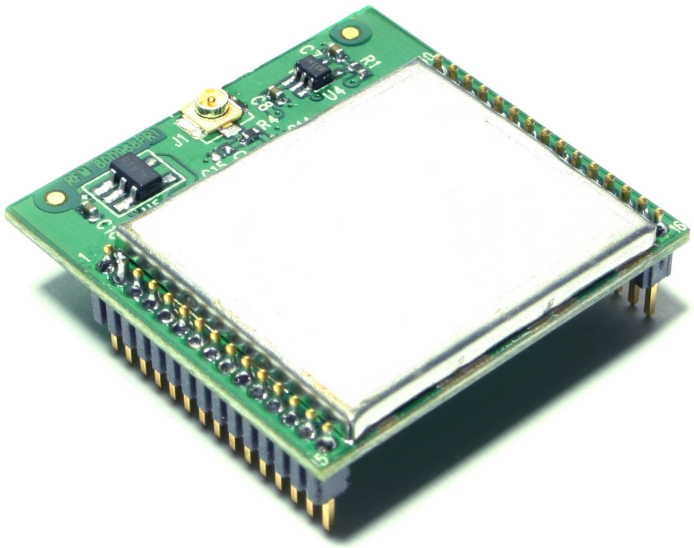
WSN802G E-Series

802.11g Wireless Sensor Network Modules



Integration Guide

Important Regulatory Information

RFM Product FCC ID: HSW-WSN802G
IC 4492A-WSN802G

Note: This unit has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their expense.

The WSN802G has been designed to operate with any dipole antenna of up to 9 dBi of gain, or any patch antenna of up to 12 dBi gain.

See Section 2.10 of this manual for regulatory notices and labeling requirements. Changes or modifications to a WSN802G not expressly approved by RFM may void the user's authority to operate the module.

Important Export Information

ECCN: 5A002.a.1 ENC
CCATS: G073573

The WSN802G products are classified under ECCN codes as 5A002.a.1 class devices and carry and ENC encryption exception. RFM has had the WSN802G products pre-screened which allows exports to countries listed in Supplement 3 to Part 740 of the Export Administration Requirements *License Exception ENC Favorable Treatment Countries*. When exporting products containing any of the WSN802G products to this list of countries, CCATS G073573 should be referenced.

Export of the WSN802G products or products containing any of the WSN802G products to other countries will require additional review and may be prohibited.

This information is provided as a guide to exporting WSN802G-based products but it is the responsibility of the entity exporting WSN802G products or devices to determine their actual requirements.

Table of Contents

1.0 Introduction

E-series WSN802G transceiver modules are a low cost, robust solution for 802.11b/g/n sensor networks. The WSN802G's low active current and very low sleep current makes long life battery operation practical. WSN802G modules are easy to integrate and compatible with standard 802.11b/g/n routers and access points. E-series WSN802G modules are optimized specifically for serial-to-Wi-Fi communications using a simple and intuitive API.

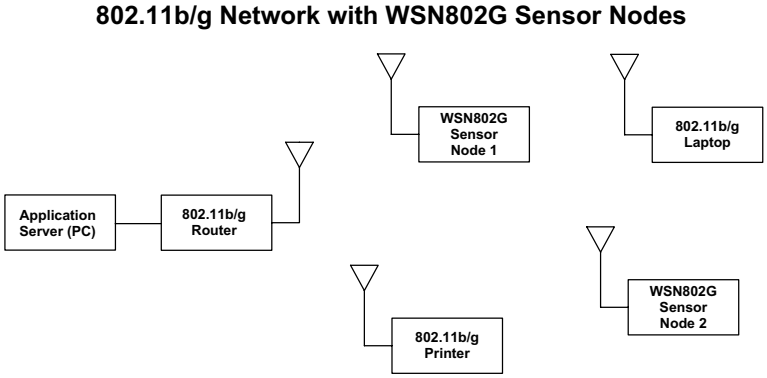


Figure 1.0.1

An example 802.11b/g/n network with WSN802G sensor nodes is shown in Figure 1.0.1. A sensor network application running on a server or PC communicates with one or more WSN802G sensor nodes through a commercial 802.11b/g/n router. WSN802G sensor nodes can be used with 802.11b/g/n routers that are also serving other applications.

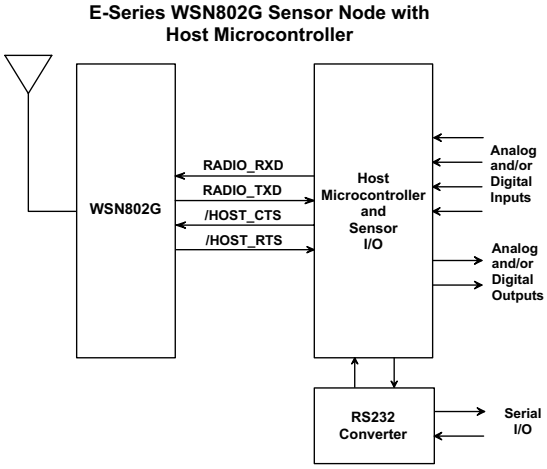


Figure 1.0.2

A WSN802G module is integrated with other components to create a sensor node. These components include a circuit board, host microcontroller, power supply (battery), sensor electronics, and a housing (external antenna also required on some WSN802G models). An example configuration is show in Figure 1.0.2. It is possible to configure serial data communications between an E-series WSN802G and its host microcontroller that requires no protocol formatting. The WSN802G formats data received from its host into packets for RF transmission, and delivers the payload data from received packets to its host. E-series WSN802G modules receive all configuration commands through their serial port.

1.1 Features

E-series WSN802G modules provide a unique set of features for wireless sensor network applications:

- Compatibility with commercial and industrial 802.11b/g/n routers and access points
- Low power consumption including sleep mode for extended battery life
- Operation over the full -40 to +85 ºC industrial temperature range
- Serial interface for data and configuration commands
- Full 14 channel 802.11b/g coverage for world wide operation
- FCC, Canadian IC and European ETSI certifications
- Four module configurations:

  WSN802GC-E - solder reflow mounting with RF connector for external antenna connection

  WSN802GCA-E - solder reflow mounting with integral chip antenna

  WSN802GP-E - plug in connector mounting with RF connector for external antenna connection

  WSN802GPA-E - plug in connector mounting with integral chip antenna

1.2 Applications

E-series WSN802G sensor networks are well suited to applications where IEEE 802.11b/g/n router compatibility, industrial temperature range operation and long battery life are important. Many applications match these criteria, including:

- Energy Monitoring and Management
- Physical Asset Management
- Cold Chain Data Logging and Food Safety
- Security and Access Control Systems
- Environmental Monitoring
- Many More

2.0 Hardware

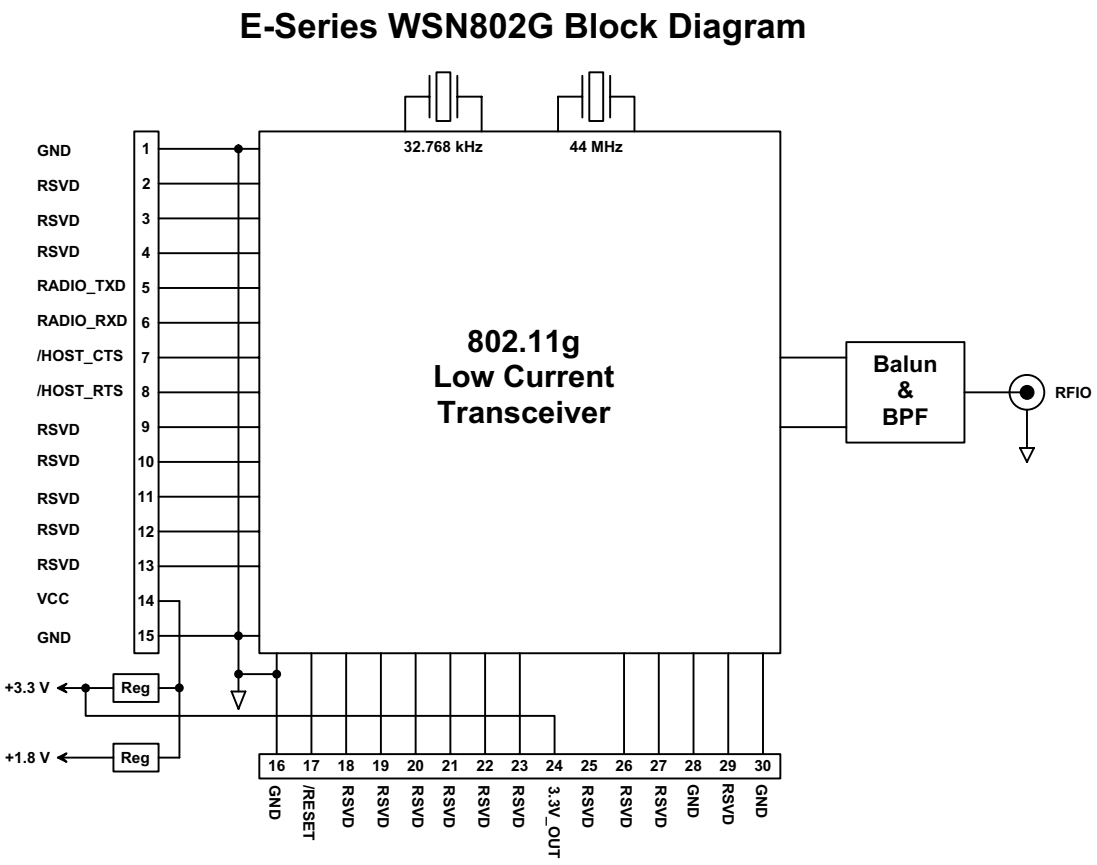


Figure 2.0.1

E-series WSN802G modules operate in the international 2.4 GHz ISM band over the frequency range of 2401 to 2474 MHz, with a nominal RF output power of 10 mW. The modules support four standard 802.11g RF data rates, 1, 2, 5.5 and 11 Mbps. The serial port supports standard serial baud rates from 1.2 to 921.6 kbps. Optional hardware or software flow control is provided.

E-series WSN802G modules are available with either RF connectors for external antennas, or with integral chip antennas. WSN802G modules are available in two mounting configurations. The WSN802GC-E and WSN802GCA-E are designed for solder reflow mounting, and the WSN802GP-E and WSN802GPA-E are designed for plug-in connector mounting.

2.1 Absolute Maximum Ratings

Rating	Sym	Value	Units
Input/Output Pins		-0.5 to +3.63	V
Ambient Temperature Range		-40 to +85	°C

Table 2.1.1

2.2 Specifications

Characteristic	Sym	Minimum	Typical	Maximum	Units
Operating Frequency Range		2401		2474	MHz
Spread Spectrum Method			Direct Sequence		
RF Chip Rate			11		Mcps
RF Data Rates			1, 2, 5.5, 11		Mbps
Modulation Type			BPSK at 1 Mbps, QPSK at 2 Mbps CCK at 5.5 and 11 Mbps		
Number of RF Channels			11		
RF Channel Spacing			5		MHz
Receiver Sensitivity, 8% PER:					
1 Mbps RF Data Rate			-92		dBm
2 Mbps RF Data Rate			-90		dBm
5.5 Mbps RF Data Rate			-84		
11 Mbps RF Data Rate			-81		
RF Transmit Power			10		mW
WSN802GC and WSN802GP RF Connector			U.FL Coaxial Connector		
Optimum External Antenna Impedance			50		Ω
WSN802GCA and WSN802GPA Antenna			Integral Chip		
Serial Port Baud Rates			1.2, 2.4, 4.8, 9.6 (default), 19.2, 28.8, 38.4, 57.6, 76.8, 115.2, 230.4, 460.8, 921.6		kbps
Power Supply Voltage Range	V_{CC}	+3		+3.63	Vdc
Power Supply Voltage Ripple				10	mV_{P-P}
Receive Mode Current				150	mA
Transmit Mode Current				200	mA
Sleep Mode Current			7.5		µA
WSN802GC and WSN802GCA Mounting			Reflow Soldering		
WSN802GP and WSN802GPA Mounting			Socket		
Operating Temperature Range		-40		85	°C
Operating Relative Humidity Range, Non-condensing		10		90	%

Table 2.2.1

2.3 Module Interface

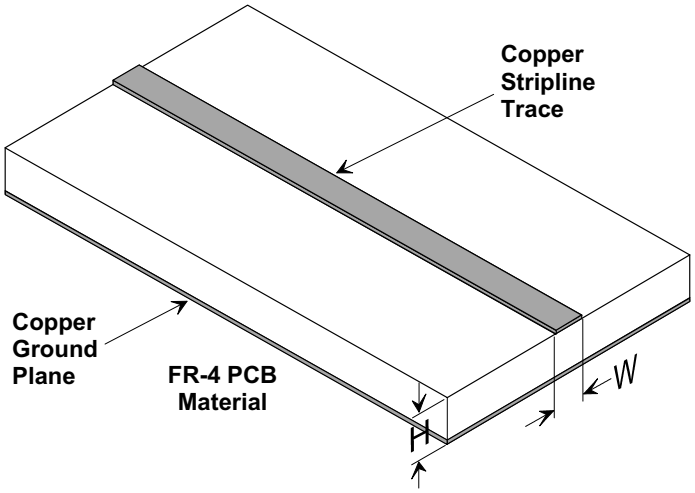
Pin	Name	I/O	Description
1	GND	-	Power supply and signal ground. Connect to the host circuit board ground.
2	RSVD	-	Reserved pin. Leave unconnected.
3	RSVD	-	Reserved pin. Leave unconnected.
4	RSVD	-	Reserved pin. Leave unconnected.
5	RADIO_TXD	O	Serial data output from the radio.
6	RADIO_RXD	I	Serial data input to the radio.
7	/HOST_CTS	O	UART flow control output. The module sets this line low when it is ready to accept data from the host on the RADIO_RXD input. When the line goes high, the host must stop sending data.
8	/HOST_RTS	I	UART flow control input. The host sets this line low to allow data to flow from the module on the RADIO_TXD pin. When the host sets this line high, the module will stop sending data to the host.
9	RSVD	-	Reserved pin. Leave unconnected.
10	RSVD	-	Reserved pin. Leave unconnected.
11	RSVD	-	Reserved pin. Leave unconnected.
12	RSVD	-	Reserved pin. Leave unconnected.
13	RSVD	-	Reserved pin. Leave unconnected.
14	VCC	I	Power supply input, +3.0 to +3.63 Vdc.
15	GND	-	Power supply and signal ground. Connect to the host circuit board ground.
16	GND	-	Power supply and signal ground. Connect to the host circuit board ground.
17	/RESET	I	Active low module hardware reset.
18	RSVD	-	Reserved pin. Leave unconnected.
19	RSVD	-	Reserved pin. Leave unconnected.
20	RSVD	-	Reserved pin. Leave unconnected.
21	RSVD	-	Reserved pin. Leave unconnected.
22	RSVD	-	Reserved pin. Leave unconnected.
23	RSVD	-	Reserved pin. Leave unconnected.
24	3.3V_OUT	O	Module's +3.3 V regulated supply, available to power external sensor circuits. Current drain on this output should be no greater than 50 mA.
25	RSVD	-	Reserved pin. Leave unconnected.
26	RSVD	-	Reserved pin. Leave unconnected.
27	RSVD	-	Reserved pin. Leave unconnected.
28	GND	-	Connect to the host circuit board ground plane.
29	RSVD	-	Reserved pin. Leave unconnected.
30	GND	-	Connect to the host circuit board ground plane.

Table 2.3.1

2.4 WSN802GC-E/WSN802GP-E Antenna Connector

A U.FL miniature coaxial connector is provided on the WSN802GC-E and WSN802GP-E modules for connection to the RFIO port. A short U.FL coaxial cable can be used to connect the RFIO port directly to an antenna. In this case the antenna should be mounted firmly to avoid stressing the U.FL coaxial cable due to antenna mounting flexure. Alternately, a U.FL coaxial jumper cable can be used to connect the WSN802G module to a U.FL connector on the host circuit board. The connection between the host circuit board U.FL connector and the antenna or antenna connector on the host circuit board should be implemented as a 50 ohm stripline. Referring to Figure 2.4.1, the width of this stripline depends on the thickness of the circuit board between the stripline and the groundplane. For FR-4 type circuit board materials (dielectric constant of 4.7), the width of the stripline is equal to 1.75 times the thickness of the circuit board. Note that other circuit board traces should be spaced away from the stripline to prevent signal coupling, as shown in Table 2.4.2. The stripline trace should be kept short to minimize its insertion loss.

Circuit Board Stripline Trace Detail



For 50 ohm impedance W = 1.75 * H

Figure 2.4.1

Trace Separation from 50 ohm Microstrip	Length of Trace Run Parallel to Microstrip
100 mil	125 mill
150 mil	200 mil
200 mil	290 mil
250 mil	450 mil
300 mil	650 mil

Table 2.4.2

2.5 Input Voltage

WSN802G radio modules can operated from an unregulated DC input (Pin 14) in the range of 3.0 V (trough) to 3.63 V (peak) over the temperature range of -40 to 85° C. *Applying AC, reverse DC, or a DC voltage outside the range given above can cause damage and/or create a fire and safety hazard. Further, care must be taken so logic inputs applied to the radio stay within the voltage range of 0 to 3.3 V. Signals applied to the analog inputs must be in the range of 0 to ADC_REF (Pin 25). Applying a voltage to a logic or analog input outside of its operating range can damage the WSN802G module.*

2.6 ESD and Transient Protection

WSN802G circuit boards are electrostatic discharge (ESD) sensitive. ESD precautions must be observed when handling and installing these components. Installations must be protected from electrical transients on the power supply and I/O lines. This is especially important in outdoor installations, and/or where connections are made to sensors with long leads. *Inadequate transient protection can result in damage and/or create a fire and safety hazard.*

2.7 Interfacing to 5 V Logic System

All logic signals including the serial ports on the WSN802G are 3.3 V signals. To interface to 5 V signals, the resistor divider network shown in Figure 2.7.1 below must be placed between the 5 V signal outputs and the WSN802G signal inputs. The output voltage swing of the WSN802G 3.3 V signals is sufficient to drive 5 V logic inputs.

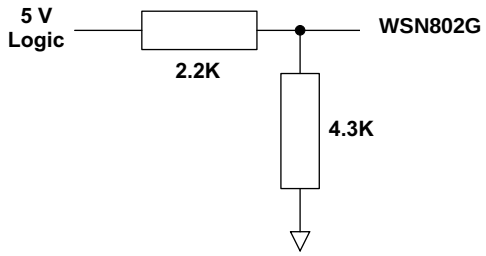


Figure 2.7.1

2.8 Power-On Reset Requirements

When applying power to the WSN802G, the /RESET pin should be held low until the power supply voltage reaches 3.3 volts for 100 milliseconds.

2.9 Mounting and Enclosures

WSN802GC radio modules are mounted by reflow soldering them to a host circuit board. WSN802GP modules are mounted by plugging their pins into a set of mating connectors on the host circuit board. Refer to Section 6.3 and/or the WSN802G Data Sheet for mounting details.

WSN802G enclosures must be made of plastics or other materials with low RF attenuation to avoid compromising antenna performance where antennas are internal to the enclosure. Metal enclosures are not suitable for use with internal antennas as they will block antenna radiation and reception. Outdoor enclosures must be water tight, such as a NEMA 4X enclosure.

2.10 Labeling and Notices

WSN802G FCC Certification - The WSN802G hardware has been certified for operation under FCC Part 15 Rules, Section 15.247. *The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.*

WSN802G FCC Notices and Labels - *This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.*

A clearly visible label is required on the outside of the user's (OEM) enclosure stating "Contains FCC ID: HSW-WSN802G."

WARNING: This device operates under Part 15 of the FCC rules. Any modification to this device, not expressly authorized by RFM, Inc., may void the user's authority to operate this device. Canadian Department of Communications Industry Notice - IC: 4492A-WSN802G

This apparatus complies with Health Canada's Safety Code 6 / IC RSS 210.

ICES-003

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus as set out in the radio interference regulations of Industry Canada.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de Classe B prescrites dans le reglement sur le brouillage radioelectrique edicte par Industrie Canada.

ETSI EN 300 328

The WSN802G module has passed ETSI EN 300 328 testing conducted by an independent test laboratory.

3.0 Application Protocol

3.1 API Overview

The Serial2WiFi stack is used to provide Wi-Fi capability to any device having a serial interface. This approach offloads WLAN, TCP/IP stack and network management overhead to the Wi-Fi module, allowing a small embedded host based on such low-cost microcontrollers as the 8051, PIC, MSP430 or AVR to communicate with other hosts on the network using a Wi-Fi wireless link. The host processor can use serial commands to configure the Serial2WiFi adapter and to create wireless and network connections.

3.2 Glossary of Terms

Term	Definition
AP	Access Point
API	Application Program Interface
BSSID	Basic Service Set Identifier
CID	Connection Identifier
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
MTU	Maximum Transfer Unit
PSK	Pre-shared Key
RSSI	Received Signal Strength Indication
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UART	Universal Asynchronous Receiver/Transmitter
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

Table 3.2.1

3.3 Standards

The following standards and conventions are considered in this design:

- IEEE 802.11a/b/g
- ITU V.25ter AT Command Set

3.4 Interface Architecture

The overall architecture of the Serial2WiFi interface is shown in Figure 3.4.1. Tx and Rx data handlers pass messages to and from the TCP/IP network. Commands related to management of the Serial2WiFi interface and the network connections are intercepted by a Command Processor. A Serial Data Handler translates data to and from a UART compatible format.

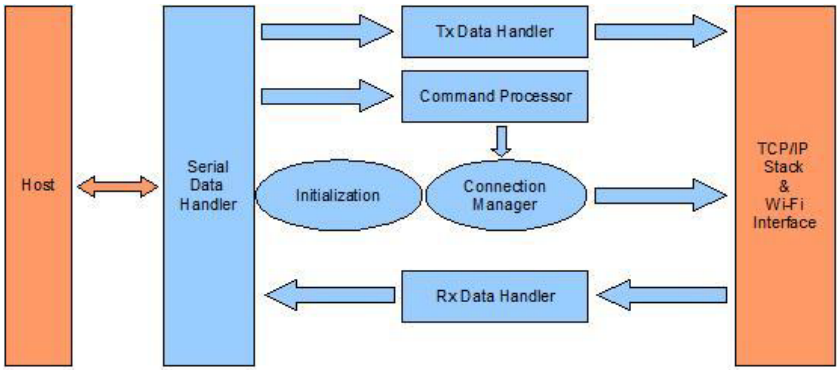


Figure 3.4.1

The system is composed of the following modules:

- System Initialization (Section 3.5)
- Command Processor (Section 3.5.4)
- Data Handlers (Section 3.7)
- Serial Data Handler (Section 2.12)
- Network Connection Manager (Section 3.13)
- Wireless Network Management (Section 3.17)

The software for the Serial2WiFi adapter is mainly driven using a state machine. During power up, initialization of all the modules is performed and then the state machine is entered. This state machine is event-driven and processes the events received from either the serial port or from the Wi-Fi/Network interface plus internal events from its own modules. The state machine calls the appropriate handler for a given event per the current state.

The Serial2WiFi adapter has three distinct operating modes (Figure 3.5.1.1). In the default command processing mode, commands to configure and manage the interface are sent over the serial interface. In the default mode, the node accepts commands entered by the host CPU and processes each of the commands. All commands are available in this mode. The user can establish a data connection here and send data.

In the *auto-connection* mode, data sent over the serial interface is transparently sent over the IP network to a single preconfigured IP address/port pair, where data from that address is transparently sent over the UART to the serial host. With auto-connect mode, the IP Layer connections are already established and the data is sent directly to the target destination. In this mode, the node does not accept all commands. To accept commands the node needs to be brought back to the command processing mode by using an escape sequence.

In *data processing* mode, data can be sent to or received from any of 16 possible connections. Each connection consists of a TCP or UDP path to a destination IP address and port. Auto-connection mode is entered using a serial command (Section 3.18.24.4) and terminated using a special escape sequence (Section 3.7). For each mode, configuration parameters are stored in non-volatile memory. In addition to factory-default parameter values, two user-defined profiles (0 and 1) are available. The parameter set to be used is determined by a user command (Section 3.18.12).

3.5 WSN802G E-series Adapter Module Description

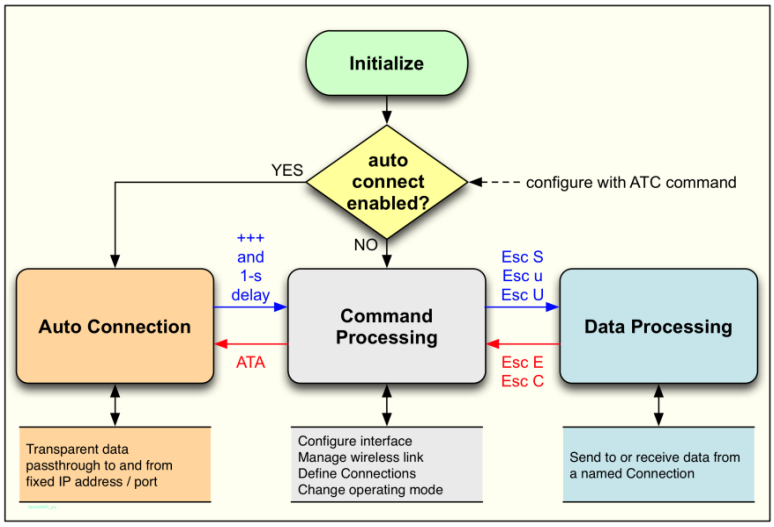


Figure 3.5.1.1

3.5.1 System Initialization

Upon startup, the Serial2WiFi interface performs the following actions, depicted graphically in Figure 3.5.1.1. During the initialization process, the module will search for a saved configuration file. The configuration file includes the auto-connection settings, default profile and profile settings. If a saved configuration file is available, it is loaded from non-volatile memory. If there is no saved configuration file, the default settings will be applied. If there are no saved parameters, the factory-default configuration is loaded. The Serial2WiFi application is initialized based on the profile settings.

If auto-connection is enabled, the interface will attempt to associate with the network previously specified by the user. Once associated, it will establish a TCP or UDP connection within the specified parameters. If successful, the interface will enter the Auto-connect mode, where all data received on the serial port is transmitted to the network destination and vice versa. If auto-connection is disabled or fails, the interface enters the command processing state.

Upon power-up, the interface defaults to 9600 baud, using 8-bit characters with no parity bits and one stop bit. Any changes to this configuration that were made in a previous session using the ATB command (Section 3.18.6.1) will be lost when power is lost. To make changes in the UART parameters that will persist across power cycling, the changes must be saved into the power-on profile using AT&W (Section 3.18.10) and AT&Y (Section 3.18.12).

3.5.2 Network Configurations

Once associated, the adapter supports instances of four types of network entities: TCP client, TCP server, UDP client and UDP server. Each client or server is associated with one or more of a possible 16 *Connection Identifiers* (CIDs), where the CID is a single hexadecimal number. More than one such entity can exist simultaneously, and a TCP server can have multiple connections, each with its own CID. When the adapter is in Auto-connect mode (Section 3.5.5), the entity called for by the Profile is created automatically upon startup. In Command modes, servers and clients are created using specific serial commands.

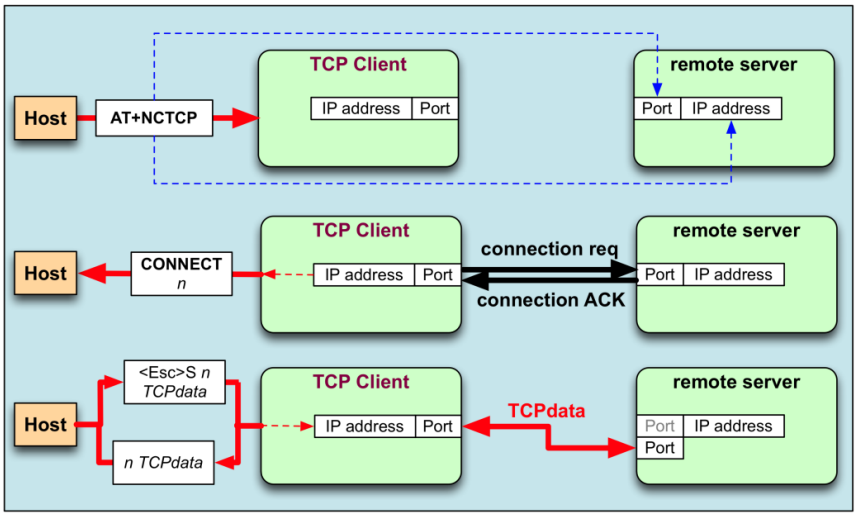


Figure 3.5.2.1

A TCP client (Figure 3.5.2.2) is created with the serial command AT+NCTCP. The client attempts to create a TCP network connection with the destination IP address and port specified within the command. If successful, it issues a CONNECT response with the CID of the client. Data can then be sent to the remote server using the <Esc>S sequence with the appropriate CID. Data from the server is passed back to the Host, with the CID to identify its source.

Figure 3.5.2.2 schematically depicts the corresponding sequence for a TCP server. A server is created with the serial command AT+NSTCP. It receives a CID, but listens passively until a remote client requests a connection. If that connection is successfully created, a second CONNECT message and a new CID are provided to the host. It is this second CID that is used to send data to the remote client and identify received data from that client. A TCP server may support multiple clients, each with a unique CID.

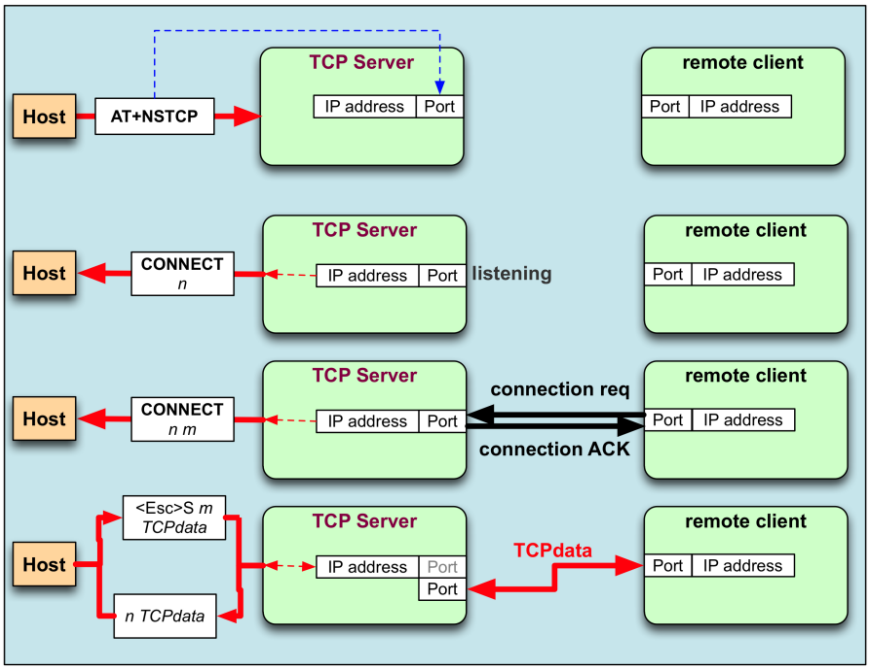


Figure 3.5.2.2

A UDP client's life is depicted in Figure 3.5.2.3. The client is created with the serial command AT+NCUDP and receives a CID. The UDP client is associated with a specific destination port and address.

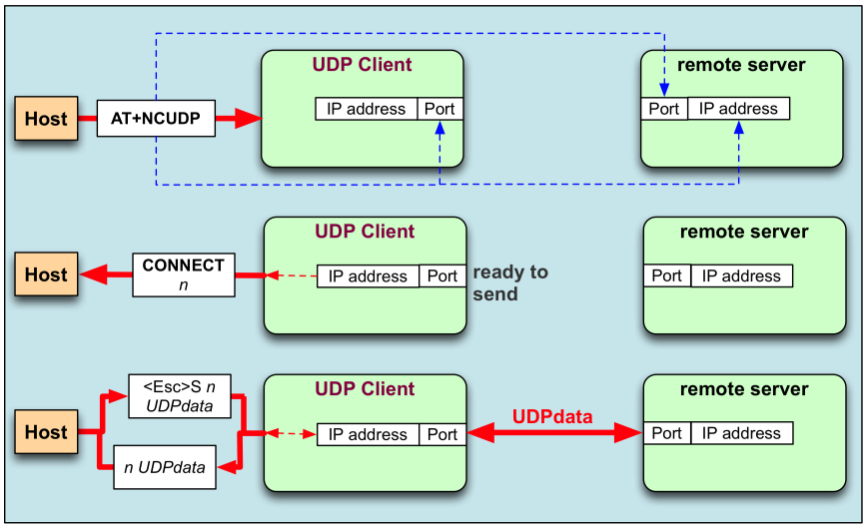


Figure 3.5.2.3

Finally, Figure 3.5.2.4 shows a UDP server. The server is created with AT+NSUDP and is assigned a CID. Individual clients do not receive unique CIDs; data sent using the UDP server must be accompanied with the destination IP address and port, and data received via the server is modified with the identifying source address and port number.

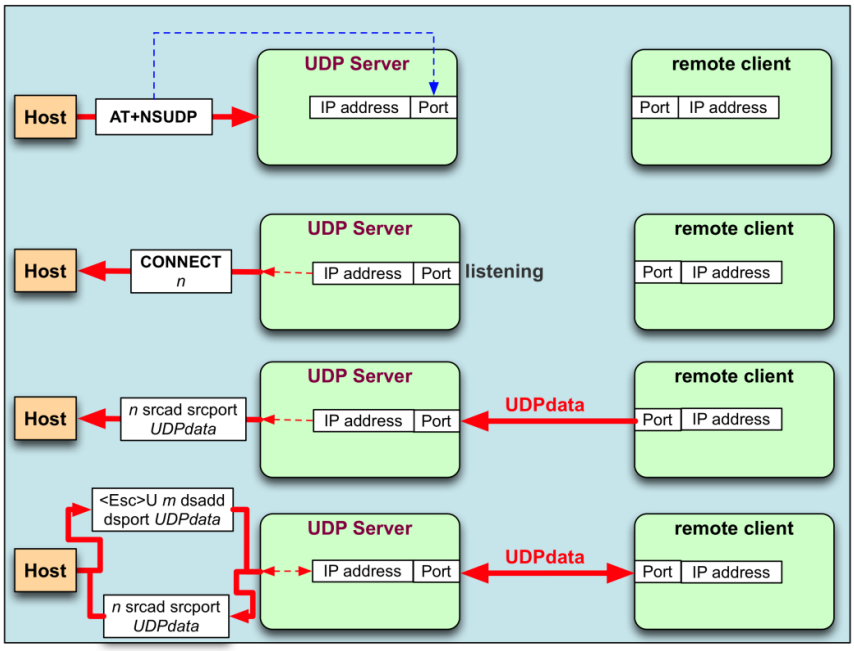


Figure 3.5.2.4

3.5.3 Profile Definition

The configuration parameter values that define the behavior of the adapter are grouped into profiles. These profiles are stored in non-volatile memory when not in use. The default configuration supports two profiles. The contents of a profile are listed in Table 3.5.3.1 below.

Parameter	Value	Reference
General Wireless Parameters		
802.11 Operating Mode	BBS, IBSS	4.6.6
Transmit Power Configuration		4.8.4
802.11 Transmit Retry Count		4.6.12
Power Save Mode	Enabled, Disabled	4.8.2
802.11 Radio Mode	Enabled, Disabled	4.8.1
Auto-connect Mode, Wireless Interface Settings		
802.11 Operating Mode	BSS, IBSS	4.13.1
Operating Channel	1 to 14	4.13.1
SSID Parameter	Any valid SSID	4.13.1
BSSID Parameter	Any valid BSSID	4.13.1
Maximum Scan Time		4.3
Auto-connect Mode, Network Interface Settings		
Mode	Server, Client	4.13.2
Protocol	TCP, UDP	4.13.2
Server Port Number	Any valid port	4.13.2
Server IP Address	Any valid IP address	4.13.2

Parameter	Value	Reference
Wireless Interface Security Configuration		
Authentication Mode	Open, Shared	4.7.1
PSK Valid	Valid, Invalid	
PSK-SSID	Any valid SSID, used for PSK key generation	
WEP Key Configuration		4.7.2
WPA Passphrase		4.7.3
TCP/IP Configuration		
DHCP Mode	Enabled, Disabled	4.9.2
IP Address	Valid IP address	4.9.3
Net Mask Address	Valid mask	4.9.3
Default Gateway Address	Valid IP address	4.9.3
DNS1	Valid DNS1 IP address	
DNS2	Valid DNS2 IP address	
UART Configuration		
Echo Mode	Enabled, Disabled	4.1.2
Verbose Mode	Enabled, Disabled	4.1.3
Bits per Character	5, 6, 7, or 8	4.2.1
Number of Stop Bits	1 or 2	4.2.1
Parity Type	None, Even, Odd	4.2.1
Software Flow Control Mode	Enabled, Disabled	4.2.2
Hardware Flow Control Mode	Enabled, Disabled	4.2.3
Baud Rate		4.2.1
Limits and Timeouts		
Network Connection Timeout	10 ms Units	4.3
Auto-association Timeout	10 ms Units	4.3
TCP Connection Timeout	10 ms Units	4.3

Association Retry Count	10 ms Units	4.3
Nagle Wait Time	10 ms Units	4.3

Table 3.5.3.1

3.5.4 Command Processing Mode

In command mode, the application receives commands over the serial port. Commands are processed line by line. Verbose Mode, when referring to commands being executing, refers to the displaying of status of any command executed in ASCII (human readable) format. When the verbose mode is disabled, the output will simply be in numeric digits, each digit indicating a particular status. Verbose Mode is enabled by default.

- If “echo” is enabled then each character is echoed back on the serial port
- Each command or response is on its own line, and then terminated with a carriage return <CR> and line feed <LF>, as <CRLF>
- If the characters “A” and “/” are entered at the beginning of a line (after <CRLF>), then the previous command is executed
- Once a complete line (ending with <CRLF>) is entered, the command contained therein is processed and an appropriate response returned

Unless otherwise specified, if verbose mode is enabled, then the response to a successful command is the characters “OK”. The response to an unsuccessful command is the word “ERROR”, followed by a detailed error message, if available. If verbose mode is disabled, command responses is numerical with OK having a value of 0 and error codes represented by positive integers. The commands are described in Section 4. Possible response codes are described in Section 3.17.3.

3.5.5 Auto-connection

If auto-connection is enabled, then at startup the adapter will:

- Attempt to associate with the specified network for a maximum time set by auto-associate timeout
- Upon association, attempt to establish a network connection based on specified parameters
- Upon successful connection, enter the pass-through auto-connect mode
- Upon failure enter the command processing state

In TCP client mode (Figure 3.5.5.1), the connection is considered established only when the client successfully connects to the server specified in the parameters. The client address may be fixed or obtained from a DHCP server. The client port is selected at random during creation of the client. The connection is attempted for a maximum time based on the Network Connection Timeout, specified in units of 10 ms (Section 4.3). Data is sent to and received from this server. If the connection is terminated, auto-connect mode also terminates and the command processing state is entered.

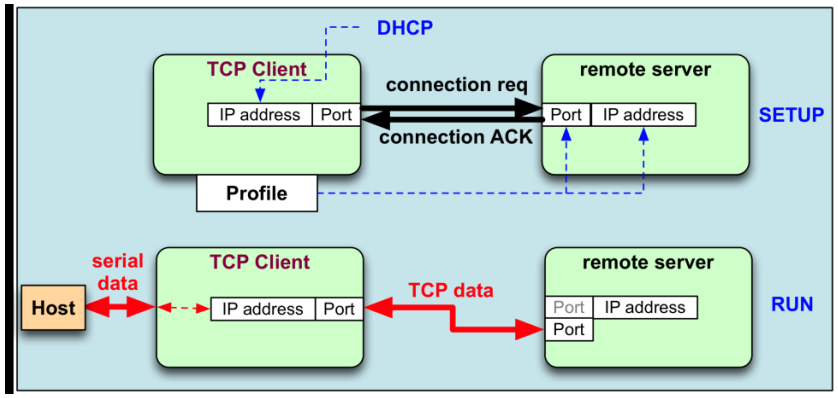


Figure 3.5.5.1

As shown in Figure 3.5.5.2, the TCP server IP address may be fixed in the profile or obtained from DHCP. The port for connection attempts to be made is obtained from the profile. In TCP server mode, the connection is considered established when the first client connects to the server. Data is sent to and received from this client. If the client disconnects, the adapter waits for the next client to connect.

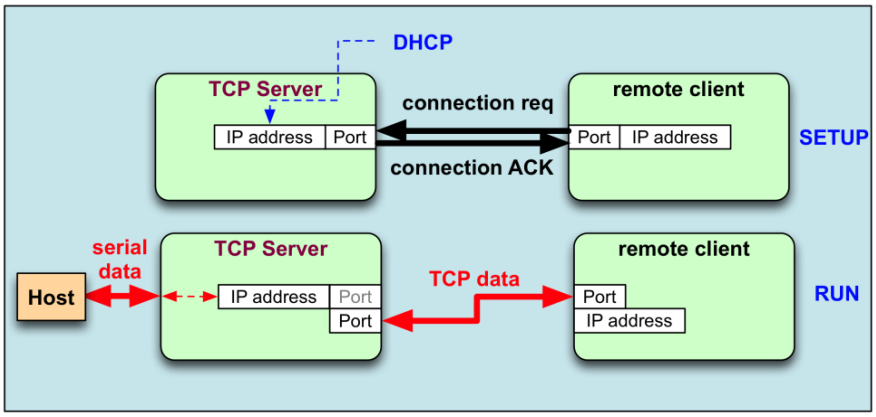


Figure 3.5.5.2

In UDP client mode, the connection is considered established when the client is created (Figure 3.5.5.3). The client IP address may be fixed or obtained from DHCP. The client port number is set at random upon creation of the client. Data is sent to and received from the configured server.

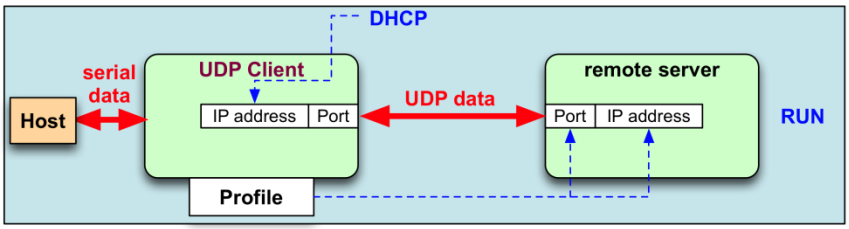


Figure 3.5.5.3

In UDP server mode, the connection is considered established when data is received from any client. The UDP server IP address may be fixed or obtained by DHCP as depicted in Figure 3.5.5.4. The port is set by the profile. Data received from any client is output on the serial port and data received on the serial port is transmitted to the client based on the last packet that was received.

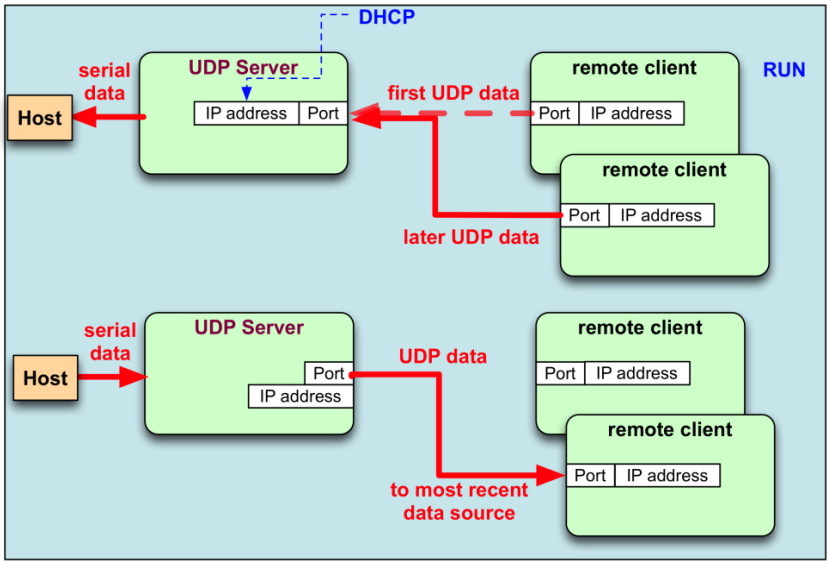


Figure 3.5.5.4

In TCP and UDP server mode, even where no connection is established, the serial host can take control of the Serial2WiFi interface by issuing a specific escape sequence.

3.6 Auto-connection Operation

Auto-connect mode acts as a cable replacement, as the interface acts like a serial interface and no commands or user intervention are required for connection management. The node automatically establishes the wireless and network connections by using parameter values from the current active profile and transfers data transparently between the host and target in data mode. No status information is sent to the host.

In auto-connection mode the adapter:

- Receives characters from the serial port and transmits them over the Wi-Fi connection
- Receives data from the Wi-Fi connection and transmits it on the serial port

The serial host may gain control of the interface by issuing the escape sequence “+++”, followed by a one-second gap where no characters are received on the serial port. When this sequence is encountered, the adapter exits auto-connection mode and resumes command processing. The host then may make changes in the network configuration or other parameters as needed. However, the adapter does not accept any new TCP/UDP client/server or auto-connection requests. The ATO command (terminated by the ASCII character “O”, not the number 0) is used to return to auto-connection mode.

In auto-connection mode, the Nagle Algorithm Wait Time (Section 3.18.7) can be used to buffer any characters to be sent, in order to avoid sending a large number of packets with small payloads onto the network. The wait time is specified in units of 10 ms. This functionality is available for both UDP and TCP connections.

3.7 Data Handling

In Data Processing Mode, data transfers are managed using various escape sequences. Each escape sequence starts with the ASCII character 27 (0x1B); this is equivalent to the ESC key. The encoding of data and related commands are described in the following pages. This encoding is used for both transmitted and received data.

The network destination, or destination source, for a given data packet is established by means of a Connection Identifier, and represented as a single hexadecimal number. Data is transferred on a per CID basis. Data is normally buffered until the end-of-data escape sequence is received. However, if the amount of data exceeds the size of the data buffer, the data thus far received is sent immediately. The data buffer size depends on the implementation, but is usually one MTU.

The process of sending a data packet is depicted in Figure 3.7.1. The sequence Esc S, Esc u or Esc U is sent to initiate the data transfer. This sequence is followed by a single-digit CID; if the CID is valid, the subsequent characters are assembled into a data stream, terminated by Esc E, Esc C, Esc S, Esc u or Esc U. With a terminating sequence, the data is sent via the requested network connection and the system either returns to command processing or to further data processing.

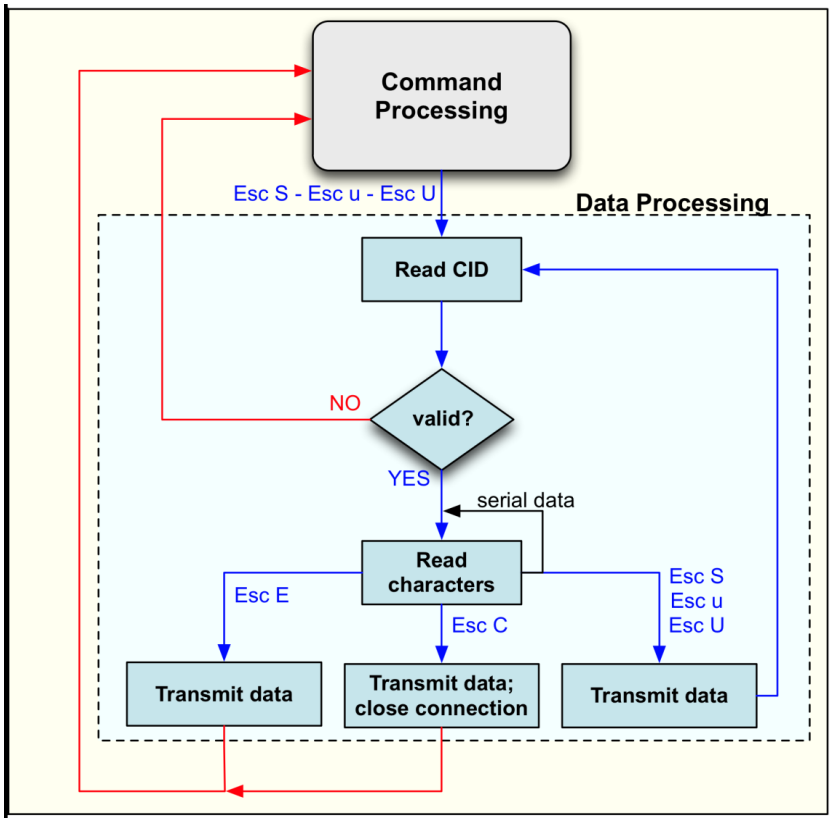


Figure 3.7.1

Operation	Escape Sequence	Description
Encode Sequence	<Esc><Esc> <Esc>S CID	This sequence is used to encode the escape character itself. This escape sequence selects the specified Connection ID as the current connection. This switches the connection to be used without exiting from the Data mode of operation. Use this sequence to send data from a TCP server, TCP client or UDP client (must be done before data can be received by that client). Example: <Esc>S10123456789<Esc>E where 1 is the UDP client CID and 012...9 is the data to be sent.
Send Sequence-Continuous	<Esc>U CID remote address: remote port:	This escape sequence is used when sending and receiving UDP data on a UDP server connection. When this command is used, the remote address and remote port is transmitted in ASCII text encoding and terminated with a ':' character. Example: <Esc>U4192.168.1.1:52:<data><Esc>E
Send Sequence-Complete	<Esc>u CID <remote address> <remote port> <Esc>E	This escape sequence is used when sending and receiving UDP data on a UDP server connection. When this command is used, the remote address and remote port is transmitted in binary encoding with the MSB being transmitted first. The following example shows the header to transmit a UDP packet using binary addressing taking up 9 bytes (d denoting decimal): <Esc>u4<192d><168d><1d><1d><0d><52d><data><Esc>E End-of-Data sequence indicates the end of a transmit frame, and start of transmission. The data received is sent on the network and the interface returns to Command mode.

Operation	Escape Sequence	Description
Send and Return to Command Mode Sequence	<Esc>C <Esc>O	This sequence causes transmission of the data received. After, the currently selected connection is closed and the interface returns to Command Mode. Any buffered data is sent before the connection is closed. "OK": This sequence is sent to the serial host by the Serial2WiFi Adapter upon successful completion of either the <Esc>S or <Esc>E commands.
Failure Indication	<Esc>F	"FAILURE": This sequence is sent to the host by the Serial2WiFi Adapter if an <Esc>S or <Esc>E command failed.

Operation	Escape Sequence	Description
Data Ignored Info	<Esc>xxx	If an unknown character 'xxx' is detected after an <Esc> character the <Esc> and the <xxx> character are ignored.
Software Flow Control	<Esc>Q <Esc>T	This sequence is used to encode a literal XON character to be transmitted when Software Flow Control is enabled. This sequence is used to encode a literal XOFF character to be transmitted when Software Flow Control is enabled. The contents of < > are either a byte or byte stream, except for <Esc>; literals outside brackets are ASCII characters.

Table 3.7.2

3.8 Raw Data Handling

In Raw Data Mode, data transfers are managed using escape sequences. Each escape sequence starts with the ASCII character 27 (0x1B), the equivalent to the ESC key. The encoding of data is described below. Encoding is used for both transmitted and received data. The Raw Ethernet Support Enable command (Section 3.18.20) must be issued before sending or receiving raw data through the adapter.

The format of a raw-data frame is:

<Esc>:R:<Length>:<DstAddr><SrcAddr><EtherType><Raw-Payload>

The contents of < > are a byte or byte stream.

- Length is the size of DstAddr, SrcAddr, EtherType and Raw-Payload
- DstAddr is the destination MAC address
- SrcAddr is the source MAC address
- EtherType is the type of the Ethernet packet. For example, for BACNET-over-Ethernet, EtherType is 0x0000.
- Raw-Payload is the raw data

3.9 Unsolicited Data Handling

In Unsolicited Data Mode (data transmission without association), data transfer is managed using escape sequences. Each escape sequence starts with the ASCII character 27 (0x1B), equivalent to the ESC key. The encoding of data is described below. This encoding is used for transmitted data only. The unsolicited data transmission enable command (Section 3.18.21) must be issued before sending unsolicited data through the adapter.

The format of an unsolicited data frame is:

<ESC>D/d<PayLoad>

Where <PayLoad> is a byte or byte stream.

3.10 Software Flow Control

Software flow control works only with ASCII data transfers and cannot be used for binary data.

If software flow control is enabled, and the interface receives an XOFF character from the serial host, it stops sending to the host until it receives an XON character. If the Adapter is receiving data over the wireless connection during the time that XOFF is enabled, it is possible for the wireless buffer to become full before XON is received. In such a case, data from the network will be lost.

If software flow control is enabled, then the interface sends an XOFF character to the host when it will be unable to service the serial port. The XON character is sent when the interface is once again able to accept data over the serial port.

Note: With initialization, the adapter treats the serial channel as clear with no restrictions on data transmission or reception; no explicit XON is transmitted by the adapter or required from the host, even if flow control is enabled.

3.11 Hardware Flow Control

If hardware flow control is enabled, an RTS/CTS handshake will occur between the serial host and the Adapter. If the receive buffers are full, the serial host is not ready to receive data, then subsequent incoming data is dropped.

3.12 Serial Data Handling

The Serial Data Handler receives and transmits data to and from the hardware serial controller. Data read from the serial port is passed to:

- The command processor in command mode
- The Tx data handler in data mode
- The auto-connection mode processor for data transfer in auto-connection mode

Then Data is transferred on the serial port from:

- The command processor in order to output responses to commands
- The Rx data handler in order to output incoming packets
- The auto-connection handler in order to output incoming data
- The connection manager in order to output status indications
- The wireless connection manager in order to output status indications

When configured in Auto-connection Mode, the adapter enters directly into Data Processing Mode after the completing the connection without sending any status information to the host.

3.13 Connection Management

The connection management module is responsible for processing connection-related events. The interface provides UDP and TCP sockets (similar to the familiar BSD network sockets). Each socket may represent either a server or client connection. Each connection has a unique, single-digit hexadecimal value (0 to 15), for the CID. The allowed maximum number of connections (up to 16) may be specified at compile time. Note that this single pool of CID's is used for TCP, UDP, Server and Client connections.

3.14 Packet Reception

When a packet is received on any open connection, and the application is not currently in auto-connect mode, the packet is transferred on the UART in the form described in Section 3.7 above. Received data payloads are encoded with the appropriate Escape sequence. The connection ID is used to inform the serial host of the origin of an IP data packet. The source IP address and port are provided along with the data when a UDP packet is received.

If auto-connect mode is enabled and a packet is received on the auto-connected CID, the packet data is sent without modification over the UART to the serial host.

3.15 Remote Close

If a TCP connection is terminated by disconnection from the remote end, an unsolicited ASCII-format response of the form DISCONNECT Connection ID is sent to the serial host, and the specified CID should be considered unavailable. If the connection ends because the remote server has shut down, the unsolicited response ERROR: SOCKET FAILURE Connection ID will be sent to the host. Note that a data packet from the remote client or server containing the same ASCII characters CLOSE Connection ID is treated as data rather than a command and forwarded to the serial host.

3.16 TCP Server Connections

Upon deployment of incoming TCP connections on a socket, the incoming connection is allowed if the limit on the maximum number of connections has not been reached. There is an unsolicited response of the form CONNECT <server cid> <new cid> <ip> <port>, where:

- server cid is the CID of the server where the connection has arrived
- new cid is the CID allocated for this client connections
- ip and port of the client encoded in the binary encoding used for UDP server data packets described in Section 3.4 above is sent to the serial host. The host can use the IP address to ascertain the source of the TCP connection request. The TCP server has no timeout limitation for an incoming connect request. It waits indefinitely, until a CLOSE command is received.

Note that if Verbose mode is disabled, the word CONNECT in the unsolicited response is replaced by the number 7.

3.17 Wireless Network Management

3.17.1 Scanning

The Serial2WiFi interface can instruct the Wi-Fi radio to scan for access points and ad hoc networks with a specified SSID, BSSID and/or channel for a specified scan time. Scanning can be performed to find networks with a specific SSID or BSSID, networks operating on a specific radio channel or a combination of these constraints.

3.17.2 Association

The Serial2WiFi interface performs all the actions required to join an infrastructure IP network:

- Scan for a specific AP (AT+WS, Section 3.18.15.5)
- Authenticate the specified network using the configured authentication mode (AT+WAUTH,
- Section 4.7)
- Associate to the AP (AT+WA, Section 4.6.7)
- Perform security negotiation if required
- Change state to Wireless Connected
- Initialize the networking stack using the configured static IP address or via DHCP (AT+NDHCP, Section 4.9.2)

In Ad Hoc mode, the interface can:

- Scan for a specified Ad Hoc Network
- Join the ad hoc network, if it exists
- If the ad hoc network does not exist, create a new ad hoc network to join
- Perform security negotiation, if required
- Change state to Wireless Connected
- Initialize the networking stack using the configured static IP address or via DHCP

3.17.3 Response Codes

The possible responses sent by the adapter to the serial host are enumerated in Table 4.

No	ASCII CHAR	Response	ASCII STRING	Meaning
1	0	S2W_SUCCESS	"OK"	Command Request Successful
2	1	S2W_FAILURE	"ERROR"	Command Request Failed
3	2	S2W_EINVAL	"ERROR: INVALID INPUT"	Invalid Command or Option or Parameter.
4	3	S2W_SOCK_FAIL	"ERROR: SOCKET FAILURE"	Socket Operation Failed
5	4	S2W_ENOCID	"ERROR: NO CID"	All allowed CID's in use, so there was no CID to assign to the new connection
6	5	S2W_EBADCID	"ERROR: INVALID CID"	Invalid Connection Identifier
7	6	S2W_ENOTSUP	"ERROR: NOT SUPPORTED"	Operation or Feature not supported.

No	ASCII CHAR	Response	ASCII STRING	Meaning
8	7	S2W_CON_SUCCESS	"\r\nCONNECT <CID>\r\n"	TCP/IP connection successful. <CID> equals the new CID in hexadecimal format.
9	8	S2W_ECIDCLOSE	"\r\nDISCONNECT <CID>\r\n"	TCP/IP connection with the given CID is closed. This response is sent to the host when a connection is closed either by the remote device or by the serial host.
10	9	S2W_LINK_LOST	"DISASSOCIATED"	Not associated to a wireless network.
11	A	S2W_DISASSO_EVT	"\r\nDisassociation Event\r\n"	Wireless network association lost.
12	B	S2W_STBY_TMR_EVT	"\n\rOut of StandBy-Timer\r\n"	Wake up from Standby due to RTC timer expiration.
13	C	S2W_STBY_ALM_EVT	"\n\rOut of StandBy-Alarm\r\n"	Wake up from Standby due to receipt of an Alarm signal.
14	D	S2W_DPSLEEP_EVT	"\r\nOut of Deep Sleep\r\n"	Wake from Deep Sleep
15	E	S2W_ENOIP	"ERROR: IP CONFIG FAIL"	IP configuration has failed

Table 3.17.3.1

3.18 Commands for Command Processing Mode

This section provides a list of Serial2WiFi commands and their effects. Formatting and processing of commands was described in Section 3.2 above. Parameters are generally ASCII characters. For example, ATEn with n=1 is thE-series of ASCII characters ‘A’, ‘T’, ‘E’, and ‘1’. Where some parameters are optional, mandatory parameters are denoted by < > and optional parameters by [ ]. If a parameter is mandatory, any associated sub-parameters are also mandatory; sub-parameters of an optional parameter are optional. Parameters must always be provided in the order given in the command description. When an optional parameter is not supplied, the comma delimiters must still be included in the command. Every command starts with the characters “AT”; any other initial characters will cause an error to be returned.

Command Response - in most cases, valid commands return the characters OK if verbose mode is enabled and 0 verbose mode is not enabled. Invalid inputs return ERROR: INVALID INPUT if verbose is enabled and 2 if it is not. Exceptions to this rule are noted explicitly below.

3.18.1 Command Interface

3.18.2 Interface Verification

The command AT can be issued to verify that the interface is operating correctly; it should return a successful response OK (or 0 if verbose mode is disabled).

3.18.3 Echo

The command to enable/disable echo is:

ATEn

If n is 0, echo is disabled and if n is 1, echo is enabled. If echo is enabled, every character received on the serial port is transmitted back on the serial port.

3.18.4 Verbose

The command to enable/disable verbose responses is:

ATVn

If n is 0, verbose responses is disabled and if n is 1, verbose responses is enabled. If verbose mode is disabled, the status response is in the form of numerical response codes. If verbose mode is enabled, the status response is in the form of ASCII strings. Verbose Mode is enabled by default.

3.18.5 Help

The command to display help is:

AT?

Upon deployment of this command, a list of all supported commands is output along with a brief one-line description of each command's functionality, followed by the standard status code OK or 0, as applicable.

3.18.6 UART Interface Configuration

3.18.6.1 UART Parameters

The command to set the UART communication parameters is:

ATB=<baudrate>[[,<bitsperchar>][,<parity>][,<stopbits>]]

All standard baud rates are supported. Allowed baud rates include: 9600, 19200, 38400, 57600, 115200, 230400, 460800 and 921600. Parity is n for no parity, e for even parity and o for odd parity. Allowed values are 5, 6, 7 or 8 bits/character, with 1 or 2 stop bits (1.5 in the case of a 5-bit character).

The new UART parameters take effect immediately. However, they are stored in RAM and will be lost when power is lost unless they are saved to a profile using AT&W (Section 4.5.1). The profile used in that command must also be set as the power-on profile using AT&Y (Section 3.18.12).

3.18.6.2 Software Flow Control

The command to configure software flow control is:

AT&Kn

If n is 0 for software flow control to be disabled and if n is 1 for software flow control to be enabled. The use of software flow control is described in Section 3.10 above.

3.18.6.3 Hardware Flow Control

The command to configure hardware flow control is:

AT&Rn

If n is 0, hardware flow control is disabled. If n is 1, hardware flow control is enabled.

3.18.7 Serial to Wi-Fi Configuration

The command to configure network and connection parameters is:

ATSn=p

where n is the parameter id to set and p is the value to set the parameter to. The parameters available are described in Table 3.18.7.1.

Parameter ID	Name	Description	Citation
0	Network Connection Timeout	The maximum amount of time allowed establishing the network connection in Auto-connect Mode. Measured in units of 10 ms. Allowed values: 1 to 65535 (but the TCP/IP stack limits the maximum timeout value). Default value: 1000 (10 seconds). If the connection attempt is a TCP client connection, and TCP Connection Timeout below is less than Network Connection Timeout, the value of Network Connection Timeout will be ignored.	
1	Auto-associate Timeout	The maximum amount of time allowed associating to the desired wireless network in Auto-connect Mode, in units of 10 ms. Allowed values: 0 to 65535. Default value: 500 (5 seconds).	
2	TCP Connection Timeout	The maximum amount of time allowed establishing a TCP client connection, in units of 10 ms. Allowed values: 0 to 65535 (but the TCP/IP stack limits the maximum timeout value). Default value: 500 (5 seconds). Note that 0 corresponds to the default TCP/IP stack timeout (75 seconds).	4.10.1
3	Association Retry Count	Not currently supported.	
4	Nagle Algorithm Wait Time	The maximum time for serial data sent in Auto-connect Mode to be buffered, in units of 10 ms. Allowed values: 0 to 65535 (but the amount of data is limited by available buffer size). Default value: 10 (100 ms).	3.3.1
5	Scan Time	The maximum time for scanning in one radio channel, in units of ms. Allowed values: 0 to 65535 (but at the high limit a 14-channel scan will consume 2.6 hours!). Default value: 20 (20 ms).	3.7.1

Table 3.18.7.1

3.18.8 Identification Information

The command to obtain identification information from the application is:

ATIn

where n is the ID of the information to obtain. The responses are listed in Table 3.18.8.1. These responses are provided as ASCII strings.

Information ID	Description
0	OEM identification
1	Hardware version
2	Software version

Table 3.18.8.1

3.18.9 Serial to Wi-Fi Configuration Profiles

Adapter configuration parameters can be stored and recalled as a profile.

3.18.10 Save Profile

The command to save the current profile is:

AT&Wn

where n shall either be 0 for profile 0 or 1 for profile 1. Higher values are allowed if more profiles are configured at compile time. Upon deployment of this command, the current configuration settings are stored in non-volatile memory under the specified profile. Note that, in order to ensure that these parameters are restored after power cycling the adapter, the command AT&Y (Section 3.18.12) must also be issued, using the same profile number selected here.

3.18.11 Load Profile

The command to load a profile is:

ATZn

where n shall either be 0 for profile 0 or 1 for profile 1. Higher values are allowed if more profiles are configured at compile time. Upon deployment of this command, the currently configured settings are set to those stored in non-volatile memory under the specified profile.

3.18.12 Selection of Default Profile

The command to select the default profile is:

AT&Yn

n shall either be 0 for profile 0 or 1 for profile 1. Higher values are allowed if more profiles are configured at compile time. The settings from the profile that is chosen as the default profile are loaded from non-volatile memory when the device is started. In addition to the standard status responses, this command returns ERROR or 1, based on verbose settings, if a valid input cannot be executed.

3.18.13 Restore to Factory Defaults

The command to reset to factory defaults is:

AT&F

Upon deployment of this command, the current configuration variables are reset to the factory defaults. These defaults are defined by macro values in the configuration header, and can be modified at compile time. Issuing this command resets essentially all configuration variables except the IEEE MAC address. Only the command AT+NMAC changes the MAC address.

3.18.14 Output Current Configuration

The command to output the configuration is:

AT&V

Upon deployment of this command, the current configuration and the configuration of the saved profiles are output on the serial port in ASCII format.

3.18.15 Wi-Fi Interface Configuration

3.18.15.1 MAC Address Configuration

The command to set the configuration is:

AT+NMAC=<MAC ADDRESS>

Upon deployment of this command, the adapter sets the IEEE MAC address as specified. The format of the MAC address is an 6-byte colon-delimited hexadecimal number. An example is shown below:

AT+NMAC=00:1d:c9:00:01:a2

The MAC address is used in the 802.11 protocol to identify the various nodes communicating with an Access Point and to route messages within the local area (layer 2) network. Fixed MAC addresses issued to network interfaces are hierarchically structured and are intended to be globally unique. Before issuing a MAC address to a given adapter, ensure that no other local device is using that address. The MAC address supplied in the AT+NMAC command is saved to flash memory, and will be used on each subsequent cold boot (from power off) or warm boot (from Standby).

The alternative command:

AT+NMAC2=<MAC ADDRESS>

stores the MAC address in RTC RAM. Each warm boot (from Standby) will use the MAC address stored in RTC RAM (from the most recent AT+NMAC2= command), but if power to the device is lost, the next cold boot will use the MAC address stored in flash memory (from the most recent AT+NMAC= command). This command is particularly useful in cases where writing to flash memory is undesirable.

3.18.15.2 Output MAC Address

The command to output the configuration is:

AT+NMAC=?

Upon deployment of the command, the adapter outputs the current MAC address of the wireless interface to the serial port, in addition to the usual status responses.

The alternate command is:

AT+NMAC2=?

may also be used, and returns the same value.

3.18.15.3 Regulatory Domain Configuration

The command to set the regulatory domain is

AT+WREGDOMAIN=<Regulatory Domain>

This command sets the regulatory domain as per the Regulatory Domain parameter passed. The supported regulatory domains are:

- FCC - supported Channel range is 1 to 11
- ETSI - supported Channel range is 1 to 13
- TELEC - supported Channel range is 1 to 14

The corresponding values for this regulatory domain that needs to be passed as the parameter are:

- FCC - 0
- ETSI - 1
- TELEC - 2

The default regulatory domain is FCC. The Regulatory domain set is required only once since it is being updated in the flash.

3.18.15.4 Regulatory Domain Information

The command to get the configured regulatory domain in the Serial2WiFi adaptor is:

AT+WREGDOMAIN=?

Upon reception of the command, the adapter outputs the current regulatory domain of the wireless interface to the serial port as the following format:

REG_DOMAIN=FCC or ETSI or TELEC, in addition to the usual status responses.

3.18.15.5 Scanning

The command to scan for access points or ad hoc networks is:

AT+WS[=<SSID>[,<BSSID>][,<Channel>][,<Scan Time>]]

Upon deployment of the command, the adapter scans for networks with the specified parameters, and displays the results. Scanning can be performed to find networks with specific SSID or specific BSSID or in a particular operating channel, or a combination of these parameters. Scanning for a specific SSID or BSSID employs active scanning, in which probe requests are transmitted with the SSID and/or BSSID

fields being filled appropriately. Upon completion, the adapter reports the list of networks and information about each found network is displayed, one per line, in the following format.

The Scan Time is units of ms and the range is 0-65535.

<SSID>,<BSSID>,<Channel>,<RSSI>,<Mode>,<Security>

Mode is INFRA for an infrastructure network and ADHOC for an ad hoc network.

3.18.15.6 Mode

The command to set the wireless mode:

AT+WM=n

If n is 0, the mode is set to infrastructure; if n is 1, the mode is set to ad hoc.

3.18.15.7 Associate with a Network, or Start an Ad Hoc Network

The command to associate to an access point, to join an ad hoc network or to create an ad hoc network is:

AT+WA=<SSID>[,[<BSSID>][,<Ch>]]

In infrastructure mode, the adapter will attempt to associate with the requested network. In ad hoc mode, if a network with the desired SSID or channel or both is not found, then a new network is created. However, if the BSSID was specified in the request and the applicable BSSID is not found, the adapter will report an error and will not create an ad hoc network. In addition to the usual status responses, this command will return ERROR or 1 (depending on verbose status) if a valid command was issued but association failed.

3.18.15.8 Disassociation

The command to disassociate is:

AT+WD

An equivalent command is:

ATH

Upon deployment of this command, the interface disassociates from the current infrastructure or ad hoc network, if associated.

3.18.15.9 Status

The command to retrieve information about the current network is:

AT+NSTAT=?

Upon deployment of this command, the adapter reports the current network configuration to the serial host:

- MAC address;
- WLAN state;
- SSID;

- Mode;
- Security;
- Channel;
- BSSID;
- Network configuration: IP Address, Subnet mask, Gateway address, DNS1 address, DNS2 address;
- TX count;
- RX count;
- RSSI value

in addition to the usual status response.

The alternate command:

AT+WSTATUS

may also be used. Upon deployment of this command, the adapter reports the current network configuration to the serial host:

- Mode;
- Channel;
- SSID;
- BSSID;
- Security;

if the adaptor associated to an access point. If no association is present, the error message NOT ASSOCIATED is returned, in addition to the usual status response.

3.18.15.10 Get RSSI

The command obtains the current RSSI is:

AT+WRSSI=?

Upon deployment of this command, the current RSSI value (in dBm) is output on the serial port in ASCII format, in addition to the status response.

3.18.15.11 Get Transmit Rate

The command obtains the current transmit rate is:

AT+WRATE=?

Upon deployment of this command, the current transmit rate used is output on the serial port in ASCII format.

3.18.15.12 Set Retry count

The command to set the wireless retry count is:

AT+WRETRY=<retrycount>

Upon deployment of this command, the current wireless retry count is set to the supplied value. The transmission retry count determines the maximum number of times a data packet is retransmitted, if an 802.11 ACK is not received. Note that the count includes the initial transmission attempt. The valid range is 4 to 7.

3.18.16 Wi-Fi Security Configuration

3.18.16.1 Authentication Mode

The command to choose the authentication mode to use is:

AT+WAUTH=n

where n is:

- 0 - None
- 1 - Open
- 2 - Shared with WEP

Note that this command configures the authentication mode, but any required encryption keys must be set using the key commands described below. This authentication mode command is specific to WEP encryption; if WPA/WPA2 operation is employed, the authentication mode may be left at the default value " None".

3.18.16.2 WEP Keys

The command to set WEP keys is:

AT+WWEPn=<key>

where n is the key index, between 1 and 4, and key is either 10 or 26 hexadecimal digits corresponding to a 40-bit or 104-bit key.

Some examples:

AT+WWEP1=123456abdc

AT+WWEP3=abcdef12345678901234567890

Upon receiving a valid command, the relevant WEP key is set to the value provided.

3.18.16.3 WPA-PSK and WPA2-PSK Passphrase

The command to set the WPA-PSK and WPA2-PSK passphrase is:

AT+WWPA=<passphrase>

The passphrase is a string containing between 8 and 63 ASCII characters, used as a seed to create the WPA pre-shared key (PSK). Upon receiving the command, the PSK passphrase is reset to the value provided.

3.18.16.4 WPA-PSK and WPA2-PSK KEY CALCULATION

Computation of the PSK from the passphrase is complex and consumes substantial amounts of time and energy. To avoid recalculating this quantity every time the adapter associates, the adapter provides the capability to compute the PSK once and store the resulting value. The key value is stored in the SRAM copy of the current profile; the profile needs to be saved in flash memory for this value to persist during a transition to Standby. The command to compute and store the value of the WPA/WPA2 PSK, derived from the passphrase and SSID value, is:

AT+WPAPSK=<SSID>,<PASSPHRASE>

The passphrase is a string containing between 8 and 63 ASCII characters, used as a seed to create the PSK. The SSID is a string of between 1 and 32 ASCII characters. When the command is issued, the adapter immediately responds with Computing PSK from SSID and PassPhrase. Computation of the passphrase can be time-consuming! When it is complete, the adapter will issue the usual OK or 0. Invalid inputs will result in ERROR: INVALID INPUT or 2, as usual.

Upon receiving the command, the adapter computes the PSK from the SSID and passphrase provided, and stores those values in the current profile. The current profile parameters PSK Valid, PSK-SSID, and WPA Passphrase are updated, and can be queried with AT&V (Section 4.5.5). The next time the adapter associates to the given SSID, the PSK value is used without being recalculated. After the PSK has been computed, the commands AT&W (to save the relevant profile) and AT&Y (to ensure that the profile containing the new PSK is the default profile) should be issued. The PSK will then be available when the adapter awakens from Standby.

3.18.16.5 WPA-PSK and WPA2-PSK KEY

The command to configure the WPA / WPA2 PSK key directly is:

AT+WPSK=<PSK>

This command directly sets the pre-shared key as provided. The argument is a 32-byte key, formatted as an ASCII hexadecimal number; any other length or format is considered invalid.

Example:

AT+WPSK= 0001020304050607080900010203040506070809000102030405060708090001

After the PSK has been entered, the commands AT&W (to save the relevant profile) and AT&Y (to ensure that the profile containing the new PSK is the default profile) should be issued. The PSK will then be available when the adapter awakens from Standby.

3.18.16.6 EAP-Configuration

The command to configure the EAP-security is:

AT+ WEAPCONF=<Outer Authentication>,<Inner Authentication>,<user name>,<password>

Upon execution of this command, the adaptor set the Outer authentication, Inner authentication, user name and password for EAP Security. This command returns the normal response codes.

The valid outer authentication values are:

Eap-FAST: 43

Eap-TLS: 13

Eap-TTLS: 21

Eap-PEAP: 25

The valid Inner Authentication values are:

Eap-MSCHAP: 26

Eap-GTC: 6

3.18.16.7 EAP

The command to configure certificate for EAP-TLS is:

AT+ WEAP=< Type >,< Format >,< Size >,< Location ><ESC>W <data of size above>

- Type: CA certificate(0)/ Client certificate(1)/ Private Key(2)
- Format: Binary(0)/Hex(1)
- Size: size of the file to be transferred.
- Location: Flash(0)/Ram(1)

This command enables the adaptor to receive the certificate for EAP-TLS. This command stores the certificate in flash or RAM, depending on the parameter.

3.18.17 Wireless MAC and Radio Configuration

3.18.17.1 Enable/Disable 802.11 Radio

The command to enable or disable the radio is:

AT+WRXACTIVE=n

If n is 0, the radio is disabled; if n is 1, the radio is enabled.

If WRXACTIVE = 1, the 802.11 radio receiver is always on. This minimizes latency and ensures that packets are received at the cost of increased power consumption. The RFM module cannot enter Deep Sleep (Section 4.12.1) even if it is enabled (PSDPSLEEP=1). Power Save mode can be enabled but will not save power, since the receiver is left on.

If WRXACTIVE = 0, the receiver is switched off after association is complete. If Power Save mode is not enabled (WRXPS not issued or WRXPS=0), the receiver will not be turned on again unless WRXACTIVE = 1 is received. Packets will not be received, and disassociation could occur. If Power Save mode is enabled (WRXPS=1) prior to issuing WRXACTIVE = 0, the receiver will be turned off, but will turn on again when it is time to listen for the next beacon from the access point. If Deep Sleep is also enabled, the receiver will turn off, and the module will enter Deep Sleep when all pending tasks are completed, but again the system will be awakened to listen to the next beacon. If a transition to Standby is requested and occurs (Section 4.12.2), the module will remain in Standby for the requested period, and will not awaken to receive a beacon during that time.

3.18.17.2 Enable/Disable 802.11 Power Save Mode

The command to configure 802.11 Power Save Mode is:

AT+WRXPS=n

If n is 0 Power Save is disabled, and if n is 1 Power Save is enabled.

In 802.11 Power Save Mode, the node (in this case, the Serial2WiFi Adapter) will inform the access point that it will become inactive, and the access point will buffer any packets addressed to that node. In this case, the module receiver is turned off between beacons. The node will awaken to listen to periodic beacons from the access point, that contain a Traffic Indication Map (TIM) that will inform the station if packets are waiting for it. Buffered packets can be retrieved at that time, using PSPoll commands sent by the node. In this fashion, power consumed by the radio is reduced (although the benefit obtained depends on traffic load and beacon timing), at the cost of some latency.

The latency encountered depends in part on the timing of beacons, set by the Access Point configuration. Many Access Points default to 100 ms between beacons; in most cases this parameter can be adjusted.

3.18.17.3 Enable/Disable Multicast Reception

The command to configure multicast reception is:

AT+MCSTSET=n

If n = 0 multicast reception is disabled; if n = 1 multicast reception is enabled.

3.18.17.4 Transmit power

The command to set the transmit power is:

AT+WP=<power>

On reception of this command, the transmit power is set to the supplied value. The desired power level shall be specified in ASCII decimal format. The value of the parameter can range from 0 to 7 for internal PA GS101x, with a default value of 0 and from 2 to 15 for external PA GS101x, with default value of 2.

3.18.17.5 Sync Loss Interval

The command to configure the sync loss interval is:

AT+WSYNCINTRL=<n>

On execution of this command the adaptor set the sync loss interval for n times the beacon interval so that if the adaptor does not receive the beacon for this time it informs the user this event as “Dissociation event”. The default value of sync loss interval is 30. This command accept the sync loss interval from 1 to 65535.

3.18.17.6 Association Keep Alive Timer

The command to configure the keep-alive timer interval is:

AT+PSPOLLINTRL=<n>

On execution of this command, the adaptor will set the keep-alive time interval for n seconds. This keep-alive timer will fire for every n seconds once the adaptors associated. This timer will keep the adaptor in associated state even there is no activity between AP and adaptor. The default vale is 45 seconds. This command accepts keep-alive timer interval from 0 to 65535 seconds. The value 0 disables this timer.

3.18.18 Network Interface

3.18.18.1 Network Parameters

Note that IP addresses in the network commands are to be given in ASCII dotted-decimal format.

3.18.18.2 DHCP Support

The command to enable or disable DHCP is:

AT+NDHCP=n

If n is 0 DHCP is disabled and if n is 1 DHCP is enabled.

If the interface is associated with a network, enabling DHCP will cause an attempt to obtain an IP address using DHCP from that network. Thus issuing this command with n=1 will cause the adapter to attempt to refresh an existing DHCP address. If the adapter is not associated when the command is received, future associations will attempt to employ DHCP. If the adapter fails to obtain an address via DHCP it will return an error response ERROR: IP CONFIG FAIL if verbose is enabled, or F(0x0F) if verbose is disabled

3.18.18.3 Static Configuration of Network Parameters

The command to statically configure the network parameters is:

AT+NSET=<Src Address>,<Net-mask>,<Gateway>

Upon deployment of this command, any previously-specified network parameters are overridden, and the adapter is configured to use the newly-specified network parameters for the current association, if associated, and for any future association. The use of DHCP is disabled if the network parameters are configured statically. The DNS address can be set using AT+DNSSET (Section 4.9.5).

3.18.18.4 DNS Lookup

The command to get an IP address from a host name is:

AT+DNSLOOKUP=<URL>, [<RETRY>, <TIMEOUT-S>]

where URL is the hostname to be identified. Upon deployment of this command, the adapter queries the DNS server to obtain the IP address corresponding to the hostname provided in URL, and returns the address if found. Retry and timeout are optional; if they are not given, or if 0 values are provided, the default value of 2 is used. Timeout is in seconds.

3.18.18.5 Static Configuration of DNS

The command to statically configure the DNS IP addresses is:

AT+DNSSET=<DNS1 IP>, [<DNS2 IP>]

This command sets the values of the DNS server addresses to be used by the adapter. The second address,
DNS2 IP, is optional.

3.18.18.6 Store Network Context

The command to store the network context and configuration prior to a transition to Standby is:

AT+STORENWCONN

This command will preserve network connection parameters (layer 2 and layer 3 information) in non-volatile memory when the module is sent to Standby mode using the Request Standby command (Section 4.12.2). Note that CID's are lost when the transition to Standby occurs.

3.18.18.7 Restore Network Context

The command to recover a saved network context is:

AT+RESTORENWCONN

This command reads the layer 3 (IP) network connection parameters saved by Store Network Context (Section 4.9.6), and reestablishes the connection that existed before the transition to Standby. If needed, the node will re-associate and re-authenticate with the specified SSID. In addition to the usual status responses, this command returns ERROR or 1 (based on verbose setting) is it is called prior to storing the network connection, or after storing the network connection but before a transition to Standby has occurred.

3.18.19 Connection Management Configuration

All connection commands, except for the transport of Raw Ethernet data (), use the embedded TCP/IP Network Stack functions to perform the required actions. Connection identifiers, denoted as <CID> below, are to be sent as single hexadecimal characters in ASCII format.

3.18.19.1 TCP Clients

The command to open a TCP client connection is be:

AT+NCTCP=<Dest-Address>,<Port>

Upon deployment of this command, the interface attempts to open a socket and connect to the specified address and port. The connection attempt shall timeout if a socket has not been opened after a delay equal to TCP Connection Timeout. On successful connection, the interface sends CONNECT <CID> to the serial host, where CID is the newly allocated connection identifier. ERROR or 1 is returned if a timeout occurs.

3.18.19.2 UDP Clients

The command to open a UDP client connection is be:

AT+NCUDP=<Dest-Address>,<Port>>[<,Src.Port>]

Upon deployment of this command, the interface opens a UDP socket capable of sending data to the specified destination address and port. If a source port is provided, the socket will bind to the specified port. On successful completion, the interface sends CONNECT <CID> to the serial host, where CID is the newly allocated connection identifier.

3.18.19.3 TCP Servers

The command to start a TCP server is:

AT+NSTCP=<Port>

Upon deployment of this command, the interface opens a socket on the specified port and listens for connections. On successful creation of the server, CONNECT <CID> is sent to the serial host, where CID is the newly allocated connection identifier, followed by OK or 0. Up to 16 total CID's can be supported by the application, so a TCP server can support up to 15 distinct client connections, if no other entity has assigned CID's.

3.18.19.4 UDP Servers

The command to start a UDP server is:

AT+NSUDP=<Port>

Upon deployment of this command, the interface:

- Allocates a CID for this connection. If no CID is available, the command fails.
- If a valid CID was allocated, a UDP socket is opened on the specified port.
- If the socket is successfully created, CONNECT <CID> is sent to the serial host, where CID is the allocated connection identifier.

3.18.19.5 Output Connections

The command to output the current CID configuration is:

AT+CID=?

This command returns the current CID configuration for all existing CID's:

- CID number;
- CID type;
- Protocol;
- Local port;
- Remote port;
- Remote IP address

followed by the usual status response. If no valid CID's are present, the message No valid CIDs is sent, followed by OK or 0.

3.18.19.6 Closing a Connection

The command to close a connection is:

AT+NCLOSE=<cid>

Upon deployment of this command, the connection associated with the specified CID is closed, if it is currently open. On completion of this command the CID is free for use in future connections. If an invalid CID is provided, the command returns ERROR: INVALID CID or 5, depending on verbose status.

3.18.19.7 Closing All Connections

The command to close all connections is:

AT+NCLOSEALL

Upon execution of this command, all open connections are closed.

3.18.19.8 SOCKET Options Configuration

The command to configure a socket which is identified by a CID is:

AT+SETSOCKOPT=<CID>,<Type>,<Parameter>,<Value>,<Length>

Upon execution of this command the adaptor configure the socket identified by CID with the value passed.

CID - the socket identifier received after opening a connection.

Type - the type of the option to be set.

- SOCKET: 65535
- IP: 0
- TCP: 6

Parameter - the option name to be set; accepts hex values.

TCP_MAXRT: 10(Hex)
TCP_KEEPALIVE: 4001(Hex)

Value - the value to be set. This in seconds. Example: 30 = 30 seconds.

Length - the length of the value in bytes. Example: in above case it is 4.

Example: to set the TCP retransmission timeout to 20 seconds send AT+SETSOCKOPT=6,10,20,4

3.18.20 Enable/Disable Raw Ethernet Support

The command to enable or disable support of Raw Ethernet data is:

AT+NRAW=<0|1|2>

The results of this command are summarized in Table 3.18.20.1:

Information ID	Description
0	Disable Raw Ethernet frame transmission / reception.
1	Enable Raw Ethernet frames with NON-SNAP 802.2LLC headers.
2	Enable all Raw Ethernet frames.

Table 3.18.20.1

When selection 1 is chosen, 802.3 frames are presumed to include an 802.2 header which is not a SNAP header. These frames are used, for example, for sending BACNET data over Ethernet. A frame of this type has the format:

<ESC>R:<Length>:<DstAddr><SrcAddr>0x0000<Raw-Payload>

When selection 2 is chosen, the 802.2 header (presumed to be a SNAP header) is removed, and a raw Ethernet II frame payload is expected, as per the format below:

<ESC>R:<Length>:<DstAddr><SrcAddr><EtherType><Raw-Payload>

This frame format is used for sending IP data over BACNET. Length is size of DstAddr, SrcAddr, Ether-Type and Payload.

If the adaptor receives DATA Frames, where the 802.2 LLC headers. SSAP and DSAP are not both 0xAA, these frames are presumed to be 802.3 frames, and are sent to the module's serial port as described above.

If the Adaptor received DATA Frames with UDP port range 0xBAC0 to 0xBACF, they are presumed to be BACNET/IP frames, BacNet Ip frame, and are sent to the module's serial port as described above.

3.18.21 Unsolicited Data Transmission

The adaptor supports unsolicited data transmission (data transmission without association). The Command to enable this is:

AT+UNSOLICITEDTX=<Frame Control>,<Sequence Control>,<Channel>,<Rate>,<WmmInfo>,

<Receiver Mac>,<Bssid of AP>,<Frame Length>

This command enables the unsolicited data transmission with the parameters configured. After issuing this command, the user needs to send the payload data as following:

<ESC>D/d <PayLoad of the above Frame length>

Frame Control - the 802.11 frame control field.
Sequence Control - the seq number of the frame.
Channel - the channel on which the data to be sent.

Rate - the rate at which the data to be send and the possible values are:

RATE_1MBPS = 2,

RATE_2MBPS = 4,

RATE_5_5MBPS = 11,

RATE_11MBPS = 22

WmmInfo - the wmm information to be sent.
Receiver Mac - the remote mac address of the frame to be sent.
Bssid - bssid of the AP.
Frame Length - the length of the payload. The maximum size of the frame is limited to 1400 bytes.

3.18.22 BATTERY CHECK

3.18.22.1 Battery Check Start

The command to initiate battery checking is:

AT+BCHKSTRT=<Batt.chk.freq>

The valid range for the parameter Batt.chk.freq is between 1 and 100. Upon deployment of this command, the adapter performs a check of the battery voltage each Batt.chk.freq number of sent packets, and stores the resulting value in nonvolatile memory. Only the most recent value is stored. Note that battery checks are performed during packet transmission to ensure that they reflect loaded conditions. Battery checks can be used to ensure that a battery-powered system is provided with sufficient voltage for normal operation. Low supply voltages can result in data corruption when profile data is written to flash memory.

3.18.22.2 Battery Warning/Standby Level Set

The command to set the battery warning/standby level to enable the adaptor's internal battery measuring logic:

AT+ BATTLVLSET=<Warning Level>,<Warning Freq>,<Standby Level>

Upon execution of this command the adaptor's internal battery level monitoring logic starts. This command should be executed before the battery check start command (Section **xxx**).

Warning Level - if the battery voltage, in mV, is low the adaptor sends the message "Battery Low" to the serial interface.

Warning Freq - the frequency at which the adaptor sends the "Battery Low" message to the serial interface once the adaptor's battery check detected low battery.

Standby Level - when the battery voltage, in mV, reaches this level the adaptor sends the message "Battery Dead" to the serial interface and goes to long standby.

3.18.22.3 Battery Check Set

The command to set/reset the battery check period after battery check has been started is:

AT+BCHK=< Batt.chk.freq >

The valid range for the parameter Batt.chk.freq is between 1 and 100. Upon receipt, the adapter records the new value of the battery check frequency. The same command can be used to get the current configured battery check period, the usage as follows:

AT+BCHK=?

3.18.22.4 Battery Check Stop

The command to stop checking the battery state is:

AT+BCHKSTOP

Upon deployment of this command, battery check is halted.

3.18.22.5 Battery Value Get

The command to retrieve the results of battery check operations is:

AT+BATTVALGET

This command should return a message with the latest value, e.g., Battery Value: 3.4 V, followed by the usual status message. If this command is issued before issuing the command to start battery checks, it returns ERROR or 1, depending on the current verbose setting.

3.18.23 Power State Management

3.18.23.1 Enable/Disable SOC Deep Sleep

The command to enable the RFM adaptor module's power-saving Deep Sleep processor mode is:

AT+PSDPSLEEP

When enabled, the SOC will enter the power-saving Deep Sleep mode when no actions are pending. In Deep Sleep mode, the processor clock is turned off, and SOC power consumption is reduced to less than 1 mW (about 0.1 mA at 1.8 V). Note that other components external to the SOC may continue to dissipate power during this time, unless measures are taken to ensure that they are also off or disabled.

The processor can be awakened by sending data on the serial port. However, several milliseconds are required to stabilize the clock oscillator when the system awakens from Deep Sleep. Since the clock oscillator must stabilize before data can be read, the initial data will not be received; "dummy" (discardable) characters or commands should be sent until an indication is received from the application.

3.18.23.2 Request Standby Mode

The command to request a transition to ultra-low-power Standby operation is:

AT+PSSTBY=x[,<DELAY TIME>,<ALARM1 POL>,<ALARM2 POL>]

The parameters are:

- x is the Standby time in ms. If a delay time (see below) is provided, the Standby count begins after the delay time has expired.
- DELAY TIME is the delay in ms from the time the command is issued to the time when the SOC goes to Standby.
- ALARM1 POL is the polarity of the transition at pin 31 of the module which will trigger an alarm input and waken the module from Standby. A value of 0 specifies a high-to-low transition as active; a value of 1 specifies low-to-high.
- ALARM2 POL is the polarity of the transition at pin 36 that triggers an alarm input, using the same convention used for Alarm1.

The parameters DELAY TIME, ALARM1 POL, and ALARM2 POL are optional. Specifying an alarm polarity also enables the corresponding alarm input.

When this command is issued, the adaptor module will enter the ultra-low-power Standby state (after the optional delay time if present), remaining there until x ms have passed since the command was issued, or an enabled alarm input is received. Any current CID's are lost on transition to Standby. On wakeup, the adapter sends the message Out of Standby-<reason of wakeup> or the corresponding error code, depending on verbose status.

In Standby, only the low-power clock and some associated circuits are active. Serial messages sent to the UART port will not be received. The radio is off and packets cannot be sent or received. Therefore, before requesting a transition to Standby, the requesting application should ensure that no actions are needed from the interface until the requested time has passed, or provide an alarm input to awaken the module when needed. The alarm should trigger about 10 ms prior to issuance of any serial commands.

The Standby clock employs a 34-bit counter operating at 131,072 Hz, so the maximum possible Standby time is 131,072,000 ms, or about 36.4 hours. Standby is not entered until all pending tasks are completed, and a few ms are required to store any changes and enter the Standby state; a similar delay is encountered in awaking from Standby at the end of the requested time. Therefore, we do not recommend Standby times less than about 32 ms.

3.18.24 Auto-connection

3.18.24.1 Wireless Parameters

The command to set the auto connection wireless parameters for the current profile is:

AT+WAUTO=<mode>,<SSID>,<BSSID>,[channel]

- Mode is 0 for Infrastructure and 1 for Ad-hoc mode;
- SSID is the SSID of the AP or Ad-hoc Network to connect to;
- BSSID is the BSSID of the AP or Ad-hoc Network to connect to;
- Channel is the operating channel.

All other parameters required to configure the wireless connection are taken from the current Profile.

3.18.24.2 Network Parameters

The command to set the network parameters for auto connection operation for the current profile is:

AT+NAUTO=<Type>,<Protocol>,<Destination IP>,<Destination Port>

- Type is 0 for Client and 1 for Server;
- Protocol is 0 for UDP and 1 for TCP;
- Destination IP is the IP address of the remote system (optional if the Adapter is acting as a server);
- Destination Port is the port number to connect to on the remote system.

3.18.24.3 Enable Auto-connection

The command to enable auto-connection is:

ATCn

n is 0 to disable auto connection or 1 to enable auto connection.

Upon receipt of this command, the configuration setting in non-volatile memory is modified according to the parameter value in the command; the resulting change (if any) takes effect on the next reboot, or the next issuance of an ATA command.

3.18.24.4 Initiate Auto-connect

The command to initiate auto-connection is:

ATA

On reception of this command, the interface initiates the auto-connection procedure, using the parameters specified by the AT+WAUTO and AT+NAUTO commands. The adapter responds with the IP address, subnet mask, and Gateway IP address, followed by OK or 0 (per verbose status), if the connection is successful. If the connection attempt is unsuccessful the adapter returns ERROR or 1 (per verbose status). After the connection is established, the adapter enters the data transfer mode.

If the adapter is already associated with a wireless network, the alternative command ATA2 below may be used.

3.18.24.5 Initiate Auto-connect - TCP/UDP Level

The command to initiate auto-connection when the adapter is already associated with an access point is:

ATA2

This command requires a pre-existing wireless association. On reception of this command, the interface establishes a network connection to a TCP or UDP server with the parameters specified by the AT+NAUTO command (4.13.2). This command assumes a pre-existing association and should not be issued unless such exists. If a valid command input was received, but the connection cannot be established due to a socket bound failure, the message ERROR: SOCKET FAILURE or 3 (per verbose settings) is returned.

3.18.24.6 Return to Auto-connect Mode

The command to return to auto connect mode is

ATO

If the interface receives this command after it has exited the auto connect mode with +++, it shall return to auto connect mode. If the connection no longer exists, the interface attempts to reestablish the previous connection, and returns to data mode if the reconnection is successful. If the Adapter was not previously connected when this command is received, it returns an error.

3.18.25 System Time

3.18.25.1 Set System Time

The command to set the adaptor system time is:

AT+SETTIME=<dd/mm/yyyy>,<HH:MM:SS>

Upon execution of this command the adaptor set its system time to the time specified as the parameters.

3.18.25.2 Get System Time

The command to get the current system is:

AT+ GETTIME=?

Upon reception of this command the adaptor sends the current system time in ms since epoch(1970) to the serial interface. The time format comes on the serial interface as follows:

“Current Time in ms since epoch=xxxxxxx”

3.18.26 Error Counts

The command to get the error count statistics is:

AT+ERRCOUNT=?

This command returns error count information to the serial host. The error counts includes:

Watchdog reset counts

Software reset counts

Wlan abort/assert counts

3.18.27 Version

The command to output the current version information is:

AT+VER=?

The command returns version information to the serial host:

- Serial-to-Wi-Fi version;
- RFM Embedded Platform Software version;
- WLAN firmware version.

4.0 References

[1] IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 802.11-2007, IEEE, www.ieee.org

[2] V.250, Serial asynchronous automatic dialing and control, and V.251, Procedure for DTE-controlled call negotiation, International Telecommunications Union, www.itu.int

[3] Communications Networks, A. Leon-Garcia and I. Widjaja, McGraw-Hill 2000, p. 582

5.0 Appendices

5.1 E-Series WSN802G Module Ordering Information

WSN802GC-E: transceiver module for solder-pad mounting with RF connector for external antenna
WSN802GCA-E: transceiver module for solder-pad mounting with integral chip antenna
WSN802GP-E: transceiver module for pin-socket mounting with RF connector for external antenna
WSN802GPA-E: transceiver module for pin-socket mounting with integral chip antenna

5.2 Technical Support

For WSN802G product support contact RFM's module technical support group. The phone number is +1.678.684.2000. Phone support is available from 08.30 AM to 5:30 PM US Eastern Time Zone, Monday through Friday. The e-mail address is tech_sup@rfm.com.

5.3 E-Series WSN802G Mechanical Specifications

WSN802GC-E Outline and Mounting Dimensions

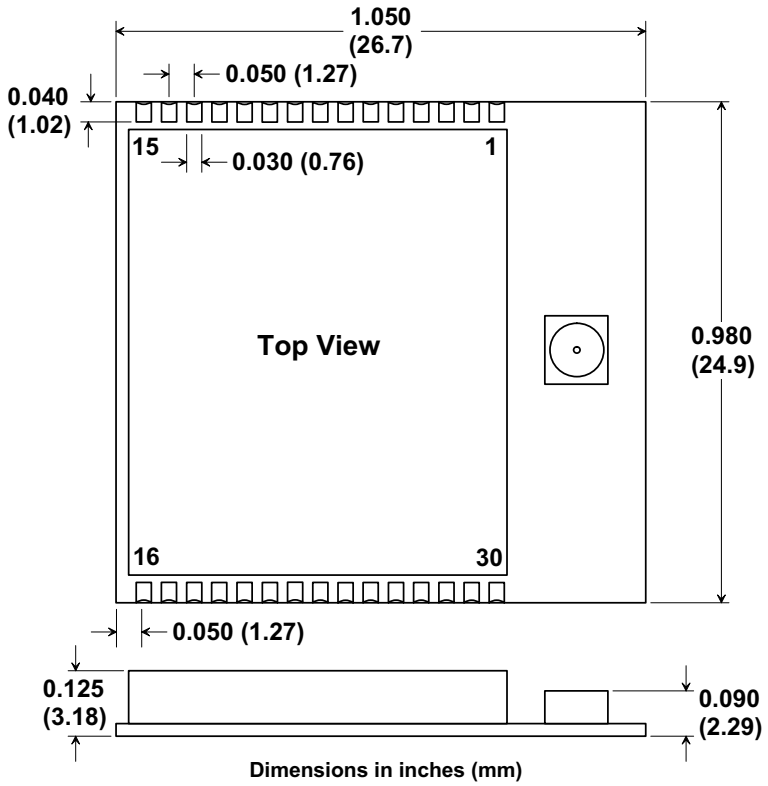


Figure 5.3.1

WSN802GC-E Solder Pad Dimensions

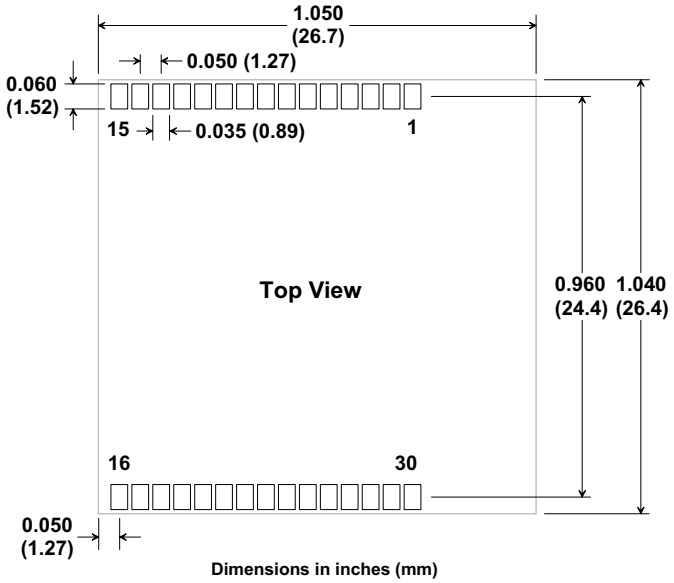


Figure 5.3.2

WSN802GP-E Outline and Mounting Dimensions

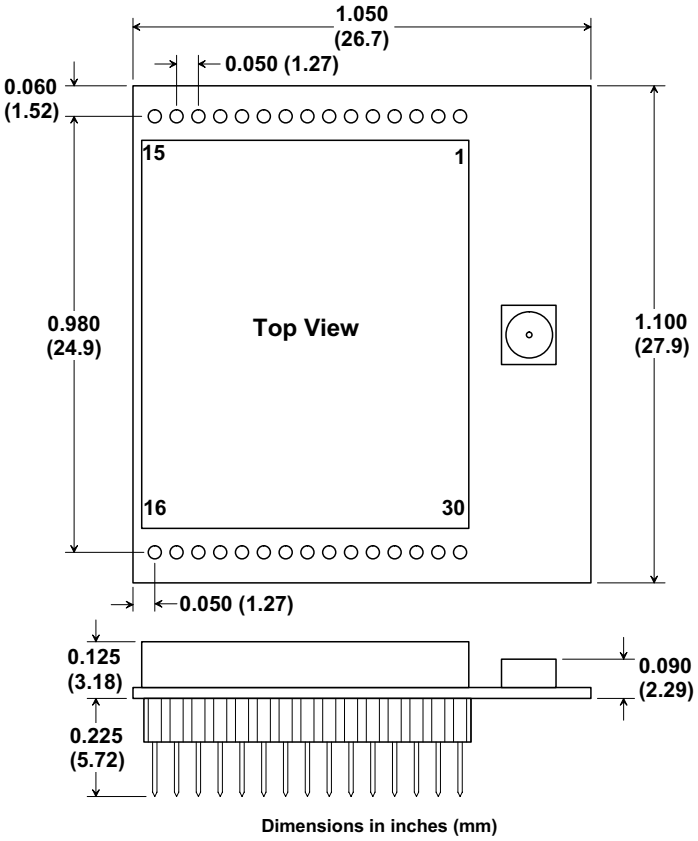


Figure 5.3.3

WSN802GP-E Interface Connector PCB Layout Detail

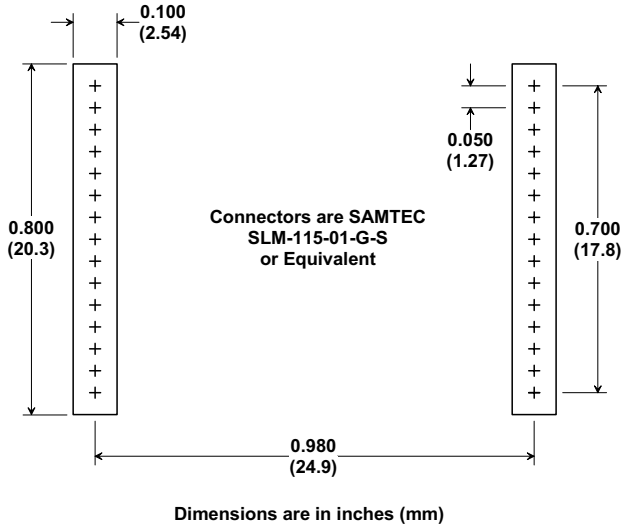


Figure 5.3.4

WSN802GCA-E Outline and Mounting Dimensions

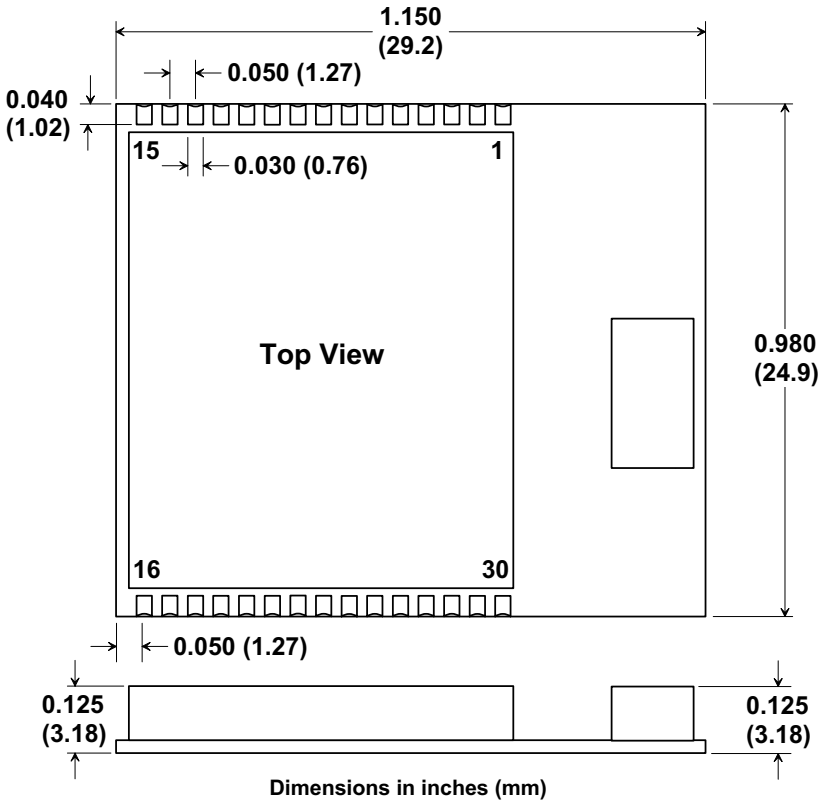


Figure 5.3.5

WSN802GCA-E Solder Pad Dimensions

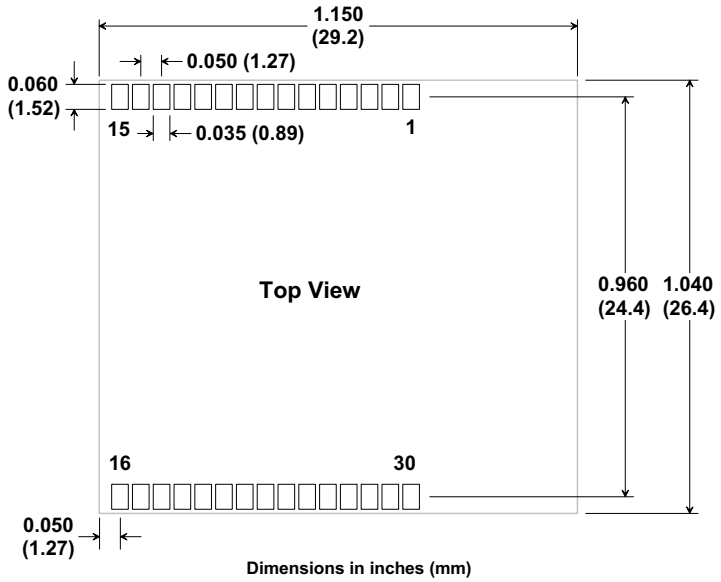


Figure 5.3.6

WSN802GPA-E Outline and Mounting Dimensions

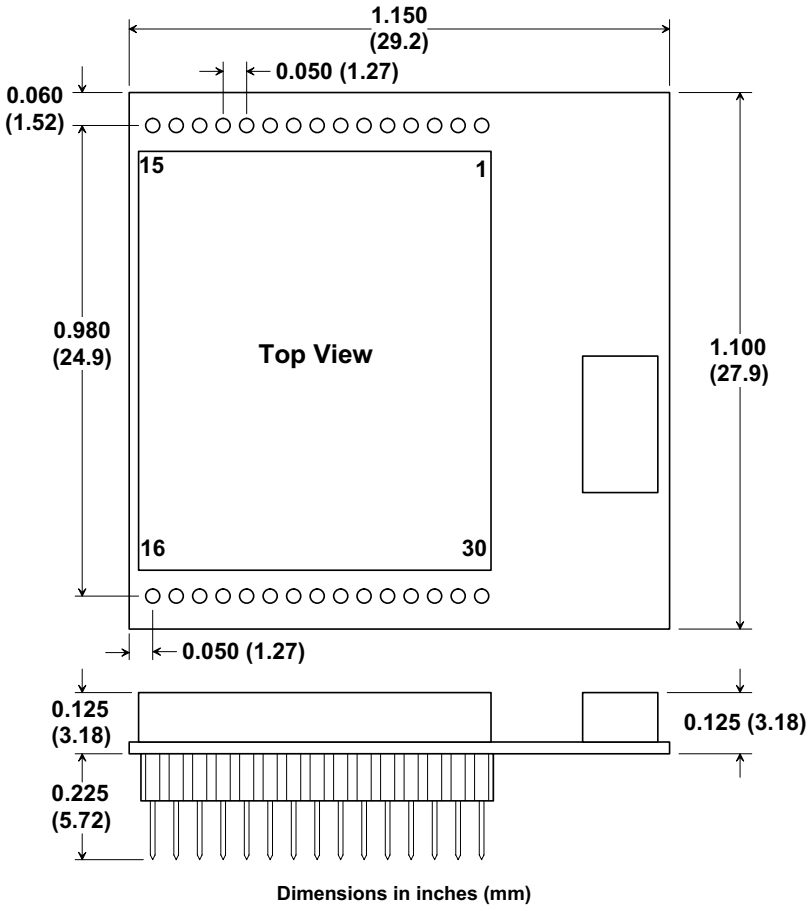


Figure 5.3.7

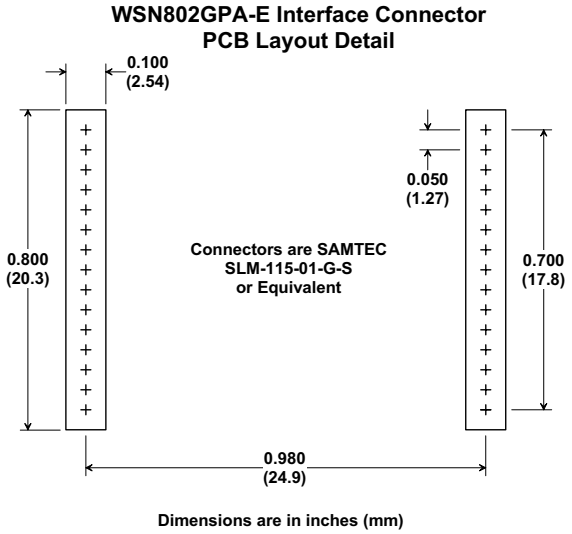


Figure 5.3.8

6.0 Warranty

Seller warrants solely to Buyer that the goods delivered hereunder shall be free from defects in materials and workmanship, when given normal, proper and intended usage, for twelve (12) months from the date of delivery to Buyer. Seller agrees to repair or replace at its option and without cost to Buyer all defective goods sold hereunder, provided that Buyer has given Seller written notice of such warranty claim within such warranty period. All goods returned to Seller for repair or replacement must be sent freight prepaid to Seller's plant, provided that Buyer first obtain from Seller a Return Goods Authorization before any such return. Seller shall have no obligation to make repairs or replacements which are required by normal wear and tear, or which result, in whole or in part, from catastrophe, fault or negligence of Buyer, or from improper or unauthorized use of the goods, or use of the goods in a manner for which they are not designed, or by causes external to the goods such as, but not limited to, power failure. No suit or action shall be brought against Seller more than twelve (12) months after the related cause of action has occurred. Buyer has not relied and shall not rely on any oral representation regarding the goods sold hereunder, and any oral representation shall not bind Seller and shall not be a part of any warranty.

THE PROVISIONS OF THE FOREGOING WARRANTY ARE IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL (INCLUDING ANY WARRANTY OR MERCHANT ABILITY OR FITNESS FOR A PARTICULAR PURPOSE). SELLER'S LIABILITY ARISING OUT OF THE MANUFACTURE, SALE OR SUPPLYING OF THE GOODS OR THEIR USE OR DISPOSITION, WHETHER BASED UPON WARRANTY, CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE ACTUAL PURCHASE PRICE PAID BY BUYER FOR THE GOODS. IN NO EVENT SHALL SELLER BE LIABLE TO BUYER OR ANY OTHER PERSON OR ENTITY FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS, LOSS OF DATA OR LOSS OF USE DAMAGES ARISING OUT OF THE MANUFACTURE, SALE OR SUPPLYING OF THE GOODS. THE FOREGOING WARRANTY EXTENDS TO BUYER ONLY AND SHALL NOT BE APPLICABLE TO ANY OTHER PERSON OR ENTITY INCLUDING, WITHOUT LIMITATION, CUSTOMERS OF BUYERS.

Part # M-0802-1002, Rev H