PROFITAP

ProfiShark 1G
User manual

Gigabit Ethernet Troubleshooter

Thank you for purchasing the ProfiShark 1G.

Package contents:

- 1* ProfiShark 1G main unit
- 1* USB key containing drivers, software and manual
- 1* USB 3.0 cable
- 1* RJ45 cable
- 1* Carrying pouch

Table of contents

The ProfiShark 1G is a handheld, Plug and Play device dedicated to inline gigabit monitoring. It facilitates in-field traffic capture and troubleshooting. The ProfiShark 1G is equivalent to a 10/100/1G aggregator TAP and two 1 Gbit/s NICs. All-in-one in a pocket-sized box, the only additional hardware required being a laptop with a free USB 3.0 port.

As it is based on USB 3.0 (5 Gbit/s), the ProfiShark 1G manages full-duplex gigabit at wire speed, without the bottleneck of an aggregator TAP. It also surpasses all standard NICs in capture mode, as the ProfiShark 1G catches any tag and encapsulation without altering frames.

The ProfiShark 1G is the perfect tool for the field engineer as well as for long-term traffic collection.

Features

- 10/100/1G monitoring on USB 3.0
- USB 3.0 powered
- Failure safe monitoring
- Hardware aggregation
- 8 ns hardware timestamp
- Real time statistics
- Low level error and bandwidth monitoring
- CRC error capture
- Capture any packet with any analyzer
- Direct capture to disk

Network TAP

The ProfiShark 1G integrated network TAP provides safe access to the network for monitoring purposes. It is a passive monitoring device, meaning it is undetectable, the original traffic staying unaltered and no extra packets being inserted. As most of the TAP's functions are performed by dedicated hardware circuits, it is much more reliable and error proof than SPAN ports.

In a gigabit network, the TAP has to negotiate with both attached devices for the highest common speed. If no common speed can be found, or if one of the devices is disconnected, the TAP propagates the error to the other attached device, allowing a redundant path to be activated.

In case of power failure, it activates its bypass circuits, connecting the two attached devices directly. The ProfiShark 1G integrates a high performance fast failover circuit and a proprietary algorithm, reducing the unavailability of the network path down to 30ms.

Note: the fast failover relies on the network setup. In case the fast failover cannot perform, the two end devices have to renegotiate the link. This operation takes about 2 seconds.

End Device 1	End Device 2	1 Cable Types
DTE	DCE	Straight Through and Crossover
DCE	DTE	Straight Through and Crossover
DCE	DCE	Straight Through and Straight Through
DTE	DTE	Straight Through and Straight Through

Note: The user should verify that the two end devices connect together with either a single cable, an RJ45 coupler or the unpowered TAP. The straight or crossover cables must be employed in case of end devices that do not support Auto MDI/MDIX operate (i.e. Auto Crossover). Experienced users can bypass this procedure.

Note: Although some vendors recommend the use of the non-IEEE compliant "Forced Gigabit" mode, we strongly recommend activating auto-negotiation when Gigabit speed is required. More generally, auto-negotiation should always be enabled on both end devices in order to avoid duplex mismatch issues.

ProfiShark 1G Visual Description

1. Port A (RJ45) connected to the network
2. Port B (RJ45) connected to the network
3. (see below)
4. (see below)
5. (see below)
6. Power indicator LED
7. USB 3.0 connector linked to your monitoring device (i.e. a laptop computer)
8. DC input (5V/1A)

The ProfiShark's state is displayed on the front LEDs (3, 4, 5). LEDs functionalities are named on top of the ProfiShark.

TAP functions:
Steady LED 10 (4): TAP is operating at 10 Mbit/s
Steady LED 100 (5): TAP is operating at 100 Mbit/s
Steady LED 10 (4) and LED 100 (5): TAP is operating at 1000 Mbit/s
Steady Link/activity (3): the port is linked up
Blinking Link/activity (3): the port is linked up and has RX/TX activity
Blinking LED 10 (4) and LED 100 (5): TAP not connected or trying to connect
Alternating LED 10 (4) and LED 100 (5): TAP cannot find a common speed between Networks A and B

General functions:
Blinking LED 10 (4): The ProfiShark is initializing
Blinking LED 100 (5): The ProfiShark HW firmware is corrupted

Driver Installation

Drivers are available for Windows 7 32/64 bits and Windows 8 32/64 bits.

To install the ProfiShark 1G drivers, execute the setup utility located on the USB flash drive in the “ProfiShark 1G Manager” folder. Please make sure that you have uninstalled any older version of ProfiShark 1G Manager before starting the setup utility.

Connect the ProfiShark 1G on a free USB 3.0 port and the drivers should install automatically. For a manual installation, the drivers can be found in the default installation folder “C:\Program Files (x86)\Profitap\ProfiShark 1G\Driver\PT3”.
When the Profishark hardware is connected for the first time, a reboot of the PC is required in order to refresh the Winpcap/Wireshark device list.
The Winpcap/Wireshark device list may also be refresh with the following command lines:
- open a CMD window,
- « net stop npf » (without quotes),
- « net start npf » (without quotes),

Please check for the latest driver release for your operating system in the User Section at www.profitap.com. You will need to register to access this area. Registering is free and will let you participate in ongoing product improvements.

Analyzer installation

To perform the analysis, you can use any of the supported analyzers. Supported analyzers are listed in the User Section at www.profitap.com.

Wireshark is recommended and provided on the USB flash drive. To install it, please follow the instructions provided by the installation wizard.

To capture network data, start your preferred network analyzer and select the new network interface named “ProfiShark 1G Device”. Please refer to your analyzer’s manual or user help to know more about how to select a network interface.

ProfiShark 1G Manager

Installation

To install the ProfiShark 1G Manager, execute the setup utility located on the USB flash drive in the “ProfiShark 1G Manager” folder. Please make sure that you have uninstalled any older version of the ProfiShark 1G Manager before starting the setup utility. The setup utility will create a launch icon in your startup menu that you can use to start the ProfiShark 1G Manager.

Please check for the latest software release for your operating system in the User Section at www.profitap.com. You will need to register to access this area. Registering is free and will let you participate in ongoing product improvements.

Description

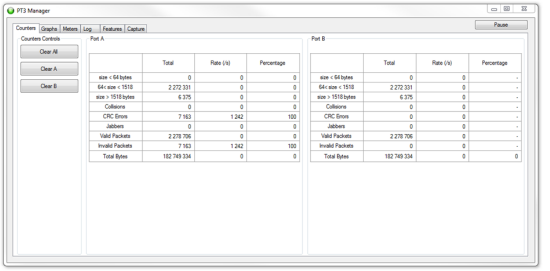
ProfiShark 1G Manager is a standalone application designed by ProfiTAP. It provides a way for statistical analysis of a network, allowing for efficient excessive bandwidth usage detection, or any low layer errors using charts prior to a deeper investigation using an analyzer. It is also used as a firmware flashing utility to update your product.

ProfiShark 1G Manager can be used at the same time as a software network analyzer, without the need to interrupt data capture.

Statistics

ProfiShark 1G Manager provides several different visual representations for network statistics. The following pages give an overview of these representations.

Counters



In the Counters tab are listed every counter embedded in the ProfiShark 1G for both network ports. The counters are 64 bits hardware counters, they are cleared at hardware startup and at link reconnection.

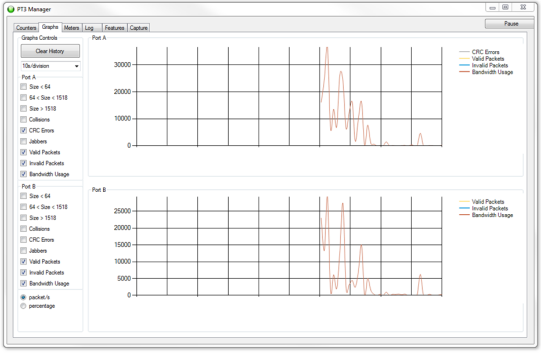
Statistics can be reset individually for each port or for the two ports at the same time using the buttons on the left.

Clearing the counters using the buttons does not clear the hardware counters, but stores all counters in reference counter. Then, the displayed counters are result of the formula *(hardware counter - reference counter)*.

Counters description:

size < 64 bytes: the CRC valid frames with a size under 64 bytes.
64< size < 1518: the CRC valid frames with a size over or equal to 64 bytes and under or equal to 1518 bytes.
size > 1518 bytes: the CRC valid frames with a size over 1518 bytes.
Collisions: the CRC error frames with a size under 64 bytes.
CRC Errors: the CRC error frames with a size over or equal to 64 bytes and under or equal to 1518 bytes.
Jabbers: the CRC errors frames with a size over 1518 bytes.
Valid frames: the CRC valid frames of any size.
Invalid frames: the CRC error frames of any size.
Total bytes: the valid frame bytes.

Graphs



The Graphs tab allows you to inspect statistical data over time, using plots.

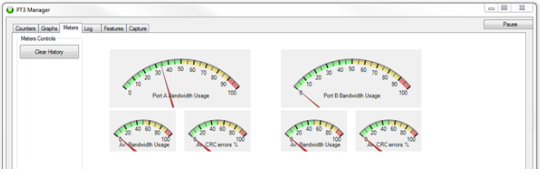
For each port, you can plot any of the statistical data by using the checkboxes on the left. Once a box is checked, the corresponding data appears on the graph on the right. Refresh rate can be selected using the drop down list on the left, allowing you to plot up to 10 hours of statistics.

When “packet/s” is selected, each series displays the corresponding number of packets per second, except for the bandwidth usage which is displayed in bytes per second. When “percentage” is selected, each series is displayed in term of percentage of the total number of packets, except for the bandwidth usage which is displayed in percentage of the total bandwidth.

Both graphs history can be reset using the Clear History button on the left. Disconnecting the ProfiShark 1G also reset the graphs’ data.

Meters

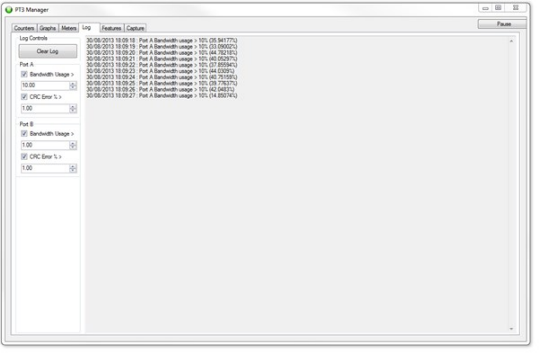
The meters tab uses meters to display the current bandwidth usage, the average bandwidth usage and the average CRC error rate for each port.
The meters' history can be reset using the Clear History button on the left.



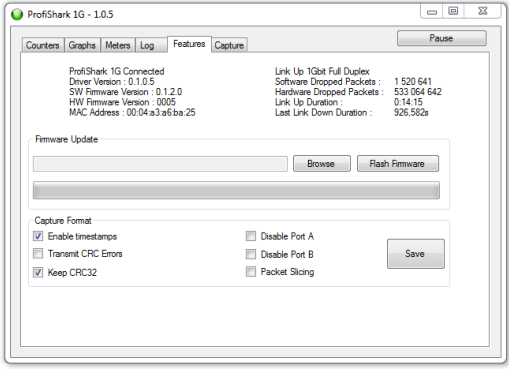
Log

The Log tab offers to set thresholds for bandwidth usage and CRC error rate. Every time the threshold is exceeded, a log entry is added, allowing to easily identify the type, date and the port of the event.

This can be used for long term analysis, where events happen randomly over a long period of time.



Features



The Features tab regroups information about the driver and firmware version, port status, the firmware update utility and a way to enable or disable ProfiShark 1G features.

To update the ProfiShark 1G firmware, press the browse button, select the firmware file and press the Flash Firmware button.

The corresponding firmware update will begin. You cannot use the ProfiShark 1G Manager while the update is in progress. The update process can take a few minutes to complete. Once it is done, please unplug and plug again the ProfiShark device to use the new firmware. Please do not unplug the USB port nor shut your computer down during the update process.

You can download the latest firmware from the User Section at www.profitap.com.

On the same screen, you can enable or disable the following features:

- **Transmit CRC Errors**: if checked, the ProfiShark will not filter out network packets with CRC errors like a normal NIC would.
- **Keep CRC32**: keep the CRC32 information (32-bit Frame Check Sequence) located at the end of the packets. FCS can be interpreted in Wireshark (Edit -> Preferences -> Protocols -> Ethernet -> Assume packets have FCS).
- **Disable Port A**: if checked, the frames which input on port A are not captured.

- **Disable Port B**: if checked, the frames which input on port B are not captured.
- **Packet Slicing**: If checked, the first 128 frames' Bytes are captured.
- **Enable timestamps** : if checked, a Unix formatted* timestamp is adjoined at the end of the packet data, after the FCS. This timestamp can be interpreted by the Profitap Wireshark dissector in live capture mode

*Unix timestamp format: the 64 bits timestamp is organized in two 32 bits words, representing the seconds since 01/01/1970, and the fraction of second.

Note: if the "Packet Slicing" feature is enabled, the hardware automatically disable the "Keep CRC32" feature. No padding is added to frames smaller than 128 Bytes.

Note: if both options "Transmit CRC Errors" and "Keep CRC32" are enabled, all the erroneous packets will be treated as fair ones.

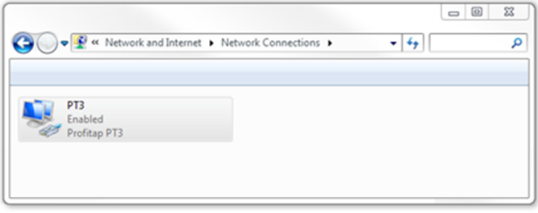
Packet capture

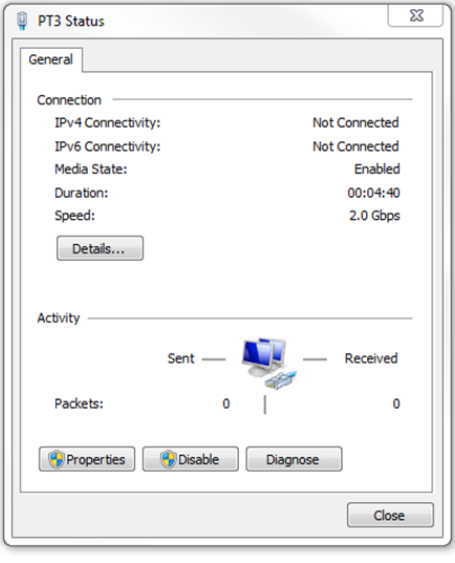
ProfiShark 1G gives you the ability to capture:

- Any type of frames (pause frames, Vlan tagged, …),
- Any encapsulated frames,
- CRC errors frames,
- Short frames (< 64 bytes),
- Jumbo frames (> 1518 bytes),
- Any frames between 10 bytes and 10 Kbytes,

Once the drivers have been properly installed, a new connection is added in the Network Connection panel. ProfiShark 1G acts as two 1 Gbit/s unidirectional NICs, regardless of the network connection speed. The frames aggregation is done in hardware respecting the original frame order. As opposed to FIFO (First In, First Out), the ProfiShark 1G employs an FCFS (First Come, First Served) mechanism.

A reboot of the computer may be required to refresh the Winpcap/Wireshark device list. ProfiShark 1G has been tested with all major capture/analyzer software.

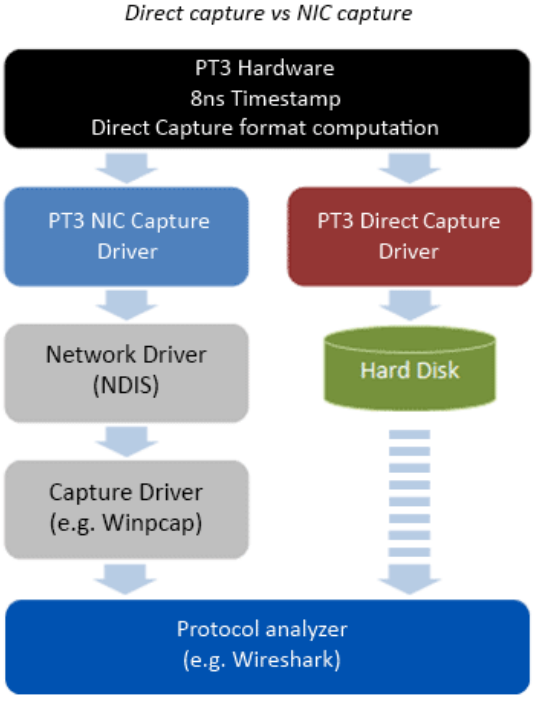

Network and Internet
Network Connections
PT3
Enabled
Profitap PT3


PT3 Status
General
Connection
IPv4 Connectivity:
Not Connected
IPv6 Connectivity:
Not Connected
Media State:
Enabled
Duration:
00:04:40
Speed:
2.0 Gbps
Details...
Activity
Sent
Received
Packets:
0
0
Properties
Disable
Diagnose
Close

Two mode of capture are available, Nic Capture mode and Direct Capture mode.

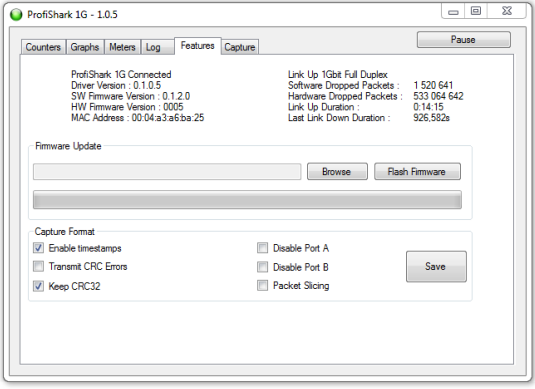
In NIC Capture mode (live capture), the capture is performed like on any other Network Card. The frames are routed to the NDIS driver.

In Direct Capture mode, the frame stream is dumped to the hard disk. The capture file format is computed in the ProfiShark 1G hardware.



Live Capture mode

ProfiShark 1G transmits network frames to the capture software without modifying them (see “Feature” chapter). It is transparent for packet size, packet type or protocols. All tags and encapsulation are preserved (e.g. Vlan, MPLS, GRE).



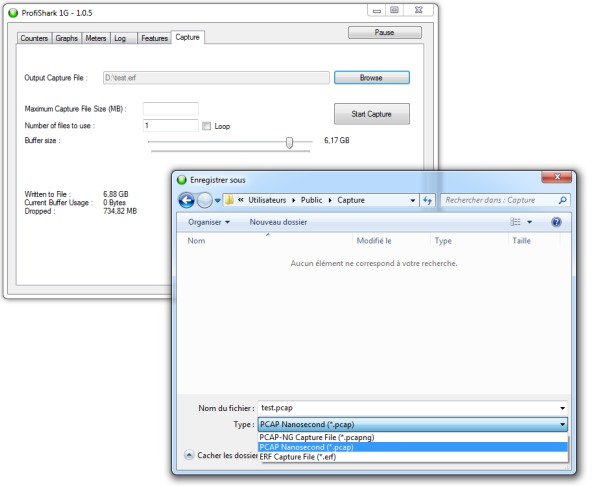
The “Software Dropped Packets” counter in the Feature tab indicates the number of packets dropped by the driver in live capture mode. It’s not representative of the dropped packets in Direct Capture (see “Direct Capture Mode” chapter). These drop events are caused by too high CPU usage.

The “Hardware Dropped Packets” counter indicates the amount of captured packets dropped due to low USB bandwidth (e.g. Gigabit capture on USB 2.0). In USB 3.0 mode this counter is not supposed to increase, even in full speed gigabit capture.

Note: small packet capture at gigabit full speed is extremely challenging for processors and can cause software drops. For that reason, another capture mode is available (see “Direct Capture Mode” chapter).

Direct Capture mode

ProfiShark 1G provides with the option to capture traffic without the need of a third-party capture software. This mode of capture is accomplished on driver level, prior to all network stacks and frame processing. With the support of direct capture, small packet capture can be performed at full wire speed.



The generated capture file format can be chosen between the following:
- PCAP Next Generation (.pcapng),
- Libpcap nanosecond (.pcap),
- ERF (.erf).

In all capture format, the packet's timestamp are hardware generated with an 8 nanosecond accuracy. The direct capture is compatible with the different hardware features: “Packet Slicing”, “Transmit CRC errors”, “Keep CRC32”, “Disable Port”. Please refer to the “Features” chapter.

Direct Capture setup:

Output Capture File: specify the name and location of the capture file. Name extension will be added to the specified name (_#####_YYYYMMDDHHMMSS).

Maximum Capture File Size (MB): the capture will stop when the file reaches the specified size in MB.

Loop: if selected, the capture does not stop. The files are erased to keep the specified amount of capture files. A round-robin capture can be done, with one or multiple files.

Number of files to use: specify the amount of capture files to be created.

Start Capture: when capture isn't running, starts the capture with the specified parameters.

Stop Capture: when capture is running, stops the capture and releases the capture file.

Written to File: indicates the amount of data written in the Output Capture File.

Current Cache Usage: indicates the RAM cache's current usage.

Dropped: indicates the amount of data dropped during the Direct Capture.

Note: the amount of dropped data depends on the data storage throughput and the amount of RAM cache. Disk arrays or SSDs can drastically improve capture performance.

Timestamping

Hardware timstamping feature can also be used in live capture mode, using the Profitap's Wireshark dissector. The files are located on the USB flash drive. It can also be downloaded in the User Section at www.profitap.com. The dissector is comatible with Wireshark (x86 and x64) 1.12 or above.

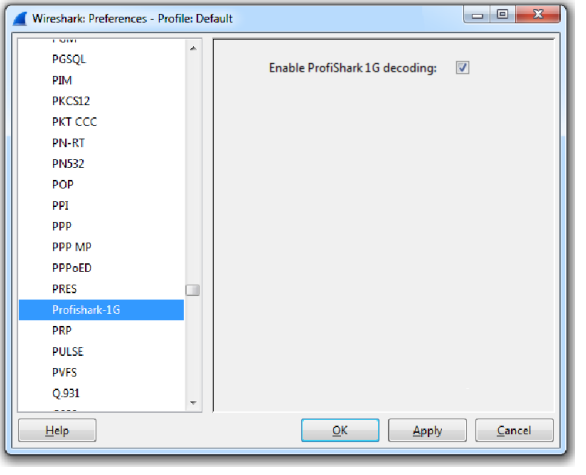
Linux :
Copy the two files (profishark_1g.la and profishark_1g.so) in '/usr/local/lib/wireshark/plugins/[wireshark_version]/', from x86 or x64 depending on the Liunx version

Windows :
Copy the file (profishark_1g.dll) in 'C:/Program Files/lib/Wireshark/plugins/[wireshark_version]/', from x86 or x64 depending on the Windows version.

The dissector can be enabled or disabled in Wireshark (Edit -> Preferences -> Protocols -> Profishark-1G -> Enable Profishark 1G decoding).

Timestamp option must be enabled in Features tab (see Features chapter).

Note: if « Enable Profishark 1G decoding » is checked, Wireshark assumes that every packet contains the Profishark timestamp.



Additional information

Ordering reference	C1AP-1G	
Dimensions Width Depth Height	 69 mm 124 mm 24 mm	 2.72 inches 4.88 inches 0.94 inches
Supported OS	Windows 8 32 & 64 bits Windows 7 32 & 64 bits Linux	
System requirements*	Dual Core Processor 4 GB memory USB 3.0 port	
Accessories	1.8m USB 3.0 cable RJ45 cable Pouch USB key	
Connectors	2 x RJ45 8 pins 1 x USB 3.0 1 x 5 VDC input	
LEDs	2 x Link activity 2 x Speed 1 x Power	
Power Consumption (5V) 1Gbps, with full traffic 100Mbps, with full traffic 10Mbps, with full traffic	 600 mA 450 mA 520 mA	
Operating Temperature Storage Temperature Relative humidity	0 to +50°C -40 to +80°C 10 to 95%, no condensing	32 to 122°F -40 to 176°F
Maximum Network Latency Link @ 1Gpbs Link @ 100Mbps Link @ 10Mbps	 370 ns 660 ns 6600 ns	
Compliance	RoHS CE	

*To achieve maximum performance and to avoid potential packet loss or malfunctions.

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

Profitap 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. Profitap 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. Profitap 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.

Notes

v2.3

CUSTOMER SUPPORT INFORMATION
To order or for technical information support:
Tel: +31 (0) 40 782 0880
Mail order:
Profitap HQ B.V.
High Tech Campus 9
5656 AE Eindhoven - The Netherlands
Website: www.profitap.com
E-mail: info@profitap.com