PROFI TAP

TAP VS SPAN

THE MAIN DIFFERENCES BETWEEN PACKET CAPTURE USING NETWORK TAPS AND SPAN PORTS

VISIT WWW.PROFITAP.COM

CAPTURING TRAFFIC: TAPS VS. SPAN

When it comes to monitoring network traffic, there are two main choices if you don't want to stand directly behind the user as they go about their business. In the following pages we will give a general overview of a TAP (Test Access Point) and a SPAN (Switch Port Analyzer). For an in-depth breakdown, packet sniffing expert Tim O'Neill has several articles on lovemytool.com that delve into granular detail, but here we will take a much more general approach.

SPAN

Port mirroring, also known as SPAN or roving analysis, is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one or more port (or VLAN) of a switch to another port where the network traffic analyzer is connected.

SPAN is often used on simpler systems to monitor multiple stations at once. The exact amount of network traffic that this tool is able to monitor depends on precisely where the SPAN is installed in relation to the data center equipment. You might get exactly what you want to see, but you can easily wind up seeing much more than you need. Spanning an entire VLAN, for instance, can result in multiple copies of the same data. This makes LAN troubleshooting more difficult, and also impacts the speed of the switch's CPU or affecting Ethernet throughput tests.

Basically, the more you SPAN, the more likely you are to drop packets. The fact that SPANs can be managed remotely, unlike TAPs, means that changing the configuration is less time consuming, but still requires a network engineer.

SPAN ports are not a passive technology as some have claimed since they can have other measurable effects on network traffic including:

- Changing the timing of the frame interactions
- Dropping packets due to oversubscription
- Discarding corrupt packets without notification, hindering analysis

SPAN ports are therefore better suited to situations where dropped packets do not affect the analysis, or where cost is likely to be an issue.

TAPs

In contrast, TAPs require money to be spent upfront on the hardware, but as a bonus they do not require much setup. In fact, because they are passive, they can connect and disconnect to the network without affecting it. TAPs are hardware devices that provide a way to access the data flowing across a computer network, typically for the benefit of network security and performance monitoring tools. The monitored traffic is referred to as the "pass-through" traffic and the ports used for monitoring are called "monitor ports." For a greater visibility into the network, a TAP can be placed between the router and the switch.

Because they do not affect the packets, TAPs can be considered a truly passive way to view network traffic. There are basically three types of TAP solutions:

- Network TAPs (1:1 ratio)
- Aggregation TAPs (Many:1)
- Regeneration TAPs (1:Many)

TAPs copy traffic either to a single passive monitoring tool or, more often, to a high-density network packet broker that services multiple (often several) QOS testing tools, network monitoring tools, and network sniffer tools such as Wireshark.

Additionally, there are different types of TAPs depending on the type of cable, including fiber optic TAPs and gigabit copper TAPs. Both work in essentially the same way, splitting part of the signal off to the network traffic analyzer while the main signal continues on uninterrupted. For fiber optic TAPs, it is the light beam that is split in two, while in the copper system, the electrical signal is copied.

COMPARING THE TWO

To begin with, SPAN ports are not adequate for full duplex 1G links. Even under circumstances that seem to fall below their maximum capacity, they can quickly become overburdened and drop packets or simply because the switch prioritizes regular port-to-port date above SPAN port data. Unlike a network TAP, SPAN ports filter out physical layer errors, making some types of analyses more difficult, and as we have seen, incorrect delta times and altered frames can cause additional problems. TAPs, on the other hand, can run full duplex 1G links.

TAPs can also handle full packet captures and carry out deep packet inspections for protocol, non-compliance, intrusions, etc. Because of this, TAP data are admissible in a court of law as evidence whereas SPAN port data are not.

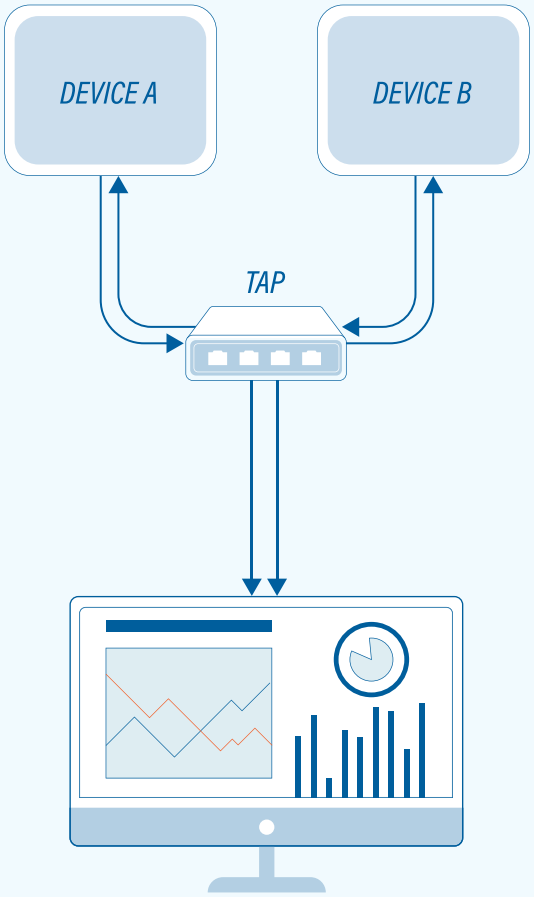
Security is another area where there are differences between the two technologies. SPAN ports are often configured for unidirectional traffic, but they can also receive traffic in some instances, creating a critical vulnerability. Conversely, TAPs cannot be addressed, have no IP address, and therefore cannot be hacked.

SPAN ports do not normally pass VLAN tags, which can lead to difficulties finding VLAN issues, but then TAPs cannot see the entire VLAN at once. TAPs don't give both channels in the same trace without the use of an aggregator tap, but you have to be careful regarding oversubscribing. There are some aggregating TAPs, like Profitap's Booster, for example, that can aggregate eight 10/100/1G ports to one 1G-10G output.

The Booster is able to insert VLAN tags to ingress packets. This way the source port information of each packet is forwarded to the analyzer.

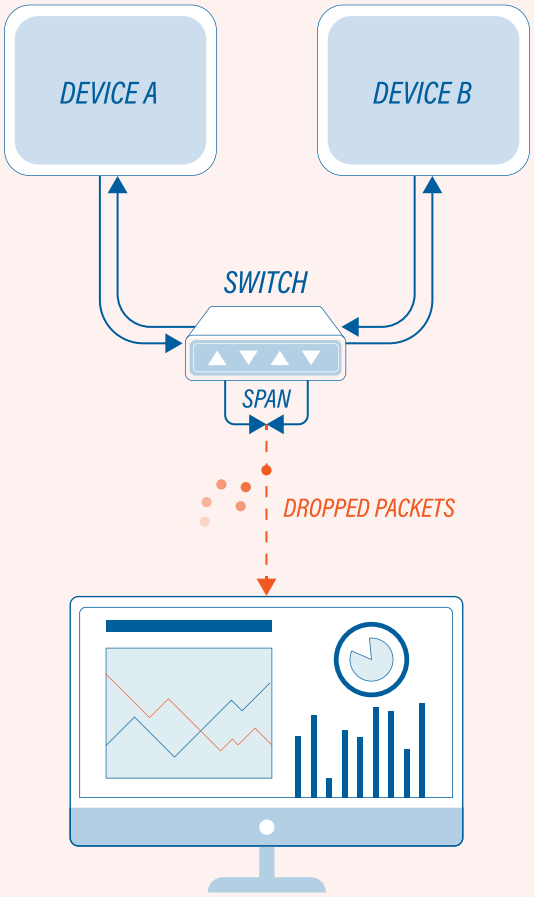
SPAN ports are still a useful tool for network administrators, but if speed and reliable access to all the network data are crucial, TAPs are the obvious choice. When deciding which approach to take, SPAN ports are better suited for lower utilized networks were dropped packets will not affect analysis or in situations where cost is a factor. On heavier traffic networks, however, the capacity, security, and reliability of TAPs will provide crucial full visibility into the traffic on your network without worrying that packets are being dropped or physical layer errors are being filtered out.

TAP



- *COMPLETE VISIBILITY*
- *COPIES ALL TRAFFIC*
  All packets of any size and type
- *PASSIVE, NON-INTRUSIVE*
  Doesn't alter the data
- *IN-LINE, DOESN'T USE SWITCH PORTS*
- *COPIES FULL-DUPLEX TRAFFIC AT WIRESPEED*
- *EASY TO SET UP*
  Plug and play
- *IMPERVIOUS TO HACKING*
  Invisible, isolates monitoring devices from the network, no IP/MAC address
- *SCALABLE*
- *SUITABLE FOR ANY SITUATION*

SPAN



- *PARTIAL VISIBILITY*
- *DOESN'T COPY ALL TRAFFIC*
  Drops packets of certain sizes and types
- *NON-PASSIVE*
  Alters packets' timing, adds delay
- *USES SWITCH PORTS*
  Each SPAN port uses a switch port
- *CANNOT HANDLE FULL-DUPLEX TRAFFIC*
  Drops packets if overloaded, may also interfere with main switch operation
- *REQUIRES CONFIGURATION BY ENGINEER*
- *NON-SECURE*
  Monitoring system is part of the network, potential security issues
- *NONSCALABLE*
- *ONLY VIABLE IN CERTAIN SITUATIONS*

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 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