

Technology Overview: Tap and Span Port Comparison

WHAT IS A TAP

Network Taps are used to create permanent access ports for passive monitoring. TAP (commonly seen as Tap) is an acronym for Test Access Port. Taps can create a monitoring access port between any two network devices, including switches, routers, firewalls, and more. Taps can function as an access port for any monitoring device used to collect in-line data. Protocol analyzers, RMON probes, intrusion detection systems, and other management and security solutions are all commonly connected to the network via Taps.

TAPS VS SPAN PORTS

Access to all packet-types on a link, and errors from all seven layers

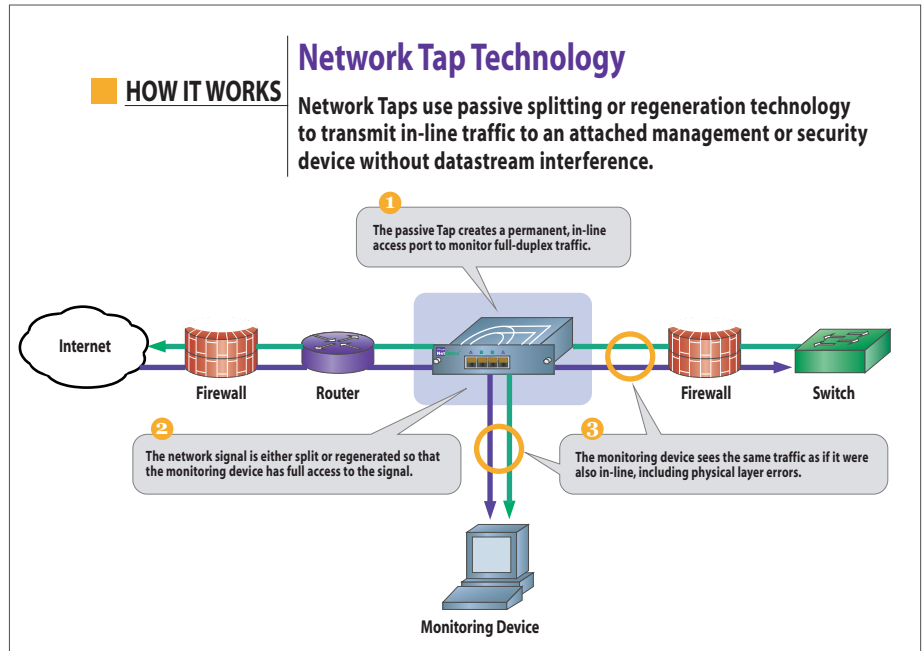
The monitoring device connected to the Tap receives the same traffic as if it were also in-line, including all errors. This is achieved through the Tap splitting or regenerating the full-duplex network signal. Neither splitting nor regeneration introduce delay, or change the content or structure of information packets.

In contrast, a monitoring device connected to a SPAN port on a switch does not see all traffic. Corrupt network packets, or packets below minimum size, are usually dropped by the ingress ports on a switch; corrupt packets visible to the monitoring device are usually generated within the egress segment.

In addition, switches eliminates layer 1 and select layer 2 errors. Without this information, it is impossible to properly troubleshoot common physical layer problems such as bad frames generated by a faulty NIC.

Access to all packets on a link, in real-time

Taps are non-blocking devices, and pass through full-duplex data at line rate. In contrast, the software architecture of low-end switches may introduce delay by requiring extra time to copy the spanned packets. Or, if



10/100 data is being aggregated through a gigabit port, delay may be introduced as the signal is converted from electrical to optical.

Furthermore, access to full-duplex traffic is constrained by the span port capacity. For example, to see full-duplex traffic on a 100 Mbps link, a span port would need 200 Mbps of capacity; a problem, unless a gigabit capacity port can be dedicated to spanning.

On the topic of gigabit spanning, it is common practice for network managers to span a VLAN, or another multiple-port combination of traffic through a gigabit port. In addition to the bandwidth constraint issue, it is often impossible to match these 'batch' packets back with a particular link. So while spanning a VLAN can be a great way to get an overall feel for network issues, pinpointing the source of actual problems is difficult.

Zero network data stream interference

Taps are passive devices that can be left permanently in-line without causing any data stream interference. In contrast, the delay introduced by spanning can apply both to monitored

traffic and to network traffic. Switch performance becomes more likely to degrade as span port subscription increases.

Even if the span port is not theoretically oversubscribed, issues such as 'back-pressure' can cause performance to degrade. In this scenario, the span port buffer fills, and the switch broadcasts a 'reset' command to the connected network devices. The span port will not transmit the signature associated with this command, so only administrators aware of this issue can properly troubleshoot when this occurs.

Optimal use of network resources

The use of Taps conserves network ports on a Switch. As demonstrated in the figure above, Taps are connected between two network devices. In contrast, spanning requires rededication of a separate network port on a switch. Finally, since usually only one port is used for spanning, network managers and security administrators must share a single port. With technology such as a Regeneration Tap, up to four devices can monitor a single link simultaneously and in real-time, eliminating the contention for monitoring resources. ■