

# Robustel GoRugged M1000 2.4G

## Industrial Serial to Wi-Fi Gateway

### For 2.4G Networks

## User Guide

Document Name: **User Guide**  
Firmware: **01.00**  
Date: **2012-08-15**  
Status: **Confidential**  
DocID: **RT\_M1000\_2.4G\_v01.00**



## About This Document

This document describes the hardware and software of the *Robustel M1000 2.4G Industrial Serial to Wi-Fi Gateway*.

**Copyright© Guangzhou Robustel Technologies Co., Limited  
All Rights Reserved.**

## 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: +86-2023354618

Fax: +86-2032016426

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

Web: [www.robustel.com](http://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 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.
- 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 26.6 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.

### Using the gateway in vehicle

- The driver or operator of any vehicle should not operate the gateway while in control of a vehicle.
- 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 follow:
- Do not expose the gateway to extreme conditions such as high humidity / rain, high temperatures, 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

2002/95/EC	Directive of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS)	
2002/96/EC	Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE)	
2003/108/EC	Directive of the European Parliament and of the Council of 8 December 2003 amending directive 2002/96/ec 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	<p>“Marking for Control of Pollution Caused by Electronic Information Products” (2006-06).</p> <p>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.</p> <p>Please see <a href="#">Table 3</a> 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.</p>	

**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	Details
2012-08-15	01.00	First Release

## Contents

Chapter 1.	Product Concept.....	6
1.1	Overview .....	6
1.2	Packing List.....	6
1.3	Specifications .....	8
1.4	Dimensions.....	9
1.5	Selection and Ordering Data.....	9
Chapter 2.	Installation.....	10
2.1	Overview .....	10
2.2	LED Indicators.....	10
2.3	Mounting the gateway .....	10
2.4	Connect the External Antenna (SMA Type).....	11
2.5	Connect the Gateway to External Device.....	11
2.6	Grounding the Gateway .....	12
2.7	Power Supply .....	13
Chapter 3.	Operate the Gateway .....	14
3.1	Working Mode Overview .....	14
3.2	Command Reference.....	14
3.2.1	Command Syntax .....	14
3.2.2	Command Organization .....	15
3.3	SET Commands.....	15
3.3.1	Adhoc Parameters .....	15
3.3.2	Broadcast Parameters.....	16
3.3.3	COMM Parameters .....	16
3.3.4	DNS Parameters.....	17
3.3.5	FTP Parameters.....	17
3.3.6	IP Parameters.....	18
3.3.7	Optional Parameters.....	19
3.3.8	System Parameters .....	20
3.3.9	Time Server Parameters .....	21
3.3.10	UART Parameters.....	21
3.3.11	WLAN Parameters.....	22
3.4	Get Commands .....	24
3.5	Status Commands .....	25
3.6	Action Commands.....	25
3.7	Terms and Abbreviations .....	27





- 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):

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



- 35mm Din-Rail mounting kit x2



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



- DB9 Male to 9-pin 5mm pluggable terminal block for serial port and DI/DO x1

## 1.3 Specifications

### Wi-Fi Interface

- Networking Standards: 802.11 b/g
- Data Rate: 802.11b up to 11 Mbps, 802.11g up to 54 Mbps
- Frequency: 2.412 to 2.484 GHz
- Modulation: 802.11 b: DSSS(CCK-11, CCK-5.5, DQPSK-2, DBPSK-1); 802.11g : OFDM
- Security: WEP, WPA, WPA2
- Protocols: DHCP, DNS, ARP, ICMP, FTP client, HTTP client, TCP, UDP
- Output Power: 0 to +12dBm
- Transmit Range: Up to 150 meters @ +12 dBm (open area)

### Antenna Interface

- Antenna Interface: SMA Female, 50 ohms impedance

### Serial Interface

- Number of Ports: 1 x DB9 Female
- Serial Standards: RS232 or RS485
- ESD Protection: 15KV
- Parameters (Wi-Fi): 8N1, 8N2, 8E1, 8E2, 8O1, 8O2, 2400bps to 115200bps (default: 8N1, 9600bps)
- Flow Control: RTS/CTS, XON/XOFF
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B), GND

### System

- LED Indicators: 3 indicators, PWR, NET and Rx/Tx

### Power Supply and Consumption

- Power Supply Interface: 2-pin 5mm pluggable terminal block
- Input Voltage: 9 to 36 VDC
- Power Consumption:  
4uA sleep, 35mA active RX, 180mA TX (at +12dBm)

### Physical Characteristics

- Housing& Weight: Metal, 300g
- Dimension (L x W x H): 102.4 x 71.4 x 29.4 mm
- Installation: 35mm Din-Rail or wall mounting or desktop

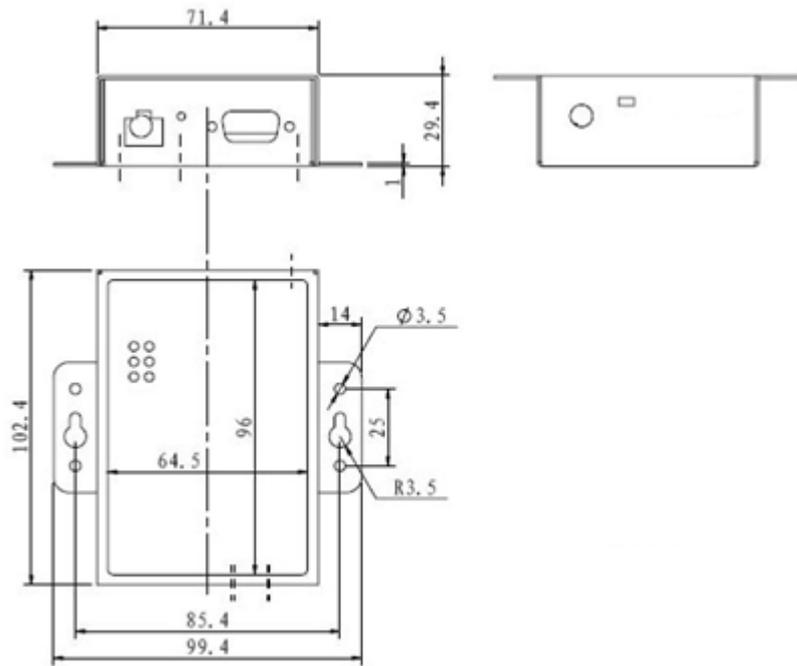
### Environmental Limits

- Operating Temperature& Humidity: -25 to 70°C, 5 to 95% RH
- Storage Temperature: -40 to 85°C

### Warranty

- Warranty Period: 1 Year

## 1.4 Dimensions

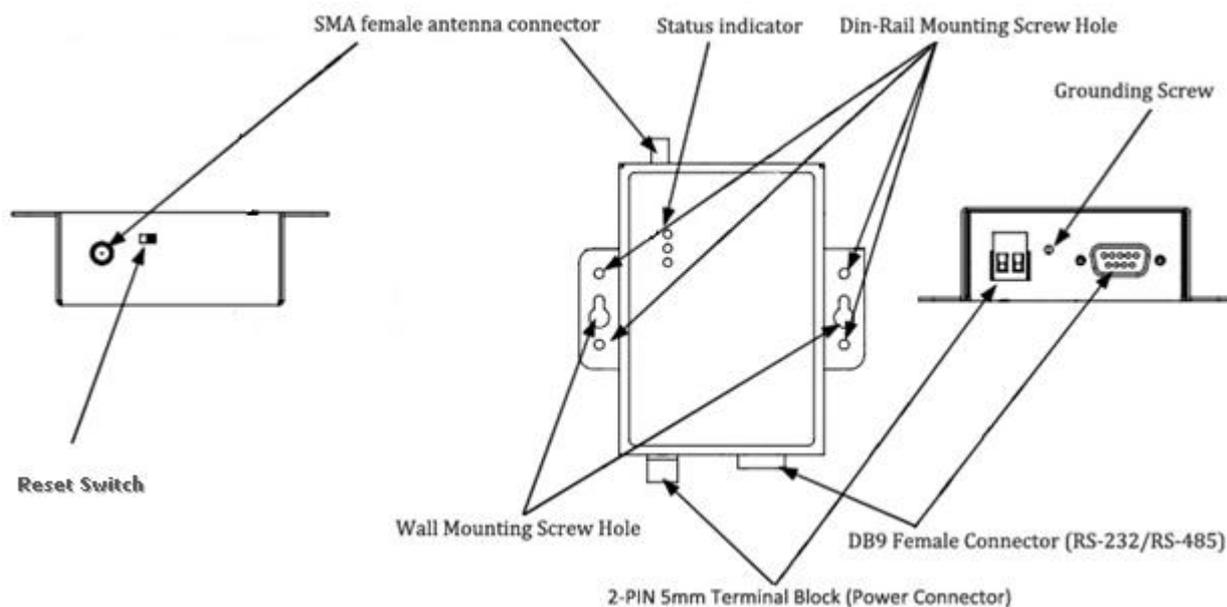


## 1.5 Selection and Ordering Data

Please refer to corresponding M1000 2.4G datasheet.

## Chapter 2. Installation

### 2.1 Overview



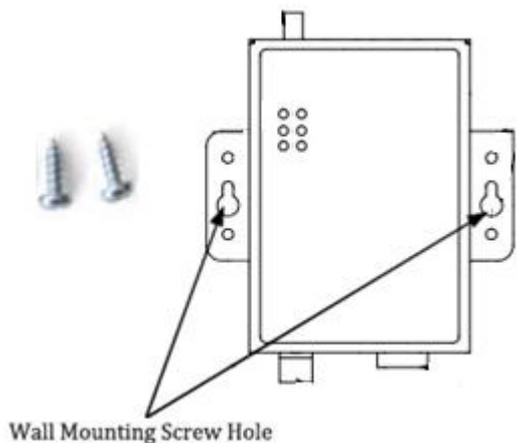
### 2.2 LED Indicators



Condition	NET	Rx/Tx	PWR
On solid	Connected over TCP	-	Power on
Fast blink	No IP address	Rx/Tx data transfer	-
Slow blink	IP address OK	-	-
Off	-	-	Power off

### 2.3 Mounting the gateway

Use 2 pcs of M3 screw to mount the gateway on the wall.

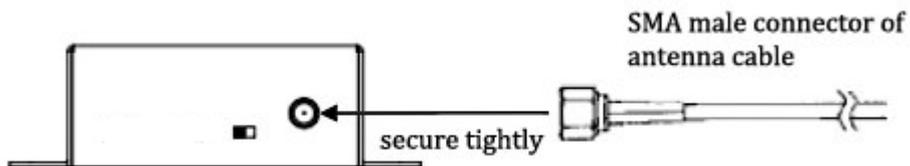


Or to mount the gateway on a DIN rail, you need two DIN rail mount adapters, and 4thread form M3 screws.



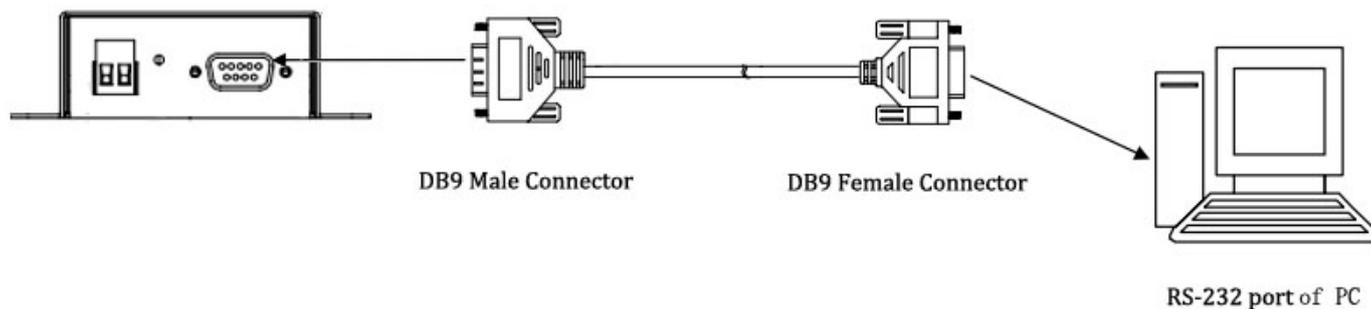
## 2.4 Connect the External Antenna (SMA Type)

Connect this to an external antenna with SMA male connector. Make sure the connector is secured tightly.

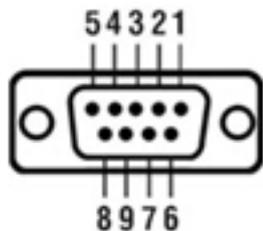


## 2.5 Connect the Gateway to External Device

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



**PIN assignment for gateway’s DB9 female connector**

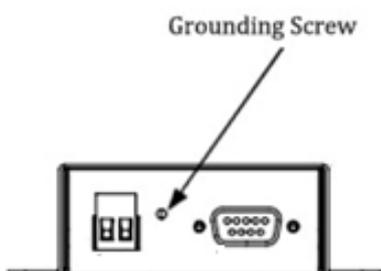


**PIN Assignment**

DB9 Female Connector

PIN	RS232	RS485 (2-wire)
1		DCD
2	RXD ->	DSR
3	TXD<-	
4		
5	GND	GND
6		
7	RTS<-	
8	CTS ->	
9		

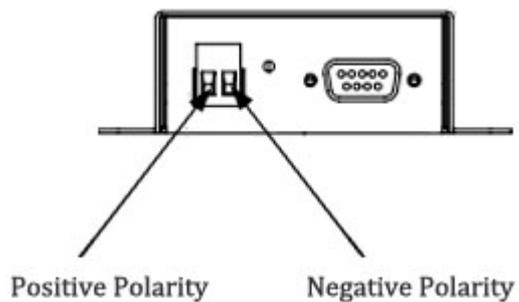
**2.6 Grounding the Gateway**



Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.

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

## 2.7 Power Supply



The power supply range is 9 to 36VDC.

**Note:** Please take care about the polarity, and do not make reverse connection.

## Chapter 3. Operate the Gateway

### 3.1 Working Mode Overview

There are two modes in the gateway, namely normal mode and config mode. At any given time, the module will either be in normal mode or in config mode.

Mode	Description
Normal Mode	<p>Upon power up, the device will be in normal mode, user could use follow functions:</p> <ol style="list-style-type: none"> <li>1. Accept incoming connections;</li> <li>2. Initiate outgoing connections.</li> </ol> <p>You can input <b>\$\$\$</b> (by default and you can change it) to switch the device to config mode. The device will respond with <b>CMD</b> indicating it is in config mode.</p>
Config Mode	<p>When device switches to <b>Normal Mode</b>, user could use follow functions:</p> <ol style="list-style-type: none"> <li>1. Configure the parameters;</li> <li>2. View the current configuration.</li> </ol> <p>While in config mode, the device will accept ASCII bytes as commands. Each command ends with a carriage return <b>&lt;cr&gt;</b>. To exit config mode, send <b>exit&lt;cr&gt;</b>. The device will respond with <b>EXIT</b> indicating that it has exited config mode and switched into normal mode.</p>

**Note:** Please **DO NOT** use HyperTerminal. Use **TeraTerm** as your terminal emulator.

### 3.2 Command Reference

#### 3.2.1 Command Syntax

Commands begin with a keyword, and have optional additional parameters, generally space delimited. Commands and options are case sensitive. Hex input data can be upper or lower case. String text data, such as SSID is also case sensitive.

The first command is fully decoded and must be complete. Other command parameters can be shorted by using only the first character.

For example,

**set uart baudrate 115200** is valid,

**set uart b 115200** is also valid,

**set u b 115200** is also valid, however,

**s uart baudrate 115200** is NOT valid.

Numbers can be entered as either decimal, (like 115200 above) or HEX. To enter HEX, use 0x<value>. For example, the HEX value FF would be entered as 0xFF.

## 3.2.2 Command Organization

Commands fall into 5 general categories:

**SET COMMANDS** Take effect immediately, permanently (when save command is issued).

**GET COMMANDS** Retrieve the permanently stored information for display to user.

**STATUS COMMANDS** See what is going on with the interface, IP status, etc.

**ACTION COMMANDS** Perform action such as scan, connect, disconnect, etc.

**FILE IO COMMANDS** Upgrade, load and save configuration, delete files, etc

**NOTE:** You must save any changes made or the gateway will load the previous settings upon reboot or power up. Configuration is saved using the save command.

## 3.3SET Commands

These commands begin with “set”. There are 6 major categories.

<b>Adhoc</b>	controls the adhoc parameters
<b>Broadcast</b>	controls the broadcast hello/heartbeat UDP message
<b>COMM</b>	communication and data transfer, timers, matching characters
<b>DNS</b>	DNS host and domain
<b>FTP</b>	FTP host address and login information
<b>IP</b>	IP settings
<b>Option</b>	optional and not frequently used parameters
<b>Sys</b>	system settings such as sleep and wake timers
<b>Time</b>	timer server settings
<b>UART</b>	serial port settings such as baudrate and parity
<b>WLAN</b>	wireless interface settings, such as ssid, chan, and security options

### 3.3.1 Adhoc Parameters

**set adhoc beacon <ms>**sets the adhoc beacon interval in milliseconds. Default is 100.

**set adhoc probe <num>**sets the adhoc probe timeout in seconds. This is the number of seconds waiting for probe responses before declaring, “ADHOC is lost” and disabling the network interface. Default is 60.

### 3.3.2 Broadcast Parameters

**set broadcast address <addr>**sets the address to which the UDP hello/heartbeat message is sent. The default address is 255.255.255.255

**set broadcast interval <value>**sets the interval at which the hello/heartbeat UDP message is sent. Interval is specified in seconds. The value is a mask that is compared to a free running seconds counter. For example if interval = 0x7, a packet will be sent every 8 seconds. The minimum interval value is 1 (every 2 seconds) and max value is 0xff (every 256 seconds). Setting the interval value to zero disables sending UDP broadcast messages. Default interval is 7.

**set broadcast port <port>**sets the port number to which the UDP hello/heartbeat message is sent. Default port is 55555.

### 3.3.3 COMM Parameters

**set comm \$ <char>**sets character used to enter config mode. Typically used when “\$\$\$” is a possible data string..Default is“\$”

**set comm close <string>**sets the ASCII string that is sent to the local UART when the TCP port is closed. If no string is desired, use 0 as the <string> parameter. Max string length is 32 characters. Default is \*CLOS\*

**set comm open <string>**sets the string that is sent to the local UART when the TCP port is opened. If no string is desired, use 0 as the <string> parameter. Max string length is 32 characters. Default is \*OPEN\*

**set comm remote <string>**sets the string that is sent to the remote TCP client when the TCP port is opened. If no string is desired, use 0 as the <string> parameter. Max string length is 32 characters. Default is \*HELLO\*

**set comm idle <secs>**sets the Idle Timer Value. This is the number of seconds with no transmit or receive data over TCP before the connection is closed automatically. Default is 0, never disconnect on idle.

**set comm match <value>**sets match character. An IP packet will be sent each time the match character appears in the data. Value is entered either as decimal (13) or hex (0xd) of the of the ASCII character. Default is 0, disabled. The match character is one of three ways to control TCP/IP packet forwarding. The others are comm size and comm timer. For more

information refer to section on UART Receiver.

**set comm size <value>**sets the flush size. An IP packet will be sent each time “value” bytes are received. Default is 64 bytes. It is recommended to set this value to the largest possible setting to maximize TCP/IP performance. Maximum value = 1420 (at 9600) bytes.

**NOTE:** *This value is set automatically when the baudrate is set, in an attempt to optimize the link. It is assumed that higher baudrates equates to more data and hence the flush size is increased.*

Flush size is one of three ways to control TCP/IP packet forwarding. The others are match character and timer. For more information refer to section on UART Receiver.

**set comm time <num>**sets the flush timer. An IP packet will be sent if no additional bytes are received for “num” milliseconds. “num” is one milliseconds interval. Default is 10 (10 milliseconds). Setting this value to 0 will disable forwarding based on the flush timer.

### 3.3.4 DNS Parameters

**set dns address <addr>**sets the IP address of the DNS sever. This is auto-set when using DHCP, and needs to be set in STATIC IP or Auto-IP modes.

**set dns name <string>**sets the name of the host for TCP/IP connections.

**set dns backup <string>**sets the name of the backup host for TCP/IP connections.

### 3.3.5 FTP Parameters

**set ftp addr <addr>**set the IP address of the FTP server.

**set ftp dir <string>**sets the directory to use on the FTP server. Default is “public”. To read/write to sub-folders, use the “\” for your directory structure. For example, to read/write to the “test” sub-folder in “demo” directory, the command is **set ftp dir demo\test**. To root directory is set by using the period “.” To set the root directory, the command if **set ftp dir .**

**set ftp filename <file>**sets the name of the file transferred when issuing the **ftp u** command. The file here refers to the firmware image. If any file other than the firmware image is set, the gateway will download the file and then issue the **UPDATE FAIL=3** error since it is not the firmware image.

**set ftp mode <mask>**sets the ftp mode. Default is passive mode (mode =0x0). Setting mode=0x1 enables active mode.

**set ftp remote <port>**sets the ftp server remote port number (default is 21).

**set ftp time <value>**sets the ftp timeout value. This timer is used to automatically close the FTP connection. The timer is 1/8th of the actual value. For example, to set a timer of 5 seconds, the command is **set ftp timer 40**. To set the timer to 10 seconds is **set ftp timer 80**.

**set ftp user <name>**sets the ftp user name for accessing the FTP server.

**set ftp pass <pass>**sets the ftp password for accessing the FTP server.

### 3.3.6 IP Parameters

**set ip address <addr>**sets the IP address of the gateway. If DHCP is turned on, the IP address is assigned and overwritten during association with the access point. IP addresses are "." delimited.

Example: **set ip a 10.20.20.1**

**set ip backup <addr>**sets a secondary host IP address. If the primary host IP is not reachable the gateway will try the secondary IP address if set.

**set ip dhcp <value>**enable/disable DHCP mode. If enabled, the IP address, gateway, net mask, and DNS server are requested and set upon association with access point. Any current IP values are overwritten.

DHCP Cache mode can reduce the time it takes the gateway to wake from deep sleep thus saving power. In cache mode, the lease time is checked and if not expired, the gateway uses the previous IP settings. If the lease has expired the gateway will attempt to associated and use DHCP to get the IP settings. DHCP cached IP address does not survive a power cycle or reset.

Mode	Protocol
0	DHCP OFF, use stored static IP address
1	DHCP ON, get IP address and gateway from AP
2	Auto-IP, generally used with Adhoc networks
3	DHCP cache mode, Uses previous IP address if lease is not expired (lease survives reboot)
4	Reserved for future use

**set ip flags <value>**set TCP/IP functions. Value is a bit mapped register. Default = 0x7.

Bit	Function
0	TCP connection status. See note below
1	Bypass Nagle algorithm and use TCP_NODELAY
2	TCP retry enabled (total of 96 packet retries)
3	UDP RETRY (attempts retry if no ACK from UDP)
4	DNS host address caching enabled
5	ARP table caching enabled
6	UDP auto pairing enabled
7	Add 8 byte timestamp to UDP or TCP packets

**set ip gateway <addr>**sets the gateway IP address, If DHCP is turned on, the gateway IP address is assign and

overwritten during association with the access point.

**set ip host <addr>**sets the remote host IP address. This command is used for making connections from the gateway to a TCP/IP server at the IP address <addr>.

**set ip localport <num>**sets the local port number.

**set ip netmask <value>**sets the network mask. If DHCP is turned on, the net mask is assign and overwritten during association with the access point.

**set ip protocol <value>**sets the IP protocol. Value is a bit mapped setting. To connect to the gateway over TCP/IP such as Telnet the device must have the use the TCP Server protocol / bit 2 set. To accept both TCP and UDP use value = 3 (bit 1 and bit 2 set).

Bit Position	Protocol
0	UDP
1	TCP Server & Client (Default)
2	Secure (only receive packets with IP address matches the store host IP)
3	TCP Client only
4	HTTP client mode

**set ip remote <value>**sets the remote host port number.

### 3.3.7 Optional Parameters

**set opt jointmr <msecs>**Join timer is the time in milliseconds the join function will wait for the an access point to complete the association process. This timer is also the timeout for the WPA handshaking process. Default is 1000.

**set opt replace <char>**replacement character for spaces. The replacement character is used when entering SSID and pass phrases that include space. This is used by the gateway command parser only. Each occurrence of the replacement character is changed into a space. The default is "\$" (0x24)

**set opt deviceid <string>**Configurable Device ID - can be used for storing serial numbers, product name or other device information. This information is sent as part of the broadcast hello packet that is sent as a UDP. The current value can be shown with the "get option" or "show deviceid" commands. Max string size is 32 bytes.

**set opt password <string>**TCP connection password.

### 3.3.8 System Parameters

**set sys autoconn <value>**TCP mode: sets the auto connect timer. This command causes the gateway periodically connect to the stored remote host. The timer <value> determines how often to connect to the stored remote host. Default=0

Value	Description
<b>0</b>	Disable auto connect timer
<b>1</b>	Connect to the stored host IMMEDIATELY upon power up or wake from sleep state
<b>2-254</b>	Connect to a stored host every <value> number of seconds
<b>255</b>	Connect to a stored host IMMEDIATELY upon power up or wake from sleep state and go back to sleep IMMEDIATELY as soon as TCP connection is closed

**NOTE:** To use the auto connect timer, the remote host IP address and port must be stored in the gateway using the **set ip host <IP address>** and **set ip remote <port>** commands.

**set sys autosleep <value>**Sets the auto-sleep timer in UDP mode. If the protocol is set to UDP ONLY, this timer is used as a quick sleep function. Device will sleep <value> milliseconds after transmission of the first UDP packet. Setting value to 0 disables the autosleep timer.

**set sys printlvl <value>**Controls debug print messages. This configures the debug messages printed by the gateway on the UART. Default=1.

Value	Description
<b>0</b>	Quiet mode. No messages printed when gateway wakes up or powers up.
<b>1</b>	All status messages
<b>2</b>	Only critical NETWORK AP connection level status is output, "Associated!" or "Disconnect from <ssid>"
<b>4</b>	DHCP and IP address status information. Once the configuration has been checked; this can then be turned off so that these messages do not interfere with the data.
<b>0x4000</b>	New scan format output
<b>0x10</b>	Enables uart heartbeat message

**set sys sleep <value>**sets the sleep timer. The sleep timer is the time in seconds after which the gateway goes to sleep. This timer is disabled during an open TCP connection. When the TCP connection is closed, the gateway counts down and puts the gateway in sleep state based on the value (in seconds). Setting the value= 0 disables the sleep counter and the gateway will not go into sleep based on this counter.

**NOTE:** Be sure to set the wake timer if not using an external wake up signal

before issuing the sleep timer or the gateway will never wake up.

**set sys trigger <value>**The gateway can wake up from sleep state using two different policies.

Bit Position	Description
0	Wake up on RX data
1	Wake up on CTS

**set sys wake <secs>**sets the auto wake timer. The wake timer is the number of seconds after which the gateway will wake from sleep state. Setting value=0 disables. See section on using system timers for more details.

### 3.3.9 Time Server Parameters

**set time address <addr>**sets the time server address. (sNTP servers)

**set time port <num>**sets the time server port number. Defaults to 123, which is almost always the sNTP server port.

**set time enable <value>**Enable or disable fetching time from the specified sNTP time server. Default=0= disabled. A value or 1 gets time only once on power up. Any value > 1 gets time continuously every <value> minutes.

**set time raw <value>**Enables setting the RTC raw value from the console. This command sets the RTC in seconds which ticks at 32768 Hz.

### 3.3.10 UART Parameters

**set uart baud <rate>**set the UART baud rate. Valid settings are {2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400}.

Example: “**set u b 9600**” sets the baud rate to 9600 baud.

**set uart instant <rate>**This immediately changes the baudrate. This setting does not affect configuration. Returns the AOK response, and then this command will exit command mode.

**set uart raw <rate>**sets a RAW UART value. Used to set non-standard rates. The lowest possible baud rate is 2400.

Example : “**set u r 7200**” sets the baud rate to 7200 baud.

Using non standard raw baud rates (with hardware flow control) can be more useful at speeds as the micro controller interfaced to the module may be able to better match the uart speeds and get better results.

The following raw baud rates are supported:

Raw baud rate	Comment
458333	This is 460800
500000	Raw baud rate
550000	Raw baud rate
611111	Raw baud rate
687599	Raw baud rate
785714	Raw baud rate
916667	This is 921600
1100000	Raw baud rate

**set uart flow <0,1>**sets the flow control mode. Default=0=Disabled, 1= hardware RTS/CTS.

### 3.3.11 WLAN Parameters

**set wlan auth <value>**Sets the authentication mode.

Value	Authentication Mode
0	Open (Default)
1	WEP-128
2	WPA1
3	Mixed WPA1 & WPA2-PSK
4	WPA2-PSK
5	Not Used
6	Adhoc, Join any Adhoc network
8	WEP-64

**set wlan channel <value>**sets the wlan channel, 1-13 is the valid range for a fixed channel. If 0 is set, then scan is performed, using the ssid, for all the channels set in the channel mask.

**set wlan join <value>**sets the policy for automatically joining/associating with network access points. This policy is used when the module powers up, including wake up from the sleep timer.

Value	Policy
0	Manual, do not try to join automatically
1	Try to join the access point that matches the stored SSID, passkey and channel. Channel can be set to 0 for scanning. (Default)
2	Join ANY access point with security matching the stored authentication mode. This ignores the stored SSID and searches for the access point with the strongest signal. The channels searched can be limited by setting the channel mask.
3	Reserved – Not used

4	Create an Adhoc network, using stored SSID, IP address and netmask. Channel MUST be set. DHCP should be 0 (static IP) or set to Auto-IP with this policy. (unless another Adhoc device can act as DHCP server) This policy is often used instead of the hardware jumper to create a custom Adhoc network
---	---

**set wlan hide <0, 1>**Hides the WEP key and WPA passphrase. When set, displaying the wlan settings shows \*\*\*\*\* for these fields. To unhide the passphrase or passkey, re-enter the key or passphrase using the set wlan key or set wlan passphrase command. Default = 0, do not hide.

**set wlan key <value>**sets the 128 bit WEP key. If you are using WPA or WPA2 you should enter a pass phrase with the set wlan passphrase command. Key must be EXACTLY 13 bytes (26 ASCII chars). Data is expected in HEX format, "0x" should NOT be used here.

Example : "**set w k 112233445566778899AABBCCDD**"

**set wlan linkmon <value>**sets the link monitor timeout threshold. If set to 1 or more, gateway will scan once per second for the AP it is associated with. The value is the threshold of failed scans before the gateway declares "AP is Lost", de-authenticates. The gateway will retry the association based on the join policy variable. A value of 5 is recommended, as some APs will not always respond to probes. Default is 0 (disabled). Without this feature, there is no way to detect an AP if it is no longer present until it becomes available again (if ever).

**set wlan mask <value>**sets the wlan channel mask used for scanning channels with the auto-join policy 1 or 2, used when the channel is set to 0. Value is a bit-map where bit 0 = channel 1. Input for this command can be entered in decimal or hex if prefixed with 0x. Default value is 0x1FFF (all channels)

**set wlan num <value>**sets the default WEP key to use. 1-4 is the valid range.

Example : "**set w n 2**" sets the default key to 2.

**set wlan phrase <string>**sets the passphrase for WPA and WPA2 security modes. 1-64 chars. The passphrase can be alpha and numeric, and is used along with the SSID to generate a unique 32 byte Pre-shared key (PSK), which is then hashed into a 256 bit number. Changing either the SSID or this value re-calculates and stores the PSK.

If exactly 64 chars are entered, it is assumed that this entry is already an ASCII HEX representation of the 32 byte PSK and the value is simply stored.

For passphrases that contain spaces use the replacement character \$ instead of spaces. For example "my pass word" would be entered "my\$pass\$word". The replacement character can be changed using the optional command **set opt replace <char>**.

Example : "**set w p password**" sets the phrase.

**set wlan rate <value>**sets the wireless data rate. Lowering the rate increases the effective range of the gateway. The

value entered is mapped according to the following table:

Value	Wireless Data Rate
0	1 Mbit/sec
1	2 Mbit/sec
2	5.5 Mbit/sec
3	11 Mbit/sec
4 - 7	Invalid
8	6 Mbit/sec
9	9 Mbit/sec
10	12 Mbit/sec
11	18 Mbit/sec
12	24 Mbit/sec (default)
13	36 Mbit/sec
14	48 Mbit/sec
15	54 Mbit/sec

**set wlan ssid <string>**sets the wlan ssid to associate with. 1-32 chars.

**NOTE:** If the passphrase or ssid contain the SPACE ( „ „) characters, these can be entered using substitution via the “\$” character.

For example, if the ssid of the AP is “yellow brick road”

You would enter “yellow\$brick\$road”

**set wlan tx <value>**Sets the Wi-Fi transmit power. Accepts value from 1-12 corresponding to 1dBm to 12dBm.

Default is 0 corresponding to 12dBm (max TX power).

Setting the value to 0 or 12 sets the TX power to 12dBm

**set wlan window <value>**sets the IP maximum buffer window size. Default is 1460 bytes.

### 3.4Get Commands

These commands begin with “get”. They display the current values.

**get adhoc** display all adhoc settings.

**get broadcast** will display the broadcast UDP address, port and interval

**get com** display comm settings.

**get dns** display DNS settings.

**get everything** displays all configuration settings, useful for debug.

**get ftp** display FTP settings.

**get ip <a>**display IP address and port number settings. Optional parameter just returns the current IP address value.

**get mac** display the device MAC address.

**get option** display the option settings like device ID

**get sys** display system settings, sleep, wake timers, etc.

**get time** display the time server UDP address and port number.

**get wlan** display the ssid, chan, and other wlan settings.

**get uart** display the UART settings.

**ver** return the software release version

## 3.5 Status Commands

These commands begin with “show”, and they return the current values of variables in the system. In some cases, for example IP addresses, the current values are received from the network, and may not match the stored values.

**show connection** Displays connection status in this HEX format: 8XYZ

Bit location	13-16	9-12	7	6	5	4	0-3
Function	Fixed	Channel	DNS found	DNS server	Authen	Assoc	TCP status
Value	8	1-13	1=resolved	1= contacted	1= OK	1=OK	0= Idle, 1= Connected 3= NOIP 4= Connecting

**show net <n>** Displays current network status, association, authentication, etc. Optional parameter displays only the MAC address of the AP currently associated.

**show rssi** Displays current last received signal strength.

**show stats** Displays current statistics, packet rx/tx counters, etc.

**show time** Displays number of seconds since last powerup or reboot

## 3.6 Action Commands

**\$\$\$** enter config mode. **X** characters are PASSED until this exact sequence is seen. If any bytes are seen before these chars, or after these chars, in a 250ms window, config mode will not be entered and these bytes will be passed on to other side.

**close** disconnect a TCP connection.

**exit** exit config mode. Exit config mode. “EXIT” will be displayed.

**factory RESET** Loads factory defaults into the RAM configuration. **Note that the RESET must be capitalized.** This command also writes the settings out to the standard config file. After this command the module then needs to be rebooted for settings to take effect.

**join <ssid>** joins the network <ssid>. If network is security enabled you must set the pass phrase with the **set wlan phrase** command prior to issuing the **join** command.

**NOTE :** This command will not work if the ssid has "space » character

**join # <num>** join a network from the scan list. <num> is the entry number in the scan list that is returned from the scan command. If network is security enabled you must set the pass phrase with the **set wlan phrase** command prior to issuing the **join** command

**leave** disconnects the gateway from the currently associated Access Point.

**lookup <hostname>** performs a DNS query on the supplied hostname.

**open <addr><port>** opens a TCP connection to the given IP port and address. If no arguments are provided, the device will attempt to connect to the **stored** remote host IP address and remote port number. <addr> can also be a DNS hostname and will be resolved if entered.

**ping <g | h | i | addr><num>** ping remote host. Default sends 1 packet. Optional <num> sends <num> pings at 10 per second.

**Ping 10.20.20.12 10** pings IP address 10 times

**ping g** pings the gateway, the gateway IP address is loaded if DHCP is turned on, otherwise it should be set with the **set ip gateway <addr>** command

**ping h** pings the stored host IP address, the host IP address can be set with the **set ip host <addr>** command

**ping 0** terminates a ping command

**reboot** forces a reboot of the device (similar to power cycle)

**scan <time><P>** Performs an active probe scan of access points on all 13 channels. Returns MAC address, signal strength, SSID name, security mode.

Default scan time is 200ms / channel = about 3 seconds.

**time is** an optional parameter, this is the time in ms per channel.

For example, "scan 30" reduces the total scan time down to about 1 second. This command also works in Adhoc mode. If the optional **P** parameter is entered, the module will perform a passive scan, and list all APs that are seen in passive mode.

**sleep** Puts the gateway to sleep mode. The gateway can come out of sleep mode by either sending characters over the uart or by using the wake timer.

**time** Sets the Real time clock by synchronizing with the time server specified with the time server parameters . This command sends a UDP time server request packet.

### 3.7 Terms and Abbreviations

Abbreviations	Description
AC	Alternating Current
AP	Access Point
ARP	Address Resolution Protocol
CCK	Complementary Code Keying
CE	Conformité Européene (European Conformity)
CTS	Clear to Send
dB	Decibel
dBi	Decibel Relative to an Isotropic radiator
DBPSK	Differential Binary Phase Shift Keying
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DHCP	Dynamic host configuration protocol
DNS	Domain Name Server
DQPSK	Differential Quadrature Phase Shift Keying
DSR	Data Set Ready
DSSS	Direct Sequence Spread Spectrum
DTE	Data Terminal Equipment
DTR	Data Terminal Ready
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
FTP	File Transfer Protocol
GND	Ground
HTTP	Hyper Text Transport Protocol
ICMP	Internet Control Messages Protocol
kbps	kbits per second
LED	Light Emitting Diode
MAC	Media Access Control
MAX	Maximum
Min	Minimum
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplexing
PC	Personal Computer
PDU	Protocol Data Unit
PPP	Point-to-point Protocol
PSU	Power Supply Unit

---

R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
Rx	ReceiveDirection
SMA	Subminiature Version A RF Connector
SSID	Service Set Identifier
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
VSWR	Voltage Stationary Wave Ratio
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
WLAN	Wireless Local Area Network