Interface Masters
TECHNOLOGIES
Innovative Network Solutions

SPAN and TAP Explained

Introduction

In a basic network infrastructure, there are out-of-band monitoring devices such as probes, intrusion detection systems, network recorders and network analyzers. The traffic to these devices will come from network devices such as firewalls, routers and switches. It is common practice to have the out-of -band monitoring devices sit passively on the network as they are not modifying or altering any of the network traffic compared with inline devices such Intrusion Prevention Systems, which in some cases will alter the traffic.

There are two common approaches to deploying a passive device in an out-of-band fashion: connecting the device to either a Switch Port Analyzer (SPAN) or a Test Access Point (TAP). Both approaches will not affect the real network traffic and the out of band appliance can be connected and disconnected from the network without any downtime or disruption. Also, if the monitoring device fails for whatever reason, such as power failure or software malfunction, traffic will continue to flow on the network as usual. This whitepaper is going to focus on the differences between the two approaches for out-of-band network visibility, SPAN and TAP.

SPAN Explained

A SPAN port is configured via a network enterprise switch. SPAN is a dedicated port on a managed switch that takes a mirrored copy of traffic that a network administrator chooses off the switch to be sent to a monitoring device. One job of a switch during normal function is to eliminate packets that are below the minimum size and to delete corrupt packets. This means that hardware and media errors are dropped, so the out of band monitoring devices may not receive all true traffic. The switch provides high priority to Network traffic, while the SPAN port traffic gets lower priority, which in turn leads to dropping SPAN port traffic during peak time and the monitoring equipment will not get the complete information. Also, traffic on a SPAN port is constituted of the aggregate of RX (receive) and TX (transmit) traffic, and as a result the port can be oversaturated and packets may be dropped.

TAP Explained

A TAP is device that will passively split traffic coming from the network to the monitoring device. The TAP will receive both directions of traffic from the network, (Ingress and Egress) in real time to make sure all data is sent to the monitoring device. This traffic is coming on separate channels (RX and TX) so that both directions of traffic will be sent to the monitoring device. The TAP will also receive all traffic, as it is passive and will not modify the traffic before being sent to the device. As a result of this, there will be full visibility even if the network is 100% saturated. There are two variations of network TAP- Passive and Active.

Passive and Active TAP

A passive TAP is used mainly in fiber optic networks, where it receives traffic from both directions of the network and will split the incoming light so that 100% of traffic is seen on the monitoring tool (see TAP mode 1). The advantage of this TAP mode is that it does not need power to run, which adds to the layer of redundancy and minimized maintenance needed which reduces overall OPEX. An example of a Passive TAP would be an Interface Masters, Niagara 3225PT which is a highly dense and modular 25 segment fiber TAP, which can support 1G, 10G, and/or 40G networks and tools.

An active TAP has a similar mode to a passive TAP where traffic can be split so that ingress traffic is sent to one monitoring tool while egress traffic is sent to the other tool port. On the other hand Active TAP supports aggregation mode, which means the ingress and egress traffic can be aggregated together so you can run more monitoring tools per TAP. The advantage of Aggregation mode is that there are monitoring tools that only have one port for traffic coming in, so to be able to achieve full visibility of the network, the traffic would have to be aggregated. An Interface Masters, Niagara 3218 is a 10G active TAP that has four segments and can support up to 8 monitoring tools. The active TAP regenerates the signal opposed to the passive TAP where there is loss the light intensity. Interface Masters also provides active TAP systems where both the network and appliance ports are able to regenerate the signal and as a result provide a better quality signal.

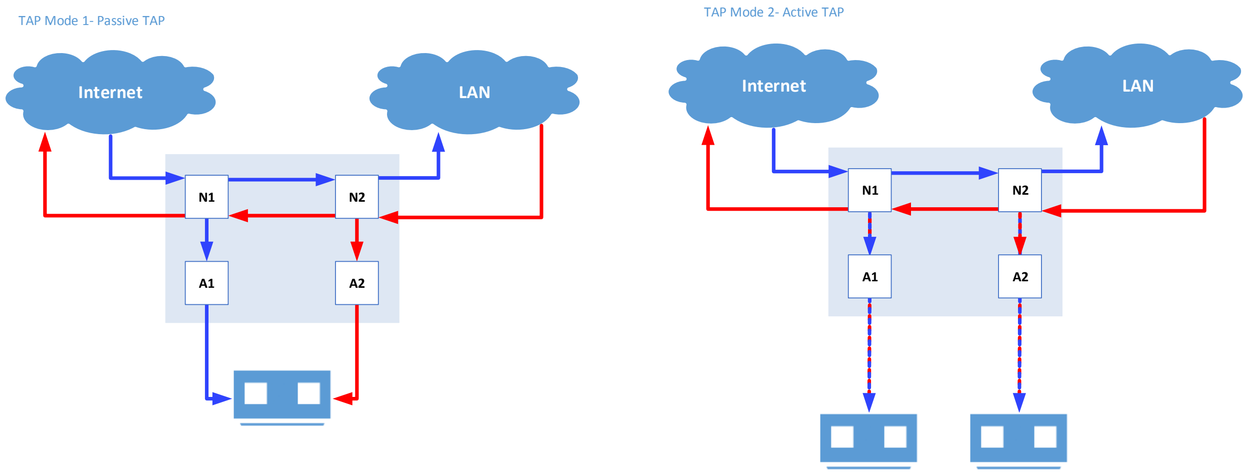

Figure 1: Two different segments of a TAP, showing passive and active TAP modes

Interface Masters Technologies

Interface Masters Technologies is a leading vendor in the high speed network visibility market based in the heart of the Silicon Valley. Flagship product lines include Network Packet Brokers, specialized 10G and 1G internal server adapter cards and NICs, 1G, 10G and 40G switches, external intelligent Network TAP and Bypass and failover systems that increase network monitoring capabilities, network reliability and inline appliance availability. Company Headquarters are located in San Jose, CA with satellite offices in Hong Kong and Europe. For more information please contact sales@interfacemasters.com or visit www.interfacemasters.com