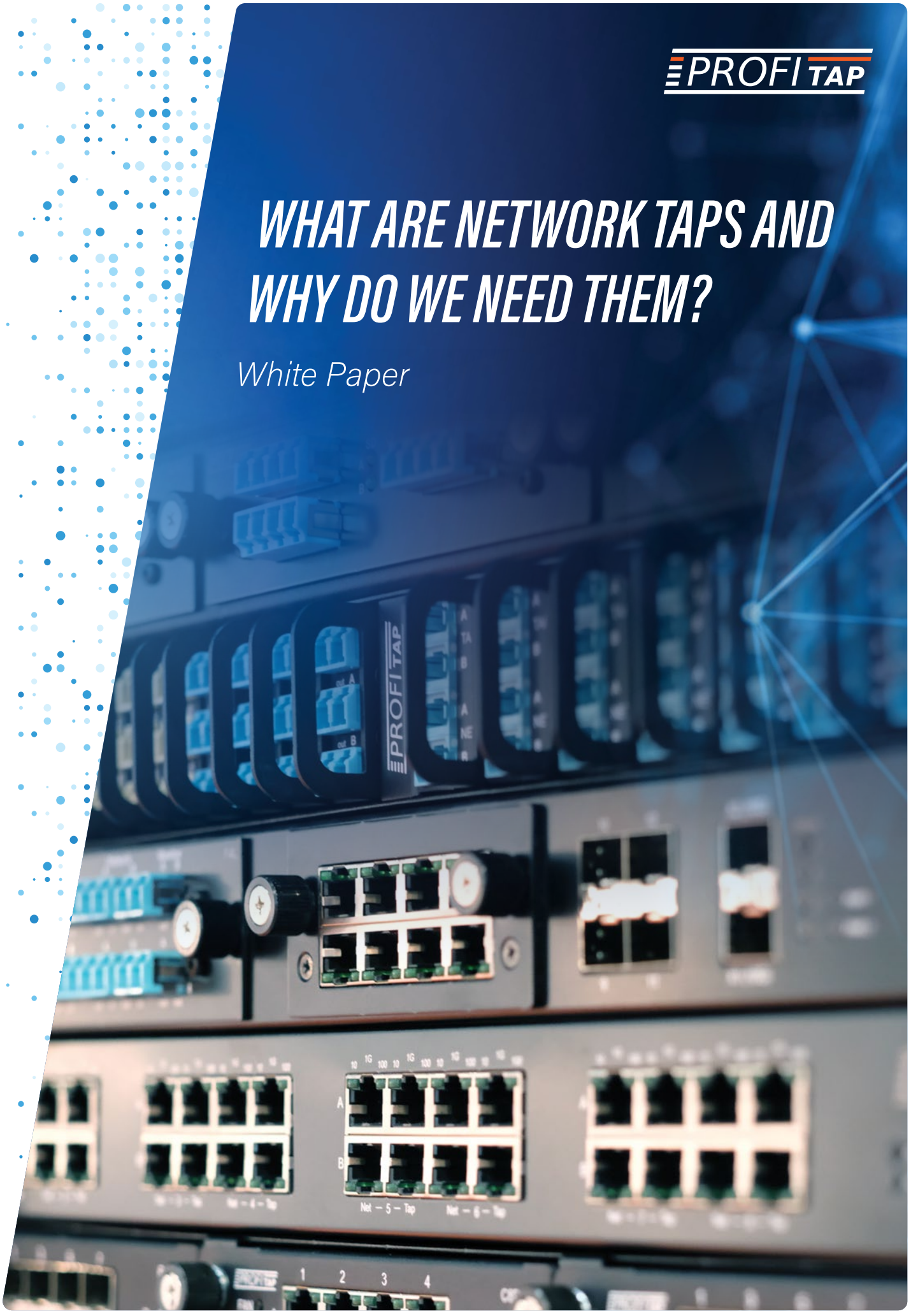
PROFI TAP

WHAT ARE NETWORK TAPS AND WHY DO WE NEED THEM?

White Paper



VISIT **WWW.PROFITAP.COM**

WHAT IS A NETWORK TAP?

When you think of the word tap, what comes to mind? Perhaps you imagine it to be a water tap or faucet on a sink for getting water or maybe the tap on a keg of Beer? If you are a well-seasoned traveler, you may know TAP is also the Logo for Air Portugal airline which technically is not a word.

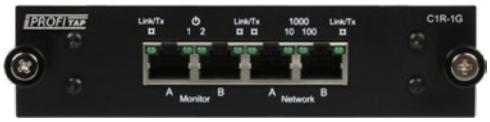


Figure 1: Network TAP

Well in our case, "TAP" is an acronym for "Traffic Access Point" or "Test Access Point" and is a hardware device inserted at a specific point in a network where data can be accessed for testing or troubleshooting purposes. They are mainly used to monitor the network traffic between two points in a network infrastructure.

Figure 2: Copper Network Link

A network TAP typically consists of four ports: a network port A and B and two monitoring ports A and B. The network ports collect traffic from the network. Network port A receives the Eastbound traffic and port B receives the Westbound traffic. The monitoring ports provide a copy of this traffic to an attached monitoring device. Monitor port A will copy the Eastbound traffic and monitor port B will copy the Westbound traffic.

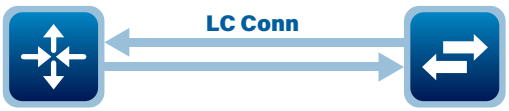


Figure 3: Fiber Network Link

Typically, a network TAP is placed between two points in the network. The network cable between points A and B is replaced with a pair of cables, which are then connected to the TAP. Traffic is passively routed through the TAP, without the network's knowledge. This allows the TAP to make a copy of the traffic, which is sent out of the monitoring port to be used by another tool without changing the network traffic flow.

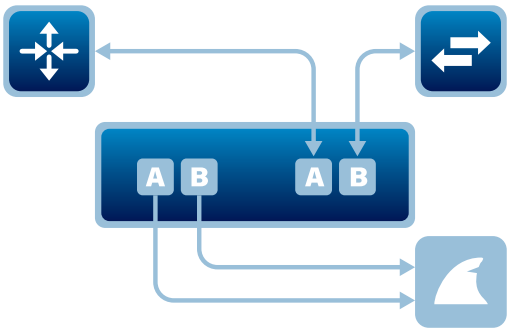


Figure 4: TAP inserted in a network Link

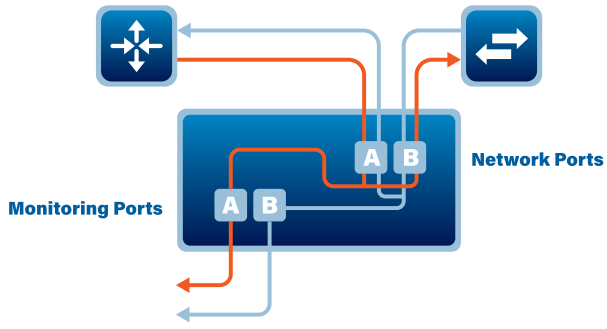


Figure 5: Network TAP traffic flow

WHY DO WE NEED A NETWORK TAP?

There are different methods for gaining access to your network. Some of the traditional methods used for gaining access to network traffic include using a SPAN/VACL port on your switch or connecting a monitoring device in-line on the network. There are challenges with both scenarios and are easily resolved with a TAP without introducing a point of failure.

The Network TAP (also known as a Breakout TAP) is the only TAP that will guarantee copying all of the network traffic, including errors, to the monitoring ports A and B. Monitor port A gets the Eastbound traffic and monitor port B gets the Westbound traffic.

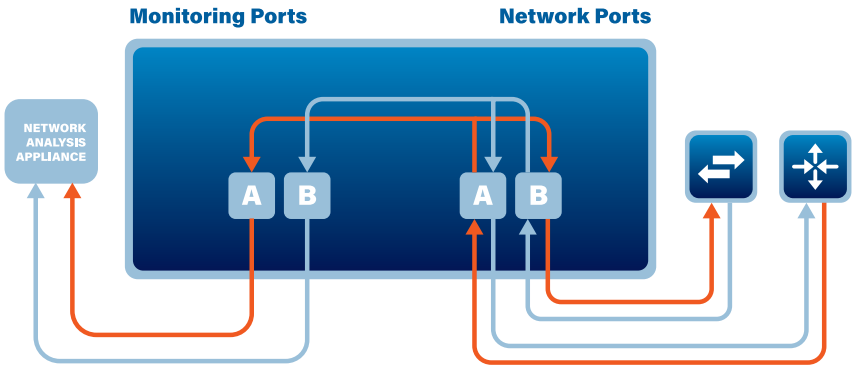


Figure 6: Network TAP traffic flow

Although the Network TAP is the TAP that lets you see all the traffic running through your network, there are other types of TAPs that can be used on a network. Two for when it is not important to see all of the traffic and one to be used with monitoring in-line devices like an Intrusion Prevention System (IPS).

Aggregating TAPs allow you to take the eastbound and westbound network traffic and aggregate it out to a single monitoring port. This will allow you to use just one monitoring port to see your eastbound and westbound traffic aggregated together on one monitor port.

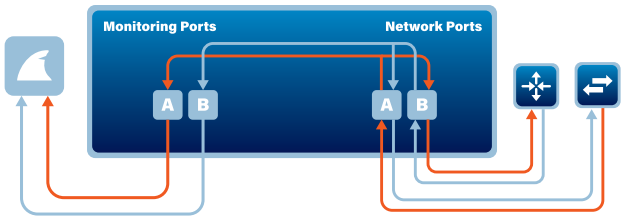


Figure 7: Aggregate TAP flow

SPAN/Regeneration TAPs will permit you to take unidirectional traffic from one network segment and send it to multiple monitoring tools. This allows you to send a single traffic stream to a range of different monitoring tools, each serving a different purpose.

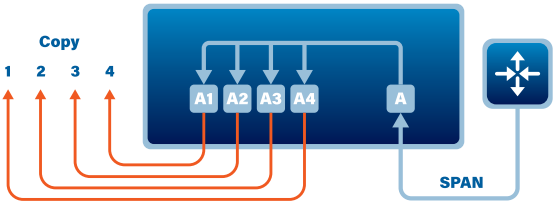
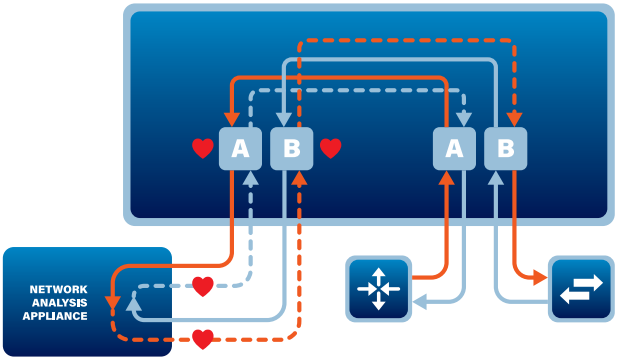


Figure 8: SPAN/Regenerating TAP flow

Bypass TAPs (also known as In-Line TAPs) allow you to place an active network tool "Inline" on your critical links. These TAPs are used where monitoring devices need to be placed inline on the network to be effective but putting these devices inline will compromise the integrity of a critical network. By placing a 'Bypass TAP' in place of the monitoring appliance and connecting the monitoring tool to the 'Bypass TAP', you can guarantee that the network link will continue to flow, and the in-line device will not become a 'point of failure'.



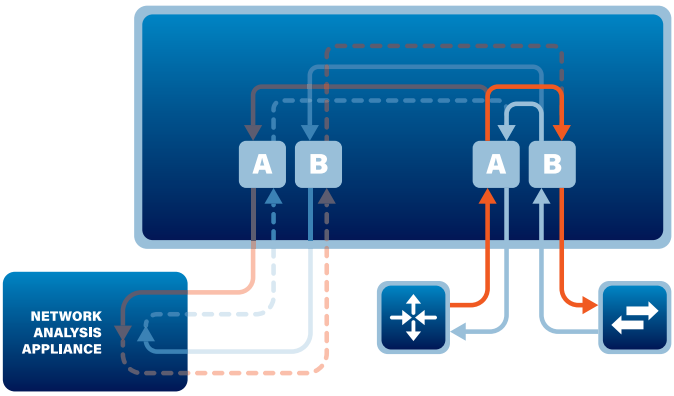
"As long as the monitor appliance is on-line, it will keep returning the heartbeat packets received from the TAP back to the TAP keeping the in-line appliance from becoming a point of failure. If the monitor appliance should go off-line for any reason the heartbeats will no longer be returned to the TAP causing the TAP to switch to the bypass mode. (See figure 10)"

Figure 9: Bypass TAP flow normal operation

There are different problems when a tool is installed in-line. Especially when dealing with a critical network, it is essential that the network is available all the time because down time can be very costly. When a device is installed in-line, the network must be brought down every time updates are required, or the tool needs to be re-booted. Similarly, if the monitoring tool fails, the network will go down as well.

These problems can be resolved by using a 'Bypass TAP'. When using an In-Line TAP, you will be guaranteed that every packet being sent from the network will get to the monitoring tool. Because these devices can never be over-subscribed, they always pass every packet including layer 1 and layer 2 errors.

The Bypass TAP when it is in its normal operating mode will keep critical traffic running through the in-line appliance and at the same time will send 'heartbeat' packets to the in-line appliance and as long as the in-line appliance passes the heartbeat packets back to the In-Line TAP the TAP will remain in the in-line mode. If the in-line appliance should go off-line for any reason, the In-Line TAP will stop getting the heartbeat packets. The In-Line TAP will switch to the by-pass mode until the TAP starts to receive heartbeat packets again which will indicate that the in-line appliance is back on-line.



"When the monitor appliance goes off-line for any reason, the heartbeat packets are no longer returned to the TAP causing the TAP to bypass the monitor appliance and keep the critical link running."

Figure 10: Bypass TAP flow in "Bypass" mode

PROFITAP

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 to 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