PROFISHARK 10G

INSTALLATION AND CONFIGURATION MANUAL

PROFITAP

www.profitap.com

BRINGING CLARITY INTO NETWORKS.
ANYTIME. ANYWHERE.

If you have any questions, you can contact us through our website:

www.profitap.com

or by email:

support@profitap.com

For the latest documentation and software, visit our Resource Center:

https://www.profitap.com/resource-center/

TABLE OF CONTENTS

INSTALLATION

1. UNPACKING

Carefully unpack all the items supplied with the ProfiShark 10G and retain the packaging for later use:

- 1 x ProfiShark 10G main unit
- 1 x USB 3.0 cable (1.8 m)
- 1 x 1.5 m USB A male to DC 5V adapter
- 1 x USB key (Software, Drivers, Documentation)
- Quick Start Guide

► NOTE: Please contact the supplier if any part is missing or damaged.

2. HARDWARE OVERVIEW

ProfiShark 10G is a portable TAP and troubleshooter, providing visibility into 1G and 10G connections, both copper and fiber. It is a non-intrusive monitoring device, undetectable to the network, leaving the original data traffic unaltered, with no extra packets being inserted.

ProfiShark 10G features 2 SFP cages for the connection to the network, accepting SFP+ modules (SR, LR, ER) of either fiber optic or copper type. Captured traffic is sent to the USB 3.0 output.

ProfiShark 10G can be set to either SPAN or In-Line mode. SPAN mode receives traffic from any connected SFP+ modules, while In-Line mode receives and transmits traffic between both ports.

ProfiShark 10G captures packets of all sizes and types, and provides real time traffic statistics, SFP+ module information, and various traffic capture settings and options. It also incorporates advanced hardware filters, deep packet inspection, and packet slicing, to optimize traffic throughput.

ProfiShark 10G can be powered from the USB 3.0 port alone when fiber optic SFP/SFP+ modules are being used. When copper SFP/SFP+ modules are being used, powering from both the USB 3.0 and the DC ports (using the included USB to DC power cable, or a 5V/1.5A power adapter) is highly recommended.

The unit can be managed by the ProfiShark Manager application, available on the supplied USB key and on the Profitap Resource Center.

FEATURES:

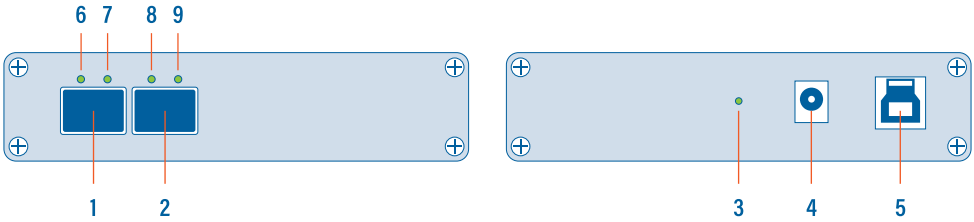
- 1G/10G monitoring on USB 3.0
- USB 3.0 powered for fiber SFP modules
- USB 3.0 + DC powered (adapter included) for copper SFP modules
- Hardware aggregation
- 5 ns hardware timestamping for accurate latency testing
- Customizable real time statistics
- Capture any type of frames
- Low level error and bandwidth monitoring
- Direct capture to disk
- In-Line and SPAN (Dual NIC) capture modes
- Advanced hardware filtering, deep packet inspection
- Packet slicing (adjustable packet size)
- In-depth network port diagnostic
- Invisible to the network
- Lightweight and portable
- Quick setup and easy to use

2.1 Technical and Electrical Specifications

SYSTEM REQUIREMENTS	LEDS
Dual Core Processor 4 GB memory USB 3.0 port	4 x Link Activity 1 x Power
MAXIMUM NETWORK LATENCY	
10 Gbps: 328 ns	
CONNECTORS	**ACCESSORIES**
2 x SFP+ 1 x USB 3.0 1 x 5V/1.5A DC input (center positive)	1.8 m USB 3.0 cable 1.5 m USB A male to DC 5V adapter USB key
DIMENSIONS (WxDxH)	**SUPPORTED OS**
105 x 124 x 26 mm 4.13 x 4.88 x 1.02 in	Windows 7 / 8 / 10 (32/64-bit) / 11 Linux, macOS High Sierra
CAPTURE PERFORMANCE	
3.2 Gbps	
WEIGHT	**STORAGE TEMPERATURE**
280g — 0.62 lb	-40 to +80 °C — -40 to 176 °F
RELATIVE HUMIDITY	**OPERATING TEMPERATURE**
10 to 95%, non-condensing	0 to +50 °C — 32 to 122 °F
COMPLIANCE	**ORDER REFERENCE**
RoHS — CE	C1AP-10G

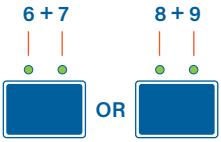
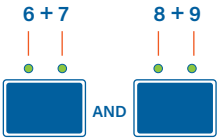
SFP STANDARD	POWER REQUIREMENTS
Fiber 1GBASE-SX/LX Fiber 10GBASE-SR/LR/ER/ZR	No additional power required
Copper 1GBASE-T Copper 10GBASE-T	Additional power required (supplied USB to DC power cable or 5V/1.5A DC power adapter)

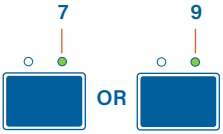
2.2 Visual Description



1, 2	SFP+ ports A and B, accepting both fiber optic and copper SFP/SFP+
3	Power indicator LED
4	DC power input (5V, 1.5A, center positive)
5	USB 3.0 port type B
6, 7, 8, 9	SFP+ status and network status LEDs

2.3 LED Functionality

LED NUMBER	LED COLOR	STATE / MEANING
	ORANGE	No SFP+ present or detected
	SLOW BLINKING GREEN	No link
	SLOW BLINKING RED	Additional power required
	ORANGE	No SFP+ present or detected
	STEADY GREEN	In-Line mode, link up
	SLOW BLINKING GREEN	No Link
	FAST BLINKING GREEN	In-Line mode, traffic activity
	SLOW BLINKING RED	Additional power required

	STEADY GREEN	SPAN mode, link up
	FAST BLINKING GREEN	SPAN mode, traffic activity
	BLINKING	Constant synchronization between system time and hardware timestamp (blink ON every even second, blink OFF every odd second)

3. CONNECTING POWER AND START-UP

To install the ProfiShark Manager on Windows, launch the setup utility located in the "\Windows\Installer\" folder of the USB flash drive. Uninstall any previous version of the ProfiShark Manager before starting the setup utility.

1. Allow the installation to proceed when prompted by Windows User Account Control, and follow the on-screen instructions.
2. When prompted, disconnect and reconnect the ProfiShark 10G.
3. Wait for the installation to complete.
4. Launch the ProfiShark Manager via the shortcut created in the start menu.

To install the ProfiShark Manager on Linux or macOS, follow the instructions in the Installation.txt file located on the USB key or in the latest "ProfiShark USB key" release located in the Resource Center at www.profitap.com/resource-center/

For the ProfiShark 10G to be ready to analyze traffic, take the following steps (any order):

- Launch the ProfiShark Manager.
- Launch the software network analyzer.
- Connect the network to be monitored to the ProfiShark 10G using copper or fiber optic SFP/SFP+ and cables.
- Connect the ProfiShark 10G to the computer, using the supplied USB 3.0 cable.
- If copper SFP/SFP+ modules are being used, connect either the supplied USB to DC power cable or a compatible 5V/1.5A power supply to the ProfiShark 10G, to ensure the required amperage is being supplied to the unit. In the absence of an additional power connection, the ProfiShark 10G is powered through the USB 3.0 port alone and can only sustain fiber optic SFP/SFP+ modules .

> ► ***NOTE:*** Connecting to a USB port of lower specification than USB 3.0 may result in insufficient powering, as well as data drops due to bandwidth limitations.
>
> ► ***NOTE:*** Connecting the ProfiShark 10G to a different USB port than the one used during the installation requires a reboot of the computer (with the ProfiShark connected) for automatic driver installation for this USB port, and proper handling of the interface by Windows.

4. ANALYZER INSTALLATION

All industry standard analyzers are supported and can be used to perform the analysis. A comprehensive list of compatible analyzers are listed on the ProfiShark 10G product page at: www.profitap.com

Wireshark is recommended, and can be downloaded at: www.wireshark.org

To start capturing network data, launch the preferred network analyzer and select the new network interface named "ProfiShark 10G Device".

MONITORING GUIDE

1. PROFISHARK MANAGER

ProfiShark Manager is a standalone application designed and developed by Profitap. It provides means for statistical analysis of a network prior to a deeper investigation using an analyzer. It also provides options for port diagnostic, port control, timestamping, and traffic capture.

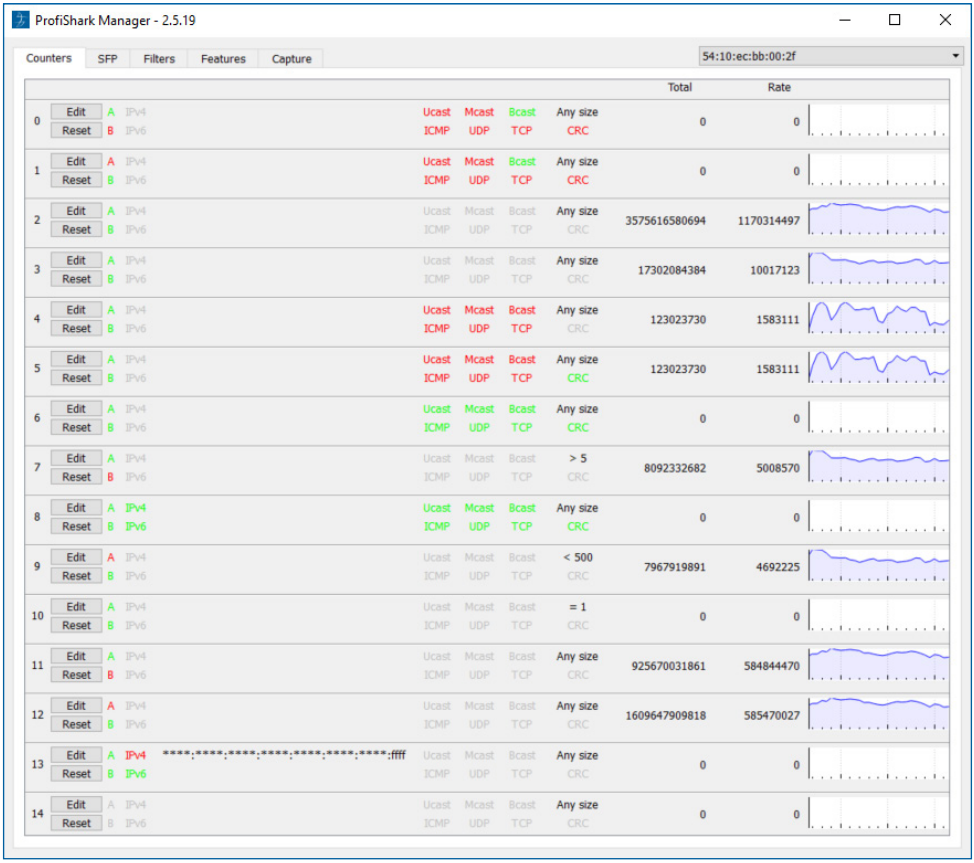
A built-in utility allows flashing the firmware and updating the device online or using a locally stored file. ProfiShark Manager can be used simultaneously with a software network analyzer, without the need to interrupt data capture.

ProfiShark Manager functionalities are grouped in the following tabs:

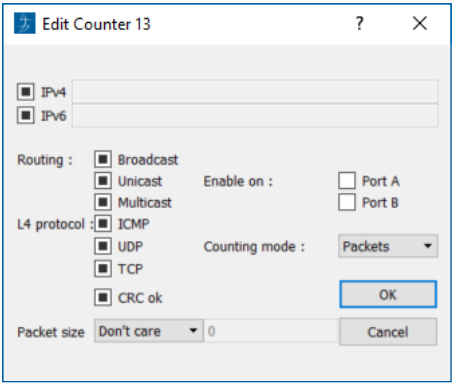
- Counter Tab
- SFP Tab
- Filters Tab
- Features Tab
- Capture Tab

1.1 Counters Tab

The *Counters* tab displays 15 customizable ProfiShark 10G counters for both SFP+ ports. Each counter can be configured to register packets matching a specific filter when passing through either SFP+ module.



EDIT	Opens the configuration window for this counter.



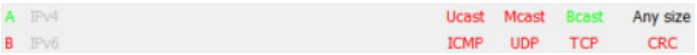
- ■ The counter ignores that frame characteristic. These frames will show in the counter.
- □ The counter filters out the matching frames. These frames will not show in the counter.
- ☑ The counter only counts the frames matching this specific filter.

IPv4 / IPv6: If checked, only packets originating from or destined to the specified IPv4 / IPv6 address will be taken into account.

Packet size: If different than *Don't care*, only packets with a size matching the configured filter will be taken into account.

Enable On: Depending on the selection made here, only packets passing through either Port A, Port B, or both ports, will be taken into account.

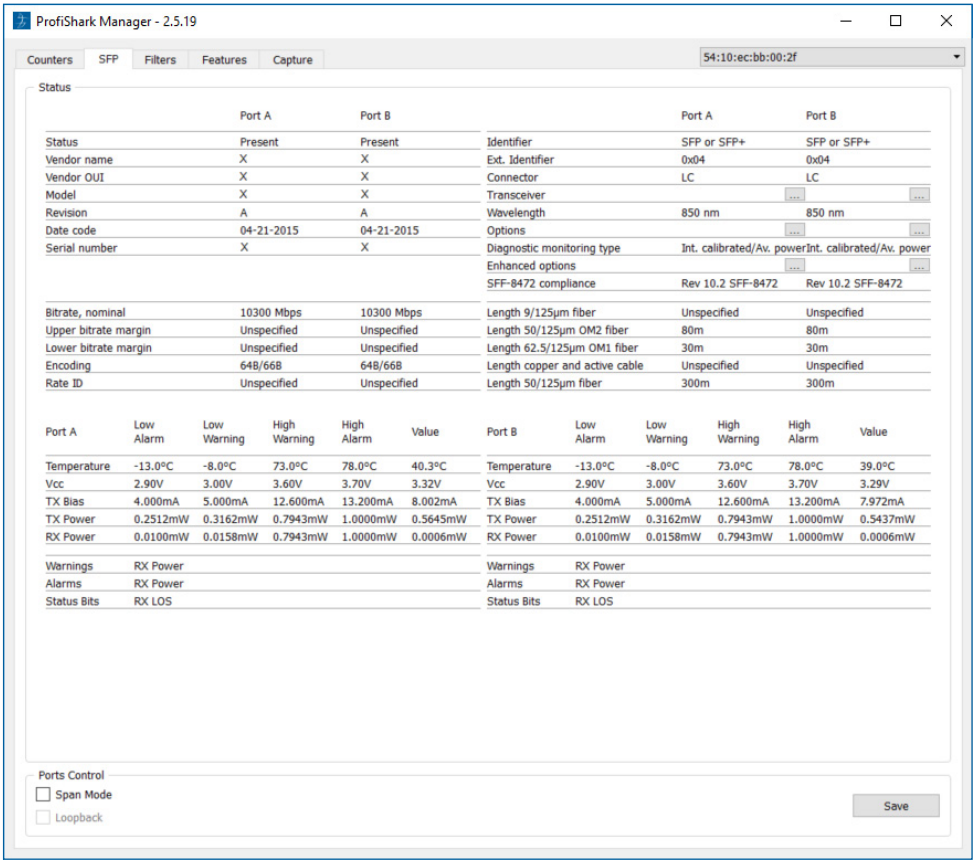
Counting mode: The *Total* and *Rate* figures can be displayed in either bytes or number of frames.

EDIT	► **Note:** If multiple filter fields are configured, only packets matching all filters will be counted.
RESET	Resets the *Total* figure for this counter. Does not reset the configured filters for this counter.
MATCHING FILTER	 This area displays the matching filters for each counter, displaying in red (▣) for ignoring, green (☑) for taking into account, and grayed out (☐) for filtered out frames. The frame size is always displayed in black.
TOTAL	Displays the total amount of packets or bytes matching the configured filter.
RATE	Displays the current rate of packets or bytes per second matching the configured filter.
CHART DISPLAY	Displays traffic statistics in a graphical representation of the frames matching the configured filter.

1.2 SFP Tab

The *SFP* Tab provides real time information about the connected SFP+ modules, offering an overview of their general capabilities and real time sensors.

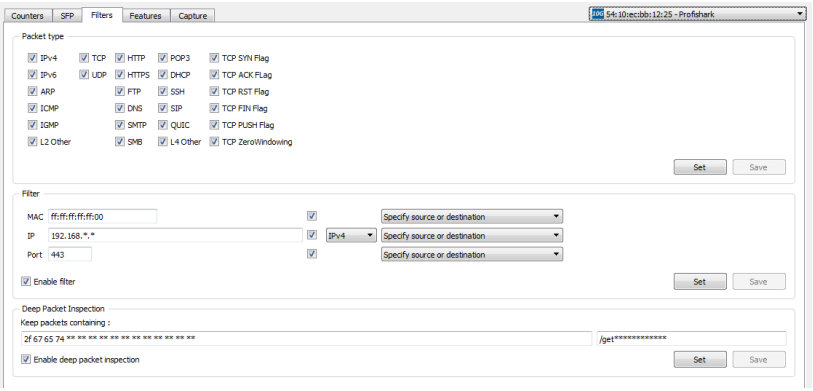
The *Ports Control* section allows the switching between SPAN mode and In-Line mode. In SPAN mode, traffic is only received, on either or both ports. In In-Line mode, traffic is transmitted between both ports. A loopback option is also available.



1.3 Filters Tab

The *Filters* Tab gives access to the ProfiShark 10G's hardware filters and deep packet inspection (DPI) feature. When enabled, only the packets matching the criteria configured in these filters and DPI will be captured in *Live Capture* and *Direct Capture*.

These filters only affect the captured traffic; they do not interfere with the counters displayed in the *Counters* Tab.



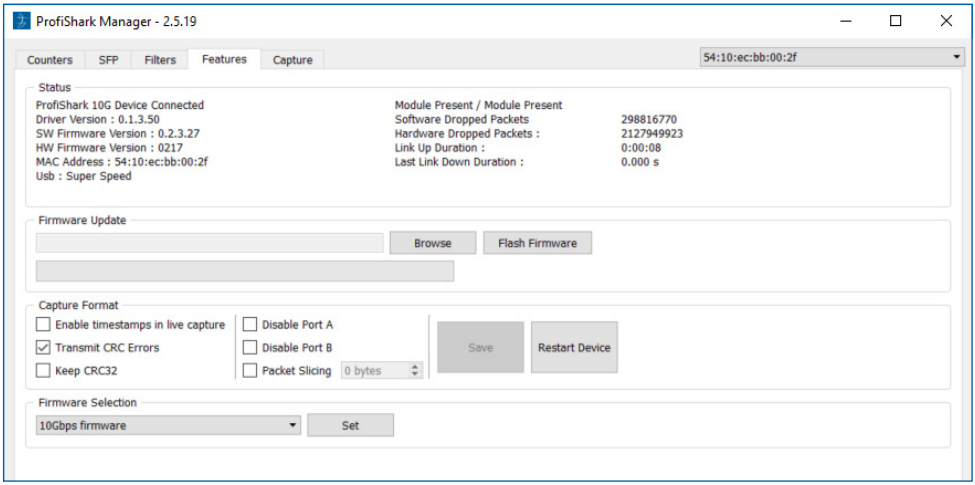
In the example above, the ProfiShark 10G has been set to capture only packets originating from or destined to any MAC address ending with 00, originating from or destined to any IPv4 address starting with 192.168, using port 443 for either incoming or outgoing traffic, and carrying matching DPI strings in their payload. The *Packet type* filter tells the ProfiShark which types of packets should be included in or excluded from the capture.

The DPI field allows users to search for a particular string (up to 16 characters in length) in the packets. This procedure is performed in real time, even at 20 Gbps. The left field accepts hexadecimal characters, while the right field accepts ASCII characters.

► ***NOTE:*** Not all hexadecimal characters can be displayed in the ASCII field.

1.4 Features Tab

The *Features* Tab contains information about the driver and firmware versions, port status, the firmware update utility, and options to enable or disable certain ProfiShark 10G features.



The *Feature* Tab is divided into 4 sections:

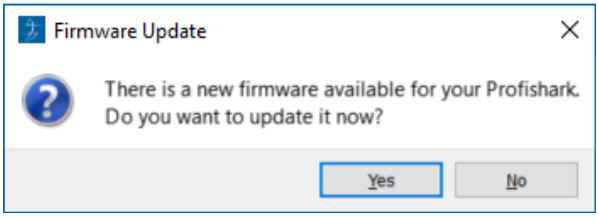
1. The ***Status*** section, displaying firmware, hardware, and network status for the connected ProfiShark 10G.

STATUS	
PROFISHARK 10G DEVICE CONNECTED	Lists the model of ProfiShark and its state: Connected, Disconnected, or Upgrading Firmware.
DRIVER VERSION	The version of the driver software currently communicating with the ProfiShark.
SW FIRMWARE VERSION	The version of the ProfiShark firmware currently loaded into the ProfiShark device.

HW FIRMWARE VERSION	The version of the logic board inside the ProfiShark device.
MAC ADDRESS	A unique identifier encoded into the ProfiShark device.
MODULE	The status of both SFP+ modules: Present, Not Present.
SOFTWARE DROPPED PACKETS	Represents the amount of packets dropped by the driver in *Live Capture* mode.
HARDWARE DROPPED PACKETS	Represents the number of packets dropped due to low USB Bandwidth, or when attempting a 10 Gbps capture without any configured filter.

2. The *Firmware Update* section, allowing users to flash the firmware of the connected ProfiShark 10G with a locally stored version. The ProfiShark 10G is unavailable during the firmware update process, which can take up to several minutes to complete. Once finished, the ProfiShark 10G may need to be replugged for the new firmware to take effect. Do not disconnect the USB port or shut the computer down during the update process. The latest firmware can be downloaded from the Resource Center at: www.profitap.com/resource-center/

► ***Note:*** The ProfiShark Manager will search for a new firmware release online every time it starts, allowing a new revision to be downloaded and installed, without the need of a locally stored update.



3. The *Capture Format* section, allowing users to enable or disable capture-related features. Additional customization of the capturing process is available in the *Capture* tab.

CAPTURE FORMAT	
ENABLE TIMESTAMPS IN LIVE CAPTURE	If checked, a Unix formatted timestamp is appended in the header of the packet data. This timestamp can be interpreted by the Profitap Wireshark dissector in *Live Capture* mode. For more information, see page 18.
TRANSMIT CRC ERRORS	If checked, the ProfiShark 10G will include packets with CRC errors in the capture. These packets are usually filtered out by network interfaces.
KEEP CRC32	If checked, the CRC32 information (32-bit Frame Check Sequence) located at the end of the packets will be kept in the capture. FCS can be interpreted in Wireshark (Edit \ Preferences \ Protocols \ Ethernet \ Assume packets have FCS).
DISABLE PORT A	If checked, frames from port A will not be captured.
DISABLE PORT B	If checked, frames from port B will not be captured.
PACKET SLICING	Enabling this feature will result in dropping the payload of every frame captured, keeping only the header information (the first 128 bytes) up to the application layer.

4. The *Firmware Selection* section, allowing users to switch between 10 Gbps and 1 Gbps firmware for the ProfiShark 10G, effectively altering the operating speed of the connected SFP+ modules.

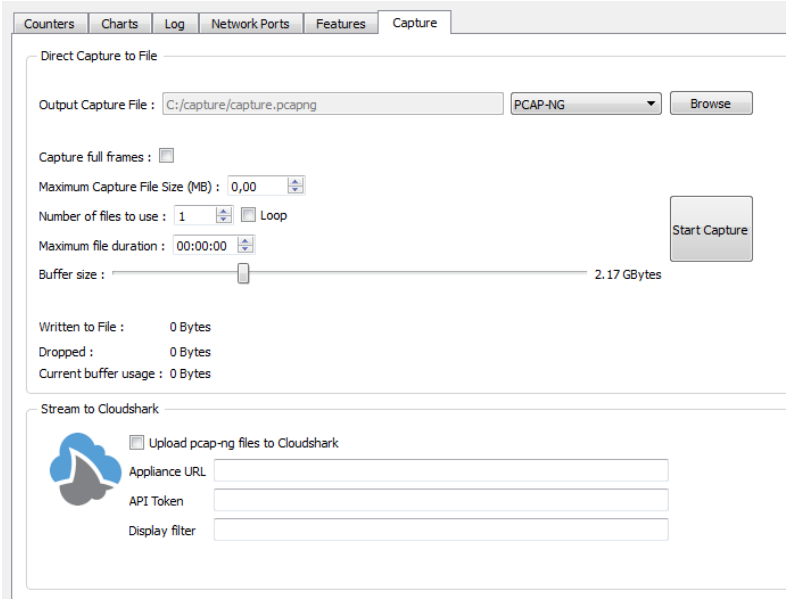
> ► Note: Switching between firmware versions takes between 4 and 8 seconds to complete, during which the network connection will be severed.

1.5 Capture Tab

1.5.1 Direct Capture Mode

ProfiShark 10G can capture traffic without the need for third-party capture software. This *Direct Capture* is performed at the driver level, prior to all network stacks and frame processing. *Direct Capture* provides the best performance, enabling small packet capture at wire speed.

The *Capture* tab contains the controls for the *Direct Capture* feature. The captured data is saved to a PCAP Next Generation file (.pcapng) with hardware-generated packet timestamps. ProfiShark Manager also provides an option for uploading capture files to Cloudshark.



OUTPUT CAPTURE FILE	Specify the name and location of the capture file. Name extension will be added to the specified name: (_#####_YYYYMMDDHHMMSS).
CAPTURE FULL FRAMES	Enable this option to capture the entire L1 Ethernet frames, which include the preamble (0x55), the SMD, and the CRC. This can be useful for TSN (Time-Sensitive Networking) capture.
MAXIMUM CAPTURE FILE SIZE	Sets the maximum file size allowed for storing the captured data. When the file size reaches this value, the capture either continues in a new file, or stops, depending on the other options.
NUMBER OF FILES TO USE	After reaching the configured maximum duration or file size, the captured traffic will be saved to a new file, until the number of files set here is reached.
MAXIMUM FILE DURATION	Sets the maximum duration for storing the captured data. When this value is reached, the capture either continues in a new file, or stops, depending on the other options.

LOOP	Enabling this option makes the capture overwrite the same file (or files, depending on the "Number of Files to Use" option) after reaching the configured maximum duration or file size.
BUFFER SIZE	In high bandwidth utilization scenarios, a bigger buffer size accommodates more data to be temporarily stored into the computer's memory before being saved to the file, helping to avoid captured data being dropped.
STATISTICS	◦ Written to File - Performance statistics. Displays the amount of data currently written in the output file, helping users determine the best buffer size. ◦ Dropped - Dropped bytes. Indicates the amount of data dropped during the capture, due to performance issues or buffer overflow. ◦ Current buffer usage - If dropped packets start to appear ("Dropped" statistic), increase the *Buffer Size* value.
UPLOAD PCAP-NG FILES TO CLOUDSHARK	Enable this option to upload capture files to Cloudshark automatically.
APPLIANCE URL	Set the appropriate URL of the Cloudshark server on which to upload the capture files.
API TOKEN	Set the appropriate token for the Cloudshark server set above.
DISPLAY FILTER	Optional display filter for the capture files uploaded to Cloudshark. Regular Cloudshark/Wireshark display filters can be set here. See: https://wiki.wireshark.org/DisplayFilters

► ***Note:*** The amount of dropped data depends on the data storage throughput and the amount of allocated memory buffer. Disk arrays or SSDs can drastically improve capture performance.

1.5.2 Live Capture Mode

ProfiShark 10G can also be used to capture network traffic and send it unaltered to a dedicated capture software. The process is transparent for packet size, packet type, and protocol. All tags and encapsulation are preserved (e.g. VLAN, MPLS, GRE).

> ► Note: Capturing traffic at high speeds is extremely CPU intensive and can cause software packet drops. For better performance, Direct Capture mode is recommended.

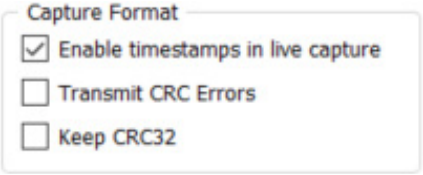
1.5.3 Live Capture Mode with Hardware Timestamping

The hardware timestamping feature can be used in both Live Capture and Direct Capture modes. It enables timestamp accuracy to the nanosecond, as opposed to the microsecond accuracy of software timestamping.

When using this feature in Live Capture mode, the ProfiShark Dissector for Wireshark must be installed for the hardware timestamping information to be properly interpreted by Wireshark.

The dissector files can be found on the provided USB key, or in the Resource Center at www.profitap.com/resource-center/

Hardware timestamping can be enabled from the Features Tab, by selecting "Enable timestamps in live capture".



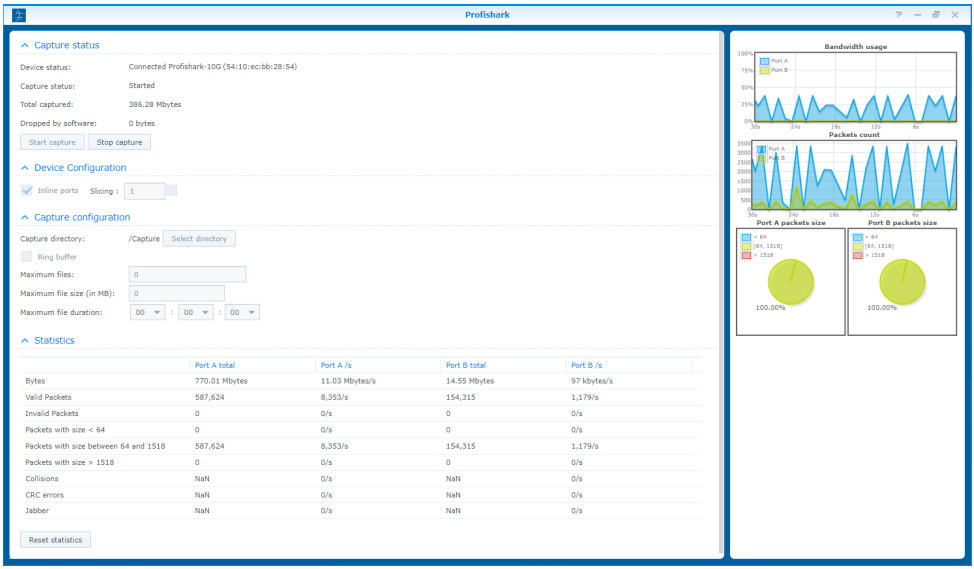
2. LONG TERM CAPTURE

The long-term capture feature expands the number of use cases for ProfiShark 10G. By combining the capture capabitilies of ProfiShark 10G with the storage capabilities of a NAS, it becomes possible to capture traffic for extended periods of time, making it easier to catch intermittent network problems in the act.

The ProfiShark USB key package (included with the product, and also available at profitap.com/resource-center/) provides packages for various Synology architectures.

Install the package corresponding to your Synology NAS. See the image file included in the packages folder for information on the type of CPU used in your Synology NAS.

For optimal capture results, an Intel-equipped Synology NAS is recommended.



DEVICE STATUS	Displays the connected TAP and its MAC address.
CAPTURE STATUS	Specifies whether the capture process is in progress.
TOTAL CAPTURED	Displays the total amount of data captured.
DROPPED BY SOFTWARE	Displays the amount of packets dropped due to performance issues or buffer overflow.
INLINE PORTS	By default, the ProfiShark 10G ports are set to In-Line Mode, meaning that devices connected through ports A and B can communicate. In this case, both ports are controlled at the same time. Unchecking "Inline ports" enables SPAN mode, setting the ProfiShark to intercept two separate data streams. In this case, communication between devices connected to ports A and B is severed, and ports A and B can be controlled independently in terms of speed, duplex mode, and autonegotiation.
CAPTURE DIRECTORY	Allows users to select the destination folder of the capture file.
RING BUFFER	If enabled, overwrites old data, using the circular buffer method of storing new data at the beginning of an existing data file.
MAXIMUM FILES	After reaching the configured maximum file duration or size, the captured traffic will be saved in a new file, until the number of files configured here is reached.
MAXIMUM FILE SIZE	This option sets the maximum file size allowed for storing the captured data. Exceeding this value will result in stopping the capture or storing the capture data in a new file.
MAXIMUM FILE DURATION	This option sets the maximum duration for storing the captured data. Exceeding this value will result in stopping the capture or storing the capture data in a new file.
STATISTICS	Displays ongoing and total traffic data for both port A and port B.

LEGAL

DISCLAIMER

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 thereof without obligation of the manufacturer to notify any person of such revision or changes.

COPYRIGHT

TRADEMARKS

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

PROFITAP HQ B.V. — High Tech Campus 84
5656AG Eindhoven — The Netherlands

sales@profitap.com
www.profitap.com

CE

RoHS compliant

FC