THE FUTURE OF PORTABILITY IN NETWORK MONITORING AND PACKET CAPTURE

PROFITAP

VISIT WWW.PROFITAP.COM

> *"Having a network TAP with you is one of the best ways to analyze your network for issues. Having a portable TAP is the best and fastest way to dive right into your network, parse the traffic on location and identify the packets creating all the trouble at the time of crisis."*

NETWORK MONITORING IN THE FIELD

This super connected world with its increasingly complex IT environment offers dozens of great possibilities for a business to grow and innovate.

But all of these came with a price, if you look at the security vulnerabilities the latest wave of ransom attacks just revealed. IoT exposed new ways for a cyberattack to infiltrate a network and cause great financial, business and reputation damage.

These days, you cannot be 100% sure your company won't be hit by a type of ransomware attack, at some point. But that doesn't mean you can't take all the necessary precautions so you are well equipped to fight attacks like these.

The security of your network must start from the inside of your IT infrastructure since network problems and security issues can happen especially when you least expect it. And when you are in the middle of such a network crisis, or better even, before the crisis, you need a network analyzer that is quick to deploy, fast to resolve, and powerful. In other words, you need quick and full visibility into what is happening on the network.

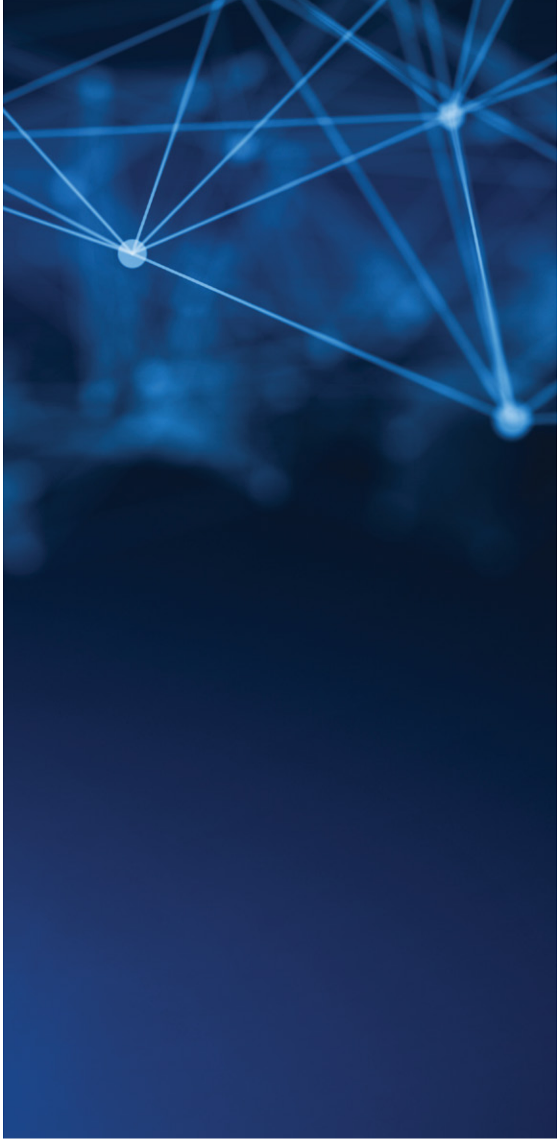
For a correct assessment of a problem on the network, it is important to see ALL the information that you can get. From there the information can be filtered and drilled down to the root cause of the problem. One of the best ways to achieve this is with a network TAP. Even the best network engineer cannot correctly assess the situation without 100% access to what is happening over the network.

Having a network TAP with you is one of the best ways to analyze your network for issues. Having a portable TAP is the best and fastest way to dive right into your network, parse the traffic on location and identify the packets creating all the trouble at the time of crisis.

Yet not all portable TAPs are as good as they sound. Some of them are powerful but complicated to handle. Some of them are easy to deploy but are not powerful enough to handle the entire traffic. Therefore, a portable TAP that is powerful enough to take on 100% of traffic, and simple and time efficient to deploy in the field, is the best tool to have.

Presently, in the field and on the market we see different versions of portable TAPs going around. The definition of what exactly portable is differs in the world of network monitoring. How can you navigate through this maze of choices and possibilities? What are the latest additions to the market and where do we go in the future?

In the following pages, we will give you an overview of the most common options in the market, together with their pro's and con's.



PORTABLE FULL-DUPLEX TAPS

Some manufacturers have introduced a basic version of their full-duplex TAP, and market it as their portable model. However these are small enough to cater to just one network link. Basically they are smaller versions of the rack-mount models and still contain rack-mount screw holders.

Being a full-duplex TAP, it does capture the traffic at full line-rate without any packet loss or timing delay. So the performance is there, but it is still difficult for an IT engineer to carry around a 'portable' TAP like this in the field, because additional hardware is required. (See figure 1)

A full-duplex TAP, or Breakout TAP, captures traffic streams from two network ports and copies them onto two 'output' or monitoring ports. This is what complicates things in the field. Besides the full-duplex TAP itself, you also need to have a lunch-box PC containing dual network-interface cards (NIC). In addition to this, the PC hosting the monitoring application would also have to perform interface- bonding or link-aggregation, to 'see' the two interfaces as one single stream of traffic.

This means double the resources, double the cost, and double the time required to start your network analysis. Let's accept it – you can't carry a desktop around in field locations, and neither do you have dual NICs in your laptop. (How many companies dish out dual-NIC high-performance laptops to their field staff anyway?)

As you can see, portability on paper and portability in practice are two very different things when it comes to network TAPs.

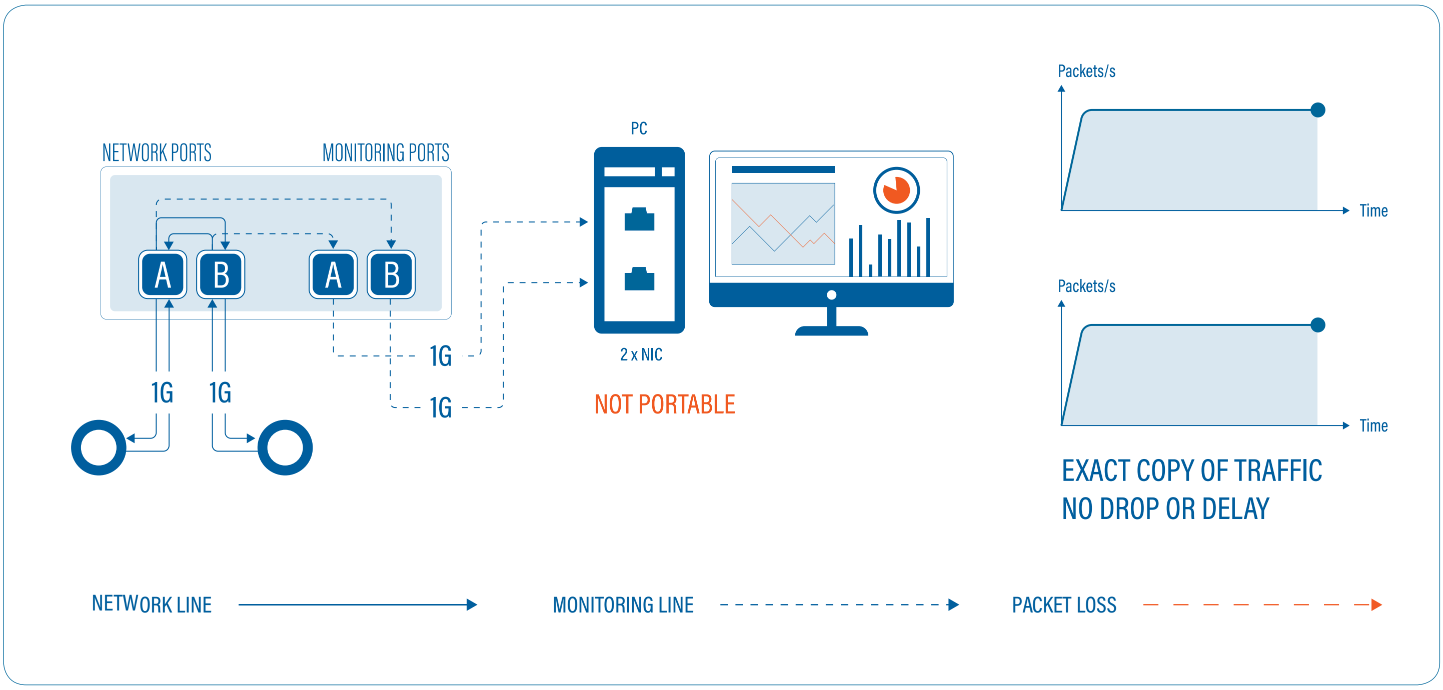
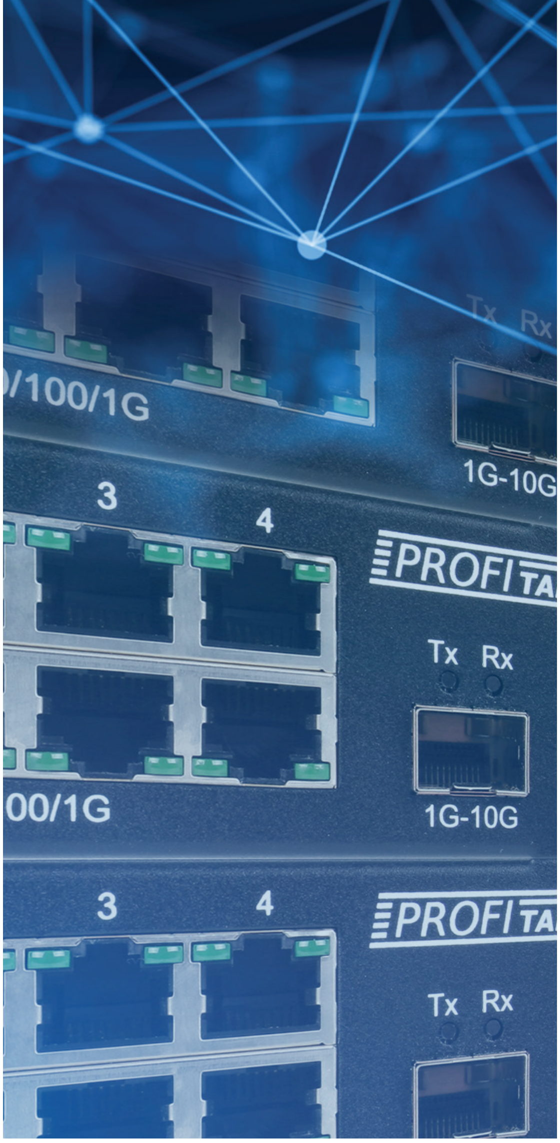


Figure 1: Schematic illustration of a Full-duplex TAP



PORTABLE AGGREGATOR TAPS

Another way TAP manufacturers address the issue of needing additional resources for full-duplex TAPs is by introducing Aggregator TAPs, also known as Aggregation TAPs. As the name suggests, an Aggregation TAP combines the two incoming traffic streams into a single flow of outgoing traffic. Hence there is a single monitoring port which receives the aggregated traffic of both network ports.

This resolves the need for dual NIC's in the analysis PC. In fact, it does away with the need of having a lunch-box PC altogether, making way for your laptop to be easily connected to the TAP. Portability at last, but at the cost of giving away performance.

If the input and output ports in a TAP are of the same data rate, then this itself could become a problem. We all know that network trunks today are of Gigabit rate (1 Gbps) at least. Therefore, to troubleshoot any of your network trunks, you have to place a TAP with Gigabit network ports. However, when the output – or monitoring port – is also a Gigabit port, then it will not be possible to completely transport 2 Gbps of combined traffic stream over a 1Gbps output. This means the traffic capture will be inconsistent. (See figure 2)

Aggregation TAPs use an internal buffer to aggregate the traffic and to cache the incoming packets to keep up with the speed of the output port. However, it depends on the size of the buffer as to how long can it sustain the flow of incoming packets before starting to drop them.

As soon as the network interface utilization shoots beyond 50%, and the buffer is full, your packets will start to fall off the bridge. As much as 50% of the total traffic could be lost if both the input network ports throttle traffic at its full capacity. Some aggregation TAPs have more memory to absorb data bursts, but it comes at the cost of a significant effect on packet timing, which is not suitable for analyzing real-time protocols.

The best way to overcome this bottleneck is to transport the aggregated traffic to a higher data rate output. It would not be feasible for TAP manufacturers to use a 10GE NIC as an output in a portable TAP. Furthermore, laptops do not possess 10GE NICs, and may not for some time. The entire point is to have portability and performance packed into one small kit.

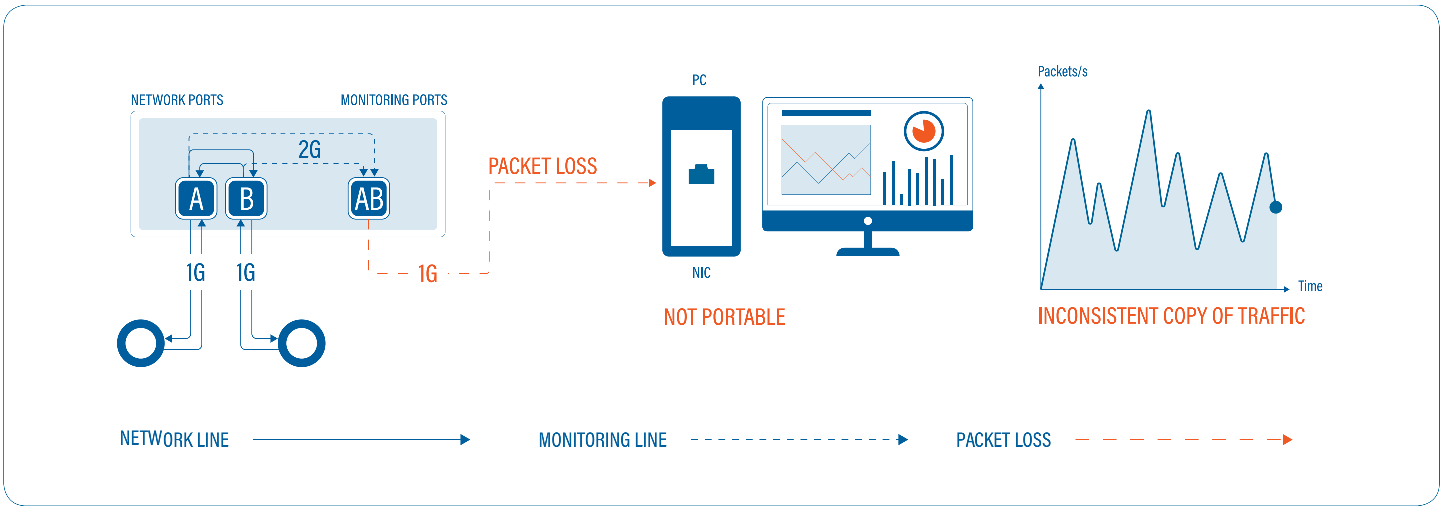


Figure 2: Schematic illustration of an Aggregation TAP

> *"Specially developed to deal with any kind of troubleshooting, in any field location, ProfiShark 1G is pocket-sized and power-packed. It works as an aggregation TAP, but does not cause bottlenecks of packet drop or time delay. With two Gigabit network ports, it seamlessly combines the two traffic streams into a single monitoring port."*

TRUE PORTABILITY WITH PROFISHARK

So, are there TAPs that give you full portability with the necessary performance? One of the latest developments in the world of portable network tapping is the ProfiShark series.

From the ProfiShark series, we will highlight the ProfiShark 1G for a fair comparison to the network TAPs that were mentioned earlier.

Specially developed to deal with any kind of troubleshooting, in any field location, ProfiShark 1G is pocket-sized and power-packed. It works as an aggregation TAP, but does not cause bottlenecks of packet drop or time delay. With two Gigabit network ports, it seamlessly combines the two traffic streams into a single monitoring port.

It does not use a Gigabit NIC as the monitoring port. Instead, it utilizes the power of USB 3.0, which can transfer data at up to 5 Gbps. So it can easily transport 2 Gbps of aggregated traffic stream (1G each from ports A and B) over a USB 3.0 link. This means that the buffer memory doesn't need to drop any packets and does not have to store packets long enough to impact their timing. (See figure 3)

Since it connects to your laptop's USB port, it has a unique plug-&-play feature that it's not dependent on an external power source.

ProfiShark 1G captures and transfers packets directly to any host computer's disk. All packets are captured in real-time with nanosecond time-stamping at hardware level, on each packet as it enters the TAP. This allows real-time protocol analysis of captured traffic with nanosecond resolution.

TAPs nowadays go even further than giving you full access to a network line in a portable package, as they can now also be used as a long-term capture solution and accessed remotely.

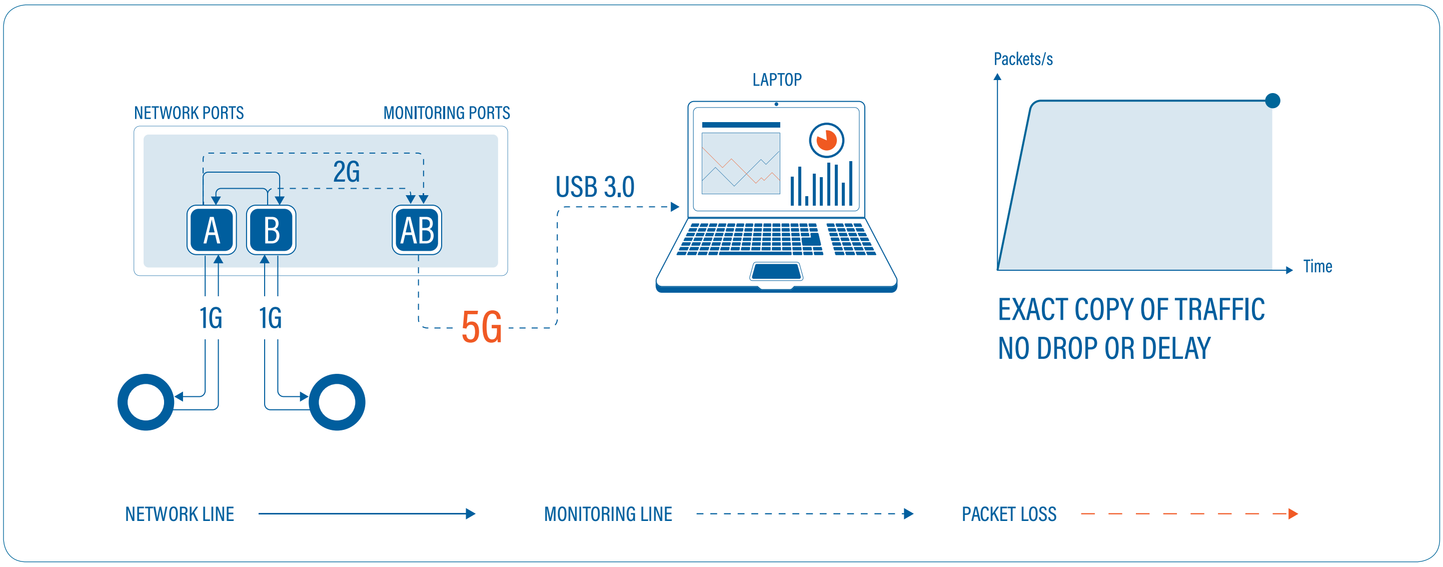


Figure 3: Schematic illustration of a ProfiShark 1G TAP

LONG-TERM CAPTURE WITH PROFISHARK 1G

Network engineers often find themselves in a troubleshooting scenario where the problems they are looking for only happen sporadically, making them impossible to reproduce. Catching intermittent problems can be very difficult and can take up a lot of space and time on your capture device. Wouldn't it be easy if you could just start a capture, let it run until the problem occurs, and analyse the capture files at a later point in time?

Of course, it's still important to know what you are looking for specifically, so you don't have to dig through Gigabytes or even Terabytes of information to find the packets you are looking for. The ProfiShark helps you with clever hardware filtering and packet slicing capabilities.

Combined with a NAS with storage tailored to your specific needs, the long-term capture feature makes it the perfect tool to catch intermittent problems in the act, while remaining the most portable solution on the market today.

> *"Combined with a NAS with storage tailored to your specific needs, the long-term capture feature makes it the perfect tool to catch intermittent problems in the act, while remaining the most portable solution on the market today."*

PROFI TAP

DISCOVER PROFISHARK

Go to: www.profitap.com/profishark ▶

IT ALL STARTS WITH VISIBILITY

Profitap develops and manufactures hardware and software solutions that help you get complete access and visibility into your network. These network visibility solutions are designed with the security, forensics, deep packet capture and network & application performance monitoring sectors in mind.

Profitap network solutions help eliminate network downtime, add security to existing and new networks all over the world, assist in lawful interception applications and reduce network complexity. All of Profitap's network monitoring tools are highly performant, secure and user-friendly, and provide complete visibility and access to your network, 24/7.

As we are experts in our field, we have developed our products set new standards in an industry where the definition of excellence is constantly being challenged.
With more than 1,000 clients from 55 countries, Profitap has become a must-have solution or many important businesses, many of which are among Fortune 500 companies.

PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS

sales@profitap.com
www.profitap.com

Profitap

@Profitap

profitap-international