



Excellence in Compliance Testing

---

## **Certification Exhibit**

**FCC ID: HSW-2410P**

**IC: 4492A-2410P**

**FCC Rule Part: 15.247**

**IC Radio Standards Specification: RSS-210**

**ACS Report Number: 08-0020 - 15C**

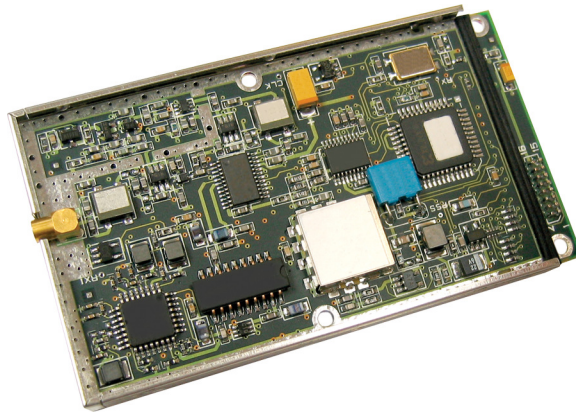
Manufacturer: Cirronet

Model: WIT2410P

## **Theory of Operation**

# WIT2410P

2.4GHz Spread Spectrum Wireless Industrial Transceiver



## Integration Guide



---

CIRRONET™

**3079 Premiere Pkwy Ste 140  
Duluth, Georgia 30097  
www.cirronet.com  
+1 (678) 684-2000**

## Important Regulatory Information

**Cirronet Product FCC ID: HSW-2410P  
IC 4492A-2410P**

---

**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.

---

### **FCC MPE Requirements**

The WIT2410P is designed for portable applications as a remote unit. These remote radios are installed in belt packs or other close to the body devices worn by the user.

The power output, duty cycle and antenna gain are set to be well below the FCC's Maximum Permissible Exposure to radio frequency energy.

See Appendix I, II and III Page 54 and 55.

# Declaration of Conformity



Warning! The RLAN transceiver within this device uses a band of frequencies that are not completely harmonized within the European Community. Before using, please read the European Operation Section of the Products User's Guide for limitations.

The WIT2410 to which this declaration relates is in conformity with the essential requirements of the R&TTE directive 1999/5/EC and complies with the following standards and/or other normative documents:

EN 300 328

## Use Within the European Union

The WIT2410P is intended for use within the European Community States and in the following non-European Union States: Norway & Switzerland

## Use of the WIT2410 in France

When used in France, the WIT2410 can only be operated with the France hopping pattern selected. This is accomplished by setting the **pe** parameter to 1. Refer to *European Union Settings* in this manual for details.

## Canadian Department of Communications Industry Canada (IC) Notice

Canadian Department of Communications Industry Canada (IC) Notice

This apparatus complies with Health Canada's Safety Code 6 / IC RSS 102.

"To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors may be subject to licensing."

## 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 présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de Classe B prescrites dans le règlement sur le brouillage radioélectrique édicté par Industrie Canada.

## NOTE!

Any changes of modifications not expressly approved by the party responsible for compliance could void the user's authority operate the equipment.

## TABLE OF CONTENTS

1. INTRODUCTION .....	1
1.1. Why Spread Spectrum? .....	1
1.2. Frequency Hopping vs. Direct Sequence.....	2
2. RADIO OPERATION .....	5
2.1. Synchronization and Registration .....	5
2.2. Data Transmission .....	6
2.2.1. Point-to-Point .....	6
2.2.2. Point-to-Multipoint .....	7
2.2.3. Handle Assignment .....	7
2.2.4. TDMA Operation .....	8
2.2.5. Full Duplex Communication.....	10
2.2.6. Error-free Packet Transmission Using ARQ.....	10
2.3. Modes of Operation .....	11
2.3.1. Control and Data Modes .....	11
2.3.2. Sleep Mode .....	11
2.3.3. Low Power Mode and Duty Cycling .....	12
2.3.4. RF Flow Control Mode .....	12
2.3.5. Co-Existing with 802.11b Networks.....	13
2.3.6. European Union Settings .....	13
3. PROTOCOL MODES .....	14
Note on Using Protocol Mode 4.....	16
3.1.1. Data Packet.....	17
3.1.3. Connect Packet.....	18
3.1.4. Disconnect Packet (base only, receive only).....	18
4. MODEM INTERFACE .....	19
4.1. Interfacing to 5 Volt Systems .....	20
4.2. Evaluation Unit and OEM Module Differences .....	20
4.3. Three Wire Operation .....	20
4.4. Power-On Reset Requirements.....	21
5. MODEM COMMANDS.....	22
5.1. Serial Commands .....	22
5.2. Network Commands .....	23
5.3. Protocol Commands.....	26
5.4. Status Commands .....	29
5.5. Memory Commands .....	30
5.6. Modem Command Summary.....	31
6. WIT2410 DEVELOPER'S KIT .....	32
7. WinCOM.....	33
7.1. Starting the program .....	35

7.2. Function Keys .....	38
7.3. WinCom Tools.....	39
7.4. Script Commands.....	41
7.5. Demonstration Procedure .....	43
8. Troubleshooting .....	44
9. APPENDICES .....	46
9.1. Technical Specifications .....	46
9.1.1 Ordering Information .....	46
9.1.2. Power Specifications.....	46
9.1.3. RF Specifications .....	46
9.1.4. Mechanical Specifications .....	46
9.2. Serial Connector Pinouts .....	47
9.3. Approved Antennas .....	47
9.4. Technical Support .....	48
9.5. Reference Design.....	49
9.6.1. Mechanical Drawing – WIT2410M4 (Pins Down) .....	50
9.6.2. Mechanical Drawing – WIT2410S4 (Pins Up).....	51
10. Warranty .....	52

#### FCC MPE Calculations

Appendix I – Operating Scenario for WIT2410P.....	54
Appendix II – Calculation of Maximum Transmit Duty Cycle.....	55
Appendix III – Calculated Average Power.....	55

## 1. INTRODUCTION

The WIT2410 radio transceiver provides reliable wireless connectivity for either point-to-point or multipoint applications. Frequency hopping spread spectrum technology ensures maximum resistance to noise and multipath fading and robustness in the presence of interfering signals, while operation in the 2.4GHz ISM band allows license-free use and worldwide compliance. A simple serial interface supports asynchronous data up to 230400 bps. An on-board 3 KB buffer and an error-correcting over-the-air protocol provide smooth data flow and simplify the task of integration with existing applications.

- Multipath fading impervious frequency hopping technology with 75 frequency channels (2401-2475 MHz).
- Supports point-to-point or multipoint applications.
- Meets FCC rules 15.247 and ETS 300.328 for worldwide license-free operation.
- Superior range to 802.11 wireless LAN devices.
- Transparent ARQ protocol w/3KB buffer ensures data integrity.
- Digital addressing supports up to 64 networks, with 62 remotes per network.
- Low power 3.3v CMOS signals
- Fast acquisition typically locks to hopping pattern in 2 seconds or less.
- Selectable 10 mW or 100 mW transmit power.
- Support for diversity antenna.
- Built-in data scrambling reduces possibility of eavesdropping.
- Nonvolatile memory stores configuration when powered off.
- Smart power management features for low current consumption.
- Dynamic TDMA slot assignment that maximizes throughput.
- Simple serial interface handles both data and control at up to 230400 bps.

### 1.1. Why Spread Spectrum?

The radio transmission channel is very hostile, corrupted by noise, path loss and interfering transmissions from other radios. Even in a pure interference-free environment, radio performance faces serious degradation through a phenomenon known as multipath fading. Multipath fading results when two or more reflected rays of the transmitted signal arrive at the receiving antenna with opposing phase, thereby partially or completely canceling the desired signal. This is a problem particularly prevalent in indoor installations. In the frequency domain, a multipath

fade can be described as a frequency-selective notch that shifts in location and intensity over time as reflections change due to motion of the radio or objects within its range. At any given time, multipath fades will typically occupy 1% - 2% of the 2.4 GHz band. This means that from a probabilistic viewpoint, a conventional radio system faces a 1% - 2% chance of signal impairment at any given time due to multipath.

Spread spectrum reduces the vulnerability of a radio system to interference from both jammers and multipath fading by distributing the transmitted signal over a larger region of the frequency band than would otherwise be necessary to send the information. This allows the signal to be reconstructed even though part of it may be lost or corrupted in transit.

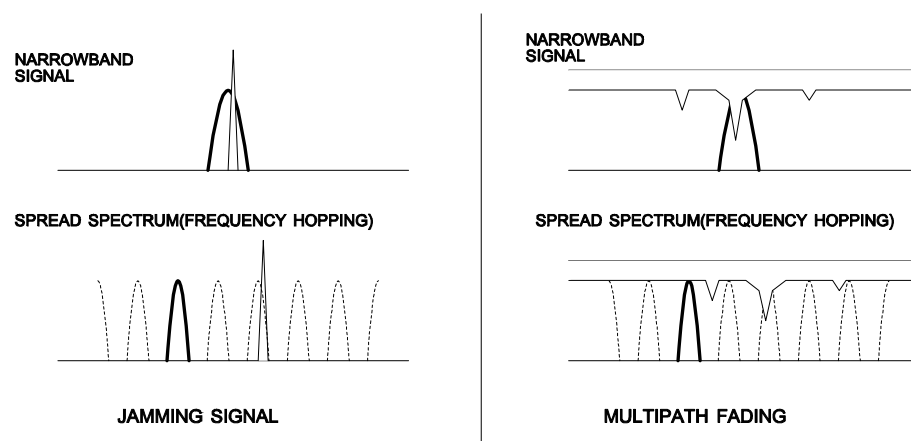


Figure 1

Narrowband vs. spread spectrum in the presence of interference

## 1.2. Frequency Hopping vs. Direct Sequence

The two primary approaches to spread spectrum are direct sequence (DS) and frequency hopping (FH), either of which can generally be adapted to a given application. Direct sequence spread spectrum is produced by multiplying the transmitted data stream by a much faster, noise-like repeating pattern. The ratio by which this modulating pattern exceeds the bit rate of the baseband data is called the processing gain, and is equal to the amount of rejection the system affords against narrowband interference from multipath and jammers. Transmitting the data signal as usual, but varying the carrier frequency rapidly according to a pseudo-random pattern over a broad range of channels produces a frequency hopping spectrum system.



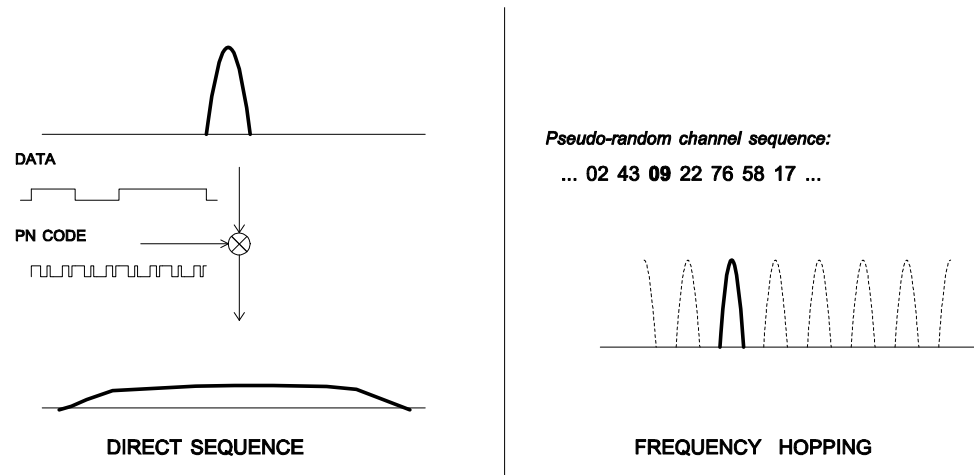


Figure 2  
Forms of spread spectrum

One disadvantage of direct sequence systems is that due to spectrum constraints and the design difficulties of broadband receivers, they generally employ only a minimal amount of spreading (typically no more than the minimum required by the regulating agencies). For this reason, the ability of DS systems to overcome fading and in-band jammers is relatively weak. By contrast, FH systems are capable of probing the entire band if necessary to find a channel free of interference. Essentially, this means that a FH system will degrade gracefully as the channel gets noisier while a DS system may exhibit uneven coverage or work well until a certain point and then give out completely.

Because it offers greater immunity to interfering signals, FH is often the preferred choice for co-located systems. Since direct sequence signals are very wide, they tend to offer few non-overlapping channels, whereas multiple hoppers may interleave with less interference. Frequency hopping does carry some disadvantage in that as the transmitter cycles through the hopping pattern it is nearly certain to visit a few blocked channels where no data can be sent. If these channels are the same from trip to trip, they can be memorized and avoided; unfortunately, this is generally not the case, as it may take several seconds to completely cover the hop sequence during which time the multipath delay profile may have changed substantially. To ensure seamless operation throughout these outages, a hopping radio must be capable of buffering its data until a clear channel can be found. A second consideration of frequency hopping systems is that they require an initial acquisition period during which the receiver must lock on to the moving carrier of the transmitter before any data can be sent, which typically takes several seconds. In summary, frequency hopping systems generally feature greater coverage and channel utilization than comparable direct sequence systems. Of course, other implementation factors such as size, cost, power consumption and ease of implementation must also be considered before a final radio design choice can be made.

As an additional benefit, RF spectrum has been set aside at 2.4 GHz in most countries (including the U.S.) for the purpose of allowing compliant spread spectrum systems to operate freely without the requirement of a site license. This regulatory convenience alone has been a large motivation for the industry-wide move toward spread spectrum.

## 2. RADIO OPERATION

### 2.1. Synchronization and Registration

As discussed above, frequency hopping radios periodically change the frequency at which they transmit. In order for the other radios in the network to receive the transmission, they must be listening to the frequency over which the current transmission is being sent. To do this, all the radios in the net must be synchronized and must be set to the same hopping pattern.

In point-to-point or point-to-multipoint arrangements, one radio module is designated as the base station. All other radios are designated remotes. One of the responsibilities of the base station is to transmit a synchronization signal to the remotes to allow them to synchronize with the base station. Since the remotes know the hopping pattern, once they are synchronized with the base station, they know which frequency to hop to and when. Every time the base station hops to a different frequency, it immediately transmits a synchronizing signal.

When a remote is powered on, it rapidly scans the frequency band for the synchronizing signal. Since the base station is transmitting over 75 frequencies and the remote is scanning 75 frequencies, it can take several seconds for a remote to synch up with the base station.

Once a remote has synchronized with the base station, it must request registration from the base station. The registration process identifies to the base station the remotes from which transmissions will be received and not discarded. Registration also allows tracking of remotes entering and leaving the network. The base station builds a table of serial numbers of registered remotes. To improve efficiency, the 24-bit remote serial number is assigned a 6-bit “handle” number. Two of these are reserved for system use, thus each base station can register 62 separate remotes. This handle is how user applications will know the remotes. Note that if a remote leaves the coverage area and then re-enters, it may be assigned a different handle.

To detect if a remote has gone offline or out of range, the registration must be “renewed” once every 256 hops. Registration is completely automatic and requires no user application intervention. When the remote is registered, it will receive several network parameters from the base. This allows the base to automatically update these network parameters in the remotes over the air. Once a parameter has been changed in the base, it is automatically changed in the remotes. The parameters automatically changed are *hop duration* and the duty cycle.

At the beginning of each hop, the base station transmits a synchronizing signal. After the synchronizing signal has been sent, the base will transmit any data in its buffer unless *data transmit delay* has been set. The *data transmit delay* parameter allows for the transmission of groups of continuous data in transparent mode (protocol mode 0). The amount of data that the base station can transmit per hop is determined by the *base slot*

*size* parameter. The maximum amount of data sent by a base station per hop is 208 bytes. If there is no data to be sent, the base station will not transmit until the next frequency.

The operation for remotes is similar to the base station without the synchronizing signal. The amount of data a remote can send on one hop is dependent upon the *hop duration*, the *base slot size* and the number of registered remotes. 212 bytes per hop is the maximum data length a remote can transmit per hop, subject to limitations imposed by the *hop duration*, the *base slot size* and the number of registered remotes. A detailed explanation of this relationship is provided in Section 2.2.3. *Minimum data length* and *data transmit delay* operate the same as with the base station.

Except for the registration process which occurs only when a remote logs onto the network, the whole procedure is repeated on every frequency hop. Refer to the section on *Modem Commands* for complete details on parameters affecting the transmission of data.

## 2.2. Data Transmission

The WIT2410 supports two network configurations: point-to-point and point-to-multipoint. In a point-to-point network, one radio is set up as the base station and the other radio is set up as a remote. In a point-to-multipoint network, a star topology is used with the radio set up as a base station acting as the central communications point and all other radios in the network set up as remotes. In this configuration, all communications take place between the base station and any one of the remotes. Remotes cannot communicate directly with each other. It should be noted that point-to-point mode is a subset of point-to-multipoint mode and therefore there is no need to specify one mode or the other.

### 2.2.1. Point-to-Point

In point-to-point mode, unless *data transmit delay* or *minimum data length* have been set, the base station will transmit whatever data is in its buffer limited to 208 bytes or as limited by the *base slot size*. If the base station has more data than can be sent on one hop, the remaining data will be sent on subsequent hops. In addition to the data, the base station adds some information to the transmission over the RF link. It adds the address of the remote to which it is transmitting, even though in a point-to-point mode there is only one remote. It also adds a sequence number to identify the transmission to the remote. This is needed in the case of acknowledging successful transmissions and retransmitting unsuccessful transmissions. Also added is a 24-bit CRC to allow the base to check the received transmission for errors. When the remote receives the transmission, it will acknowledge the transmission if it was received without errors. If no acknowledgment is received, the base station will retransmit the same data on the next frequency hop.

In point-to-point mode, a remote will transmit whatever data is in its buffer up to the limit of its *maximum data length*. If desired, *minimum data length* and *data transmit delay* can

also be set, which force the remote to wait until a certain amount of data is available or the specified delay is exceeded before transmitting. If the remote has more data than can be sent on one hop, it will send as much data as possible as a packet, adding its own address, a packet sequence number and 24-bit CRC. These additional bytes are transparent to the user application if the protocol mode is 00 (which is the default). In the event a remote has more data to send, the data will be sent on subsequent hops. If the transmission is received by the base station without errors, the base station will acknowledge the transmission. If the remote does not receive an acknowledgment, it will retransmit the data on the next frequency hop. To the user application, acknowledgments and retransmissions all take place behind the scenes without the need for user intervention.

The WIT2410 has a point-to-point direct mode which fixes the remote radio's handle at 30H. This mode is recommended for point-to-point applications, especially if the remote is likely to periodically leave and re-enter the coverage area of the base. See the section on *Network Commands* for details of this mode.

### **2.2.2. Point-to-Multipoint**

In point-to-multipoint mode, data sent from the user application to the base station must be packetized by the user application unless the remote device can distinguish between transmissions intended for it and transmissions intended for other remote devices. This is necessary to identify the remote to which the base station should send data. When the user packet is received by the remote, if the remote is in transparent mode (protocol mode 0), the packetization bytes are stripped by the remote. In this instance the remote host receives just data. If the remote is not in transparent mode, the remote host will receive the appropriate packet header as specified by the remote's protocol mode. Refer to the section *Protocol Modes* for details on the various packet formats.

When a remote sends data to a base station in point-to-multipoint mode, the remote host does not need to perform any packetization of the data. Remotes can operate in transparent mode even though the base is operating in a packet mode. The remote will add address, sequence and CRC bytes as in the point-to-point mode. When the base station receives the data, the base station will add packetization header bytes according to its *protocol mode* setting.

### **2.2.3. Handle Assignment**

Handles are used to reduce overhead by not sending the unique 24-bit serial number ID of a remote when sending or receiving data. The use of the various protocol modes causes the base radio to issue CONNECT packets when a new remote registers with the base. In addition to indicating the presence of a new remote, the CONNECT packets provide the current relationship between remote serial numbers and handles.

When a remote links to a base and requests registration, it requests by default that it be assigned handle 30H. This default request can be changed by the Set Default Handle command. If that handle is not currently in use by another remote, the base will assign that handle to the remote. If the requested handle is already in use by another remote, the base will assign the next higher handle that is available. Thus, if a remote requests handle 30H and that handle is already assigned, the base will assign the remote handle 31H if that is available. If 31H is already assigned, the base will assign handle 32H if that is available and so on.

When a remote leaves the coverage area of the base or otherwise loses link, e.g. the remote was turned off or put into sleep mode, the base detects this event when the remote does not renew its registration within 255 hops. With the default setting of 10msec per hop, this could be as long as 2.55 seconds. If within this time the remote re-establishes link with the base, the previous handle assigned to this remote will still be marked active in the base radio. Thus the remote will be assigned a new handle. If the base radio is in one of the protocol modes, a new CONNECT packet will be issued indicating the current handle assigned to the remote. The remote is identified by the serial number that is contained in the CONNECT packet.

If the radio is to be used in a point-to-point mode where there is only one base and one remote, using the point-to-point mode command of the radios will override this handle mechanism and always assign the remote the same handle.

#### **2.2.4. TDMA Operation**

For applications needing guaranteed bandwidth availability, the TDMA operation of the WIT2410 can meet this requirement. In the WIT2410 TDMA scheme, each remote has an assigned time slot during which it can transmit. The base station time slot is set independently of the remote time slots through the *Set Base Slot Size* command. The base station assigns each remote a time slot and informs the remotes of the size of the time slot. All remote time slots are the same size that is determined by the number of remotes registered with the base station. The slot size is a dynamic variable that changes as the number of registered remotes changes. The remotes are continually updated with the time slot size. This approach continually maximizes the data throughput. The base station divides the amount of time available per hop by the number of registered remotes up to a maximum of 16 times slots per hop. If the number of registered remotes is greater than 16, the time slots will be spread across the required number of hops. For networks with more than 16 possible remotes, the *Set Duty Cycle* command must be used to specify a duty cycle -- the number of hops over which the time slots must be spread. For 1 to 16 remotes, no duty cycle is required; for 17 to 32 remotes a duty cycle of at least  $\frac{1}{2}$  is required; and for 33 to 62 remotes a duty cycle of  $\frac{1}{4}$  or more is necessary. An added benefit of using the power save mode to set a duty cycle is improved average current consumption efficiency. Refer to the *Status Commands* section for details of this command.

When setting up a network, keep in mind that time slot length, maximum packet size and hop duration are all interrelated. The *hop duration* parameter will determine the time slot size and the maximum amount of data that can be transmitted per hop by the remotes. There is a hard limit of the absolute maximum amount of data that can be sent on any given hop of 212 bytes regardless of any parameters. (Note that this is different than the 208 byte maximum for the base station.) The base station requires 1.7 ms overhead for tuning, the synchronization signal and parameter updating, as well as a guard time of 500 $\mu$ s between each remote slot. Thus the amount of time allocated per remote slot is roughly:

$$\frac{\text{hop duration} - \text{base slot} - 1.7\text{ms} - (\# \text{ of registered remotes} - 1) \cdot 500\mu\text{s}}{(\# \text{ of registered remotes})}$$

Take for example a network comprised of a base station and 10 remotes. A hop duration of 10 ms is chosen. We decide that the base station needs to be able to send up to 32 bytes each hop (equivalent to a capacity for the base of ~ 32 kbps). Counting the 1.7 ms overhead for the base packet and making use of the fact that our RF rate is 460.8 kbps, we determine that the base slot requires approximately:

$$\frac{32 \cdot 8}{460.8\text{kbps}} + 1.7 \text{ ms} = 2.3 \text{ ms}$$

Each remote time slot will be:

$$\frac{10 \text{ ms} - 2.3 \text{ ms} - (9) \cdot 0.5 \text{ ms}}{10} = 0.32 \text{ ms}$$

From our RF data rate of 460.8 kbps we see that it takes 17.36  $\mu$ s to send a byte of data, so each remote will be able to send up to

$$\frac{0.32 \text{ ms}}{17.36\mu\text{s}} = 18 \text{ bytes of data per hop.}$$

Note that the 18 bytes is the actual number of data bytes that can be sent. If the WIT2410 is using a protocol mode, the packet overhead does not need to be considered. So in this example, the total capacity per remote would be:

$$\frac{18 \text{ bytes}}{10 \text{ ms}} = 18 \text{ kbps}$$

If we figure a minimum margin of safety for lost packets and retransmissions of about 20%, we see that this would be more than sufficient to support 14.4 kbps of continuous data per remote. It is also useful to remember that the asynchronous data input to the WIT2410 is stripped of its start and stop bits during transmission by the radio, yielding a "bonus" of 10/8 or 25% in additional capacity.

The above calculations are provided as a means of estimating the capacity of a multipoint WIT2410 network. To determine the precise amount of capacity, you can actually set up

the radio system and then query the *maximum data length* from one of the remotes in control mode to discover its exact setting. Divide this number by the hop duration as above to get the remote's exact capacity.

### 2.2.5. Full Duplex Communication

From an application perspective, the WIT2410 communicates in full duplex. That is, both the user application and the remote terminal can be transmitting data without waiting for the other to finish. At the radio level, the base station and remotes do not actually transmit at the same time. If they did, the transmissions would collide. As discussed earlier, the base station transmits a synchronization signal at the beginning of each hop followed by a packet of data. After the base station transmission, the remotes will transmit. Each base station and remote transmission may be just part of a complete transmission from the user application or the remote terminal. Thus, from an application perspective, the radios are communicating in full duplex mode since the base station will receive data from a remote before completing a transmission to the remote.

### 2.2.6. Error-free Packet Transmission Using ARQ

The radio medium is a hostile environment for data transmission. In a typical office or factory environment, 1% - 2% of the 2.4GHz frequency band may be unusable at any given time at any given station due to noise, interference or multipath fading. For narrowband radio systems (and also many spread spectrum radio systems which use direct sequence spreading), this would imply a loss of contact on average of over 30 seconds per hour per station. The WIT2410 overcomes this problem by hopping rapidly throughout the band in a pseudo-random pattern. If a message fails to get through on a particular channel, the WIT2410 simply tries again on the next channel. Even if two thirds of the band is unusable, the WIT2410 can still communicate reliably.

Data input to the WIT2410 is broken up by the radio into packets. A 24-bit checksum is attached to each packet to verify that it was correctly received. If the packet is received correctly, the receiving station sends an acknowledgment, or **ACK**, back to the transmitting station. If the transmitter doesn't receive an **ACK**, at the next frequency hop it will attempt to send the packet again. When ARQ is enabled, the transmitting radio will attempt to send a packet *packet attempts limit* times before discarding the packet. A value of **00H** disables ARQ. When it is disabled, any transmission received with errors is discarded. It is the responsibility of the user application to track missing packets. A second parameter, *ARQ Mode*, allows the choice between using ARQ to resend unsuccessful transmissions or always sending a transmission *packet attempts limit* times regardless of the success or failure of any given transmission.

All of this error detection and correction is transparent to the user application. All the user application sees is error-free data from the modem. However, if the ARQ mode is disabled, transmissions with errors are discarded, and missing data detection will be the



responsibility of the user application. Refer to the *Protocol Commands* section for complete details.

## 2.3. Modes of Operation

### 2.3.1. Control and Data Modes

The WIT2410 has two modes of operation: Control mode and Data mode. When in Control Mode, the various radio and modem parameters can be modified. When in Data Mode, only data can be transmitted. The default mode is Data Mode. There are two ways to enter Control Mode. The first way is to assert the Configure (CFG) pin on the modem. Upon entering Control Mode, the modem will respond with a > prompt. After each command is entered, the modem will again respond with a > prompt. As long as the CFG pin is asserted, data sent to the modem will be interpreted as command data. Once the CFG pin is deasserted, the modem will return to Data Mode.

The second method for entering Control Mode is to send the escape sequence `:wit2410` (all lower case) followed by a carriage return. In the default mode, the escape sequence is only valid immediately after power up or after deassertion of the Sleep pin on the modem. The modem will respond in the same way with a > prompt. To return to Data Mode, enter the *Exit Modem Control Mode* command, `z>`, or assert and deassert the Sleep pin. There are three modes for the escape sequence, controlled by the *Set Escape Sequence Mode* command, `zc`:

<code>zc = 0</code>	Escape sequence disabled
<code>zc = 1</code>	Escape sequence available once at startup (default setting)
<code>zc = 2</code>	Escape sequence available at any time

The `zc2` mode setting is useful if the user application has a need to change the modem settings "on the fly". In this mode the escape sequence is always enabled and may be sent at any time after a pause of at least 20ms. The modem will respond in the same way as when in the default mode. It is necessary to issue the *Exit Modem Control Mode* command, `z>`, before resuming data transmission. The escape sequence must be interpreted as data until the last character is received and as such may be transmitted by the modem to any listening modems.

### 2.3.2. Sleep Mode

To save power consumption for intermittent transmit applications, the WIT2410 supports a Sleep Mode. Sleep Mode is entered by asserting the Sleep pin on the modem interface. While in Sleep Mode, the modem consumes less than 50µA. This mode allows the radio to be powered off while the terminal device remains powered. After leaving Sleep Mode, the radio must re-synchronize with the base station and re-register.

### 2.3.3. Low Power Mode and Duty Cycling

To conserve power, WIT2410 remotes power down the receiver and transmitter between hops when not in use. Base stations must remain active all the time to handle any transmission from any remote. Remotes can save even more power by enabling the duty cycle feature. This feature causes a remote to power down for  $2^N$  frequency hops where  $1/2^N$  is the duty cycle. Rather than attempting to transmit on every frequency hop when data is in the transmit buffer, a remote will attempt to transmit only every  $2^N$  hops. Roughly speaking, this will proportionately reduce the average power consumption while increasing average latency. When there are more than 16 remotes being operated, duty cycling must be enabled since a maximum of 16 time slots is available per hop.

When a remote radio is powered up but is out of range of a base station, it will continuously scan the frequency bands for the presence of a base radio. During this scanning the radio can consume up to 80mA of current. A low power seek mode is available in which the remote radios seek base stations only 50% of the time. This will reduce current consumption by about 50% but will double the time it can take a remote to link with a base up to 4 seconds.

### 2.3.4. RF Flow Control Mode

Because of slight differences in baud rates between transmitting and receiving hosts, when sending large amounts of data (100's of KB) in one direction in a point-to-point application, it is possible to overrun the receive buffer of the receiving radio. For example a nominal 115.2Kbaud at the transmitting radio's host might really be 115,201 and at the receiving radio's host it might be 115,199. This is similar to a situation where the transmitting radio is sent data at a higher baud rate than the baud rate at which data is received by the receiving host. To compensate for the variations in nominal baud rates, the WIT2410 supports an RF flow control mode for point-to-point operation. In this mode, when the receive buffer of the receiving WIT2410 is close to full, the receiving WIT2410 stops acknowledging transmissions. The transmitting radio is set to infinite retries which invokes the RF flow control mode (See *Set Packet Attempts Limit* in Section 5.3). The receiving radio will not begin acknowledging transmissions from the transmitting radio until more room in the receive buffer has become available. This will cause data in the transmit buffer of the transmitting radio to back up. If it backs up to the point where the transmit buffer fills up, the transmitting radio will deassert CTS stopping data from the transmitting radio's host device. Once room is available in the receiving radio's buffer, the receiving radio will begin acknowledging transmissions from the transmitting radio allowing the transmitting radio's buffer to begin to empty which will cause the transmitting radio to reassert CTS. Either one or both of the radios in a point-to-point installation can be configured for the RF flow control. If this mode is invoked in a point-to-multipoint installation, communications with all radios will be stopped when any one radio's receive buffer becomes full.

### 2.3.5. Co-Existing with 802.11b Networks

In some cases, if a WIT2410-based network is located in close proximity to an 802.11b network, the WIT2410-based network can interfere with the 802.11b network. To avoid causing this interference, the WIT2410 radio supports a selection of hopping patterns that avoid the various 802.11b direct sequence channels. These limited band hopping patterns allow WIT2410-based networks to be used with 802.11b networks without impacting the performance of the 802.11b networks. The hopping pattern is selected using the **pe** command. Please refer to the section 5.3 *Protocol Commands* for details.

### 2.3.6. European Union Settings

When operating the WIT2410 in France, a limited frequency mode must be selected. **pe** values of 5, 6 or 7 may be used. To select the limited frequency band **pe** = 5, at the > configuration mode prompt enter:

```
pe5<CR>
```

Save this setting by typing:

```
m><CR>
```

The limited frequency operation will take effect immediately and will be saved into memory for use when power is cycled.

Use of the WIT2410 within the European Union is limited to a maximum transmit power including antenna gain of 20dBm. If gain antennas are to be used, the low power setting of the WIT2410 must be selected. This setting sets the transmit power at the antenna connector to 10dBm. In this setting a maximum of 10dB of antenna gain may be used. To select low power mode, at the > configuration mode prompt enter:

```
wp0<CR>
```

To save this parameter in non-volatile memory type:

```
m>
```

### 3. PROTOCOL MODES

In point-to-point applications, it is generally desired that the radios operate in a transparent mode. That is, raw unformatted data is sent from the host to the radio and is received as raw data from the receiving end. The addressing and error detection and correction are still performed by the radios, but it is transparent to the user application. To set up a point-to-point network, one radio has to be set up as a base station. When the radios are powered on, the base station will send out the synchronization signal at the beginning of each hop. The remote will synchronize with the base and automatically request registration. Once the remote is registered, the radios can transmit data. Protocol mode operation is available in point-to-point mode if desired.

If the base station is to be responsible for directing data to a specific remote in point-to-multipoint mode, the data sent to the base station by the user application must adhere to a packet format. This allows transmissions from the base station to be directed to a specific remote. Data received by a base station from a remote is similarly formatted to identify to the user application the remote that sent the transmission. The remotes may still use transparent mode without formatting to send data to the base, if desired. The WIT2410 supports 10 protocol formats that are described in detail below. The protocol format is selected through the *Set Protocol Mode* command.

Base and remote radios can use protocol modes to insure that a packet is transmitted to the base without being broken up over multiple hops. The *data length* value in the data packet becomes the effective *minimum packet length* and *maximum packet length* for that packet. Note that if the remote *data length* is set to a number of bytes that is longer than the number of bytes that can be transmitted by a remote on a single hop, the packet will be discarded. For the base, this value is set by the *Set Base Slot Size* command. For remotes this value is dynamically available through the *Get Maximum Data Length* command or may be calculated based on the maximum number of remotes that can ever be registered at one time. See Sections 5.3 and 2.2.3 respectively. Also note that using protocol modes effectively disables *Data Transmit Delay*. This means that a packet will not be transmitted until the entire packet has been sent to the radio, regardless of the amount of time it takes.

If the remote hosts can determine what data is directed to them in point-to-multipoint mode, the data can be sent to the base station without using a packet format. In this situation, broadcast mode is selected at the base station by using the *Set Default Handle* and selecting **3FH** as the default handle. In this mode, the automatic retransmission of unsuccessful transmissions is disabled. This is required since all of the remote modems will attempt to acknowledge each base transmission when ARQ is enabled. Transmissions that are received with errors are discarded by the radio. The remote devices must be able to detect a missing packet and request a retransmission by the base device.

## Protocol Modes Definitions

- mode 00      Transparent mode used for point-to-point networks or multipoint remotes; does not support any packet types.
- mode 01      This is the simplest protocol mode supporting Data packets only. This mode is not recommended for base radios. No CONNECT or DISCONNECT packets are supported and no sequence numbers are provided.
- packet types supported:    Data
- mode 02      This mode includes notification when remotes are registered or dropped through CONNECT and DISCONNECT packets that are sent to the user application at the base station and at the remote. No sequence numbers are provided.
- packet types supported:    Data  
   CONNECT  
   DISCONNECT
- mode 04      This is the packet format used by the WIT2400. This allows legacy software to operate the WIT2410 with a minimum of changes. Note however, that since different air data rates are used, WIT2410s and WIT2400s cannot be mixed in a network.
- packet types supported:    2400 data format  
   (*addresses must be limited to 1..62*)
- modes 05 – 08    *reserved for future use.*
- mode 09      This mode sends the protocol mode 01 packets during transmit but receives data transparently.
- mode 0A      This mode sends the protocol mode 02 packets during transmit but receives data transparently.
- mode 0C      This mode sends the protocol mode 04 packet during transmit but receives data transparently.
- modes 0D – 0F    *reserved for future use.*
- mode 11      This mode sends data transparently but supports protocol mode 1 during reception.

- mode 12     This mode sends data transparently but supports protocol mode 2 during reception.
- mode 14     This mode sends data transparently but supports protocol mode 4 during reception.

### **Note on Using Protocol Mode 4**

An important difference between the WIT2400 and the WIT2410 is the dynamic assignment of time slots and handles in the WIT2410. The WIT2400 required that each remote be configured with a static address which distinguished one remote from another. In the WIT2410, remotes are distinguished by their factory-assigned serial number. When using protocol Mode 4 in the WIT2410, the static address of the WIT2400 is replaced with the current handle of the WIT2410. In point-to-multipoint configurations, a remote's handle is not guaranteed to remain the same if the remote drops link with the base and then re-establishes link. In a point-to-point system, the point-to-point mode of the WIT2410 can be set to guarantee the remote handle does not change.

If protocol Mode 4 is used, the data stream being transmitted from the remotes to the base should contain information indicating the remote sending the data as the handle assigned to the remote can change when the link to the base is dropped and re-established.

### 3.1. Packet Formats

The byte formats for each packet type are shown in the table below. Packet fields are organized to fall on byte boundaries. In the case of bit-level fields, most-significant bits are on the left.

WIT2400 packet type (mode 04):

Base	DATA	0000 0010	00HH HHHH	LLLL LLLL	<0-208 bytes data>	0000 0011
Remote	DATA	0000 0010	0000 0000	LLLL LLLL	<0-212 bytes data>	0000 0011

M RTP (WIT2410) packet types (modes 01-03):

Transmit and Receive:							
Base	DATA	1110 1001	00HH HHHH	LLLL LLLL	<0-208 bytes data>		
Remote	DATA	1110 1001	0000 0000	LLLL LLLL	<0-212 bytes data>		
Receive only:							
ID>	CONNECT	1110 1001	10HH HHHH	R RRR TTTT	00NN NNNN	<3 byte remote	
	DISCONNECT	1110 1001	11HH HHHH	0111 1111			
	H	: handle number (0-63)					
	L	: data length (0-208 for base, 0-212 for remote)					
	N	: remote's previous network number (if roamed)					
	R	: receive sequence number (from previous cell)					
	T	: transmit sequence number (from previous cell)					

**Note that while the packet length can be set to 212, the maximum number of bytes transmitted per hop is limited to the lesser of 212 or the length specified by maximum data length. Packets with a data length longer than that will be discarded and not sent. See Get Maximum Data Length for more details.**

#### 3.1.1. Data Packet

Modes 01 & 02:

Base	1110 1001	00HH HHHH	LLLL LLLL	<0-208 bytes data>
Remote	1110 1001	0000 0000	LLLL LLLL	<0-212 bytes data>

Mode 04 (WIT2400):

0011	Base	0000 0010	00HH HHHH	LLLL LLLL	<0-208 bytes data>	0000
0011	Remote	0000 0010	0000 0000	LLLL LLLL	<0-212 bytes data>	0000

H	:	handle number (0-63)
L	:	data length (0-208 for base, 0-212 for remote)

This packet carries user data. The handle number is the handle of the receiving remote. When data is being sent from a remote to the base, no handle number is required. Up to 212 bytes (208 for base radios) of user data may be carried per data packet but no more than is specified by the *maximum data length* parameter. The radio will not break up a packet over multiple hops. Packets with a data length greater than *maximum data length*

will not be sent and will be discarded. This parameter is variable and depends on the number of remotes currently registered.

Handle 63 is reserved for broadcast packets from the base to all remotes.

Acknowledgment requests are not supported for broadcasts. For this reason, it is a good idea to send broadcast messages several times to increase the odds of reaching all remotes.

### 3.1.3. Connect Packet

1110 1001 10HH HHHH RRRR TTTT 00NN NNNN <3-byte remote ID> (base, receive only)

H : handle number (0-62)  
 R : receive sequence number (from previous cell)  
 T : transmit sequence number (from previous cell)  
 N : network number of the previous base (if roamed)

1110 1001 10HH HHHH RRRR TTTT 00NN NNNN <3-byte base ID> (remote, receive only)

H : handle number (0-62)  
 R : receive sequence number  
 T : transmit sequence number  
 N : network number of base

Remotes must go through an automatic registration process when roaming from one base to another, after loss of contact, or when acquiring a base signal for the first time after power up. The base then assigns the remote a handle value, may or may not assign it a dedicated time slice depending on the user settings, and notifies the user application of the new remote with a connect packet.

The network number of the last base the remote was connected to is given to aid user software in resending orphan packets that may have been sent to the remote's previous cell. If the remote has been powered up for the first time and this is the first base contacted, the last base ID will be reported as 80H.

### 3.1.4. Disconnect Packet (base only, receive only)

1110 1001 11HH HHHH 0111 1111

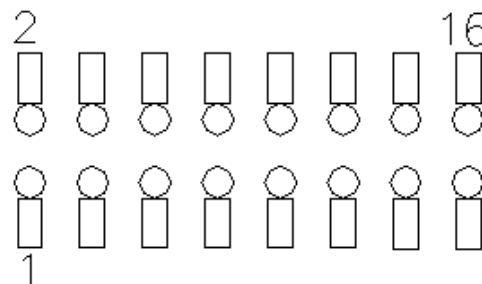
H : handle number (1-62)

When a remote goes out of range or roams to another cell, the base issues a disconnect packet to indicate that the remote is no longer available.



## 4. MODEM INTERFACE

Electrical connection to the WIT2410 is made through a 16-pin male header on the modem module. The signals are 3.3 volt signals and form an RS-232 style asynchronous serial interface.

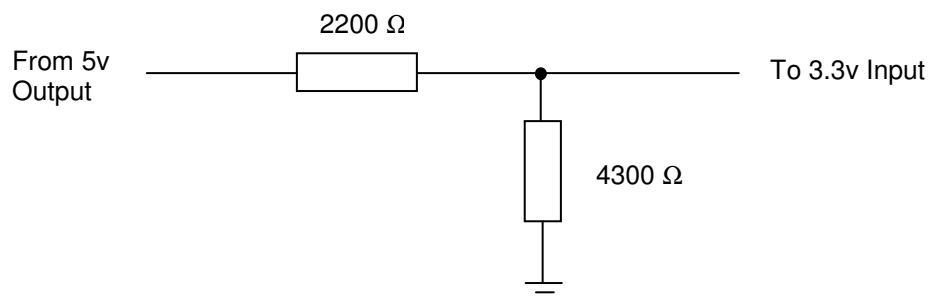


The table below provides the connector pinout.

Pin	Signal	Type	Description
1	GND	-	Signal and chassis ground
2	TXD	Input	Transmit data. Input for serial data to be transmitted. In Control Mode also used to transmit modem commands to the modem.
3	RXD	Output	Receive data. Output for received serial data. In Control Mode, also carries receive modem status from the modem.
4	$\overline{\text{CFG}}$	Input	Configuration selector. Used to switch between Control and Data Modes. Normally, CFG will be set for Data Mode. An internal 10K pull-up enables Data Mode if this signal is left unconnected. Control Mode is also accessible by transmitting an escape sequence immediately after wake up or power up.  (0v) 1 = Control Mode (3.3v) 0 = Data Mode
5	$\overline{\text{RTS}}$	Input	Request to send. Gates the flow of receive data from the radio to the user on or off. In normal operation this signal should be asserted. When negated, the WIT2410 buffers receive data until RTS is asserted.  (0v) 1 = Receive data (RxD) enabled (3.3v) 0 = Receive data (RxD) disabled.
6	SLEEP	Input	Sleeps/wakes radio transceiver. In sleep mode all radio functions are disabled consuming less than 50 $\mu$ A. At wake up, any user programmed configuration settings are refreshed from non-volatile memory, clearing any temporary settings that may have been set.  (3.3v) 1 = Sleep Radio (0v) 0 = Wake Radio
7	$\overline{\text{DCD}}$	Output	Data carrier detect. For remotes, indicates the remote has successfully acquired the hopping pattern of the base station.  (0v) 1 = Carrier detected (synchronized) (3.3v) 0 = No carrier detected (not synchronized)
8	$\overline{\text{CTS}}$	Output	Clear to send. Used to control transmit flow from the user to the radio.  (0v) 1 = Transmit buffer not full, continue transmitting (3.3v) 0 = Transmit buffer full, stop transmitting
9	-	-	Reserved for future use. Do not connect.
10	$\overline{\text{Reset}}$	Input	Resets the radio.
11-15	-	-	Reserved for future use. Do not connect.
16	VCC	-	Positive supply. Min 3.3 v, 5.0 v nominal, 10.0 v max.

## 4.1. Interfacing to 5 Volt Systems

The modem interface signals on the WIT2410 are 3.3 volt signals. To interface to 5 volt signals, the resistor divider network shown below must be placed between the 5 volt signal outputs and the WIT2410 signal inputs. The output voltage swing of the WIT2410 3.3 volt signals is sufficient to drive 5 volt logic inputs.



## 4.2. Evaluation Unit and OEM Module Differences

The evaluation unit has an RS-232 transceiver that translates RS-232 level signals to 3.3 volt signals for input into the OEM module inside the evaluation unit. A typical schematic is shown in Appendix 7.5. The OEM module does not have any type of RS-232 transceiver and cannot handle the RS-232 voltages. This allows the OEM module to be easily integrated into any 3.3 volt system without any logic signal translation. In order for the OEM module to function properly several pins need to be driven low or tied to ground. Pin 5 (RTS) and pin 6 (SLEEP) need to be pulled to ground on the 16-pin male header. If you have the OEM module interfaced to an RS-232 transceiver, RTS and DTR need to be pulled high on the transceiver side. In the evaluation unit, RTS and DTR are pulled high on the transceiver side so the evaluation unit will work with these signals not connected.

## 4.3. Three Wire Operation

The WIT2410 can be operated in a three wire configuration using just TxD, RxD and Ground. To operate the WIT2410 in this configuration, the Sleep and RTS signals must be tied to ground. These signals are pulled up on the WIT2410 module and if left disconnected will put the radio into sleep mode and RTS will be deasserted.

The WIT2410 does not support software flow control (XON/XOFF). Thus when using a three wire configuration, there is no flow control. The radio configuration and/or the application must insure the transmit and receive buffers do not overflow. The WIT2410 has a 2048-byte transmit buffer and a 1024-byte receive buffer. For example, the default settings for the *base slot size* and *hop duration* are **08H** and **90H** respectively. The **08H** base slot size allows the base to send 32 bytes of data per hop. The **90H** hop duration provides a 10ms hop dwell time. These default settings provide a base throughput of

40kbps (Since the over the air transmission is synchronous, the 32kbps synchronous over the air rate is equivalent to 40kbps asynchronous into the radio serial port). If the base transmits continuously at a higher rate than this, unless the default settings are changed, the transmit buffer will eventually overflow. To allow a higher base throughput, either increase the base slot size or the hop duration or both. A similar analysis needs to be performed for the remote radios. Refer to *Section 2.2.3 TDMA Mode* for the remote throughput calculation.

#### 4.4. Power-On Reset Requirements

The WIT2410 has an internal reset circuit that provides a reset signal to the microprocessor if the supply voltage to the WIT2410 falls below 2.7 volts. Operation of the microprocessor at voltages below this voltage is unspecified and can result in corruption of the program memory. When the radio is first powered on, there is an inrush current in excess of 250mA. The power supply in the host must be capable of sourcing this current without the voltage falling below 2.7 volts at the radio. Failure of the power supply to meet this requirement can result in “motorboating” of the radio where the inrush current of the radio pulls the supply voltage below 2.7 volts causing the reset circuit to fire which resets the radio removing the current requirement. Once the voltage recovers to a level above 2.7 volts, the reset signal is removed from the radio which causes the inrush current which causes the voltage to drop causing the reset circuit to fire and so on.

If the host circuitry has a reset circuit that generates a reset signal to the radio anytime the power supply voltage falls below 2.7 volts, the on-board reset circuit can be disabled. Cirronet recommends leaving the reset circuit enabled unless it causes a problem due to a soft turn-on of the power supply voltage by the host. Please contact Cirronet Technical Support for details on disabling the reset circuit.

## 5. MODEM COMMANDS

The WIT2410 is configured and controlled through a series of commands. These commands are sent to the modem directly when the modem is in Control Mode when the modem is in Data Mode if the escape sequence is enabled. The command syntax is the same for either method, a one- or two-letter command followed by one or more parameters. The modem will respond with a two-byte message that indicates the new modem parameter value. The commands are loosely grouped into five different categories: Serial commands, Network commands, Protocol commands, Status commands and Memory commands. Each command is described in detail below. In the descriptions, brackets ([,]) are used to denote a set of optional arguments. Vertical slashes (/) separate selections. For example, given the string `wn[?|0..3f]`, some legal commands are `wn?`, `wn0`, `wn3` and `wna`. Most commands which set a parameter also have a `?` option which causes the modem to respond with the current parameter setting, e.g., `wn?`. Each modem command must be followed by either a carriage return or a line feed.

### 5.1. Serial Commands

These commands affect the serial interface between the modem and the host. The default settings are 9600 bps and protocol mode 0.

Command	Description
<code>sd[? 00..FF]</code>	Set Data Rate Divisor Data Rate    Divisor (hex) 1200 bps    =    BF 2400 bps    =    5F 9600 bps    =    17 14400 bps   =    0F 19200 bps   =    0B 28800 bps   =    07 38400 bps   =    05 57600 bps   =    03 115200 bps  =    01 230400 bps  =    00
<code>sp[? 00..14]</code>	Set Protocol Mode 00    = point-to-point transparent mode 01    = basic command and data only 02    = command, data and connection notification 04    = WIT2400 protocol mode 05 – 08 = <i>reserved for future use</i> 09    = mode 01 during transmit, transparent receive 0A    = mode 02 during transmit, transparent receive 0C    = mode 04 during transmit, transparent receive 0D – 10 = <i>reserved for future use</i> 11    = transparent transmit, mode 01 during receive 12    = transparent transmit, mode 02 during receive 14    = transparent transmit, mode 04 during receive

*Set Data Rate Divisor*

Sets the serial bit rate between the modem and the host. This command takes effect immediately and will require adjusting the host serial rate to agree. Nonstandard rates may be programmed by entering a data rate divisor computed with the following formula:

$$\text{DIVISOR} = (230400/\text{RATE}) - 1$$

Round all non-integer values down.

*Set Protocol Mode*

Enables the base station to operate in a multipoint network. Depending on the user application, more or less acknowledgment may be desired by the application. Remotes can operate in transparent mode even though the base station is operating in one of the nontransparent modes.

When using a protocol mode, make sure to count in packet overhead when calculating network performance. Refer to the section on *Protocol Modes* for details on each format.

## 5.2. Network Commands

Network commands are used to set up a WIT2410 network and to set radio addressing and configuration.

Command	Description
wb[? 0 1]	Set Transceiver Mode 0 = remote (default) 1 = base station
wd[? 1-3f]	Set Default Handle Used to override automatic handle assignment by the base station 30 = default
wg[? 0 1]	Enable Global Network Mode 0 = Link only to hop pattern specified by wn parameter (default) 1 = Link to any hop pattern, regardless of wn parameter
wl[? 0-ff]	Set lockout key allowing network segregation beyond network number 0 = default
wn[? 0-3f]	Set Hopping Pattern (Network Number) 0 = default
wp[? 0 1]	Set Transmit Power 0 = 10mW 1 = 100mW (default)
wr?	Read Receive Signal Strength
wu[? 0 1]	Set Point-to-Point Direct Mode 0 = Multipoint mode (default) 1 = Point-to-point direct mode
dx[? 0-ff] (remote only)	Set Range optimization 0 = default

*Set Transceiver Mode*

Sets modem operation as either base station or remote. Default is remote.

*Set Default Handle*

Sets handle number between 1 and 62 inclusive for a remote. This handle will override the automatic handle assignment by the base station. This command can be used in applications where it is desired to have specific modems have specific handles. When specified for the base, the default handle determines which remote it will address when transparent protocol mode is in effect. When **3FH** is specified for the base, broadcast mode is entered.

*Enable Global Network Mode*

For networks with multiple base stations, remotes are ordinarily only able to link to one base station, set by the hopping pattern. Mode 1 enables the global mode that allows remotes to link to any base station they can hear, acquiring whatever hop pattern is required. In this mode a remote can only change base stations once it is no longer registered with a base station.

*Set Lockout Key*

Allows further network segregation beyond the network number. This feature allows multiple co-located networks in which global roaming is enabled. In global roaming, a remote is allowed to link to any base regardless of the network number as long as the lockout key agrees. By using different lockout keys, the bases to which remotes link can be limited or segregated.

*Set Hopping Pattern*

The WIT2410 has 64 preprogrammed hopping patterns (also referred to as network numbers). By using different hopping patterns, nearby or co-located networks can avoid interfering with each other's transmissions. Even if both networks tried to use the same frequency, on the next hop they would be at different frequencies.

*Set Transmit Power*

The WIT2410 has two preset transmit power levels, 10mW (10dBm) and 100mW (20dBm). Control of the transmit power is provided through this command. Default is 100mW.

*Read Receive Signal Strength Indicator (RSSI)*

This command reports the relative signal strength averaged over the last 10 hops. This command returns a one byte value that is proportional to received signal strength and can range from **00H** to **FFH**. Typical values range from **30H** to **80H** where the lower the number the lower the received signal strength and the higher the number the higher the received signal strength. This is a relative indication and does not directly correspond to a field strength number. This is available only at the remotes as the base station is the only source that transmits on a regular basis. Plus, in a point-to-multipoint network the base will receive different signal strengths from each remote.

*Set Point-to-Point Direct Mode*

Sets point-to-point mode that is recommended for point-to-point applications, especially where the remote radio is mobile and may leave and re-enter the range of the base. This mode fixes the remote handle assignment to always be 30H and improves the re-registration process. Must be set in both base and remote radios.

*Set Range Optimization (remote only)*

This command applies an adjustment factor to the over-the-air timing of remotes to compensate for the effects of propagation delay at long ranges. The default setting of **00H** is suitable for ranges of 0 to 0.8 miles (1287 m), with optimal performance at 0.1 miles (162m). Each increment of this parameter adds 0.1 miles (162 m) to the working range. Thus the optimal and max ranges are determined by:

$$\begin{aligned} \text{optimal} &= 0.1\text{mi} + 0.1\text{mi} \times \mathbf{dx} = 0.17\text{km} + 0.17\text{km} \times \mathbf{dx} \\ \text{max} &= 0.8\text{mi} + 0.1\text{mi} \times \mathbf{dx} = 1.33\text{km} + 0.17\text{km} \times \mathbf{dx} \end{aligned}$$

The following table presents various values of dx and the associated optimal and max ranges.

<i>dx setting</i>	<i>range: min</i>	<i>optimal</i>	<i>max</i>
00H	0mi/0km	0.1mi/0.2km	0.8mi/1.3km
01H	0mi/0km	0.2mi/0.3km	0.9mi/1.5km
04H	0mi/0km	0.5mi/0.8km	1.2 mi/2.0km
06H	0.1mi/0.2km	0.7mi/1.2km	1.4mi/2.3km
09H	0.4mi/0.7km	1.0mi/1.6km	1.8 mi/3.0km
13H	1.4mi/2.3km	2.0mi/3.3km	2.8mi/4.7km
31H	4.4mi/7.3km	5.0mi/8.3km	5.8 mi/9.7km
45H	6.4mi/10.7km	7.0mi/11.7km	7.8mi/13.0km
64H	9.4mi/15.7km	10.0mi/16.7km	10.8mi/18.0km
C8H	19.3mi/32.3km	20.0mi/33.3km	20.8mi/34.7km
FAH	24.4mi/40.7km	25.0mi/41.7km	25.8mi/43.0km

*Optimal 'dx' setting for various distances.*

### 5.3. Protocol Commands

These commands can be used to tune the transceiver for optimum transmission of data across the RF link. For most applications, the default values are adequate.

Command	Description
pe[? 0-B]	Set Alternative Frequency Band 0 = USA operation. (~2400 – 2472MHz) (default) 1 = ~2448 – 2474MHz, avoids 11b channels 1 – 6 & 14 2 = Spain (~2448 – 2474MHz), avoids 11b channels 1 – 6 & 14 3 = Japan (~2471 – 2497MHz), avoids 11b channels 1 - 10 4 = Canada (~2452 – 2477MHz), avoids 11b channels 1 – 6 & 14 5 = ~2400 – 2425MHz, avoids 11b channels 6 - 14 6 = ~2409 – 2435MHz, avoids 11b channels 8 - 14 7 = ~2419 – 2445MHz, avoids 11b channels 1 & 10 – 14 8 = ~2430 – 2455MHz, avoids 11b channels 1, 2 & 12 – 14 9 = ~2440 – 2465MHz, avoids 11b channels 1 – 4 & 14 A = ~2449 – 2475MHz, avoids 11b channels 1 – 6 & 14 B = ~2459 – 2485MHz, avoids 11b channels 1 – 7
ph[? 00-fe] (base only)	Set Hop Duration 90H = default (=10ms)
pk[? 00-d0]	Set Minimum Data Length 01 = default
pl? (remote only)	Get Maximum Data Length (read only) D4 = default (=212 bytes)
pn[? 01-3e] (base only)	Set Maximum Number of Remotes 3e = default (=62 remotes)
pr[? 00-ff]	Set Packet Attempts Limit 10H = default FFH = Infinite retry (RF flow control point-to-point only)
pt[? 00-ff]	Set Data Transmit Delay 00H = default
pv[? 0 1] (base only)	Set Slot Assignment Mode 0 = default (dynamic slot assignment) 1 = static slot assignment
pw[? 00-34] (base only)	Set Base Slot Size 08H = default (=32 bytes)
px[? 0 1]	Set ARQ mode. 0 = ARQ enabled (default) 1 = ARQ disabled (redundant transmission)

**Note:** Incorrect setting of these parameters may result in reduced throughput or loss of data packets.

#### *Set Alternative Frequency Band*

When set to 1, limits the operating RF channel set to the 2448 to 2473MHz frequency band for compliance with French regulatory standards. When set to 2, sets appropriate operation for Spain. When set to 3, sets appropriate operation for Japan. This setting



should be set to 0, for FCC-compliant operation in the US (this is the default). For Canadian operation, set this parameter to 4.

Additional 25 channel bands have been provided to avoid hopping through the various 802.11b channels. If the WIT2410 is to be used in close proximity to 802.11b networks, these alternative hopsets can be used to avoid interfering with the 802.11b networks.

#### *Set Hop Duration*

Sets the length of time the transceiver spends on each frequency channel. A smaller value will allow the remote to lock on to the base signal faster at system startup, and will generally decrease packet latency. A larger value increases network capacity, due to decreased overhead in channel switching. The hop duration is specified in 69.4 $\mu$ s increments. The default value of **90H** corresponds to a duration of 10ms. The maximum value of **FEH** is 17.627ms. For best results, do not specify a duration of less than 3 ms. This value only needs to be set in the base which broadcasts the parameter to all remotes. However, link time can be reduced if this value is also programmed into the remotes, which use it as a starting value when scanning for the base.

#### *Set Minimum Data Length*

This sets the minimum threshold number of bytes required to form a packet in transparent mode. The radio will wait until the *data transmit delay* elapses before sending a data packet with less than this number of bytes. Can be used to keep short, intermittent transmissions contiguous. In packet modes, the length parameter in the data packet will override this value (See Section 3.1). This value is subject to the *maximum data length* even in packet mode. See *Get Maximum Data Length* below.

#### *Get Maximum Data Length (remote only, read only)*

This parameter indicates the largest number of bytes that a remote will transmit per hop, based on the size of the slot it has been allocated by the base. In general more remotes mean less data can be transmitted per remote. By reading this parameter and dividing by the hop duration, the remote's data rate capacity can be determined. Attempting to send protocol mode packets longer than *maximum data length* will result in the packet being discarded without being sent. See Section 2.3.3 on the tradeoffs between *hop duration* and data length.

#### *Set Maximum Number of Remotes (base only)*

This parameter limits the number of remotes that can register with a given base. The default is 62 remotes which is the maximum number of remotes that can be registered with a base at one time. This command is useful when used in conjunction with global roaming for load balancing when base stations are collocated. It is also useful to assure a minimum remote throughput.

#### *Set Packet Attempts Limit*

If *ARQ Mode* is set to 0, sets the number of times the radio will attempt to send an unsuccessful transmission before discarding it. If *ARQ Mode* is set to 1, it is the number of times every transmission will be sent, regardless of success or failure of a given

attempt. When this parameter is set to **FFH**, RF flow control mode is entered for transmissions from the radio (See Section 2.3.4). This mode can be entered for one or both radios in a point-to-point system. When used in a point-to-point system the **wu** parameter should be set to 1. Using this mode in a point-to-multipoint system will stop transmissions to all radios when any one radio has a full buffer or if the base radio attempts to send data to a remote that has recently (<2.5 seconds) left the range of the base.

#### *Set Data Transmit Delay*

When used in conjunction with the *minimum data length* parameter, this sets the amount of time from the receipt of a first byte of data from the host until the radio will transmit in transparent mode. Default is **00H** which causes transmission to occur without any delay. When a host is sending a group of data that needs to be sent together, setting this parameter will provide time for the group of data to be sent by the host before the radio transmits. If the length of data to be sent together is longer than the time slot can send, the data will not be sent together but will be broken up over multiple hops. The length of time the radio will wait is equal to the specified value times the hop duration.

#### *Set Slot Assignment Mode (base station only)*

Sets whether the base station will assign remote transmit slots dynamically, based on the number of remotes currently registered or whether the base station will assign remote transmit slots statically, based on the *maximum number of remotes* parameter. If static slot assignment is selected, make sure *maximum number of remotes* is correctly set. Otherwise remote transmit performance will suffer as transmit time will be reserved for remotes that may not exist. The dynamic assignment mode will generally be preferred; however, the static assignment mode will result in a static *maximum data length* parameter.

#### *Set Base Slot Size (base station only)*

Sets the amount of time allocated for transmission on each hop for the base station time slot in 69.4µs increments, corresponding to 4 bytes per unit. Maximum value is **34H** which corresponds to 208 bytes. If using a protocol mode, attempting to send a packet with a length longer than this setting will cause the packet to be discarded.

#### *Set ARQ Mode*

Sets ARQ mode when set to 0 which is the default. In this mode the radio will resend an unsuccessful transmission until either successful or *packet attempt limit* attempts have been made. When set to 1 selects redundant transmit mode that will send every transmission *packet attempt limit* times regardless of success or failure of any given attempt. When redundant transmit mode is used, receiving radios will discard all subsequent retransmissions once the transmission has been successfully received. Thus the receiving host will receive just one copy of the transmission.

## 5.4. Status Commands

These commands deal with general interface aspects of the operation of the WIT2410.

Command	Description
zb[? 0 1]	Banner Display Disable 0 = disabled 1 = enabled (default)
zc[? 0..2]	Set Escape Sequence Mode 0 = disabled 1 = once after reset (default) 2 = unlimited times
zh?	Read factory serial number high byte.
zm?	Read factory serial number middle byte.
zl?	Read factory serial number low byte.
zp[? 0-4]	Set the duty cycle at which the modem will wake up to send and receive data. Duty cycle equals $1/2^N$ where the argument of the command equals N.
zq[? 0 1] (remote only)	Low Power Acquisition Mode Enable 0 = Disabled (default) 1 = Enabled
z>	Exit Modem Control Mode

### *Banner Display Disable*

Enables or disables display of the banner string and revision code automatically at power-up. May be disabled to avoid being mistaken for data by the host.

### *Set Escape Sequence Mode*

Enables or disables the ability to use the in-data-stream escape sequence method of accessing Control Mode by transmitting the string ":wit2410". When this mode is set to 1, the escape sequence only works immediately after reset (this is the default). When set to 2, the escape sequence may be used at any time in the data stream when preceded by a pause of 20 ms. For backwards compatibility with the WIT2400, the string ":wit2400" is also accepted for entering Control Mode. Note that the escape sequence must be interpreted as data by the radio until the last character is received, and as such will be generally be transmitted to a receiving radio station, if any.

### *Read Factory Serial Number High, Middle and Low Bytes.*

These read only commands return one of the three bytes of the unique factory-set serial number, which are also visible in the startup banner.

### *Set Duty Cycle*

Allows reduced power consumption by having a remote wake up only every  $2^N$  hops to receive and transmit. Power consumption is roughly proportional to the duty cycle selected. For example, if  $N=2$ , the remote will wake up every fourth hop. Power

consumption will be roughly  $\frac{1}{4}$  the consumption as when  $N=0$ . This parameter must be set to the appropriate value when more than 16 remotes are in use.

*Enable Low Power Acquisition Mode.* When a remote is searching for a base to acquire and register with, it scans the frequency band very rapidly. This mode consumes about 80mA of current during this mode. To reduce the frequency consumption when a remote is in acquisition mode, a low power acquisition mode is provided. In this mode, the remote only scans the frequency band every other hop. This will reduce the average current consumption during acquisition to about 40mA. The tradeoff is it can take twice as long to acquire and register with a base, or up to 4 seconds.

## 5.5. Memory Commands

The WIT2410 allows the user to store a configuration in nonvolatile memory, which is loaded during the initialization period every time the radio is powered up. Note that changes to the serial port baud rate from recalling the factory defaults or recalling memory will not take effect until DTR is toggled or power to the radio is cycled.

Command	Description
m0	Recall Factory Defaults
m<	Recall Memory
m>	Store Memory
m!	Display Modified Parameters

### *Recall Factory Defaults*

Resets the WIT2410 to its factory default state. This is useful for testing purposes or if there is a problem in operation of the system and the configuration is suspect. Use the *Store Memory* command afterwards if you wish the factory default settings to be remembered the next time you cycle power or reset the radio.

### *Recall Memory*

Useful for restoring the power-on settings after experimenting with temporary changes to data rate, protocol or network parameters, etc.

### *Store Memory*

This command is necessary after any command to change the data rate, transceiver address, or other radio setting that you wish to make permanent.

### *Display Modified Parameters*

This command lists all parameter settings that are different from the factory default settings. This will list changed parameters whether or not they have been stored with the m> command. Note that issuing this command will cause the radio to lose link with the base and will cause all remotes to lose link when issued to the base radio.

## 5.6. Modem Command Summary

### *Serial Commands*

sd[?|00..ff] Set Data Rate Divisor  
 sp[?|00..14] Set Protocol Mode

### *Network Commands*

wb[?|0|1] Set Transceiver Mode  
 wd[?|1..3f] Set Default Handle  
 wl[?|0..ff] Set Lockout Key  
 wn[?|00..3f] Set Hopping Pattern  
 wg[?|0|1] Enable Global Network Modes  
 wp[?|0|1] Set Transmit Power  
 wr? Read Receive Signal Strength (remote only)  
 wu[?|0|1] Set Point-to-Point Direct Mode  
 dx[?|0..62] Set Range Optimization (base only)

### *Protocol Commands*

pe[?|0..4] Set Alternative Frequency Band  
 ph[?|00..fe] Set Hop Duration (base only)  
 pl? Get Maximum Data Length (remote only, read only)  
 pn[?|01..3e] Set Maximum Number of Remotes (base only)  
 pk[?|00..d4] Set Minimum Data Length  
 pr[?|00..ff] Set Packet Attempts Limit  
 pt[?|00..ff] Set Data Transmit Delay (remote only)  
 pv[?|0|1] Set Slot Assignment Mode (base only)  
 pw[?|00..34] Set Base Slot Size (base only)  
 px[?|0|1] Set ARQ Mode

### *Status Commands*

zb[?|0|1] Banner Display Disable  
 zc[?|0..2] Set Escape Sequence Mode  
 zh? Read Factory Serial Number High Byte  
 zm? Read Factory Serial Number Middle Byte  
 zl? Read Factory Serial Number Low Byte  
 zp[?|0..4] Set Duty Cycle  
 zq[?|0|1] Enable Low Power Acquisition (remote only)  
 z> Exit Modem Control Mode

### *Memory Commands*

m0 Recall Factory Defaults  
 m< Recall Memory  
 m> Store Memory  
 m! Display Changed Parameters

Note: Brackets ([,]) as used here denote a set of optional arguments. Vertical slashes separate selections. For example, given the string wn[?|00..3f], legal commands would be wn?, wn0, wn3, and wn2a. Most commands which set a parameter also have a ? option which displays the current parameter setting; e.g., wn?.

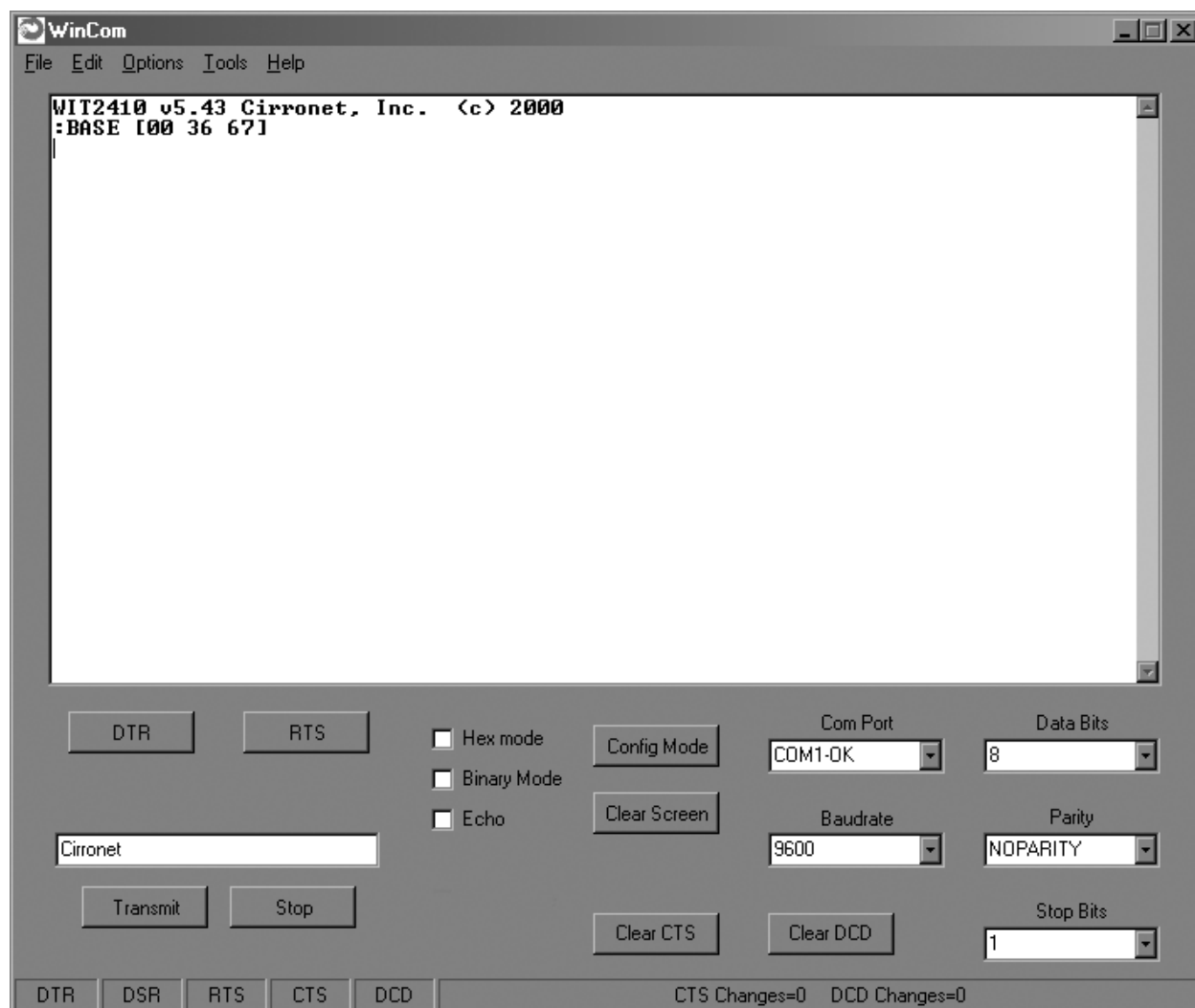
## 6. WIT2410 DEVELOPER'S KIT

The WIT2410 Developer's Kit contains two self-contained wireless modems (HN-510s) built around the WIT2410M OEM module. In addition, two WIT2410M OEM modules are included in the kit. The self-contained units allow developers to get up and running quickly using standard RS-232 interfaces without having to build a CMOS level serial interface. In addition, the self-contained modems include status LEDs to provide modem status information visually. The built-in battery pack allows the developer to use the modems without being tethered to a power source. This provides a simple way to test the range of the radios. Other than the true RS-232 signals of the serial interface, the self-contained modems operate exactly as the OEM modules.

Connection is made to the HN-510s through a standard DB-9 connector. The HN-510s are set up as DCE devices requiring the use of a straight-through cable to connect to DTE devices. The pinout is provided in Section 7.3. The modems can be used with just a three wire connection. Transmit data, receive data and ground are the three required connections. Note that in this configuration, no flow control is available as the WIT2410 does not support software flow control.

When the developer's kit is shipped from the factory, one HN-510 is set up as a base station and the other is set up as a remote. The interface rate for both modems is set at 9600 bps. The default setting for the network key allows the modems to communicate without changing any settings. As a quick test, separate the two modems by about 5 feet, plug in the power and turn the modems on. Do not connect the modems to any device. The Carrier Detect (CD) LED on the base station will come on immediately. After a few seconds, the CD LED on the remote will come on. This indicates that the modems have synchronized and have established a communications link.


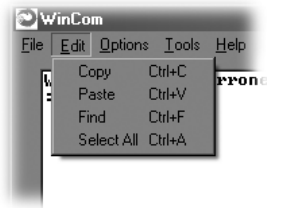
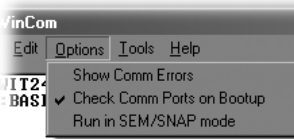
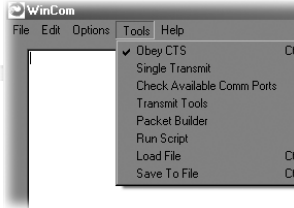

An important point to remember is that if the base station is in Sleep mode, no communications can take place until (1) the base station is taken out of sleep mode and (2) the remote has synchronized with the base station. As the Sleep signal is brought out on the pin usually occupied by DTR, connecting the base station to a PC serial port with DTR de-asserted will put the modem into sleep mode. Some communications programs will attempt to communicate immediately after asserting DTR. The base station will transmit this data, but the remote will not be synchronized with the base station and will not receive the transmission. In this instance, do not connect the Sleep signal to DTR of the serial port.



## 7. WinCOM

Provided with the developer's kit is a configuration program designed especially for Cirronet's wireless industrial transceivers or WIT radios. WinCOM is located on the Manuals and Software CD included in the developer's kit. Install WinCOM by navigating to the Software Tools directory on the Manuals and Software CD and double-click on wincom2.1.exe follow the installation wizard. Once it has installed, open WinCOM by double-clicking on the WinCOM icon on the desktop.

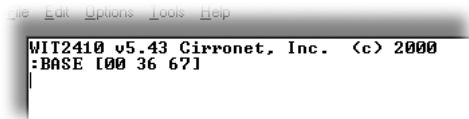
WinCom's menu structure is typical of Windows conventions with File, Edit, Options, Tools and Help selections.

 <p>A screenshot of the WinCom application window with the File menu open. The menu items are: Save Settings (Ctrl+S), Print (Ctrl+P), and Exit.</p>	<p>Under File, Save Settings (Ctrl S) saves the current WinCom settings to the hard drive, Print (Ctrl P) sends whatever text is in the display field to the printer and Exit terminates the program.</p>
 <p>A screenshot of the WinCom application window with the Edit menu open. The menu items are: Copy (Ctrl+C), Paste (Ctrl+V), Find (Ctrl+F), and Select All (Ctrl+A).</p>	<p>Under Edit, Copy, Paste, Find (search) and Select All perform the familiar Windows functionality in typical fashion.</p>
 <p>A screenshot of the WinCom application window with the Options menu open. The menu items are: Show Comm Errors, Check Comm Ports on Bootup (checked), and Run in SEM/SNAP mode.</p>	<p>The Options menu contains the selections, Show Comm Errors which lists any errors encountered in the PC UART. Check Comm Ports on Bootup tells WinCom to verify each available port and lists them as such in the Com Port drop down field.</p>
 <p>A screenshot of the WinCom application window with the Tools menu open. The menu items are: Obey CTS (Ctrl+O), Single Transmit, Check Available Comm Ports, Transmit Tools, Packet Builder, Run Script, Load File (Ctrl+L), and Save To File (Ctrl+S).</p>	<p>See the section entitled WinCom Tools for an explanation of this drop down.</p>
 <p>A screenshot of the WinCom application window with the Help menu open. The menu item is: About.</p>	<p>The Help menu displays the About screen which lists the version number, hardware and software information for the system being used.</p>



## 7.1. Starting the program

When started, WinCOM de-asserts and re-asserts the DTR line to the radio which resets the radio causing the sign-on banner to be displayed. If the baud rate on the computer doesn't match the baud rate of the radio, illegible characters will be displayed. By hitting the PgUp or PgDn key to change the baud rate, then pressing F1 twice to toggle DTR (resets the radio) and causes a new banner to be displayed. Continue changing baud rates in this fashion until a legible banner is displayed as shown below.

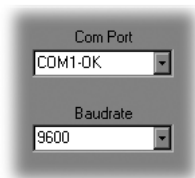


```

File Edit Options Tools Help
WIT2410 v5.43 Cirronet, Inc. <c> 2000
:BASE [00 36 67]

```

The banner indicates the radio firmware version, whether the radio is operating as a base or a remote and the unique factory serial number of the radio module. If nothing is displayed in the communications window of WinCOM, verify the COM port and baud rate settings, then reset the radio (by hitting F1 twice). Cycling power to the radio also will cause the sign on banner to be displayed unless the banner is disabled via the Banner Display Disable command (**zb0**).



The COM port and baud rate can be changed using the drop down menus on the bottom right. All the available COM ports will be listed in the menu but will have OK or N/A designated. If another program that uses a COM port is open, that COM port will not be available for use by WinCOM.



The boxes on the lower right of the WinCOM window provide the status of the COM port flow control being used to communicate with the radio. Note that DCD is only asserted by radios configured as remotes when they are linked to a base radio. Radios configured as bases always assert DCD even if no remotes are linked. Clicking on the DTR or RTS buttons will change the state of the respective signal line in the COM port.

The radio is normally in data mode – data that is sent to it from the PC is transmitted over the wireless connection. When the WinCOM window is active, keys typed on the keyboard will be sent to the radio and will be transmitted. Unless the “Echo” box is checked the typed data will not be displayed in the WinCOM window of the sending radio.

To change configuration parameters, the radio must be put into configuration mode by clicking on the Config Mode button on the WinCOM window immediately after opening WinCOM or after cycling power to the radio. Another method is to toggle the DTR by pressing the F1 key twice, which de-asserts then re-asserts DTR, then pressing the F3 key (or Config Mode button).

```
WIT2410 v5.43 Cirronet, Inc. <c> 2004
:BASE [00 36 6?]
>
```

When the radio is in configuration mode, a “>” prompt character is displayed in the WinCom window as shown above. Configuration parameters are sent to the radio by entering them in the WinCom window after the “>” prompt and pressing the Enter key.

```
:BASE [00 36 6?]
WIT2410 v5.43 Cirronet, Inc. <c>
:BASE [00 36 6?]
> xd0
Error
>
```

If an invalid command or value is entered, the radio will respond with “Error” as shown above. Until the command to save the parameters (**m>**) is issued, the new parameters will only be valid until power is cycled or DTR is toggled by pressing the F1 key twice.

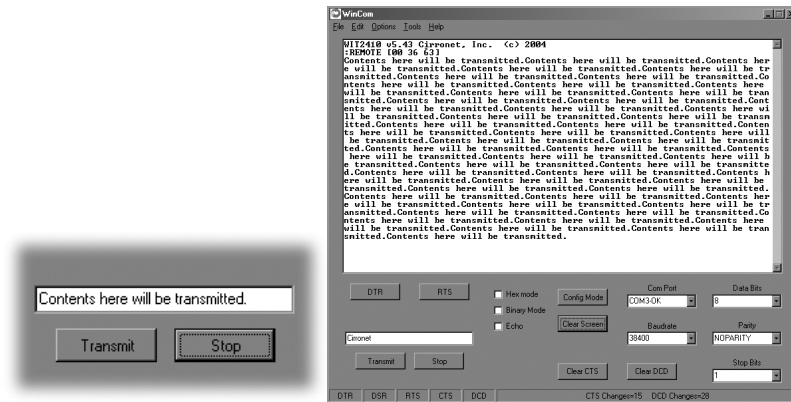
New parameter values that have been issued are saved to non-volatile memory using the “**m>**” command. Refer to the *Memory Commands* section for details on this and other helpful memory commands.

To exit configuration mode from the WinCom screen, use the “**z>**” command and press Enter as shown below.

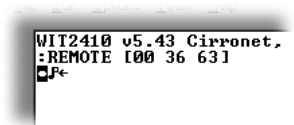
```
WIT2410 v5.43 Cirronet, Inc. <c>
:BASE [00 36 6?]
> m0
> z>
```

The return to the data mode is indicated by an absence of the “>” prompt. Refer to the *Configuration Commands* section below for details on all the configurable parameters.

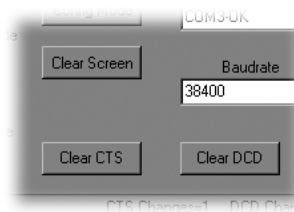
When the radio is linked to another radio, a communications test can be run by clicking on the Transmit button or pressing the F6 key. Whatever ASCII string is in the Transmit String window will be transmitted as shown below.



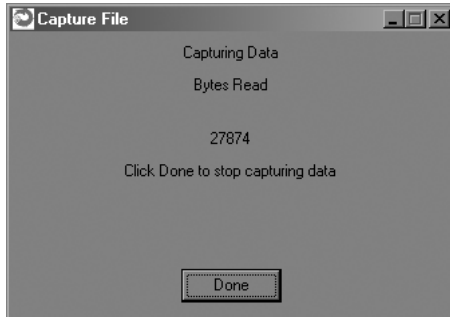
If the other radio is sending data, the received data will be displayed in the WinCOM window.



If the Binary box is checked, all characters received will be displayed subject to the limitations of Windows. For example, a carriage return will not return the cursor to the left side of the window but the character corresponding to 0x0d value of the carriage return will be displayed. Similarly, if the Hex Mode box is checked, all characters are displayed in hexadecimal format.



The Clear Screen button deletes all the text in the display window. The Clear CTS and Clear DCD buttons reset the respective changes counters to zero.



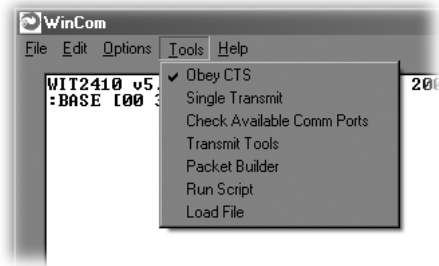
After naming the file and clicking on OK, the Capture Data window opens and shows the amount of data being received. Clicking on Done stops the loading of received data into the file.

## 7.2. Function Keys

All of the function key shortcuts are described below:

- F1** Toggles state of DTR (Sleep). State is shown in status line.
- F2** Toggles state of RTS. State is shown in status line.
- F3** Transmits “:wit2400”. Used to enter control mode.
- F5** Toggles local echo. If you are transmitting characters through one modem to another WIT2450, this allows you to see what you are typing.
- F6** Toggles stream mode. Causes WinCOM to transmit a repeating pattern of characters. Useful for testing.
- F8** Toggles binary mode. Displays extended ASCII and control characters. Useful for testing.
- PgUp** Sets data rate of PC serial port to next higher value. Value is displayed in status line. Useful when WinCOM is used to change the WIT2450 interface data rate. WinCOM can communicate at new data rate without having to exit and re-enter WinCOM.
- PgDn** Sets data rate of PC serial port to next lower value. Value is displayed in status line.

### 7.3. WinCom Tools

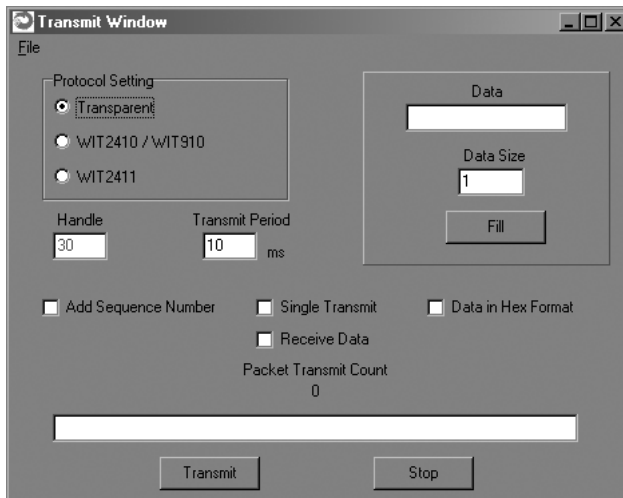


There are seven selections under the Tools menu. The first, Obey CTS is useful when just a three wire connection is made between the radio and the computer. Some PCs let the CTS input line float. If CTS is not asserted, the PC COM port will not send data.

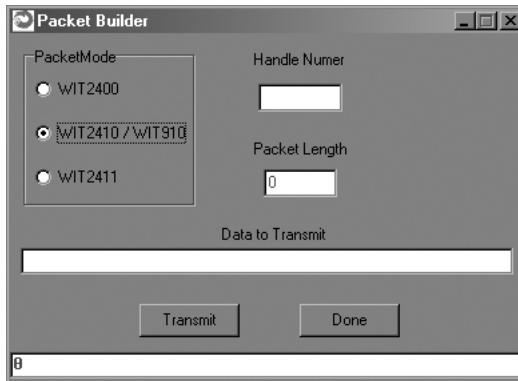
***Note: Unchecking this selection will have the PC COM port ignore the state of CTS and transmit data.***

When WinCOM's transmit mode is used, data is sent continuously until the user stops it by clicking on Stop or pressing F6. If the second tool, Single Transmit, is checked, clicking the Transmit button will send the Transmit String a single time. There is no need to click Stop. Clicking on the Transmit button a second time will have the string transmitted a second time.

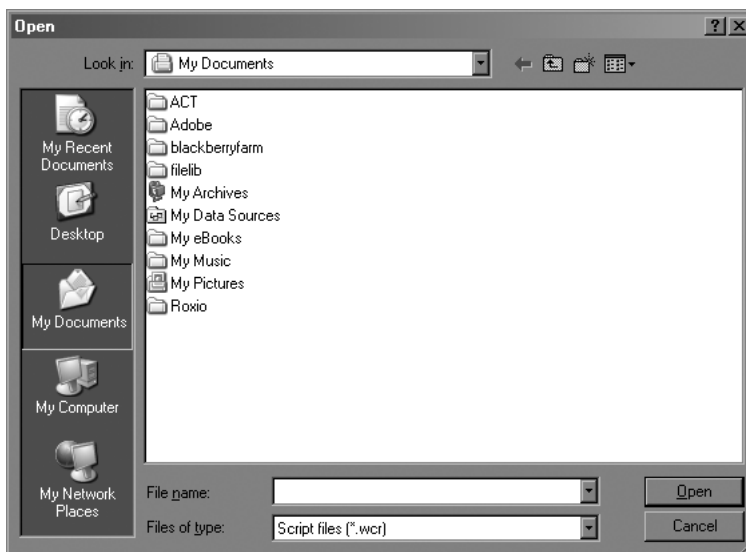
The third allows for checking of available Comm Ports and is useful for refreshing the list.



The fourth, Transmit Tools allows for testing of the Transparent, WIT2410/WIT910 or WIT2411 settings. Parameters related to how the transmission will take place can be set including Handle, Transmit Period, whether or not a Sequence Number should be added, if the Transmission will be continuous or one time, if the data should be sent in Hex Format and whether or not data can be received. Data is entered into the Data field, then Data Size can be set and clicking Fill loads the data into the Transmit Field.



The Packet Builder is an easy way to test the multipoint addressing mode of the WIT241x radio. Since the WIT241x operates in a star configuration in multipoint mode, only the base radio needs to address data to specific remotes. All remotes send data back to the base and do not need to address the data to the base. To send a packet of data to a specific remote in a multipoint network, enter the handle of the desired remote in the Handle window. Type whatever data to be transmitted in the Data to Transmit window. In the bottom window, you will see the entire packet being built as the data is entered in the windows. When all the data has been entered, click on the Transmit button to send the data.



WinCOM has the ability to perform any function or sequence of functions WinCOM can perform through a script file. A script file is a text file that contains one or more commands and arguments save with a wcr filename extension. Each command is separated by a carriage return and linefeed. Configuration commands need to have wait periods between them. The list of commands and their definitions is below:

## 7.4. Script Commands

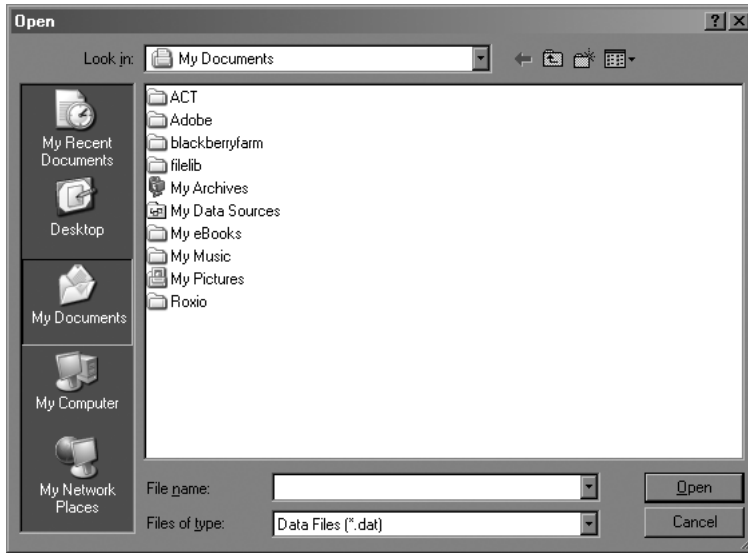
cp <arg>	Selects the COM port to use
br <arg>	Selects the baud rate to use
do	Asserts DTR
df	De-asserts DTR
ro	Asserts RTS
rf	De-asserts RTS
cm	Sends configuration escape sequence
oo	Obey CTS/RTS
of	Do not obey CTS/RTS
sc <cmd(arg)>	Send WIT910 format configuration command
wt <arg>	Pause for arg milliseconds

An example script file is shown below:

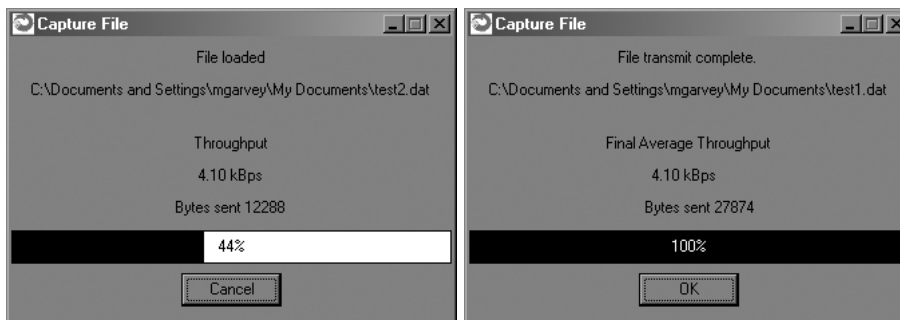
```
br 115200
df
wt 200
do
wt 200
cm
wt 200
sc m!
```

This script file sets the baud rate of the PC COM that WinCOM is using to 115,200 kbps, de-asserts DTR, waits 200 milliseconds, asserts DTR, waits 200 milliseconds, sends the configuration mode escape sequence, waits 200 milliseconds and then sends the m! command to the radio. What this script file does is set the PC COM port baud rate to 115.2 kbps, puts the radio in config mode and the issues the command to display all of the radio parameters that have been changed from factory default. Note that this script file leaves the radio in config mode. Cycling power or toggling DTR will return the radio to data mode.

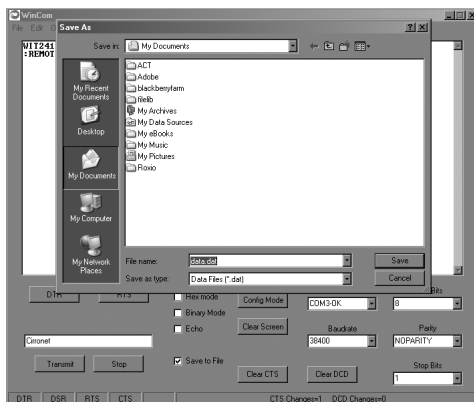
WinCOM prompts you to select the desired .wcr file. Opening the script file causes it to executed immediately.



The seventh tool allows the loading of a data file for transmission. Navigate to a file then click Open and the file is transmitted immediately.



The Capture File dialog displays with a bar showing loading progression. Once the file has finished transmitting, the Final Average Throughput and Bytes sent numbers will be displayed.



Finally, the eighth tool is Save to File which launches a Save As dialog that allows any data received to be loaded into a file.



## 7.5. Demonstration Procedure

The procedure below provides a quick demonstration of the WIT241x.

1. Attach a transceiver to each computer, preferably between 5' and 30' apart for convenience.
2. Start WinCOM running on both computers. If you prefer, almost any other serial communications program such as Procomm or QModem set for 9600 bps will also work.
3. Turn the radios on and use the function keys to set DTR and RTS to 1 (if you are using a terminal program other than COM24, these are typically set automatically). The radio should respond by setting both DSR and CTS to 1, and transmit a short sign-on message including the firmware version and whether the unit is configured as a base or remote. Watch the states of the hardware control lines on the status bar as you do this. The DCD indicator should be lit on the base station. After a few seconds, the remote unit will acquire the base station's signal and also assert its DCD signal.
4. Access modem control mode for each unit. To access modem control mode, use the F1 key to toggle DTR to 0 and back to 1 and then press the F3 key, which sends the ":wit2400" escape sequence. If you are not using COM24, simply turn the radio off and back on and then type ":wit2400" (must be lower case, no backspace characters). The transceiver should echo back ">" to indicate that you have entered modem control mode. Check the remote unit's hopping pattern by entering "wn?" at the prompt. The remote should respond with "0", the default setting. Check that the base station's hopping pattern matches this by entering "wn?" at the base station.
5. Exit control mode by entering "z>". Do this for both radios. At this point, you should be able to type characters into either radio and see them appear at the other side. If you are using WinCOM, you can press the F6 key to transmit a repeating test pattern.
6. For a range test, disconnect the remote station from the computer and power supply. The DCD indicator should remain lit as long as the base station is in range..
7. Exit COM24 by pressing the ESC key.

## 8. Troubleshooting

### **Radio is not responding.**

Make sure DTR is asserted to bring the radio out of sleep mode. DSR should be on to indicate the radio is ready.

### **Can't enter modem control mode.**

Make sure the host data rate is correct. The WIT2410 defaults to 9600 bps asynchronous. Evaluation units do not have external access to the CFG\_SEL signal; you must use the :wit2410 power-on escape sequence to access modem control mode. The first characters typed after the radio wakes up should be the escape sequence. Make sure you type the colon (:) and enter the letters in lower case; the characters following the colon echo to show you have typed them correctly. If using the “on-the-fly” escape sequence command, make sure a pause of at least 20ms precedes the escape sequence.

### **Remote never detects carrier.**

Check that the base station is running, and that the remote is programmed to the same hopping pattern. Also check that the hop duration for base and remote are the same, and that the remote has a non-zero link margin.

### **Carrier is detected, but no data appears to be received.**

Make sure that RTS is asserted to enable receive character flow. In a point-to-point application, if a remote is not receiving data, check that the base's default handle is the same as the remote's. In a multipoint application, check that the remote is not configured for protocol mode and that the base is using the correct protocol format and destination handle.

### **Radio is interfering with other nearby circuits.**

It is possible for the RF energy envelope to be rectified by nearby circuits that are not shielded for RFI, manifesting as a lower frequency noise signal. If possible, place the antenna at least 1 foot away from the transceiver module, and 3 feet from other circuit boards and obstructions. Place sensitive circuits in a grounded metal casing to keep out RFI.

### **Sign-on banner or modem control mode prompt is unreadable.**

If the problem is repeatable, check whether the data rates between host and transceiver match.

### **Range is extremely limited.**

This is usually a sign of poor antenna coupling. Check that the antenna is firmly connected. If possible, remove any obstructions in the near field of the antenna (~3' radius).

### **Transmitting terminal flashes CTS occasionally.**

This indicates that the transmitter is unable to reliably get its data across. This may be the result of an interfering signal, but most often is caused by overloading of the network. Adjusting the protocol parameters may increase the network efficiency.

**Receiving terminal drops characters periodically.**

Set the number of retries to a high number and send a few characters. Check that the transmitted data can get through under these conditions. Sometimes this symptom is caused by an application that is explicitly dependent on the timing of the received data stream. The nature of the packetized RF channel imposes a degree of unpredictability in the end-to-end transmission delay.

**Cannot communicate with the OEM module.**

Make sure DTR and RTS are asserted. DSR should be on to indicate the radio is ready.

**OEM Module is in an unknown state.**

Use the `m0` command to restore the factory defaults. Note that the serial baud rate must be known for the module to receive this command.

## 9. APPENDICES

### 9.1. Technical Specifications

#### 9.1.1 Ordering Information

WIT2410M4 OEM Module, Serial connector pins down - Standard  
 WIT2410S4 OEM Module, Serial connector pins up

#### 9.1.2. Power Specifications

Vcc Input Range: 3.3v to 10.0v  
 Operating Temperature Range: -30° C to +70° C

Current Consumption (Max transmit power, 230.4Kbps I/O)

Mode	Remote	Base Station
Sleep	50µA	N/A
Standby	20mA	N/A
Typical Average	50mA	80mA
Peak (Tx)	80mA	100mA

#### 9.1.3. RF Specifications

FCC Certification	Part 15.247, no license required
ETSI (European) Certification	brETSI 300.328, no license required
Rated RF Power	+18 dBm (+20 dBm effective radiated)
Line-of-site Range	approx. 6/10 of a mile w/2dB dipole
Frequency Range	2401 – 2495MHz
Number of Channels	75 US; Canada, France, Spain & Japan: 25
Receiver Sensitivity	-93dBm
Channel Data Rate	460Kbps
IF Adjacent Channel Rejection	>55dB

#### 9.1.4. Mechanical Specifications

Weight	35g
Dimensions (including shield)	80.2 x 46.5 x 8.6mm (refer to section 7.6 for mechanical drawing)
RF Connector:	
WIT	Huber/Suhner: 85 MMCX 50-0-1
Mating	Huber/Suhner: 11 MMCX-50-2-3 (straight) Huber/Suhner: 16 MMCX-50-2-2 (rt. angle)
Data/Power Connector:	
WIT	Samtec: DIS5-108-51-L-D
Mating	Samtec: CLP-108-02-G-D (PCB mount) Samtec: FFSD-08 (IDC cable)

## 9.2. Serial Connector Pinouts

Signal	WIT2410M/S4 OEM Pinout	HN-510 DB9 Pinout
GND	1	5
TXD	2	3
RXD	3	2
CFG	4	-
RTS	5	7
SLEEP	6	4
DCD	7	1
CTS	8	8

**Note: The WIT2410M4 is the standard part number and has the serial connector pins pointing down allowing connection to a mother board without using a cable. WIT2410S4 has the serial connector pins pointing up.**

The HN-510 is wired as a DCE device and as such can be connected to DTE devices such as PCs with a straight-through cable. When connecting a HN-510 to a DTE device, a “null modem” cable is required. To effect a null modem cable, cross-wire TXD and RXD and connect ground. The HN-510 can operate with just these three wires connected. However, as the WIT2410 does not support software flow control, there will be no flow control in this mode. If the DTE device fails to respond, connect DCD from the HN-510 to the DTR and RTS inputs to activate the DCE device whenever the WIT2410 asserts carrier.

When connecting to the WIT2410M/S4, make sure that all of the inputs (TXD, CFG, RTS and SLEEP) are terminated for proper operation.

## 9.3. Approved Antennas

The WIT2410M/S4 is designed to ensure that no antenna other than the one fitted shall be used with the device. **The integrator must permanently affix the antenna by using an adhesive on the coupling such as *Loctite***, or ensure the antenna has a unique coupling. The table below lists the antennas which can be purchased directly from Cirronet. Contact Cirronet Technical Support with any questions.

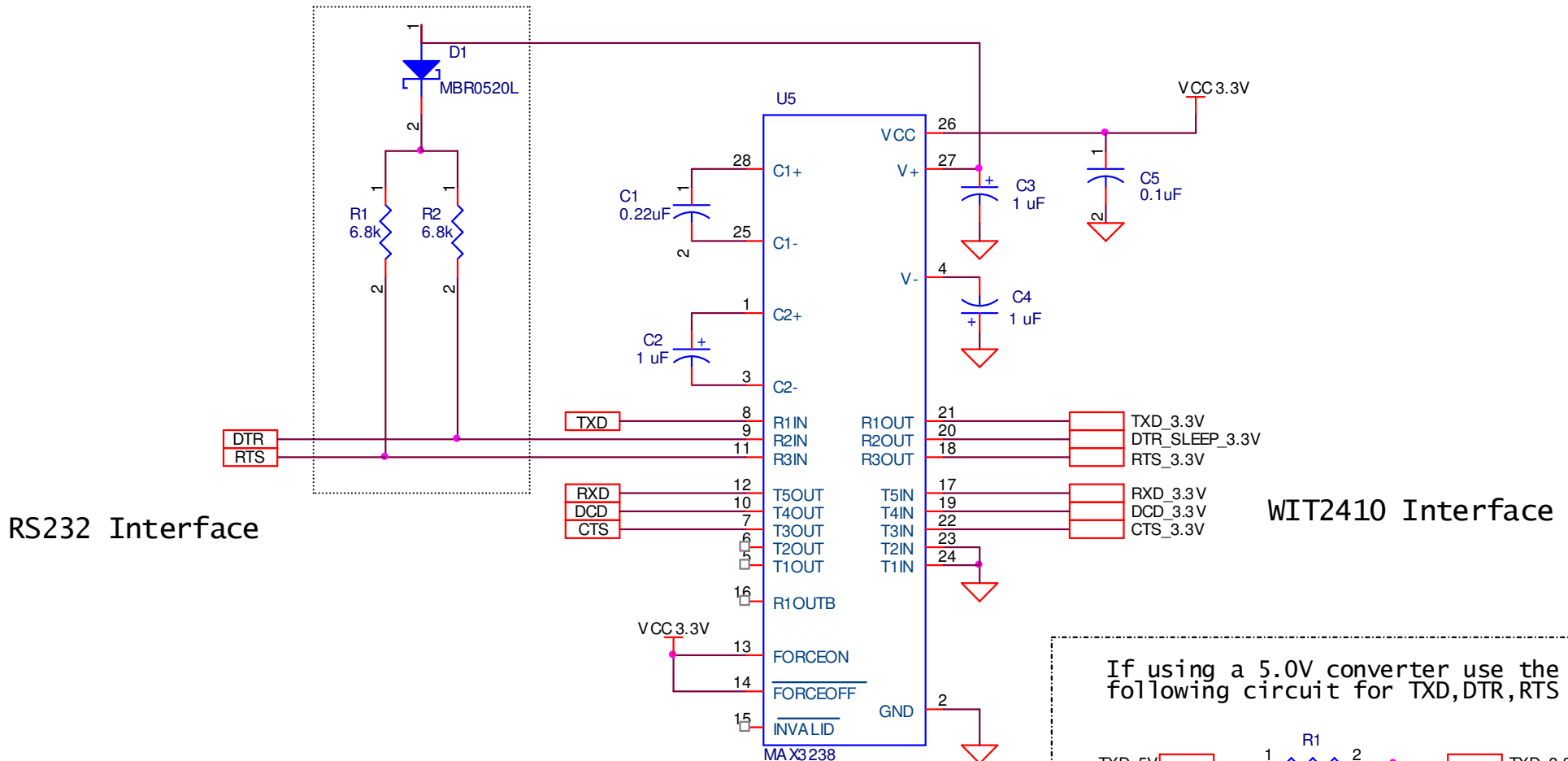
Description	Gain	Part Number	Coupling
24dB Parabolic Dish	24dB	PAR2424	Reverse N
18dB Parabolic Dish	18dB	PAR2418	Reverse N
15dB Yagi Directional	15dB	YAGI2415	Reverse N
14dB Corner Reflector	14dB	CORNER2414	Reverse N
12dB Omnidirectional	12dB	OMNI2412	Reverse N
9dB Omnidirectional	9dB	OMNI249	Reverse N
9dB Corner Reflector	9dB	CORNER249	Reverse N
6dB Cirronet Patch	6dB	PA2400	Reverse MMCX
5dB Mobile Mount	5dB	MAG245	Reverse N
2dB Cirronet Patch	2dB	PA2410	Reverse MMCX
2dB Rugged Body Mount	2dB	RBM242	Reverse N
Dipole	2dB	RWA249R	Reverse SMA

#### **9.4. Technical Support**

For technical support call Cirronet™ at (678) 684-2000 between the hours of 8:30AM and 5:30PM Eastern Time.

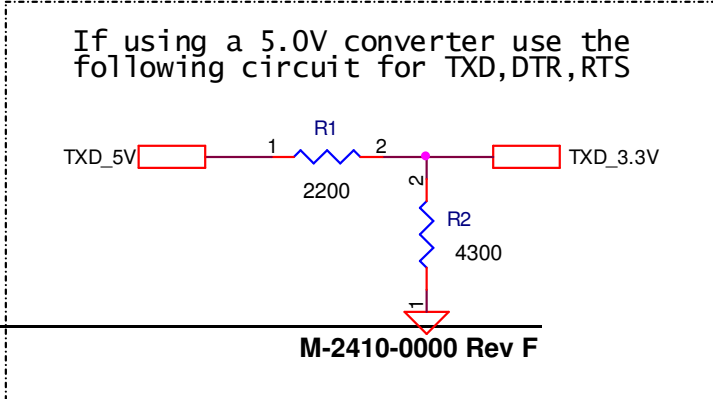
9.5. Reference Design

Optional pullups to keep RTS and DTR asserted when left unconnected

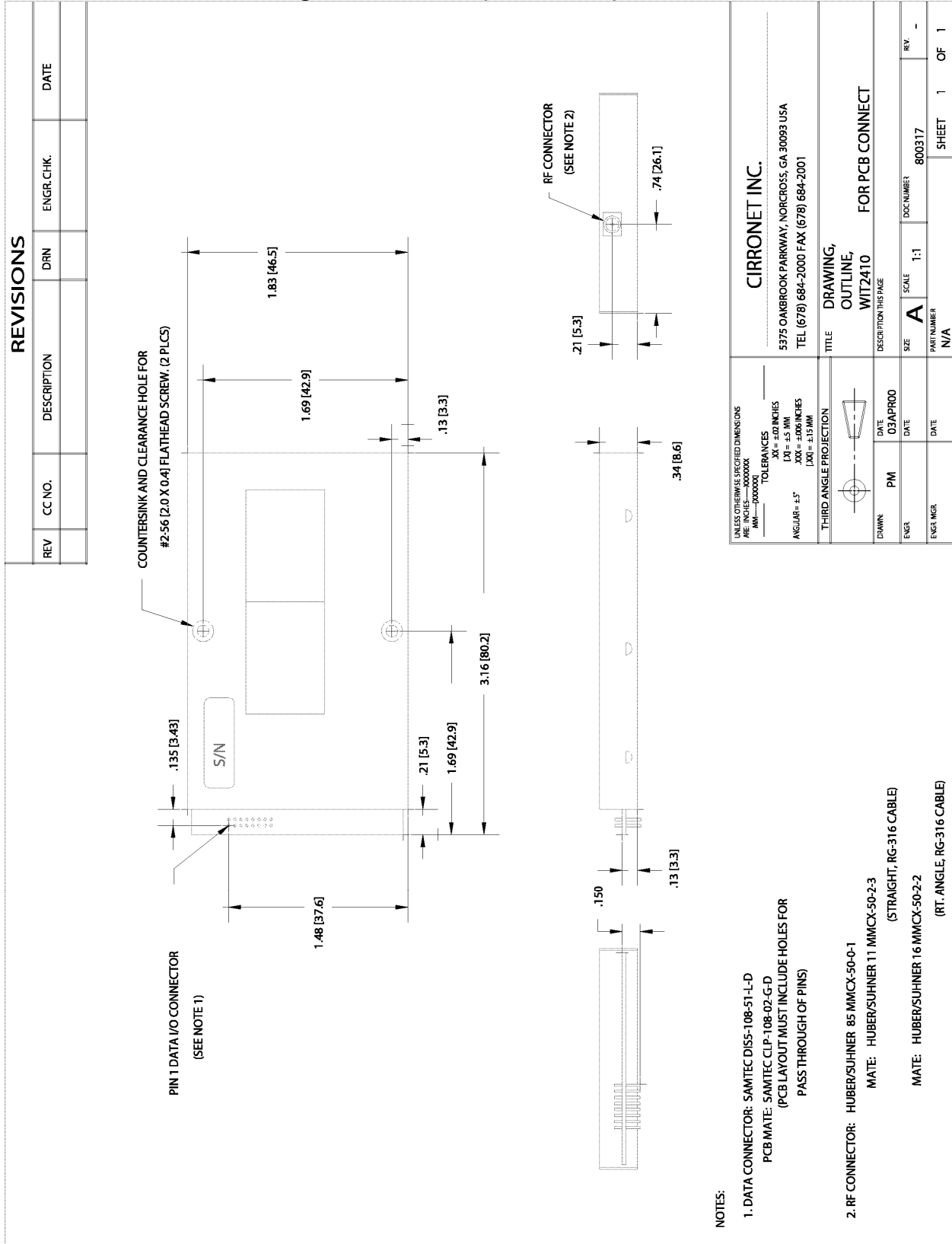


RS232 Interface

WIT2410 Interface



9.6.1. Mechanical Drawing – WIT2410M4 (Pins Down)



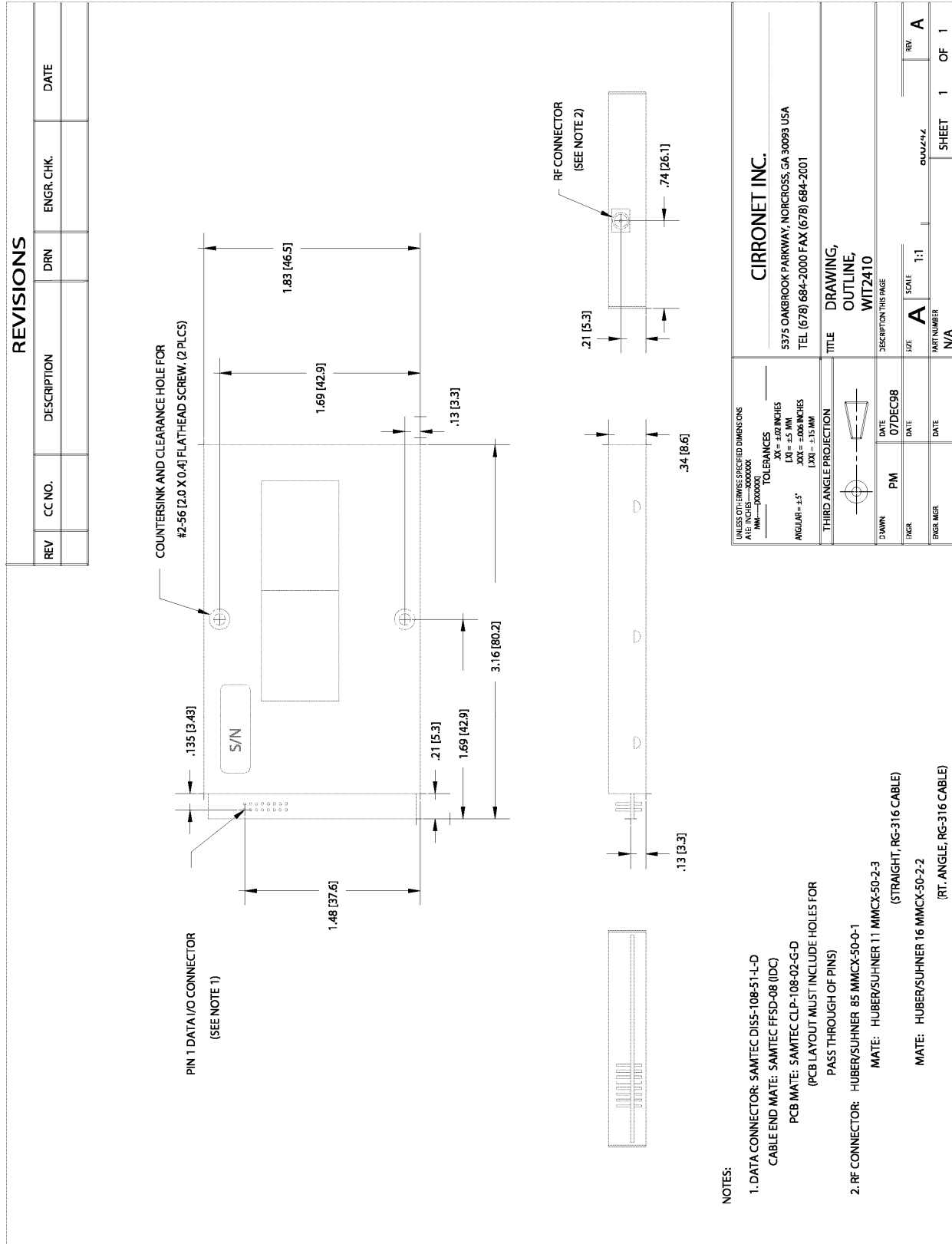
NOTES:

- DATA CONNECTOR: SAMTEC DIS5-108-51-L-D  
PCB MATE: SAMTEC CLP-108-02-G-D  
(PCB LAYOUT MUST INCLUDE HOLES FOR PASS THROUGH OF PINS)
- RF CONNECTOR: HUBER/SUHNER 85 MMCX-50-0-1  
MATE: HUBER/SUHNER 11 MMCX-50-2-3 (STRAIGHT, RG-316 CABLE)  
MATE: HUBER/SUHNER 16 MMCX-50-2-2 (RT. ANGLE, RG-316 CABLE)

<p><b>CIRRONET INC.</b> 5375 OAKBROOK PARKWAY, NORCROSS, GA 30093 USA TEL (678) 684-2000 FAX (678) 684-2001</p>	<p><b>TOLERANCES</b> XX = ±.00 INCHES X = ±.05 MM XX = ±.000 INCHES X = ±.15 MM</p> <p>ANGULAR: ±5°</p>
<p><b>TITLE</b> DRAWING, OUTLINE, WIT2410 FOR PCB CONNECT</p>	
<p><b>DESCRIPTION THIS PAGE</b></p>	
<p><b>DATE</b> 03/APRO</p>	<p><b>SCALE</b> 1:1</p>
<p><b>ENGR</b> PM</p>	<p><b>DOC NUMBER</b> 800317</p>
<p><b>ENGR MGR</b></p>	<p><b>REV</b> -</p>
<p><b>DATE</b></p>	<p><b>SHEET</b> 1 OF 1</p>
<p><b>PART NUMBER</b> N/A</p>	



9.6.2. Mechanical Drawing – WIT2410S4 (Pins Up)



## 10. 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.**



## Appendix I – Operating Scenario for WIT2410P

The WIT2410P is used in a portable application. The system is set up as a star network with a number of radios, called remotes, all linked to one central base radio. These remote radios are installed in belt packs that fit around the waist of the user. Given this configuration, the remote radios will generally be closer than 2.5 cm to the user and will require a portable designation as part of the grant. The Base radio is placed at some central point, usually as high as possible, in the facility to provide better coverage to all remotes.

Any remote can communicate with any other remote by means of data packets routed back and forth through the base radio. The base radio provides synchronization for the entire system, passes messages from one remote to another, and provides broadcast messages for all remotes to hear.

The WIT2410P uses Frequency Hopping technology to mitigate the effects of fading and jamming. The dwell time for this system is set to 10 milliseconds. In any 10 ms dwell period, the following process takes place sequentially in time:

### Start of dwell

1. Base broadcasts messages to all remotes,
  2. Remote #1 sends its message to Base,
  3. Remote #2 sends its message to Base,
  4. Remote #3 sends its message to Base,
  5. Remote #4 sends its message to Base,
  6. Remote #5 sends its message to Base
- To N... Remotes

After the last Remote sends its message to the Base, the 10 millisecond dwell time is complete and all radios hop to the next frequency channel in their hopset and the cycle is repeated.

We are asking for portable designation of the remote radios since they will be operated in close (< 2.5 cm) proximity to the user. The operation of the Base radio is already covered by our current WIT2410G grant with its 20 cm exclusion zone around the antenna

## Appendix II – Calculation of Maximum Transmit Duty Cycle

As outlined in Appendix I, each remote WIT2410P can transmit only once during a dwell time. The maximum length of the transmitted packet from each remote is set by the system design and cannot be adjusted by the user. That packet length is calculated as follows:

Preamble	9 bytes
Sync and CRC	10 bytes
Data Payload	<u>13 bytes</u>
Maximum packet length	32 bytes
Bit time (1/460 Kbps)	2.1739 us
Byte time (bit time * 8)	17.3912 us
Maximum packet time (byte time * 32)	556.5184 us

The maximum amount of time that our Remote transmitter can operate in any 10 millisecond period is 556.5 us. Therefore, our source-averaged transmit duty cycle becomes 0.0556 (556.5 us / 10 ms). Note that this duty cycle is not dependent on our use of Frequency Hopping. We are not averaging our power over the number of hops. The above calculation is strictly based on the maximum amount of time our transmitter can transmit in any 10 ms time period – regardless of the channel the radio happens to be on at the time.

## Appendix III – Calculated Average Power

**The Power Threshold for ‘General Population’ portable designation without SAR testing is: (based on Oct 2005 TCB workshop PPT slide)**

$(60 / F_{\text{GHz}})$  mW for distances < 2.5 cm

For the 2.4 GHz frequency band, this results in a limit of **25 mW**.

Note that we use the more restrictive “General Population” limit in this case even though the individuals using this product will certainly be aware of its function and would qualify under the ‘occupational’ category.

**Given the maximum transmit duty cycle specified in Appendix II, the average transmitted power of a WIT2410P remote can be calculated as:**

Maximum Pout = **63 mW** (18 dBm nominal)

Maximum Antenna Gain = **6 dBi** (for portable use)

Maximum Transmit Duty cycle (per Appendix II) = **0.0557**

Pave (Source-based average) =  $0.063 * 4 * 0.0557 = \mathbf{14\ mW}$

### Conclusion:

The WIT2410P Remote meets the MPE limits for a ‘Portable’ device operating in the ‘General Population’.