AVCOM
Of Virginia Inc.

# Remote Spectrum Analyzer Protocol

## Models

RSA-1100B
RSA-2150B
RSA-2500B

• Span (MHz) = 320 Samples . RBW (MHz)
(Samples)

Avcom of Virginia
7730 Whitepine Road
Richmond, VA 23237
USA

SBS Protocol rev1
Printed May 2009

# TABLE OF CONTENTS

# 1. INTRODUCTION

The following document describes the protocol used to communicate with the AVCOM spectrum analyzer models RSA-1100B, RSA-2150B and RSA-2500B. If you need to communicate with an older-generation analyzer, contact AVCOM to request the protocol document for that analyzer.

## 2. COMMUNICATION

1. A controlling program (control) can communicate with the spectrum analyzer by ethernet or serial.

   Ethernet:
   - DTR and RTS must be **unasserted.** A serial cable may be plugged into the analyzer during ethernet mode as long as it does not affect DTR and RTS state since DTR and RTS are internally pulled low.

   Serial:
   - DTR unasserted
   - **RTS asserted**

2. Serial port settings: If communicating with the analyzer via serial port, the PC communicating with the analyzer must set the serial port DTR and RTS lines according to the mode described in step 1 above and send data at 115200 bits per second, 8 data bits, no parity, 1 stop bit, no flow control.

3. Ethernet addressing: The factory default IP address is 192.168.118.242 and port is 26482. If you need to change either parameter, AVCOM has developed an application called ConfigTool that can assist in setting up the ethernet controller. The ConfigTool is located on the main GUI menu under "Configure>Ethernet Connection".
   The ethernet controller converts the data from ethernet to RS232. The output baud rate setting is critical to communications.
   All RSA models with –SBS or –CLM option require 230400 baud.
   All RSA models without –SBS or –CLM option require 115200 baud.

4. Begin communication by sending a Get Hardware Description request to discover basic information about the analyzer such as Product ID (see Table 1), firmware revision, current Center Frequency, Span, etc. Once that packet is received the control can assume the settings of the analyzer. If the firmware revision is 2.6 or greater, then the control needs to determine any internal LNB Power options that are available by sending a Get LNB Power Description request.

*Table 1:* **Product ID for SBS models**

| Model | Product ID |
|---|---|
| RSA-2150 | 0x3A |
| RSA-1100 | 0x4A |
| RSA-2500 | 0x5A |
| RCTV-5000 | 0x5A |

*Table 2:* **PCB Revision**

| Model | Valid Products | Hardware Limits (based on PCB Revision byte) | PCB Revision | | | | |
|---|---|---|---|---|---|---|---|
| | | | A | B | C | D | E |
| FAB-08D02 | RSA-2150 | Band 1: 930MHz – 2500MHz | 0x41<br>0x0A | 0x42<br>0x0B | 0x43<br>0x0C | | |
| FAB-08H01 | RSA-1100<br>RSA-2150<br>RSA-2500 | Band 1: 5MHz – 1300MHz<br>Band 2: 930MHz – 2500MHz | 0x1A | 0x1B | 0x1C | | |
| FAB-09D09 | RCTV-5000 | Band 1: 5MHz – 1300MHz<br>Band 2: 750MHz – 2300MHz | 0x2A | 0x2B | 0x2C | | |

0x2D

Example:

*Control sends a "Get HW Description" packet [0x02, 0x00, 0x03, 0x07, 0x00, 0x03]*

*The spectrum analyzer will respond with a "Hardware Description packet", described later in this document, which contains Product ID, firmware revision, current setting, available RF Inputs, and other information about the analyzer hardware.*

*If the firmware revision is 2.6 or greater then Control sends "Get LNB Power Description" packet [0x02, 0x00, 0x02, 0x0D, 0x03]*

*Using the "LNB Power Description" packet the control discovers which RF Inputs (if any) have internal LNB Power and how they are used..*

*Request a Waveform Packet and interpret it according to the firmware revision discovered in the HW description packet.*

*Send a Changes Settings command according to the firmware revision discovered in the HW description packet.*

5. Notes about Data Packets:
   - All data packets start with a packet header consisting of
     - Start Transmission (STX = 0x02) byte
     - Two Length bytes whose value **does not include the STX and Length bytes**
     - Packet Type byte
   - All data packets end with End Transmission (ETX = 0x03) byte
   - A Waveform packet is either 341 bytes (firmware revision < 1.9) or 344 (firmware revision => 1.9) bytes in length. The first 320 bytes of data (starting after the header) are unsigned 8-bit waveform data and is converted to power by the waveform scaling described in the Waveform Packet table. The remaining bytes will tell the control the "current" state of center frequency, span, reference level, etc. The control can assume the settings of the analyzer or set its own.
   - The control must send a "waveform request" each time it wants to view a waveform. The control should wait for the analyzer to respond before sending another waveform request.

# 3. COMMAND AND RESPONSE PACKETS

→ Indicates direction of data flow

*Table 3:* **List of Data Types**

| Data Type | Packet Type Description | Direction | Notes: |
|---|---|---|---|
| 0x03 | Waveform Request | GUI → SBS | Responds with 0x09 type |
| 0x04 | Change Control Settings | GUI → SBS | |
| 0x07 | Hardware Description | GUI ↔ SBS | |
| 0x08 | Unknown Command | SBS → GUI | Used in debugging |
| 0x09 | 8-bit Waveform | SBS → GUI | |
| 0x0D 13 | LNB Power Description | GUI ↔ SBS | Firmware v2.6 and higher required |
| 0x0F 15 | 12-bit Waveform | SBS → GUI | Firmware v2.10 and higher required |
| 0x60 96 | Error Message | SBS → GUI | |

*Table 4:* **Get HW Description** **GUI → SBS**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x0003 |
| 3 | Type | 0x07 |
| 4 | Padding | 0x00 |
| 5 | End | ETX |

Get HW Description is recommended to be performed first to determine what GUI control options can be presented for normal running.

*Table 5:* **Get LNB Power Desc (Firmware Rev => 2.6)** **GUI → SBS**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x0002 |
| 3 | Type | 0x0D |
| 4 | End | ETX |

SBS replies with "LNB Power Desc" (Firmware Rev >= 2.6)

*Table 6:* **Waveform Transmission Settings** **GUI → SBS**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x0003 |
| 3 | Type | 0x03 |
| 4 | Send normal waveform | 0x00 = Stop stream - implemented for Stream AM<br>0x01 = StreamOn (not implemented),<br>0x03 = Send Single 8-bit resolution<br>0x04 = Stream AM waveform data only (not yet implemented)<br>0x05 = Send Single 12-bit resolution (Firmware Rev >= v2.10) |
| 5 | End | ETX |

*Table 7:* **HW Description Packet:** **SBS → GUI**

| Byte | Description | Value (or Range) |
|---|---|---|
| 0 | STX | BYTE |
| 1-2 | Length MSB-LSB = 0x0055 | WORD |
| 3 | Type = 0x07 | BYTE |
| 4 | Product ID – See Table 1 | BYTE |
| 5 | FW version Major | BYTE |
| 6 | FW version Minor | BYTE |
| 7 | Stream Mode (Single, Stream, OFF) | BYTE |
| 8-11 | Current Center Frequency | DWORD |
| 12-15 | Current Span | DWORD |
| 16 | Current Reference Level | BYTE |
| 17 | Current RBW | BYTE |
| 18 | Available RBW | BYTE |
| 19 | Current RF Input (10d – 15d for inputs 1 through 6) | BYTE |
| 20 | Available RF Inputs (10d – 15d for inputs 1 through 6) | BYTE |
| 21 | Current Splitter Gain Cal | BYTE |
| 22 | Bit Sets:<br>b0 = 1: Has Splitter<br>b1 = 0: Do not use<br>b2 = 1: Has 60dB range<br>b3 = 1: PSA-SBS model<br>b4 = 1: MSA-SBS model | BYTE |
| 23 | Current Com Port | BYTE |
| 24 | Available Com Ports | BYTE |
| 25-26 | Current Internal Extender Freq MSB-LSB | WORD |
| 27-28 | Current External Extender MSB-LSB | WORD |
| 29-44 | Serial Number[16 bytes] | BYTES[16] |
| 45 | PCB Revision | BYTE |
| 46 | Cal Day (+10deci) | BYTE |
| 47 | Cal Month (+10deci) | BYTE |
| 48-49 | Cal Year MSB-LSB | WORD |
| 50 | Board Temperature (nom 0x80 = 0degC) | BYTE |
| 51 | Board Temperature MIN (nom 0x80 = 0degC) | BYTE |
| 52 | Board Temperature MAX (nom 0x80 = 0degC) | BYTE |
| 53 | Reserved | BYTE |
| 54 | Has LNB Power<br>(Firmware Rev >= v1.9)<br>0b0000 0000 = No LNB Power<br>0b0000 0001 = has LNB Power<br>(Firmware Rev >= v2.6)<br>0b0000 0011 = input1 has LNB Power<br>0b0100 0001 = input6 has LNB Power<br>0b0111 1111 = All inputs have LNB Power | BYTE |

Table continued on next page

*Table 7 (continued*

| | | |
|---|---|---|
| 55 | Current LNB Power Settings Bits (See Table 14)<br>(Firmware Rev >= v1.9) | BYTE |
| 56 | Is First Run (save Flag) | BYTE check ? |
| 57 | Is Locked (0xAA = is Locked) | BYTE |
| 58 | **Project ID – firmware ignores values 0x00, 0x02, or 0xFF.**<br>(Firmware Rev >= v2.10) | BYTE |
| 59 | (Firmware Rev <= 2.13) Reserved<br>(Firmware Rev >= 2.14) -70dB RL availability<br>Bit[7] = always '1'<br>Bit[6] = don't care<br>Bits[5-0] = RF inputs 6-1 (1=Enabled, 0=Disabled)<br>If set then that RF Input Reference Level can go to -70dB | BYTE |
| 60-86 | These bytes are for engineering use only | BYTE |
| 87 | ETX | BYTE |

*Table 8:* **LNB Power Description (Firmware Rev => 2.6)  SBS → GUI**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x002D (45d) |
| 3 | Type | 0x0D |
| 4 | RF LO Offset Mask<br>bit 5 – bit 0 for RF Inputs 6-1<br>1=always use Low Band offset<br>0=Use LNBP Mask to determine offset<br>b7 = 1 always | BYTE |
| 5 | LNBP Mask<br>bit 5 – bit 0 for RF Inputs 6-1<br>1 = uses voltage to select band<br>0 = uses 22kHz to select band<br>b7 = 1 always | BYTE |
| 6 | RF Input block power<br>0x00 – 0x06 (sent + 10d) | BYTE |
| 7-8 | RF1: Int Ext Offset 1; 13V/22kHz OFF | Low Band: Signed word - MSB-LSB |
| 9-10 | RF1: Int Ext Offset 2; 18V/22kHz ON | High Band: Signed word - MSB-LSB |
| 11-12 | RF2: Int Ext Offset 1; 13V/22kHz OFF | Low Band: Signed word - MSB-LSB |
| 13-14 | RF2: Int Ext Offset 2; 18V/22kHz ON | High Band: Signed word - MSB-LSB |
| 15-16 | RF3: Int Ext Offset 1; 13V/22kHz OFF | Low Band: Signed word - MSB-LSB |
| 17-18 | RF3: Int Ext Offset 2; 18V/22kHz ON | High Band: Signed word - MSB-LSB |
| 19-20 | RF4: Int Ext Offset 1; 13V/22kHz OFF | Low Band: Signed word - MSB-LSB |
| 21-22 | RF4: Int Ext Offset 2; 18V/22kHz ON | High Band: Signed word - MSB-LSB |
| 23-24 | RF5: Int Ext Offset 1; 13V/22kHz OFF | Low Band: Signed word - MSB-LSB |
| 25-26 | RF5: Int Ext Offset 2; 18V/22kHz ON | High Band: Signed word - MSB-LSB |
| 27-28 | RF6: Int Ext Offset 1; 13V/22kHz OFF | Low Band: Signed word - MSB-LSB |
| 29-30 | RF6: Int Ext Offset 2; 18V/22kHz ON | High Band: Signed word - MSB-LSB |
| 31 | RF1: LNBP state | BYTE – See Table 14 |
| 32 | RF2: LNBP state | BYTE – See Table 14 |
| 33 | RF3: LNBP state | BYTE – See Table 14 |
| 34 | RF4: LNBP state | BYTE – See Table 14 |
| 35 | RF5: LNBP state | BYTE – See Table 14 |
| 36 | RF6: LNBP state | BYTE – See Table 14 |
| 37-46 | Reserved | |
| 47 | End | ETX |

*Table 9:* **8-bit Waveform Packet (Firmware Rev => v1.9)** **SBS → GUI**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x0155 |
| 3 | Type | 0x09 |
| 4-323 | Waveform data –<br>320 8-bit points cover span range centered on CF.<br>Scale to dB power values using → | Normal Waveform scaling: dB = +0.20 * X + b<br>Where RL = -10dB: b = -50<br>-30dB: b = -70<br>-50dB: b = -90<br>-70dB: b = -110 |
| 324 | Product ID | See Table 1 |
| 325-328 | CF (4 bytes) | RX Value /10000 = MHz (resolution 0.1kHz) |
| 329-332 | Span (4 bytes) (Span = Stop – Start) | RX Value /10000 = MHz (resolution 0.1kHz) |
| 333 | Ref Level | -10 = 10d, -30 = 30d, -50 = 50d |
| 334 | RBW | ~~3MHz = 0x80~~, 1MHz = 0x40, 300kHz = 0x20, 100kHz = 0x10, 10kHz = 0x08, ~~3kHz = 0x04~~ |
| 335 | Input Connector (1 byte) | 10d – 15d for inputs 1 through 6 respectively |
| 336-337 | Internal Extender MSB-LSB | Signed word |
| 338-339 | External Extender MSB-LSB | Signed word |
| 340 | LNB Power for current RF Input only (See Table 14) | BYTE |
| 341 | reserved | BYTE |
| 342 | reserved | BYTE |
| 343 | End | ETX |

*Table 10:* **8-bit Waveform Packet (Firmware Rev < v1.9)** **SBS → GUI**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x0152 |
| 3 | Type | 0x09 |
| 4-323 | Waveform data –<br>320 8-bit points cover span range centered on CF.<br>Scale to dB power values using → | Normal Waveform scaling: dB = +0.20 * X + b<br>Where RL = -10dB: b = -50<br>-30dB: b = -70<br>-50dB: b = -90<br>-70dB: b = -110 |
| 324 | Product ID | 0x3A for SBS-2150 |
| 325-328 | CF (4 bytes) | RX Value /10000 = MHz (resolution 0.1kHz) |
| 329-332 | Span (4 bytes) (Span = Stop – Start) | RX Value /10000 = MHz (resolution 0.1kHz) |
| 333 | Ref Level | -10 = 10d, -30 = 30d, -50 = 50d |
| 334 | RBW | 3MHz = 0x80, 1MHz = 0x40, 300kHz = 0x20, 100kHz = 0x10, 10kHz = 0x08, 3kHz = 0x04 |
| 335 | Input Connector (1 byte) | 10d – 15d for inputs 1 through 6 respectively |
| 336-337 | Internal Extender MSB-LSB | Signed word |
| 338-339 | External Extender MSB-LSB | Signed word |
| 340 | End | ETX |

*Table 11:* **12-Bit Waveform Packet (Firmware Rev => v2.10) SBS → GUI**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x01F5 |
| 3 | Type | 0x0F |
| 4-483 | 12-bit Waveform data cover span range centered on CF. Each set of 3 nibbles is a data point. Nibbles 1 and 2 are the integer value. The 3rd nibble value divided by 16 is the fractional value added to the integer. The sum is used in the waveform scaling as normal. Scale to dB power values using → | Normal Waveform scaling: dB = +0.20 * X + b<br>Where RL = -10dB: b = -50<br>-30dB: b = -70<br>-50dB: b = -90<br>-70dB: b = -110 |
| 484 | Product ID | See Table 1 |
| 485-488 | CF (4 bytes) | RX Value /10000 = MHz (resolution 0.1kHz) |
| 489-492 | Span (4 bytes) (Span = Stop – Start) | RX Value /10000 = MHz (resolution 0.1kHz) |
| 493 | Ref Level | -10 = 10d, -30 = 30d, -50 = 50d |
| 494 | RBW | 3MHz = 0x80, 1MHz = 0x40, 300kHz = 0x20, 100kHz = 0x10, 10kHz = 0x08, 3kHz = 0x04 |
| 495 | Input Connector (1 byte) | 10d – 15d for inputs 1 through 6 respectively |
| 496-497 | Internal Extender MSB-LSB | Signed word |
| 498-499 | External Extender MSB-LSB | Signed word |
| 500 | LNB Power for current RF Input only (See Table 14) | BYTE |
| 501 | reserved | BYTE |
| 502 | reserved | BYTE |
| 503 | End | ETX |

*Table 12:* **Change Settings (Firmware Rev => v1.9)** **GUI → SBS**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x0010 |
| 3 | Type | 0x04 |
| 4-17 | Settings (Firmware Rev >= 2.6, LNB changes for current input only) | CF-CF-CF-CF-SP-SP-SP-SP-RL-RBW-RF input-LNB-reserved-reserved |
| 18 | End | ETX |

Note: No reply to Change Settings command

CF bytes sent = CF(MHz) * 10,000. Maximum & minimum CF value based on model.

Span bytes sent = Span(MHz) * 10,000 Span range is 0.000-1300.000 MHz

Reference Level (RL)

(Firmware Rev <= 2.13)

RL = Integer values between 10d and 50d correspond to reference levels between -10dBm and -50dBm.

(Firmware Rev >= 2.14)

RL = Integer value between 10d and 70d correspond to reference levels between -10dBm and -70dBm.

-51 to -70dBm depends on preamp availability bits (Table 7, byte 59, Hardware Description packet).

RBW byte sent = 3MHz = 0x80, 1MHz = 0x40, 300kHz = 0x20,

100kHz = 0x10, 10kHz = 0x08, 3kHz = 0x04

RF Input sent = 10d + RF Input (RF Input numbering starts at zero, so input 1 is 10d.)

**LNB = See Table 14.**

*Table 13:* **Change Settings (Firmware Rev < 1.9)** **GUI → SBS**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x000D |
| 3 | Type | 0x04 |
| 4-14 | Settings | CF-CF-CF-CF-SP-SP-SP-SP-RL-RBW-RF input |
| 15 | End | ETX |

*Table 14:* **LNB Power Bits**

| Name | Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 | Function |
|---|---|---|---|---|---|---|---|---|---|
| | | | TEN | | VSEL | EN | | | |
| Vout | 0 | 1 | x | 0 | **0** | 1 | 0 | 0 | Vout = 13V |
| | 0 | 1 | x | 0 | **1** | 1 | 0 | 0 | Vout = 18V |
| 22kHz | 0 | 1 | **0** | 0 | x | 1 | 0 | 0 | 22kHz OFF |
| | 0 | 1 | **1** | 0 | x | 1 | 0 | 0 | 22kHz ON |
| Power | 0 | 1 | 0 | 0 | 0 | **0** | 0 | 0 | Disable Power |

*Table 15:* **Unknown Command (for debugging)** **SBS → GUI**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x0003 |
| 3 | Type | 0x08 |
| 4 | Type (requested by GUI) | Type byte that was in the unknown command sent by the GUI |
| 5 | End | ETX |

*Table 16:* **Error Message** **SBS-→ GUI**

| Byte # | Description | Value (or range) |
|---|---|---|
| 0 | Start of Packet | STX |
| 1-2 | Length | 0x00xx |
| 3 | Type | 0x60 |
| xx – xx | Error Message | |
| xx | End | ETX |