Network TAPs vs. SPAN Ports & Hubs

Application Note

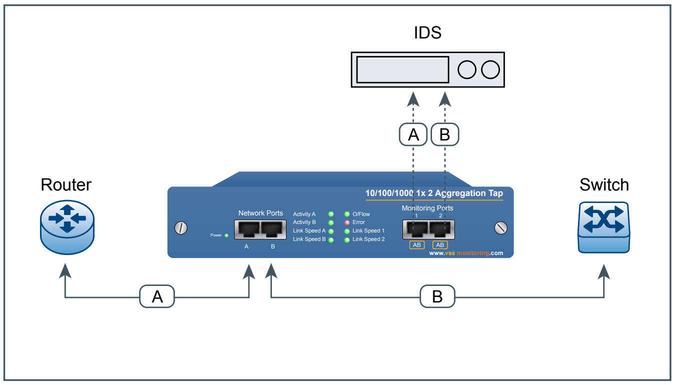
What is a TAP?

A network tap is a dedicated inline network monitoring solution for use with analyzers, IDSes, IPSes and other test access monitoring devices. Designed to be permanently installed in any inline network, a tap is a failsafe unit that will not interrupt the network connection during power failure, nor adversely affect traffic itself.

The tap provides the user with total visibility of all passing traffic so that both sides of a conversation can be monitored seamlessly at a full line rate without packet loss or asymmetrical delay. As a further benefit, a tap provides a layer of stealth in the monitoring process so that intruders on the network are blocked from viewing the tap and thereby prevented from attacking the user's network monitoring system.

Problems with SPAN Ports

- Packet Loss
  - SPAN ports are low priority in switches routing hierarchy
  - Duplex monitoring is often not possible
  - Layer 1 & Layer 2 errors are not monitored
  - Port is frequently over subscribed
- Limited Stealth from Detection
- Potential Point Failure



Packet Loss

SPAN port traffic is always a lower priority over other port routing in most switches. Hence, during heavy utilization, a switch's CPU performance will decline leaving the span port subject to packet loss and possible shut down.

SPAN ports, such as the Cisco Catalyst snoop port, don't allow duplex monitoring, thereby leaving the user unable to listen to both sides of the conversation. This is a fundamental shortfall in network security and VoIP monitoring.

SPAN ports prevent monitoring of many types of Layer 1 and Layer 2 errors! For example, a CRC is a component in every Ethernet frame that serves as a comprehensive 'Layer 2' checksum of a packet size and content. If an element in the packet becomes corrupt, the CRC will show the error. A switch with a MAC layer chip will drop any packet with a CRC error and thereby not transmit the frame to the monitoring device. Hence, using a span port to monitor line errors is impossible because you will not know when they occur.

SPAN ports are also usually oversubscribed (too many ports being mirrored onto one) which causes extensive packet loss. The alternative is a dedicated inline network monitoring system that does not fatigue or have inherent failings.

Limited Stealth from Detection

Many SPAN ports allow receiving as well as sending data packets, leaving the monitoring device often vulnerable to malicious intrusions.

Potential Point of Failure

Switches do not allow fail-safe monitoring. If a switch fails, then so does the network. A tap provides a fail-safe monitoring solution where, if power is lost, the network connection remains unaffected.

Problems with Hubs

- Reduces Link Bandwidth By 50% +
- Induces False Collisions
- No Gigabit Solution
- Potential Point Failure

Reduces link bandwidth by over 50%

A hub is a half duplex Ethernet device that broadcasts packets from a source along all path simultaneously. During a broadcast, traffic from the opposite direction is not allowed. Hence, as a monitoring tool, the hub only ever allows one side of conversation to be seen at one time.

Induces False Collisions

When using a hub, unnecessary collisions frequently occur when two opposite side transmit simultaneously. Each collision is recognized by both end stations and the packets are retransmitted after some back-off period. These collisions would not occur if a duplex device, such as a tap, was being used. In addition to inducing unnecessary collisions, the back-off period causes the potential link bandwidth to diminish.

No Gigabit Solution

Hubs are not available for 10/100/1000 or Gigabit networks. This further reflects the hub's limited usefulness and dated application as a monitoring device.

Potential Point of Failure

A hub does not allow fail-safe monitoring. If a hub fails, then the link it sits inline with does as well. A tap provides a fail-safe monitoring environment where, if power is lost, the network connection remains unaffected.

Benefits of TAPs

Visibility

VSS Monitoring's taps provide total visibility of the data on the network and ensure 100% data capture (including errors) at line rate over any duplex network being monitored.

Stealth

VSS Monitoring's taps provide a layer of stealth and first line of defense for both the tap and monitoring device such that each tap is 100% hidden from all intruders, eliminating the potential for hacks or malicious intrusions on either the tap or monitoring device.

Security

VSS Monitoring's taps provide a level of security that ensures 100% network connectivity and data throughput even in the event of power supply failure. The tap removes the potential point of failure, otherwise caused by span ports and hubs, as an inline network monitoring tool.

VSS
monitoring
Network Visibility. Optimized.

USA
(Corporate HQ)
+ 1 650 697 8770 phone
+ 1 650 697 8779 fax
38 Adrian Court
Burlingame, CA 94010
USA
www.vssmonitoring.com

Japan
+ 81 422 26-8831 phone
+ 81 422 26-8832 fax
T's Loft 3F, 1-1-9,
Nishikubo, Musashino,
Tokyo, 180-0013
Japan
www.vssmonitoring.co.jp

China
+ 86 10 6563-7771 phone
+ 86 10 6563-7775 fax
C519, 5 Floor,
CBD International Tower
16 Yong'An Dong Li,
Beijing, China 100022
www.vssmonitoring.com.cn

VSS Monitoring, Inc. is the world's leading innovator of Distributed Traffic Capture Systems and network taps, focused on meeting the rapidly evolving requirements of security and performance conscious network professionals. Distributed Traffic Capture Systems herald a new architecture of network monitoring, one which fundamentally improves its capability and price-performance.

VSS, Distributed Traffic Capture System, vAssure, vStack+, and LinkSafe are trademarks or registered trademarks of VSS Monitoring, Inc. in the United States and other countries. Any other trademarks contained herein are the property of their respective owners.

© Copyright 2003 – 20010. VSS Monitoring Inc. All rights reserved.