WHITE PAPER

Top 6 Considerations When Purchasing Network Taps

Ensure you have the best technology and value for your deployment by understanding the key differences in network taps.

Network visibility and data access to your traffic ensure that your network runs efficiently. A network tap (Test Access Port) is an inexpensive and permanent access port used throughout the network to enable monitoring and analysis without interrupting data transmission.

There are many benefits for choosing a network tap solution instead of diverting data with a port connection on a switch. With so many network taps available on the market, choosing the right tap provides significant savings. For example, did you know that signal loss and degradation may result in thousands spent for additional cable roll-outs in data centers? Ensure you have the best technology and value for your deployment by understanding the key differences in network taps.

When and Where to Deploy Taps

The decision of when and where to tap is based on the monitoring needs. Ixia offers network taps to support a variety of media and speeds.

When? Anytime. Network taps are mostly passive and require little to no configuration for deployment. They can be put onto a network link anytime. You can then connect a monitoring tool any time after the tap is deployed without disrupting network operation.

KEYSIGHT TECHNOLOGIES

Where? Anywhere. Unlike other monitoring methods, such as SPAN ports, network taps are able to be deployed on any connection and will continuously create copies of the traffic regardless of utilization. With a network tap your monitoring infrastructure can extend to network segments that are beyond traffic between network switches.

Network Tap Versus Port Connection (Span Port)

Most major switch vendors support SPAN (Switched Port Analyzer) ports or mirror ports for monitoring and intrusion detection. An administrator configures port mirroring by assigning a port from which to copy all packets and another port to which those packets will be sent. Traffic is sent to both the analyzer port as well as the original designated port.

Network taps are able to be deployed on any connection and will continuously create copies of the traffic regardless of utilization.

Tap vs. SPAN

There are three major drawbacks to SPAN ports:

- Increased load onto the switch results in more CPU or memory requirements which are expensive
- Most vendors' switches remove low level Layer 1 and some Layer 2 errors from the data steam when sent to SPAN ports making it impossible to do low level trouble shooting
- Loss of large amounts of data from your monitoring and analysis tools as SPAN port traffic is low priority in switching deployments. If your link is running at full line rate in full duplex, mirroring the data requires a SPAN port to also run at full line rate to get both directions of traffic. Most deployments drop the SPAN traffic instead
- Adds to operational expenses (OPEX) to maintain and manage the switches and SPAN ports

Implementing a network tap solution uses passive fiber splitter or copper taps on the main network links eliminating the challenges and expense with SPAN ports. With network taps, you:

- View 100% of the traffic including VoIP, HTML, application and Layer 1 and 2 errors
- Require little to no configuration as network taps are plug-and-play
- Provide a permanent access port avoiding breaking a network link each time a tool is connected
- Deliver a reliable solution with passive technology to ensure maximum network uptime as the mean time between failures (MTBF) of fiber taps is 10's of years

If a tool is required to sit inline, then an Ixia iBypass Switch and Network Packet Broker (NPB) are the correct devices to leverage.

Network Tap Versus Inline Tool Connection

Another possible solution to monitoring is to place the analysis tool inline. Unfortunately, it is not cost effective to leave the analysis tool inline in the many segments that need monitoring. As a result, the network manager needs to break into the connection whenever they need to monitor. Additionally, the analysis tool introduces a possible point-of-failure in the network.

If a tool is required to sit inline, then an Ixia iBypass Switch and Network Packet Broker (NPB) are the correct devices to leverage. Learn more here.

What Type of Tap Should I Use?

The typical taps types are network taps, port aggregation taps, regeneration taps, link aggregation taps, BiDi (bidirectional) taps, and virtual taps.

Network taps are used to connect a monitoring tool to the network without affecting the network link and performance, moving cables and interrupting traffic. Network taps are completely passive so even if the tap loses power, it fails-open to ensure traffic continuity. Network taps provide 100% visibility because they pass 100% of all network traffic without introducing bottlenecks or points of failure into your network design.

Port aggregation taps are very similar to network taps and allow access to a single network segment. However, with a port aggregation tap, you can plug in one or two monitoring devices depending on the size of the port aggregator. This enables you to view full duplex traffic with a single network interface card (NIC) per device instead of two.

Regeneration taps regenerate network traffic copies from a single link onto multiple monitoring ports. They provide permanent passive monitoring access into your network's critical links with simultaneous support for multiple devices such as IDS/IPS (Intrusion Detection/Prevention System), RMON (remote network monitor) probes, protocol analyzers, and more. Each monitoring devices sees exactly the same traffic at the same time for complete visibility into the health of the network.

Link aggregation taps provide the reverse service of the regeneration tap. Depending on the model, a link aggregation tap aggregates network traffic copies from multiple links onto a single monitoring port.

BiDi taps are fiber taps designed for use in Cisco 40G BiDi networks, specifically Application Centric Infrastructure (ACI). BiDi transceiver technology utilizes multiple wavelengths within a single cable so the standard fiber tap technology will not work.

Virtual taps provide visibility into traffic between virtual machines (VMs). Since traffic in virtual machines may never cross a physical port, virtual taps are able to view east-west traffic and send monitored traffic via encapsulated tunnels to physical monitoring tools. Select the virtual taps that support the maximum number of hypervisor deployments. Ixia virtual taps support VMware ESXi and NSX, Openstack KVM and Microsoft Hyper-V giving you the best hypervisor flexibility.

Network taps provide 100% visibility because they pass 100% of all network traffic.

Scale and Flexibility

Taps need to scale to support your network speeds and size and monitoring requirements. Whether you use copper or fiber taps depends the type of media used on the network segment to be tapped. Fiber taps divert a small amount of light to produce an exact copy of the original network traffic. They are 100% passive with no power needed. They have no IP address which means they are inaccessible and not vulnerable to hackers. Ixia offers Flex Taps that are high density and modular, available in speeds from 1Gb to 100Gb, fiber types of single mode or multimode, connectors of Little Connector (LC) or Multiple-Fiber Push-On/Pull-Off (MTP/MPO), and even support for Cisco 40G BiDi.

Network visibility is critical to your network health and ensuring you eliminate blind spots.

Copper taps replicate the electronic signal to produce an exact copy of the original network traffic. Although not completely passive, they are very reliable. In the event of a power failure, the tap's relays will close to ensure the link stays active and with Zero Delay, a battery guarantees that the network link stays up for the duration of the battery's charge. However, in both cases the monitoring ports will no longer transmit traffic. Similar to fiber taps, copper taps are also isolated with no IP address access.

Ixia's assortment of aggregation and regeneration taps fit specific use cases such as low utilization network links or limited network monitoring ports. If you are looking for the most comprehensive and scalable taps in the market, then Ixia is both the technology and market leader for network taps.

Signal Loss and Cost Impact

Whenever you use a fiber tap, signal degradation occurs. That is due to diverting a small amount of light to create a replica of the data. The amount of signal loss varies by vendor. Ixia Flex Taps have an insertion loss of 1dB less than the closest competitors.

This means that when you use Ixia Flex Taps, your signal will be 25% stronger than the nearest competitor, which in turn translates to cost savings. First, it means you do not need to regenerate the signal as much. More importantly, it means that you can extend your existing cable pulls by up to 50 meters. If you are using taps from other vendors, less distance can be covered by your cables and it may mean costly new cable deployments in difficult to reach places.

Your Tap Choice Matters

Network visibility is critical to your network health and ensuring you eliminate blind spots. Ixia has been designing and manufacturing network taps since 1996. Ixia offers a comprehensive portfolio of taps for any type of physical or virtual environment. Ixia taps are engineered and built to be practical and reliable. The most trusted names in networking and more than half of the Fortune 100 depend on Ixia taps in their network. Ixia continues to lead network tap innovation. Choosing Ixia network taps gives you the most flexibility, scale and business value. You can find more information about Ixia Network Taps and Ixia's visibility portfolio at https://www.ixiacom.com/products/visibility.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES