PROFITAP

World's best and truly *portable* network TAP

When you are in the middle of a network crisis you need something that is handy, quick to deploy, fast to resolve, and yet powerful enough to counter the crisis. Network problems and security issues can erupt at any time. Especially when you least expect it. You don't want to deal with additional complexities or inaccuracies right at the moment when you already have a problem on your head to sort out. Having network TAPs with you is one of the best ways to analyse your network for issues. And having a *portable* TAP is the best *and fastest* way to dive right into your network, parse the traffic and get hold of the packets creating all the trouble at the *time* of crisis.

But not all portable TAPs are as good as they sound. Some of them are powerful but complex as well to handle. Some of them are easy to deploy but not powerful enough to handle the traffic fully. A portable TAP that is powerful enough to take on the full traffic, and yet easy to deploy on the field fast enough, is the right tool to have.

Before we introduce you to this right tool, let's first have a look at other portable TAPs available in the market and why they lag behind.

Portable Full-duplex TAPs

Some manufacturers have introduced a basic version, small enough to cater just one network link, of their full-duplex TAPs and market it as a *portable* model. The funny thing is that they are just smaller versions of their rack-mount models and still contain rack-mount screw holders. More of a desktop version you can say. Being a full-duplex TAP, it does capture the traffic at full line-rate without any packet loss or timing delay.

No doubt about that. But it comes at the cost of needing additional resources. And because of this an IT engineer would find it hard to carry around this *so-called* portable TAP on the field.

A full-duplex TAP, also known as a Breakout TAP, captures traffic streams from two network ports and copies them onto two 'output' or monitoring ports. This is where the complexity pops up. To utilise a full-duplex TAP you also need to have a lunch-box PC containing dual network-interface cards (NIC). On top of that, the PC hosting the monitoring application would also have to perform interface-bonding or link-aggregation to 'see' the two interfaces as one single flow of traffic stream.

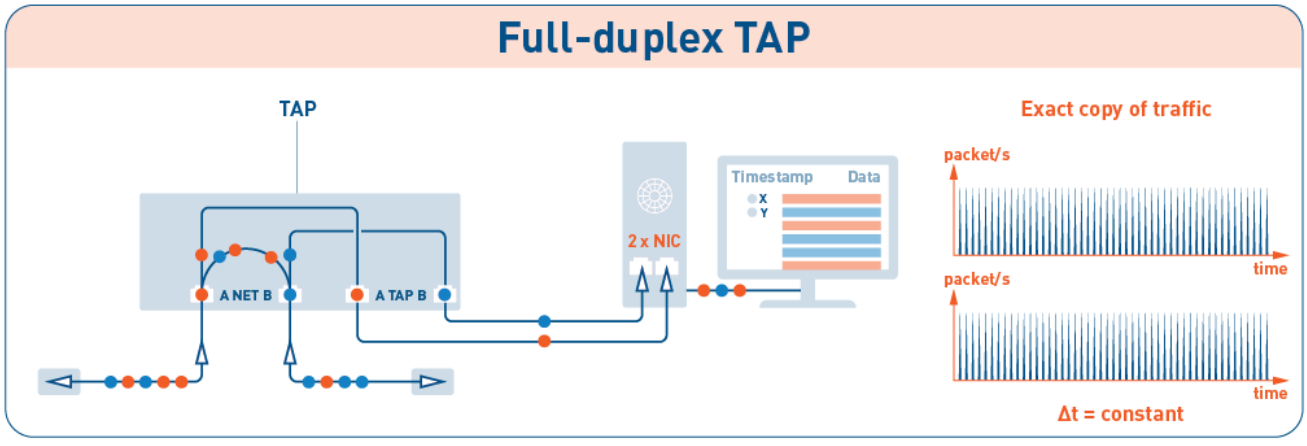


Figure 1: Schematic illustration of a Full-duplex TAP

This means double the resources, double the cost, and double the time required to hit the ground running. Let's accept it – you can't carry a desktop around in field locations, and you don't have dual NICs in your laptop as well. (How many companies can afford to dish out dual-NIC high-performance laptops to their field staff any way?)

Well, there goes the *portability* of your network TAP then.

Portable Aggregator TAPs

Another way TAP manufacturers went on to address the resource complexity of full-duplex TAPs was by introducing Aggregator TAPs. As the name reveals, an Aggregator 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 requirement of having dual NICs in the analysis PC. In fact it does away with the need of having a lunch-box PC in the first place, making way for your laptop to be easily connected to the TAP. Here comes the *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 could become a source of problem itself. For all practicality, we all know that network trunks today are of Gigabit rate (1 Gbps) at least. So to troubleshoot any of your network trunks, you would place a TAP having Gigabit network ports. And this is where the *performance* problem starts. If the output or monitoring port is also a Gigabit port, then it is not possible to completely transport 2 Gbps of combined traffic stream over a 1Gbps output. This means something has to be compromised.

Aggregator 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. But 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.

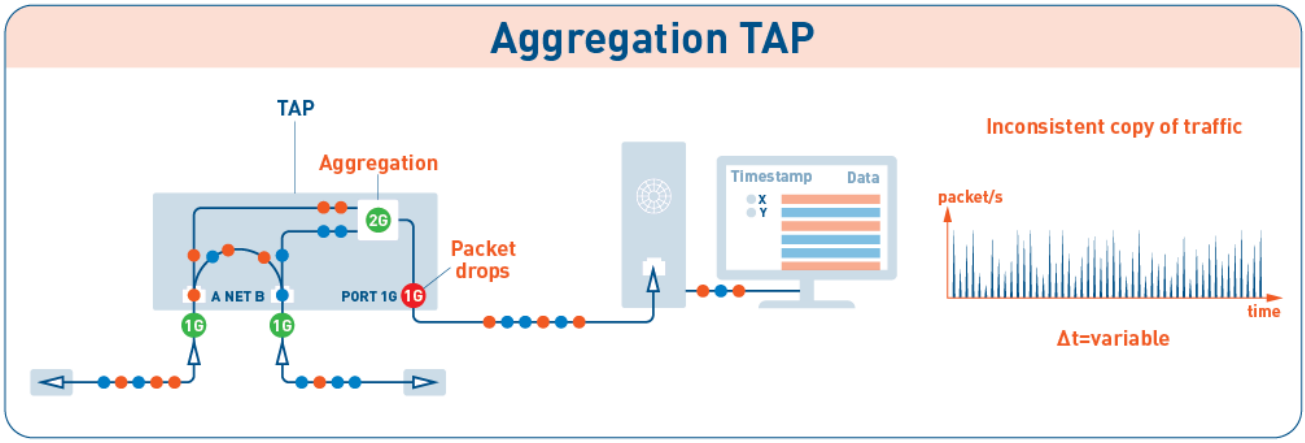
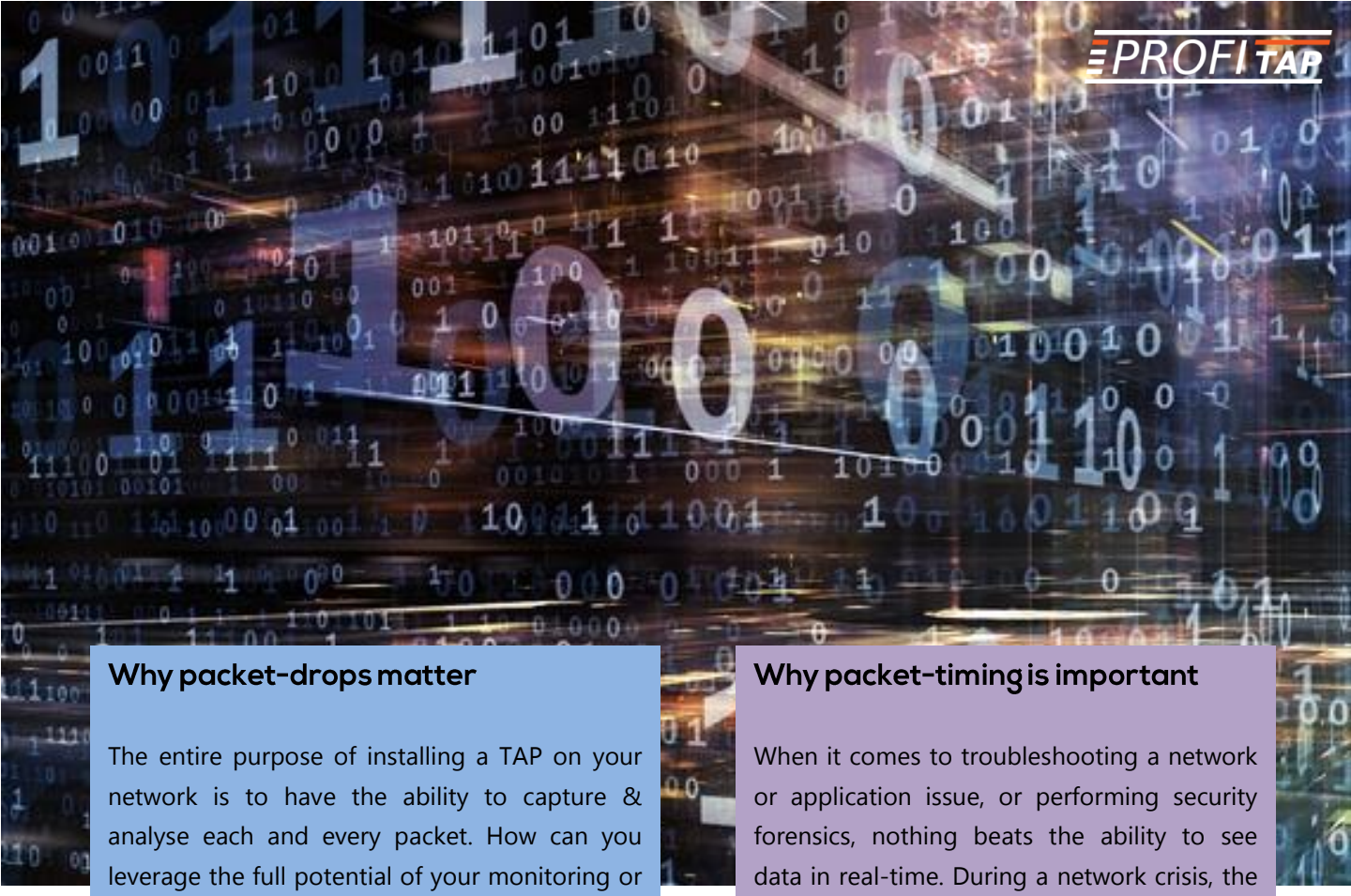


Figure 2: Schematic illustration of an Aggregation TAP

As soon as the network interface utilisation shoots beyond 50%, and the buffer is full, your precious packets would start to fall off the bridge. And as much as 50% of the total traffic could be lost if both the input network ports throttle traffic at its full capacity. Some aggregator 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 at all for analysing real-time protocols.

The best way to overcome this bottleneck is to transport the aggregated traffic to a higher data rate output. But it would not be feasible for TAP manufacturers to use a 10GE NIC as an output in a portable TAP. Plus, laptops are not going to have 10GE NICs anywhere in the near future. The entire point is to have *portability* and *performance* packed into one small kit.



Why packet-drops matter

The entire purpose of installing a TAP on your network is to have the ability to capture & analyse each and every packet. How can you leverage the full potential of your monitoring or security application if it does not receive some of the packets in the first place? Sure it is still going to receive some traffic. But what if the critical packets, e.g. the ones containing the application layer problem identifiers or a network intruder's signature, do not reach your analyser at all?

Some IT users seem to be settled with the fact that it is fine if a small number of packets (e.g. 10-20%) is not captured by their analyser. And that is where their practice is flawed. When it comes to traffic monitoring & analysis, you simply cannot afford to miss out any packet. On top of that, analysers would not be able to reconstruct actual network flows if there are packets missing in between. Thus they cannot show the true picture of what is happening on your network. And if you're not able to see the true picture, then your entire investment in having a TAP goes to waste.

Why packet-timing is important

When it comes to troubleshooting a network or application issue, or performing security forensics, nothing beats the ability to see data in real-time. During a network crisis, the network and system teams resort to their usual blame game in the absence of any correlation between network and server data that matches packet to packet response times. Having a monitoring application that is able to correlate the packets in real-time as it happens on the network is the key to ensuring timely resolution of problems.

Similarly, the difference between getting busted with a network penetration versus preventing the security issue in the first place is being able to detect & identify threats as it happens in real-time. Thus, the ability to capture packets from your traffic in real-time is a key factor to benefit from having a TAP on your network. Delayed delivery, or incorrectly timed packets, makes you lag behind in effectively identifying problems in your network in spite of having a TAP.

Meet world's best and truly *portable* network TAP

ProfiShark 1G

In comes the world's best, fastest and truly portable network TAP ready to hit the ground running for any kind of troubleshooting in any field location. **ProfiShark1G** is pocket-sized and yet power-packed. It works as an aggregator TAP but without the bottleneck of any packet drop or time delay. With its two Gigabit network ports, it easily combines the two traffic streams to transport over a single monitoring port. And it does not use a Gigabit NIC as the monitoring port. Instead, it utilises the power of USB 3.0.

USB 3.0 is the third major revision of the Universal Serial Bus standard that uses a new transfer mode, SuperSpeed, which can transfer data at up to 5 Gbps. Hence 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 doesn't have to store packets long enough to impact its timing.

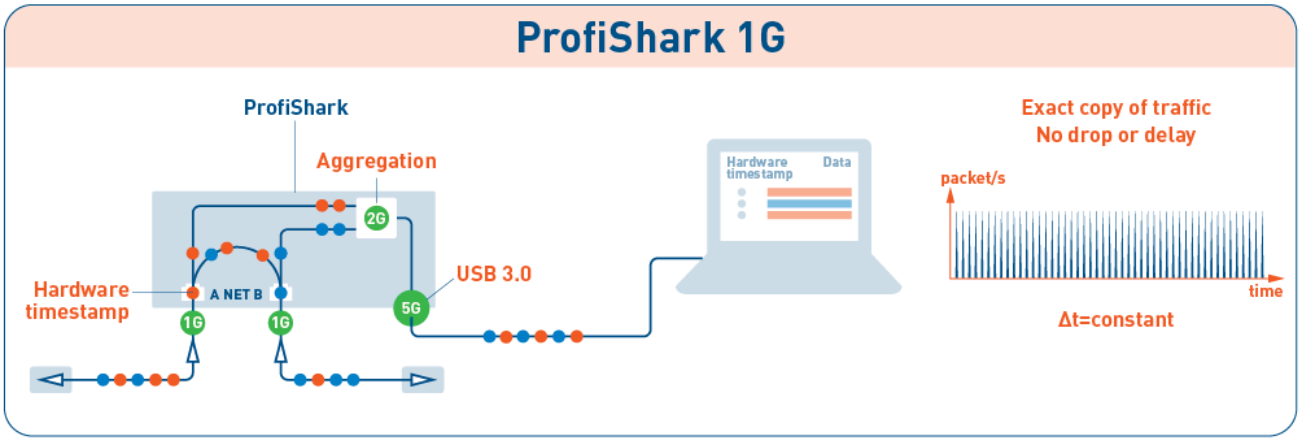


Figure 3: Schematic illustration of a ProfiShark 1G TAP

And because it can easily connect to your laptop's USB port, the best part of the plug-&-play ProfiShark1G is that it is not dependent on an external power source. Combined with a laptop, you have a truly portable and powerful troubleshooting kit ready to use at any location without depending on a power source.

The ProfiShark 1G captures packets and transfers 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.

Plus, it has the ability to capture any type of frame, be it VLAN, VXLAN, MPLS, etc., between 10 bytes and 10 Kilobytes. It also captures low level error frames, e.g. CRC errors, which makes it a perfect tool to perform troubleshooting at the lowest level as well. On top of that, ProfiShark1G is PoE (Power over Ethernet) compliant as well, allowing the network links to transport power to the network equipments without any hindrance.

Book a *date* with the ProfiShark1G

Please feel free to contact us to try a demo of the world's best and truly *portable* network TAP.

Profitap HQ B.V.
sales@profitap.com
+31 (0) 45-21 00 145