TAP

(Test Access Point)

A simple hardware device that copies all network traffic for monitoring, analysis, and security.

HOW?

Taps provide full, unfiltered access to bi-directional traffic streams at a low cost. Passive taps replicate optical signals at the physical layer whereas active and bypass taps replicate traffic and provide fail-to-wire protection.

VS

SPAN

(Switch Port Analyzer / Mirror)

Software built into switches and routers that copies selected packets passing through the device.

HOW?

Specified traffic is replicated and transmitted out a single egress port that can become oversubscribed. To keep production traffic running smoothly, SPAN traffic is given lower priority and may be dropped when processing spikes.

Why Network TAPs are preferred over SPAN ports:

- Taps forward all traffic at full line rate and are never oversubscribed or rate limited the way SPAN ports can be
- There are few SPAN ports compared to the number of network interfaces; taps can access all the interfaces
- Taps provide continuous access to traffic and require no user intervention or configuration once installed
- Incorrect SPAN configuration can impact device performance, disrupt production traffic, and even cause network outages

Exceptions where SPAN ports make sense:

- Ad hoc monitoring in locations where taps have not already been installed
- Installing taps does require bringing down a link during a maintenance window which is not always feasible
- Remote locations that cannot justify a permanent tap but have SPAN access for modest monitoring needs
- SPANs provide access to traffic that stays within a switch and/or never reaches a tapped network link

BEST PRACTICES

TAPs: Use taps where 100% visibility and traffic fidelity is required or when monitoring moderate to high traffic volumes.

SPANs: Leverage SPANs in locations that require occasional monitoring of modest traffic loads or where a tap is not physically viable.

Deployment: SPANs were never intended for long-term production monitoring and security. Consider installing taps when building out racks and cabling. Even if not required immediately, having taps in place beforehand eliminates the need to schedule a network outage to install them later and greatly improves incident response times.

1033-01 06/16

Gigamon