GARLAND TECHNOLOGY
See every bit, byte, and packet®

OT TAP vs SPAN

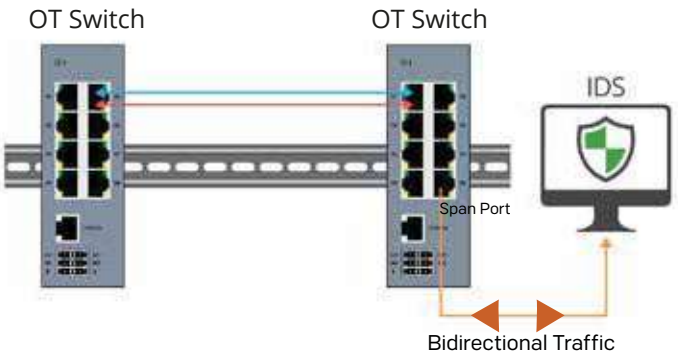
Solving Visibility Challenges within Critical Infrastructure

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

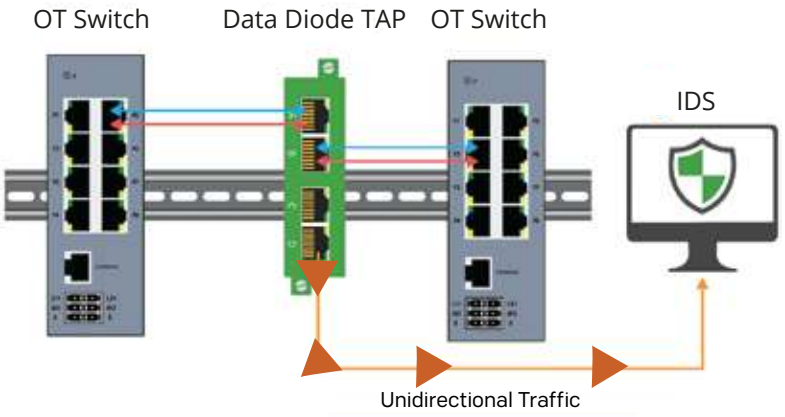
A common visibility use case is to route mirrored traffic from a SPAN port on the switch to a security or monitoring tool. Port mirroring also known as SPAN (switched Port Analyzer), is a designated port on a network switch that is programmed to mirror, or send a copy, of network packets seen on a specific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

GARLAND TECHNOLOGY
See every bit, byte, and packet®

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.

TAPs VS SPAN

- Provides 100% full duplex copies of network traffic
- Ensures no dropped packets, passing physical errors and supports jumbo frames
- Does not alter the time relationships of frames
- Passive or failsafe, ensuring no single point of failure (SPOF)
- TAPs are secure, do not have an IP address or MAC address, and cannot be hacked
- CALEA (Commission on Accreditation for Law Enforcement Agencies) approved for lawful intercept, providing forensically sound data, ensuring 100% accurate data captured with time reference
- Data Diode TAPs provide unidirectional traffic to protect against back flow of traffic into the network
- Scaleable for traffic optimization and can aggregate multiple links down to one

- Provides access to packets for monitoring
- Can take up high value ports on the switch
- SPAN traffic is the lowest priority on the switch
- Some legacy switches do not have SPAN available
- SPAN ports drop packets, an additional risk for security and regulation solutions
- Will not pass corrupt packets or errors
- Can duplicate packets if multiple VLANs are used
- Can change the timing of the frame interactions, altering response times
- Bidirectional traffic opens back flow of traffic into the network, making switch susceptible to hacking
- Administration/programming costs for SPAN can get progressively more time intensive and costly

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

Learn More
otd.salesgrp@onlineteknikdestek.com