

OT TAP vs SPAN

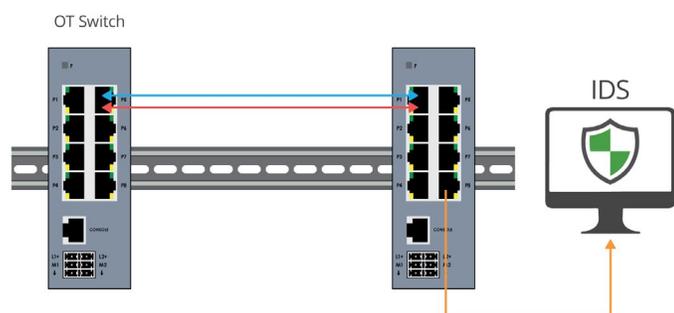
Solving Visibility Challenges within Critical Infrastructure

Securing and monitoring your network is the ultimate goal. But OT teams face complex challenges when it comes to architecting connectivity throughout large and sometimes aging infrastructure that wasn't initially designed with network security in mind.

There are two options to access network packets for security and monitoring solutions to properly analyze threats and anomalies, as well as performances and regulatory conditions — network TAPs and SPAN ports.

SWITCH SPAN PORTS

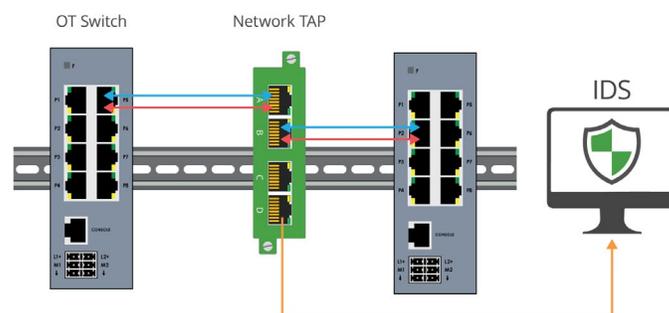
A common visibility use case is to route mirrored traffic from a SPAN port on the switch to a security or monitoring tool. Port mirroring also known as SPAN (switched Port Analyzer), is a designated port on a network switch that is programmed to mirror, or send a copy, of network packets seen on a specific port (or an entire VLAN), where the packets can be analyzed.



- Provides access to packets for monitoring
- SPAN sessions do not interfere with the normal operation of the switch
- Configurable

NETWORK TAPS

The industry best practice for packet visibility are network TAPs (Test access points). Network TAPs are purpose-built hardware devices that create an exact copy of the network packet data, continuously 24/7 without compromising network integrity.



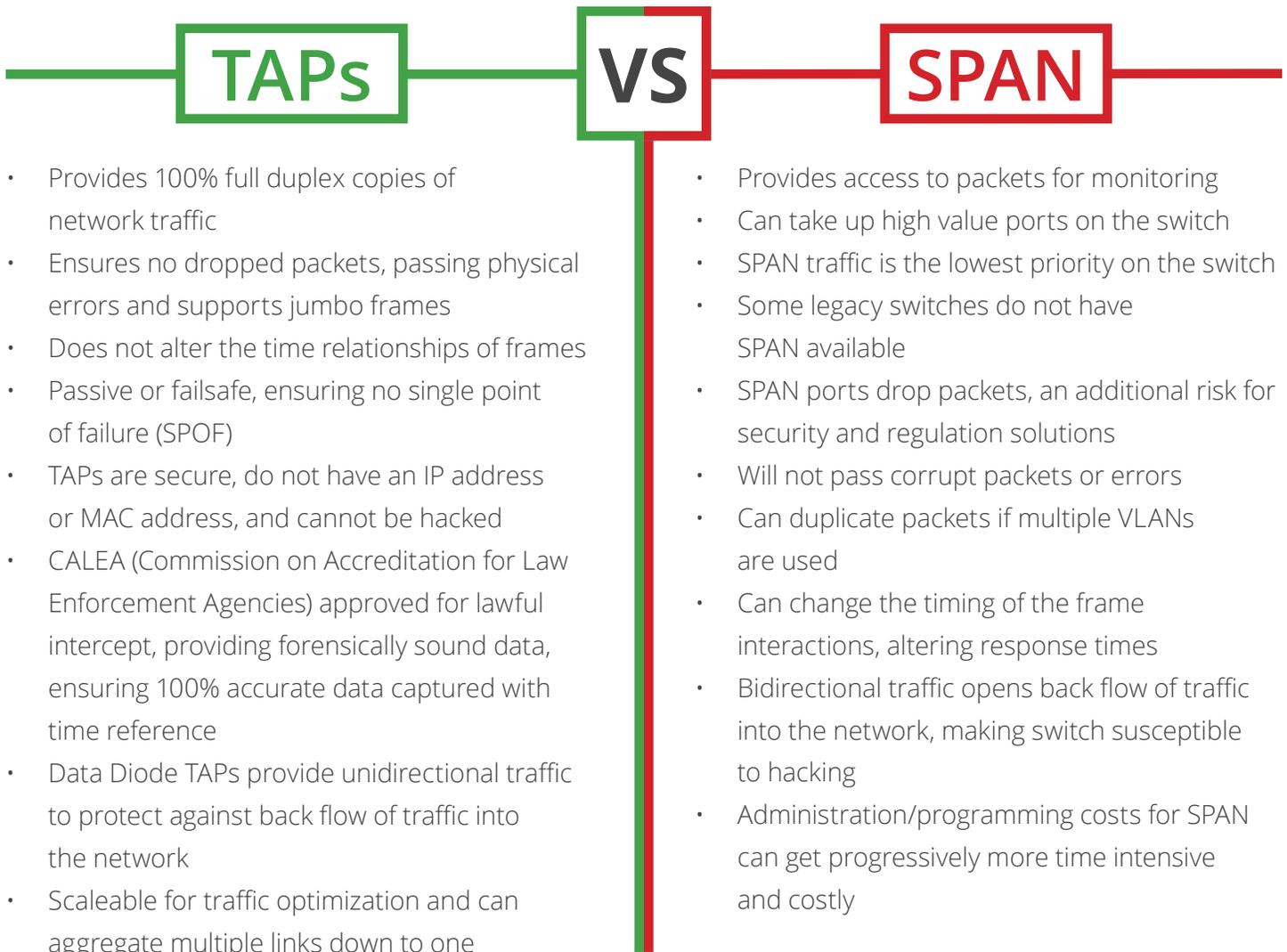
- Network TAPs make a 100% full duplex copy of network traffic
- Network TAPs do not alter the data or drop packets
- Network TAPs are scalable and can either provide a single copy, multiple copies (regeneration), or consolidate traffic (aggregation) to maximize the production of your monitoring tools



OT TAP vs SPAN

Solving Visibility Challenges within Critical Infrastructure

Determining where you use SPAN ports or network TAPs comes down to a multitude of issues. And many times a combination of both is a visibility architecture reality. But there are some significant differences which affect the integrity of the traffic that is being analyzed, as well as the performance of the network traffic. Let's review some of the pros and cons of each to help you decide what works best for your network.



Following critical infrastructure's guiding principles — you want your network to be built to last, while ensuring minimal to no network downtime. These concepts rest on the network infrastructure and visibility architecture. Being built by incorporating best practices are what's going to help you achieve these goals.

ADDITIONAL RESOURCES

TAP vs SPAN Webpage: garlandtechnology.com/tap-vs-span

ICS Visibility Solutions: garlandtechnology.com/it-security-and-visibility-solutions-for-industrial

