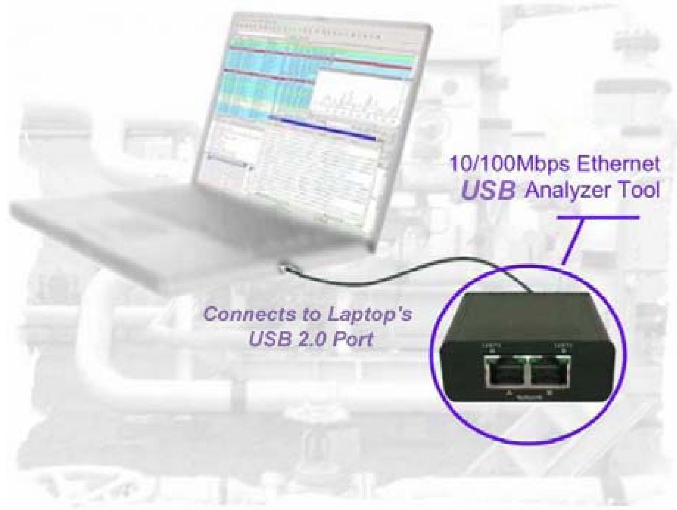
EtherShark™ Tap User's Manual

USB 2.0 10/100 Ethernet Protocol Analyzer *Aggregating* Tap



Package contents:

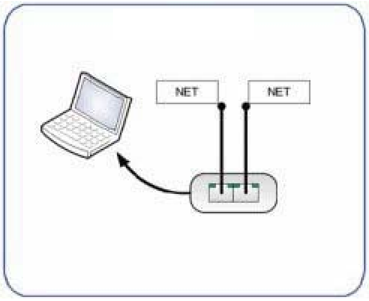
1 - Cordura Zippered Case
1 - **EtherShark™ Tap** Main Unit
1 - USB key containing drivers and software
1 - RJ45 CAT5 patch cord (straight through)
1 - USB 2.0 cable
1 - User's manual (also included on USB key). See **readme_first.txt** on USB key for latest info.

Table of Contents

1. General Information

The **Ethershark™ Tap** is an aggregating Ethernet tap, which will send all the packets, sent or received, from both sides of an Ethernet 10/100 BaseT connection. A non-aggregating tap would give you the packets from the workstation or the switch, but not both at the same time (not very useful for troubleshooting).

It's installed in-series with the patch cord that's normally going to a PC or any other type of workstation, Ethernet Switch, Router or VoIP device.



EtherShark™ Tap sees and monitors all seven protocol layers, and captures and aggregates **full-duplex** traffic at wire-speed (200Mb).

It requires only one USB 2.0 (480Mb) port on a laptop or PC (USB 1.1 *won't* work). The hardware setup takes less than a minute, and it can be used with multiple operating systems (Windows, Mac OS and Linux).

Power is supplied by your laptop or PC via the USB 2.0 direct connection (*not* through a USB hub). No extra power adapter is required. The **'Permanent Network Link'** feature guarantees permanent network connectivity and no packet loss, even when the laptop or PC power fails, or the USB port is disconnected.

Once installed in-line using a patch cord, **EtherShark™ Tap** is invisible to the network and does not interfere in auto-negotiation, speed or duplex settings.

One LED shows Power, two LEDs show Link/Activity, two more LEDs show CRC errors on the monitored link.

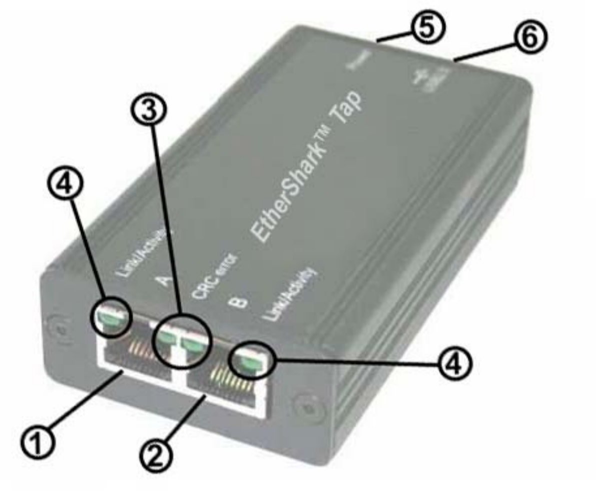
802.3af **Power over Ethernet** (PoE) is supported to the connected Ethernet device (the **EtherShark™ Tap** gets its power from the USB 2.0 port, ***not*** POE).

The **EtherShark™ Tap** is designed to work with third party software like **Wireshark** (or the obsolete Ethereal), Optiview, Etherpeek, etc. The included USB key holds the necessary drivers and the open source analyzer software Wireshark.

By design, the **EtherShark™ Tap**, unlike ordinary NIC's, passes information about MAC level faults like CRC, etc. to the analyzer software. There are several ways to indicate these kinds of errors with the **EtherShark™ Tap**: via LEDs on the front panel, via the included EasyStat software (found on the USB key), or using Wireshark or your favorite analyzer software.

The included **EasyStat** software (Java application, which will run on Windows, MAC and Linux machines) will give you transmit and receive statistics, as well as error counts. EasyStat will run while your are using analyzer software like Wireshark, and can help you spot problems very quickly by giving you statistics and a graphical representation of the data.

2. EtherShark™ Tap Connections and Indicators



① Port A (RJ45) connected to the network
② Port B (RJ45) connected to the network
③ Two green LEDs to indicate whether a CRC error occurs (located next to each other)
④ Two green LEDs to indicate the activity on the network
⑤ Green LED gives you information about power supply status (lit LED = device powered)
⑥ USB 2.0 connector linked to your monitoring device (i.e. a laptop computer)

3. Installation

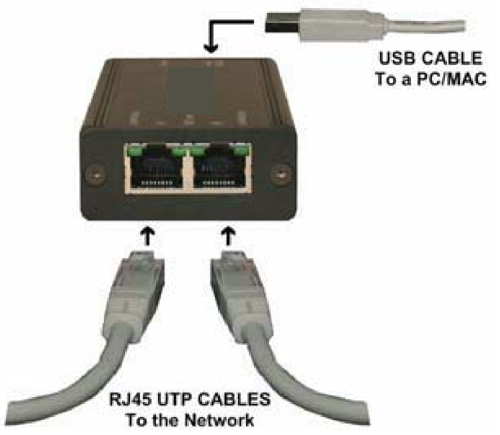
3.1 Hardware & driver installation (see **readme_first.txt** on USB key for later installation notes)

a. Insert the USB key to copy to an installation folder.

Note: Please copy the contents to a directory (folder) on your hard disk ***first*** so you don't accidentally delete/overwrite the files unintentionally.

After copying, disconnect the USB. If you're careful, you can use the USB key for the installation procedures and connect the **EtherShark™ Tap** to a second USB 2.0 port (and remove the USB key when finished with the installation).

b. Connect EtherShark™ Tap to the network using Category 5 UTP cables (patch cords):



Connections:

EtherShark™ Tap *Port A*: to DCE by straight Cable / to DTE by cross-over cable.

EtherShark™ Tap *Port B*: to DTE by straight Cable / to DCE by cross-over cable.

NOTE: When using analyzer software, it doesn't matter whether **Port A** or **Port B** goes towards the workstation or switch. When running **EasyStat** to get statistics on packets and errors, the TX or RX (transmit or receive) statistics will depend on which patch cord is plugged into the ports. You should be able to note the direction easily when looking at the statistics, and swap the patch cords if the TX / RX direction matters to you.

You would normally use the included straight patch cord (a normal patch cord) to put the **EtherShark™ Tap** between a workstation or VoIP phone, and the Ethernet switch.

The maximum total distance between any of the connected devices is **90 meters**.

c. Connect the USB port

Connect the USB port with the included cable to a PC/MAC USB 2.0 port. Power LED will light.

The USB cable length should not exceed 5 meters (about 15 feet).

d. Install the driver

Install the driver from the directory you created according to your operating system.

The current available drivers are located on the USB key at the driver section or within your installation directory you created on your hard disk.

Supported OSs are:

Windows ME/98/CE 5.0
Windows XP/2000/Vista 32-bit and 64-bit
Windows 7 32-bit and 64-bit
Windows 8 32-bit and 64 bit
MAC OS X 32-bit/64-bit/x86/PowerPC
Linux kernel 2.6.0 ~ 2.6.13
Linux kernel 2.6.14 ~ 2.6.22

Call **630-980-7710** to check for the latest driver for your operating system if you are having problems with the driver:

e. Setup the EtherShark™ Tap virtual network card (NIC) in your operating system

After installation, the **EtherShark™ Tap** will be a virtual Network Interface Card (NIC) to your operating system, and to any analyzer software.

The following settings are internal on your laptop or PC only – there are no external effects, nor are those settings presented or exposed to the monitored link.

We recommend you set an IP address for the virtual NIC card in your operating system's Network settings (this IP is ***needed*** to run the included EasyStat packet statistics software, but not for analyzer software):

Configure the TCP/IP Protocol Stack under Network Properties for this connection:

IP Address :	**192.168.0.1**	
Submask :	**255.0.0.0**	**(*NOT* the more common 255.255.255.0!)**

Note : Gateway and DNS settings must be undefined (blank)

f. Setting up Winpcap

Winpcap is ***required*** to communicate in the background with the **EtherShark™ Tap**.

If you are using Wireshark, this is part of the auto-installation procedure.

Winpcap must be installed manually if any other analyzer is chosen. Verify the presence of Winpcap on your computer. There is a version of Winpcap on the USB key, but the latest version from the Winpcap web site is a good idea: **www.winpcap.org**

EtherShark™ Tap is now ready to use with your analyzer or EasyStat (included) **software.**

3.2 Analyzer Installation

To perform analysis you can use any analyzer software (most will work). The powerful open source Wireshark software is provided on the USB key. Check the Wireshark web site for an updated version: **www.wireshark.org**

a. Selecting EtherShark™ Tap as the source for your analyzer software

Start your analyzer software and select the new virtual device showing up at the "select NIC" window. Refer to your analyzer's manual, or the user help about how to select a Network Interface Card.

b. Using alternate analyzer software

As an option you may install alternate analyzer software from any source (most will work).

Notes :

• Always follow the specific instructions of the chosen analyzer software.

• In addition, perform step **a. (above)** to enable the **EtherShark™ Tap** to be the selected resource for analysis.

• Make sure to use the latest available versions of the analyzer software and Winpcap.

• Remember to install Winpcap. The easiest way to identify its presence is to see **»EtherShark™ Tap is connected»** when opening the EasyStat program included on the USB key.

If Winpcap is not active, the EasyStat program indicates **«EtherShark™ Tap not found«** in the lower left corner of the EasyStat window (which can also be caused by your firewall blocking Java).

4.1 EasyStat packet statistics software (included on the USB key)

NOTE: EasyStat is a **Java** program. It may not run on later versions of Java that have been changed to increase security, and the runtime included may not work on later versions of Windows.

a. Installation

Using EasyStat software requires the installation of the Java based application, located on the USB key or in the folder you copied the USB key contents to on your local hard disk.

Locate the folder "EasyStat" on the USB key, or in the directory you put it in on your hard disk. Copy the folder "EasyStat" with its subdirectories to another location on your hard disk. You may create a shortcut on your desktop for EasyStat after it's installed.

Note : EasyStat software ***requires*** the Java Runtime Environment installed on your PC. This program is also provided on the USB key.

When installing the Java Runtime if your **firewall** asks you to keep blocking, ***you must allow it*** for EasyStat to find the **EtherShark™ Tap**. You can also manually go into your firewall and allow the **Java Platform binary** if EasyStat can't find the Tap.

The Java Runtime is available as a free download for various Operating systems at: **www.java.com**

b. Description

EasyStat is a stand alone packet statistics application designed for the **EtherShark™ Tap**.

There is no need to shut down your analyzer software while performing any actions with EasyStat, as long as you have **Stat Mode** checked in the upper left corner. **Tap Mode** won't let the packets get to your analyzer.

Locate the executable file EasyStat<version>.jar in the folder "EasyStat" (or other location you put it in), and double-click on it to execute the application in a new window.

If **Connected** doesn't appear in the lower left corner, and your analyzer works OK, you need to make sure the **Java Platform binary** is allowed in your firewall.

Each time you start EasyStat the program will ***automatically*** create two csv files in the same folder as the .jar file. These files will be used to store the collected statistics and will be updated and expanded during monitoring. You may erase these files ***after closing*** EasyStat, or keep them for further reference. They are date stamped.

EasyStat will give you a packet overview (without analyzer functionality). This troubleshooting tool will display the bandwidth or any low layer errors by chart or graph, prior to a deeper investigation performed by analyzer software.

In addition to the display of CRC errors via LEDs on the front of **EtherShark™ Tap** unit, EasyStat displays detailed information about the RX and TX lines of the monitored link. Once **EtherShark™ Tap** is connected to the network and the USB 2.0 port, it will monitor all seven layers of the link.

When EasyStat is in **Stat Mode**, it uses the **EtherShark™ Tap** exclusively, and an analyzer won't get the packets (by default). To run an analyzer (like Wireshark) at the same time, click the **Tap Mode** under Setup (top left). Toggle between modes by selecting **Stat** or **Tap**.

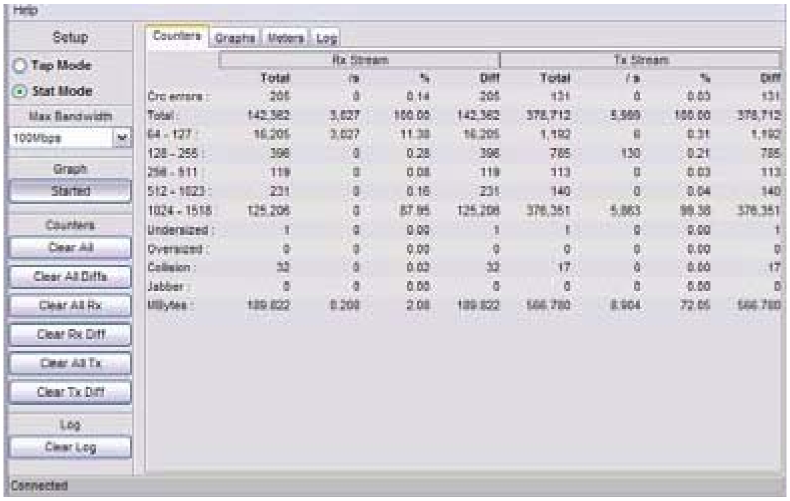
Note : In some systems the *.jar extension is associated to a different program like Winrar or Nokia's Cellphone applications. In this case, EasyStat will be *opened* instead of being executed. Occasionally an undefined error may occur. Correct this by de-associating the JAVA .jar extension in your operating system's configuration settings.

c. *Usage*

EasyStat provides several ways to display information about traffic statistics. The following pages give an overview about all the options.

Counters

This screen shot shows the set of counters and information available for the monitored transmitted (TX) and received (RX) lines:



○ Tap Mode
● Stat Mode

Max Bandwidth: 100Mbps

Graph: Started

	Rx Stream				Tx Stream			
	Total	/s	%	Diff	Total	/ s	%	Diff
Crc errors :	205	0	0.14	205	131	0	0.03	131
Total :	142,362	3,027	100.00	142,362	378,712	5,989	100.00	378,712
64 - 127 :	16,205	3,027	11.38	16,205	1,192	6	0.31	1,192
128 - 255 :	396	0	0.28	396	785	130	0.21	785
256 - 511 :	119	0	0.08	119	113	0	0.03	113
512 - 1023 :	231	0	0.16	231	140	0	0.04	140
1024 - 1518 :	125,206	0	87.95	125,206	376,351	5,863	99.38	376,351
Undersized :	1	0	0.00	1	1	0	0.00	1
Oversized :	0	0	0.00	0	0	0	0.00	0
Collision :	32	0	0.02	32	17	0	0.00	17
Jabber :	0	0	0.00	0	0	0	0.00	0
MBytes :	189.822	0.200	2.08	189.822	566.780	8.904	72.05	566.780

Connected

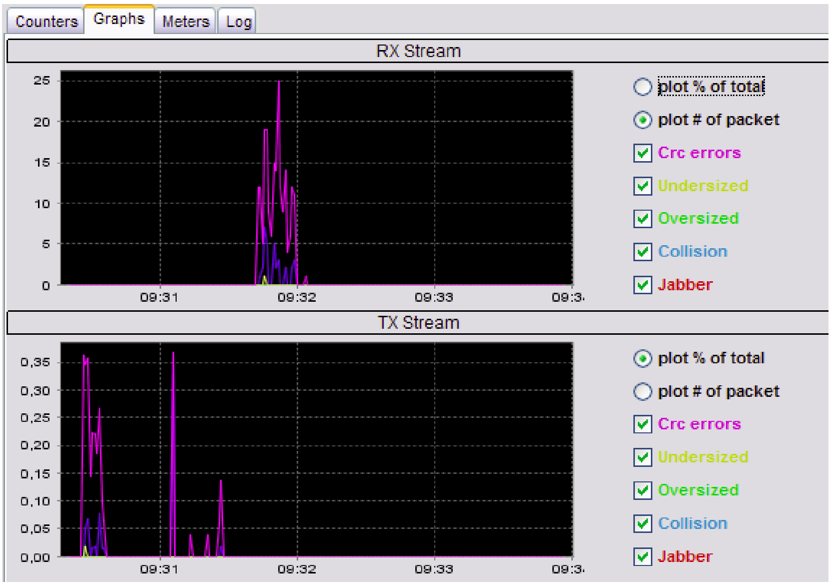
EtherShark™ Tap counts the following events: CRC error, size bracket of frames, undersized and oversized frames, collisions and jabbers. Furthermore the lower row gives the total of bytes seen.

In addition to the above information for average value per second, percentage and differential stats are provided.

Each column can be cleared by clicking on the buttons to the left of the window.

Graphs

This screenshot shows a different way to display information:



RX Stream:

○ plot % of total
● plot # of packet
☑ Crc errors
☑ Undersized
☑ Oversized
☑ Collision
☑ Jabber

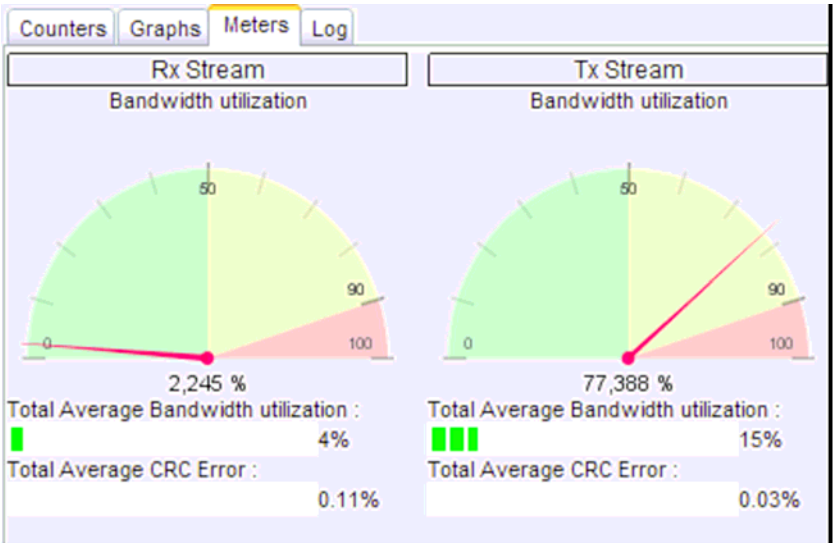
TX Stream:

● plot % of total
○ plot # of packet
☑ Crc errors
☑ Undersized
☑ Oversized
☑ Collision
☑ Jabber

Select the checkboxes (on the right) to monitor the kind of events you want track in real time on the graphs. It's also possible to display the events on percentage in total, or by number of packets.

You may zoom in by drawing an area with the cursor starting with the top-left corner to the bottom-right corner of the selection box. To cancel the zoom, just perform another selection starting with the bottom-right corner to the top-left corner.

Meters

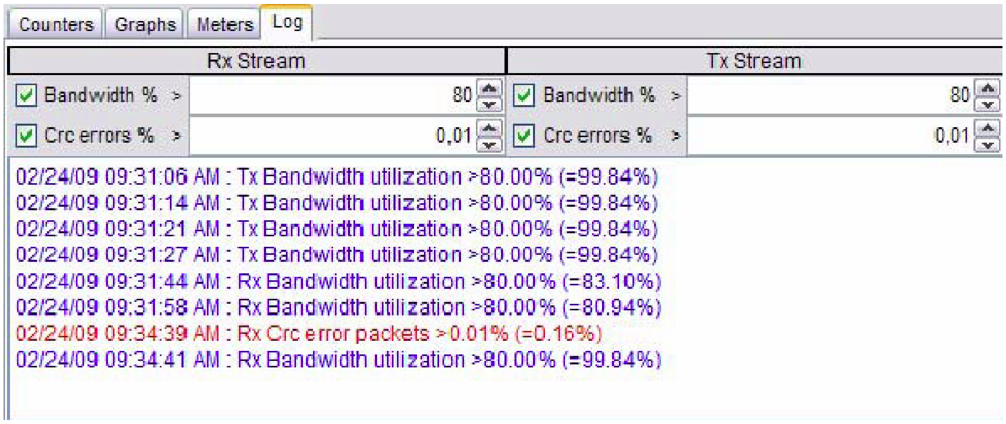


Rx Stream
Bandwidth utilization
2,245 %
Total Average Bandwidth utilization : 4%
Total Average CRC Error : 0.11%

Tx Stream
Bandwidth utilization
77,388 %
Total Average Bandwidth utilization : 15%
Total Average CRC Error : 0.03%

This view use meters and gauges to display the average bandwidth utilization, and CRC error occurrences. The values are percentage of the total of seen packets on the monitored TX and RX lines.

Log



Rx Stream		Tx Stream	
☑ Bandwidth % >	80	☑ Bandwidth % >	80
☑ Crc errors % >	0,01	☑ Crc errors % >	0,01

```
02/24/09 09:31:06 AM : Tx Bandwidth utilization >80.00% (=99.84%)
02/24/09 09:31:14 AM : Tx Bandwidth utilization >80.00% (=99.84%)
02/24/09 09:31:21 AM : Tx Bandwidth utilization >80.00% (=99.84%)
02/24/09 09:31:27 AM : Tx Bandwidth utilization >80.00% (=99.84%)
02/24/09 09:31:44 AM : Rx Bandwidth utilization >80.00% (=83.10%)
02/24/09 09:31:58 AM : Rx Bandwidth utilization >80.00% (=80.94%)
02/24/09 09:34:39 AM : Rx Crc error packets >0.01% (=0.16%)
02/24/09 09:34:41 AM : Rx Bandwidth utilization >80.00% (=99.84%)
```

This tab allows you to set up thresholds for bandwidth traffic and CRC errors, and to write an event into a log if the values exceed the thresholds. The recorded entries can be identified easily by type of event and its value, and direction on the monitored link.

4.2 **TraceBuster FREE** software from **Touschstone Technoligies, Inc.** (included on USB key)

TraceBuster FREE software is included in the **TraceBuster** folder on the USB key, in a ZIP file. It will work on **Windows XP** and **Windows 7**. *It does **not** work on **Vista**.*

TraceBuster FREE software allows you to capture packets, and come back later to analyze the captured packets with SIP/H323 Analysis, Call Flow Diagrams, and Signaling Metrics. There is a limit to the number of calls you can capture in the **FREE** version. **TraceBuster** does not do real-time analysis (other **Touchstone** products will do real-time).

Touchstone has two paid versions of this software, available at:

http://www.touchstone-inc.com/tracebuster.php

With the paid **TraceBuster Professional** you get more options like Media Capture, Analysis, and DTMF analysis. You can set Alerts and Alarms options and Reporting options with the **Pro** version. The call capacity is also increased in **Pro** version.

TraceBuster Professional w/QoS adds QoS information to the regular **Pro** version. It gives you MOS scores, R-Factor, Jitter Buffer Emulation, RTCP XR decoding, etc. Touchstone is offering **EtherShark™ Tap** owners a 25% discount on the **QOS** version of **TraceBuster Professional**.

On the **Touchstone** web site you'll also find their **WinSIP** product, which is an easy-to-use software solution for **generating bulk calls**, performing feature and function testing, and testing advanced media capabilities. They offer **WinSIP** licenses for generating four concurrent calls, all the way to an unlimited number of concurrent calls.

5. Additional information

5.1 EtherShark™ Tap System requirements

To achieve maximum performance and to avoid potential packet loss or malfunctions, the minimum required configuration should be:

- **USB 2.0 Port** (USB 1.1 is ***not*** fast enough). A laptop with a USB 2.0 port should be both modern enough ***and*** fast enough to run the **EtherShark™ Tap** and analyzer software. USB 3.0 should work since it's backwards compatible with USB 2.0 (not tested).

- **Dual Core Processor**

- **1GB memory**

5.2 Technical and electrical features

Power Consumption: 5V 300mA
Operating Temperature: 0 - +50°C
Storage Temperature: -40 - +120°C
Relative Humidity: 10 to 95%, non-condensing
Compliance: RoHS, CE, FCC class A

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Warranty and Liability

MSE, Inc. warrants that this product is free from defects in material and workmanship at time of shipment. The warranty period is two years from the date of purchase. MSE, Inc. assumes no liability for products that have been subjected to abuse, modification, misuse, or if the model or serial number has been altered, tampered with, defaced or removed.

MSE, Inc. is not liable under any contract, negligence, strict liability or other legal or equitable theory for any loss of use of the product, inconvenience or damages of any character, whether direct, special, incidental or consequential (including, but not limited to, damages for loss of goodwill, loss of revenue or profit, work stoppage or malfunction).

Copyright

Trademarks

The trademarks mentioned in this manual are the sole property of their owners.

Mike Sandman Enterprises, Inc.
• Unique Telecom Products •
630-980-7710

www.sandman.com • www.ethersharktap.com