Wi-Fi Terminus NT-110ST Wi-Fi Enabled GPS

JANUS REMOTE COMMUNICATIONS

CONTENTS

Figure and Table Contents

1 Description

1.1 Introduction

The Wi-Fi Terminus NT-110ST (Wi-Fi Terminus) combines GPS technology with Wi-Fi transport. Incorporating sister company, NavSync's CW20 module with ultra sensitive GPS receiver, the NT-110ST provides an 802.11b/g transmission containing NMEA streams giving device location (longitude and latitude) and UTC time. The 802.11b/g supports WPA2 encryption and is fully configurable to a specific network.

1.2 GLOBAL POSITIONING SYSTEM (GPS)

The Global Positioning System (GPS) is a military satellite based navigation system developed by the U.S. Department of Defense and made freely available to civil users. Civilian use of GPS is available at the user's own risk, subject to the prevailing DOD policy or limitations, and to individuals understanding of how to use the GPS.

In today's satellite constellation there are a minimum of 24 operational satellites (plus several operational spares) in 6 orbital planes, at an altitude of approximately 22,000 km. The GPS system can give accurate 3-D position, velocity, time, and frequency, 24 hours a day, anywhere in the world. GPS satellites transmit a code for timing purposes, and also a 'navigation message' that includes their exact orbital location and system integrity data. Receivers use this information, together with data from their internal almanacs, to establish the precise satellite location. The receiver determines position by measuring the time taken for these signals to arrive. At least three satellites are required to determine latitude and longitude if the altitude is known (e.g. a ship at sea), and at least a fourth to obtain a 3-D fix.

1.3 GPS Positioning and Navigation

The Wi-Fi Terminus needs to be able to see at least 4 satellite vehicles (SV's) to obtain an accurate 3-D position fix. When traveling in a valley or built-up area, or under heavy tree cover, the Wi-Fi Terminus may experience difficulty acquiring and maintaining a coherent satellite lock. Complete satellite lock may be lost, or only enough satellites (3) tracked to be able to compute a 2-D position fix, or even a poor 3D fix due to insufficient satellite geometry (i.e. poor DOP). *Note, inside a building or beneath a bridge, it probably will not be possible to update a position fix. The receiver can operate in 2-D mode if it goes down to seeing only 3 satellites by assuming its height remains constant. But this assumption can lead to errors, especially when a change in height does occur. A 2-D position fix is not to be considered a good or accurate fix – it is simply a "better than nothing" fix.*

The receiver's antenna must have a clear view of the sky to acquire satellite lock. It is the location of the antenna which will be given as the position fix. The antenna is located under the Wi-Fi Terminus label and should face upwards for best signal reception. If the antenna faces downwards, it may not be possible to successfully track any satellites. Mounting the Wi-Fi Terminus in a vertical position is also acceptable, but the antenna may not be able to receive the satellite signals from those satellites out of line-of-sight from the front of the enclosure, making this a less than ideal position. Please also note that any obstructions (dense foliage, tall buildings) can obstruct the line-of-sight to the satellites and make tracking more difficult.

To measure the range from the satellite to the receiver, two criteria are required: signal transmission time and signal reception time. All GPS satellites have several atomic clocks to keep precise time. These are used to time-tag the message (i.e. code the transmission time onto the signal) and to control the transmission sequence of the coded signal. The receiver has an internal clock to precisely identify the arrival time of the signal. Transit speed of the signal is a known constant (the speed of light), therefore: time x speed of light = distance.

Once the receiver calculates the range to a satellite, it knows that it lies somewhere on an imaginary sphere with a radius equal to this range. If a second satellite is then found, a second sphere can again be calculated from this range information. The receiver now knows it lies somewhere on the circle of points produced by the intersection of these two spheres. When a third satellite is detected and a range determined, a third sphere intersects the area formed by the other two. This intersection occurs at just two points. The correct point is apparent to the user, who has a rough idea of position. A fourth satellite is then used to synchronize the receiver clock to the satellite clocks. In practice, 4 satellite measurements are sufficient for the receiver to determine a position, as one of the two points will be totally unreasonable (possibly many kilometers out into space).

This assumes the satellite and receiver timing to be identical. In reality, when the Wi-Fi Terminus compares the incoming signal with its own internal copy of the code and clock, the two will no longer be synchronized. Timing error in the satellite clocks, the receiver, and other anomalies, means the measurement of the signals transit time is in error. This effectively is a constant for all satellites, since each measurement is made simultaneously on parallel tracking channels. Because of this, the resultant ranges calculated are known as "pseudo-ranges".

To overcome these errors, the Wi-Fi Terminus matches or "skews" its own code to become synchronous with the satellite signal. This is repeated for all satellites in turn, thus measuring the relative transit times of individual signals. By accurately knowing all satellite positions, and measuring the signal transit times, the user's position can be accurately determined. Utilizing its considerable processing power, the Wi-Fi Terminus rapidly updates these calculations from satellite data to provide a real time position fix.

The following DOP terms are computed by the Wi-Fi Terminus:

HDOP   Horizontal Dilution of Precision (Latitude, Longitude)

VDOP   Vertical Dilution of Precision (Height)

PDOP   Position Dilution of Precision (3-D positioning)

Estimated accuracy = DOP x measurement accuracy

While each of these terms can be individually computed, they are formed from covariances and are not independent of each other. Horizontal accuracy figure of 95% is the equivalent to 2RMS (twice root-mean-square) or twice the standard deviation radial error. Similarly, for vertical and time errors, a figure of 95% is the value of 2 standard-deviations of vertical or time error.

- Root-mean-square (RMS) error is the value of one standard deviation (67%) of error.

- Circular Error Probability (CEP) is the value of the radius of a circle, centered at a position containing 50% of the position estimates.

- Spherical Error Probability (SEP) is the spherical equivalent of CEP, which is centered at a position containing 50% of the position estimates.

CEP and SEP are not affected by large errors, which could make the values an overly optimistic measurement. These probability statistics are not suitable for use in a high accuracy positioning system. The Wi-Fi Terminus reports all accuracies in the form of a standard deviation (RMS) value.

1 Description continued

1.4 Operation
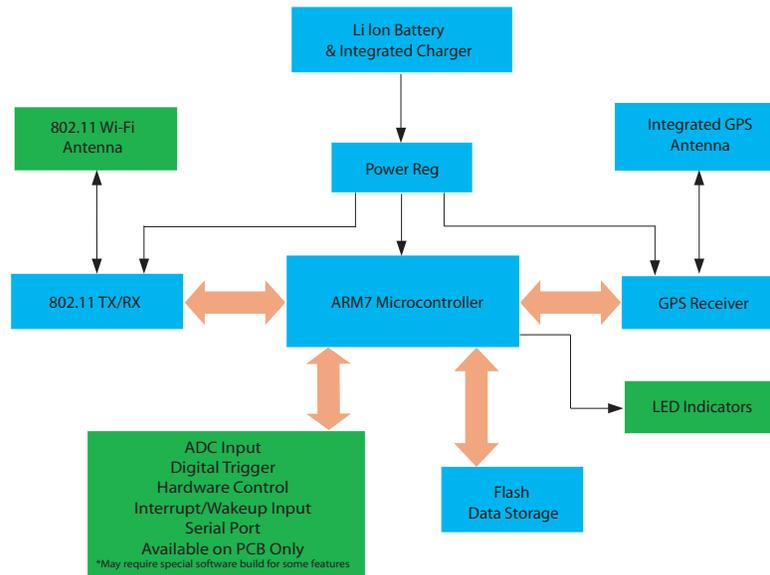
Figure 1 Wi-Fi Terminus NT-110ST Block Diagram

The default 802.11 network settings of the NT-110ST are as follows:

Topology:	Infrastructure Mode
Source IP:	DHCP client (Version V4.00 and below), 192.168.1.3 (Version V04-01 and above)
Source Port:	Varies
Channel:	6
Network SSID:	CW85_Setup (higher priority) or LTRX_IBSS (lower priority)
Data Rate:	1 Mbps

WPA2 Security Passphrase: GSDemo123

Note: The unit will also transmit on a network with security disabled even though the phrase is configured.

Packet type:	UDP
Destination IP:	192.168.1.2
Destination Port:	9999

The Wi-Fi Terminus must be charged prior to first use.

Upon power up, the Wi-Fi Terminus will scan for 802.11b/g networks and attempt to associate with the configured SSIDs. During this time, the GPS receiver is turned on and the Wi-Fi Terminus will attempt to obtain a valid GPS fix. Once the GPS receiver is turned on, a 'heartbeat' LED (power) will blink once per second indicating that the Wi-Fi Terminus unit is fully operational.

Note: The 'heartbeat' LED blinks with each GPS update, which is 1s by default. Changing the GPS fix rate will change the 'heartbeat' rate.

The 'status' LED will give an indication of network status and GPS status as indicated in Table 1.

1 Description continued

1.4 Operation continued

Status LED

Condition	Status LED
No network detected and no GPS fix	OFF
Network detected but no GPS fix	Blinks once every 2.5 seconds
No network detected but GPS fix	Blinks once every 5 seconds
Network detected and GPS fix	Blinks once every 0.5 seconds

Table 1: Status LED

As soon as the Wi-Fi Terminus associates with the network it will try to resolve the destination IP. Once this has been accomplished, the Wi-Fi Terminus will begin sending UDP packets to the destination IP. Data from the GPS receiver is saved to flash memory until the destination IP is resolved. This default behavior may be changed by the user via SNMP – see Section 3 'Device Configuration via SNMP'.

When the unit first powers on, the GPS "cold" starts, which means that the GPS has no ephemeris or almanac information. This mode requires higher satellite signal strength to acquire a GPS fix than is required for tracking. Once the unit begins tracking satellites, it begins to download the almanac and ephemeris information. Depending on the number of satellites in view with sufficient strength, this could take 12-15 minutes, although in an open-sky situation it will occur more quickly. After the GPS has successfully downloaded the ephemeris and almanac information, lower level signal testing may be done.

   Note: The accuracy numbers quoted in the specifications section assume that the unit has valid ephemeris and almanac information.

The operation of the Wi-Fi Terminus unit is highly user configurable. Not only can the network settings be configured via the SNMP interface, but the operational parameters can be changed. Appendix 1 lists the parameters that are configurable, as well as their default values. By default, the device will send out all of the NMEA sentences via UDP. However, individual sentences can be turned off, and the rate at which these sentences can be sent out can vary (see Section 1.6). Additionally, the user can choose to send out packets via TCP/IP instead of UDP/IP for both the current GPS data, and for the logged data in flash memory.

Changes to the connection type (TCP/UDP) will not take effect until the device is restarted. Changes to the TCP port or destination IP will also take effect after the device is restarted. Alternatively, because UDP is a 'connectionless' protocol, any changes to the port or destination IP will take effect on the next transmission. Additionally, changes to most of the other network settings require a restart to take effect. This allows the user to fully configure the device before those changes take effect.

The Wi-Fi Terminus will check for association prior to sending out NMEA sentences at the configured transmission rate. If the unit is not associated with a network, it will rescan every 10 seconds until it finds one of the configured networks. There are three different SSIDs that the unit can be configured to scan, each one with its own channel. These networks can be used for either Infrastructure mode or Ad Hoc mode *(Note: to utilize Ad Hoc mode for normal situations, do not use the GSNADHOCSSID and corresponding channel settings, but use the GSNAPSSID1-3 settings).* In Ad Hoc mode, the unit will not create an Ad Hoc network, but will scan for an existing network.

Security options can be set per SSID. Available security options in Infrastructure mode are no encryption, WEP64, WEP128, WPA, or WPA2-PSK. In Ad Hoc mode, only the WEP or open security options are available. Each SSID can support all of these security options, or a subset. This is selectable through the SNMP interface. By default, all security options are supported. It is recommended to enable only those security options that are necessary to enable the most secure operation. It is important to note that although different security options may be enabled for each SSID, only one security type for each SSID is expected to be used at any one time and it is not intended that the Wi-Fi Terminus switch between these security options during operation. The Wi-Fi Terminus needs to have its power cycled if the security type is changed on the network. Failure to do so can lead to undefined operation.

1 Description continued

1.4 Operation continued

The Wi-Fi Terminus utilizes flash memory for saving the NMEA streams in case the unit is unable to transfer the data. This can occur if a network is not present, if the unit is unable to associate with the network, or if there is a TCP socket problem (if TCP has been set as the default for transmission). The user can control how often the messages are saved to flash memory. For example, the unit can be configured to transmit every 3 seconds, while, at the same time, the unit may only save to flash memory every other period (every 6 seconds) to maintain the longest history possible in memory. Once the Wi-Fi Terminus unit has re-associated with the network (or, with TCP, has re-established the socket connection), it will send out the contents of its flash memory, starting with the oldest data and ending with the newest, then erase its memory after the entire contents have been successfully transmitted. As long as the Wi-Fi Terminus is able to detect that it is on the network, it will continue its normal operation of sending out the selected NMEA streams at the selected rate.

If the Wi-Fi Terminus is configured for TCP rather than UDP communications, any socket error on the TCP connection causes the data to be saved to flash memory. If the socket connection is closed, it will attempt to restart it.

Additional functionality has been built into the Wi-Fi Terminus to enhance the data logging feature. There are commands to save all data, even if there is no network issue. The rate at which the data is saved is controlled in the same way as when it is saving only unsuccessful transmissions. A command to force a log dump over the configured IP/Port is available in this mode, as well as a command to erase the entire log. Because the data is saving continuously to the flash memory, a dump of the flash memory will not occur automatically. The user must tell the unit to dump its memory. As the log becomes full, the oldest data is erased and overwritten with the newest data. If the device is powered down with data in its memory, it will recover the beginning and end of the lost data when it is powered on again. New data will saved in a continuous fashion right after the newest data in memory. If no data is in memory when the dump command is given, an internal flag in volatile RAM will remain set until the first data bytes are stored in memory. The unit will then attempt to send out this data. Since this is a volatile flag, it will not remain set following a power cycle.

After a data log is sent out, the ASCII characters "log complete" will be sent out at the end of the transmission, signaling that all of the data has been retrieved from memory. At that point, the flash memory is given the command to erase the data log. Erases are done in the spare time of the system, and a full log erase can take up to 2 minutes, although typical time is about 1 minute. New data will still be saved to memory during the log erase. If a unit is powered off during the erase cycle, it will not continue to erase on the next power up. Instead, the new data being stored into the flash will be appended to whatever data remained in memory.

Beginning with version 4-10 and greater, additional configuration options have been added for greater control over the GPS fix data. A new option, NTSendFix, allows the user to send only fix information over the network connection. If NTSendFix is 1 or greater, then NTNumFix will allow the user to select the number of fixes the unit should get before sending fix information out. For example, if NTSendFix = 1, and NTNumFix = 3, then the Wi-Fi Terminus will start sending fixes from the 4th fix on. The first three GPS fixes will be discarded. Another configuration option, NTNumSend, will configure the device to repeat each transmission the configured number of times.

1 Description continued

1.5 Safe Mode

The Wi-Fi Terminus has been configured with a Safe Mode. If the unit cannot associate with any of the three configured SSIDs, or it loses its association and cannot re-associate, it will enter a mode that will search for the Ad Hoc network NT_ADHOC on channel 11, with no security. In this mode, the IP address of the device changes to 192.168.1.50 and it searches for an SNMP manager at 192.168.1.51. It will search for approximately 25-30 seconds, after which time it will go back to its normal search for the three configured SSIDs. This behavior will only be displayed once per power on.

Safe Mode has been implemented for situations where a Wi-Fi Terminus may have been configured incorrectly and no network connection can be established. The recommended method for entering this mode is to power the device off, and turn off any of the networks it is configured to associate with. Then start the NT_ADHOC network, using the IP 192.168.1.51 and turn the Wi-Fi Terminus on. Once the Wi-Fi Terminus sees the Ad Hoc network, configuration via SNMP is available. The Wi-Fi Terminus will remain in this mode until the connection has been lost for a short period of time. Please note, this mode occurs during the normal operational mode, so the device is still obtaining GPS data during this time. If the Wi-Fi Terminus is able to resolve the destination IP, it will attempt to send packets.

The Wi-Fi Terminus also supports a setting for returning to its original factory configuration. This command will reset the device to the defaults in Appendix 1. However, the MAC address **will be reset** to the value 00 50 C2 9B A0 00. The MAC address MUST be reset to its initial value (written on the label on the backside of the unit) after using this command. Failure to do so may result in an unusable unit. After receiving the command to reset the MAC address, the Wi-Fi Terminus should have the power cycled.

1.6 Special Considerations When Modifying GPS Update Rate/Messages

NTGPSUPDATERATE - .1.3.6.1.4.1.28295.99.1.2.1.16.5

This takes effect when the internal counters controlling each GPS message reach 0. For example, if the message rate is 100 seconds, and then changed to 10, the Wi-Fi Terminus waits until the 100 second period is up before the 10 second period takes effect. Also note, all messages that are to be enabled should be occurring at a common interval prior to changing this rate or changing them may result in different GPS messages reporting at different epochs.

NTFLASHUPDATERATE - .1.3.6.1.4.1.28295.99.1.2.1.19.5

This takes effect when the internal counters controlling the GPS save rate reach 0. If the data transmission rate is set to 3, and this rate is set to 1, then data will save every 3 seconds if the network is not detected. If the data transmission rate is set to 3, and this is set to 2, then this would save every 6 seconds if the network is not detected.

NTMESSAGEENABLE - .1.3.6.1.4.1.28295.99.1.2.1.21.5

This OID controls which GPS messages are enabled. The bit map of the binary representation of the number configured is as follows:

BIT	NMEA message
0	GPGGA
1	GPGLL
2	GPGSA
3	GPGSV
4	GPRMC
5	GPZDA
6	GPVTG

For example: 127 is 0111 1111b, which enables all messages (the default)

3 is 0000 0011b, which enables GPGGA and GPGLL

Note that if the current transmission rate is not 1 second intervals, then messages that are newly enabled could be on a different epoch than previously enabled messages. The recommended method of changing the messages is to set the transmission rate to 1 second, enable the required messages, wait until all messages are appearing on 1 second intervals together, and then change the data rate to the desired number. At least one of the enabled sentences must have the FS (fix status) or Status fields in order for the Wi-Fi Terminus to indicate fix status appropriately. The GPGSV, GPZDA, and GPVTG sentences do not have an FS or a Status field. Thus, these should be enabled in conjunction with the GPGGA, GPGLL, GPGSA, or GPRMC for appropriate fix indicator operation.

Failure to follow the above can result in messages being sent that are not from the same epoch, as each message runs on its own counter and updating the interval does not update the counter for a message until that counter = 0.

It is necessary to mention here that the GPGSV sentence (enabled by default) does not transmit prior to having satellite data, and thus the counter for that message is not active until it has data. If the message rate is changed before the GPGSV sentence is sent, it is possible for the GPGSV sentence(s) to be out of sync with the rest of the sentences when they do begin. This is a condition that could occur on a power cycle if the message rate is other than 1s and the GPGSV sentence is enabled. If this occurs, the message rate should be set back to 1 second until all messages are on the same epoch, and then the new message rate can be changed.

1 Description continued

1.7 Diagnostic Messages

NTTESTVAR - .1.3.6.1.4.1.28295.99.1.2.1.11.5

A diagnostic message containing the RSSI and VBAT voltage as measured on board is available on command to be sent out the data port.

Each time a 0 or a 1 is written to the appropriate OID, a message of the form:

<MAC ADDRESS>,$PNVTC, RSSI, VBAT*<checksum>

where RSSI is the received signal strength and VBAT indicates battery level.

This VBAT voltage is not the actual battery voltage at the battery, but the voltage as measured on board the ARM processor. Currently, this number corresponds to the levels where the unit goes into 'forever standby' mode.
These limits may vary based on the specific hardware. Please refer to Appendix 1, GSNBATTERYWARNINGLEVEL and GSNBATTERYSTANDBYLEVEL for specific limits.

If 1 is written to the appropriate OID, the GPS will also send out a string with software version information over the wireless connection. This sentence may be delayed for a second or more after the PNVTC sentence.

1.8 SNMP Traps

The Wi-Fi Terminus unit is designed to send out three different types of SNMP traps, which are unsolicited messages from the intrinsic SNMP agent. The traps are sent to port 162, from port 161 (default values). The community name for these messages is GSN_TRAP (see Section 3 for more information on SNMP).

The first type of trap is a linkup trap. This is a message designed to help maintain a network connection when used with the standby mode of operation. The standby mode is not yet available for release, and so this trap is generally unused. It is possible to reduce the frequency of this message using OID .1.3.6.1.4.1.28295.1.1.4.14.0 (GSNTRAPLINKUPINTNEWTMR).

The second type of trap is a config trap. This message is also intended for use with the standby mode of operation, not yet available for release. When the unit is in standby, this interval controls how often the unit will wake up to check for updates from the SNMP manager. Reducing the frequency of this message is possible using OID .1.3.6.1.4.1.28295.1.1.4.13.0 (GSNTRAPCONFIGINTNEWTMR).

The third type of trap is a low battery warning trap. This trap is designed to warn the system that the battery will soon reach an unsafe level, causing a system shutdown. The levels are set to start sending warning messages at least 30 minutes prior to the unit going into shutdown mode. Shutdown mode will occur when the battery voltage reaches an unsafe level to prevent any memory corruption issues from a brown-out condition during transmission. The values for this limit are factory calibrated, but are user accessible at OIDs .1.3.6.1.4.1.28295.1.1.1.8.0 (GSNBATTERYWARNINGLEVEL) and .1.3.6.1.4.1.28295.1.1.1.9.0 (GSNBATTERYSTANDBYLEVEL). Any user is strongly advised AGAINST changing these levels without first contacting the factory. Changing these levels can result in an unusable device.

1.9 Key Features of the Wi-Fi Terminus
- Sensitive GPS receiver with tracking as Low as -150dBm
- 802.11b/g compliant
- WPA2 encryption
- Integrated rechargeable battery
- User programmable update rates
- Internal flash memory for saving GPS data

The specifications in the following sections refer to the standard software builds of the Wi-Fi Terminus. The performance and specification of the Wi-Fi Terminus can be modified through the user configuration and additional I/O capabilities may be available with special software builds. Please contact the factory for more details.

Please refer to Section 4-NMEA Messages for detailed information on the available NMEA messages.

2 Specifications

2.1 Performance

NT-110ST Wi-Fi ENABLED GPS SPECIFICATIONS

GPS RECEIVER SPECIFICATIONS

Physical		Notes
Module Dimensions (without external antenna)	3.773" (w) x 3.149" (h) x 1.253" (d) 95.97mm (w) x 79.99mm (h) x 31.83mm (d)	

GPS Performance		
GPS Channels	16	
Frequency	1575.42 MHz – L1 C/A code	
TTFF Cold Start @ -135 dBm	46 seconds	1, 6
Re-acquisition Time @ -147 dBm	<3 seconds	2
Acquisition Sensitivity	-147 dBm	4
Tracking Sensitivity	-150 dBm	5
Static Accuracy 50% Confidence (CEP)	2 m	6
95% Confidence (CEP)	4 m	6
Maximum Horizontal Speed	515 m/s	7
Maximum Vertical Speed	15 m/s	8
Maximum Altitude	18 Km	7
Maximum Acceleration (g)	2 g	

Wi-Fi SPECIFICATIONS

Wi-Fi Performance	
Maximum Transmit Power	15 dBm
Frequency Band	2.4GHz ISM
Transmission Speed	1Mbps default, contact factory for 2Mbps
Modulation	Direct Sequence Spread Spectrum (DSSS)
Protocol	802.11b/g compatible
Security	802.11i (WPA2-PSK), WPA-PSK, WEP128, WEP64 9
AES Encryption/Decryption	Hardware implemented

DATA FLASH MEMORY SPECIFICATIONS

Size	8Mbit / 1Mbyte
Type	Circular buffer
Data retention	20 years

JANUS REMOTE COMMUNICATIONS

2 Specifications continued

2.1 Performance continued

GENERAL SPECIFICATIONS

Power (Avg.) Transmitting	~1.1W	Notes
Operation When Not Transmitting	<0.3W	10
Internal Li Ion Rechargeable Battery	900 mAH	
Battery Life (Initial capacity)	12+ hours	11
Battery Cycle Life	~500 cycles to 80% of rated initial capacity	
Battery Charge Voltage/Current	5V/500mA max	12
Battery Charge Temperature Range	0°C to 45°C	
Operating Temperature Range	-15°C to 60°C	13
Storage Temperature Range	-20°C to 45°C	14
Humidity	5% - 95%, Non-Condensing	
GPS Fix Rate Maximum	Once per second	
Wireless Transmission Period	Default is once per second, user configurable via SNMP	

ANTENNA REQUIREMENTS

802.11 Antenna	Reverse SMA connection with 0 dBi antenna. Certification valid with up to 5 dBi antenna gain.
GPS Antenna	Internal passive antenna provided

The specifications refer to the standard software builds of the NT-110ST. The performance and specification of the NT-110ST can be modified with the use of customized software builds.

Table 2 NT-110ST Specification

Notes:

1. *These are RMS values.*
2. *Maximum sensitivity -147 dBm.*
3. *Simulator test, all signals at specified power level.*
4. *Estimated.*
5. *Simulator test, continuous fix with all signals at specified power level.*
6. *Open sky, 24 hr field test. No sky-view obstructions. Accuracy relative to actual surveyed position, not self-relative survey.*
7. *Limited by International Traffic in Arms Regulation (ITAR).*
8. *Defined by navigation integrity check.*
9. *WEP encryption is by key only. Passphrases are supported only for WPA/WPA2 security.*
10. *0.3W is for Infrastructure mode, which implements a polling mode to conserve power. Ad Hoc mode current draw is ~0.78W.*
11. *Continuous transmission, 1 fix per second, Infrastructure mode, 27°C, fully charged battery.*
    12 hours of operation are not guaranteed for the entire operational temperature range.
12. *Total current drawn by the device via USB port. If the device is operating during charge, the current required for operation reduces the available charge current, maintaining a maximum draw of 500mA.*
13. *Although the battery will continue to function from -15° to 60°C, the battery lifetime is reduced if temperature is maintained above 45°C for long periods.*
14. *Exceeding the specifications for storage range will decrease the life and capacity of the Lithium Ion battery.*
    The unit will continue to operate above the storage temperature, but the battery life will be significantly shorter.

2 Specifications continued

2.2 Transmission Distance

Estimation of maximum transmission distance on 802.11b/g signal versus transmission rate:

	Open Plan Building	Semi Open Office	Closed Office
2.0 Mbps	400 m (1300 ft)	90 m (300 ft)	40 m (130 ft)
1.0 Mbps	550 m (1750 ft)	115 m (375 ft)	50 m (165 ft)

The Wi-Fi Terminus transmits at 1.0 Mbps. Contact factory if 2.0 Mbps is desired.

Table 3 Wi-Fi Transmission Distance

The above estimates may not apply to many situations and the typical performance in most situations is probably about 50-60% of the above values. Factors such as antenna polarization, electronic noise, obstructions in line-of-site between device and access point, multipath errors as well as reflections from the ground play an immense role in degrading the signal. These variables can vary tremendously from site to site. The above numbers are maximum estimates based on specific setups. The best way to determine transmission disance in a given environment is to set up a network and take empirical data.

The transmit power and receive sensitivity of the access point plays a role equal to the power/sensitivity of the Wi-Fi Terminus device and therefore must be considered in any calculations for maximum transmit distance. The Friis Transmission Equation may be used to calculate transmission distance in an ideal way, but it does not take into account signal reduction due to electrical noise, multipath errors, obstructions, and antenna polarization mis-match. There is no 'one size fits all' equation for this; often the best way to estimate is to use empirical data.

That being said, the Friis Transmission Equation could be used to estimate the relative change in transmission distance due to modifying parameters such as antenna gain or receiver sensitivity; this information, coupled with empirical data collected from the deployment site, can be used to help determine necessary modifictions to a setup to help achieve desired distances. Therefore, the Friis Transmission Equation is given here for reference: $\frac{Pr}{Pt} = G_t G_R \left(\frac{\lambda}{4 \Pi R} \right)^2$, where Pr is the power at the receiver antenna, Pt is the power supplied to the transmitting antenna, Gt/Gr are the transmitter and receiver antenna gains, respectively, in watts.

Manipulations of this equation give the following form which is more applicable to the information generally available in device datasheets. By substituting for the power and gain (in watts) in the previous paragraph with $P(W) = 10^{\left(\frac{PdB}{10}\right)}$, and by using 3×10^8 m/s for the speed of light, we can solve for R, the distance in km: $R(km) = \frac{10^{(gt + gr + pt - pr)/20}}{41.88 * 2442 \, Mhz}$

Using typical receiver sensitivity at -90 dB, receiver antenna gain of 2 dBi, Wi-Fi Terminus power of 15 dBm, and Wi-Fi Terminus antenna gain at 0 dBi gives over 2 km transmission distance, which is unachievable in anything but a completely ideal situation. However, using the same numbers with a Wi-Fi Terminus 5 dBi antenna shows a distance of over 3.8 km. This indicates that in a given situation, replacing the O dBi antenna on the Wi-Fi Terminus with a 5 dBi antenna could give nearly a 2x change in transmission distance.
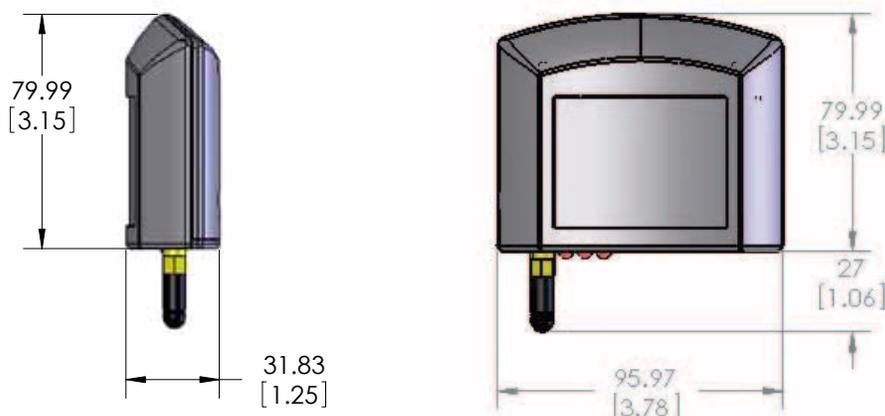
2.3 Mechanical Dimensions

Figure 2 Wi-Fi Terminus NT-110ST Dimensions

2 Specifications continued

2.4 External Connections

ON/OFF SWITCH

R90
[3.54]

Antenna Connection   **External LED Indicators**   **USB Battery Charge**
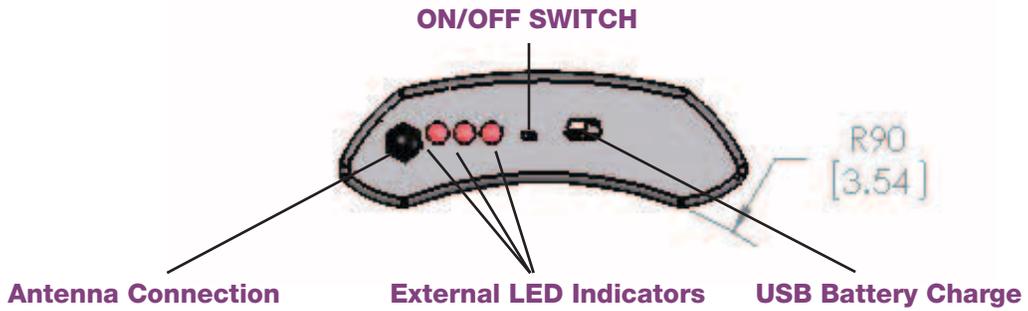
Figure 3 External Connections

2.5 Optimal Orientation

SATELLITE

SATELLITE   **SATELLITE**
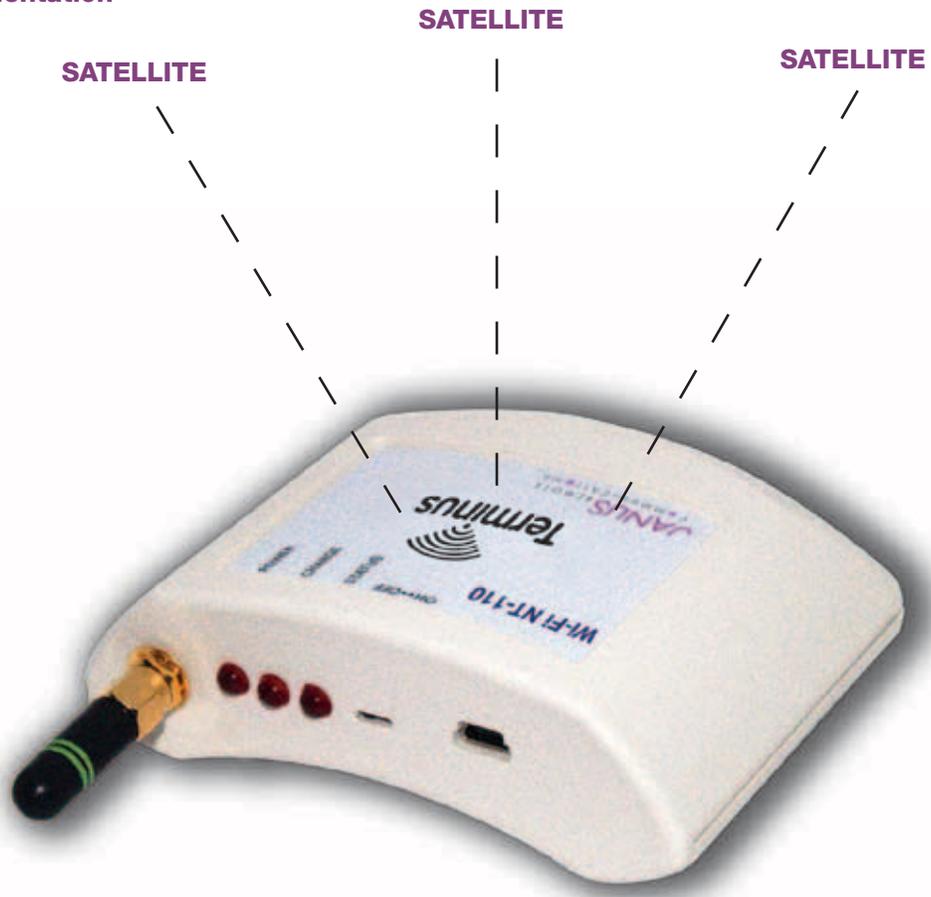
Figure 4 Wi-Fi Terminus NT-110ST Optimal Position

JANUS REMOTE COMMUNICATIONS

3 Device Configuration via SNMP

3.1 General Information

The Wi-Fi Terminus parameters are configured via a Simple Network Management Protocol (SNMP) manager. SNMP is an industry standard protocol for networked devices. It defines the messaging protocol and the structure (but not the content) of an information database, called the Management Information Base (MIB), which is contained in managed network devices. There are several versions of SNMP. The Wi-Fi Terminus supports version 1 (SNMPv1).

The structure of the MIB is hierarchical in nature with several well defined levels of parameters and the ability to define more parameters at the device level. An SNMP agent and the MIB reside in the device, giving access to read-only and configurable parameters. Each parameter has a unique object identifier (OID) – a dotted decimal notation which describes its location in the SNMP hierarchy.

Managed devices in an SNMP network also have specified 'community names'. These are used to group managers and devices and help identify where information is sent. A managed device can have different community names for reading and writing operations.

The output format specifier (-O) is followed by a single character which will control how the response string is formatted. See Table 4: Data Type for available output options.

We recommend using Net-SNMP software as an easy method to understand and manage the Wi-Fi Terminus parameters using SNMP. The Net-SNMP homepage is www.net-snmp.org. The latest version can be downloaded free of charge from SourceForge.net at http://sourceforge.net .

Once installed, the net-SNMP software can be used to read (get) and write (set) to the Wi-Fi Terminus parameter database using the "snmpget" and "snmpset" commands.

The format of a snmpget command is:

snmpget [OPTIONS] AGENT OID

Desired options include:

The SNMP version specifier, '-v 1'. The Wi-Fi Terminus uses SNMPv1.

An output format specifier, '-O a', which requests string values to be printed as ASCII text.

The community name, '-c GSN_GET'. The community name for reading a Wi-Fi Terminus device is "GSN_GET".

The agent for the Wi-Fi Terminus is the IP address of the unit, which is configured to 192.168.1.3 by default. See Section 1.4 and Section 6 for the default network settings and details on how to bring the device up on a network.

The OID's for the Wi-Fi Terminus parameters are given in the Wi-Fi Terminus OID Table. Each OID is prefixed with .1.3.6.1.4.1.28295.1 -or- .1.3.6.1.4.1.28295.99.1. Using the 1st table entry "GSNSENSORSERVERIP" as an example, the SNMP data read request would be:

snmpget –v 1 -O a -c GSN_GET 192.168.1.3 .1.3.6.1.4.1.28295.99.1.2.1.6.5

A typical response string would look like:

SNMPv2-SMI::enterprises.28295.99.1.2.1.6.5 = IpAddress: 192.168.1.2

Writing to parameter database is accomplished using the snmpset command.

The format of a snmpset command is:

snmpset [OPTIONS] AGENT OID TYPE VALUE

Necessary options are the same as snmpget, although the '-O' output specifier is not used. The type of the value parameter must be specified in a single character, as shown in the following Data Type Table 4. The data type for each Wi-Fi Terminus parameter appears in the in the Wi-Fi Terminus OID Table.

3.2 Data Type Table

Type	TypeSpecifier	Description
INTEGER	i	A whole number
STRING	s	Character string
IpAddress	a	Four-octet string of hexadecimal data
HEX	x	Hexadecimal String

Table 4: Data Type

The parameter value itself should be enclosed in quotations. It is not always necessary to enclose the parameter in quotations, but it is required if the parameter value has spaces. It is recommended to always use quotations and to verify that the response string on a Set matches the intended input type and value. If the response shows the parameter in brackets, then the Wi-Fi Terminus will not use the parameter.

Using the same example as above, writing to the 1st table entry "GSNSENSORSERVERIP" would look like:

snmpset –v 1 -c GSN_SET 192.168.1.102 .1.3.6.1.4.1.28295.99.1.2.1.6.5 a "192.168.1.4"

In this example, the Wi-Fi Terminus sensor server IP address is being set to "192.168.1.4". The response string should be:

SNMPv2-SMI::enterprises.99.1.2.1.6.5 = IpAddress: 192.168.1.4

If the response string was of the form: SNMPv2-SMI::enterprises.99.1.2.1.6.5: (192.168.1.4), this indicates a problem with the formation of the SNMPSET command and the Wi-Fi Terminus will not set the parameter appropriately.

For security purposes, all WEP/WPA/WPA2 security settings are read disabled by default. The Wi-Fi Terminus will respond to a read of the security settings with "Read-Disabled" if it is a String or Hex String, and with 255 if it is an integer. To confirm a settings change, please note the SNMP response string that is sent with an SNMPSET command. If the new value is set appropriately, you will see the new value in the response string in the form "INTEGER = XXXX" or "STRING = XXXX". If the value is returned in parenthesis, it was not acknowledged properly.

There is additional information on the format and use of these and many other operations available in the documentation that accompanies the Net-SNMP software package.

4 NMEA Messages

4.1 General NMEA Information

The following Approved NMEA messages are available from the Wi-Fi Terminus NT-110ST:

NMEA Message	NTMSGENABLE Bit	Reference Section
GPGGA	0	4.2
GPGLL	1	4.3
GPGSA	2	4.4
GPGSV	3	4.5
GPRMC	4	4.6
GPZDA	5	4.7
GPVTG	6	4.8

Each NMEA message is preceded by the ASCII value of the MAC address. This is separated from the NMEA message by a comma, and intended to be used as a unique identifier for each message. All messages start with $, have fields delimited by commas and end with <CR><LF>. Approved NMEA messages are recognized by the first 5 characters after the $ which define both the kind of talker providing the information (2 characters, GP in the case of a GPS) and the type of information (3 characters).

EXAMPLE OUTPUT – no FIX

0050C29BA003,$GPGGA,195713.000,0000.0000,S,00000.0000,W,0,00,00.0,0.0,M,0.0,M,,*5A

0050C29BA003,$GPGLL,0000.0000,S,00000.0000,W,195713.000,V,A*49

0050C29BA003,$GPGSA,A,1,,,,,,,,,,,,,0.0,0.0,0.0*30

0050C29BA003,$GPRMC,195713.000,V,0000.0000,S,00000.0000,W,0.00,0.00,281008,,,A*7D

0050C29BA003,$GPZDA,000000.000,22,08,1999,01,00*57

0050C29BA003,$GPVTG,0.00,T,,,0.00,N,0.00,K,A*70

Note: The GPGSV sentence is not sent out on start up until it contains non-zero data.

EXAMPLE OUTPUT – with a FIX

0050C29BA003,$GPGGA,193927.070,4154.8388,N,08845.3577,W,1,08,00.9,279.1,M,-34.9,M,,*59

0050C29BA003,$GPGLL,4154.8388,N,08845.3577,W,193927.070,A,A*43

0050C29BA003,$GPGSA,A,3,04,08,09,11,17,20,28,32,,,,,1.7,0.9,1.4*32

0050C29BA003,$GPGSV,2,1,08,4,38,201,40,8,13,177,33,9,21,314,31,11,22,051,34*4C

0050C29BA003,$GPGSV,2,2,08,17,73,333,47,20,23,088,37,28,66,115,47,32,16,062,24*7C

0050C29BA003,$GPRMC,193927.070,A,4154.8388,N,08845.3577,W,0.00,134.12,281008,,,A*72

0050C29BA003,$GPZDA,193927.070,28,10,2008,01,00*56

0050C29BA003,$GPVTG,134.12,T,,,0.00,N,0.00,K,A*75

4 NMEA Messages continued

4.2 GPGGA, GPS Fix Data

Time and position, together with GPS fixing related data.

$GPGGA,hhmmss.sss,Latitude,N,Longitude,E,FS,NoSV,HDOP,Altref,M,msl,M,DiffAge,DiffStation*cs

Field	Description
$GPGGA	NMEA sentence header (Position Data)
hhmmss.sss	UTC Time in hours, minutes, seconds. and decimal second format.
Latitude	User datum latitude degrees, minutes, decimal minutes format (ddmm.mmmmmm)
N	Hemisphere: 'N'= North, 'S' = South
Longitude	User datum longitude degrees, minutes, decimal minutes format (dddmm.mmmmmm)
E	Longitude Direction: 'E'= East, 'W' = West
FS	Fix Status:
	0 No fix
	1 Standard GPS
	2 Differential GPS
NoSv	Number of satellites used in the position solution
HDOP	2-D Horizontal Dilution of Precision (0.00 to 99.99)
AltRef	Altitude (meters) above user datum ellipsoid.
M	Units of height (meters)
msl	Mean Sea Level
M	Units of Mean Sea Level (meters)
DiffAge	Age of differential correction
DiffStation	Differential base station ID
cs	Message checksum in hexadecimal

4.3 GPGLL, Geographic Position, Lat/Lon

Latitude and longitude, with time of position fix and status.

$GPGLL,Latitude,N,Longitude,E,hhmmss.sss,Status,Mode*cs

Field	Description
$GPGLL	NMEA sentence header (Position Data)
Latitude	User datum latitude degrees, minutes, decimal minutes format (ddmm.mmmmmm)
N	Hemisphere: 'N'= North, 'S' = South
Longitude	User datum longitude degrees, minutes, decimal minutes format (dddmm.mmmmmm)
E	Longitude Direction: 'E'= East, 'W'= West
hhmmss.sss	UTC Time in hours, minutes, seconds. and decimal second format.
Status	Status: V=navigation receiver warning, A=data valid
Mode	Mode Indicator:
	D = Differential
	A = Autonomous
cs	Message checksum in hexadecimal

JANUS REMOTE COMMUNICATIONS

4.4 GPGSA, GPS DOP and Active Satellites

GPS receiver operating mode, satellites used for navigation, and DOP values.

$GPGSA,Smode,FS,sv,sv,sv,sv,,,,,,,,PDOP,HDOP,VDOP*cs

Field	Description
$GPGSA	NMEA sentence header (Satellite Data)
Smode	A= Automatic switching 2D/3D; M=Manually fixed 2D/3D
FS	Fix Status:
	1 No fix
	2 2D GPS Fix
	3 3D GPS Fix
sv	Satellites in use, null for unused fields (12 available fields)
PDOP	3-D Position Dilution of Precision (0.00 to 99.99)
HDOP	2-D Horizontal Dilution of Precision (0.00 to 99.99)
VDOP	Vertical Dilution of Precision (00.0 to 99.9).
cs	Message checksum in hexadecimal

4.5 GPGSV, GPS Satellites in View

The number of satellites in view, together with each PRN, elevation and azimuth, and C/No value. Up to four satellite details are transmitted in one message, with up to four messages used as indicated in the first field.

$GPGSV,NoMsg,MsgNo,NoSv,sv,elv,az,cno,sv,elv,az,cno,sv,elv,az,cno,sv,elv,az,cno*cs

Field	Description
$GPGSV	NMEA sentence header (satellite data)
NoMsg	Total number of GPGSV messages being output
MsgNo	Number of this message
NoSv	Number of satellites in view
sv	Satellites ID
elv	Satellite elevation angle (degrees)
az	Satellite azimuth angle (degrees)
cno	Satellite signal/Noise ration (dB/Hz)
cs	Message checksum in hexadecimal

4.6 GPRMC, Recommended Minimum Data

The 'Recommended Minimum' sentence defined by NMEA for GPS/Transit system data.

$GPRMC,hhmmss.sss,status,latitude,Hemisphere,longitude,E,spd,cmg,ddmmyy,mv,mvd,Mode*cs

Field	Description
$GPRMC	NMEA sentence header (recommended minimum sentence)
hhmmss.sss	UTC time in hours, minutes, seconds
status	Status: V=navigation receiver warning, A=data valid
Latitude	User datum latitude degrees, minutes, decimal minutes format (ddmm.mmmmmm)
N	Hemisphere: 'N'= North, 'S' = South
Longitude	User datum longitude degrees, minutes, decimal minutes format (dddmm.mmmmmm)
E	Longitude direction: 'E'= East, 'W'= West
spd	Speed over ground (knots)
cmg	Course made good
ddmmyy	Date in Day, Month, Year format
mv	Magnetic variation
mvd	Magnetic variation direction
Mode	Mode indicator:
	D = Differential
	A = Autonomous
cs	Message checksum in hexadecimal

4.7 GPZDA UTC Time and Date

This message transfers UTC time and date. Since the latency of preparing and transferring the message is variable, and the time does not refer to a particular position fix, the seconds' precision is reduced to 2 decimal places.

$GPZDA,hhmmss.sss,dd,mm,yyyy,Int,Unsigned*cs

Field	Description
$GPZDA	NMEA sentence header (time and date)
hhmmss.sss	UTC Time in hours, minutes, seconds
dd	UTC day
mm	UTC month
yyyy	UTC year
Int	Local zone hours
Unsigned	Local zone minutes
cs	Message checksum in hexadecimal

4 NMEA Messages continued

4.8 GPVTG, Course Over Ground and Ground Speed

Velocity is given as Course Over Ground (COG) and ground speed

$GPVTG,cogt,T,cogm,M,knots,N,kph,K,Mode*cs

Field	Description
$GPVTG	NMEA sentence header (speed and heading)
cogt	Course over ground (true)
T	True - fixed field
cogm	Course over ground (magnetic)
M	Magnetic - fixed field
knots	Speed over ground (knots)
N	Knots - fixed field
kph	Speed over ground (kph)
K	Kilometers per hour – fixed field
Mode	Mode indicator:
	D = Differential
	A = Autonomous
cs	Message checksum in hexadecimal

5 Lithium Ion Battery and Integrated Charger

The Wi-Fi Terminus unit contains a 900mAH lithium ion rechargeable battery and integrated battery charger. To charge the battery, a user needs to connect a 5V, 500mA capable power supply. The interface provided for charging the battery is a mini-USB connector. There is no serial data connection to the connector, just power and ground. No data is available to or from this port.

The operation range of this battery is -15° to 60°C, while the charging and storage temps are restricted to 0° to 45°C and -20° to 45°C, respectively. Although the battery will operate from 45° to 60°C, long term storage at that temperature can cause a considerable reduction in battery capacity. Long term operation above 45°C is not recommended for the best battery life.

The unit does contain circuitry for over/under temperature protection of the charging circuitry. The internal temperature protection will restrict a user from charging a battery below 0°C or above 45°C. This temperature is not measured ambient temperature, but is the temperature inside the enclosure. It is accurate to within about 3°C. There is hysteresis (approximately 3 degrees) built into the charging circuitry to help prevent the battery charger from toggling on/off at a rapid rate. If the battery charger detects the out-of-temperature band, it will flash the battery charging LED at a very rapid rate and will not charge the battery.

If an error is detected when charging the battery (ie – the battery voltage is too low and possible internal damage is suspected), the battery charging LED will also flash at a rapid rate. If 2-3 successive attempts to charge the battery fail, the battery should be replaced. Please contact the factory for details on replacement batteries.

The battery is charged using a constant-current, constant-voltage method. There is a safety timeout period of 2 hours once the charging is in the constant-voltage mode. This will prevent damage to the battery from leaving power connected for too long. Noise from the 5V, 500mA charging power supply can degrade device performance; therefore, specifications apply to battery-powered operation only. The LED provided on the front panel for charging status will be lit when battery charging begins and will be constantly on until the battery is 90% charged. The LED will go off when the battery reaches 90% of its capacity, so it is advised to leave the battery charging for approximately 30 minutes after the LED goes off. Total battery charging time depends on how depleted the battery is at the time of charge. If the battery voltage is not so low as to require trickle charging prior to entering constant-current mode, the charge cycle is approximately 4.5 hours. Lithium ion batteries should not be stored at full charge. This decreases the overall battery lifetime (number of charge cycles). For maximum overall life of the battery, store units with less than 50% charge and charge just before use. Please note that if the Wi-Fi Terminus unit turns off due to a low battery condition, the charge indicator is turned off, even if the device is on the charger. This is because the microcontroller is in a special mode until the power is cycled to ensure a proper shutdown in low battery conditions. To re-enable the LED indicator that shows the battery is charging properly, please do the following: charge the battery for a few minutes. Remove the charger and cycle the power. Then re-insert the charger. The LED should function properly after this procedure. It is NOT necessary to follow this procedure to charge the battery, this is just to re-enable the indicator if the unit goes into its low battery shutdown mode.

6 Installation Instructions for Initial Setup

1. Power the Wi-Fi Terminus by turning the switch to the "ON" position (you may need to use a paper clip). Make sure the Wi-Fi antenna is properly connected and the internal GPS antenna is properly oriented (the Wi-Fi Terminus label should be facing upwards towards an open view of the sky).

   Proceed with 2a for an Infrastructure network and with 2b for an Ad Hoc network.

2. a. Provide a wireless router or a network access point
   The SSID should be set to 'CW85_Setup' and configured for channel 6 with wireless encryption disabled.
   The recommended settings are to have the router at 192.168.1.X (Please do not use 192.168.1.2 or
   192.168.1.3 – those addresses are pre-configured for the data server and the Wi-Fi Terminus respectively) and to use the 255.255.255.0 Subnet.
   If this is not the first time that you have installed the Wi-Fi Terminus unit and you have altered the SSID and channel settings in the device, please use your altered settings.

   b. Create an Ad Hoc network with IP 192.168.1.2 using SSID 'CW85_Setup' and channel 6. Go to Step 4.

3. Provide the host computer(s) IP settings to match those of the Wi-Fi Terminus GSNPRIMARYSNMPMGRIP address (for SNMP parameter management) and the GSNSENSORSERVERIP address (for GPS data). The default values for these are 192.168.1.2. Please note that if this computer is connected wirelessly to the network, then it must have the same SSID/channel/encryption settings as above.

4. Obtain and install a copy of Net-SNMP on the host computer configured with the GSNPRIMARYSNMPMGRIP as the IP address (default: 192.168.1.2); see www.net-snmp.org. Use the Net-SNMP commands to read (snmpget) and write (snmpset) the Wi-Fi Terminus configurable parameters. See Section 3 – Configuration via SNMP.

5. If you don't already have server software that is listening for the incoming data stream, or if you would like an easy-to-setup program for viewing the NMEA streams/debugging, we suggest using NetCat; see http://netcat.sourceforge.net/. Netcat can be used to display the ASCII GPS data being sent from the Wi-Fi Terminus. Once the unit has associated with the network and resolved 192.168.1.2, it will begin transmitting UDP packets to 192.168.1.2, port 9999.
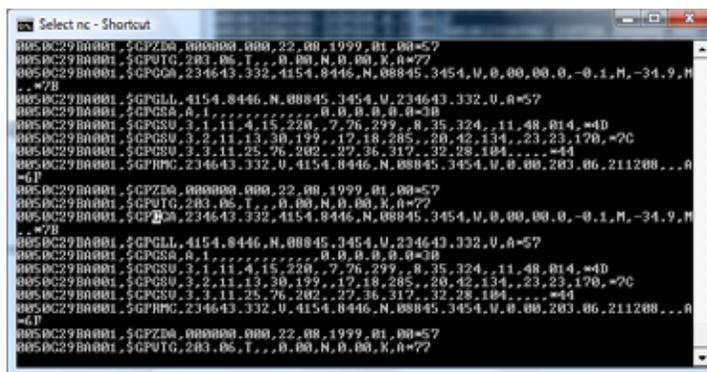
6. Monitoring the GPS data using Netcat:
   Netcat is a utility that can be used to read the UDP packets containing the GPS data from the Wi-Fi Terminus. The Netcat utility is freely available at http://netcat.sourceforge.net/.
   The Wi-Fi Terminus GPS receiver communicates on port 9999. A simple Netcat command line to display the GPS data would look like:

   nc –l –p 9999 –u

   An example of the output that would be seen in a NetCat window:

JANUS REMOTE COMMUNICATIONS

7. Configuring the device for the new network

a. Configuring the new IP settings

These network settings take effect on a power cycle, so they should all be changed (including encryption, if necessary) and then the unit should be rebooted for these settings to take effect. It is highly recommended to change just the settings for SSID1 so that if something is not right, it is easy to go back into the device using the CW85_Setup on SSID2. IMPORTANT - once the network settings are modified and the Wi-Fi Terminus is ready to be rebooted - bring down the CW85_Setup network so that the device can no longer see it and try to connect.

These are the settings that will most likely need to be changed for the new network:

> GSNIPADDRESS
>
> GSNSUBNETADDRESS
>
> GSNGATEWAYIPADDRESS
>
> STATIC IP ENABLED
>
> GSNPRIMARYSNMPMGRIP
>
> GSNAPSSID1
>
> GSNAPCHANNEL1

Details follow below for specific information on changing each OID:

- GSNIPADDRESS - .1.3.6.1.4.1.28295.1.1.3.1.0
  This changes the IP address of the Wi-Fi Terminus.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.3.1.0 a "new IP address"
  The new IP address should be in decimal-dot notation, enclosed in quotes.

- GSNSUBNETADDRESS - .1.3.6.1.4.1.28295.1.1.3.2.0
  This changes the subnet address of the Wi-Fi Terminus.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.3.2.0 a "new subnet"
  The new subnet should be in decimal dot notation, enclosed in quotes.

- GSNGATEWAYIPADDRESS - .1.3.6.1.4.1.28295.1.1.3.3.0
  This changes the gateway IP address of the Wi-Fi Terminus.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.3.3.0 a "new gateway"
  The new gateway should be in decimal dot notation, enclosed in quotes.

- STATIC IP ENABLED - .1.3.6.1.4.1.28295.1.1.3.4.0
  To set the device for DHCP, leave the above OIDs as they are and set this OID to 0 (default   is 1).
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.3.4.0 i 0
  This will enable DHCP.

- GSNPRIMARYSNMPMGRIP - .1.3.6.1.4.1.28295.1.1.4.3.0
  Change the SNMP manager to the machine on the new network that you want to control the Wi-Fi Terminus on. Leave the GSNSECOND-ARYSNMPMGRIP at 192.168.1.2 so that you can still go back to the CW85_Setup SSID if you need to. Once the unit has been brought up on the new network, you can change the GSNSECONDARYSNMPMGRIP to the new IP, set it to 0.0.0.0 to disable it, or leave it at the default.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.3.0 a "new IP address"
  The new IP address should be in decimal-dot notation, enclosed in quotes.

- GSNAPSSID1 - .1.3.6.1.4.1.28295.1.1.4.5.1.2.1
  Use this OID to change SSID1.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.2.1 s "new ssid"
  Please be sure to enclose the new SSID in quotes or it may be truncated.

- GSNAPCHANNEL1 - .1.3.6.1.4.1.28295.1.1.4.5.1.3.1
  Use this OID to change the channel for SSID1.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.3.1 i channelNumber
  Channel number can be 1-11.

b. Configuring the new security settings

Encryption may need to be added for the new network. Please note that these options are read-disabled - so close attention must be paid to the response string when setting these options for confirmation that they are set appropriately for the network.

 WEP Settings for SSID1 (note that there is no passphrase option - only hex key):

 GSNWEPKEYIDSSID1

 GSNWEPKEYLENSSID1

 GSNWEPKEYAUTHMODESSID1

 GSNENCRYPTIONMODESSID1

 GSNAPWEPKEYVALSSID1

- GSNWEPKEYIDSSID1 - .1.3.6.1.4.1.28295.1.1.4.5.1.4.1
  This sets which key to use - 0-3, 0 is default
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.4.1 i key

- GSNWEPKEYLENSSID1 - .1.3.6.1.4.1.28295.1.1.4.5.1.5.1
  This sets WEP64 or WEP128 - default is WEP64. 13 sets to WEP128
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.5.1 i 13

- GSNWEPKEYAUTHMODESSID1 - .1.3.6.1.4.1.28295.1.1.4.5.1.8.1
  Default is Open Key (1), can be changed to Shared Key (2)
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.8.1 i keyMode

6 Installation Instructions for Initial Setup continued

- GSNENCRYPTIONMODESSID1 - .1.3.6.1.4.1.28295.1.1.4.5.1.9.1
  This OID controls which encryption types are allowed on SSID1. By default, all possible encryption types are enabled. This should be reduced to only the appropriate type - eg for WEP - set to integer value 1.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.9.1 i encryptionMode

- GSNAPWEPKEYVALSSID1 - .1.3.6.1.4.1.28295.1.1.4.5.1.6.1
  This OID sets the encryption key, in hex. There is no passphrase option for WEP.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.6.1 x hexKey
  Example1: use 0x0102030405060708090a0b0c0d for the WEP-128 hex key: 0102030405060708090a0b0c0d
  Example2: use 0x0102030405 for the WEP-64 hex key: 0102030405
  WEP128 keys have 26 digits (0-9, A-F) and WEP64 keys have 10 digits.

**It is important to note that the device does not expect to have Identical SSIDs configured for different security options, ex SSID1 configured for WEP and SSID2 configured as OPEN with identical SSID/Channel numbers. This can cause issues with association.

WPA/WPA2 settings for SSID1:
GSNAPPSKPASSPHRASESSID1
or
GSNPSKKEY1
GSNENCRYPTIONMODESSID1

- GSNAPPSKPASSPHRASESSID1 - .1.3.6.1.4.1.28295.1.1.4.5.1.7.1
  This OID will change ONLY the passphrase for SSID1... GSNPSKPASSPHRASE changes all three and is deprecated.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.7.1 s "passphrase"
  Be sure to enclose the passphrase in quotes or it may be truncated.

- GSNPSKKEY1 - .1.3.6.1.4.1.28295.1.1.2.10.0
  Use this OID to set the key INSTEAD of using a passphrase. It is not necessary to use this if you use the passphrase.
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.2.10.0 x 0x(64digits)
  Where the 64 digits are 0-9 and A-F

- GSNENCRYPTIONMODESSID1 - .1.3.6.1.4.1.28295.1.1.4.5.1.9.1
  This OID changes which encryption options are enabled per SSID. By default, all possible encryption modes are enabled. This should be reduced to only the appropriate type - for WPA2 - set to integer value 16, for WPA set to integer value 2
  Use the form
  snmpset -v1 -Oa -c GSN_SET 192.168.1.3 .1.3.6.1.4.1.28295.1.1.4.5.1.9.1 i encryptionMode
  Binary of 16 (00010000b) -- so 16 corresponds with bit 4 in the OID Table - See Appendix I for more details
  Binary of 2 (00000010b) -- so 2 corresponds to bit 1 in the OID Table

Once all of the appropriate settings have been changed, bring the CW85_Setup network down and reboot the Wi-Fi Terminus device. You should see the status indicator flash appropriate that is is able to associate with the new network. You should also be able to communicate with the device with the newly configured SNMP manager. If the device fails to associate with the new network, bring that network down and restore the CW85_Setup network and double check the settings. For the security settings, you need to pay close attention to the SNMP response when you set them as this is the only way to confirm that it used the right values - you cannot read them back over SNMP for protection.

8. Configuring the device for desired operation - basic settings

To send data to the new server, you may need to change the IP and Port for the real-time GPS data stream.

GSNSENSORSERVERIP
GSNSENSORDATAPORTNUM

- GSNSENSORSERVERIP - .1.3.6.1.4.1.28295.99.1.2.1.6.5
  This OID sets the destination IP for the real-time GPS data.
  Use the form
  snmpset -v1 -Oa -c GSN_SET <Device IP addr> .1.3.6.1.4.1.28295.99.1.2.1.6.5 a "destination"
  Please use decimal dot notation for the IP addresses, eg - 192.168.1.3

- GSNSENSORDATAPORTNUM - .1.3.6.1.4.1.28295.99.1.2.1.9.5
  This OID sets the destination port for the real-time GPS data.
  Use the form
  snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.9.5 i newPort

To change the IP and port for the logged GPS data use
NTLOGSERVERIPADDR
NTLOGSERVERPORTNUM

- NTLOGSERVERIPADDR - .1.3.6.1.4.1.28295.99.1.2.1.6.3
  This OID sets the destination IP for the logged GPS data.
  Use the form
  snmpset -v1 -Oa -c GSN_SET <Device IP addr> .1.3.6.1.4.1.28295.99.1.2.1.6.3 a "destination"
  Please use decimal dot notation for the IP addresses, eg - 192.168.1.3

- NTLOGSERVERPORTNUM - .1.3.6.1.4.1.28295.99.1.2.1.9.3
  This OID sets the destination port for the logged GPS data.
  Use the form
  snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.9.3 i newPort

No change is required to the packet type if you want to use UDP. To use TCP for either the real time data or the data log, use one or both of the following:
NTDATASERVERPORTTYPE
NTLOGSERVERPORTTYPE

- NTDATASERVERPORTTYPE - .1.3.6.1.4.1.28295.99.1.2.1.7.5
  This OID sets the data server port type (real-time data).
  Use the form
  snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.7.5 i 2
  For this OID, 2 is TCP and 1 is UDP. No other options are valid.

- NTLOGSERVERPORTTYPE - .1.3.6.1.4.1.28295.99.1.2.1.7.3
  This OID sets the log server port type (logged GPS data)
  Use the form
  snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.7.3 i 2
  For this OID, 2 is TCP and 1 is UDP. No other options are valid.

6 Installation Instructions for Initial Setup continued

To configure which data is sent and how often it is sent, use the following:

NTGPSUPDATERATE
NTMSGENABLE

NTGPSUPDATERATE - .1.3.6.1.4.1.28295.99.1.2.1.16.5
This OID controls the rate at which the GPS gives real-time updates to position.
Use the form
snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.16.5 i rate
The rate is in seconds. Setting rate as 2 sets the device to report every other second, 3 sets the device to report every three seconds... etc.

- NTMSGENABLE - .1.3.6.1.4.1.28295.99.1.2.1.21.5
  This OID controls the enabling of the GPS messages by the bitwise binary representation of the integer msgs.
  Use the form
  snmpset -v1 -Oa -c GSN_SET <Device IP address> .1.3.6.1.4.1.28295.99.1.2.1.21.5 i msgs
  Order of the bitwise binary representation (MSB to LSB):
  0, GPVTG,GPZDA, GPRMC   GPGSV,GPGSA,GPGLL, GPGGA
  GPRMC only is 0001 0000b, which is the integer 16
  GPGLL only is 0000 0010b, which is the integer 2
  GPGGA only is 0000 0001b, which is the integer 1
  For GPRMC, GPGLL and GPGGA, you would send 19 (16+2+1) in this string.

If all of the messages are disabled, the Power indicator will no longer flash... the flash interval is based on the GPS update rate and if the rate is 0 or the messages are all disabled, this light will no longer flash. If the rate changes, the rate that this LED flashes will also change. The duration of the flash is based on the number of messages that are enabled - a longer flash indicates more messages are being sent.

Unlike the network settings, which need a reboot to take effect, these changes are all immediate EXCEPT for packet type. Also, if the TCP connection is already established, the new IP/Port won't take effect until a new socket connection is made.

Please see Appendix I for more configuration options for the Wi-Fi Terminus.

OID relative to .1.3.6.1.4.1.28295.99.1.2.1

NAME	OID[1]	Access	Type	Default	Range	Comments
GSNSENSORSERVERIP	6.5	R/W	IP ADDRESS	192.168.1.2	All possible values	IP address of the sensor data server for the Wi-Fi Terminus.
GSNSENSORDATAPORTNUM	9.5	R/W	INTEGER	9999	All possible values	Port number of the sensor data server for the Wi-Fi Terminus.
NTLOGSERVERIPADDR	6.3	RW	IP ADDRESS	192.168.1.2	All possible	IP for the data log server. Changes for UDP are automatic, changes for TCP take effect following a reboot.
NTLOGSERVERPORTNUM	9.3	RW	INTEGER	9998	All possible	Port for the data log. Changes for UDP are automatic, changes for TCP take effect following a reboot.
NTLOGSERVERPORTTYPE	7.3	RW	INTEGER	1(UDP)	1-2(TCP is 2)	Packet type for the log. Change to this take effect following a reboot.
NTDATASERVERPORTTYPE	7.5	RW	INTEGER	1(UDP)	1-2(TCP is 2)	Packet type for the data. Changes to this take effect following a reboot.
NTTESTVAR	11.5	RW	INTEGER	0	0-1	Writing a 0 or 1 to this will cause a diagnostic sentence to be sent containing RSSI and battery status.
NTGPSUPDATERATE	16.5	RW	INTEGER	1	0-86399	Data transmission rate in seconds.
NTFLASHUPDATERATE	19.5	RW	INTEGER	1	0-86399	Data save rate as a multiple of the transmission rate.
NTSENDFIX	20.5	RV	INTEGER	0	0-127	0 means continual sending of GPS data at the rate in 16.5. 1 causes data transmission only when the GPS has a fix. Refreshed each boot.
NTMSGENABLE	21.5	RW	INTEGER	127	Meaningful range currently 0 - 127	The binary representation of this integer number controls which GPS messages are enabled. See Section 1.6 for individual message details.
NTNUMSEND	23.5	RV	INTEGER	1	0-5	Controls the number of times the unit attempts to send out data. Refreshed each transmission.
NTNUMFIX	24.5	RV	INTEGER	1	0-127	Active only when 20.5 is non-zero. Controls the number of fixes that must be acquired prior to transmitting any fix data. Once this number of fixes has been acquired, then the Wi-Fi Terminus will begin sending fix data the number of times specified in 20.5. refreshed each boot.
NTFLASHALWAYSSAVE	27.5	RW	INTEGER	0	0-1	Setting this bit enables the always save feature. This will cause data to be saved to flash memory at the configured rate even if the network is detected and the data transmits. Note that if this is set to 1, data will not be sent out the data log until given command 28.5.
NTFLASHDUMP	28.5	RW	INTEGER	0	0-1	Data log dump command. Writing a 0 or 1 to this bit provides a one time successful dump of the data log. Reading this bit returns the last value set. This bit does not have to be cleared or set specifically, writing either will cause the dump operation.
NTFLASHERASE	29.5	RW	INTEGER	0	0-1	Data log erase command. Writing a 0 or a 1 to this bit forces the data log to erase. Reading this bit returns the last value set. This bit does not have to be cleared or set specifically, writing either will cause the erase operation.

For security purposes, all WEP/WPA/WPA2 security settings are read disabled by default. The Wi-Fi Terminus will respond to a read of the security settings with "Read-Disabled" if it is a String or Hex String, and with 255 if it is an integer. To confirm a settings change, please note the SNMP response string that is sent with an SNMPSET command. If the new value is set appropriately, you will see the new value in the response string in the form "INTEGER = XXXX" or "STRING = XXXX". If the value is returned in parenthesis, it was not acknowledged properly.

Table 5: Wi-Fi Terminus NT-110ST OID Table

Notes
1. The OID column includes the ending 'instance identifier' which must be included in the MIB variable.
2. These values are assigned via DHCP, which is by default enabled on the device.
3. On V3.0, the 2nd GSNAPSSID was LTRX_IBSS and the 3rd was CW85_Setup. For V3.01 and above, the table shows the correct values.

OID Relative to .1.3.6.1.4.1.28295.1.

NAME	OID[1]	Access	Type	Default	Range	Comments
GSNFWVERSION	1.1.2.0	R	INTEGER		All possible values	Integer returned, convert to hex for firmware version. Example: 67108867 = ID: 0x00040003 (Version 4.00.03)
GSNPLATFORMVERSION	1.1.3.0	R	INTEGER		All possible values	Platform version
GSNRESTOREFACTORYCFG	1.1.4.0	RW	INTEGER	-		**Please consult factory prior to use. This will reset the MAC address. Use** .1.3.5.0 to re-set the MAC to original state.
GSNLASTERROR	1.1.5.0	RW	STRING	-		Last error occurred
GSNREBOOTNODE	1.1.6.0	RW	INTEGER	-		Restart network
GSNBATTERYWARNINGLEVEL	1.1.8.0	RW	INTEGER	Varies[4]	-	Battery warning level - Do Not Chnage
GSNBATTERYSTANDBYLEVEL	1.1.9.0	RW	INTEGER	Varies[4]	-	Battery standby level - Do Not Change
GSNSCANTYPE	1.2.1.0	RW	INTEGER	1(Active)	0(Passive)-1(Active),	DO NOT CHANGE FOR NORMAL OPERATION
GSNADHOCSSID	1.2.2.0	RW	STRING	"<null>"	-	SSID in Ad Hoc mode. This is used for a special mode when you need to create an Ad Hoc network. Use GSNAPSSID1-3 for normal operation when wanting to join an existing Ad Hoc network. If this is configured, the unit will continue to try and create this Ad Hoc network rather than continuing to search for the other SSIDs.
GSNADHOCCHANNEL	1.2.3.0	RW	INTEGER	6	All supported channels	Channel in Ad Hoc mode
GSNAUTHALGO	1.2.4.0	R	INTEGER			Auth algo used - Do Not Change
GSNPSKPASSPHRASE	1.2.5.0	W Read Disabled	STRING	GSDemo123		Deprecated. Use .1.3.6.1.4.1.28295.1..1.4.5.1.7 (1-3) GSNAPPSKPASSPHRASE SSID (1-3)
GSNOUTERAUTHTYPE	1.2.6.0	R	INTEGER	-		DOES NOT EXIST FOR WPA2_PSK VERSION
GSNINNERAUTHTYPE	1.2.7.0	R	INTEGER	-		DOES NOT EXIST FOR WPA2-PSK VERSION
GSNUSERNAME	1.2.8.0	RW	STRING	-		DOES NOT EXIST FOR WPA2-PSK VERSION
GSNPASSWD	1.2.9.0	RW	STRING	-		DOES NOT EXIST FOR WPA2-PSK VERSION
GSNPSKKEY1	1.2.10.0	W Read Disabled	HEX	"<null>"	256-bit pseudo-random sequence.	Pre computed PSK key. This key is derived from SSID1 and the pass phrase. Enter as 'Ox', followed by 64 digits using 0-9 and a-f
GSNPSKKEY2	1.2.11.0	W Read Disabled	HEX	"<null>"	256-bit pseudo-random sequence.	Pre computed PSK key. This key is derived from SSID1 and the pass phrase. Enter as 'Ox', followed by 64 digits using 0-9 and a-f
GSNPSKKEY3	1.2.12.0	W Read Disabled	HEX	"<null>"	256-bit pseudo-random sequence.	Pre computed PSK key. This key is derived from SSID1 and the pass phrase. Enter as 'Ox', followed by 64 digits using 0-9 and a-f

Table 5: Wi-Fi Terminus NT-110ST OID Table

For security purposes, all WEP/WPA/WPA2 security settings are read disabled by default. The Wi-Fi Terminus will respond to a read of the security settings with "Read-Disabled" if it is a String or Hex String, and with 255 if it is an integer. To confirm a settings change, please note the SNMP response string that is sent with an SNMPSET command. If the new value is set appropriately, you will see the new value in the response string in the form "INTEGER = XXXX" or "STRING = XXXX". If the value is returned in parenthesis, it was not acknowledged properly.

Notes
1. *The OID column includes the ending 'instance identifier' which must be included in the MIB variable.*
2. *These values are assigned via DHCP, which is by default enabled on the device.*
3. *On V3.0, the 2nd GSNAPSSID was LTRX_IBSS and the 3rd was CW85_Setup. For V3.01 and above, the table shows the correct values.*
4. *Hardware calibrated number. Typical values for V4.0 and V4.01 are 600 (warning) and 479 (standby).*

JANUS REMOTE COMMUNICATIONS

OID Relative to .1.3.6.1.4.1.28295.1.

NAME	OID[1]	Access	Type	Default	Range	Comments
GSNIPADDRESS	1.3.1.0	RW	IP ADDRESS	192.168.1.3	All possible values	IP address of the Wi-Fi Terminus
GSNSUBNETADDRESS	1.3.2.0	RW	IP ADDRESS	255.255.255.0	All possible values	Subnet of Wi-Fi Terminus
GSNGATEWAYIPADDRESS	1.3.3.0	RW	IP ADDRESS	"<null>"	All possible values	Gateway IP in Infrastructure mode.
STATICIPENABLED	1.3.4.0	RW	INTEGER	1	0-1	Set to 1 to enable static IP. Set to 0 to enable DHCP.
GSNMACADDRESS	1.3.5.0	RW	HEX	0x0054A9BAYYY	All possible values	Mac address. Read with -O t option To be used only in conjunction with GSN restore factory CFG
GSNPRIMARYSNMPMGRIP	1.4.3.0	RW	IP ADDRESS	192.168.1.2	All possible values,	IP of SNMP manager
GSNSECONDARYSNMPMGRIP	1.4.4.0	RW	IP ADDRESS	192.168.1.2	All possible values,	IP of backup SNMP manager
GSNAPSSID1	1.4.5.1.2.1	R/W	STRING	"CW85_Setup"	All possible values	SSID's of the access point to be used in infrastructure
GSNAPSSID2	1.4.5.1.2.2	R/W	STRING	"CW85_Setup"[3]	All possible values	mode. They will be searched in order.
GSNAPSSID3	1.4.5.1.2.3	R/W	STRING	"LTRX_IBSS"[3]	All possible values	
GSNAPCHANNEL1	1.4.5.1.3.1.	R/W	INTEGER	6	1-11	Access point channel number for the corresponding SSID.
GSNAPCHANNEL2	1.4.5.1.3.2	R/W	INTEGER	6	1-11	
GSNAPCHANNEL3	1.4.5.1.3.3	R/W	INTEGER	6	1-11	
GSNAPWEPKEYIDSSID1	1.4.5.1.4.1	RW	INTEGER	0	0-3	WEP Key ID
GSNAPWEPKEYIDSSID2	1.4.5.1.4.2	RW	INTEGER	0	0-3	WEP Key ID
GSNAPWEPKEYIDSSID3	1.4.5.1.4.3	RW	INTEGER	0	0-3	WEP Key ID
GSNAPWEPKEYLENSSID1	1.4.5.1.5.1	RW	INTEGER	5 (WEP64)	5 or 13 (WEP128)	WEP Key Length
GSNAPWEPKEYLENSSID2	1.4.5.1.5.2	RW	INTEGER	5 (WEP64)	5 or 13 (WEP128)	WEP Key Length
GSNAPWEPKEYLENSSID3	1.4.5.1.5.3	RW	INTEGER	5 (WEP64)	5 or 13 (WEP128)	WEP Key Length
GSNAPWEPKEYVALSSID1	1.4.5.1.6.1	RW	HEX	0x00, 0x00, 0x00, 0x00, 0x00	5 Bytes or 13 Bytes using O-F and 0-9	WEP Key Value Enter as 0x0000000000, using 10 or 26 digits after "0x".
GSNAPWEPKEYVALSSID2	1.4.5.1.6.2	RW	HEX	0x00, 0x00, 0x00, 0x00, 0x00	5 Bytes or 13 Bytes using O-F and 0-9	WEP Key Value Enter as 0x0000000000, using 10 or 26 digits after "0x".
GSNAPWEPKEYVALSSID3	1.4.5.1.6.3	RW	HEX	0x00, 0x00, 0x00, 0x00, 0x00	5 Bytes or 13 Bytes using O-F and 0-9	WEP Key Value Enter as 0x0000000000, using 10 or 26 digits after "0x".
GSNAPPSKPASSPHRASESSID1	1.4.5.1.7.1	RW	STRING	"<null>"	-	AP Pass Phrase
GSNAPPSKPASSPHRASESSID2	1.4.5.1.7.2	RW	STRING	"<null>"	-	AP Pass Phrase
GSNAPPSKPASSPHRASESSID3	1.4.5.1.7.3	RW	STRING	"<null>"	-	AP Pass Phrase

For security purposes, all WEP/WPA/WPA2 security settings are read disabled by default. The Wi-Fi Terminus will respond to a read of the security settings with "Read-Disabled" if it is a String or Hex String, and with 255 if it is an integer. To confirm a settings change, please note the SNMP response string that is sent with an SNMPSET command. If the new value is set appropriately, you will see the new value in the response string in the form "INTEGER = XXXX" or "STRING = XXXX". If the value is returned in parenthesis, it was not acknowledged properly.

Table 5: Wi-Fi Terminus NT-110ST OID Table

Notes
1. *The OID column includes the ending 'instance identifier' which must be included in the MIB variable.*
2. *These values are assigned via DHCP, which is by default enabled on the device.*
3. *On V3.0, the 2nd GSNAPSSID was LTRX_IBSS and the 3rd was CW85_Setup. For V3.01 and above, the table shows the correct values.*

JANUS REMOTE COMMUNICATIONS

OID Relative to .1.3.6.1.4.1.28295.1.

NAME	OID[1]	Access	Type	Default	Range	Comments
GSNWEPKEYAUTHMODESSID1	1.4.5.1.8.1	RW	INTEGER	1 (Open)	1-2 (Shared)	Authentication
GSNWEPKEYAUTHMODESSID2	1.4.5.1.8.2	RW	INTEGER	1 (Open)	1-2 (Shared)	Authentication
GSNWEPKEYAUTHMODESSID3	1.4.5.1.8.3	RW	INTEGER	1 (Open)	1-2 (Shared)	Authentication
GSNENCRYPTIONMODESSID1	1.4.5.1.9.1	RW	INTEGER	219(DBh)	All possible Values	Encryption control for SSIDX.. Bitmap of the binary equivalent controls which encryption methods are allowed. Note: Bit 3 and 6 are not available on WPA2-PSK version. Not available on version 4.0 and prior.
GSNENCRYPTIONMODESSID2	1.4.5.1.9.2	RW	INTEGER	219(DBh)	All possible Values	Bit 0 WEP, Bit 1 WPA-Personal, Bit 2 RESERVED - Set to 0 Bit 3 WPA-Enterprise
GSNENCRYPTIONMODESSID3	1.4.5.1.9.3	RW	INTEGER	219(DBh)	All possible Values	Bit 4 WPA2-Personal Bit 5 RESERVED - Set to 0 Bit 6 WPA2-Enterprise (N/A), Bit 7 Open Encryption (none)
GSNCONFIGCOMPLETE	1.4.6.0	RW	INTEGER			DO NOT CHANGE
GSNGETCOMMSTRING	1.4.10.0	R	STRING	GSN_GET		DO NOT CHANGE
GSNSETCOMMSTRING	1.4.11.0	R	STRING	GSN_SET		DO NOT CHANGE
GSNTRAPCOMMSTRING	1.4.12.0	R	STRING	GSN_TRAP		DO NOT CHANGE
GSNTRAPCONFIGINTNEWTMR	1.4.13.0	RW	HEX	0x0000001400000000 HEX String (10 seconds)		Wakeup interval for config traps. May be set to 0 to disable. Calculate based on 1 second as 0x0000_0000_0200_0000 (0xB8B7_B6B5_B4B3_B2B1) but send as 0x0000_0020_0000_0000 (0xB1B2_B3B4_B5B6_B7B8) Read the HEX value with the -Ot/Ox option rather than -Oa.
GSNTRAPLINKUPINTNEWTMR	1.4.14.0	RW	HEX	0x0000002800000000 HEX String (20 seconds)		Wakeup interval for linkup traps. Maybe set to 0 to disable. Calculate based on 1 second as 0x0000_0000_0200_0000 (0xB8B7_B6B5_B4B3_B2B1) but send as 0x0000_0020_0000_0000 (0xB1B2_B3B4_B5B6_B7B8) Read the HEX value with the -Ot/Ox option rather than -Oa.

For security purposes, all WEP/WPA/WPA2 security settings are read disabled by default. The Wi-Fi Terminus will respond to a read of the security settings with "Read-Disabled" if it is a String or Hex String, and with 255 if it is an integer. To confirm a settings change, please note the SNMP response string that is sent with an SNMPSET command. If the new value is set appropriately, you will see the new value in the response string in the form "INTEGER = XXXX" or "STRING = XXXX". If the value is returned in parenthesis, it was not acknowledged properly.

Notes

1. The OID column includes the ending 'instance identifier' which must be included in the MIB variable. (
2. These values are assigned via DHCP, which is by default enabled on the device.
3. On V3.0, the 2nd GSNAPSSID was LTRX_IBSS and the 3rd was CW85_Setup. For V3.01 and above, the table shows the correct values.

Table 5: Wi-Fi Terminus NT-110ST OID Table

JANUS REMOTE COMMUNICATIONS

OID Relative to .1.3.6.1.4.1.28295.1.

NAME	OID[1]	Access	Type	Default	Range	Comments
GSNFWUPDATEIP	1.6.1.0	RW	IPAD-DRESS	192.168.1.2	All possible values	Consult Factory before use.
GSNFWUPDATEPORT	1.6.2.0	RW	INTEGER	8355	All possible values	Consult Factory before use.
GSFWUPGRADENEEDED	1.6.3.0	RW	INTEGER	0		DO NOT USE
GSNHRDWAREVERSION	2.10.1.0	R	INTEGER		All possible values, not defined	The hardware version is loaded at boot time by the software from a hardware register.
GSNBOOTROMVERSION	2.10.2.0	R	INTEGER		All possible values, not defined	The boot ROM version is loaded at boot time by the software from a specific memory location
GSNWLANFWVERSION	2.10.3.0	R	INTEGER		-	Firmware version
GSNBUPVERSION	2.10.4.0	R	INTEGER		-	BUP version
GSNMODEMBVERSION	2.10.5.0	R	INTEGER		-	Modem B version
GSNSTREAMVERSION	2.10.6.0	R	INTEGER		-	Stream processor version
GSNLASTERRCODE	2.10.7.0	R	INTEGER		-	Last error code
GSNLASTERRPARAM	2.10.8.0	R	STRING		-	Last error parameter
GSNRANDOMVECTOR	2.10.9.0	R	STRING		-	Rx timestamp LSBs for random calculation
GSNRANDOMELEMENTS	2.10.10.0	R	INTEGER		-	
GSNLOWPOWERXTAL	2.10.11.0	R	INTEGER		-	

Table 5: Wi-Fi Terminus NT-110ST OID Table

Notes
1. The OID column includes the ending 'instance identifier' which must be included in the MIB variable.
2. These values are assigned via DHCP, which is by default enabled on the device.
3. On V3.0, the 2nd GSNAPSSID was LTRX_IBSS and the 3rd was CW85_Setup. For V3.01 and above, the table shows the correct values.

For security purposes, all WEP/WPA/WPA2 security settings are read disabled by default. The Wi-Fi Terminus will respond to a read of the security settings with "Read-Disabled" if it is a String or Hex String, and with 255 if it is an integer. To confirm a settings change, please note the SNMP response string that is sent with an SNMPSET command. If the new value is set appropriately, you will see the new value in the response string in the form "INTEGER = XXXX" or "STRING = XXXX". If the value is returned in parenthesis, it was not acknowledged properly.

Wi-Fi Terminus
NT-110ST
Wi-Fi
Enabled GPS

Revision History of Version 3.0

Revision	Date	Released By	Notes
P00	01/29/09	Engineering	Preliminary Release
P01	06/10/09	Engineering	OID Table Revisions, Updated Operation Description
R00	10/28/09	Engineering	Revisions to Specs, OID tables and External Release
R01	02/03/10	Engineering	Addition of Device Configuring for network, Flash Specifications
R02	05/02/11	Engineering	Release with new Name
R03	09/27/11	Engineering	Released with updates to Operation Section & OID Charts
R04	12/19/12	Engineering	Update to Sections 1.6, 1.7, and Appendix

Table 6 Revision History

Other Documentation

Use the following links for additional documentation that may be of use in understanding this document. Or, visit the Janus website to download documents – www.janus-rc.com.

Document
Quick Start Guide
Configuring for Wi-Fi Networks
Resetting to Default Configuration

Table 7 Additional Documentation List