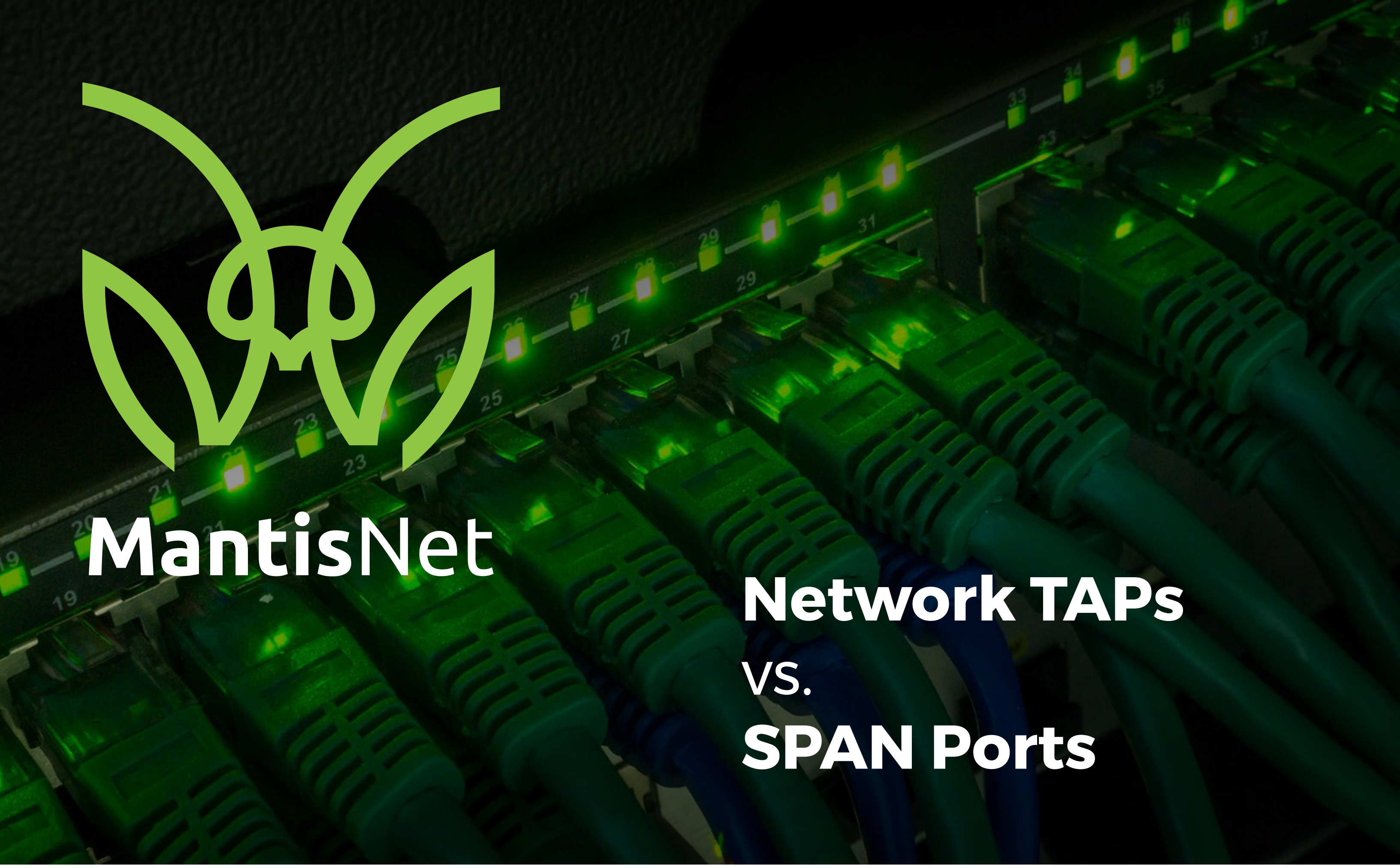
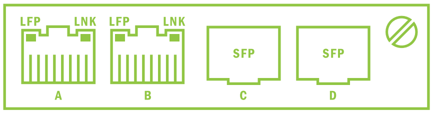


MantisNet

Network TAPs vs. SPAN Ports

TAPs



TAP (Test Access Point)

TAPs are used to passively copy 100% of traffic flowing on the network (both transmit and receive signals)

SPAN

SPAN (Switched Port Analyzer)

SPAN/Mirror ports send copies of traffic from one port (or group of ports) to another port for analysis

Features

	TAP	SPAN
100% PACKET CAPTURE?	Yes—TAPs capture every piece of information, does not drop packets	No—SPAN ports drop packets when they are oversubscribed. Data from a SPAN port is unpredictable—it is completely reliant on the available resources.
REAL TIME DATA	TAPs do not affect packets in any way, shape, or form—including relationship of frames, spacing, and response times	Can distort real time communications, such as VOIP
PASSIVE?	Yes—TAPs do not affect your network traffic, delivering a fully passive solution.	No—SPAN ports run on production switches and routers, and directly impact network traffic (to include dropped packets)
EXPOSURE TO HACKING	TAPs are they most secure piece of networking equipment- they do not have an IP or MAC address	High—SPAN ports are vulnerable to any threat once it has breached a network
FAIL SAFE?	Yes—network TAPs are 100% fail safe. If a TAP fails, or any application connected to the TAP fails, network traffic will continue to flow without impact	No—there is no fail safe
ACTIVE AND FAIL SAFE?	Yes—with the use of BYPASS TAPs. These TAPs allow you to flip a switch to go from passive/“out-of-band” to active/“in-line”. The TAP is 100% fail-safe while operating in either setting	No—see above

Background on the SPAN port

SPAN ports were originally created by networking equipment vendors as an afterthought to provide some data for testing and troubleshooting. SPAN/mirror port technology was never intended for large-scale network analytics...

...here are three excerpts from Cisco's own whitepaper on "Using the SPAN port for SAN Analysis":

"Cisco warns that the switch treats SPAN data with a lower priority than regular port-to-port data. In other words, if any resource under load must choose between passing normal traffic and SPAN data, the SPAN loses and the mirrored frames are arbitrarily discarded"

"Knowing that the SPAN port arbitrarily drops traffic under specific load conditions, what strategy should users adopt so as not to miss frames? According to Cisco, the best strategy is to make decisions based on the traffic levels of the configuration and, when in doubt, to use the SPAN port only for relatively low-throughput situations"

"Users should also be aware that the port cannot be flow-controlled by the destination (analysis) device, because flow-controlling the SPAN mirrored output would, as a consequence, push back the flow-controlling action to the actual network traffic. This design choice is a consequence of the decision by Cisco not to affect the original network traffic while it is mirrored. Therefore, mirrored data issued from the SPAN port must be captured as quickly as it is produced, or the mirrored data may be lost. This characteristic becomes important if the analyzer connected to the SPAN port requires flow control. Flow-control related loss is unpredictable and leads to poor analysis result"

Reference:
https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/san-consolidation-solution/net_implementation_white_paper0900aecd802cbe92.htm

Advantages of network TAPs

- TAPs provide access to 100% of your network traffic. They do not sample data
- TAPs do not alter the time relationships of packet frames, allowing for real time data analysis
- TAPs do not introduce any additional jitter or distortion to the network data
- TAP's have a limited scope—they do not have access to anything other than the LAN they are monitoring
- TAPs pass all information—VLAN tags are not passed through SPAN ports, leading to false issues detected and extreme difficulty in troubleshooting VLAN issues
- TAPs do not alter data or filter out errored packets
- TAPs do not alter or drop the interframe gap
- TAPs DO NOT DROP PACKETS, regardless of the bandwidth
- TAPs are completely passive and do not cause any distortion even on full bandwidth networks
- TAPs are 100% fault tolerant
- TAPs do not care if the traffic is IPv4 or IPv6, they pass all traffic through