DATACOM SYSTEMS INC.™

You Can't Monitor What You Can't See

TAP vs. SPAN

TAP

How TAPs work:

- Taps are completely passive, "plug and play" devices dedicated to traffic capture inserted between two network endpoints
- Tx and Rx delivered to analysis tool on separate ports
- Complete traffic capture even when network utilization is 100%
- Every packet is delivered in the correct order

What you get:

- Total visibility into full duplex links without risk of oversubscription
- Permanent access port for monitoring that won't affect network
- 100% of ALL traffic including Layer 1 and 2 errors and VLAN Tags
- Valid delta times and no altering to the time relationships of frames

Other Considerations:

- Necessary for real-time data access and many compliance applications
- Cannot monitor intra-switch traffic
- Use an aggregation tap for single-receive capture interface solutions or to receive all traffic in one trace file

Analyzer

VERSUS

SPAN

How SPAN works:

- Switches are managed devices dedicated to switching network traffic
- User configuration required to capture data from switch
- Limited number of SPAN ports provide copy of switch traffic to connected analyzer as long as switch utilization is not too high
- Forwards copies of traffic but alters timing of the frame interaction

What you (may) get:

- Dropped packets resulting from port oversubscription or high switch utilization
- Network outages resulting from improperly configured SPAN sessions
- Certain traffic like corrupt packets and VLAN tags filtered out
- Packets delivered to connected tools out of order

Other Considerations:

- You might not have permission to configure SPAN ports to meet your needs
- If spanning a VLAN, you might get multiple copies of the same packet
- A network switch can be vulnerable to security threats
- A SPAN port is not a scalable technology

Analyzer

9 Adler Drive | East Syracuse, NY 13057 | (T) 315.463.9541 | (F) 315.463.9557 | datacomsystems.com

Datacom Systems Inc. © Copyright 1992-2009. All rights reserved.