Stinger 2.4 GHz Transceiver

Installation and Operation Instructions

NOTICES

U.S. Federal Communication Commision (FCC)

This device complies with part 15 of the U. S. FCC Rules and Regulations Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the U.S. FCC Rules These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications.   If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.
- Reorient or relocate the receiving antenna.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate the equipment.

FCC IDs and Industry Canada Certification Numbers are listed in the following table:

Module Types	Operating Frequency Range	Maximum Transmitter Power	Reflector, Stinger, Superstinger	FCC ID	
SM AP BH	ISM 2403-2483 MHz	500mW	Allowed on SM and BH	S4D STINGER-01	

FCC RF Exposure Statement

This equipment complies with FCC radiation exposure limits set for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. When using the Classic Stinger slip on reflector the system must be installed to provide a separation distance of at least 40 cm between the radiator and your body. When using the Super Stinger slip on parasitic antenna the system must be installed to provide a separation distance of at least 64 cm between the radiator and your body. When adding the Stinger reflector dish the reflector dish must be installed to provide a separation distance of a least 1 m between the radiator and your body.

This equipment is installed by professional installers which are instructed and trained to limit the RF exposure during installation.

This transmitter must not be co-located or operation in conjunction with any other antenna or transmitters.

GETTING STARTED

WELCOME
Congratulations on the purchase of the Stinger subscriber module from WB Manufacturing! The Stinger subscriber module is the latest innovation in high-speed wireless networking that lets you easily network at high speeds.

FEATURES
The following is a subset of features included with your Stinger subscriber module:

◆ Broadband network speeds.
◆ Small, compact design.
◆ No special setup on your PC.

INTENDED USE

This manual is intended to be used with Stinger software release version 3.x or greater. The intended audience for this manual is system operators and equipment installers.

PRODUCT DESCRIPTION

Stinger Subscriber Module

The base cover of your Stinger subscriber module is easily removed by depressing the release lever on the back of the cover.

Base Cover

Base Cover
Release
Lever
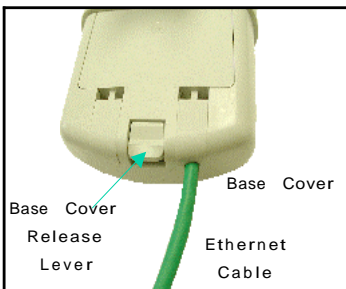
Ethernet
Cable

Remove the base cover as shown in FIGURE 1 to access the Ethernet connection and to view the LED indicators.

· The RJ-45 connector is used to attach the Ethernet cable.
· The LED's indicate system status and can be used for alignment.

Stinger SM

RJ45
Connector
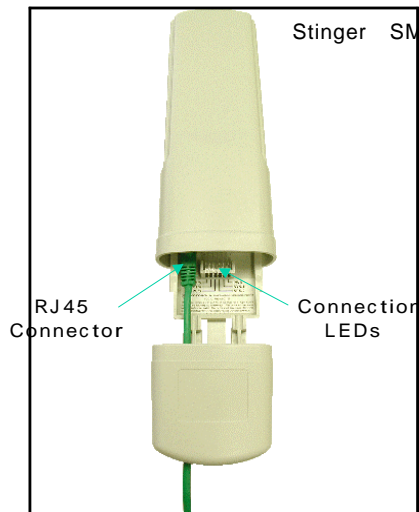
Connection
LEDs

The Connection LEDs report information about the current status of the subscriber module.   The following descriptions explain the function of each LED.

Operational Mode

When looking at the LEDs on the module the following descriptions go from left to right.

LNK: The link LED displays the status of the Ethernet link to the Stinger module. The LED will be constantly lit if there is an Ethernet link present. The LED is colored green.

ACT/4: The activity LED displays the status of any data activity on the Ethernet link. The LED will flash (at no particular speed) when data is being transferred on the Ethernet link. The LED is colored orange.

GPS/3: This LED is not used on the subscriber module.

SES/2: The session LED displays status of whether or not a subscriber module is in session (registered). The LED will be constantly lit if the unit is in session. The LED is green.

SYN/1: The sync LED displays sync status. In short, this LED will be lit if the unit is in session (i.e. registered – SES/2 LED is lit). The operator should minimize any flicker in this LED. The LED is orange.

PWR: The power LED displays the status of power to the module. The LED will be constantly lit if power is applied correctly. The LED is red.

When the subscriber module is not registered to an access point module the SYN/1, SES/2, and GPS/3 LEDs will cycle on and off from left to right.

Alignment Mode

When a subscriber module is placed in Alignment Mode the LEDs take on an entirely different purpose. The power LED will still indicate whether or not power is applied to the module. The 6 LEDs and are turned into a 6-position bar graph. The more LEDs that are lit, the better the RSSI and Jitter values the module is seeing. The colors of the LEDS have no particular meaning other than to assist is distinguishing one position from the next. See Alignment section for more information on alignment mode.

BACKGROUND INFORMATION ON NETWORKING

Computers are assigned IP addresses by network operators, which have two methods available, static or dynamic IP addressing. The user of this document will need to understand how IP addressing is done at their particular location.

All Stinger radio products (Subscriber Modules, Access Point Modules, and Backhaul Modules) have the default IP address of 169.254.1.1. For a computer to talk to Stinger, as it comes from the factory, either of the following conditions must be met:

- · If the computer is not configured for DHCP, then it has to have a static IP address on the 169.254 network (i.e. 169.254.1.5)
- · If the computer is configured for DHCP, then it will automatically obtain an IP address on the 169.254 network after minute or two as long as it is not connected to the network.

INSTALLATION

The following steps are required to install the Stinger subscriber module.
- Unpack the Stinger products
- Configure the subscriber module for the Stinger network
- Install the module
- Align the module

UNPACK THE STINGER PRODUCTS

Upon receipt, carefully inspect all shipping boxes for signs of damage. If there is damage, immediately notify the transportation company.

Unpack equipment, making sure that all ordered components have arrived. It is recommended that you save all the packaging materials. They can be used for transportation of the equipment to and from installation sites.

CONFIGURING THE SUBSCRIBER MODULE

⚠ In all cases, when a configuration parameter is modified, the change must be saved and the module must be rebooted.

The subscriber module, from the factory, is configured to scan all available frequencies in its specific frequency band. An operator will need to verify the following information:

- The operator may program a unique IP address into the subscriber module or can leave it at its defaults. The subscriber module is programmed to utilize the local IP address of 169.254.1.1. When configured in this manner the IP address is not accessible from the far side of a RF link to the module. If the operator requires that the LAN IP of the subscriber module be accessible from across the RF link then the public IP address feature is recommended. This feature will require that a routable IP address and appropriate subnet mask and gateway be utilized.
- The operator must configure the appropriate color code on the subscriber module so that it can register with an access point module. The color codes must match.
- The operator can prevent unauthorized users from connecting to the subscriber module's web based interface by assigning a password. There is no default password and password protection is turned off from the factory.
  Passwords can be from 1 to 16 characters. Any combination of characters is allowed, except for these special characters: " , . ' { } / \ ; : [ ] ( ) ` ~
  NOTE: If the operator forgets either the password or the IP address for the subscriber module, a Stinger default plug can be used to regain access. See Configuration section for information on default plug.
  There are two types of passwords that can be configured: display-only or full-access. The display-only password allows the operator to view the module's current status. The full-access password allows the operator to view the module's current status and change its configuration. By viewing the red lettering to the right of the entry fields, the operator can discern that a password is set.
- The operator can enter in information about the Site Name, Location, and Contact. This is optional.

In the 2.4 GHz band, the Stinger passive reflector can be used to establish links up to 15 miles. The subscriber module should be mounted to the reflector in the following manner. The reflector arm has a molded claw to receive

the plastic housing of the subscriber module. The module is now properly aligned within the reflector.

INSTALLATION OF THE SUBSCRIBER MODULE

When power is applied to a Stinger module or the unit reset via the web-based interface, the module will take approximately 25 seconds to boot up. During this boot up time, power on self-tests and other diagnostics are being performed.

The following steps must be performed for successful installation:
· Select a mounting location that is free from objects, such as buildings, large trees, etc., that will interfere with the line of sight to the Access Point cluster location. Be mindful of the Fresnel Zone.
· The Stinger module should be mounted vertically as shown in FIGURE 3. All Stinger modules' antennas are vertically polarized in this direction.
· Mount the Stinger subscriber module to a secured location on the side/roof of the building. The mount must be rigid and the subscriber module must not sway from outside forces.
· Illustrated in FIGURE 3 is an example of mounting the unit to an antenna mast.

Bare Stinger
(Bare SM)

· Leave the unit mounting means loose enough to allow for movement when performing the alignment procedure. They must be tightened after the alignment procedure is completed.

Classic Stinger

Super Stinger

Important Note about EIRP Limitations and Transmitter Power Settings

Stinger Type	Antenna Gain	Transmitter Power Setting	EIRP (dBm)	EIRP (watts)
Bare Stinger	8 dBi	+25 dBm (max)	33 dBm	2
Classic Stinger	14 dBi	+22 dBm	36 dBm	4
Super Stinger	18 dBi	+18 dBm	36 dBm	4
Stinger Reflector RCL1	19 dBi	+17 dBm	36 dBm	4
Stinger Reflector RCL2	20 dBi	+16 dBm	36 dBm	4
Stinger Reflector RCL3	22 dBi	+14 dBm	36 dBm	4

In order to comply with FCC EIRP limits, the transmitter output power may need to be reduced depending on the antenna configuration.

As with any such installed devices, the Stinger subscriber module and the Ethernet cable must be grounded in accordance with the latest revision of the National Electrical Code (NEC) and/or all

country and local electrical codes to provide some protection against damage caused by near-miss lightning strikes and other electrical discharges. The Stinger Ethernet surge suppressor is such a device for this situation.

·   Connect one end of an Ethernet cable to the Stinger subscriber module RJ-45 connector.
·   Connect other end of the Ethernet cable to the RJ-45 connector in the Stinger surge suppressor. Refer to the Surge Suppressor User Manual for specifications.
·   Connect one end of another Ethernet cable to the other RJ-45 connector in the Stinger Surge Suppressor.
·   Connect the other end of the Ethernet cable to the AC adapter.

The unused pins of the Ethernet cable (4,5,7 and 8) transmit power to the Stinger subscriber module. DO NOT place other networking equipment on the Ethernet cable between the AC adapter and the subscriber module. The module can be up to 328 feet (100 meters) from the power supply.

·   Plug the AC Adapter into an AC outlet.
·   Plug the other side of the AC adapter's Ethernet "pig tail" into the computer or network computer's Ethernet port. DO NOT plug the Ethernet "pig tail" from the AC adapter into the subscriber module. See following wiring diagram.

Wiring Diagram of Stinger subscriber module to Computer with Surge Suppressor
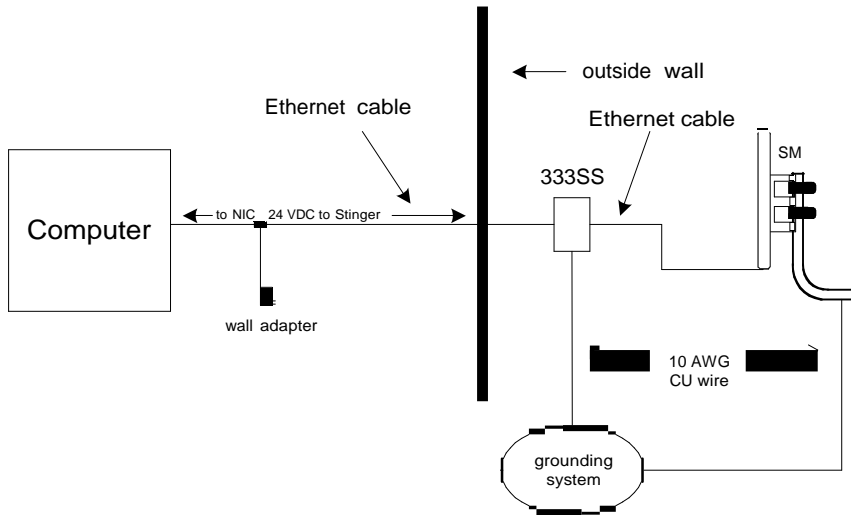
ALIGN THE SUBSCRIBER MODULE

There are two methods that can be utilized for aligning a subscriber module to an access point module. The first is to monitor the RSSI and Jitter values on the subscriber. The second is to utilize the built-in alignment tool on the subscriber module. In either case it is necessary for a computer to be connected to the subscriber module to gain access to the web-based interface.

Monitoring RSSI and Jitter

The RSSI (received signal strength indicator) and Jitter are two parameters that can be used for alignment of a subscriber module. The RSSI level must be above 700 and the Jitter must be 9 or below (with 5 being the best) for a link to be acceptable.

·   Point subscriber module in direction of the access point. Remember that when using the internal patch antenna the energy is radiated out in a 60° horizontal by 60° vertical pattern.

> IF USING A PASSIVE REFLECTOR on 2.4 GHz SUBSCRIBER MODULE: the passive reflector will change the radiated pattern to 6° horizontal by 6° vertical.

·   The module has a series of states that it will go through to register to an access point. Those states are: scanning, syncing, registering, and registered. RSSI and Jitter will not report on the web page till the unit is registered. If the module will not register ensure that there is line-of-sight, the access point module is transmitting, the color codes match, and that the subscriber is within the appropriate distance to the access point as specified by the max range value on the access point module.
·   After the module has registered, slowly adjust the positioning of the subscriber module until RSSI has been maximized and Jitter has been minimized. Lock down the module when appropriate.
·   Perform a link test to check the efficiency of the link. See Link Test for further information. The efficiencies must be above 90% in both the up and down link for packet loss to not occur.

USing Alignment Mode

The Alignment web page will display, in graphical form, levels for RSSI, Jitter, and the number of registered users at the access point.

- Point subscriber module in direction of the access point. Remember that when utilizing the internal patch antenna the energy is radiated out in a 60° horizontal by 60° vertical pattern.

- Set the web page to auto-refresh (see Configuration section for further information)

- Go to Alignment web page. Ensure that "RSSI Only Mode" is disabled.

- Click "Enable Aiming Mode" button.

- The module has a series of states that it will go through to register to an access point. Those states are: scanning, syncing, registering, and registered. RSSI and Jitter will not report on the web page till the unit is registered. If the module will not register ensure that there is line-of-sight, the access point module is transmitting, the color codes match, and that the subscriber is within the appropriate distance to the access point as specified by Stinger.

- Slowly adjust the positioning of the subscriber module and monitor the Alignment web page for a reading of the RSSI and Jitter. Lock down the module when appropriate.

- Click "Disable Aiming Mode" button.

- Perform a link test to check the efficiency of the link. See Link Test section for further information. The efficiencies must be above 90% in both the up and down link for major packet loss to not occur.

CABLING

The RF environment the Subscriber Module operates in often will permit use of unshielded cable. However, in cases where cable interference issues are suspected, or as part of A/B comparisons to debug field problems, use of shielded cable with Subscriber Modules may be warranted.

It is strongly recommended to use shielded cable for all Stinger infrastructure cabling associated with Backhauls, Access Points, and Cluster Management Modules. The environment these modules operate in often has significant or unknown or varying RF energy, and experience has been that the additional cost of shielded cabling is more than compensated by predictable operation and reduced debugging and support costs.

The following information describes the wiring standards for installing a Stinger system. All diagrams use the EIA/TIA 568B color standard.
Currently shipping modules auto-sense the Ethernet cable type – either RJ-45 straight-thru cable or RJ-45 crossover cable can be used to connect a network interface card (NIC), hub, router, or switch to a module.

Very early modules did not auto-sense. In cases where older modules are used:

· When connecting a Stinger device directly to a network interface card (NIC) use a RJ-45 straight-thru cable.
· When connecting a Stinger device directly to a hub, switch, or router use a RJ-45 crossover cable.

When using the Stinger AC wall adapter the +V is +11.5VDC to +30VDC with a nominal value of +24 VDC, and the maximum Ethernet cable run with the AC wall adapter is 328 feet (100 meters).

RJ-45 Straight-Thru:

- pin 1 →   white / orange   ← pin 1
- pin 2 →   orange   ← pin 2
- pin 3 →   white / green   ← pin 3
- pin 4 →   blue   ← pin 4
- pin 5 →   white / blue   ← pin 5
- pin 6 →   green   ← pin 6
- pin 7 →   white / brown   ← pin 7
- pin 8 →   brown   ← pin 8
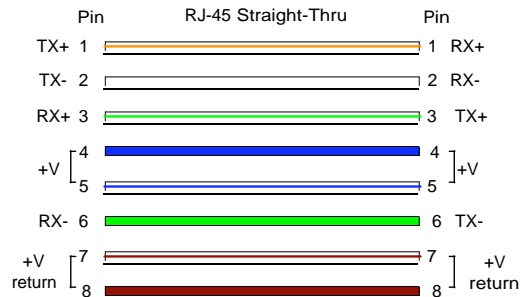
Pins 4, 5, 7, and 8 are used to carry power to the Stinger modules.

RJ-45 Crossover:

- pin 1 → white / orange ← pin 3
- pin 2 → orange ← pin 6
- pin 3 → white / green ← pin 1
- pin 4 → blue ← pin 4
- pin 5 → white / blue ← pin 5
- pin 6 → green ← pin 2
- pin 7 → white / brown ← pin 7
- pin 8 → brown ← pin 8

Pin	RJ-45 Crossover	Pin
TX+		3 RX+
TX-		6 RX-
RX+ 3		1 TX+
+V 4 / 5		4 / 5 +V
RX- 6		2 TX-
+V return 7 / 8		7 / 8 +V return
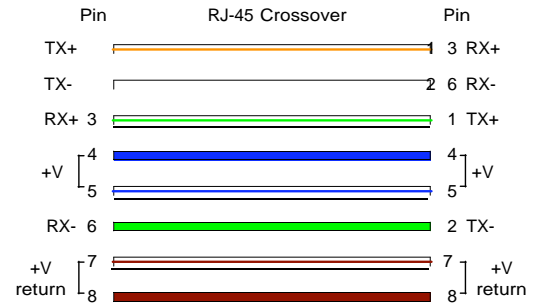
Pins 4, 5, 7, and 8 are used to carry power to the Stinger modules.

ADVANCED FEATURES

These features may be utilized in the Stinger System but are not required for basic operation.

SECURITY - DES ENCRYPTION

Standard Stinger modules provide Data Encryption Standard (DES) encryption. DES is a secret key encryption scheme using a 56 bit key. The basics of DES are that it performs a series of bit permutations, substitutions, and recombination operations on blocks of data using a secret key.

On the Stinger system, encryption of the over the air link is enabled or disabled per Access Point module or per Backhaul timing master module. The Stinger modules contain unique factory programmed secret keys to establish the encrypted link. If an authentication key (must be the same key on each end of the backhaul link) has been entered using the Backhaul Configuration page, then that key is also used to establish the DES encryption key. Encryption does not affect the performance or throughput of the system.

SECURITY - AES ENCRYPTION

WB Manufacturing also offers Stinger products that provide Advanced Encryption Standard (AES) encryption. Like DES, AES is a secret key encryption scheme, but AES uses the Rijndael algorithm and 128 bit keys to establish a higher level of security than DES.

Due to the level of security provided by AES, the US government has established export controls on communications products that use AES. These export controls may mean that outside of the US AES products are only available in certain regions – check with your Stinger distributor or reseller for availability in your area.

Stinger AES products run the same software as DES products, so the features available are exactly the same and work the same with the only exception being that the AES products provide AES instead of DES encryption when enabled for encryption on the Configuration screen. All the interface screens, Status pages, Configuration pages, etc. are identical. As new software features become available on DES products, the same software and the same features will be available for AES products.

DES backhauls are available in both 10 Mbps and 20 Mbps signaling rates. AES backhauls are only available with a 10 Mbps signaling rate.

Stinger DES products are not upgradeable to AES. To have the option of AES encryption, you must purchase AES products.

Stinger AES products use a different FPGA load than DES products. However, the FPGA will be upgraded as needed to provide new features or services similar to the DES products.

The same as with DES, encryption of the over the air link is enabled or disabled per Access Point module or per Backhaul timing master module. The Stinger modules contain unique factory programmed secret keys to establish the encrypted link. If an authentication key (must be the same key on each end of the backhaul link) has been entered using the Backhaul Configuration page, then that key is also used to establish the AES encryption key.

Stinger AES products and DES products do not interoperate when enabled for encryption, as DES and AES are different encryption schemes. An AES AP with encryption enabled can only communicate with AES SMs, and similarly an AES Backhaul timing master module with encryption enabled can only communicate with an AES Backhaul timing slave module. However, if encryption is disabled, AES modules can communicate with DES modules.

BRANDING

On each Stinger module, the web-based interface screens have a WB Mfg logo that can be replaced with an operator's company logo. The WB Mfg logo file is called canopy.jpg and the replacement file must also be called canopy.jpg. The new file is transferred via FTP to the module and then added to a special filesystem through a telnet session. The following command can be used during a telnet session:

- addwebfile – add a custom logo file to the filesystem
- clearwebfile – clear the customer logo file from the filesystem
- lsweb – list the custom logo file and display the storage space available on the filesystem

The following is a sample FTP session:

```
> ftp 169.254.1.1
Connected to 169.254.1.1
220 FTP server ready
Name (169.254.1.1:none): root
331 Guest login ok
Password: <password-if-configured>
230 Guest login ok, access restrictions apply.

ftp> binary
200 Type set to I

ftp> put canopy.jpg
ftp> quit
221 Goodbye
```

The following is a sample telnet session:

```
Login: root
Password: <password-if-configured>

Telnet+> lsweb

Flash Web files
free directory entries: 32
free file space    64336 bytes

Telnet+> addwebfile canopy.jpg
Telnet +> lsweb

Flash Web files
/Stinger.jpg    7867
free directory entries: 31
free file space: 56468

Telnet +> clearwebfile
Telnet+> lsweb

Flash Web files
free directory entries: 32
free file space    64336 bytes
```

THE INTERFACE SCREENS

The Stinger subscriber module contains a series of web pages that are used to interface to the unit. The following is a quick reference to interface screens. Note: These screens are subject to change by subsequent software versions. To access the web based interface you first must be on a computer that is in some way connected to the subscriber module. This can be done either directly or through a network. Enter the IP address of the subscriber module (default is 169.254.1.1) into the address bar of your browser and hit enter on your keyboard. The following web based interface pages are accessible:

- Status
- Configuration
- Event Log
- AP Eval Data
- Ethernet Stats
- Expanded Stats

The default page, when accessing the IP address of the Stinger unit is, the Status page.

STATUS PAGE

The Status page contains information on the operation of the product. It is the default webpage. The following parameters are displayed:

Device Type: displays the type of Stinger module that is currently being viewed. This field will let the operator know the frequency band of the module, the protocol that it is utilizing, and the MAC address of the module. The protocol for a subscriber module is multipoint. The MAC address will

be in the following format, 0a-
00-3e-xx-xx-xx.

Software Version: displays the version of the software that is currently loaded into the module.
Please make note of this information when obtaining technical support.

FPGA Version: displays the version of the FPGA (field programmable gate array) that is currently
loaded into the module. Please make note of this information when obtaining technical support.

Uptime: displays the length of time the module has been operating since a rest of the module
occurred.

System Time: displays the current time, which is inherited from the Stinger System via the
registration to an access point module. When the module is registered to a Stinger System where
a Cluster Management Module (CMM) is being utilized the time is displayed in Greenwich Mean
Time (GMT).

Ethernet Interface: displays the configuration of the Ethernet interface on the module.

Session Status: displays the current session state the module is in. There are five (5) options
that will display in this field, scanning, syncing, registering, registered, and alignment

- Scanning – module is cycling through the RF frequencies that it is configured to scan and looking for
  an access point module.
- Syncing – module is attempting to synchronize timing to a single access point module
- Registering – module sent a request for registration and is awaiting a response
- Registered – module is locked on to a specific access point module and ready to transmit and
  receive data packets
- Alignment – module is in alignment mode

RSSI: displays the current value for the Radio Signal Strength Indicator. This parameter will only
display information when the module is registered to an access point module and the value is only
updated by either refreshing the web browser screen or configuring the Stinger module to auto-
refresh (see Configuration web page.) An acceptable RSSI value for a registered link is greater
than 700; however it is important to view this value in conjunction with the Jitter value.

Jitter: displays the current value for the quality of the received signal. This parameter will only

display information when the module is registered to an access point module and the value is only updated by either refreshing the web browser screen or configuring the Stinger module to auto-refresh (see Configuration web page.) The value range for Jitter is 5-15, with the quality being better on the low end of the scale. Jitter must be below 9 for a link to be of acceptable quality.
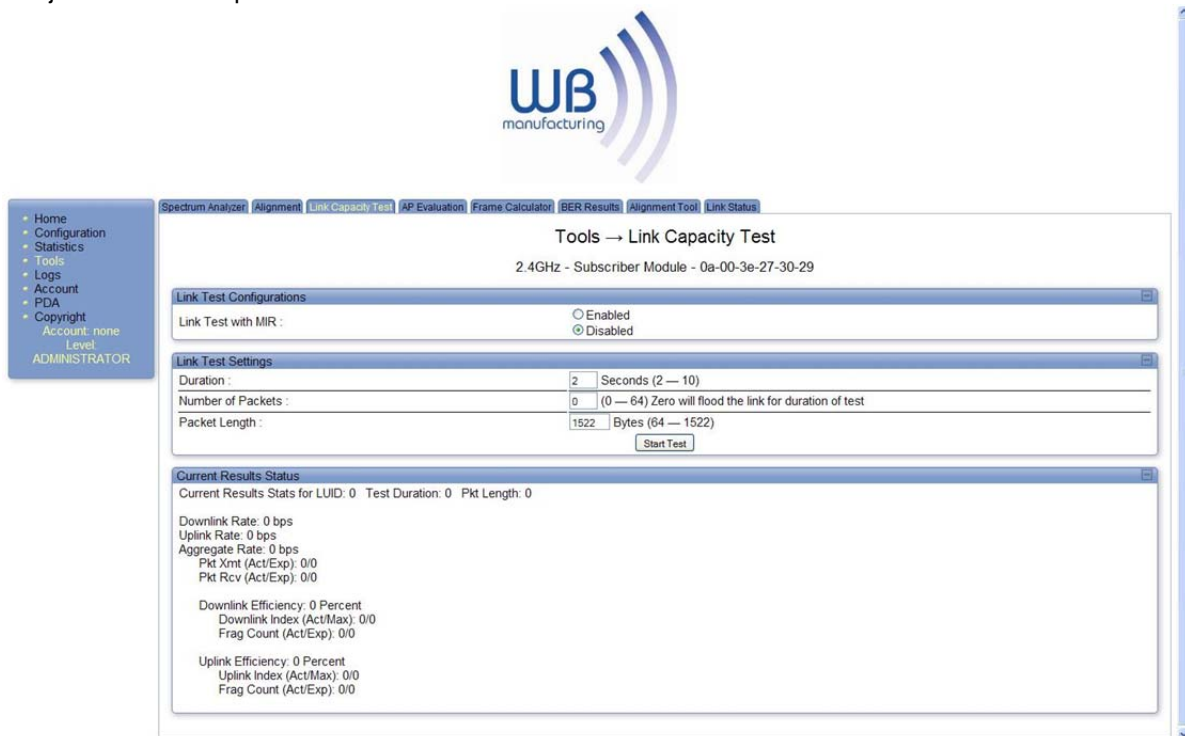
Air Delay: display the distance from the subscriber module to the registered access point module. At close range, 0-200 feet, the distance will not report accurately.

Radio Slicing Value: displays information to be used by Stinger technical support.

Radio Transmit Gain Setting: displays information to be used by Stinger technical support.

Site Name: displays information relating to the name of the physical module. This parameter can be set by the operator on the Configuration web page. This information is set into the sysName SNMP MIB-II object and can be polled via a SNMP management server.

Site Contact: displays contact information for the physical module. This parameter can be set by the operator on the Configuration web page. This information is set into the sysContact SNMP MIB-II object and can be polle

- Home
- Configuration
- Statistics
- Tools
- Logs
- Account
- PDA
- Copyright
  Account: none
  Level:
  ADMINISTRATOR

Tools → Link Capacity Test

2.4GHz - Subscriber Module - 0a-00-3e-27-30-29

Link Test Configurations

Link Test with MIR :
- ○ Enabled
- ⊙ Disabled

Link Test Settings

Duration :	2	Seconds (2 — 10)
Number of Packets :	0	(0 — 64) Zero will flood the link for duration of test
Packet Length :	1522	Bytes (64 — 1522)

[Start Test]

Current Results Status

Current Results Stats for LUID: 0   Test Duration: 0   Pkt Length: 0

Downlink Rate: 0 bps
Uplink Rate: 0 bps
Aggregate Rate: 0 bps
    Pkt Xmt (Act/Exp): 0/0
    Pkt Rcv (Act/Exp): 0/0

    Downlink Efficiency: 0 Percent
        Downlink Index (Act/Max): 0/0
        Frag Count (Act/Exp): 0/0

    Uplink Efficiency: 0 Percent
        Uplink Index (Act/Max): 0/0
        Frag Count (Act/Exp): 0/0

d via a SNMP management server.

CONFIGURATION

The Configuration webpage contains information and configurable parameters pertaining to the operation of the product.

Custom RF Frequency Scan Selection (SM) **List**: Choose the frequencies that the subscriber module will scan when looking for access point modules. 20 MHz wide channels are centered every 2.5 MHz. The default for this parameter for 2.4GHz modules is to scan 2415 MHz, 2435 MHz, and 2457.5 Mhz – only those 3 check boxes are
selected by default.

Select 2.4 GHz scan frequencies at least 5 MHz apart. Do not simply select all frequencies by checking every box. Stinger gives you checkboxes in the 2.4 GHz band for channels centered every 2.5
MHz, so you have flexibility for RF engineering based on your local RF environment. However, if you select scan frequencies only 2.5 MHz apart (in other words, if you check two boxes in sequence), there is potential for the SM to successfully register to an AP that is actually transmitting at a frequency 2.5 MHz higher as it scans up the selected frequencies. Registration may be successful, but the link is not as good as if it had registered 2.5 MHz higher, on the actual AP frequency.

WB manufacturing

General | IP | Radio | SNMP | Quality of Service (QoS) | Security | VLAN | VLAN Membership | DiffServ | Protocol Filtering | NAT | PPPoE | NAT Port Mapping | Unit Settings

- Home
- Configuration
- Statistics
- Tools
- Logs
- Account
- PDA
- Copyright
  Account: none
  Level:
  ADMINISTRATOR

Configuration → NAT

2.4GHz - Subscriber Module - 0a-00-3e-27-30-29

NAT Enable

NAT Enable/Disable :	○ Enabled ⊙ Disabled

Save Changes

WAN Interface

Connection Type :	DHCP ▾
IP Address :	0.0.0.0
Subnet Mask :	0.0.0.0
Gateway IP Address :	0.0.0.0
Reply to Ping on WAN Interface :	○ Enabled ⊙ Disabled

LAN Interface

IP Address :	169.254.1.1
Subnet Mask :	255.255.255.xxx
DMZ Enable :	○ Enabled ⊙ Disabled
DMZ IP Address :	xxx.xxx.xxx. 52

LAN DHCP Server

DHCP Server Enable/Disable :	⊙ Enabled ○ Disabled
DHCP Server Lease Timeout :	30 Days (Range : 1 — 30)
DHCP Start IP :	xxx.xxx.xxx. 2
Number of IP's to Lease :	50
DNS Server Proxy :	○ Enabled ⊙ Disabled
DNS IP Address :	⊙ Obtain Automatically (From WAN DHCP or PPPoE) ○ Set Manually
Preferred DNS IP Address :	0.0.0.0
Alternate DNS IP Address :	0.0.0.0

Remote Configuration Interface

Interface Enable/Disable :	○ Enabled ⊙ Disabled
Connection Type :	○ DHCP ⊙ Static IP
IP Address :	0.0.0.0
Subnet Mask :	0.0.0.0
Gateway IP Address :	0.0.0.0

NAT Protocol Parameters

ARP Cache Timeout :	20 Minutes (Range : 1 — 30)
TCP Session Garbage Timeout :	120 Minutes (Range : 4 — 1440)
UDP Session Garbage Timeout :	4 Minutes (Range : 1 — 1440)

Save Changes

Reboot

LAN1 I n t e r f a c e : enter in the IP address that will be associated with the Ethernet connection on this module. The default address is 169.254.1.1.

The radio buttons to the right of the IP address field offer the ability to make the LAN either a local or publicly accessible address. If the address is designated a local address it will only be

accessible via the host computer (network) that is connected to the module via the Ethernet cable. If the address is designated a public address it will be accessible network-wide. The default for this feature is for the address to be local. If the IP address is forgotten, the operator will need physical access to the module and will need to create a Stinger "default plug". See steps at the end of this section for creation and use of a default plug.

LAN1 Subnet Mask: enter in an appropriate subnet mask for the module to "talk" on the network. The default value for this parameter is 255.255.255.0

Default Gateway: enter in an appropriate gateway address for the module. The default value for this parameter is 169.254.0.0.

Color Code: enter in a value (0-254). The color code on the subscriber module and the access point module must match in order for registration to occur. Color code is not a security feature. It is a means for the Stinger System operator to segregate an individual network or neighboring Stinger networks. Also, color code can be used to force a subscriber module to only register to a specific access point module even though the subscriber module may be able to see multiple access point modules. The default value for this parameter is 0 on all Stinger modules.

Display-Only Password: enter the same password in both fields for verification. The display-only password, when used, will allow only view activities to the module. When the display-only password is set and not the full-access password, the display-only password will be tied to telnet and FTP sessions to the module. If the full-access password is also set then it has precedence on the telnet and FTP sessions. If the password is forgotten, the operator will need physical access to the module and will need to create a Stinger "default plug" to override the unit. See steps at end of section for use and creation of a default plug.

Full-Access Password: enter the same password in both fields for verification. The full-access password, when used, will allow view and change activities to the module. When the full-access password is set, the password will also be tied to telnet and FTP sessions to the module. When prompted for the password via the web-based interface, there is no username required; however when prompted for the password via a telnet or FTP session, the user that MUST be used is "root". If the password is forgotten, the operator will need physical access to the module and will need to create a Stinger "default plug" to override the unit. See steps at end of this section for use of a default plug.

Webpage Auto Update: enter time period (in seconds) desired to have the web browser refresh the web-based interface. The default setting is 0, which will cause the web-based interface to never refresh.

SM Power Up Mode with No 802.3 Link: choose which mode the module will default to when there is no Ethernet connection sensed by the module. There are two modes available, the first is Alignment mode and the second is Operational mode. See Alignment section for more information. Operational Mode is the default setting.

Bridge Timeout Entry: choose the appropriate bridge timeout for correct network operation with existing network infrastructure.

Authorization Key: each module ships with a unique, pre-programmed authorization key that is to be utilized when an operator configures the Stinger System for DES encryption of the over the air link. The default key is permanently stored on the module.

Site Name: enter information relating to a name given to the physical module. This parameter will

set the supplied information into the sysName SNMP MIB-II object and can be polled by a SNMP management server. The buffer size for this field is 128 characters.

Site Contact: enter contact information relating to the module. This parameter will set the supplied information into the sysContact SNMP MIB-II object and can be polled by a SNMP management server. The buffer size for this field is 128 characters.

Site Location: enter information relating to the physical location of the module. This parameter will set the supplied information into the sysLocation SNMP MIB-II object and can be polled by a SNMP management server. The buffer size for this field is 128 characters.

Save Changes: by clicking on this button, any changes that have been made on the Configuration page will be committed to flash memory and will take effect after the next module reboot.

Undo Save Changes: by clicking on this button, any changes that have been made and not committed through a reboot of the module will be undone.

Set to Factory Defaults: depressing this button will change all of the configurable parameters (all of which are contained on the Configuration page) back to their factory settings.

Reboot: depressing this button will reboot the module.

Stinger Default Plug

When inserted, the default plug brings the module up with a default configuration. This allows the operator to regain control of a module, which may be using an IP address and/or password that has been forgotten. The default plug will also override the passwords for access and change control and set the LAN1 IP address back to 169.254.1.1. This does not, by itself, change any configuration, rather, it allows the operator to attach to the module using the default configuration so that they can read the actual non-default values and set them accordingly.

The following steps outline the creation of a default plug (this plug can also be purchase for a nominal fee at http://www.best-tronics.com/WB Manufacturing):
   · Obtain a RJ-11, 6-pin connector and a small length of CAT 5 cable.
   · Pin-out all 6-pins according the following diagram and then short (i.e. solder) together pins 4 and 6 on the other end. Remaining wires should not be connected to anything.

   The following diagram shows the wiring of a default plug:
   - pin 1 → white / orange
   - pin 2 → white / green
   - pin 3 → white / blue
   - pin 4 → green   solder to orange
   - pin 5 → blue
   - pin 6 → orange   solder to green

   · Insert "default plug" in the GPS sync port of the module and apply power to the module via its Ethernet cable.

When the module is booted up (power applied) it will be in default mode where the IP address will be 169.254.1.1 and the passwords will be blank. All other configurations will have been preserved.

EVENT LOG

This page contains information that is recorded from the subscriber module for troubleshooting purposes. Please make note of the information that is gathered here when calling for technical support.

Clear Event Log: this button will clear the event log.

AP EVAL DATA

The AP Eval Data web page contains information on each of the access point modules that the subscriber module has visibility to. For each access point module that can be seen certain bits of information are shown on this web page. An example of the information shown on this web page for each access point module:

```
Index: 0 Frequency: 0 MHz ESN: 0a-00-3e-00-01-d5
Jitter: 5 RSSI: 1295 Beacon Count: 37
Type: Multipoint Avail: 1 Age: 0 Lockout: 0 RegFail 0 Range: 245 feet TxBER: 1
Session Count: 3 No LUIDS: 0 Out of Range: 0 Rescan Req: 0
FrameNumber: 568 SectorID: 0 Color Code: 0 BeaconVersion: 1 SectorUserCount: 1
PercentDataDwn: 75 PercentDataUpHi: 0 NumDAckSlots: 3 NumContSlots: 3 NumUAckSlots: 3
```

Descriptions of the parameters that can be useful for managing and troubleshooting a Stinger System are:

Index: each access point module that a subscriber module can see is assigned an index value for purposes of this web page only. The index number starts with 0 and increases by 1. This index is used to tell the operator which access point module the subscriber is currently registered to. For example, the first line of text on the web page says "Current entry index: 5", the operator would then scroll down the list of access point modules to the module with "Index: 5" to view information about the link.

Frequency: displays the transmit frequency of the access point module.

ESN: displays the electronic serial number (MAC address) of the access point module.

Jitter: displays the last jitter value captured between the subscriber and access point module.

Range: displays the distance (in feet) between the subscriber and access point module. This parameter will only be valid when observing the data for the access point module that the subscriber is currently registered to.

Session Count: displays the number of times the subscriber module has gone in and out of session with the access point. If this number is particularly large, it typically signifies that there is some sort of issue with the link (i.e. non line of sight, interferers, etc.)

Out of Range: displays a counter for the number of times the access point module has seen a subscriber module who has attempted to register and has been farther away than the max range parameter on the access point.

Sector ID: displays the sector ID of the access point module.

Color Code: displays the color code of the access point module.

Sector User Count: displays the numbers of registered subscriber modules on the access point module.

Rescan APs: click on this button to force the subscriber module to redo the scanning process. The subscriber module will scan, through the frequencies checked on the Configuration web page, for all available access point modules and register to the one that provides the best results for RSSI, Jitter, and number of registered users.

ETHERNET STATS

The Ethernet Stats web page reports TCP throughput and error information for the Ethernet connection of the subscriber module. The following definitions are available:

inoctets count: displays the total number of octets received on the interface, including framing characters.

inucastpkts count: displays the total number of subnetwork-unicast packets delivered to a higher layer protocol

innucastpkts count: displays the total number of non-unicast (i.e. subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher layer protocol.

indiscards count: displays the total number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their be deliverable to higher layer protocol. One possible reason to discard could be to free up buffer space.

inerrors count: displays the total number of inbound packets that contained errors preventing them from being delivered to a higher layer protocol.

inunknownprotos count: displays the total number of packets received via the interface which were discards because of an unknown or unsupported protocol.

outoctets count: displays the total number of octets transmitted out of the interface, including framing characters.

outucastpkts count: displays the total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

outnucastpkts count: displays the total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e. subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.

outdiscards count: displays the total number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

outerrrors count: displays the total number of outbound packets that could not be transmitted because of errors.

RxBabErr: displays the total number of receiver babble errors

EthBusErr: displays the total number of Ethernet bus errors on the Ethernet controller.

CRCError: displays the total number of CRC errors on the Ethernet controller.

RxOverrun: displays the total number of receiver-overrun errors on the Ethernet controller.

Late Collision: displays the total number of late collisions on the Ethernet controller. A normal collision occurs during the first 512 bits of the frame transmission. If a collision occurs after the 512

bit times, then it is considered a late collision. A late collision should be taken as a serious network problem, since it causes the frame being transmitted to be discarded. The most common cause of late collisions is a mismatch between duplex configurations at each end of a link segment.

RetransLimitExp: displays the total number of retransmit limit expirations.

TxUnderrun: displays the total number of transmission-underrun errors on the Ethernet controller.

CarSenseLost: displays the total number of carrier sense lost errors occurred on the Ethernet controller.

EXPANDED STATS

When clicking on the Expanded Stats button and then clicking on one of the standard web page (i.e. Status or Configuration) more fields may be displayed on that page. To go back to the non-Expanded Stats view just have the web browser refresh on the IP address of the module.

Clicking on the Expanded Stats link will display a number of pages of statistics that are maintained by the Stinger module. Stinger Technical Support may ask the operator for specific information in this section when troubleshooting an issue. There are 3 areas in the Expanded Stats that an operator can use for managing and troubleshooting a Stinger System. Those 3 areas are:
- Link Test
- Alignment
- BER Display

Link Test

The Link Test is a test for measuring the throughput and efficiency of the RF link between two Stinger modules.

To perform a link test enter a number into the field labeled "Duration". The duration is the number of seconds the RF link will be tested. Start the link test by clicking the "Start Test" button. The test will now run for the set duration. If the web page is not set to automatically refresh, click the "Refresh Display" button to see the results. For a Stinger System link to be considered acceptable it is necessary for the efficiencies of the link test to be greater than 90% in both the uplink and downlink direction. It is recommended that when a new link is installed that a link test be executed to ensure that the efficiencies are within recommended guidelines.

The key fields are:

- Downlink RATE, bits per second
- Uplink RATE, bits per second
- Downlink Efficiency, percent
- Uplink Efficiency, percent

Alignment

The Alignment web page contains tools to assist in the alignment of a subscriber module to an access point module. There are two modes that can be utilized when aligning a module: 1) RSSI only and 2) normal alignment mode.

RSSI Only is a mode where the module will report the signal strength based on the amount of energy present at a selected frequency. The subscriber module does not have to be registered to an access point module for information on signal strength to be reported back. This can simplify the aiming process for long links when the Stinger passive reflector is being used.

To utilize RSSI only mode:

- Choose the frequency to monitor from the pick list (this would be the same frequency that the access point module is transmitting on)
- Click the radio button to highlight "Enable" on RSSI Only mode
- Click "Enable Aiming Mode"

The module will now report back the level of RF energy present at that specific frequency. To refresh the screen, click the Enable Aiming Mode button as appropriate or configure the web page auto-refresh option.

The normal operation of alignment mode will report information as it relates to the RSSI level, Jitter value, and number of users on the access point module. To utilize normal alignment mode, ensure that the Disabled radio button is checked and then click Enable Aiming Mode button. As with the previous mode to refresh the mode either continue clicking the Enable Aiming Mode button or configure the auto-refresh option. Also, during normal alignment mode the LEDs on the outside of the Stinger module will report back information on the performance of the link. There are 6 LEDs and when in alignment mode the LEDs are turned into a 6-position bar graph. The more LEDs that are lit, the better the RSSI and Jitter values the module is seeing. The colors of the LEDS have no particular meaning other than to assist is distinguishing one position from the next.

The minimum values that are needed for an acceptable link are RSSI this above 700, Jitter that is between 5 and 9, and link efficiencies that are greater than 90% in both the up and down link. If any one of these criteria are not met the link may still be operational but may have issues time to time.

If a Stinger module is placed into Alignment Mode it will automatically drop into Operational Mode after 15 minutes.

BER Display

Bit Error Rate (BER) Display is utilized by the operator to measure the amount bit errors present in a link. BER Display will only work if the access point module is configured to send the BER stream.

IMPORTANT If one access point module in a cluster is set to send a BER stream then all other access point modules in that cluster must be configured in the same fashion.

The field, Measured Bit Error Rate, will display a value that corresponds to the BER at the moment of web browser refresh. An acceptable link will have a BER that is less than 10^{-4}. If the BER is greater than 10^{-4} then the operator needs to evaluate the subscriber and/or access point module

installation for potential issues. To refresh the screen, click the Refresh Display button as appropriate or configure the web page auto-refresh option.

ACCESSORIES

The following accessories are available for use with the Stinger System. To purchase accessories, please contact an authorized Stinger dealer, unless otherwise noted.

- Universal mounting bracket (part numbers M-10 and M-20)

SuperStinger (part number 24-SS)

- Passive reflector dishes (part number RCL-1, 2 and 3)

Classic Stinger (part number S-24)

- 102-132 V AC power supply with North American plug, part number ACPS110
- 100-240 V AC power supply with North American, UK, and Euro plugs, part number ACPSSW-02

SPECIFICATIONS

Operating Frequency Ranges	2.4 Modules: ISM 2.4 to 2.4835 GHz
Access Method	TDD/TDMA
Signaling Rate	10 / 20 Mbps
Modulation Type	High Index 2-level and 4-level Frequency Shift Keying (FSK) (Optimized for interference
Carrier to Interference (C/I) also known as Jitter	3dB nominal
Receiver Sensitivity	-83dBm 10^{-4} BER
Operating Range (All Weather)	Up to 15 miles (24 km) with passive reflector in the 2.4 GHz band.
Transmitter Power	Meets FCC U-NII/ISM and IC LELAN ERP Limit
DC Power measured at DC converter	0.3A @ 24 VDC (7.2 watts) typical
Interface	10/100 BaseT, half/full duplex Rate auto negotiated (802.3 compliant)
Protocols Used by Stinger	IPV4, UDP, TCP, ICMP, Telnet, HTTP, FTP, SNMPv2c, DES
Protocols Supported by Stinger	Switched Layer 2 Transport with support for all common Ethernet protocols including IPV6, NetBIOS, DHCP, IPX, etc.
Software Upgrade Path	Remotely downloaded into FLASH via RF link
Network Management	HTTP, TELNET, FTP, SNMP
Temperature	-40°C to +55°C (-40°F to +131°F)
Dimensions	11.75" H x 3.4" W x 3.4" D (29.9 cm H x 8.6 cm W x 8.6 cm D)
Weight	1 lb. (.45kg)

Hardware Warranty in U.S.