USER MANUAL
VAMPIRE
DATA RECORDER AND ANOMALY DETECTION

PART NUMBER:
NW-1553-ML-VA01

NuWaves RF Solutions

NuWaves RF Solutions
132 Edison Drive
Middletown, Ohio 45044
Tel: 513-360-0800
www.nuwaves.com
sales@nuwaves.com

Table of Contents

Table of Figures

Table of Tables

1 VAMPIRE OVERVIEW

The purpose of Vampire is to capture MIL-STD-1553 bus traffic. It performs this function in 2 ways: streaming the bus content to an internal SD card for post processing of the data and sending the decoded data out of the device over the Ethernet connection.

The Vampire hardware, shown in Figure 1, decodes the bus controller (BC) / remote terminal (RT) interaction and transmits the information over the Ethernet connection. For efficiency, one Ethernet packet is transmitted from Vampire for every eight MIL-STD-1553 BC/RT interactions. Vampire also creates high precision timestamps for the BC and RT traffic. Each BC message has a timestamp resolution of 5 nanoseconds (ns) which is 4x the industry standard. The RT response also has a resolution of 5 ns which is 20x the industry standard. To protect the avionics busses, Vampire performs as a one-way device. Vampire is not capable of transmitting MIL-STD-1553 packets and is unable to receive Ethernet data.

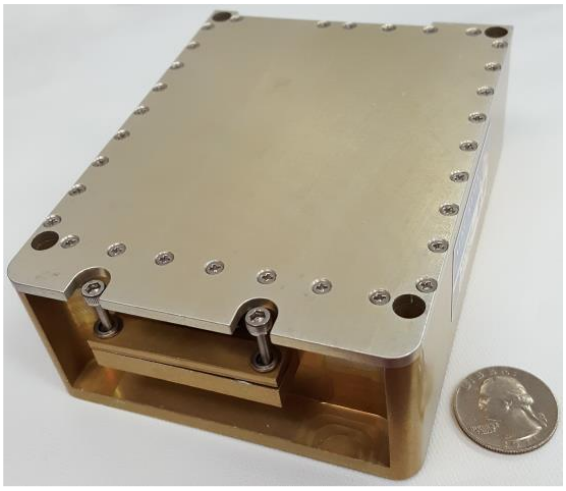


Figure 1: Vampire offers a ruggedized design in a favorable package size.

2 SETTING UP VAMPIRE

2.1 INTERFACE DEFINITIONS

The connector pin-out definitions for the module's connector are provided in Table 1. In a typical installation, the Vampire module is mated to a MIL-STD-1553 data bus and power supply via an interface cable.

Table 1: Vampire Pin-Out Definitions

Pin Number	Pin Name	I/O	Description
1	+28 VDC	I	DC Supply Voltage, +28 Volts.
2	28 VDC Ret	I	DC Supply Voltage Return
3	USB D-	I/O	USB Data (Negative)
4	USB D+	I/O	USB Data (Positive)
5	USB VCC	I	USB Voltage
6, 8, 16, 19, 21, 23, 24, 25, 27, 29	GND	I	DC Ground.
7	BI_DD-	I/O	Ethernet, Bidirectional Data Bus D (Negative)
9	BI_DD+	I/O	Ethernet, Bidirectional Data Bus D (Positive)
10	BI_DC-	I/O	Ethernet, Bidirectional Data Bus C (Negative)
11	BI_DC+	I/O	Ethernet, Bidirectional Data Bus C (Positive)
12	BI_DA+	I/O	Ethernet, Bidirectional Data Bus A (Positive)
13	BI_DA-	I/O	Ethernet, Bidirectional Data Bus A (Negative)
14	BI_DB-	I/O	Ethernet, Bidirectional Data Bus B (Negative)
15	BI_DB+	I/O	Ethernet, Bidirectional Data Bus B (Positive)
17	CH1_H	I/O	MIL-STD 1553 Channel 1 (Positive)
18	CH1_L	I/O	MIL-STD 1553 Channel 1 (Negative)
20	CH2_L	I/O	MIL-STD 1553 Channel 2 (Negative)
22	CH2_H	I/O	MIL-STD 1553 Channel 2 (Positive)
26	CH3_L	I/O	MIL-STD 1553 Channel 3 (Negative)
28	CH3_H	I/O	MIL-STD 1553 Channel 3 (Positive)
30	CH4_L	I/O	MIL-STD 1553 Channel 4 (Negative)
31	CH4_H	I/O	MIL-STD 1553 Channel 4 (Positive)

2.2 INTERFACE CABLE (PURCHASE OPTION)

The 36” shielded interface cable is comprised of a micro-D connector on one end, with four MIL-STD-1553 connectors, one power connector, ethernet, and USB-A for interfacing with the user’s implementation. This cable provides input power to the Vampire module and allows interfacing with the MIL-STD-1553 data bus. Figure 2 shows NuWaves part number CYB-CBL-01-F.

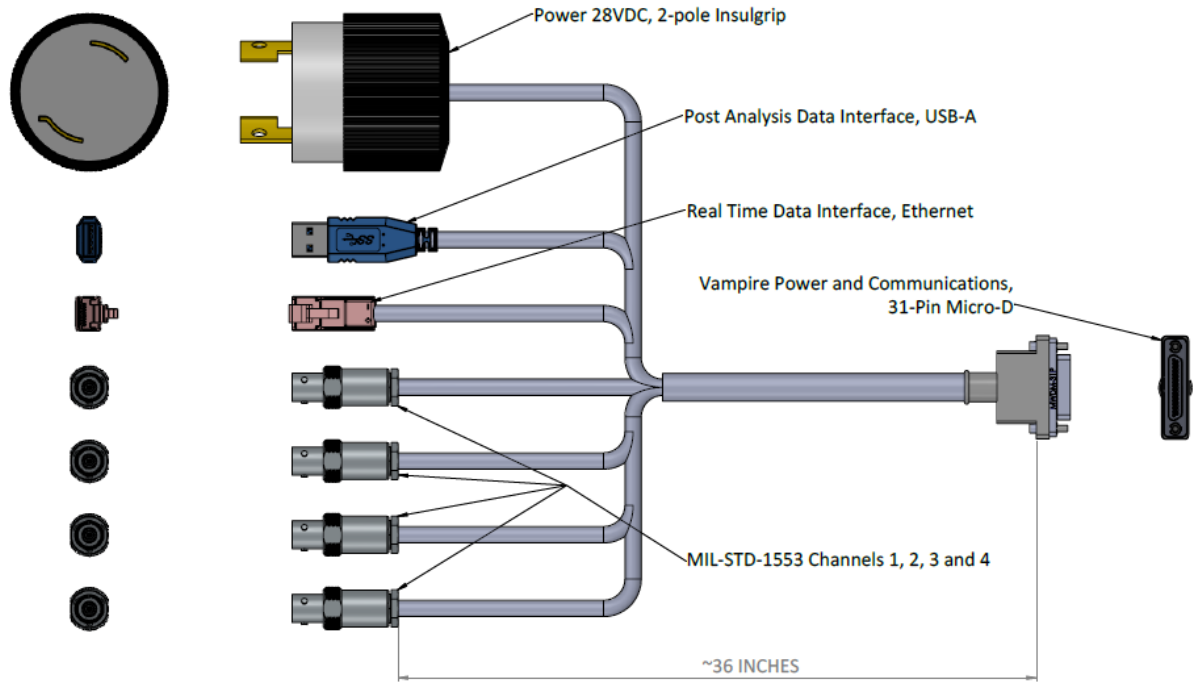


Figure 2: CYB-CBL-01-F Vampire Interface Cable

2.3 POWER CONNECTION

The nominal operating voltage of Vampire is 28V DC, but it is capable of handling 10V to 36V DC. The power is supplied to the device through the miniature sub-d connector. The current draw of Vampire is approximately 300 mA, but is dependent on the number of busses being connected to the device and the traffic loading on the busses.

2.4 MIL-STD-1553 BUS CONNECTIONS

Figure 3 illustrates how Vampire can be connected to four MIL-STD-1553 channels. The four channels may be any combination of an “A” or “B” bus. The bus traffic on all four channels is decoded and sent out of the module over the Ethernet connection. However, only the traffic on CH1 and CH2 is written to the SD card.

The MIL-STD-1553 connections on the end of the Vampire interface cable are Trompeter CJ70-29.

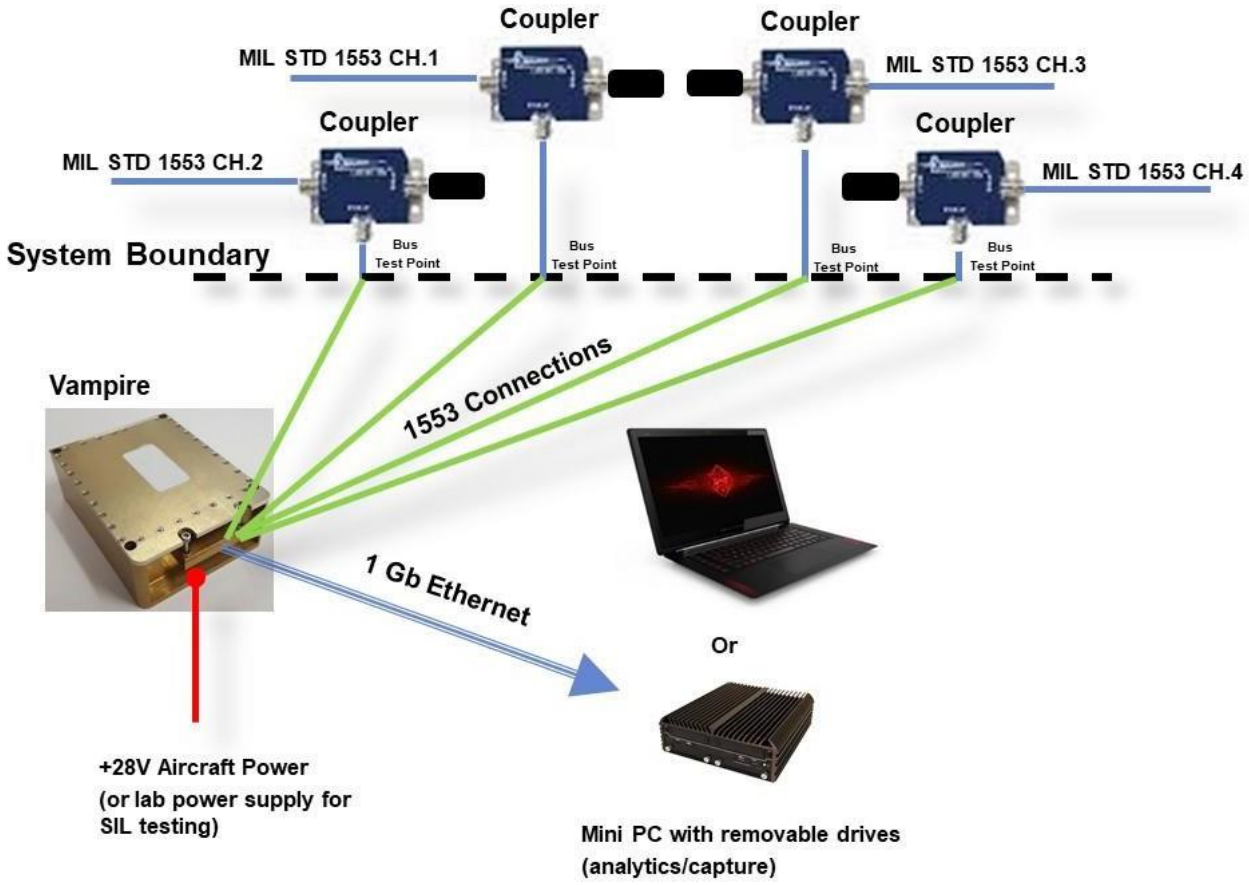


Figure 3: Example implementation of Vampire to four MIL-STD-1553 channels

2.5 LED CONFIGURATION

Vampire has 5 tri-color light emitting diodes (LED) internal to the module as seen in Figure 5. These LEDs can be viewed by removing the back cover via the thumb screws. The color of the LEDs indicates the status of the system as see the Table 2.

Table 2: LED Color Matrix

	D32	D31	D30	D29	D28
Blue (solid)	CH1 & 2 Active	CH3 & 4 Active	NA	NA	NA
Green (solid)	NA	NA	Power up successful	NA	NA
Red (solid)	SD card inserted, no bus activity	SD card inserted, no bus activity	NA	NA	Ethernet Active (100 Mbps)
Purple (flashing)	Recording to SD card	Recording to SD card	NA	NA	NA
Yellow/Orange (solid)	NA	NA	NA	NA	Ethernet Active (1Gbps)
Off	No bus activity, no SD card	No bus activity, no SD card	No unit power	NA	No Ethernet

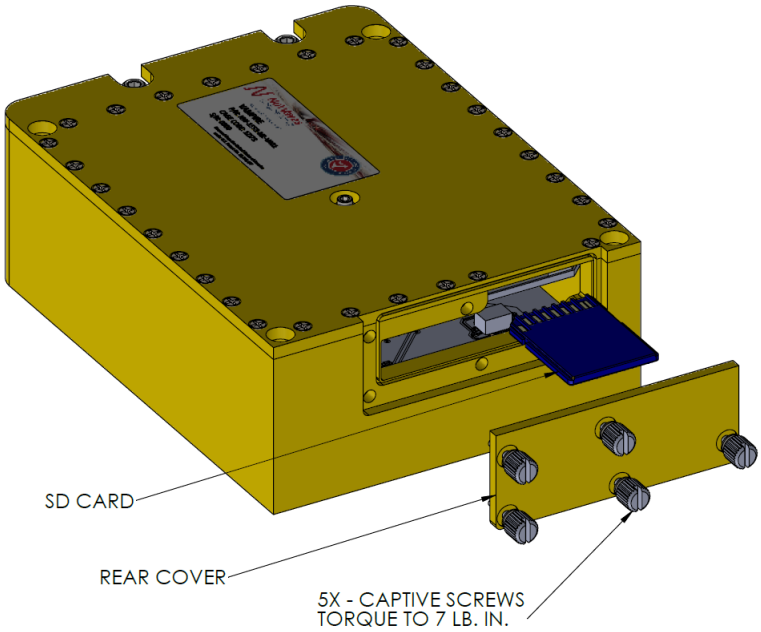


Figure 4: Rear Access Panel

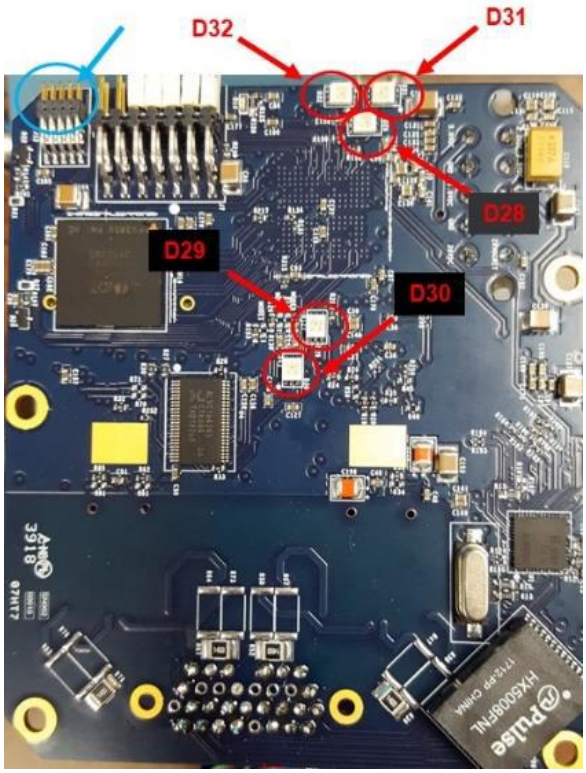


Figure 5: Board level indicators and configuration jumpers

2.6 SD CARD RECORDING AND DATA CAPTURE

If the SD Card is unlocked, Vampire begins recording all 4 input channels ~20 seconds after power up. Vampire will continue to record to the SD Card until the card is full. Once the card is full, Vampire will stop recording. The SD Cards are hot swappable. In other words, they can be removed or inserted at any time while the device is powered. If an unlocked SD Card is inserted while Vampire is powered up, it will complete an initialization sequence and then start recording from the beginning of the SD Card.

Vampire uses MIL-STD-1553 bus transceivers to convert each MIL-STD-1553 channel into 2 digital signals. This is a standard MIL-STD-1553 architecture. Vampire captures both digital signals from each of the 4 channels at 10 MHz and continuously records the data to the SD Card.

The SD Card can be a standard size SD memory card or a micro SD card (as long as it is in a standard size SD card carrier). **The memory card also needs to be a minimum of class 10, UHS1 [3] and type XC.** A 256 GB SD card will hold approximately 10 hours of recorded data.

2.7 SETTING THE IP ADDRESS

The jumper pins behind the back cover are used to set the IP address of Vampire. The location of the pins is circled in blue in Figure 5. There are currently 2 hardware versions of Vampire: one has a dual row of 10 pins with a spacing of 0.05 inches, and the other has a dual row of 8 pins with a spacing of 0.1 inches. The method of setting the address is dependent on the version of the hardware (see 3 and 4 below). The orientation of the pins in the tables are looking at the pins with the cover removed.

Table 3: IP Configuration 0.05 Jumpers

IP address	1	2	3	4	5
183					
184	■				
185		■			
186			■		
			■		
187				■	
				■	
188					■
					■

Table 4: IP Configuration 0.1 Jumpers

IP address	1	2	3	4
183	X			
	X			
184	X	■		
	X	■		
185	X		■	
	X		■	
186	X	■	■	
	X	■	■	
187	X			■
	X			■
188	X	■		■
	X	■		■
189	X		■	■
	X		■	■
190	X	■	■	■
	x	■	■	■

2.8 ETHERNET

Once powered on and Vampire sees MIL-STD-1553 traffic, the Ethernet port automatically sends out broadcast packets. The packets are UDP packets sent from IP address 169.254.115.183. The packets can be captured for post processing using Wireshark software on a PC, or they can be captured and analyzed in real time with software such as RYWA's Cyber-physical Intrusion Detection Software (CIDS). The format of the UDP packets can be seen in the Appendix, Table 7.

The Ethernet connection on the end of the Vampire interface cable is an L-Com TRD815SPL-7.

3 DATA ANALYSIS

This section provides an overview of the AFRL/RYWA software tools available for analyzing the data captured by Vampire either on the SD Card or over the Ethernet output. It is not meant to be a complete user guide for the tools. Because the Ethernet output is not proprietary, it makes Vampire a great front-end tool for other researchers to develop their own analysis system using Vampire's output.

3.1 POST FORENSICS ANALYSIS OF CAPTURED DATA FROM VAMPIRE'S ETHERNET OUTPUT

AFRL/RYWA has created a software program named Day-Walker (see Figure 6) for performing post forensics analysis of the captured Ethernet traffic from Vampire. By opening the pcap file saved by Wireshark, Day-Walker can: generate a report of the bus traffic (see example in Appendix 8.4), show the frequency of the RTs being called by the BC, show the available sub addresses of the RTs, plot the response times of the RTs, plot individual word values over time and convert the pcap file to a comma delimited file.

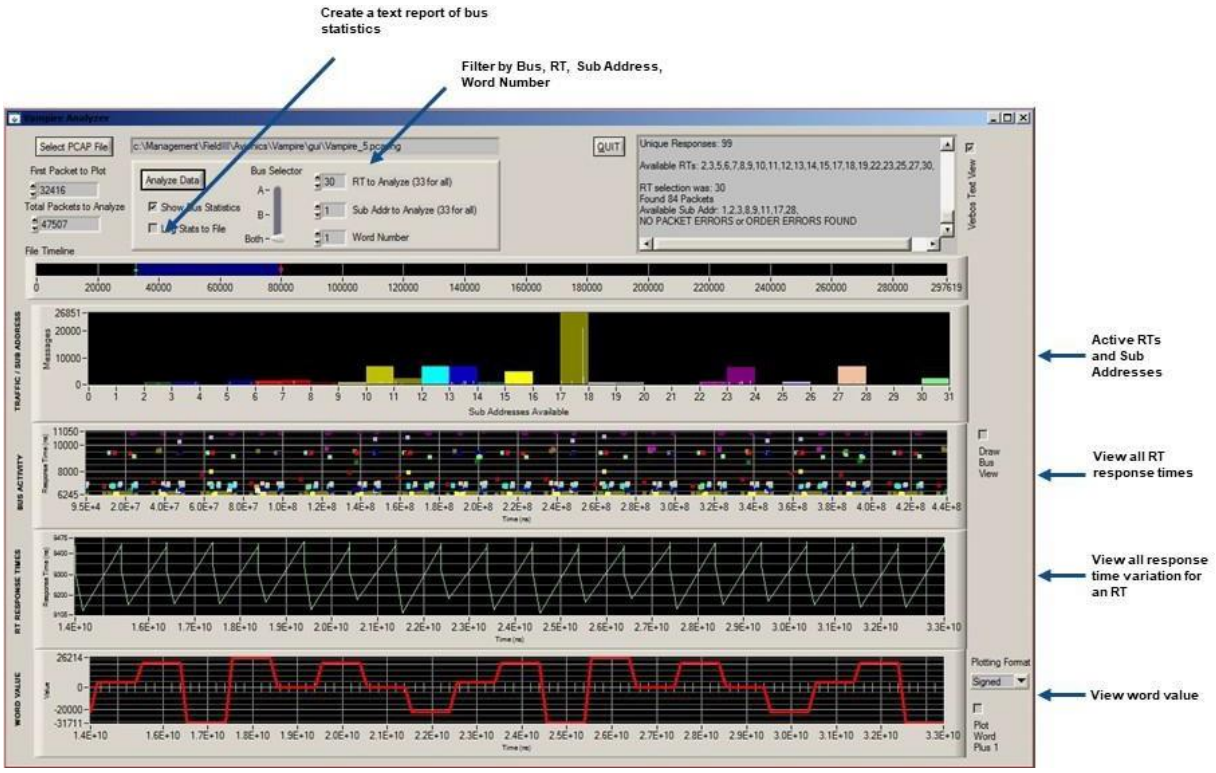


Figure 6: Post forensics data analysis using Day-Walker

3.2 REAL TIME BUS ANALYSIS USING VAMPIRE

AFRL has created a software program called CIDS which parses the incoming UDP packets for visualization and anomaly detection. The software has several levels of analysis which can be performed on the real-time Ethernet data. Several screens are shown in the following figures.

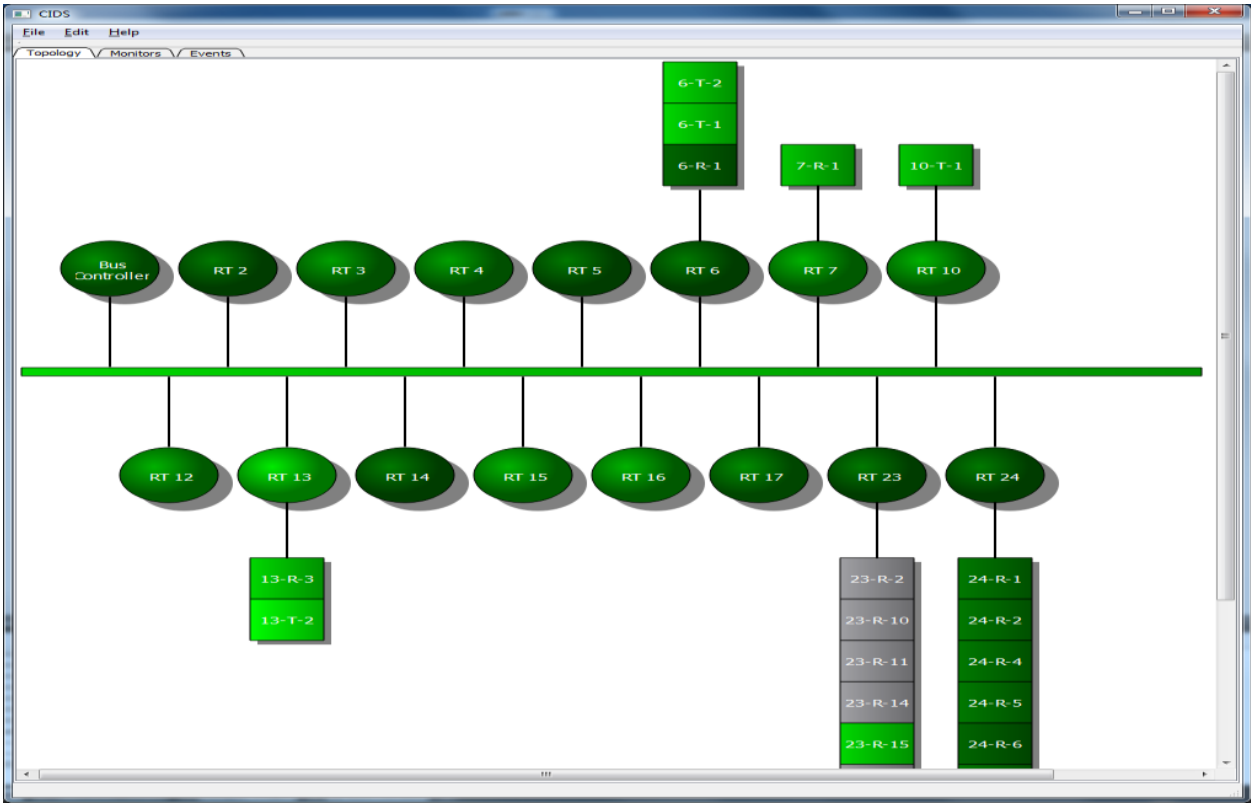


Figure 7: Visualizing the MIL-STD-1553 bus in real time with CIDS

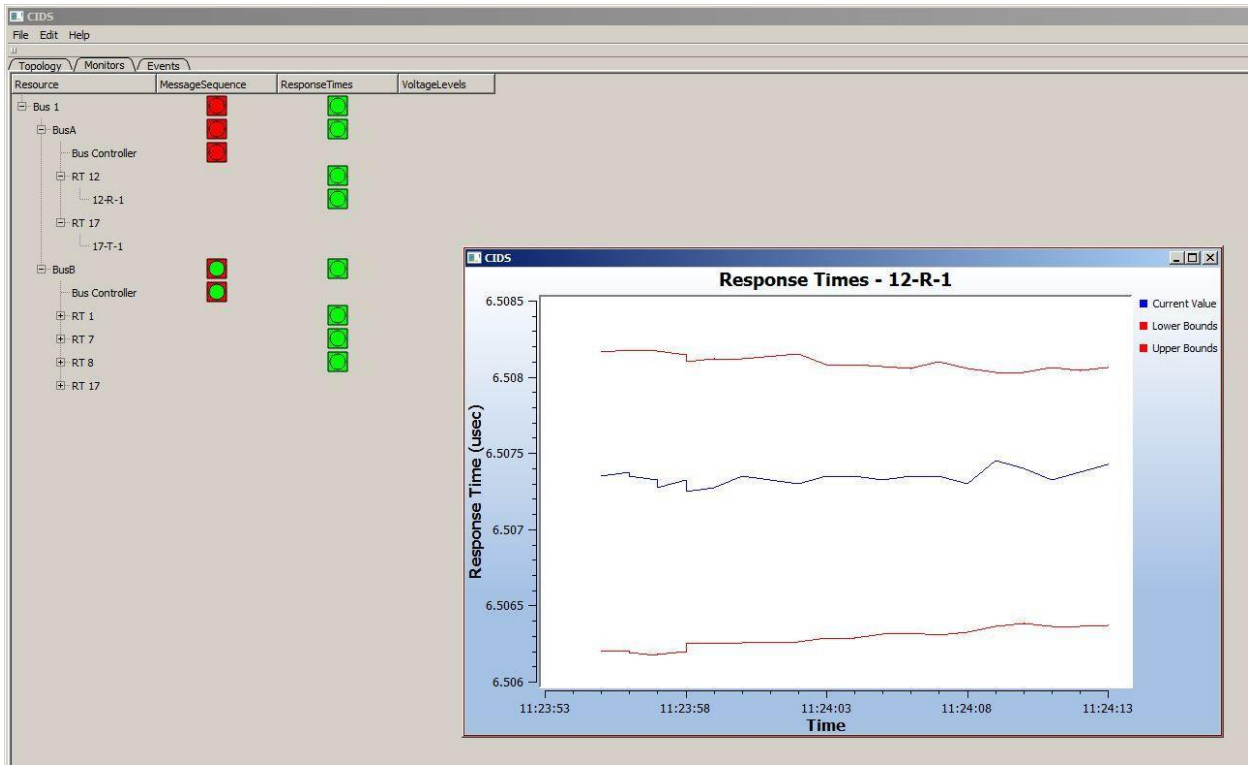


Figure 8: Anomaly detection using RT response times with CIDS

Figure 9: Bus errors as tracked by CIDS

3.3 ANALYSIS OF DATA CAPTURED ON THE SD CARD

The data on the SD Card can be analyzed with AFRL/RYWA's Sandstorm software. Sandstorm helps the end user to visually inspect the MIL-STD-1553 bus. Because the raw traffic is recorded to the SD Card instead of decoded traffic, problems on the bus can be analyzed in-depth. Figure 10 shows a screen capture Sandstorm.

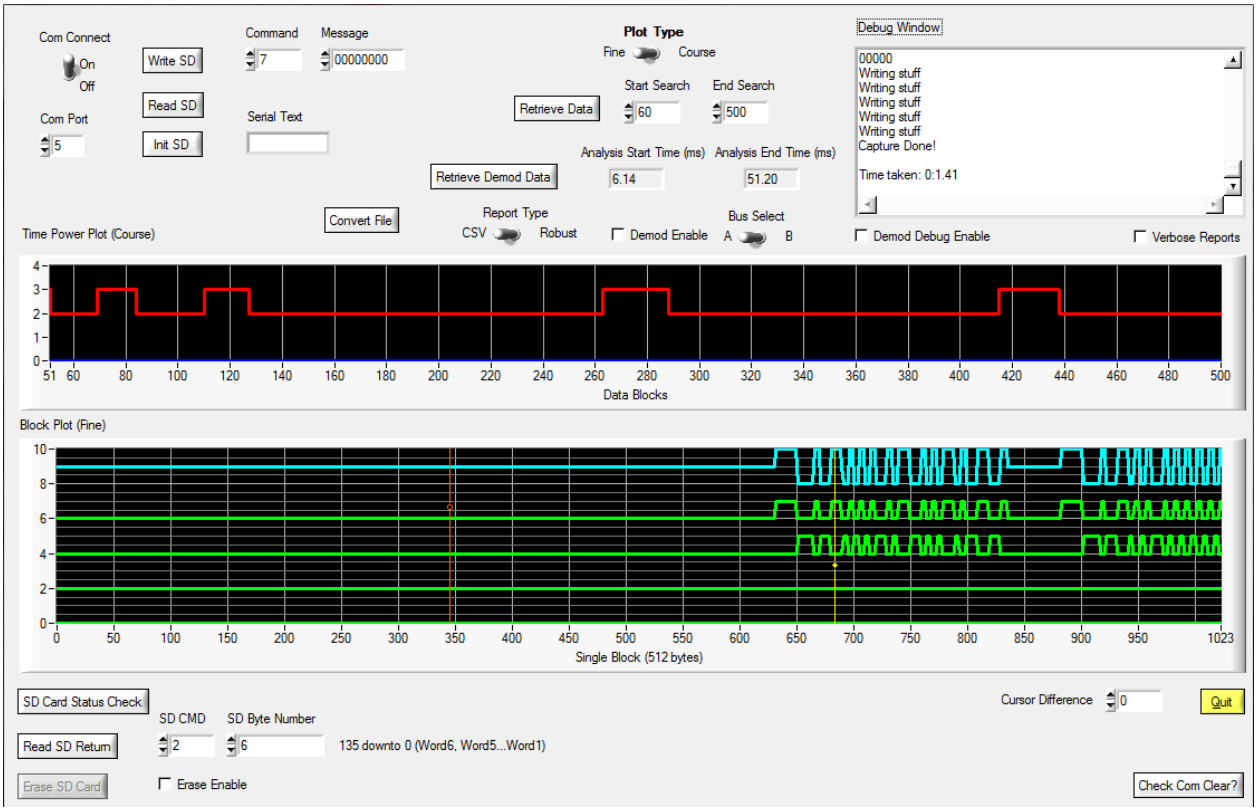


Figure 10: Bit transitions captured and graphed by Sandstorm

4 MECHANICAL

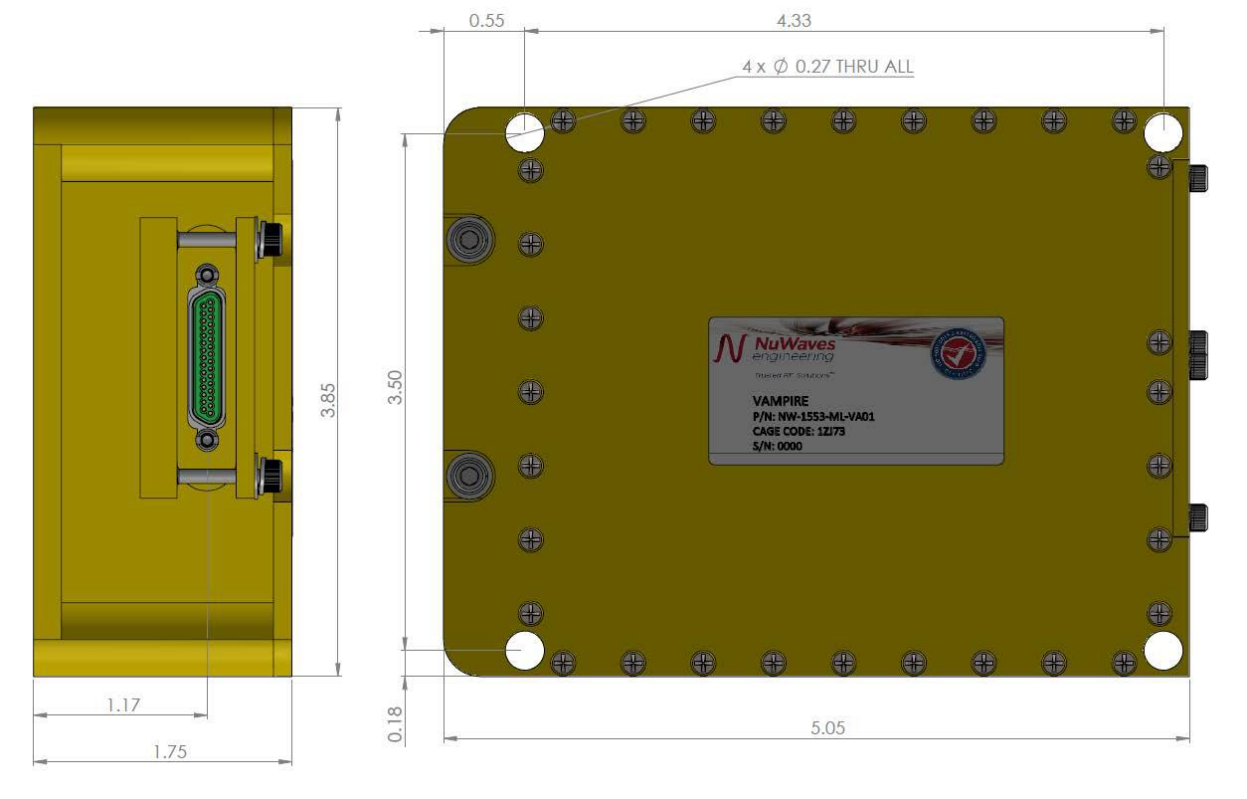


Figure 11: Vampire Mechanical Outline

Table 5: Vampire Mechanical Specifications

Parameter	Specification
Interface Connector	31 Pin Micro-D
Dimensions (LxWxH)	5.05” x 3.85” x 1.75”
Weight	2.0 lbs

5 TROUBLESHOOTING

Common questions and answers to troubleshooting Vampire.

Q: Why am I not seeing any Ethernet traffic using CIDS?

A: Ethernet traffic is only available if there is MIL-STD-1553 traffic. Verify there is traffic on the bus by checking the 2 LEDs behind the back cover. If the LEDs are not red or purple, there is no traffic, or the wrong MIL-STD-1553 connector could be plugged into the stub coupler.

Q: Why am I not seeing any Ethernet traffic on my computer and the LEDs are on?

A: Make sure the firewall on the computer is off. If using Wireshark, make sure it is in promiscuous mode. Additionally, the Ethernet connection is 1Gb. If the Ethernet is plugged into a switch, the switch must support 1Gb.

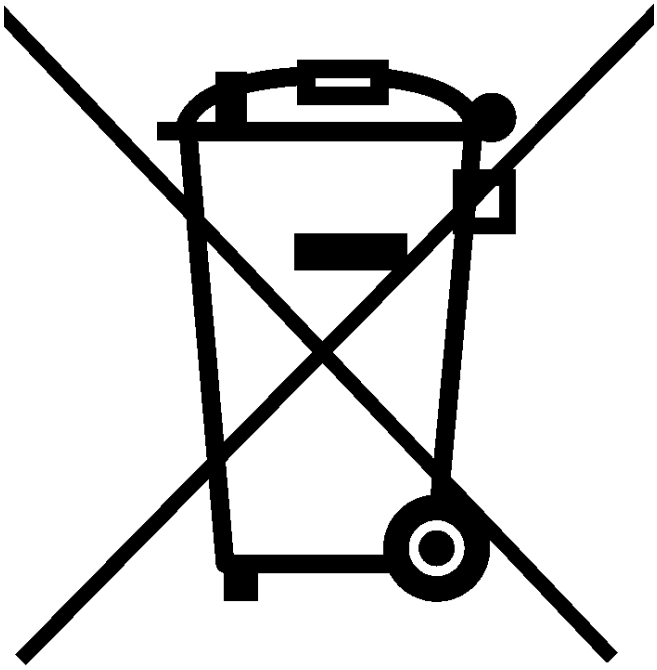
Q: Why can't I connect to Vampire over the serial port using the SD Analyzer GUI?

A: Make sure the correct COM port is being selected in the GUI. You might have to check Windows Device Manager to see which COM port showed up.

6 PRODUCT DISPOSAL – END-OF-LIFE

Safety is a guiding principle of NuWaves RF Solutions. We ensure safe production and operation of our products, as well as end-of-life disposal. Improper disposal can adversely affect the environment, wildlife and human health. Please follow these guidelines when disposing of a NuWaves product:

- Do not remove the cover or any hardware.
- Do not remove components from the circuit card assembly.
- Do not incinerate.
- Do not crush or shred.
- Do not dispose of as unsorted municipal waste.
- Do not export e-waste outside of the original destination country for recycling.
- Utilize an e-Steward or ISO14001 certified e-waste recycler.
- Consider export controls during recycler selection.
- If a NuWaves product is incorporated into a larger system or sub-system, ensure that these guidelines are followed at system end-of-life.



7 GETTING HELP - APPLICATIONS ENGINEERING

NuWaves RF Solutions offers technical support for basic configuration help and troubleshooting, Monday through Friday, 8 a.m. to 5 p.m. Eastern Time.

Technical Assistance and Application Engineering:

Email: sales@nuwaves.com

Phone: (513) 360 - 0800

NuWaves Home Page: https://www.nuwaves.com/

Product Warranty:

https://products.nuwaves.com/wp-content/uploads/NuWaves_Warranty_Repair.pdf

7.1 GENERAL INFORMATION

8 APPENDIX

Table 6: Acronyms

Abbreviation	Definition
BC	Bus Controller
FPGA	Field Programmable Gate Array
GUI	Graphical user interface
LED	Light emitting diode
RT	Remote Terminal
SD	Secure digital

8.1 REFERENCES

1. Day-Walker User Guide, AFRL/RYWA, 2020.
2. Sandstorm User Guide, AFRL/RYWA, 2020.
3. CIDS User Guide, AFRL/RYWA, 2020.

8.2 SERIAL PORT

The serial port baud rate is 115k baud. Packets are 8 ASCII hex characters in length. Write packets start with a "$" while read packets start with a "#". Register addresses are 2 ASCII hex characters and the register data is 5. Therefore, a register writes to address 1 with data 6 would look like "$0100006". A read would look like "#0100000". (The quotes are not part of the message.)

All serial packet writes are followed automatically by a return message on the serial port. The response packet is the value of the register after it was written to.

8.3 EHTERNET PACKET PARSING

Table 7: UDP Packet Format (1 packet of 8)

Vampire Ethernet Parser
6/2/2020

Ethernet Header: 0x7BB7

	Bit Number																																
32bit Field	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	
0	Bus Letter				0x9				0x0				0x9				8 high bits of pkt cntr								0	0	0	0	0	0	0	0	* Bus letter is ether A, B, C, D
1	8 low bits of pkt counter								0xE				error bits				place hold				0				0	0	0	0	0	0	0	0	
2	24 High bits of 44 bit timestamp																								0	0	0	0	0	0	0	0	*Timestamp is 5 ns per bit
3	20 low bits of 44 bit timestamp																				Fine Rez				0	0	0	0	0	0	0	0	*Fine rez is 0.5 ns per bit
4	24 bits of normal message reply time																								0	0	0	0	0	0	0	0	*Reply time is 5 ns per bit
5	24 bits of RT 2 RT reply time																								0	0	0	0	0	0	0	0	*RT 2 RT is related to the commanded RT
6	Sync			Decoded command message (17 bits) RT 2 RT																	0	0	0	0	0	0	0	0	0	0	0	0	*RT 2 RT is related to the commanded RT
7	Sync			Decoded command message (17 bits)																	0	0	0	0	0	0	0	0	0	0	0	0	
8	Sync			Decoded status message (17 bits) RT 2 RT																	0	0	0	0	0	0	0	0	0	0	0	0	*RT 2 RT is related to the commanded RT
9	Sync			Decoded status message (17 bits)																	0	0	0	0	0	0	0	0	0	0	0	0	
10	Sync			Decoded Data 0																	0	0	0	0	0	0	0	0	0	0	0	0	* All syncs are 010 for cmd, 000 for data
11	Sync			Decoded Data 1																	0	0	0	0	0	0	0	0	0	0	0	0	
12	Sync			Decoded Data 2																	0	0	0	0	0	0	0	0	0	0	0	0	
13	Sync			Decoded Data 3																	0	0	0	0	0	0	0	0	0	0	0	0	
14	Sync			Decoded Data 4																	0	0	0	0	0	0	0	0	0	0	0	0	
15	Sync			Decoded Data 5																	0	0	0	0	0	0	0	0	0	0	0	0	
16	Sync			Decoded Data 6																	0	0	0	0	0	0	0	0	0	0	0	0	
17	Sync			Decoded Data 7																	0	0	0	0	0	0	0	0	0	0	0	0	
18	Sync			Decoded Data 8																	0	0	0	0	0	0	0	0	0	0	0	0	
19	Sync			Decoded Data 9																	0	0	0	0	0	0	0	0	0	0	0	0	
20	Sync			Decoded Data 9																	0	0	0	0	0	0	0	0	0	0	0	0	
21	Sync			Decoded Data 10																	0	0	0	0	0	0	0	0	0	0	0	0	
22	Sync			Decoded Data 11																	0	0	0	0	0	0	0	0	0	0	0	0	
23	Sync			Decoded Data 12																	0	0	0	0	0	0	0	0	0	0	0	0	
24	Sync			Decoded Data 13																	0	0	0	0	0	0	0	0	0	0	0	0	
25	Sync			Decoded Data 14																	0	0	0	0	0	0	0	0	0	0	0	0	
26	Sync			Decoded Data 15																	0	0	0	0	0	0	0	0	0	0	0	0	
27	Sync			Decoded Data 16																	0	0	0	0	0	0	0	0	0	0	0	0	
28	Sync			Decoded Data 17																	0	0	0	0	0	0	0	0	0	0	0	0	
29	Sync			Decoded Data 18																	0	0	0	0	0	0	0	0	0	0	0	0	
30	Sync			Decoded Data 19																	0	0	0	0	0	0	0	0	0	0	0	0	
31	Sync			Decoded Data 20																	0	0	0	0	0	0	0	0	0	0	0	0	
32	Sync			Decoded Data 21																	0	0	0	0	0	0	0	0	0	0	0	0	
33	Sync			Decoded Data 23																	0	0	0	0	0	0	0	0	0	0	0	0	
34	Sync			Decoded Data 24																	0	0	0	0	0	0	0	0	0	0	0	0	
35	Sync			Decoded Data 25																	0	0	0	0	0	0	0	0	0	0	0	0	
36	Sync			Decoded Data 26																	0	0	0	0	0	0	0	0	0	0	0	0	
37	Sync			Decoded Data 27																	0	0	0	0	0	0	0	0	0	0	0	0	
38	Sync			Decoded Data 28																	0	0	0	0	0	0	0	0	0	0	0	0	
39	Sync			Decoded Data 29																	0	0	0	0	0	0	0	0	0	0	0	0	
40	Sync			Decoded Data 30																	0	0	0	0	0	0	0	0	0	0	0	0	
41	Sync			Decoded Data 31																	0	0	0	0	0	0	0	0	0	0	0	0	
42				Extra Data																	0	0	0	0	0	0	0	0	0	0	0	0	
43				Extra Data																	0	0	0	0	0	0	0	0	0	0	0	0	
44				Extra Data																	0	0	0	0	0	0	0	0	0	0	0	0	

* Errors: 0x0 - No errors, 0x1 - Cmd sync error, 0x2 - Cmd error, 0x3 - Data sync error, 0x4 - Word decode error, 0x5 - Transfer error, 0x6 - Busy, 0x7 - No reply

8.4 EXAMPLE TEST REPORT FROM DAY-WALKER SOFTWARE

*** Some content was removed for consolidation purposes.

Vampire Analysis of Flight Data

File Name: c:\Management\FieldIII\Avionics\Vampire\gui\Vampire_6.pcapng

File Size is: 50001216 bytes.

BC / RT interactions (approximate): 288184

**RT: 2, Total Messages = 504 Sub Addresses. Messages = 1.92, Reply Time (Max): 8840, (Min): 8590, (Median): 8671

2.114, Reply Time (Max): 8905, (Min): 8815, (Median): 8823

14.23, Reply Time (Max): 8585, (Min): 8560, (Median): 8565

15.115, Reply Time (Max): 8730, (Min): 8685, (Median): 8604

17.114, Reply Time (Max): 8840, (Min): 8755, (Median): 8769

18.23, Reply Time (Max): 8705, (Min): 8685, (Median): 8685

28.23, Reply Time (Max): 8855, (Min): 8815, (Median): 8828

**RT: 3, Total Messages = 506 Sub Addresses.

Messages = 1.92, Reply Time (Max): 9415, (Min): 9335, (Median): 9344

17.46, Reply Time (Max): 9435, (Min): 9370, (Median): 9387

28.368, Reply Time (Max): 9440, (Min): 9325, (Median): 9277

**RT: 11, Total Messages = 1517 Sub Addresses.

Messages = 1.92, Reply Time (Max): 9760, (Min): 9350, (Median): 9601

2.919, Reply Time (Max): 9605, (Min): 9355, (Median): 9355

3.23, Reply Time (Max): 9600, (Min): 9560, (Median): 9575

8.115, Reply Time (Max): 9480, (Min): 9390, (Median): 9399

9.115, Reply Time (Max): 9440, (Min): 9355, (Median): 9374

11.115, Reply Time (Max): 9440, (Min): 9390, (Median): 9405

17.23, Reply Time (Max): 9710, (Min): 9665, (Median): 9679

28.115, Reply Time (Max): 9600, (Min): 9560, (Median): 9562

**RT: 17, Total Messages = 17737 Sub Addresses.

Messages = 0.23, Reply Time (Max): 6320, (Min): 6270, (Median): 6285

1.920, Reply Time (Max): 6330, (Min): 6250, (Median): 6209

13.919, Reply Time (Max): 6335, (Min): 6250, (Median): 6250

26.14036, Reply Time (Max): 6335, (Min): 6245, (Median): 6249

27.1839, Reply Time (Max): 6330, (Min): 6240, (Median): 6242

Available RTs: 2,3,5,6,7,8,9,10,11,12,13,14,15,17,18,19,22,23,25,27,30,

RT selection was: 33
Found 0 Packets
Available Sub Addr: 0,1,2,3,4,5,7,8,9,11,13,14,15,16,17,18,19,23,24,26,27,28,
NO PACKET ERRORS or ORDER ERRORS FOUND