 Export and Import Profiles

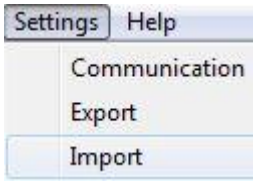
Users could export gateway settings from one gateway, and then import the same settings to other gateways, which makes it convenient to carry out "mass deployment" and "pre-configuration".

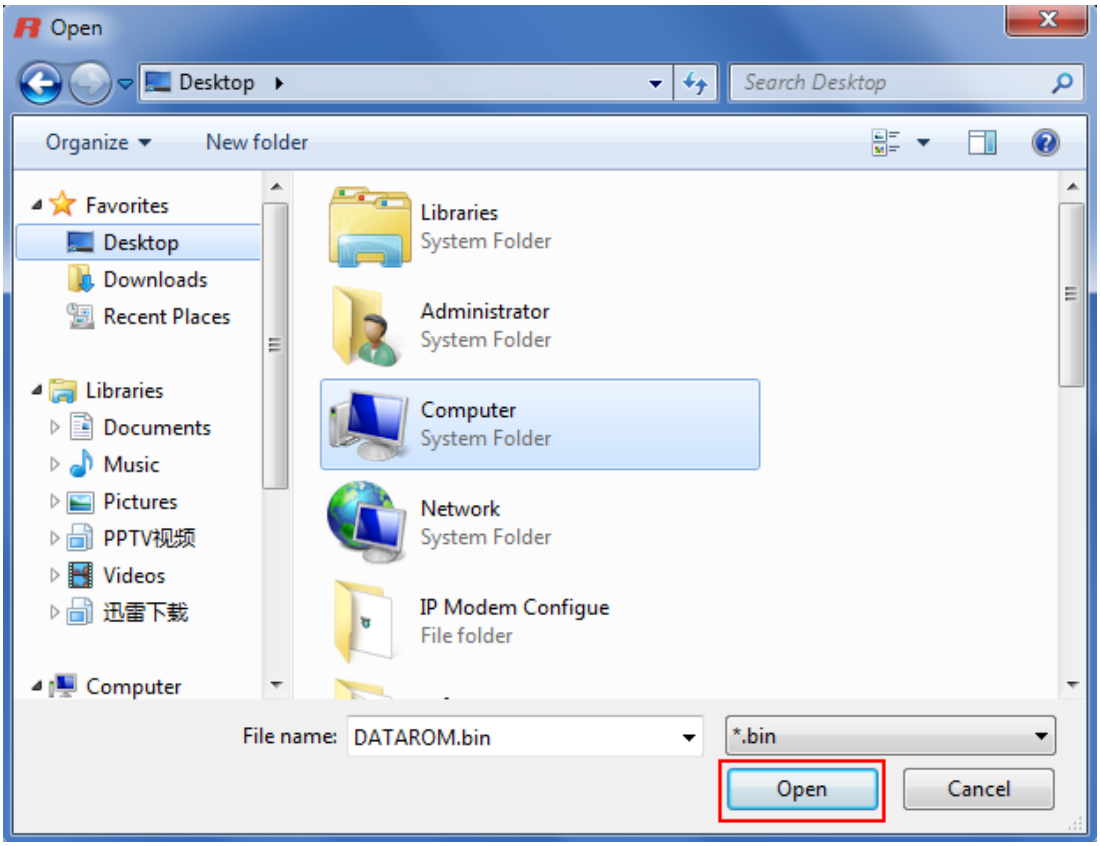
1. Select **Export** from the **Settings** menu. Then select a folder and enter the file name for the profile. Click on **Save**, then it will popup "**Export Succeed**" windows.



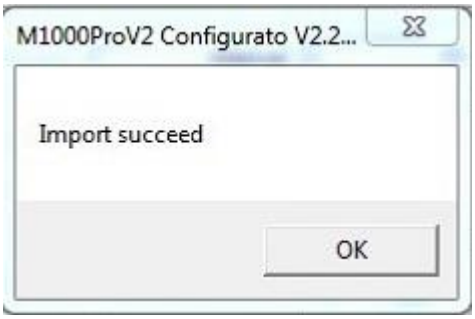


2. Select **Import** from the **Settings** menu. Then select a profile. Click on **Open**.



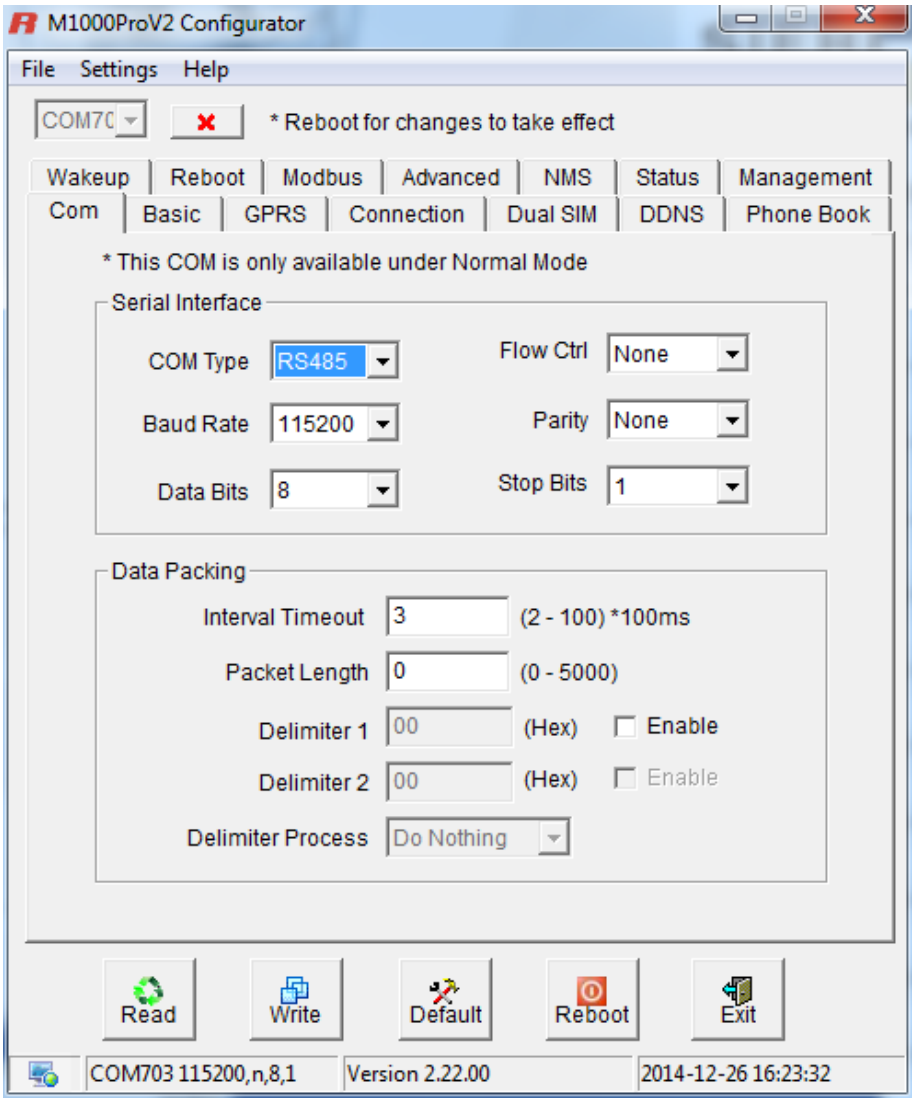


3. Click "**Write**" button then it will popup "**Import Succeed**" windows.



3.2.5 COM

This tab allows user to set the parameters of serial com port:

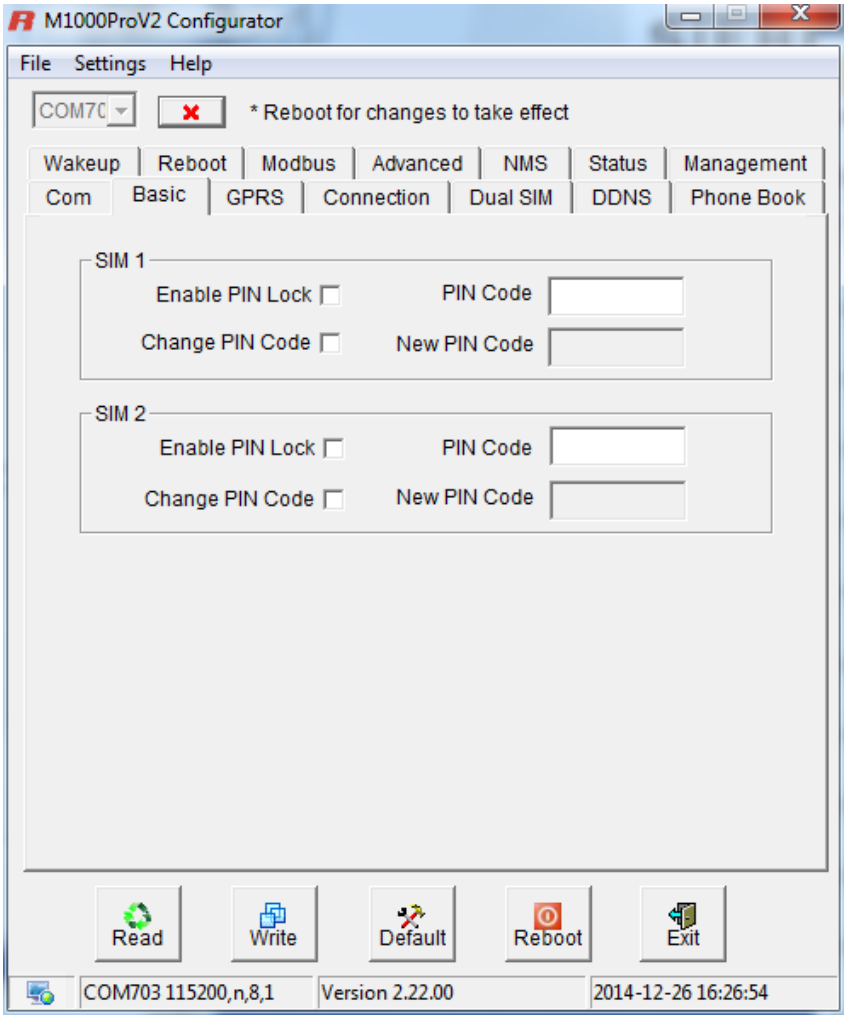


COM		
Item	Description	Default
COM Type	Select from “RS232” and “RS485”.	RS232
Baud Rate	Select from “1200”, “2400”, “4800”, “9600”, “19200”, “38400”, “57600” and “115200”.	115200
Data Bits	Select from “7” and “8”.	8
Flow Ctrl	Select from “None” and “Hardware”.	None
Parity	Select from “None”, “Odd”, “Even”, “Mark” and “Space”.	None
Stop Bits	Select from “1” and “2”.	1
Interval Timeout	This value allows gateway to packet the received data as a TCP/UDP packet and sends it out even the size of them hasn’t reached the limit of *Packet Length*.	3

Packet Length	The limits size of the received data that gateway will packet as a TCP/UDP packet. ***Note:*** *0 is the same as the default value of TCP MSS, 1460.*	0
Delimiter	The delimiter indicate gateway to packet the received data as a TCP/UDP packet and sends it out even the size of them hasn't reached the limit of *Packet Length*.	00
Delimiter Process	Select from "Do Nothing" and "Strip Delimiter".	Do Nothing

3.2.6 Basic

This tab allows user to set follow items:



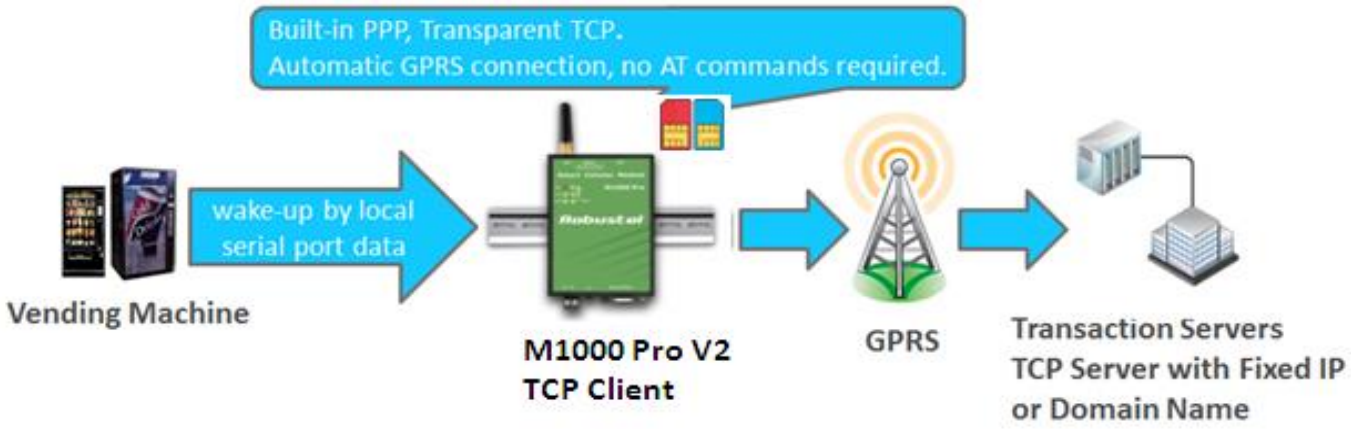
Basic		
Item	Description	Default
SIM Card PIN Setup	Select from “Disable PIN Lock” and “Enable PIN Lock”. After enable PIN lock, user could input your SIM’s PIN and store the current PIN in its memory, and then enter the PIN automatically each time the system boots up. ***Note**: Please ask your local GSM ISP to see whether your SIM card requiring PIN or not.* If user wants to change the SIM PIN, please tick the “Change PIN Code” checkbox to enable it, and then input the new PIN at “Input New PIN Code”. The PIN will be changed after reboot.	Disable

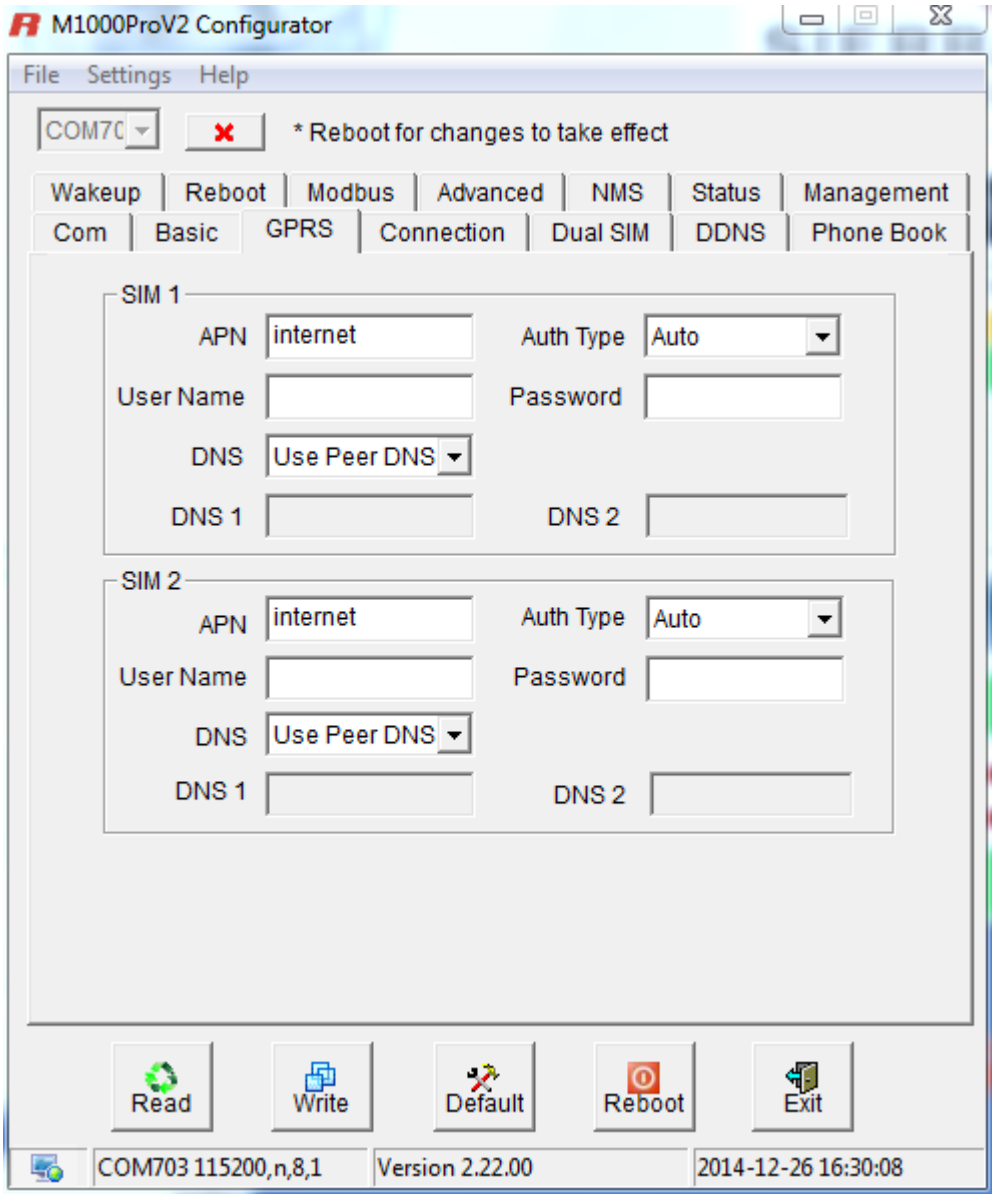
3.2.7 GPRS

The major difference between M1000 Pro V2 serial to GPRS/UMTS gateway and traditional modem such as M1000/M1000 Lite is that M1000 Pro V2 built-in PPP and TCP/IP protocols, supports automatic GPRS/UMTS connection, no AT commands required, which can enable transparent TCP/UDP transmission.

Traditional GPRS gateway can only dialup to internet via external PPP enabled host device such as PC, PLC with built-in PPP protocol.

This tab allows user to set GPRS/UMTS and related items for automatic GPRS/UMTS connection:

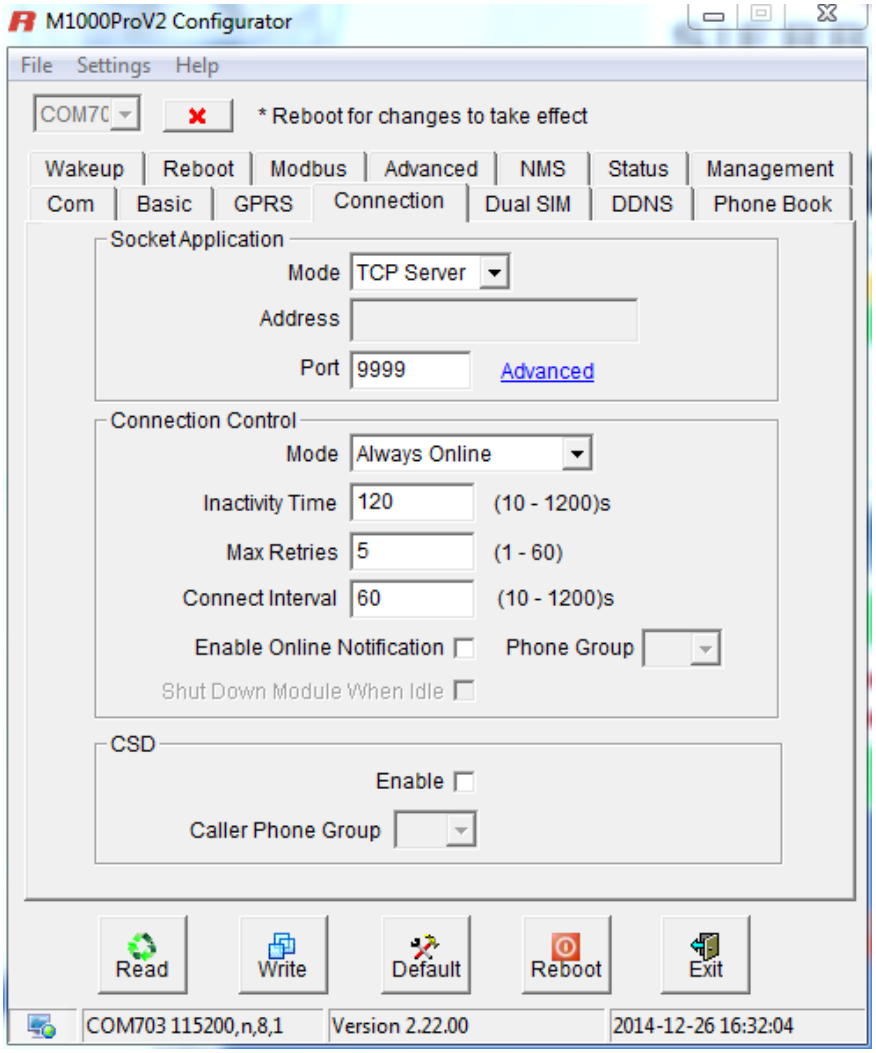


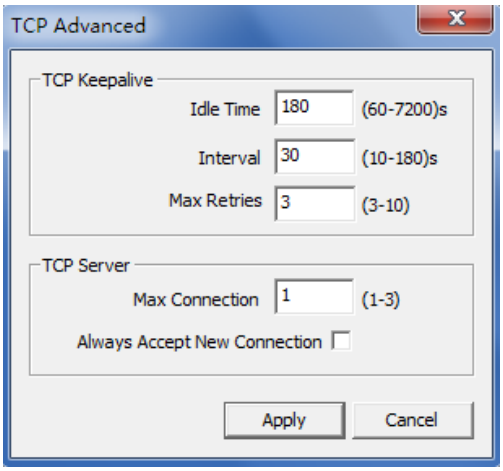


GPRS		
Item	Description	Default
APN	Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Auth Type	Selected from “None”, “Auto”, “PAP” and “CHAP” as the local ISP required.	Auto
User Name	User Name for cellular dial-up connection, provided by local ISP.	Null
Password	Password for cellular dial-up connection, provided by local ISP.	Null
DNS	Selected from “Use Peer DNS” and “Manual”. Use Peer DNS: to automatically have DNS server assigned from local ISP. Manual: input DNS server’s IP address manually in DNS 1 and DNS 2 field.	Use Peer DNS
DNS 1	Input DNS server’s IP address after enable DNS->Manual.	Disable
DNS 2	Input secondary DNS server’s IP address after enable DNS->Manual.	Disable

3.2.8 Connection

This tab allows user to set the TCP/UDP connections and other related parameters.



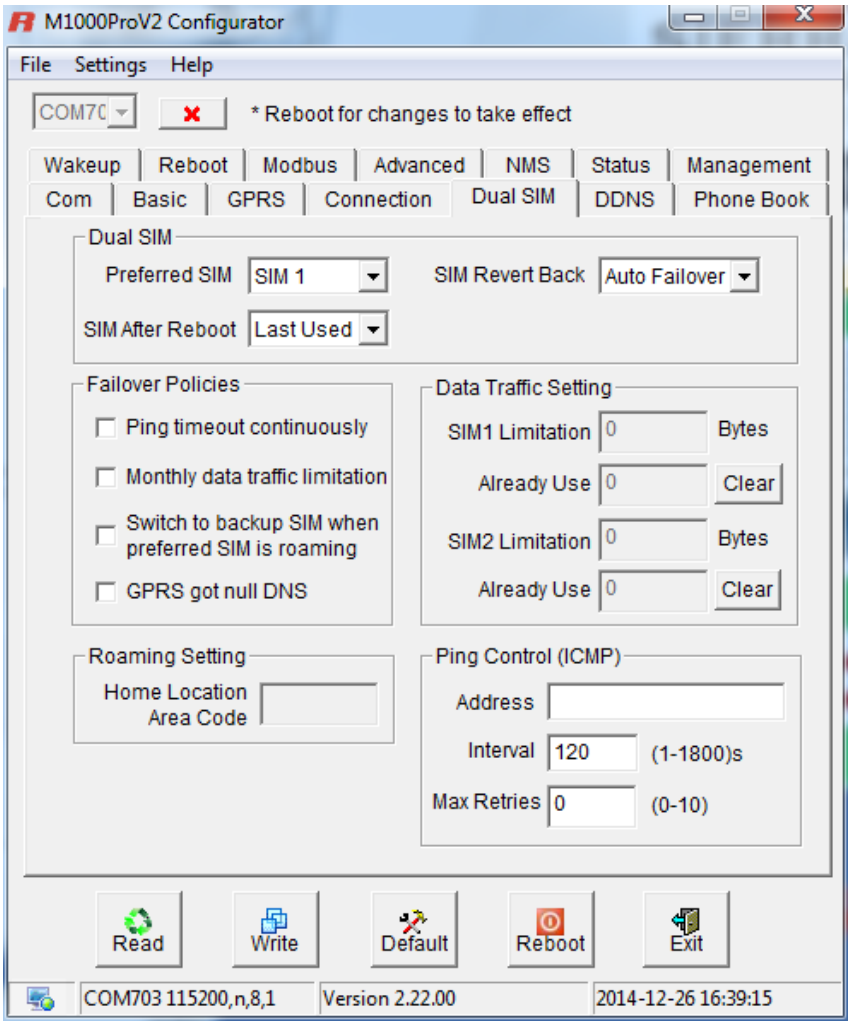


Connection		
Item	Description	Default
Mode @ Socket Application	Selected from “UDP”, “TCP Client” and “TCP Server”. UDP: Gateway works as UDP client. TCP Client: Gateway works as TCP client, initiate TCP connection to TCP server, y TCP Server: Gateway works as TCP server, listening for connection request from TCP client.	TCP Server
Address @ Socket Application	When gateway works as TCP client, user should input peer TCP server’s IP or domain in this item. When gateway works as TCP server, this item cannot be configured. When gateway works as UDP client, user should input peer UDP server’s IP or domain in this item.	null
Port @ Socket Application	When gateway works as TCP client, user should input peer TCP server’s port in this item. When gateway works as TCP server, user should input TCP server’s listening port in this item. When gateway works as UDP client, user should input peer UDP server’s port in this item.	9999
Advanced @ Socket Application	Click to set advanced settings of “Socket Application”.	
Idle Time	Whether gateway is set as TCP Client or TCP Server, keepalive feature can be used to detect whether TCP connection is disconnected by sending specific packets in the transport layer. User can set idle timeout interval in this item, gateway will send out keepalive packet if there is no data for more than “Idle Time”. “Idle Time” ranges from 60 to 7200 seconds.	180
Interval	No matter whether the response is received, it will send keepalive packet after the timeout, and then it will count the times of no response is received, until this maximum interval.	30
Max Retries	If gateway re-sends keepalive packet continuously for Max Retries times and doesn’t receive correct respond packets, it will detect that the TCP connection is disconnected and it try to establish TCP connection again. “Max Retries” ranges from 3 to 10 times.	3
Max Connection	When gateway is set as TCP Server, it will wait for TCP connection from TCP Client site. If TCP connection from TCP Client reaches to “Max Connection” it will drop a new TCP connection request. “Max Connection” ranges from 1 to 3.	1
Always Accept New Connection	After click to enable this item, M1000 Pro V2 will always accept new TCP connection and drop the earliest one at the same time.	Disable
Mode @ Connection Control	Select from “Always Online” and “Connect On Demand”. Always Online: Gateway will automatically initiate a GPRS/UMTS connection after power on and each restarts, this will remain and will be re-established after an interruption. Connect On Demand: After select this option, user could configure wakeup at preset time, wakeup periodically, wakeup by Call, wakeup by SMS, wakeup by local serial port data at ***Wakeup*** Tab.	Always Online

Inactivity Time	This field specifies the idle time setting for GPRS/UMTS auto-disconnection and trying to revert back to preferred SIM card. User could configure this field after setting gateway under Connect On Demand mode, input from 10 to 1200 seconds.	120
Max Retries @ Connection Control	The maximum retries times for automatically re-connect when gateway fails to dial up, input from 1 to 60. After maximum retries, If the gateway still cannot dial up successfully, it will reboot the wireless module and try to re-connect again. If another SIM card is detected, the gateway will try to switch to the other SIM card and then re-connect with maximum retries. If there is one SIM card the gateway will use the same SIM card to re-connect with maximum retries. When connecting successful, the Max Retries counter will be set to 0.	5
Connection Interval	Gateway will automatically re-connect with this interval when it fails communicating to peer via TCP or UDP; also gateway will automatically re-dial with this interval if PPP dial up failed. Input from 10 to 1200 seconds.	60
Enable Online Notification	Click to enable Online SMS Notification function, which will send SMS to the phone numbers included in the *Phone Group* tab. Online SMS Notification includes follow information: Name: Reg: RSSI: Operator: Local IP: Time: ***Note**: Local IP is the gateway's IP address assigned by ISP when dial-up to cellular network successful.*	Disable
Phone Group	Select the phone group which the online notification SMS sent to.	1
Shut Down Module When Idle	Enable to set the gateway to shut down module when connectivity is in idle state. This function can only be configured under *Connect On Demand* mode.	Disable
Enable @ CSD	Click to enable CSD feature.	Disable
Caller Phone Group @ CSD	Gateway will only receive CSD call from specific phone numbers which are authorized in this Phone Group.	1

3.2.9 Dual SIM

This tab allows user to set the SIM cards' priorities, backup policies and other related parameters.

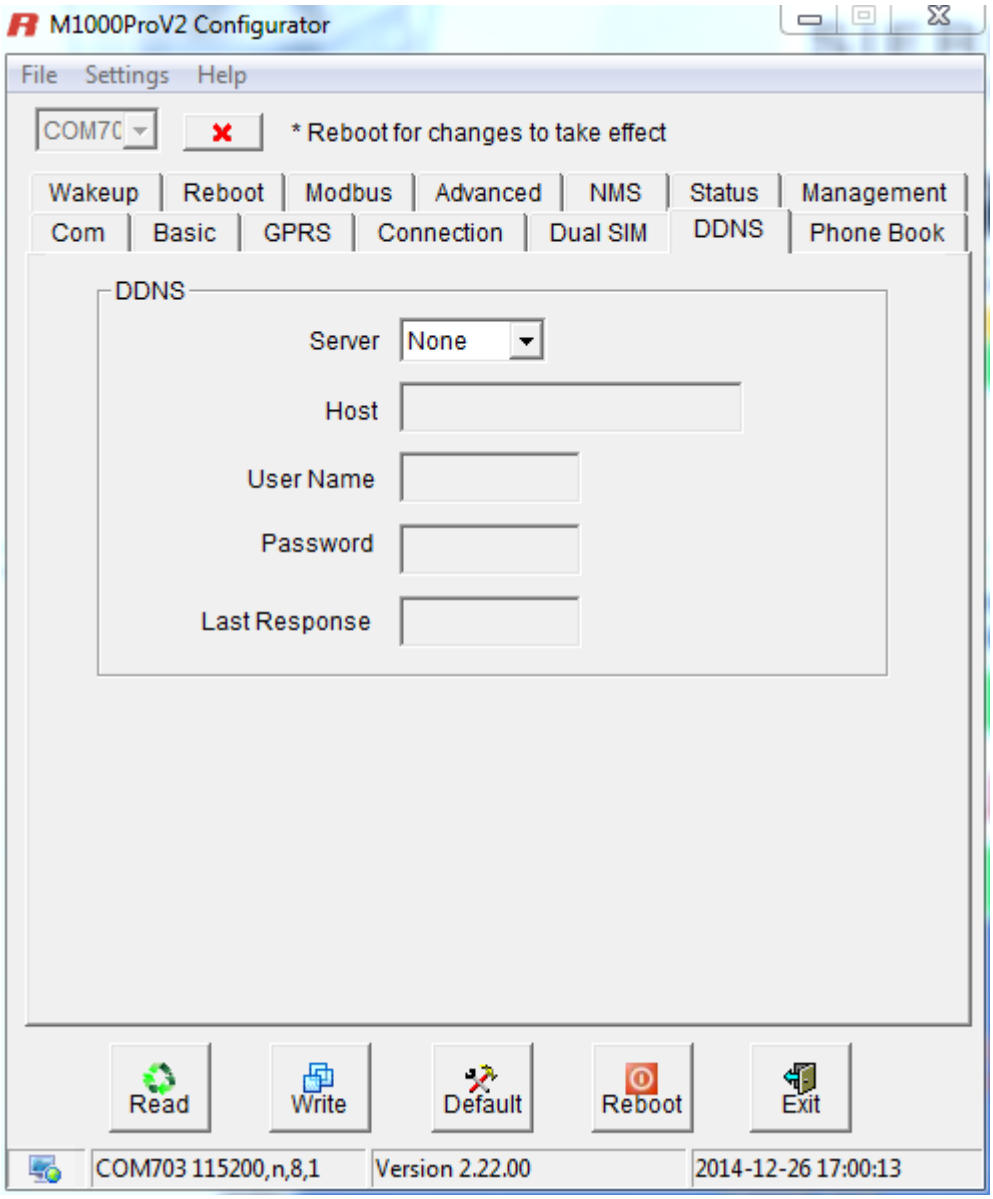


Dual SIM		
Item	Description	Default
Preferred SIM	Set the preferred SIM card from SIM 1 or SIM 2.	SIM 1
SIM Revert Back	Set revert back policies when the gateway work with 2 SIM cards. Auto Failover: Gateway will revert back to another SIM card when dial up fail or according to the failover policy you select. Try Preferred: Gateway will try to revert back to preferred SIM card when the GPRS/ UMTS connectivity is in idle state. ***Note**: the idle state of GPRS/* UMTS *connectivity is depending on the inactivity time you set in Connection -> Connection Control -> Inactivity Time.*	Auto Failover
SIM After Reboot	Select from "Last Used" and "Preferred". Last Used: Gateway will select the last used SIM card after reboot.	Last Used

	Preferred: Gateway will select the "Preferred SIM" after reboot.	
Failover Policies	Set the failover policies to switch to another SIM card: Ping timeout continuously: If gateway ping the preset address timeout continuously for Max Retries time, it will switch to the other SIM card. *Note: User can preset the address/Interval/Max Retries time in Dual SIM -> Ping Control (ICMP).* Monthly data traffic limitation: If the SIM card that the gateway worked with currently has reached the preset data traffic limitation, it will switch to the other SIM card. Switch to backup SIM when preferred SIM is roaming: Gateway will Switch to the other SIM card when preferred SIM card is roaming. GPRS got null DNS: In some countries, normal SIM card will not get DNS when it run out of GPRS traffic or need to be charge. This feature will allow M1000 Pro V2 switch to another SIM card when SIM card get null DNS. ***Note**: Sometimes VPDN SIM card do not get DNS (it depends on local network in different countries), but can connect to Internet normally. So when using VPDN SIM card, don't click to enable "GPRS got null DNS". Or M1000 Pro V2 will keep switching SIM card and will not get it online.*	null
Home Location Area Identifier	The identifier for gateway to check if it is in home location area or in roaming area, and decide if it needed to switch back to preferred SIM card.	null
Data Traffic Setting	SIM limitation: Set the monthly data traffic limitation. Already Use: Current used data traffic amount.	0
Address @ Ping Control (ICMP)	Gateway will ping this address to check that if the current connectivity is active.	null
Interval	Set the ping interval time.	120
Max Retries @ Ping Control (ICMP)	If gateway ping the preset address timeout continuously for Max Retries time, it will try to re-connect to GPRS/UMTS network or will switch to the other SIM card if *Ping timeout continuously* in *Failover Policies* is enabled. Ranges from 0 to 10. 0 stands for gateway only try to keep pinging the address continuously and will do nothing else even timeout every time. It used to keep the connection always activity to avoid ISP shut down the PPP link in a certain idle time.	0

3.2.10 DDNS

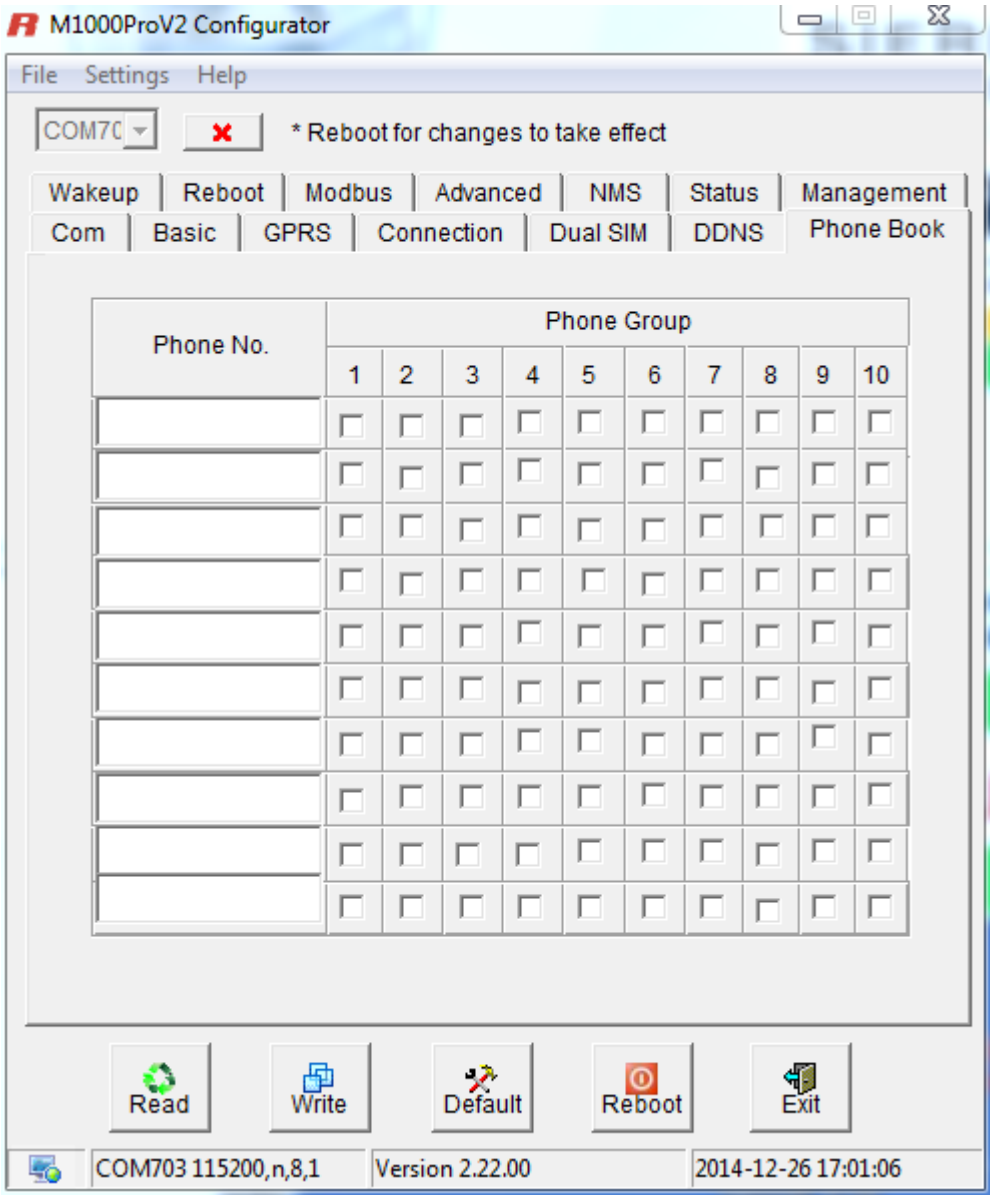
This tab allows user to set the DDNS server and other related parameters.



DDNS		
Item	Description	Default
Server	Selected from *None, dyndns, 3322* and *No-IP.* *None:* Disable DDNS function. *dyndns, 3322* and *No-IP:* Corresponding to three DDNS service providers.	None
Host	Enter the Host name the DDNS server provided.	null
User Name	Enter the user name the DDNS server provided.	null
Password	Enter password the DDNS server provided.	null
Last Response	Show the last response from the DDNS server.	null

3.2.11 Phone Book

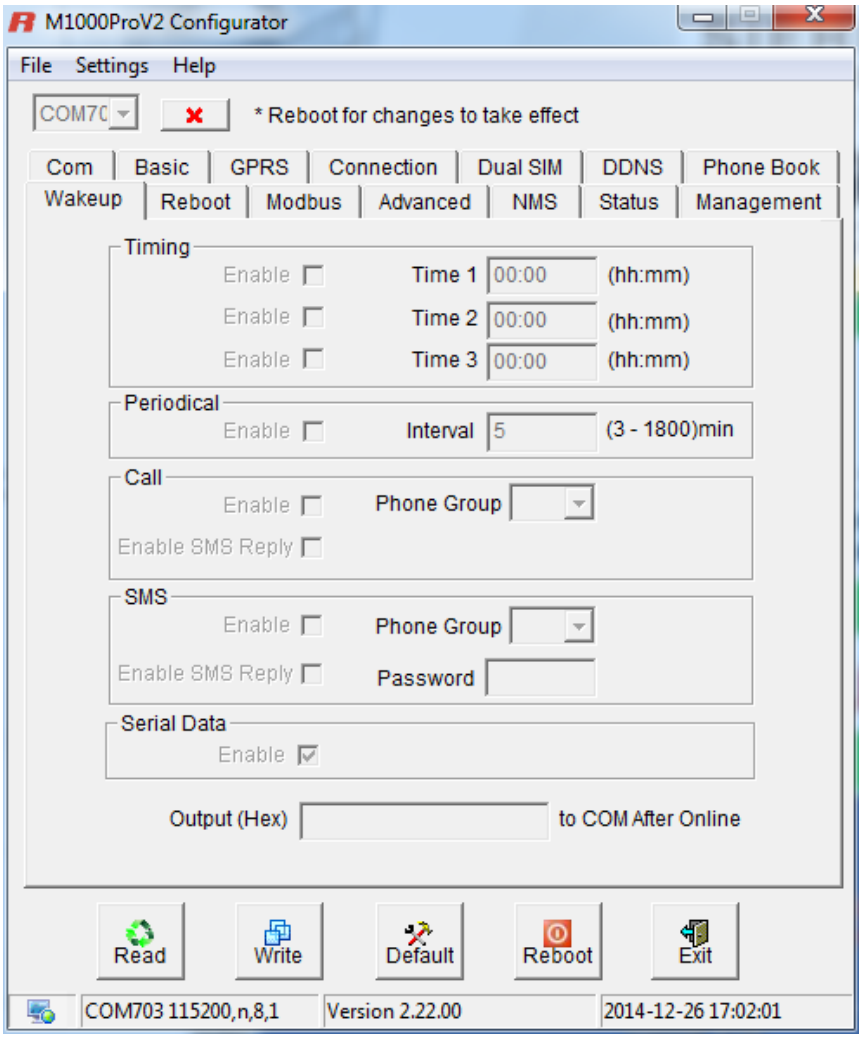
This tab allows user to set the phone numbers and which phone group they are belonged to.



Phone Book		
Item	Description	Default
Phone NO.	Input the telephone number.	Null
Phone Group	Select different phone numbers to include them in the same phone group.	Null
***Note**: The **Phone NO.** is required to be written in international format, starting with "+" followed by the country code.*		

3.2.12 Wakeup

M1000 Pro V2 supports various dial-up policies, wakeup at preset time, wakeup periodically, wakeup by Call, wakeup by SMS, wakeup by local serial port data. In this page, user can set up different wakeup policies.



Wakeup ***Note: This function is available under "Normal Mode".***		
Item	Description	Default
Time	Tick *Enable* to allow gateway automatically connects to GPRS/UMTS with preset time schedule every day, support maximum 3 time schedule/day (e.g. 07:00, 11:00 and 23:30 every day).	Disable
Periodical	Tick *Enable* to allow gateway automatically connects to GPRS/UMTS with preset interval, select from 1 to 1800 minutes. The interval is defined as time interval between two GPRS/UMTS connections.	Disable
Call	Tick *Enable* to allow gateway automatically connects to GPRS/UMTS with incoming call from specified *Caller ID* (phone number).	Disable
Phone Group @ Call	Set the Phone Group which was allowed to wake up the gateway by call.	1

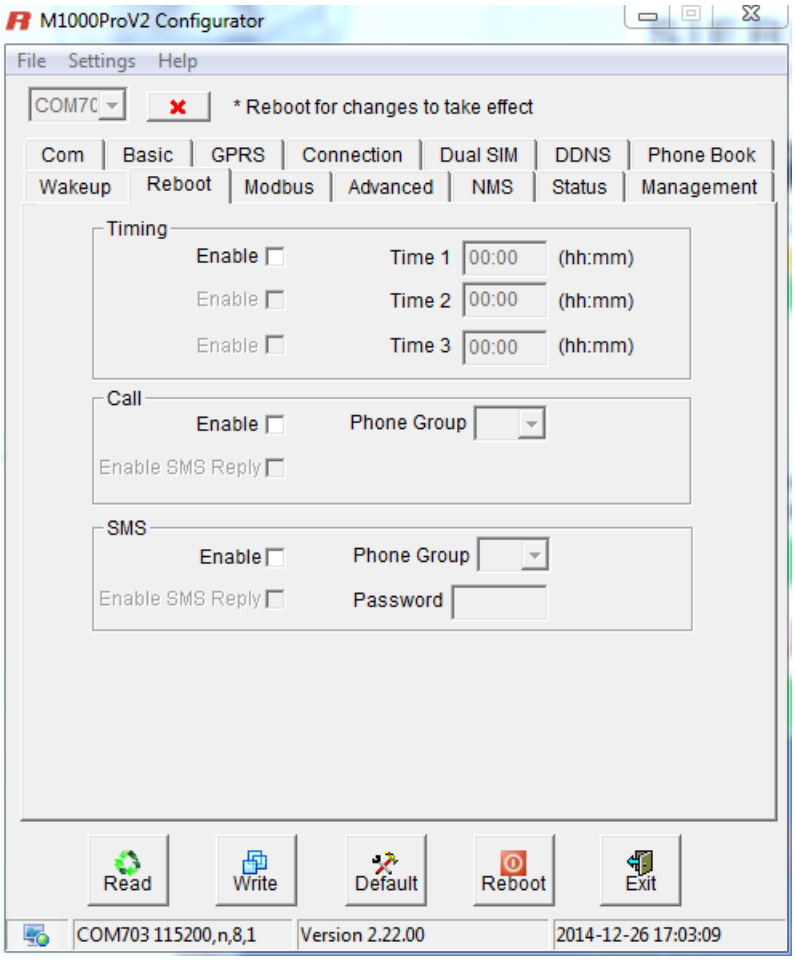
Enable SMS Reply @ Call	Tick *Enable* to allow gateway send reply short message after automatically connects to GPRS/UMTS by Call Wakeup from specified *Caller ID* (e.g. GPRS on ok!). ***Note**: Only support text format SMS.*	Disable
SMS	Tick the *SMS* checkbox to allow gateway automatic connects to GPRS/UMTS with incoming specified short message from specified *Caller ID* (phone number). Specified short message is set at *Password* item. (e.g. GPRS on)	Disable
Phone Group @ SMS	Set the Phone Group which was allowed to wake up the gateway by SMS.	1
Password	The specified short message which was used to wake up the gateway	Null
Enable SMS Reply@ SMS	Tick *Enable SMS Reply* to allow gateway to send reply short message after automatic connects to GPRS/UMTS by SMS Wakeup from specified *Caller ID* (e.g. GPRS on ok!). ***Note**: Only support text format SMS.*	Disable
Serial Data	Tick *Enable* to allow gateway automatic connects to GPRS/UMTS from idle mode when there is data (any data) come out from serial port. After gateway has connected to GPRS/UMTS and established TCP connection, the "triggered" data will be sent to destination site.	Enable
Output (Hex) to COM after online	No matter the gateway is set into "Always Online" mode or "Connect On Demand" mode gateway will output a massage with this configured string format data to gateway serial port when it has been triggered to establish PPP connection (dial up). Maximum 30 bytes. ***Note**: Note: If need to output a hex format massage, user need to add "\x" in front of the massage.*	Disable

***Note**:*

1. *Time format for Time reboot is 24-hours.*
2. *The phone numbers for **Call** and **SMS** function can be set in Phone Book tab.*
3. *The **Caller ID** is required to be written in international format, starting with "**+**" followed by the country code.*

3.2.13 Reboot

Since cellular network is not as stable as fixed line, M1000 Pro V2 supports various auto reboot function to keep gateway working 24x7 without hang up.

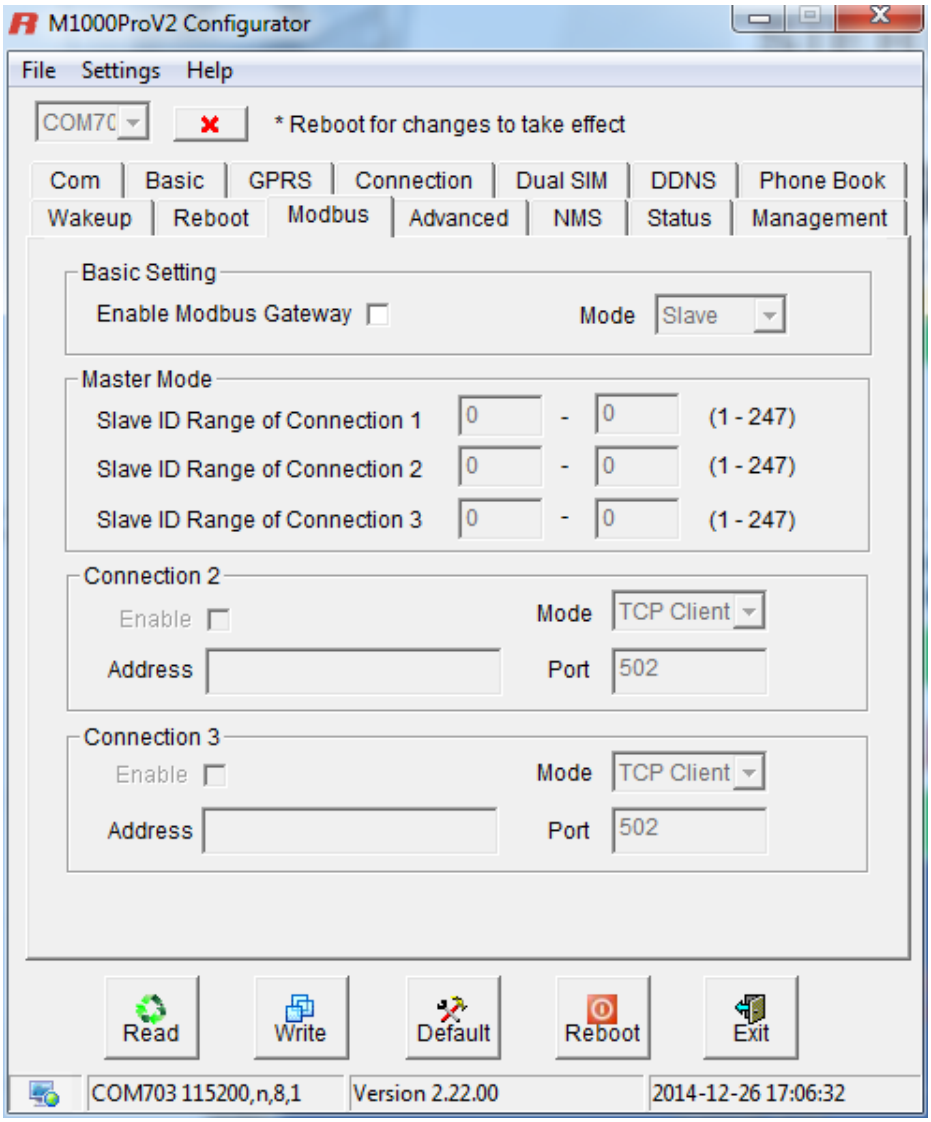


Reboot		
Item	Description	Default
Timing	Tick *Enable* to allow gateway auto reboot with preset time schedule every day, support maximum 3 time schedule/day (e.g. 07:00, 11:00 and 23:30 every day).	Disable
Call	Tick *Enable* to allow gateway auto reboot with incoming call from specified *Caller ID* (phone number). The *Caller ID* (phone number) should be specified in *Phone Book* tab by inputting the phone number and tick *Call Reboot* checkbox.	Disable
Phone Group @ Call	Set the Phone Group which was allowed to reboot the gateway by call.	1
Enable SMS Reply @ Call	Tick the *Enable SMS Reply* checkbox to allow gateway send reply short message after auto reboot by Call Reboot from specified *Caller ID*.	Disable
SMS	Tick *Enable* to allow gateway auto reboot with incoming specified	Disable

	short message from specified *Caller ID* (phone number). Specified short message is set at *Password* item. (e.g. reboot)	
Phone Group @ SMS	Set the Phone Group which was allowed to reboot the gateway by SMS.	1
Enable SMS Reply @ SMS	Tick the *Enable SMS Reply* checkbox to allow gateway send reply short message after auto reboot by SMS Reboot from specified *Caller ID* .	Disable
Password	The specified short message which was used to reboot the gateway	null
***Note**:* *1. Time format for Time reboot is 24-hours.* *2. The phone numbers for **Call** and **SMS** function can be set in Phone Book tab.* *3. The **Caller ID** is required to be written in international format, starting with "**+**" followed by the country code.*		

3.2.14 Modbus

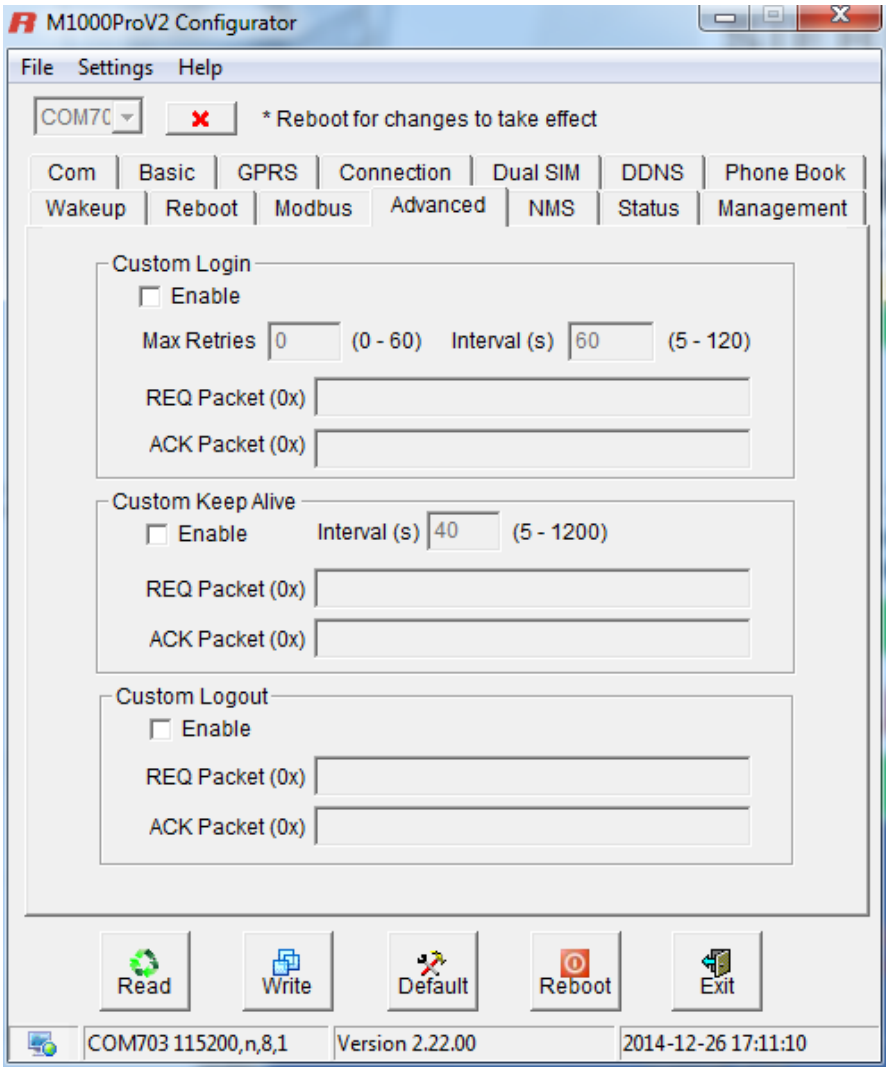
This tab allows user to set the related parameters of Modbus RTU to Modbus TCP gateway.



Modbus		
Item	Description	Default
Enable Modbus Gateway	Tick this checkbox to enable Modbus RTU to Modbus TCP and vice versa.	Disable
Mode	Selected from "Slave" and "Master". Slave: Selected when gateway connect to Modbus slave device with serial COM port. Master: Selected when gateway connect to Modbus Master device with serial COM port. ***Note**: Generally, If you select Slave mode, gateway need to work under TCP server mode, and If you select Master mode, gateway need to work under TCP client mode.*	Slave
Slave ID Range of Connection 1 @ Master Mode	Available when enable Modbus Gateway and select Master mode. This item is corresponding to the default TCP connection which can be set in *Connection* tab. Enter the remote Modbus slave IDs here.	0-0
Slave ID Range of Connection 2 @ Master Mode	Available when enable Modbus Gateway, select Master mode and enable Connection 2. Enter the remote Modbus slave IDs here which is corresponding to "Connection 2".	0-0
Slave ID Range of Connection 3 @ Master Mode	Available when enable Modbus Gateway, select Master mode and enable Connection 3. Enter the remote Modbus slave IDs here which is corresponding to "Connection 3".	0-0
Connection 2	Tick this checkbox to enable the second TCP connection to the remote TCP server. This TCP connection is usually used to connect to the second Modbus slave gateway. User need to enter the TCP server's IP and port here. Serial data come from Master device to M1000 Pro V2 will be sent to different TCP server's IP address according to the Slave ID.	Disable
Connection 3	Tick this checkbox to enable the third TCP connection to the remote TCP server. This TCP connection is usually used to connect to the third Modbus slave gateway. User need to enter the TCP server's IP and port here. Serial data come from Master device to M1000 Pro V2 will be sent to different TCP server's IP address according to the Slave ID.	Disable
***Note**: Connection 2 and Connection 3 only can work under TCP client mode, cannot be configured.*		

3.2.15 Advanced

This tab allows user to set advanced settings after TCP connection is established. Whether need to set this tab is depend on user's application requirement.

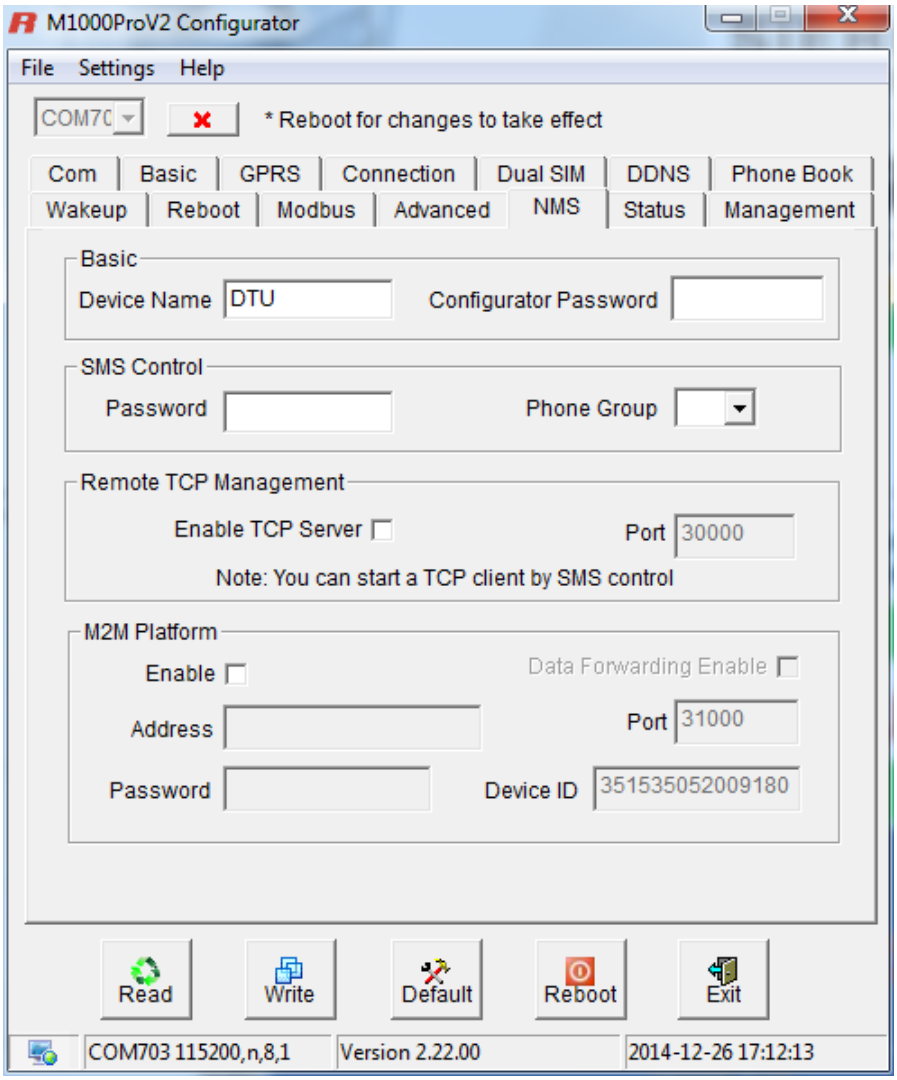


Advanced		
Item	Description	Default
Custom Login	Tick to enable. Some TCP servers required Login Request Packet with follow flow: A TCP connection begins with the client opening a TCP/IP socket to the server and sending a Login Request Packet. If the login request is valid, the server responds with a Login Acknowledge Packet and begins sending Sequenced Data Packets. The connection continues until the TCP/IP socket is broken. Login Acknowledge Packet is optional.	Disable
Max Retries	Login Request Packet The maximum retries times for sending Login Request Packet to the server with preset time interval, selecting from 0 to 60.	0

	After maximum retries, gateway will not retry again, and image login successfully.	
Interval	Time interval between two retries, selecting from 5 to 120 seconds.	60 seconds
REQ Packet	Login Request Packet, written in Hex format, maximum 64 bytes.	Null
ACK Packet	Login Acknowledge Packet, written in Hex format, maximum 32 bytes. Login Acknowledge Packet is optional.	Null
Custom Keep Alive	When using GPRS/UMTS with a session running most ISPs will monitor the traffic flow, if there is none for a predetermined period of time then it will shut the connection down at either the DHCP server or the APN, this is performed so that system resources are not taken up unnecessarily. To stop this happening you will need to send periodic Keep Alive bytes to *keep the gateway always online*.	Disable
Interval	Time interval between two Keep Alive packets, selecting from 5 to 1200 seconds.	40 seconds
REQ Packet	Keep Alive Request Packet, written in Hex format, maximum 64 bytes.	Null
ACK Packet	Keep Alive Acknowledge Packet, written in Hex format, maximum 32 bytes. Keep Alive Acknowledge Packet is optional.	Null
Custom Logout	Tick to enable. Some TCP servers required Logout Request Packet with follow flow: A TCP connection ends with the client sending a Logout Request Packet. If the logout request is valid, the server responds with a Logout Acknowledge Packet and ends the connection. Logout Acknowledge Packet is optional.	Disable
REQ Packet	Logout Request Packet, written in Hex format, maximum 64 bytes.	Null
ACK Packet	Logout Acknowledge Packet, written in Hex format, maximum 32 bytes. Logout Acknowledge Packet is optional.	Null

3.2.16 NMS

This tab allows user to set the related parameters of TCP Network Management.

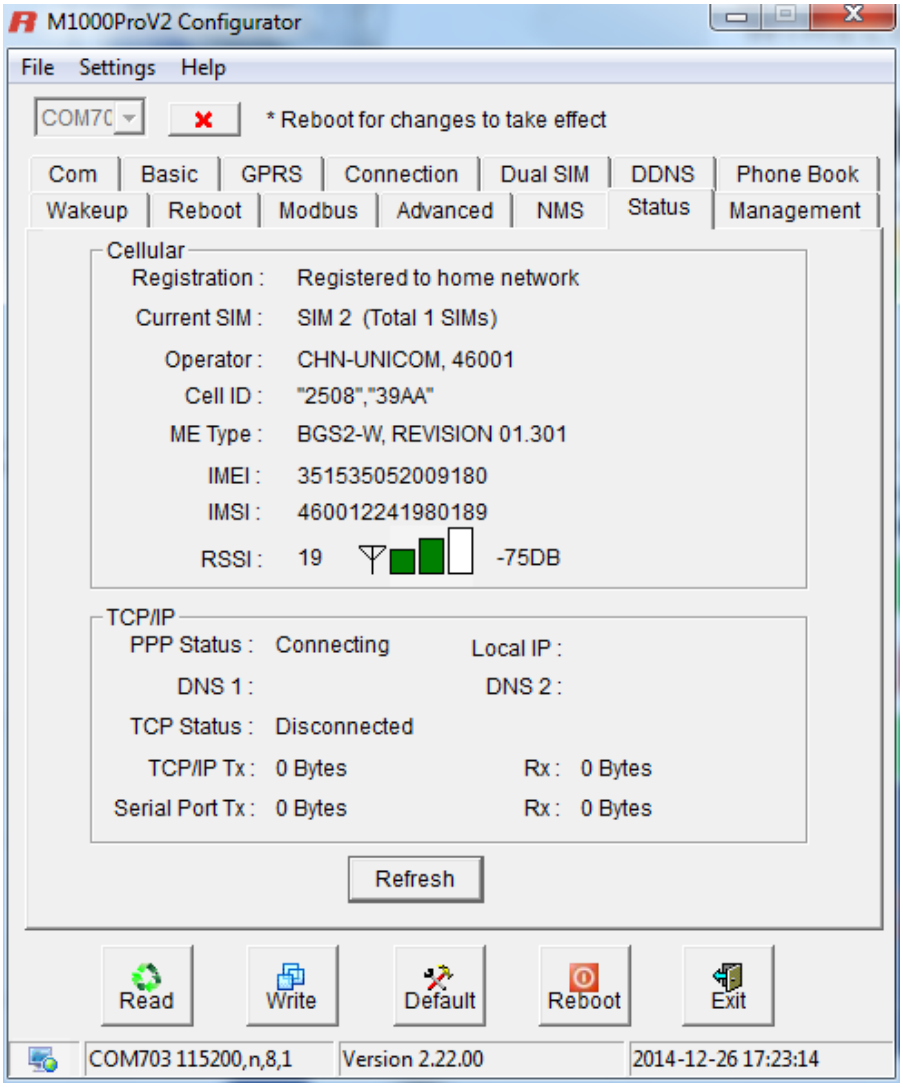


NMS		
Item	Description	Default
Device Name	Write down the description name of the gateway, such as write down the gateway installation site name in order to identify each gateway.	DTU
Configurator Password	Set password for the Configurator. When run M1000 Pro V2 Configurator you need to enter this password.	
Password @ SMS Control	Set password for SMS control, including remote configuration and remote reading gateway status. The password can be left as null, maximum 20 ASCII characters.	null
Phone Group @ SMS Control	Set the Phone group which is permitted to SMS control this gateway.	1
Enable TCP Server @	Tick this checkbox to enable Remote TCP Management.	Disable

Remote TCP Management	Normally, gateway works under TCP server mode for NMS function, but it also can work under TCP client mode (start by SMS control). Please refer to ***3.2.2 Management via TCP connection*** to get the detail information.	
Port @ Remote TCP Management	Set the listening port of TCP server for NMS function.	30000
Enable @ M2M Platform	When click to enable this checkbox, gateway will works as TCP Client site and be managed via RobustLink (Robustel centralized management and administration system).	Disable
Data Forwarding Enable @ M2M Platform	When enable this feature, all serial data from gateway will be forwarded to M2M Platform, will not forward to address that configured in “Connection” -> “Socket Application”. At the same time, “Connection” -> “Socket Application” can’t be configured. When disable this feature, all serial data from gateway will not be forwarded to M2M Platform, will forward to address that configured in “”Connection” -> “Socket Application”. M2M Platform just acts as a remote management platform this time.	Disable
Address @ M2M Platform	Enter IP address or domain of M2M Platform.	Null
Port @ M2M Platform	Enter the port number of M2M Platform.	Null
Password @ M2M Platform	Enter password in this item, which shall be the same as the password set in M2M Platform.	Null
Device ID @ M2M Platform	This item let you know the default single ID of M1000 Pro V2, can’t be configured.	N/A

3.2.17 Status

This tab allows user to check the running status of M1000 Pro V2.

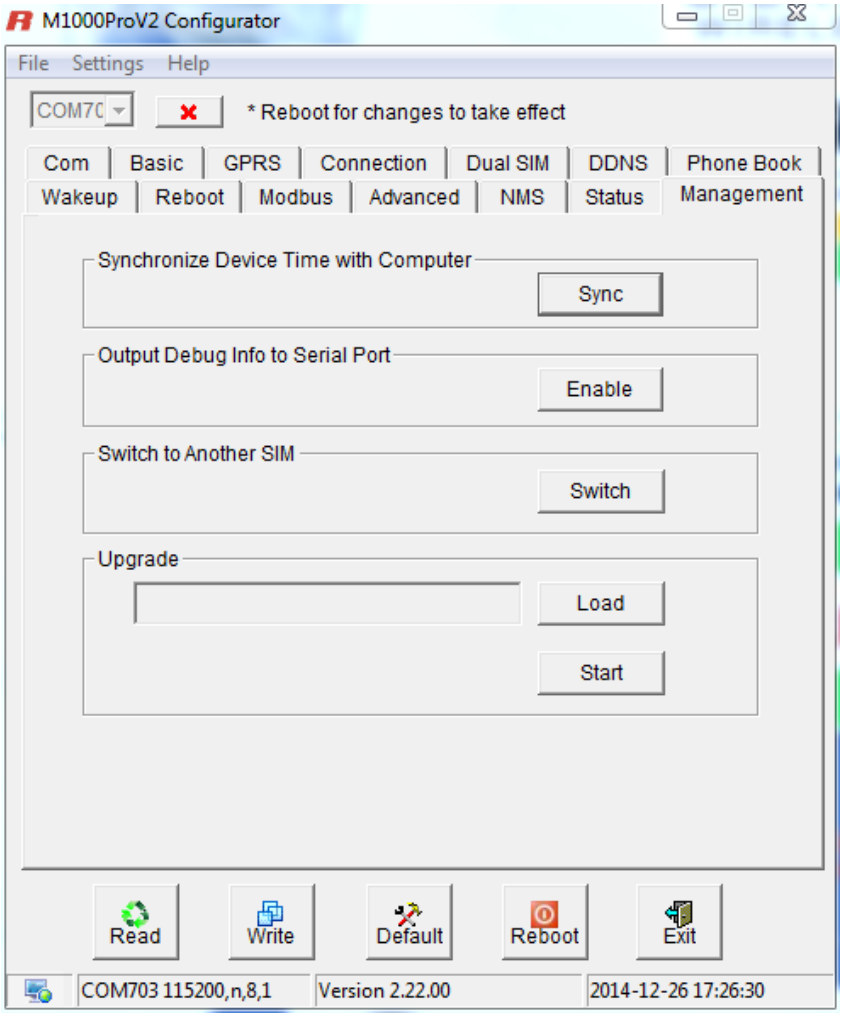


Cellular @ Status		
Item	Description	Default
Registration	Show the gateway's current registration status. There are 6 status: 1. Not registered. 2. Registered to home network. 3. Searching new operator. 4. Registration denied. 5. Registered, roaming. 6. Unknown	N/A
Current SIM	Show the SIM card which the gateway works with currently: SIM1 or SIM2. It will also show how many SIM cards you have inserted.	N/A
Operator	Show the gateway's current registered operator name.	N/A

Cell ID	Show the gateway's current register base station cell ID.	N/A
ME Type	Show the gateway's current module information.	N/A
IMEI	Show the gateway's current IMEI number.	N/A
IMSI	Show the gateway's current IMSI number.	N/A
RSSI	Show the gateway's current RSSI from 0 to 31 and corresponding DB.	N/A
TCP/IP @ Status		
PPP Status	Show the gateway's current PPP status. There are 4 status: 1. Unknown. 2. Down. 3. Error. 4. Up.	N/A
Local IP	After connecting to GPRS, the gateway will be auto assigned one IP by ISP.	Null
DNS 1	Show the gateway's current primary DNS server.	Null
DNS 2	Show the gateway's current secondary DNS server.	Null
TCP Status	Show the gateway's current PPP status. There are 2 status: 1. Disconnected. 2. Connected	Null
Tx / Rx @ TCP/IP	Show how many bytes have been sent / Received via TCP.	Null
Tx / Rx @ Serial Port	Show how many bytes have been sent / Received via serial port.	Null
***Note**:* *1. Click "Refresh" to refresh the "**Cellular**" and "**TCP/IP**" status.*		

3.2.18 Management

This tab provides some system tools for user.



Management		
Item	Description	Default
Synchronize Device Time with Computer	Synchronize gateway's RTC to PC's clock. The gateway's current RTC will be showed at bottom right side of the configurator.	Null
Output Debug info to Serial Port	Enable to output the gateway's debug info to serial port. Then you can use a hyper terminal to receive the debug info. This function is often used when we need to diagnose the problem of the gateway. **Note:** *This function will take effect immediately after you enable it.*	Disable
Switch to Another SIM	Switch to another SIM card manually.	Null
Upgrade	Upgrade the firmware of gateway via serial port or TCP connection. The upgrade steps are as bellow:	Null

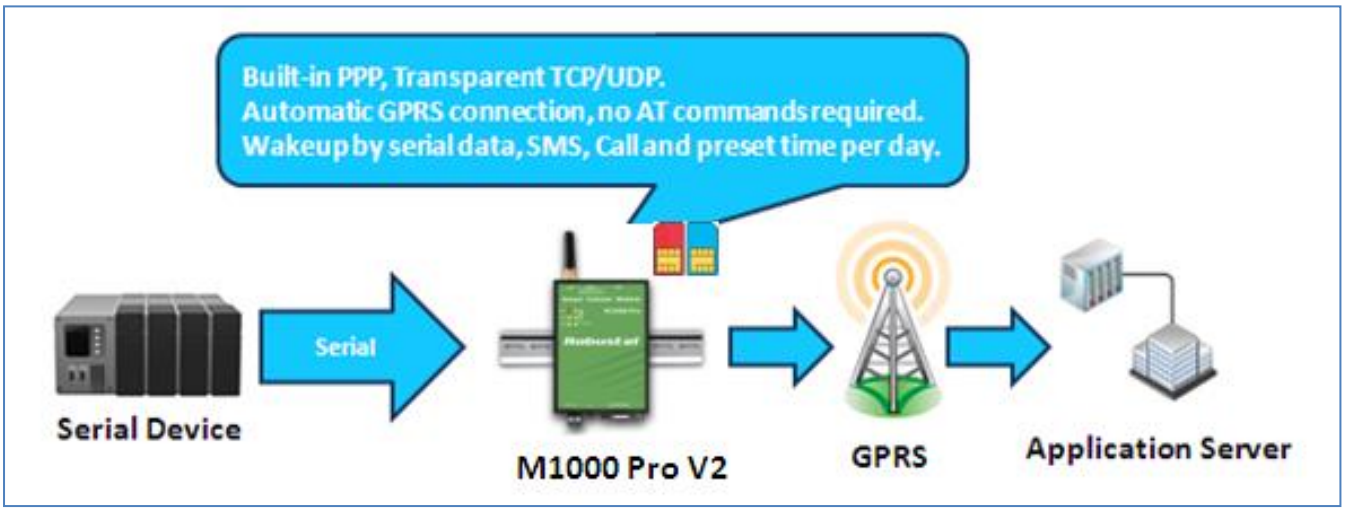
	1. Click *"load"* button and select the FW file in your computer; 2. Click *"Start"* button to get started, then you can see a process bar; 3. The updating will last for several minutes, after that you will see a pop window to indicate the updating is successful.	

Chapter 4 Typical Applications

4.1 Overview

Cellular data transmission is an increasingly attractive mechanism for communication with remote, non-permanent or mobile devices. Being able to collect and distribute data virtually anywhere without requiring the limitation of working within specific fixed line networks is a powerful force for efficiency and reliability. However, the fact that cellular data is metered means that the frequency of transmission and amount of data sent in each exchange can have significant cost and performance impact.

In order to understand this impact, let us start with a fairly typical example, where there is a device in the field and an application on a server at a central site location that collects information from that device.



In general, the purpose of communication with the device will be for one of two reasons:

• Monitoring - Status monitoring data, such as the level or temperature of a storage tank, the velocity and pressure of a pipeline, the condition of a controller or the status of a register.

• Transaction data – Discrete event data, such as cash or credit transactions, PBX call records or mission-critical and safety related alarms.

Status monitoring data is often “polled.” The application sends out periodic queries and gets responses to those queries. The application can usually retry if it does not get an answer, and determine that a problem exists if it does not get a response after a certain amount of retries.

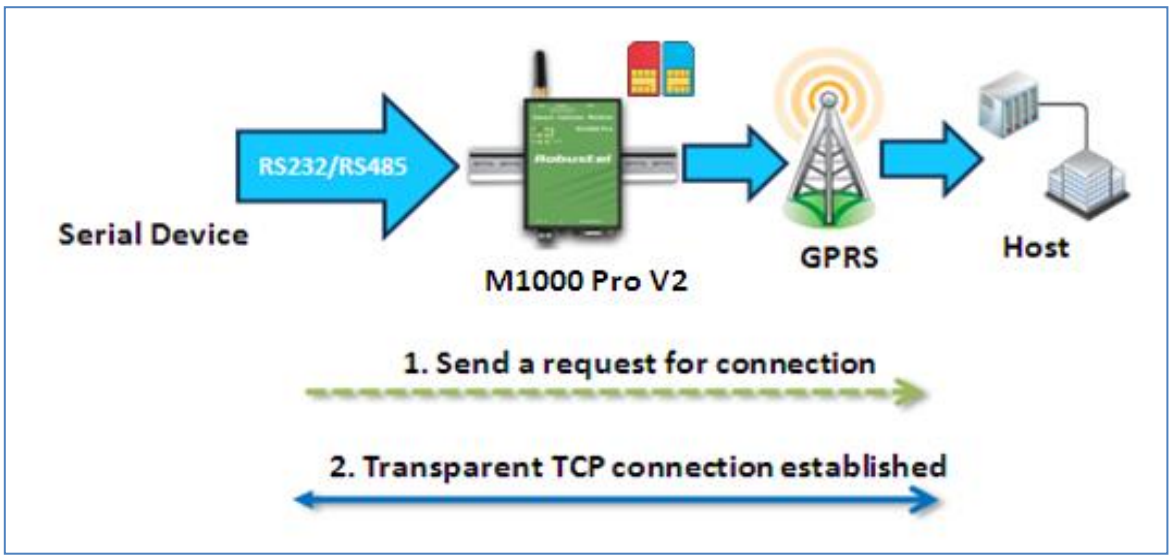
Discrete event data is usually “unsolicited.” The application does not expect to get information on any regular basis, and therefore the failure to hear from the device is the normal case (though some sort of “all is well” message may be sent at a longer interval).

Most applications will likely involve one or both of these methods and data is transmitted in TCP or UDP packets.

4.2 Typical Applications

4.2.1 TCP Client Mode

In TCP Client mode, the gateway can actively establish a TCP connection to a pre-defined host computer when serial data arrives. After the data has been transferred, the gateway can automatically disconnect from the TCP server by using the Inactivity time settings.
As illustrated in the figure below, data transmission proceeds as follows:
(1) The gateway, configured as TCP Client mode, requests a connection to the host.
(2) Once the connection is established, data can be transmitted in both directions between the host and the gateway bidirectional.

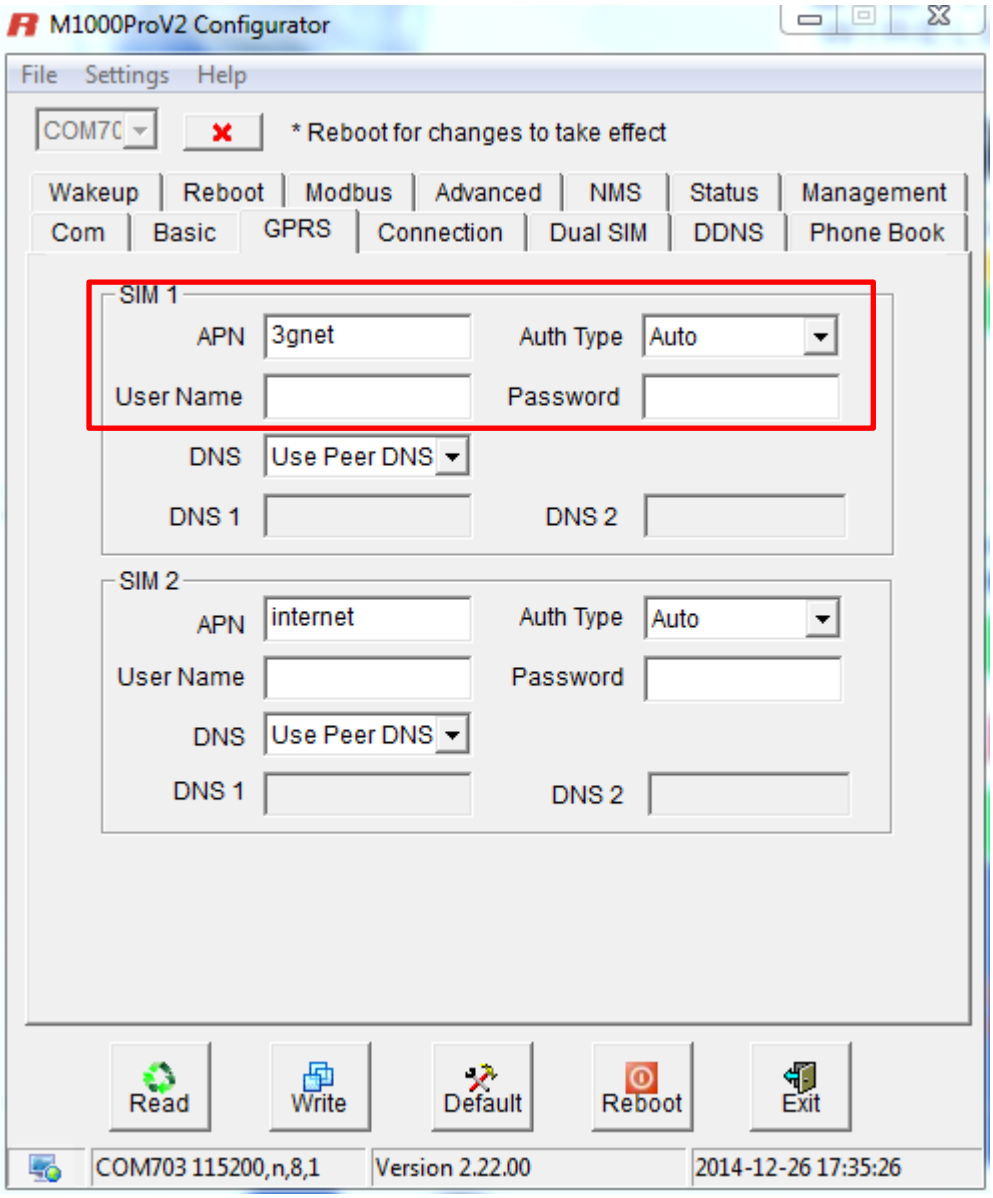


Types of TCP Client Connection:

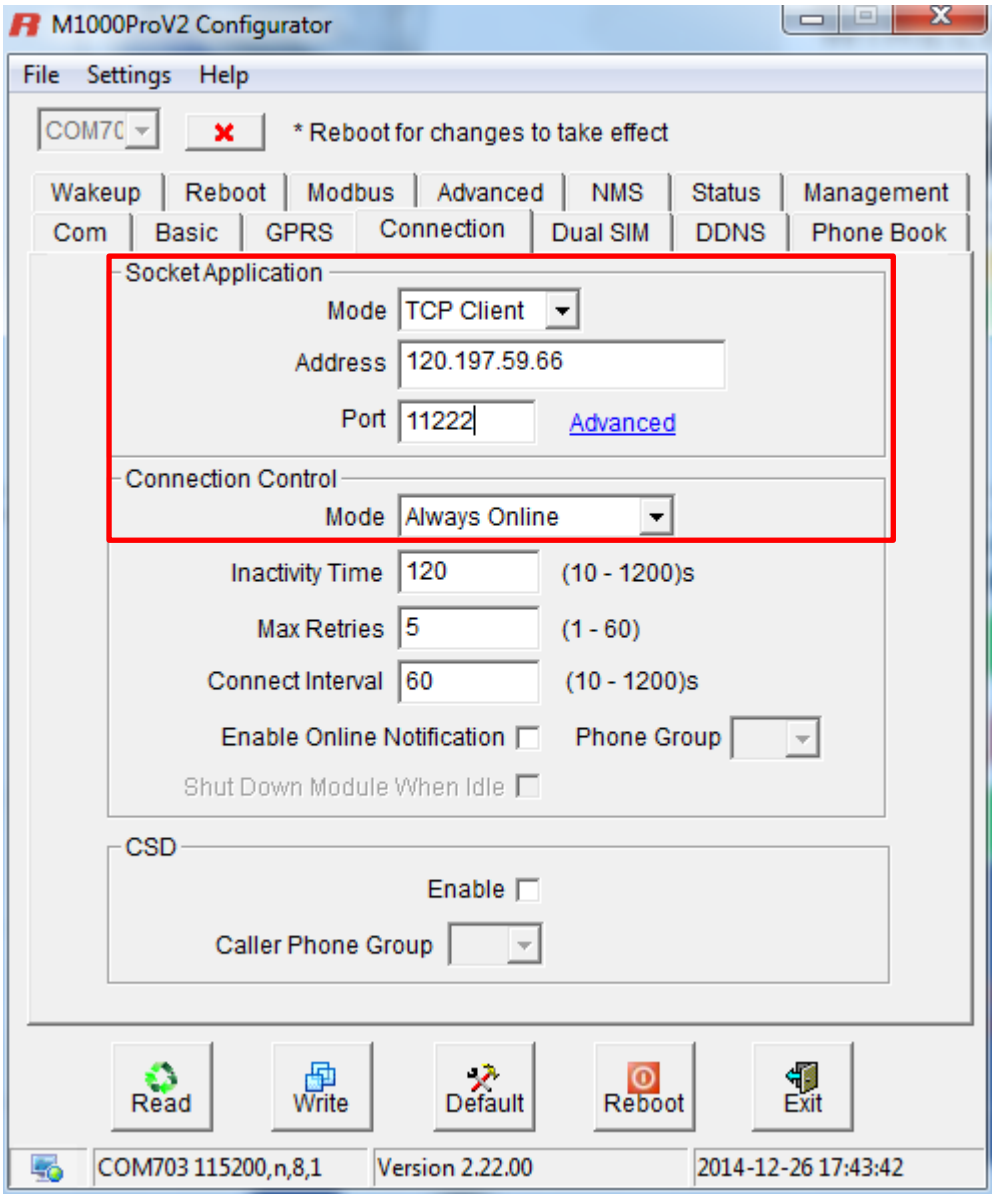
1. Fixed Public IP (or dynamic public IP with domain name) for the host PC
   The gateway will only be able to connect to a host PC if the PC is using a fixed public IP address (or dynamic public IP with domain name), gateway can be any IP (either a private IP or public IP).
2. Connecting TCP client and TCP server within the same cellular service provider.
   In order to connect properly, the IP addresses of the two gateways must belong to the same sub network. To ensure that this is the case, use the same cellular ISP to connect the devices to the network. In addition, you will need to request that the cellular ISP provide you with two private fixed IP addresses (e.g., 192.168.1.1 and 192.168.1.2).

Configuration and Operation:

1. Turn the gateway to Config mode and connect it to your PC properly.
2. Open the M1000 Pro V2 Configurator.
3. Turn to *GPRS* tap. Set APN, Username and Password of SIM 1. If you need to use SIM 2, you also need to set these parameters of SIM 2. Then click *"Write"*.



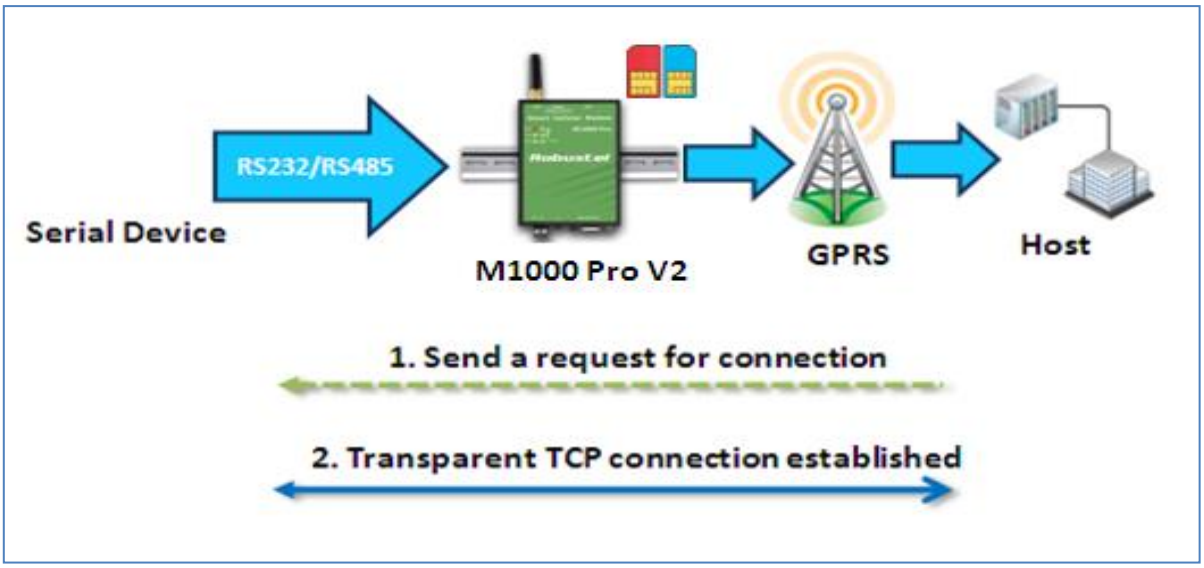
4. Turn to *Connection* tap. Select Socket Application Mode as *TCP Client*. Input remote TCP server's address and port. Select Connection Control Mode as *Always Online* or *Connect On Demand*. Then click *"Write"*.



5. Turn the gateway back to Normal mode and reboot it.

4.2.2 TCP Server Mode

In TCP Server mode, the serial port on the gateway is assigned a port number. The host computer initiates contact with the gateway, establishes the connection, and receives data from the serial device.
As illustrated in the figure, data transmission proceeds as follows: The host requests a connection from the gateway, which is configured for TCP Server mode. Once the connection is established, data can be transmitted between the host and the gateway bidirectional.

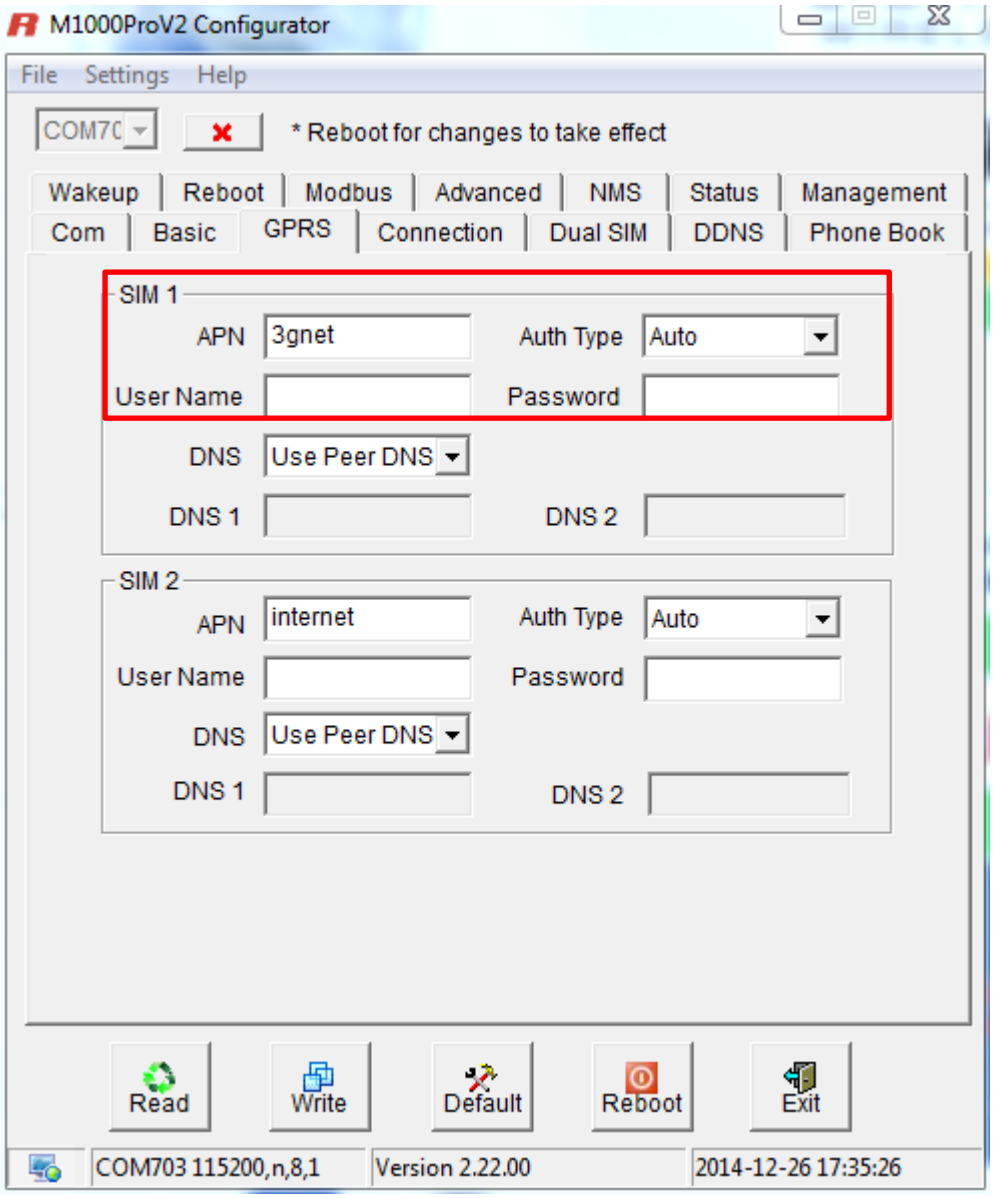


Types of TCP Server Connection:

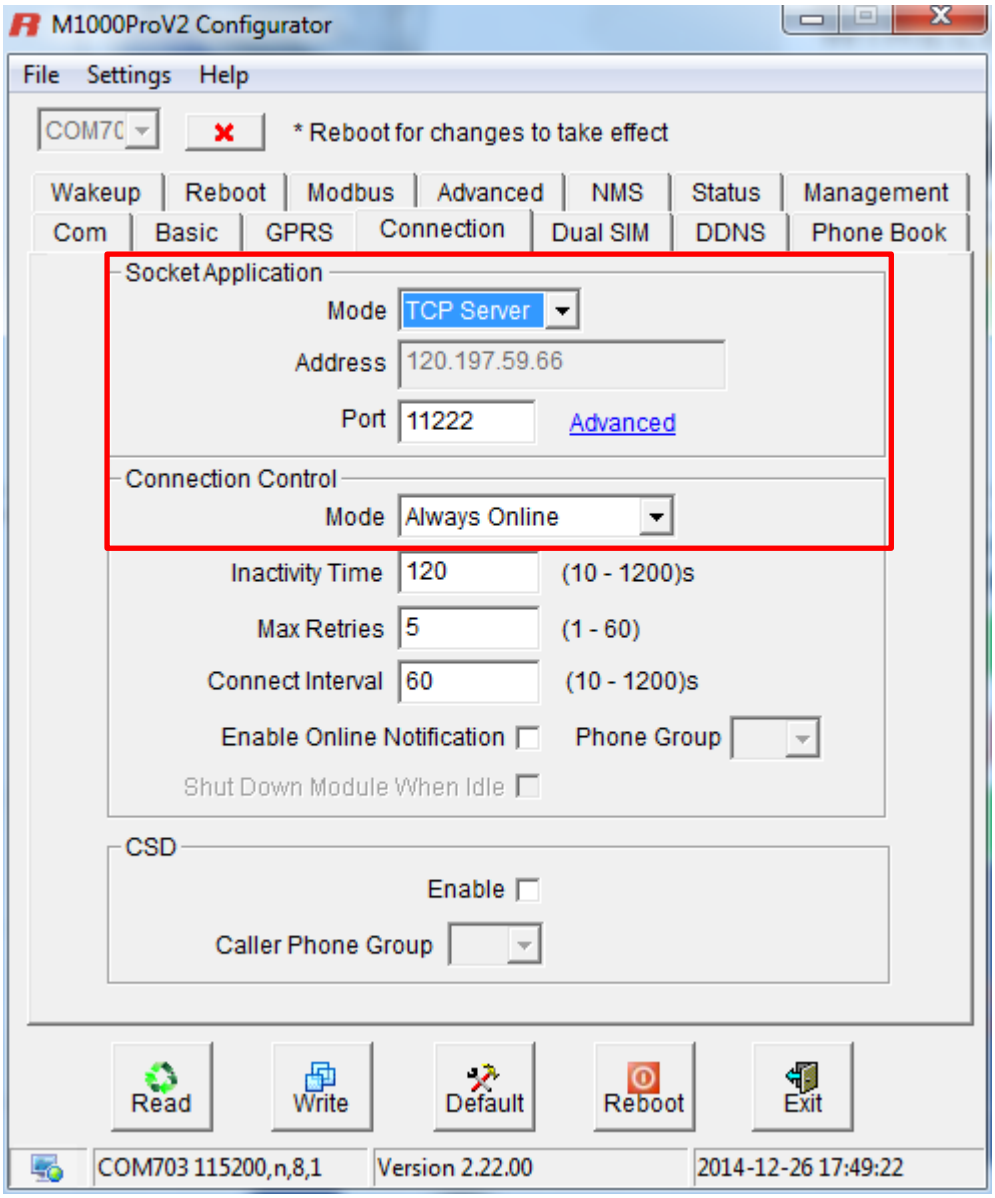
1. Fixed Public IP for the gateway.
   If your cellular service provider offers a fixed public IP address after you connect to the cellular network, you can access the gateway from a host PC using either a private IP or public IP.
2. Dynamic public IP with domain name for the gateway.
   If your cellular service provider offers a dynamic public IP address after you connect to the cellular network, you can use the DDNS function to get a domain name from the domain name server for the gateway. Then you can access the gateway from a host PC using this domain name.
3. Connecting TCP client and TCP server within the same cellular service provider.
   In order to connect properly, the IP addresses of the two gateway devices must belong to the same sub network. To ensure that this is the case, use the same cellular ISP to connect the devices to the network. In addition, you will need to request that the cellular ISP provide you with two private fixed IP addresses (e.g., 192.168.1.1 and 192.168.1.2).

Configuration and Operation:

1. Turn the gateway to Config mode and connect it to your PC properly.
2. Open the M1000 Pro V2 Configurator.
3. Turn to *GPRS* tap. Set APN, Username and Password of SIM 1. If you need to use SIM 2, you also need to set these parameters of SIM 2. Then click *"Write"*.



4. Turn to *Connection* tap. Select Socket Application Mode as *TCP Server*. Input local listening port. Select Connection Control Mode as *Always Online* or *Connect On Demand* as your need. Then click *"Write"*.

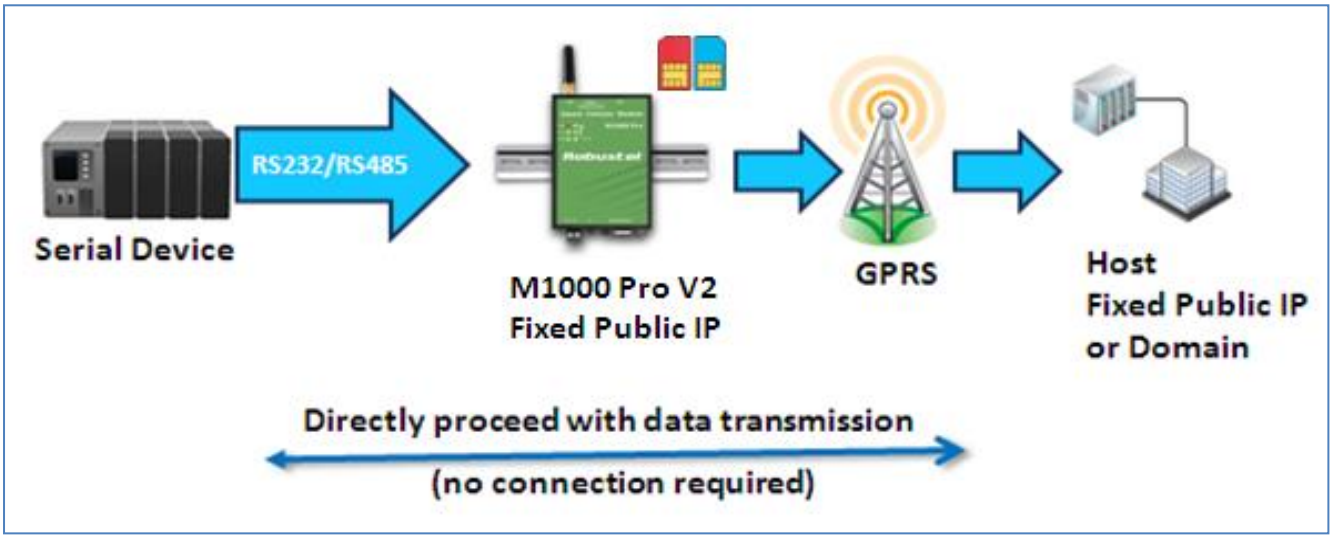


5. Turn the gateway back to Normal mode and reboot it.

4.2.3 UDP Mode

The main difference between the TCP and UDP protocols is that TCP guarantees delivery of data by requiring the recipient to send an acknowledgement to the sender. UDP does not require this type of verification, making it possible to offer faster delivery. UDP also allows you to unicast data to one IP, or multicast the data to a group of IP addresses.

These traits make UDP mode especially well-suited for message display applications.



1. If your cellular ISP offers a fixed public IP address after you connect to the cellular network, you can access the gateway from a host PC that has a fixed public IP bidirectional.
2. If your cellular service provider offers a dynamic public IP address after you connect to the cellular network, you can use the DDNS function to get a domain name from the domain name server for the gateway. Then you can access the gateway from a host PC that has a fixed public IP bidirectional.
3. If gateway has no fixed public IP or domain name, then it can unicast data to one host unidirectional.

***Note**: M1000 Pro V2 supports unicast only.*

4.2.4 Virtual COM Mode

One of the major conveniences of using Virtual COM mode is that it allows you to use Virtual COM software that was written for pure serial communication applications. The Virtual COM driver intercepts data sent to the host's COM port, packs it into a TCP/IP packet, and then redirects it through the host's Ethernet to the Internet. At the other end of the connection, the gateway accepts the IP frame from the cellular network, unpacks the TCP/IP packet, and then transparently sends the data through the serial port to the attached serial device.

We provide application notes to introduce how to work with 3rd parties' popular virtual com software, please contact us to get more information.

***Note**:*

Virtual COM software (COM port redirector) is a specialized software (often including device driver and user application) that includes the underlying network software necessary to access networked device servers that provide remote serial devices or modems.

The purpose of the redirector is to make the virtual COM port exhibit behavior that closely resembles that of a "real" COM port, i.e., a COM port driver for local serial port hardware. A virtual COM port itself is a relatively simple software mechanism that can be implemented by driver software similar to that of a conventional COM port driver. The main challenges arise in two other areas: the network connection to the device server and the behavior of the device server. These issues are described in the Technology section below.

Chapter 5 Appendix

5.1 Factory Settings

Factory setting of the modem COM port under **Config Mode and Normal Mode** is:
Data bits = 8
Parity = none
Stop bits = 1
Baud = 115200 bps
Flow control = none

5.2 SMS Command for Remote Control

5.2.1 SMS Commands Structure

M1000 Pro V2 supports remote configuration and remote modem status reading via SMS.
An SMS command has following structure: **Password: cmd**

- Password: SMS control password is configured at **NMS->SMS Control->Password**, which is an optional parameter.
  When there is a password, SMS command has following structure: **Password: cmd**
  When there is no password, SMS command has following structure: **cmd**
- Cmd1, cmd2, cmd3 to cmdn, which are command identification number 0000 – 9999

5.2.2 SMS Control Steps

1. Use command **Password:cmd** or **cmd** to set new parameters.
2. After setting new parameters for M1000, and then send another SMS: **0004** to save parameters and reset the modem, then the new parameters will take effect.
3. One command in one SMS, if you want to send another command, for example, 0004, you need to send another SMS.

***Note**: E.g., 1234:0101,1*
1234:0004
In this command, password is 1234, 0101 is the cmd to set device's COM type, 1 means M1000 Pro V2 select RS485, then save parameters and reset the modem to take effect with command 0004.
You can find out more SMS configuration examples after the SMS Comands List below.

5.2.3 SMS Commands List

Cmd	Description	Syntax	Comments
Control Commands			
0000	Set Factory Defaults	passwd:cmd or cmd	if no passwd,please use command "cmd", or use command" passwd:cmd" if there is a password. * - means can be null Following commands are the same.
0001	Reset Device	cmd	
0002	Save Parameters	cmd	
0003	Get Device Status	cmd	
0004	Save Parameters and Reset Device	cmd	
0005	Clear Event Count	cmd	
0006	Start Event Counter	cmd	
0007	get Event Count Value	cmd	
0008	switch SIM card	cmd	
0009	Start NMS TCP Client	cmd,addr or domain,port	
Set Commands ("cmd,value" or "cmd,flag" to set new configuration; "cmd" can be used to get configuration)			
M1000_ProV2_ComPort:			
0101	COM type set	cmd,flag	flag:0 - RS232 1 - RS485
0101	COM type get	cmd	
0102	baudrate	cmd,flag	flag: 0 : 1200, 1 : 2400, 2 : 4800, 3 : 9600, 4 : 19200, 5 : 38400, 6 : 57600, 7 : 115200
0103	dataBits	cmd,flag	flag:0 -7, 1 - 8
0104	stopBits	cmd,flag	flag:0 – 1, 1 – 2
0105	parity	cmd,flag	flag:0 – None, 1 – Odd, 2 – Even 3 – Mark, 4 – Space
0106	flowCtrl	cmd,flag	flag:0 – None, 1 – Hardware
0107	packingInterval	cmd,flag	flag:2 – 100, default 5
0108	packingLength	cmd,flag	flag:0 – 5000
0109	enableDelimiter1	cmd,flag	flag:0-disable,1-enable
0110	delimiter1	cmd,value	Value: 0x00 - 0xff (Hex)
0111	enableDelimiter2	cmd,flag	flag:0 - disable,1 – enable
0112	delimiter2	cmd,value	value: 0x00 - 0xff (Hex)
0113	delimiterProcess	cmd,flag	flag:0 – Do Nothing 1 – Strip Delimiter
M1000_ProV2_Gprs:			
0201	authTypeSim1	cmd,flag	flag:0 – None, 1 – Auto 2 – PAP, 3 – CHAP

0233	authTypeSim2	cmd,flag	flag:0 – None, 1 – Auto 2 – PAP, 3 – CHAP
0202	SIM1 APN	cmd,value	value: string, max length 50
0234	SIM2 APN	cmd,value	value: string, max length 50
0203	SIM1 GPRS user name	cmd,value	value: string, max length 32
0235	SIM2 GPRS user name	cmd,value	value: string, max length 32
0204	SIM1 GPRS password	cmd,value	value: string, max length 32
0236	SIM2 GPRS password	cmd,value	value: string, max length 32
0205	specifyDnsSim1	cmd,flag	flag: 0 – Use Peer DNS 1 – Manual
0237	specifyDnsSim2	cmd,flag	flag:0 – Use Peer DNS 1 – Manual
0206	Dns1Sim1	cmd,value	value: string, max length 15
0238	Dns1Sim2	cmd,value	value: string, max length 15
0207	Dns2Sim1	cmd,value	value: string, max length 15
0239	Dns2Sim2	cmd,value	value: string, max length 15
0217	enablePinLockSim1	cmd,flag	flag: 0 - disable,1 - enable
0249	enablePinLockSim2	cmd,flag	flag: 0 - disable,1 - enable
0218	pinCodeSim1	cmd,value	value: string, max length 8
0250	pinCodeSim2	cmd,value	value: string, max length 8
0219	changePinSim1	cmd,flag	flag: 0 - disable,1 - enable
0251	changePinSim2	cmd,flag	flag:0 - disable,1 - enable
0220	newPinCodeSim1	cmd,value	value: string, max length 8
0252	newPinCodeSim2	cmd,value	value: string, max length 8
M1000_ProV2_Connection:			
0301	peerAddr	cmd,value	value: string, max length 64
0302	Socket port	cmd,value	value: range: 1-65535
0303	Socket type	cmd,flag	flag: 0 – UDP 1 – TCP Client 2 – TCP Server
0304	workingType	cmd,flag	flag:0 – Always Online 1 – Connect on Demand
0305	idleTime	cmd, value	value: 10-1200, default:120
0306	connectInterval	cmd, value	value: 10-1200, default:60
0307	connectRetryTimes	cmd,value	value: 1-60, default:5
0308	onlineNotifyEnabe	cmd,flag	flag: 0 - disable,1 - enable
0309	onlineNotify PhoneGroup	cmd,flag	flag: 0-10, 0 means no phone group
0310	shutDownModuleIdle	cmd,flag	flag: 0 - disable,1 - enable
0311	pingEnable	cmd,flag	flag: 0 - disable,1 - enable
0312	pingTarget	cmd,value	value: string, max length 64
0313	pingInterval	cmd,flag	flag: 1-1800, default:120

0314	ping Retry Times	cmd,flag	flag:0-10
0316	csdBackupEnable	cmd,flag	flag:0 - disable,1 - enable
0317	csdBackup PhoneGroup	cmd,flag	flag: 0-10; 0 means no phone group
M1000_ProV2_DualSim_Ddns:			
0401	preferred Sim	cmd,flag	flag: 0 – SIM1, 1 – SIM2
0402	sim Revert Back Type	cmd,flag	flag:0 – Auto Failover 1 – Try Preferred
0403	fail over Policy	cmd,flag	flag: Bit0 represent “Ping timeout continuously”: 1- enable , 0 – disable; Bit 1 represent “Monthly data traffic limitation”: 1 – enable, 0 – disable; Bit 2 represent “Switch to backup SIM when preferred SIM is roamin” 1 – enable, 0 – disable; Bit 3 represent “GPRS got null DNS”: 1 – enable, 0 – disable; *Note: please check example below.*
0404	homeLai	cmd,value	value: string, max length 6
0405	dataLimitSim1	cmd,value	value: 0 - 4294967295
0406	dataLimitSim2	cmd,value	value: 0 - 4294967295
0416	ddnsEnable	cmd,value	value: 0 - disable,1 - enable
0417	ddnsServerType	cmd,flag	flag: 0 – DYNDNS 1 – 3322 2 – NoIP
0418	ddnsDomainName	cmd,value	value: string, max length 64
0419	ddnsUserName	cmd,value	value: string, max length 24
0420	ddnsPassword	cmd,value	value: string, max length 24
M1000_ProV2_Nms:			
0501	deviceName	cmd,value	value: string, max length 20
0502	smsCtrl Password	cmd,value	value: string, max length 20
0503	smsCtrl PhoneGroup	cmd,flag	flag: 0-10; 0 means no phone group
0504	nmsLoginPassword	cmd,value	value: string, max length 16
0505	tcpNmsEnable	cmd,flag	flag: 0 - disable,1 - enable
0506	nmsTcpPort	cmd,value	value: default:30000
0516	m2mPlatformEnable	cmd,flag	flag: 0 - disable,1 - enable
0517	m2mProtocol		(not used)
0518	m2mPlatformAddr	cmd,value	value: string, max length 64
0519	m2mPlatformPort	cmd,value	value: default:31000
0520	m2mDataForward Enable	cmd,flag	flag: 0 - disable,1 - enable
0521	m2mHeartbeatInterval		(not used)
M1000_ProV2_PhoneGroup:			

0601	phoneNumber1	cmd,value	value: string, max length 20
0602	phoneNumber2	cmd,value	value: string, max length 20
0603	phoneNumber3	cmd,value	value: string, max length 20
0604	phoneNumber4	cmd,value	value: string, max length 20
0605	phoneNumber5	cmd,value	value: string, max length 20
0606	phoneNumber6	cmd,value	value: string, max length 20
0607	phoneNumber7	cmd,value	value: string, max length 20
0608	phoneNumber8	cmd,value	value: string, max length 20
0609	phoneNumber9	cmd,value	value: string, max length 20
0610	phoneNumber10	cmd,value	value: string, max length 20
0633	phoneGroupMapping1	cmd,flag	flag: Bit0 refers to Phone No.1": 1- add to Phone Group 1, 0 – do not add to Phone Group 1; Bit 1 refers to Phone No.2": 1- add to Phone Group 1 , 0 – do not add to Phone Group 1; Bit 2 refers to Phone No.3": 1- add to Phone Group 1, 0 – do not add to Phone Group 1; …… Bit 9 refers to Phone No.10": 1- add to Phone Group 1, 0 – do not add to Phone Group 1; Following commands such as "phoneGroupMapping2" and "phoneGroupMapping3", etc are the same.
0634	phoneGroupMapping2	cmd,flag	
0635	phoneGroupMapping3	cmd,flag	
0636	phoneGroupMapping4	cmd,flag	
0637	phoneGroupMapping5	cmd,flag	
0638	phoneGroupMapping6	cmd,flag	
0639	phoneGroupMapping7	cmd,flag	
0640	phoneGroupMapping8	cmd,flag	
0641	phoneGroupMapping9	cmd,flag	
0642	phoneGroupMapping10	cmd,flag	
M1000_ProV2_Wakeup:			
0701	timingWakeupEnable1	cmd,flag	flag: 0 - disable,1 - enable
0702	wakeupHour1	cmd,value	value: 0-23
0703	wakeupMinute1	cmd,value	value: 0-59
0704	timingWakeupEnable2	cmd,flag	flag: 0 - disable,1 - enable
0705	wakeupHour2	cmd,value	value: 0-23

0706	wakeupMinute2	cmd,value	value: 0-59
0707	timingWakeupEnable3	cmd,flag	flag: 0 - disable,1 - enable
0708	wakeupHour3	cmd,value	value: 0-23
0709	wakeupMinute3	cmd,value	value: 0-59
0717	periodWakeupEnable	cmd,flag	flag: 0 - disable,1 - enable
0718	wakeupPeriod	cmd,value	value: 3-1800，default:0
0719	callWakeupEnable	cmd,flag	flag: 0 - disable,1 - enable
0720	callWakeup PhoneGroup	cmd,flag	flag: 0-10; 0 means no phonegroup
0721	callWakeup ReplyEnable	cmd,flag	flag: 0 - disable,1 - enable
0722	smsWakeupEnable	cmd,flag	flag: 0 - disable,1 - enable
0723	smsWakeup PhoneGroup	cmd,flag	flag: 0-10; 0 means no phonegroup
0724	smsWakeupPassword	cmd,value	value: string, max length 20
0725	smsWakeup ReplyEnable	cmd,flag	flag: 0 - disable,1 - enable
0726	dataWakeupEnable	cmd,flag	flag: 0 - disable,1 - enable
0727	outputDataLen	cmd,value	value: 0 - 30
0728	onlineOutputContent	cmd,value	value: hex format string.[0-9,a-f],max length 60 outputDataLen is half of the length of onlineOutputContent. e.g. 3132 means "12", outputDataLen is 2
M1000_ProV2_Reboot:			
0801	timingRebootEnable1	cmd,flag	flag: 0 - disable,1 - enable
0802	rebootHour1	cmd,value	value: 0-23
0803	rebootMinute1	cmd,value	value: 0-59
0804	timingRebootEnable2	cmd,flag	flag: 0 - disable,1 - enable
0805	rebootHour2	cmd,value	value: 0-23
0806	rebootMinute2	cmd,value	value: 0-59
0807	timingRebootEnable3	cmd,flag	flag: 0 - disable,1 - enable
0808	rebootHour3	cmd,value	value: 0-23
0809	rebootMinute3	cmd,value	value: 0-59
0817	callRebootEnable	cmd,flag	flag: 0 - disable,1 – enable
0818	callReboot PhoneGroup	cmd,flag	flag: 0-10; 0 means no phonegroup
0819	callReboot ReplyEnable	cmd,flag	flag: 0 - disable,1 – enable
0820	smsRebootEnable	cmd,flag	flag: 0 - disable,1 – enable
0821	smsReboot PhoneGroup	cmd,flag	flag: 0-10; 0 means no phonegroup
0822	smsRebootPassword	cmd,value	value: string, max length 20
0823	smsReboot ReplyEnable	cmd,flag	flag: 0 - disable,1 – enable
M1000_ProV2_Modbus:			
0901	modbusEnable	cmd,flag	flag: 0 - disable,1 – enable
0902	modbusMode	cmd,flag	flag: 0 – Slave 1 – Master

0903	conn2Enable	cmd,flag	flag: 0 - disable,1 – enable
0904	conn2Addr	cmd,value	value: string, max length 64
0905	conn2Port	cmd,value	value: 0 – 65535
0906	conn2SocketType		(not used)
0907	conn3Enable	cmd,flag	flag: 0 - disable,1 - enable
0908	conn3Addr	cmd,value	value: string, max length 64
0909	conn3Port	cmd,value	value: 0 - 65535
0910	conn3SocketType		(not used)
0917	modbusAddrStart1	cmd,value	value: 1-247
0918	modbusAddrEnd1	cmd,value	value: 1-247
0919	modbusAddrStart2	cmd,value	value: 1-247
0920	modbusAddrEnd2	cmd,value	value: 1-247
0921	modbusAddrStart3	cmd,value	value: 1-247
0922	modbusAddrEnd3	cmd,value	value: 1-247
M1000_ProV2_Advanced:			
1001	loginEnable	cmd,flag	flag: 0 - disable,1 - enable
1002	loginRetryTimes	cmd,value	value: 0-60，default:3
1003	loginRetryInterval	cmd,value	value: 5-120，default:60
1004	loginReqLen	cmd,value	value: 0 – 32
1005	loginReqContent	cmd,value	value: hex format string.[0-9,a-f], max length 64 loginReqLen is half of the length of loginReqContent. e.g. 3132 means "12", loginReqLen is 2
1006	loginAckLen	cmd,value	value: 0 - 32
1007	loginAckContent	cmd,value	value: hex format string.[0-9,a-f], max length 64 loginAckLen is half of the length of loginAckContent. e.g. 3132 means "12", loginAckLen is 2
1017	heartbeatEnable	cmd,flag	flag: 0 - disable,1 - enable
1018	heartbeatInterval	cmd,value	value: 5-1200，default:300
1019	heartbeatReqLen	cmd,value	value: 0 – 32
1020	heartbeatReqContent	cmd,value	value: hex format string.[0-9,a-f], max length 64 heartbeatReqLen is half of the length of heartbeatReqContent. e.g. 3132 means "12",

			heartbeatReqLen is 2
1021	heartbeatAckLen	cmd,value	value: 0 - 32
1022	heartbeatAckContent	cmd,value	value: hex format string.[0-9,a-f], max length 64 heartbeatAckLen is half of the length of heartbeatAckContent. e.g. 3132 means "12", heartbeatAckLen is 2
1033	logoutEnable	cmd,flag	flag: 0 - disable,1 - enable
1034	logoutReqLen	cmd,value	value: 0 - 32
1035	logoutReqContent	cmd,value	value: hex format string.[0-9,a-f], max length 64 logoutReqLen is half of the length of logoutReqContent. e.g. 3132 means "12", logoutReqLen is 2
1036	logoutAckLen	cmd,value	value: 0 - 32
1037	logoutAckContent	cmd,value	value: hex format string.[0-9,a-f], max length 64 logoutAckLen is half of the length of logoutAckContent. e.g. 3132 means "12", logoutAckLen is 2

5.2.4 SMS Control examples

Command SMS configuration examples			
Configuration Category	Configuration Description	SMS Content	Comments
Enable Configuration	enableDelimiter1	0109,1	Enable Delimiter1.
	enableDelimiter2	0111,0	Disable Delimiter2.
Option Configuration	Parity	0105,1	Be configured as Odd parity.
	authTypeSim1	0201,2	SIM1 is configured as PAP authType.

Hex character Configuration	delimiter1	0110,31	“31” represents the hex number 0x31, representing the character "1", delimiter ranges 0x00-0xff.
	delimiter2	0112,32	“32” represents the hex number 0x32, representing the character "2", delimiter ranges 0x00-0xff.
Integer Configuration	packingLength	0108,1024	Data packing length is configured as 1024 bytes.
	Socket port	0302,8888	Port number is configured as 8888.
String Configuration	peerAddr	0301,www.robustel.net.cn	Remote IP address is configured as www.robustel.net.cn.
	SIM1 APN	0202,CMNET	SIM 1’s APN is configured as “CMNET”.
Hex String Length Value Configuration	outputDataLen	0727,2	Output data length when the gateway dial up is configured as 2.
	loginReqLen	1004,2	Login Request length is configured as 2, if “loginReqContent” is configured as “3334”, means string “34”, so “loginReqLen” is configured as 2.
Hex Sting Configuration	onlineOutputContent	0728,3132	Output Online Content when the gateway dial up is configured as “3132”.
	loginReqContent	1005,3334	The data packet to login platform is configured as “3334”.
Phone Group Configuration	phoneGroupMapping1	0633,1	3 = 0000000001, it means Phone No.1 is added to Phone Group 1.
	phoneGroupMapping2	0634,3	3 = 0000000011, it means Phone No.1 and Phone No.2 are added to Phone Group 1.
Choose Phone Group	csdBackup PhoneGroup	0317,1	Assign Phone Group 1 as CSD backup Phone Group.
	smsReboot PhoneGroup	0821,2	Assign Phone Group 2 as SMS reboot Phone Group.

5.3 Troubleshooting

This section of the document describes possible problems encountered when using the Robustel M1000 Pro V2 and their solutions.

5.3.1 The gateway's LED does not light:

- Check if gateway has connected to a 9 to 36VDC power supply properly.
- Check if the power connector is properly inserted.

5.3.2 No connection with gateway through serial link

- Check if the serial cable has been connected properly.
- Check if the serial cable has been made by following pin assignment given in table **PIN Assignment** for RS232 and RS485.
- Check if your program has proper setting. Factory setting of the gateway under **Normal Mode** is listed at **5.1**.
- Check if there is another program interfering with the communication program, such as conflict on communication port access.

5.3.3 GPRS/UMTS connection cannot be established

- Check if the APN, User Name and Password have been input correctly.
- Check if the SIM card balance is enough or not.

5.4 Terms and Abbreviations

Abbreviations	Description
AC	Alternating Current
APN	Access Point Name of GPRS/UMTS Service Provider Network
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CSD	Circuit Switched Data
CTS	Clear to Send
dB	Decibel

dBi	Decibel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DDNS	Dynamic Domain Name Server
DNS	Domain Name Server
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
GND	Ground
GPRS	General Package Radio Service
GSM	Global Standard for Mobile Communications
IMEI	International Mobile Equipment Identification
kbps	kbits per second
LED	Light Emitting Diode
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PPP	Point-to-point Protocol
PIN	Personal Identity Number
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
Rx	Receive Direction
SIM	Subscriber Identification Module
SMA	Subminiature Version A RF Connector

SMS	Short Message Service
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UDP	User Datagram Protocol
USSD	Unstructured Supplementary Service Data
VSWR	Voltage Stationary Wave Ratio