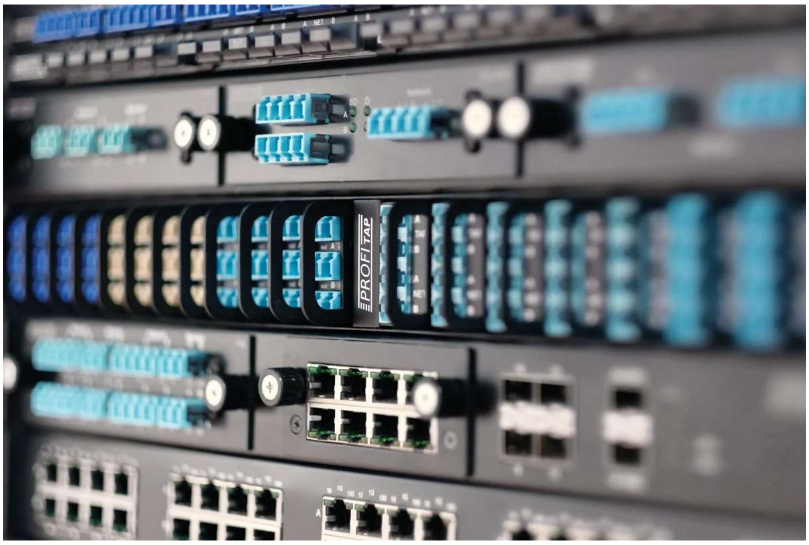
Exploring the Different Types of Network TAPs

by Profitap | May 30, 2017 | Copper TAPs, Fiber TAPs, Network Packet Brokers

In this article, we will delve deeper into the different types of TAPs and their passive and active solutions. In addition, we would also introduce a brief about Network Packet Brokers and their usability with TAP devices for added security.



To begin with, there are three types of TAP solutions. Each of these perform the same basic function of copying network traffic and sending that copy to any attached network traffic monitoring tool. What differentiates them is their ratio of network ports to monitoring ports.

> Network TAP (1:1) one-to-one ratio
> Aggregation TAP (M:1) many-to-one ratio
> Regeneration TAP (1:M) one-to-many ratio

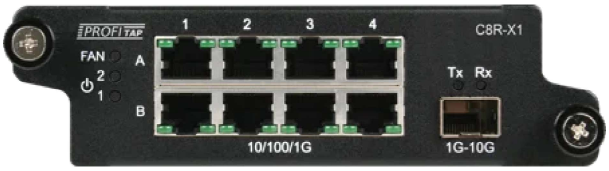
Network TAPs

The 1:1 ratio of a TAP means that each network port has a corresponding monitoring port. Often, the network ports will be labeled A and B, with their corresponding monitor ports also labeled A and B. In this system, segments of network traffic are copied and sent to a monitoring tool. This can be a single passive monitoring tool, or a network packet broker (NPB), which then sends the copied traffic on to several network monitoring tools, such as to the traffic analyzers, performance analyzers, traffic/packet capture systems, intrusion detection systems (IDS), or a network analyzer like Wireshark.

> This tools offer network engineers an easy solution to maximize visibility into the network, as they can be placed almost anywhere. Also, because they are passive TAPs, monitoring tools can be connected and disconnected from them, without interrupting the data flow.

To reduce the risk of having even the slightest impact on the network, some copper TAPs, such as Profitap copper TAPs, feature a “No Break” functionality, which has the capability to drastically reduce the fail-over time in the event of a power failure. It instantly resumes the link once power is restored. This is in contrast to SPAN ports, which as we've seen before, can affect the flow of network traffic negatively, even during normal operations.

Aggregation TAPs

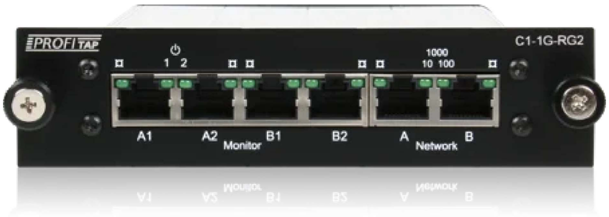


By contrast, aggregation TAPs connect MANY network ports to ONE monitoring port (M:1). This means that network traffic from multiple segments can be sent to a single network traffic analyzer. This is especially useful when that single monitoring tool has a limited number of ports. This type of ratio, however does have a potential downside, as packets may be dropped if the traffic exceeds the output bandwidth.

If, for example, you are using a 1Gbit/s aggregation TAP with a 1Gbit/s aggregated output link, the total bandwidth can be as large as 2Gbits/s when full duplex, over-burdening the TAP and leading to dropped packets.

Products like the Profitap Booster or the ProfiShark 1G can help avoid these dropped packets. For example, the ProfiShark 1G provides the capture output via USB3 cable with a total bandwidth of up to 5Gbits/s, easily handling the 2Gbits/s aggregated maximum of a 1Gbit/s full duplex link.

Regeneration TAPs



That crucial network segment’s traffic could then be monitored by an intrusion detection system (IDS), recorded for later forensic examination, captured for future use, or analyzed for performance issues. This type of TAP is useful when a critical segment needs to be monitored by an array of security and compliance tools simultaneously.

Passive vs. Active Network Monitoring Tools

The Intrusion Detection System mentioned above is an example of a passive monitoring tool. The traffic that is copied by the TAP and then sent to the IDS for analysis, terminates there and does not proceed any further. This type of tool is known as a 'passive' tool because the monitoring system does not alter the traffic and instead, issues alerts based on predefined criteria. Traffic flows into it and then stops.

Other security and performance tools are deployed inline, traffic flows into and then out of the device so that it can alter, or even block traffic, making them 'active' tools. A common example of this type of active security tool is the intrusion prevention system (IPS). Unlike the passive IDS, authorized network traffic constantly flows into and out of the IPS, while unauthorized traffic is stopped from proceeding further. Network engineers would determine the parameters of such unauthorized traffic, but it is most often security risks such as malware that they are seeking to block.

> TAPs can only support passive network monitoring tools such as the IDS. For active tools, you will need a Network Packet Broker (NPB) or a simpler Bypass TAP.

Bypass TAPs

Bypass TAPs and NPBs can support active inline network security and performance tools. Bypass TAPs were designed to avoid the "single point of failure" problem with other security appliances. In the event that the active tool fails, either due to a hardware malfunction, power loss, or software problem, a bypass TAP will keep the link flowing. This way it acts as a fail-safe point of access, for inline network monitoring tools.

> A Bypass TAP functions by sending heartbeat packets to the security appliance. As long as it receives them back, it will continue sending traffic to that appliance. If, for any reason, the security tool stops returning the heartbeat packets, the bypass TAP automatically bypasses that device to keep the link traffic flowing.

Paradoxically, this would seem to make the bypass TAP itself a single point of failure. However, should a bypass TAP fail for any reason, they would still be able to maintain any critical links, because they are designed to “fail open”.

Network Packet Brokers

The main function of a NPB is to filter specific network traffic to a specific monitoring tool, in order to optimize security and traffic flow. They are usually rack mounted and have copper or fiber inputs, and in many cases, both. By maintaining a many-to-many (M:M) port mapping of network ports to monitoring ports, they can then direct network traffic more efficiently. This enables network engineers to filter on actionable data only, which allows the network tools to analyze much more efficiently.

NPBs not only improve efficiency when it comes to traffic flow, but also help in speeding up incident analysis and in reducing response times. This is because NPBs provide network engineers the flexibility to direct that traffic exactly how they need. By using filters, they can also choose to receive the exact data required by the engineers.

> An efficient NPB, as is our own XX-1800 High-Density NPB, should provide true link layer visibility including port and time stamping. Other features would include filtering, load balancing, microburst buffering, and intelligent aggregation, all while maintaining high availability and resiliency.

Bypass TAPs are designed to "fail open" in order to maintain uptime. NPBs, on the other hand, "fail closed". Such a configuration is most often used to protect highly sensitive networks, as it terminates the network connection.

Which type of TAP you need will depend on what type of network you wish to monitor. Is it fiber or copper? In the case of fiber optics, which fiber type and connector type will you require? What is your network bandwidth? And, of course, how many lines do you need to monitor?

Hopefully, this quick overview will help you answer these questions and assist you in finding the right TAP solution to help keep your network up and running smoothly.

Tweet Like 38 Share

Recent Posts

- Inspecting affected clients of 3CX DLL sideloading attack with IOTA
- Profitap IOTA v3.0.0 Release Notes
- The advantages of ProfiShark for portable network traffic capture
- How to TAP 40/100G BiDi connections
- Profitap IOTA: Efficient analysis of VoIP issues

Categories

- Network Monitoring
- Insights
- Copper TAPs
- Fiber TAPs
- ProfiShark
- **see all**

Archives

- April 2023

February 2023

January 2023

December 2022

October 2022

see all

Stay up to date

First name

Last name

Email*

Profitap Insights covers all on network visibility, performance monitoring, troubleshooting, hardware, software, anything that brings clarity into networks. Anytime. Anywhere. If you don't want to receive the monthly email updates anymore, you can always unsubscribe.

Subscribe

Follow

Follow 237 people are following t

- 100M Copper TAPs
- 1G Copper TAPs
- 10G Copper TAP
- Gigabit Copper Port Replicator
- Dual Output Gigabit Copper TAP

Fiber TAPs

- High-Density Modular TAP
- Diode Fiber TAP
- LC Fiber TAPs
- MTP Fiber TAPs
- BiDi Fiber TAPs
- SC Fiber TAPs
- Regeneration TAPs

Virtual TAP

- Profitap vTAP

Centralized Management

- Supervisor

Aggregation TAPs

- Booster In-Line
- Booster SPAN

Bypass TAPs

- 1/10G Bypass TAP
- 40G Bypass TAP
- 4x10G Bypass TAP

Managing & Optimizing Data Flow

Network Traffic Aggregators

- XX-720G
- XX-1800G
- XX-3200G
- XX-12800G

Network Packet Brokers

- X3-Series
- X2-2000G
- X2-3200G
- X2-6400G

Traffic Capture & Analysis

Packet Capture & Analysis

- IOTA 1G
- IOTA 1G+
- IOTA 10G
- IOTA 10G+

Packet Capture

- ProfiShark 100M
- ProfiShark 1G
- ProfiShark 1G+
- ProfiShark 10G
- ProfiShark 10G+

Resource Center

Partner Portal

Product Updates

Knowledge Base

Blog

News

Academy

Accessories

Partner with Us

Tech Partners

Locate a Reseller

Our Story

Careers

Events

Professional Services

Contact Us

Get a Quote

Product Portfolio