ixia

What is a Tap, and Why Are Taps Critical to Network Visibility and Security?

Taps provide non-intrusive access to data flowing across the network and enable monitoring of network links

Taps are primarily used to optimize IT's ability to easily and passively monitor a network link. They are normally placed between any two network devices, including switches, routers, and firewalls to provide network and security personnel a connection for monitoring devices. Taps are used for troubleshooting and offer continuous, non-disruptive network access.

Protocol analyzers, RMON probes and intrusion detection and prevention systems can now be easily connected to and removed from the network when needed. By using a tap, you also eliminate the need to schedule downtime to run cabling directly to the monitoring device from network devices, thus saving time and eliminating possible cabling issues.

Any monitoring device connected to a tap receives the same traffic as if it were inline, including all errors. This is achieved as the tap duplicates all traffic on the link and forwards it to the monitoring ports. Taps do not introduce delay, nor alter the content or structure of the data. They also fail open so that traffic continues to flow between network devices in the event a monitoring device is removed or power to the device is lost.

Ixia's Net Optics Tap Family—Part of an End-to-End Visibility Architecture

Ixia's comprehensive tap portfolio is the foundation of our integrated Visibility Architecture for enterprises and service providers, which includes network access solutions, network packet brokers, network, application and session visibility solutions, and a centralized management platform. These taps pass all network traffic, including Layers 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, multimode and single mode fiber at speeds up to 100Gbps with media conversion models available.

Taps vs. SPAN Ports

As shown below, taps offer significant advantages over the use of SPAN ports to monitor the network. For one, SPAN ports require an engineer to configure the switch or switches. Switches also introduce mechanisms on ingress ports to eliminate corrupt packets or packets that are below a minimum size. The problem with this is that the monitoring device normally captures data within the egress segment. In addition, switches may drop layer 1 and select layer 2 errors, depending on what has been deemed as high priority. On the other hand, a tap passes all data on a link, capturing everything needed to properly troubleshoot common physical layer problems, including bad frames that can be caused by a faulty NIC.

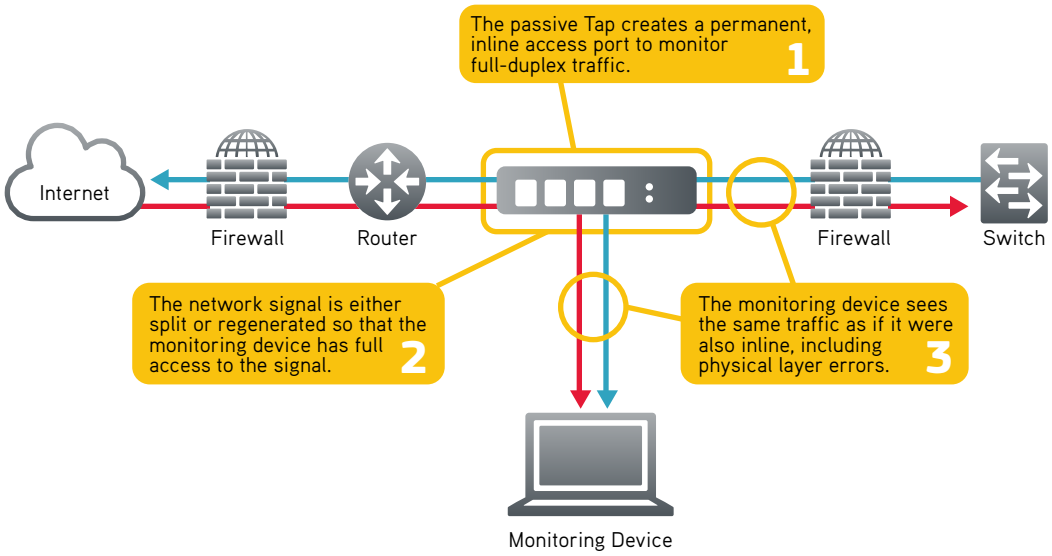
Comparison of Tap and SPAN Technologies

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. doesn't 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	

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.



Real-Time Accessibility

Taps are designed to pass through full duplex traffic at line rate non-blocking speeds. In contrast, the software architecture of low-end switches may introduce delay while packets are copied to the SPAN ports. As well, data being aggregated from 10/100 Mb ports to a gigabit port may also introduce signal delay.

Furthermore, accessing full-duplex traffic may also be constrained by using a SPAN port. For example, to capture the traffic from a 100 Mb link, a SPAN port would need 200 Mb of capacity. This simple oversight can cause problems, so a gigabit link is often required as a dedicated SPAN port.

It is also a common practice for network engineers to span VLANs across gigabit ports. In addition to the need for additional ports that 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 can be a great way to get an overall feel for network issues, pinpointing the source of actual problems may be difficult.

Some switches may have a problem processing normal network traffic, depending on loads. Add the fact that the switch will also need to make decisions on what traffic to copy to a SPAN port, and you may introduce performance issues for all traffic. Taps provide permanent, passive, zero delay alternatives.

Advantage: Taps

Lastly, the use of taps optimizes both network and personnel resources. Monitoring devices can be easily deployed when and where needed, and engineers do not need to re-cable a network link to monitor traffic or re-configure switches. The example above illustrates a typical tap deployment for one monitoring device. In contrast, a tap that includes two monitoring ports eliminates the need for both the network and security teams to share the one SPAN port that may have been configured to capture traffic for monitoring devices. A regeneration tap can simultaneously capture data from one link for four monitoring devices, and aggregation taps can capture data from multiple links to one monitoring device.

Ixia Worldwide Headquarters
26601 Agoura Rd.
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800
(Fax) 818.871.1805
www.ixiacom.com

Ixia European Headquarters
Ixia Technologies Europe Ltd
Clarion House, Norreys Drive
Maidenhead SL6 4FL
United Kingdom

Sales +44 1628 408750
(Fax) +44 1628 639916

Ixia Asia Pacific Headquarters
101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
Fax +65.6332.0127