NIAGARA NETWORKS

SPAN AND NETWORK TAP EXPLAINED

150 E Brokaw Road
San Jose, CA 95112, USA

www.niagaranetworks.com
info@niagaranetwroks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529

NIAGARA NETWORKS

INTRODUCTION

In a basic network infrastructure, there are out-of-band security tools such as probes, intrusion detection systems, network recorders, and network analyzers. Traffic flowing to these devices will come from other network devices, such as firewalls, routers and switches.

It is common practice to have the out-of-band tools sit passively on the network. Out-of-band tools are not modifying or altering any of the network traffic, as compared to inline devices like Intrusion Prevention Systems, which in some cases will alter the network 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 a power failure or software malfunction, traffic will continue to flow on the network as usual.

This white paper focuses on the differences between the two approaches for out-of-band network visibility, SPAN and network TAP.

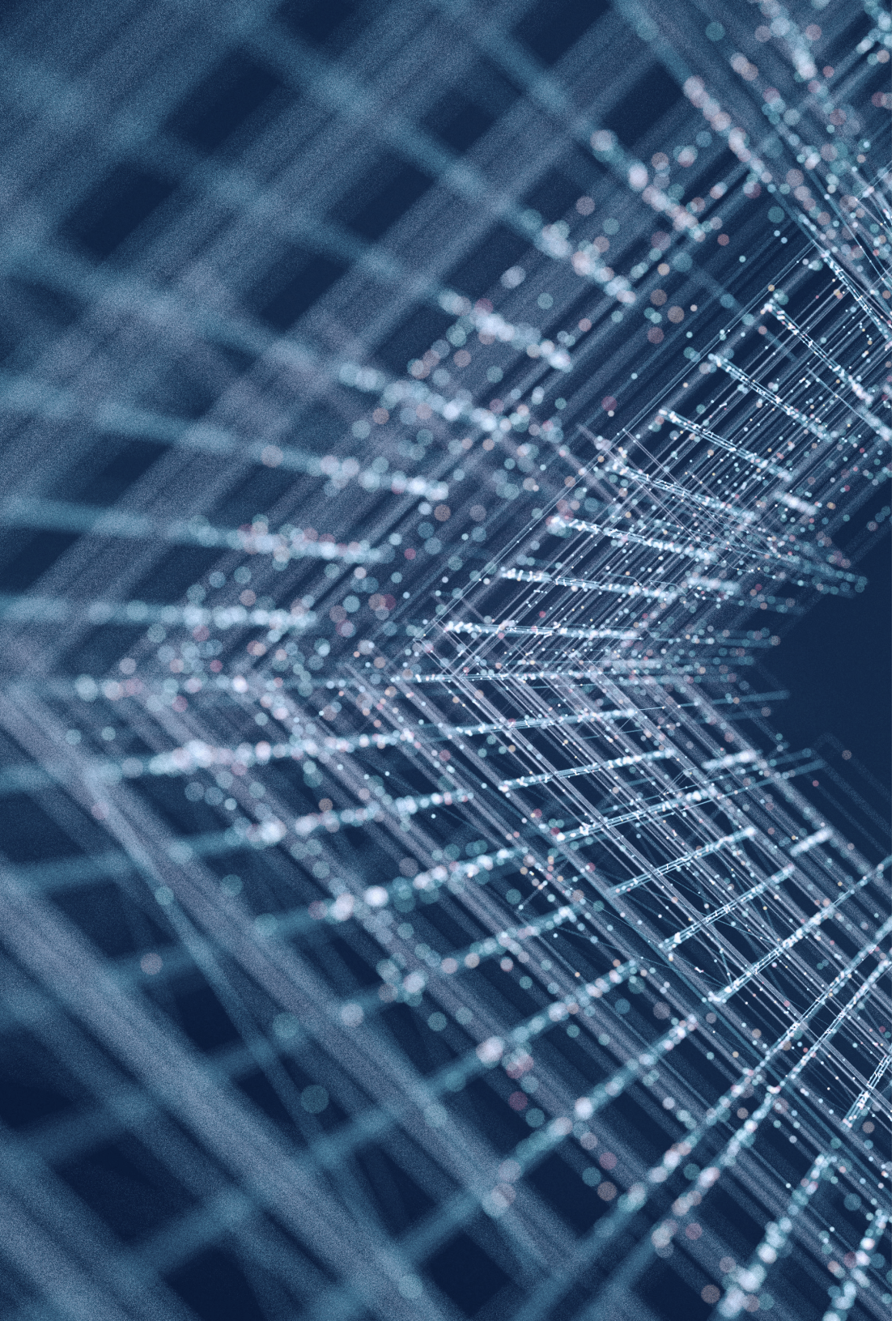
NIAGARA NETWORKS

SPAN EXPLAINED

A SPAN port is configured via a network enterprise switch or service provider switch/router. SPAN is a dedicated port on a managed switch that takes a mirrored copy of network traffic (which a network administrator chooses) off the switch to be sent to a monitoring device. One job a switch has 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 gives 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 over-saturated and packets may be dropped.



NETWORK TAP EXPLAINED

A network TAP is a device that passively splits network traffic flowing from the network to the security tool.

The network TAP receives network traffic in real time on separate channels (RX and TX) and from both directions, (Ingress and Egress), to make sure all data is sent to the monitoring device.

Because the network TAP is passive, it receives all network traffic and will not modify traffic before it's sent to the tool. Therefore, there will be full visibility even if the network is 100% saturated.

There are two variations of a network TAP: Passive and Active.

NIAGARA NETWORKS

PASSIVE AND ACTIVE NETWORK TAP

A passive network 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 3).

The advantage of this network TAP mode is that it does not need power to run, which adds to the layer of redundancy and minimizes maintenance, which reduces overall operational expenses. An example of a passive network TAP is the Niagara Networks 3225 model. This network TAP is a highly dense and modular 25 segment fiber network TAP, which can support 1Gb, 10Gb, 25Gb, 40Gb and 100Gb networks and security tools. An active TAP has a similar function as a passive network TAP, traffic is tapped and ingress- and egress traffic can be sent to separate monitoring tools.

Additionally, an active network TAP supports aggregation mode, which means the ingress and egress traffic can be aggregated together so that a single monitoring tool can receive both ingress- and egress traffic without the requirement for an aggregation device or multiple network connections on the tool. The active network TAP regenerates the signal opposed to the passive network TAP where there is loss of light intensity.

Niagara Networks bypass switches have active TAP functionality built-in and have additional ports to feed the tapped traffic to reporting tools or a packet broker. Niagara Networks fixed and modular bypass switches offer active TAP functionality for speeds up to 100Gb.

Niagara Networks also provides active network TAP systems where both the network and appliance ports are able to regenerate the signal and as a result, provide better quality.

For more details about Niagara Networks TAP solutions, visit our website

Figure 1: Aggregation tap mode (Active TAP)

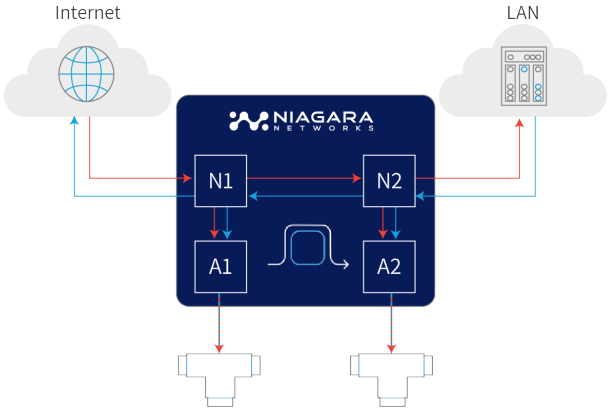


Figure 2: Split TAP mode (Active TAP)

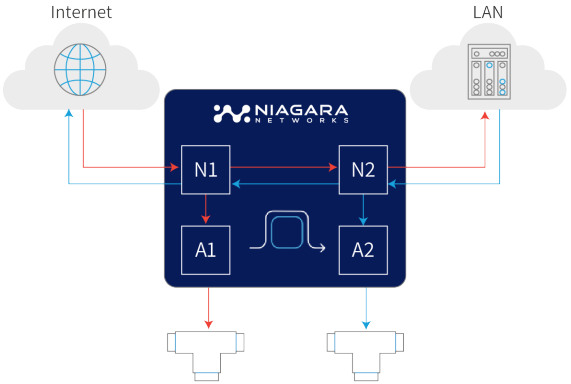
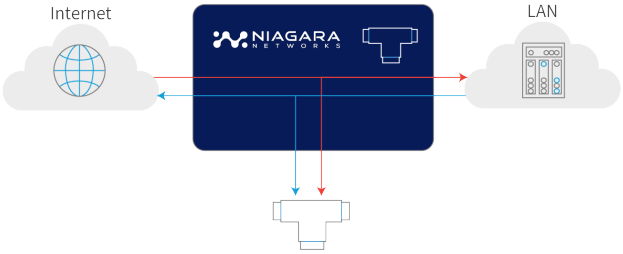


Figure 3: segments of a TAP, showing Passive network TAP modes



ABOUT NIAGARA NETWORKS

Niagara Networks™ is a Silicon Valley based company that pioneered the Open Visibility Platform™ to bring desperately needed agility to network security.

Niagara Networks provides high-performance, high-reliability network visibility and traffic delivery solutions for the world's most demanding service provider and enterprise environments.

We Design, Develop and Manufacture our Products in Silicon Valley, USA.

150 E Brokaw Road
San Jose, CA 95112, USA

www.niagaranetworks.com
info@niagaranetworks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529