SOLUTION BRIEF

Why are Taps Critical to Network Visibility and Security?

TAPS PASSIVELY ACCESS AND MONITOR NETWORK DATA

IT managers have a nearly impossible job. They must understand, manage, and secure the network all the time against all problems. Anything less than a 100 percent working network is a failure. As the network grows larger, visibility becomes harder as blind spots creep into the network. These blind spots, or the inability to completely see what is happening on the network, can compromise network quality. Taps provide an unobtrusive way to capture network monitoring data and begin the process of removing blind spots.

Taps are used to help IT groups easily and passively monitor all network data. They are normally placed between any two network devices, including switches, routers, and firewalls. This provides continuous, non-disruptive network access to monitor devices and troubleshoot problems. Eliminating the need to take down links and interrupt traffic, taps simplify how network monitoring and security devices are connected to and removed from the network. Any monitoring device connected to a tap receives all inline traffic. The tap duplicates all traffic on the link and forwards it to the monitoring ports. Taps do not introduce delay, or alter the content or structure of the data. They also “fail open.” Traffic continues to flow between network devices in the event a monitoring device is removed or power is lost.

Network taps provide the details that SPAN ports do not.

ixia
A Keysight Business

915-6686-01-1071 Rev C

TAPS VS. SPAN PORTS

Taps offer significant advantages over the use of switch port analyzer (SPAN) ports to monitor the network. SPAN ports require an engineer to configure the switch or switches. Switches also eliminate corrupt packets or packets that are below a minimum size. In addition, switches may drop Layer 1 and select Layer 2 errors, depending on what has been deemed as high priority. This means SPAN ports do not get all the traffic. On the other hand, a tap passes all data on a link. Taps capture everything needed to properly troubleshoot common physical-layer problems. This includes bad frames that can be caused by a faulty network interface card (NIC).

REAL-TIME ACCESSIBILITY

Taps pass through full duplex traffic at line-rate non-blocking speeds. Low-end switch SPAN ports can introduce delay while packets are copied to them. Data being aggregated from lower-speed ports to a higher-speed port can also introduce signal delay. Furthermore, a SPAN port needs 200Mb of capacity to capture all the data from a 100Mb link. If capacity is limited, full data is not captured. This means a higher-speed SPAN port is needed to get all the data from a lower-speed link. This is not an efficient solution!

Common networking practice is to SPAN virtual local area networks (VLANs) across gigabit ports. In addition to requiring more ports than may be available in one switch, it is often difficult to "combine" or match packets to a particular originating link. So while spanning a VLAN is an accepted way to get an overall feel for network issues, pinpointing the source of actual problems becomes difficult. Some switches have problems processing normal network traffic, depending on loads. With SPAN, the switch also needs to determine what traffic gets sent to monitoring tools. This extra processing may introduce performance issues. Taps provide permanent, passive, zero-delay alternatives.

FUNCTIONALITY	TAP	SPAN
Provides access to monitoring packets	X	X
Delivers a complete copy (100%) of data (including bad data vital for diagnosis)	X	
Has full system resource priority during crisis (i.e., does not drop frames)	X	
Less vulnerable to security attacks	X	
Does not create unnecessary, duplicate packets	X	
Does not create time stamp issues	X	
Recommended for lawful intercept	X	
Relieves SPAN port contention	X	
Plug & play: no configuration needed	X	

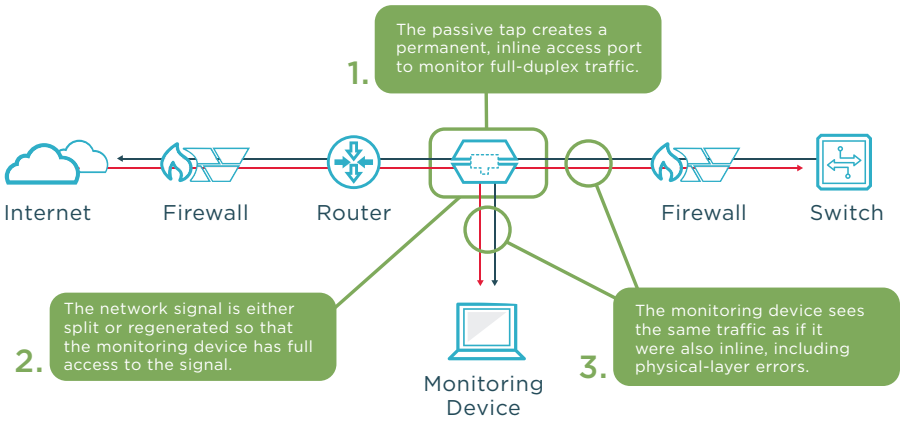
TAP VS. SPAN FUNCTIONALITY

ADVANTAGE: TAPS

The use of taps optimizes both network and personnel resources. Monitoring devices can be easily added when and where they are needed. No extra cables are needed to monitor traffic or reconfigure switches. The example to the right illustrates a typical tap deployment for one monitoring device. A tap that includes two monitoring ports means the network and security teams do not share the one SPAN port. They get all the data they need.

HOW IT WORKS

Network Tap Deployment
Network taps use passive splitting or regeneration technology to transmit inline traffic to an attached management or security device without datastream interference.



IXIA'S TAP FAMILY

Ixia's comprehensive tap portfolio is the foundation of our integrated IxVision Visibility Architecture. Our taps pass all network traffic, including Layer 1 and 2 errors, without introducing bottlenecks or points of failure. Regardless of interface or location in the network, Ixia provides a tap solution, supporting copper, or multimode and single-mode fiber at speeds up to 100Gbps with media conversion models available.

IXIA WORLDWIDE

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 1.818.871.1805

www.ixiacom.com

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127