ATC-2000WF Command Reference

(Version 2.0)

1.0 Configuration

1.1 Entering Command Mode

Upon power up, the device will be in data mode. To enter command mode, exactly the three characters **$$$** must be sent. The device will respond with **CMD**.

While in command mode, the device will accept ASCII bytes as commands.To exit command mode, send **exit<cr>.** The device will respond with "EXIT".

Parameters, such as the SSID, channel, IP address, Serial Port settings, and all other settings can be viewed and configured in command mode. ASCII characters can be sent through a terminal emulator connected to the UART or via Telnet. When using the UART communications settings should match the settings used when ATC-2000WF connects,

for example: ***the default is 9600 baudrate ,8 bits, No Parity, 1 stop bit, and hardware flow control disabled.***

Run your favorite terminal emulator, ***You can find on CD/tool/pcommlite.***

Type **$$$** on your terminal emulator. You should see "**CMD**" returned to you. This will verify that your cable and comm. settings are correct. Most valid commands will return an "**AOK**", response, and invalid ones will return an"**" ERR"** description.

To exit command mode, type **"exit"<cr>.**

NOTE: You can enter command mode locally over the serial port at any time when not connected, and also when connected if the appropriate settings are enabled.

Remote configuration using ADHOC mode

Using adhoc mode to configure the device eliminates the need for the module to be associated with a network access point. In adhoc mode the module creates it own "on demand" network that you can connect to via your computer like you would to any other network.

To enable adhoc mode via hardware set inner SW1 DIP1 to ON(Default is OFF).(You should open the ATC-2000WF metal case).The module will creates an adhoc network with the following

SSID: WiFly-GSX-XX where XX is the final two bytes of the devices MAC address

Channel: 1

DHCP: OFF

IP address: 169.254.1.1

Netmask: 255.255.0.0

From your computer, connect to the WiFly-GSX-XX network. This is an open network which does not require a pass phrase or pass key. Note: currently the WiFly only supports OPEN mode for creating adhoc networks.

NOTE: It may take a couple of minutes for Auto IP in Windows to assign an IP address and connect to the network. You can check IP address of your Windows computer by running the ipconfig command in the command window. If connected, this command will show you the IP address and net mask for your computer.

The IP address assigned by Auto IP must be on the subnet 169.254.1.X otherwise the WiFly GSX module will not be accessible.

NOTE: If your machine has both a wireless and wired interface hardware you will need to disable the wired LAN interface hardware before connecting to the adhoc network. If the wired LAN is enabled the computer will assign an IP address that is not on the same subnet as the WiFly module.

Once connected and you have a good IP address, telnet into the WiFly module on port 2000

telnet 169.254.1.1 2000

You should see the response "*HELLO*"

You can now enter command mode and configure the module.

2.0 ATC-2000WF Command Reference

2.1 Command Syntax

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

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

For example,

set uart baudrate 115200 is valid,

set uart b 115200 is also valid,

set u b 115200 is also valid, however,

s uart baudrate 115200 is NOT valid.

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

2.2 Command Organization

Commands fall into 5 general categories:

·**SET COMMANDS** -Take effect immediately, permanently (save command issued).
·**GET COMMANDS** -Retrieve the permanently stored information for display to user.
·**STATUS COMMANDS** -See what is going on with the interface, IP status, etc.
·**ACTION COMMANDS**- Perform action such as scan, connect, disconnect, etc.
·**FILE IO COMMANDS** - Upgrade, load and save configuration, delete files, etc.

NOTE: You must save the configuration or the module will load the previous settings upon reboot or power up. When the system boots, all configuration data is loaded into RAM variables from the file called "config". The set commands actually only modify the RAM copy of variables in the system. This allows temporary change of parameters "on the fly" to test features, minimizes power usage and saves on flash re-write cycles.

Once all configuration is complete, the user must save the settings using the **save** command to store the configuration data, otherwise it will not take effect upon reboot or reset. Multiple configurations can be stored by using the **save <filename>** command, and these configurations can be loaded using the **load <filename>** command. These files can be upload to remote FTP site, such that once a desired configuration is created, it can quickly be copied into additional devices (cloning).

3.0 SET Commands

These commands begin with "set".There are 6 major categories.

·**ADHOC** - controls the adhoc parameters
·**BROADCAST** - controls the broadcast hello/heartbeat UDP message
·**COMM** - communication and data transfer, timers, matching characters
·**DNS** - DNS host and domain
·**FTP** - FTP host address and login information
·**IP** - IP settings
·**OPTION** - optional and not frequently used parameters
·**SYS** - system settings such as sleep and wake timers
·**TIME** - timer server settings
·**UART** - serial port settings such as baudrate and parity
·**WLAN** - wireless interface settings, such as ssid, chan, security options

3.1 ADHOC Parameters

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

set adhoc probe <num> sets the adhoc probe retry count. Default is 5. This is the number of consecutive probe responses that can be lost before declaring. "ADHOC is lost" and disabling the network interface.

3.2 BROADCAST Parameters

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

set broadcast interval <value>
sets the interval at which the hello/heartbeat UDP message is sent. Interval is specified in seconds. The value is a mask that is compared to a free running seconds counter. For example if interval= 0x7, a packet will be sent every 8 seconds. The minimum interval value is 0x01 (every 2 seconds) and max value is 0xff (every 256 seconds). Setting the value to zero turns off the UDP broadcast. The default interval is 7.

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

3.3 COMM Parameters

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

set comm open <string>

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

set comm remote <string>

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

set comm idle <secs>

sets the Idle Timer Value. This is the number of seconds with no transmit or receive data before the connection is closed automatically. Default is 0, never disconnect on idle.

set comm match <value>

sets matching character initiate forwarding data across the TCP/IP connection. The value is entered as the decimal value of the of the ASCII character. Default is 0, disabled. For more information see section 1Errore: sorgente del riferimento non trovata.4

set comm size <value>

sets the Flush Size value. This is the number of bytes to receive on the UART before forwarding. 0 disables forwarding based on byte count. Default is 64 bytes (at 9600). Maximum value = 1420 bytes.

NOTE: This value is set automatically when the baudrate is set, in an attempt to optimize the link. It is assumed that higher baudrates suggest larger buffer sizes and hence the size will increase at higher baudrate settings.

set comm time <num>

sets the Flush Timer. This is the number of 1 millisecond intervals after the last UART byte is received before the data is sent over Wifi.1 is the minimum value. Default is 10 (10 milliseconds). Setting this value to 0 will disable forwarding based on time delay.

3.4 DNS Parameters

set dns address <addr>

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

set dns name <string>

sets the name of the host for TCP/IP connections.

set dns backup <string>

sets the name of the backup host for TCP/IP connections.

3.5 FTP Parameters

set ftp filename <file>

sets the name of the file transferred when issuing the “ftp u” or “ftp g” commands.

set ftp addr <addr>

sets the ftp server IP address.

set ftp remote <port>

sets the ftp server remote port number (default is 21).

set ftp user <name>

sets the ftp user name for accessing the FTP server.

set ftp pass <pass>

sets the ftp password for accessing the FTP server.

3.6 IP Parameters

set ip address <addr>

sets the IP address of the ATC-2000WF. If DHCP is turned on, the IP address is assigned and overwritten during association with the access point. IP addresses are “.” delimited.

Example: *“set ip a 192.168.1.10”*

set ip backup <addr>

sets a secondary host IP address.

set ip dchp <0,1>

e enable/disable DHCP mode. If enabled, the IP address, gateway,netmask, and DNS server are requested and set upon association with access point. Any current IP values are overwritten. DHCP Cache mode can reduce the time it takes the module to wake from deep sleep thus saving power. In cache mode, the lease time is checked and if not expired the module uses the previous IP settings. If the lease has expired the module will attempt to associated and use DHCP to get the IP settings. DHCP cached IP address does not

Bit Value	Protocol
0	DHCP OFF, use stored static IP address
1	DHCP ON, get IP address and gateway from AP
2	Secure (only receive packets with IP address matches the store host IP)
3	DHCP cache mode, Uses previous IP address if lease is not expired (lease survives reboot)
4	Reserved for future use

survive a power cycle or reset.

the default setting)

set ip flags <value>

Set IP related advanced functions. Value is a bit mapped flag register. Default = 0x7.

set ip gateway <addr>

sets the gateway IP address, If DHCP is turned on, the gateway IP address is assign and overwritten during association with the access point.

set ip host <addr>

sets the remote host IP address. This command is used for making connections from the ATC-2000WE to a TCP/IP server at the IP address <addr>.

set ip localport <num>

sets the local port number.

set ip netmask <value>

sets the network mask. If DHCP is turned on, the net mask is assign and overwritten during association with the access point.

set ip protocol <value>

sets the IP protocol. Value is a bit mapped setting. To connect to the ATC-2000WF module over TCP/IP such as Telnet the device must have the use the TCP Server protocol / bit 2 set. To accept both TCP and UDP use value = 3 (bit 1 and bit 2 set)

Bit Value	Protocol
0	UDP
1	TCP Server & Client (Default)
2	Secure (only receive packets with IP address matches the store host IP)
3	TCP Client only
4	Future Use

set ip remote <value>

sets the remote host port number.

3.7 OPTIONAL Parameters

set opt jointmr <msecs>

Join timer is the time in milliseconds (default=1000) the join function will wait for the an access point to complete the association process.This timer is also the timeout for the WPA handshaking process.

set opt replace <char>

replacement character for spaces. The replacement character is used when entering SSID and pass phrases that include space. This is used by the ATC-2000WFcommand parser only. Each occurrence of the replacement character is changed into a space. The default is “$” (0x24)

set opt deviceid <string>

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

set opt password <string>

TCP connection password. Used to challenge the remote device to authenticate the connection. When set all incoming connections will be challenged and the first characters sent must match the stored password or the connection will be closed. When the password is set the WiFly module will send the string “PASS?” to the remote connection. All characters in the string must be sent in one TCP packet. Max string size is 32 bytes. To disable the password feature use string=0 which is the default.

3.8 SYSTEM Parameters

Bit	Function
0	TCP stack copies RX buffer before sending
1	Bypass Nagle algorithm and use TCP_NODELAY
2	TCP application level single retry enabled
3	RETRY multi - retries 4 times
4	DNS host address caching enabled
5	ARP table caching enabled
6	Reserved

set sys autoconn <secs>

TCP mode: sets the auto connect timer. This command causes the module periodically connect to the host. The timer <secs> determines how often to connect to the stored remote host. If set to 1, the module will only make one attempt to auto connect uponpower up. If set to 2 or greater auto connect will re-open the connection after the connection is closed. Default=0 disables.

set sys autosleep <num *10ms>

Sets the auto-sleep timer. 0 disables. If the protocol is set to UDP ONLY, this timer is used as a quick sleep function. Device will sleep <num> ms after transmission of the first UDP packet.

set sys iofunc <value>

sets the IO port alternate functions. Bit-mapped value. For

more details see section 10.5

set sys mask <mask>

sets the IO port direction mask. Bit-mapped value. For more information see section 1Errore: sorgente del

riferimento non trovata.5

set sys printlvl <value>

sets numerous print functions. 0 = quiet 1 = connect information Default is 1.

set sys output <value> <mask>

sets output PIO pins to HIGH or LOW.

Bit-mapped value. Optional mask only sets a subset of pins.

set sys sleep <secs>

sets the sleep timer. 0 disables.

NOTE: If not using Sensor pins to wake the module, be sure to set the wake timer before issuing the sleep timer or the module will not wake up. See section 8.1 for more details on using system timers

set sys trigger <value>

sets the sensor input(s) to wake on (1-4). Bit-mapped value. 0 disables.

set sys wake <secs>

sets the auto wake timer. 0 disables. See section Errore: sorgente del riferimento non trovata for more details on using system timers

3.9 TIME Server Parameters

set time address <addr>

sets the time server address. (SNTP servers)

set time port <num>

sets the time server port number. Defaults to 123 which is almostalways the SNTP server port.

set time enable <value>

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

Bit Value	Function
0	NO ECHO - disables echo of RX data while in command mode
1	Reserved for future RAW mode protocol
2	Reserved for future RAW mode protocol
3	Enable Sleep on RX BREAK signal

3.10 UART Parameters

set uart baud <rate>

set the UART baud rate. Valid settings are {2400, 4800, 9600,19200, 38400, 57600, 115200, 230400, 460800, 921600}.

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

set uart instant <rate>

This immediately changes the baudrate. This is useful when testing baudrate settings, or switching baudrate “on the fly” remotely while connected over TCP. This setting does not affect configuration.Returns the AOK response, and then this command will exit command mode.

set uart raw <rate>

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

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

set uart flow <0,1>

sets the flow control mode. Default=0=off, 1= hardware RTS/CTS.

NOTE: once flow control is enabled, it is important to properly Drive the CTS pin (active LOW enabled) If CTS is HIGH, data will NOT be sent out the UART, and further configuration in command mode will be problematic as no response will be received.

set uart mode <value>

sets the UART mode register. This is a bit-mapped value.

set uart tx <0, 1>

Disables or enables the TX pin= PIO10 of the UART. Disable will set PIO10 to an INPUT with weak pulldown.

NOTE: Due to an issue in the UART hardware, the UART does not support even or odd, parity.

4.11 WLAN Parameters

set wlan auth <value>

Sets the authentication mode. Not needed unless using auto join mode 2. i.e. set wlan join 2

Note: During association the WiFly module interrogates the Access Point and automatically selects the authentication mode.The current release of 2000WF firmware supports these security modes:

- WEP-128 (open mode only, NOT shared mode)
- WPA2-PSK (AES only)
- WPA1-PSK (TKIP only)
- WPA-PSK mixed mode (some APs, not all are supported)

set wlan channel <value>

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

set wlan ext_antenna <0, 1>

determines which antenna is active, use 0 for chip antenna, 1 for UF.L connector. Default = 0. Only one antenna is active at a time and the module must be power cycled after switching the antenna.

set wlan join <value>

sets the policy for automatically joining/associating with networkaccess points. This policy is used when the module powers up,including wake up from the sleep timer.

Value	Policy
0	Manual, do not try to join automatically
1	Try to join the access point that matches the stored SSID, passkey and channel. Channel can be set to 0 for scanning. (Default)
2	Join ANY access point with security matching the stored authentication mode. This ignores the stored SSID and searches for the access point with the strongest signal. The channels searched can be limited by setting the channel mask.
3	Reserved – Not used
4	Create an Adhoc network, using stored SSID, IP address and netmask. Channel MUST be set DHCP should be 0 (static IP) or set to Auto-IP with this policy. (unless another Adhoc devicecan act as DHCP server) This policy is often used instead of the hardware jumper to creat a custom Adhoc network

set wlan hide <0, 1>

Hides the WEP key and WPA passphrase. When set, displaying the wlan settings shows ****** for these fields. To unhide the passphrase or passkey, re-enter the key or passphrase using the set wlan key or set wlan passphrase command. Default = 0, don't hide.

wlan key <value>

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

Example : "set w k 11223344556677889AABBCCDD"

Hex digits > 9 can be either upper or lower case.

The ATC-2000WF only supports "open" key mode, 128 bit keys for WEP.WEP-128, shared mode is not supported as it is known to be easily compromised and has been deprecated from the Wi-Fi standards.

set wlan linkmon <value>

sets the link monitor timeout threshold. If set to 1 or more, ATC-2000WF will scan once per second for the AP it is associated with. The value is the threshold of failed scans before the ATC-2000WF declares "AP is Lost",de-authenticates. The ATC-2000WF will retry the association based on the join policy variable. A value of 5 is recommended, as some APs will not always respond to probes. Default is 0 (disabled). Without this feature, there is no way to detect an AP is no longer present until it becomes available again (if ever).

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

set wlan mask <value>

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

set wlan num <value>

sets the default WEP key to use. 1-4 is the valid range. Example : "set w n 2" sets the default key to 2.

set wlan phrase <string>

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

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

For passphrases that contain spaces use the replacement character $ instead of spaces. For

example “my pass word” would be entered “my$pass$word”. The replacement character can be changed using the optional command set opt replace <char>.

Example : “set w p password” sets the phrase.

set wlan rate <value>

sets the wireless data rate. Lowering the rate increases the effective range of the ATC-2000WF module. The value entered is mapped according to the following table.

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

set wlan ssid <string>

sets the wlan ssid to associate with. 1-32 chars.

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

For example, if the ssid of the AP is “yellow brick road” You would enter “yellow$brick$road”

Using the ‘get w” command will properly display the value:SSID=yellow brick road.

set wlan window <value>

sets the IP maximum buffer window size. Default is 1460 bytes.

4.0 GET Commands

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

get adhoc display all adhoc settings.

get broadcast will display the broadcast UPD address, port and interval

get everything displays all configuration settings, useful for debug.

get com display comm. settings.

get dns display DNS settings.

get ftp display FTP settings.

get ip display IP address and port number settings.

get mac display the device MAC address.

get optional display the optional settings like device ID

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

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

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

get uart display the UART settings.

Ver return the software release version

5.0 STATUS Commands

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

show net Displays current network status, association,authentication, etc.

show rssi Displays current last received signal strength.

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

show time Displays number of seconds since last power up or reboot

6.0 ACTION Commands

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

close disconnect a TCP connection.

exit exit command mode. Exit command mode. “EXIT” will be displayed.

factory RESET

Loads factory defaults into the RAM configuration.
Note that the RESET must be capitalized. After this command the new settings must be save to the config file using the save command and the module rebooted for them to take effect.

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

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

leave disconnects from currently associated Access Point.

open <addr> <port>
opens a TCP connection to the given IP port and address. If noarguments are provided, the device will attempt to connect to the stored remote host IP address and remote port number. <addr> can also be a DNS hostname and will be resolved if entered.

Ping <g / h | l | addr > <num>
ping remote host. Default sends 1 packet. Optional <num> sends <num> pings at 10 per second.
Ping 10.20.20.12 10 – pings IP address 10 times

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

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

ping l pings a known Internet server at www.neelum.com by first resolving the URL (proves that DNS is working and proves the device has internet connectivity).

ping 0 terminates a ping command

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

scan <time> Performs an active probe scan of access points on all 13 channels.Returns MAC address, signal strength, SSID name, security mode.Default scan time is 200ms / channel = about 3 seconds.time is an optional parameter, this is the time in ms per channel.For example, “scan 30” reduces the total scan time down to about 1 second. This command also works in Adhoc mode (version 2.11).

time Sets the Real time clock by synchronizing with the time server specified with the time server parameters (see section 5.9) This command sends a UDP time server request packet.

7.0 FILE IO Commands

del <name> <num>
Deletes a file. Optional <num> will override the name and use the sector number shown in the “ls” command.

load <name> Reads in a new config file.

Ls Displays the files in the system

Save Saves the configuration to “config” (the default file).

save <name>
Saves the configuration data to a new file name

boot image <num>
Makes file <num> the new boot image.

ftp get <name>
Retrieves a file from the remote FTP server. If <name> not specified, the stored ftp filename is used.

ftp update <name>
Deletes the backup image, retrieves new image and updates the boot image.

8.0 Advanced Features and Settings

8.1 System Timers and Auto Connect Timers

There are 2 timers that can be used to put the module to sleep, and perform a wake up. If the sleep timer is enabled, the module will automatically go into deep sleep, low power mode once the timer counts down to 0. The sleep timer is disabled if the module has an IP connection, or the module is in COMMAND mode. The timer is reset when characters are received on the UART.

The sleep timer is set with : **set sys sleep <time>** time=decimal in seconds.

The wake timer will bring the module out of deep sleep. The wake timer is set with: **set sys wake <time>** time=decimal in seconds.

For example, if you wanted the module to wake up, join a network and be available to accept TCP connections for 30 seconds every 2 minutes you would set the timers as such

set wlan ssid my_net

set wlan passphrase my_pass
set sys sleep 30
set sys wake 90
save
reboot

UDP sleep, and Connection timers

There is another timer than can be used to put the device to sleep.

In UDP protocol mode, the autoconn timer is used as an auto-sleep timer.

Upon the start of transmission of the first UDP data packet this timer will count down.

set sys autosleep <value> UDP mode: sets the auto-sleep timer. 0 disables

the timer is decremented every xx milliseconds, based on the value of the comm flushtimer. Using a minimum value of 2 (when the default flushtime=10 ms) is recommended to ensure that the UDP packet gets transmitted. For larger packets the value should be increased.

In TCP-Client mode, the auto-conn timer is used as a connect out timer. If set, the device will automatically attempt a connection when the timer expires.

set sys autoconn <secs>

In TCP-Client AND TCP-Server mode, there is also a disconnect timer.

set comm idle <secs> sets the idle disconnect timer. This causes a disconnect if no transmit or receive data is seen.

8.2 UART Receiver, RTS/CTS Hardware Flow Control

The UART receive buffer is approx. 1024 bytes, and at lower baudrates (9600, 19200) the system can process data into the device without need for flow control.

If constant streaming of data into RX on the device is required, care should be taken to set the comm parameters to optimize the performance. If data has a termination char, this can be used.

Also, if data has a particular frame size, this can be used.

set comm match <value>

sets the value of the packet terminator.

set comm size <value>

sets the number of bytes to receive before forwarding 0-1 forwards immediately. maximum value = 1460 bytes.

The **comm size** is automatically set whenever the baudrate is set, but can be modified.

Even at higher baudrates (115K and higher) it is possible to operate without flow control if packets are uniform and a protocol is used to ensure that data is delivered on the remote side before the next packet is sent.

However, given the uncertainty of packet delays in a TCP/IP network and the affects of interference and retries inherent in wireless networks, flow control is usually required to guarantee no data is lost.

By default flow control is disabled. To enable hardware flow control, use **set uart flow 1.**

8.3 Using the Real Time Clock Function

The real time clock in the module keeps track of the number of seconds since the module was powered on and the actual time when synchronized with the sNTP time server. By default the module keeps track of up time but does not synchronize with the time server since this requires being associated with a network that can access the sNTP server.

The default sNTP server is at

ADDR=129.6.15.28:123

ZONE=7 (GMT -7)

Use the **show time** command to see the current time and uptime

<2.10> **show t**

Time=08:43:10

UpTime=10 s

Time can be set by using the time command

<2.10> **show t**

Time NOT SET

UpTime=8 s

<2.10> time

<2.10> show t

Time=08:51:31

UpTime=15 s

NOTE: the WiFly module must by successfully associated with a network for the module to contact the sNTP server.

Alternatively, the module can be configured to get the time whenever it powers up by setting the time enable to 1. Any value greater than 1 gets time continuously

every <value> minutes.

To configure the Wifly module to get time upon power up

<2.10> **set time enable 1**

AOK

<2.10> **get time**

ENA=1

ADDR=129.6.15.28:123

ZONE=7

To view a complete listing of the time variable use the command

<2.10> **show t t**

Time=09:02:10

UpTime=653 s

Powerup=1792 s

RTC=7753271426558 ms

timera=66885

8.4 Using the UDP Broadcast function

The WiFly module can be setup to automatically generate UDP broadcast packets. This is useful for a number of reasons:- Some Access Points will disconnect devices that sit idle and don't send any packets after a time. Using the UDP broadcast informs the AP that WiFly is alive and wants to stay associated. This feature can be used by application programs to auto-discover and auto configure the WiFly module. If an application is listening for the UDP broadcast, a number of useful parameters are present in the package that can be used for auto-discovery. For example, the IP address and port number of the WiFly are both part of the packet, and thus the Wifly can be connected to and configured remotely with this information.

- The MAC address of the associated AP, channel, and RSSI value are available in this packet,

thus enabling a simple location and tracking based function.

By default the Wifly module now sends out a UDP broadcast to 255.255.255.255 on port 55555 at a programmable interval. The broadcast address, port and interval are set using the "set broadcast" commands.

8.5 Joining Networks and Making Connections

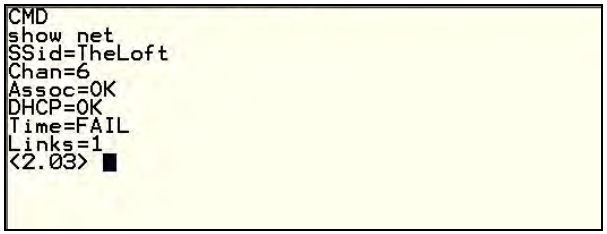
Configuring the module to make connections is a two set process. First you need to associate with a network access point and second you need to open a connection.To configure the module over the WiFi link is a chicken and egg problem. The module must be associated to a network to connect to it and program the network settings. This problem can be solved by configuring the module from the UART or over the air using adhoc mode.If configuring the module using adhoc mode, see section Errore: sorgente del riferimento non trovata. Once in adhoc mode open up a telnet window on IP address 169.254.1.1 port 2000

If configuring the module using the UART mode either using the RS232 or development board, open a terminal emulator on the COM port associated with that deveice. The default baud rate is 9600, 8 bits no parity.

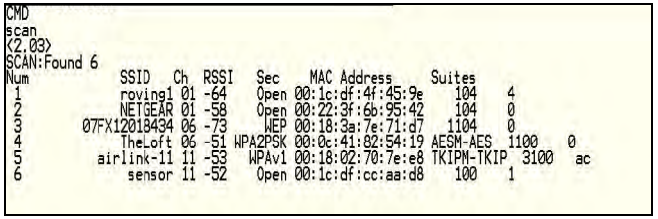
8.6 Associate with a network access point

From within the terminal window, put the WiFly GSX module into command mode by typing $$$ in the terminal window. You should get CMD back confirming you are in command mode.

Type ***show net*** to display the current network settings.

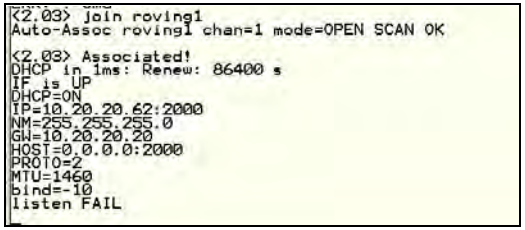


Now finding all available networks with the ***scan*** command



If the network you're connecting to is open, you can simply use the join command to associate with the access point. From the scan list above you can see that roving1 is an open network access point.

Type ***join roving1*** to associate with an access point.



You could also have specified the roving1 access point by using the command ***join # 1***

If the access point is security enabled you will need to set the pass phrase prior to issuing the ***join*** command. The ATC-2000 module will attempt to inquire and determine the security protocol of the access point so you do not have to set the authentication mode. To set the pass phrase for WPA use the command ***set wlan phrase <string>***. For WEP set the key using the ***set wlan key <num>*** command.

Once you have successfully associated to the network the access point SSID is stored.This along with the pass phrase can be saved to the config file so the module can associate with the network each time it is booted up.

8.7 Making connections

To make a connection into the module simply open a IP socket and connect to the IP address of the module. Telnet is a simple way to test this connection. From in Telnet type open <addr> <port>. In the example above the telnet command you look like ***open 10.20.20.62 2000***. Once open you can type characters into the UART window and see them on the Telnet window or visa versa.

To make a connection from the module you will need IP address and port number of your a server application. A simple program to test this functionality is a COM port redirector. This software opens an IP port and transfers all data it receives to a specified COM port on your machine. A free com port redirector program is available from Pira at

http://www.pira.cz/eng/piracom.htm

After installing and starting this program, note the IP address of the machine it is running on. This can be found by running ipconfig in the Microsoft command window. With the ATC-2000WF module in command mode type ***open <addr> <port>***. The server will report the connection is open and you can type characters into the UART window and see them on the server window or visa versa.

8.8 Setting up Automatic Connections

Often, it is desired on power up (or wakeup) to automatically connect out to a remote server, send data, and then disconnect. This can be configured to happen automatically.

In the following example assume the network SSID and security have been set correctly and autojoin is set to 1. This will also work in adhoc mode(autojoin 4), however there will be delay in connecting to the adhoc network from the remote computer so set the sleep timer large enough to allow the network to get set up and the autoconn establish a TCP connection. When the module wakes up or is powered on the autoconn timer will cause the module to attempt a connection to the stored remote IP address and port. While this connection is open the sleep timer will not decrement. While data is flowing the idle timer will not decrement. Once data stops for 5 seconds the connection will be closed. The sleep timer will the kick in and put the module in deep sleep. Finally the wake timer will start the whole cycle again one minute later.

set ip host X.X.X.X (set up the IP address of the remote machine)

set ip remote_port num (set up the IP port of the remote machine)

set sys autoconn 1 (automatically connect out after READY)

set com idle 5 (disconnect after 5 seconds with no data activity)

set sys sleep 2 (sleep 2 seconds after connection is closed)

set sys wake 60 (wakeup after 1 minute of sleeping)

save

8.9 Utilizing the Backup IP address/connect function

ATC-2000WF contains a feature for auto-retry and redundancy. If the first IP host address connection fails, the backup IP will be used (if set) . If this fails (or is not set) then the first DNS name will be used. If this fails (or is not set) then the Backup DNS name will be used.

To set the backup IP address, use:

set ip backup <address>

To set the backup DNS name, use:

set dns backup <string>

8.10 Firmware Upgrade over FTP

WiFly module has a file system for storing firmware, web pages and config files. Use the **ls** command to view files. File size is displayed in sectors and the active boot image is identified in the final message.

FL# SIZ FLAGS

11 18 3 WiFly_GSX-2.10
29 1 10 config
226 Free, Boot=11, Backup=11

Multiple firmware images and config files can be stored on the module file system.

FTP Upload and Upgrade

WiFly contains a built in FTP client for getting files and updating the firmware. The client uses passive mode FTP, which allows operation thru firewalls and the Internet.

To upload the latest released firmware from Roving Networks the following setting are required:

FTP username = roving

FTP password = Pass123

FTP filename = wifly-GSX.img

FTP directory = ./public (this parameter can not be modified)

To use FTP to upgrade the firmware, enter the following command:

ftp upload <string> (string is an optional filename, use to bypass the default firmware filename)

The ftp upload command will retrieve the file and switch the boot image to the new file.

<2.10> ftp update

<2.10> FTP connecting to 208.109.78.34

FTP file=30

.....

FTP OK.

The previous firmware will become the backup image. Here is an example of what you should see after a successful update:

FL# SIZ FLAGS

11 18 3 WiFly_GSX-2.05

29 1 10 config

30 18 3 WiFly_GSX-2.10

208 Free, Boot=30, Backup=11

Note the module must be rebooted or power cycled to use the new firmware. To boot a different firmware use the following command:

Boot image <num> sets the current boot image <num>

For example to boot the previous image from above use

<2.10> boot image 11

Set Boot Image 11, =OK

To upload your own firmware or config file to the module, change the stored FTP settings: See section 5.5 for more details on the FTP commands. To upload your file w following command:

ftp get <string> Retrieves remote file with name <string>

8.11 Restoring Default configuration settings:

As of version 2.10 you can now specify a USER configuration as the factory reset settings. Prior to this release only the hardcoded factory defaults would be restored.From command interface use the **factory RESET** command to restore the defaults.From hardware, setting PIO9 high on power up arms the factory reset functional and toggling PIO9 five (5) times there after causes the configuration setting to restored to the factory reset.

Now however if there is a config file named "user", it is read in as the factory defaults instead of using the previous hardcoded defaults. If no "user" config file is present, the hardcoded factory defaults are used.

The "user" config file is created using the "save user" command which save the current configuration settings into the “user” file.

Even if there is a “user” config file arming and toggling PIO9 7 times will override the “user” settings and restore the wifly module to the factory hardcoded defaults. This is a bypass mechanism in case a bad configuration is saved into the “user” file.

Note: Factory defaults should be saved to the config file using the **save** command and the module rebooted for the new settings to take effect.

8.12 Supported Access Points

Access points that are set to MIXED mode (WPA1 and WPA2) may cause problems during association because some of these incorrectly report their security mode.We also currently do not support WPA2-Enterprise (radius server authentication, EAP-TLS) The Wifly GSX should work with any standard Access Point. We have tested the WiFly-GSX module with the following access points

- Cisco Aeronet series
- Linksys (both standard and openWRT linux)
- Netgear WGR614 v8
- Netgear WGN54
- DLINK dir-615
- Airlink 101
- Apple Airport express
- ADHOC MODE (Apple Iphone, Microsoft windows PC

with XP, Vista , Ubuntu Linux)