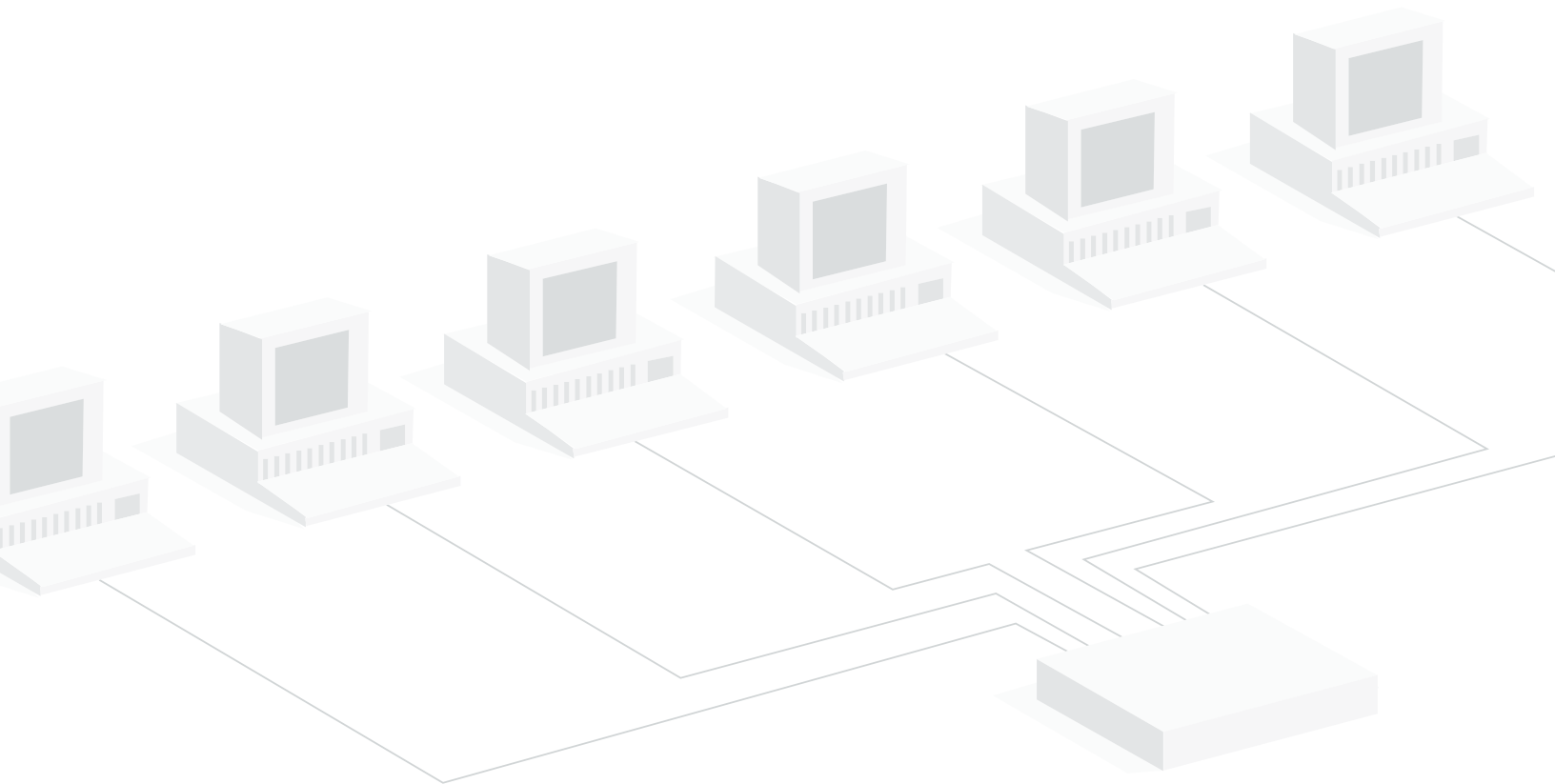


Best Practices in Gigabit Capture

How to obtain accurate, line-rate captures with your gigabit investment

Analysis is a necessary component of network management. Understanding the amounts and types of traffic traversing the network can profoundly affect a business' bottom line. Effective analysis begins with accurate packet captures, which is generally a function of hardware. This is especially true of gigabit traffic. This paper discusses the technical "best practices" that should be taken into consideration when purchasing gigabit network analysis equipment.



Introduction

Organizations around the world are recognizing that gigabit links can improve business functions, increase productivity, and enhance customer service. Most of the time, these gigabit links are deployed on the most critical parts of the network. However, gigabit links also come with a unique set of challenges. To maximize the advantages of deploying gigabit links, organizations need to invest in reliable analysis tools. At the heart of these tools is gigabit capture technology, which dictates the speed and accuracy of analysis. This paper illustrates various types of capture technology and the best practices that should be considered when choosing an analyzer.

The Variables Involved in Analysis

There are a number of factors that gigabit analysis depends on: how data is transferred off the wire, timestamping, formatting, how much processing is done on the card, and the type of network routing. Other factors also play a critical role such as SFP-based technology, whether the technology supports industry regulations, and how the technology gets deployed. The first step in maintaining accurate gigabit captures is determining how the data is retrieved from the network.

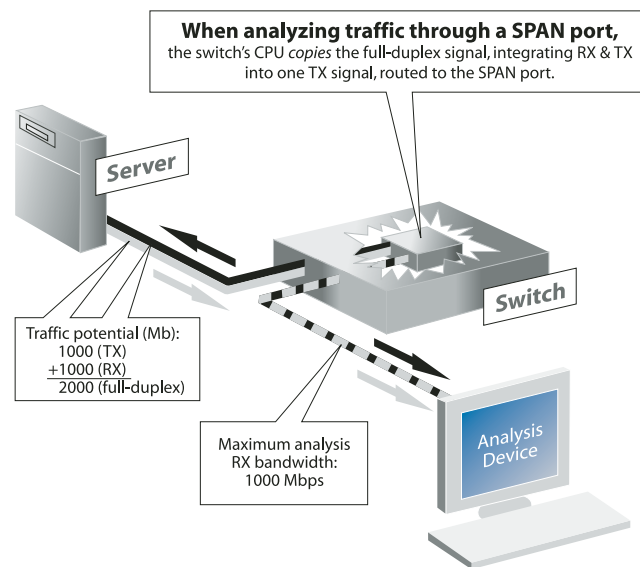
Points to consider when choosing capture technology

Accessing Network Traffic	How does the analyzer retrieve data from the network?
Timestamping	Can the analyzer accurately timestamp data passing through multiple ports simultaneously?
Formatting the Raw Data	How many steps does it take the capture technology to convert network data into native analyzer format?
System Memory	Does the analyzer rely strictly on the buffer on the capture card or on system memory?
SFP-Based Technology	Can the analyzer support different media?
Ideal Points of Visibility	Is the analyzer monitoring the most critical areas of the network?

Accessing Network Traffic

Ensuring complete visibility of network data is the first critical component of analysis. There are three common ways for a monitoring device to access network traffic: using a switch's SPAN session, a port aggregator, or a network TAP (Test Access Port). Each method has its advantages and disadvantages, but depending on the network, there are situations where one method is more viable than another.

In a SPAN session, the switch copies both the send and receive data from each port of interest and reconstructs an integrated data stream from the channels. It then routes the integrated signal through the send channel of the SPAN port to a monitoring device. Because both the send and receive channels are integrated into a single send channel, the SPAN port can only support a maximum of 1000 Mbps. A full-duplex data stream can reach 2000 Mbps on a fully saturated link (1000 Mbps in each direction). Once link utilization crosses 1000 Mbps, packets destined for the analyzer are instantly dropped. This is why you should not depend on a SPAN session to analyze highly utilized links.



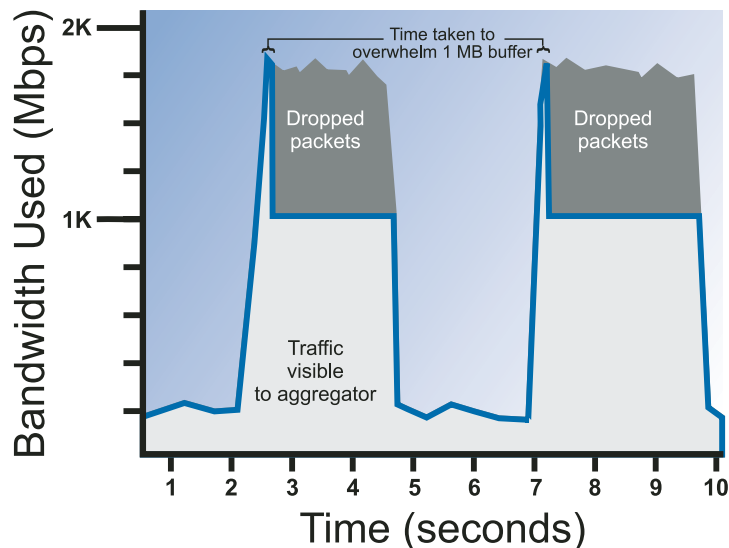
A SPAN session is also inappropriate for business-critical links because in addition to losing critical analysis data, a SPAN session does not reveal physical errors that traverse the network, and hides jitter from the monitoring device.

Typically, a SPAN session is the best method to access traffic on lower-utilized links that do not support business-critical traffic.

A port aggregator is essentially a small switch devoted to mirroring a link for analysis. It includes network in and out ports that provide link connectivity for the devices, and a single port, which mirrors traffic traversing the link. Like a switch, a port aggregator suffers the same limitations as a SPAN session. Therefore, port aggregators cannot handle traffic exceeding 1000 Mbps.

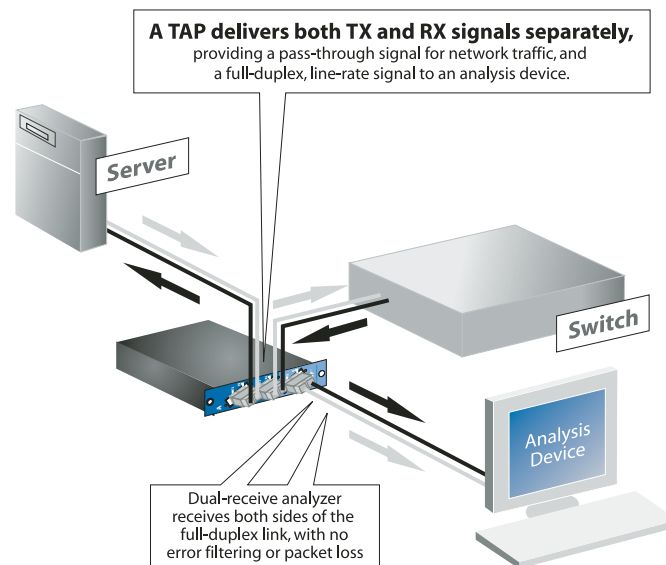
A port aggregator also typically includes an internal memory buffer, most commonly 1 MB to 256 MB. Although vendors may claim the port aggregator's memory buffer provides some protection against packet loss, it does not offer much. On a fully saturated gigabit line, a 1 MB buffer provides 1/120 of a second and a 256 MB buffer provides 2 seconds. Longer capture windows than this are typically required to analyze or solve most network problems.

The bandwidth utilization graph below was taken when a user downloaded files across a gigabit link from a server. All of the usage spikes shown are more than 2 seconds, and would therefore overwhelm the aggregator's small memory buffer.



Unlike a SPAN session, a port aggregator is independent from a switch. And unlike a switch, a port aggregator is not an addressable device on the network and therefore not susceptible to security threats. Similar to a switch's SPAN session, port aggregators are more suited for accessing non-critical, lower-utilized links.

A TAP is a passive splitting mechanism installed between a "device of interest" and the network. TAPs transmit both the send and receive data streams simultaneously on dedicated channels, ensuring all data (up to 2000 Mbps) arrives at the monitoring device in real time. For that reason, a TAP requires the monitoring device to be equipped with a dual-receive capture card capable of aggregating the two data streams.



TAPs never drop packets, regardless of speed or bandwidth saturation and unlike a SPAN session on a switch, a TAP reveals physical layer errors to the monitoring device. And a TAP is completely passive; it cannot interfere in any way with the full-duplex network.

Best Practice: Rely on a TAP to access highly utilized or business-critical links. A switch's SPAN session and a port aggregator may be adequate for less critical, lower-utilized links.

Timestamping

A switch's SPAN session, a port aggregator, or a network TAP transfers data to the monitoring device. The capture technology within the monitoring device immediately timestamps all the data as it arrives. When processing millions of packets, a dedicated capture card is the best solution. One benefit of a dedicated capture card is its ability to take workload away from the system processor. This frees up resources for critical processes such as Expert analysis. Another benefit of a dedicated capture card is its ability to timestamp packets in order, ensuring accurate analysis. This analysis is jeopardized by relying on multiple cards to capture and aggregate multiple physical data streams. If one of those cards gets even slightly out of sync, the analysis device will timestamp data incorrectly. Also, if data shows up at the same time on multiple cards, the analysis device has to guess which card received the data first (not a reliable option).

Accurate timestamping is crucial for troubleshooting network problems. For example, inaccurately timestamped VoIP packets can look like jitter to an analyzer even though there is no actual problem with VoIP communications. Investigating false positives wastes valuable company time and money. In order to accurately timestamp across one or multiple gigabit links, the key is to have one card (one clock) with nanosecond resolution responsible for timestamping all of the data across each link.

Best Practice: For accurate timestamping across multiple gigabit links, rely on one card (one clock) with nanosecond resolution to timestamp all of the data.

Formatting the Raw Data

A continued challenge in full-duplex gigabit analysis is for analysis vendors to develop the right technology mix that maximizes hardware and software efficiency in performing captures, data processing, and Expert analysis. For optimal performance, analyzers may need to utilize every available CPU cycle available to process and display captured data. To ensure the best performance for all types of real-time analysis, the gigabit capture card should pre-format the gigabit data stream into the native analyzer format. This can be done directly on the capture card prior to moving the data to the analyzer system. This pre-formatting on the card saves system CPU resources. The more the system is dedicated to data processing, the faster the analysis, particularly when monitoring full-duplex, line-rate gigabit links.

Relying on collection technology, that formats the data within the system and not on the card, slows down the analysis process and wastes CPU resources.

Best Practice: For analysis efficiency, choose a gigabit capture technology that can convert data into the native analyzer format on the capture card.

System Memory

Depending on the vendor, after getting timestamped, network data either goes directly to the buffer on the card or is streamed to the buffer in physical system memory. Relying on the buffer on the capture card, which is typically 128 MB, is not adequate because this technology only permits a line-rate capture that lasts for .5 seconds. This method is not only limited by time, but also requires a manual transfer of the data to the physical system for analysis—making real-time analysis impossible.

For real-time analysis, the data needs to be continually streamed to the buffer in the analyzer's physical system memory. (When choosing this type of solution, be sure the bus on the capture device can support link rate.) Ensure the buffer in physical system memory can support your network analysis needs. Buffers as large as 4 GB are available for 32-bit Windows operating systems. This permits a 16-second gigabit line-rate capture window, which should be long enough to catch most anomalies. Buffers as large as 124 GB are currently available for 64-bit operating systems, permitting potentially a 512-second line-rate capture window. Using circular buffers can extend this window indefinitely. Although this amount of buffer space is quite extreme, it is more than enough to investigate any anomaly.

Some vendors support what they call "quasi-real-time analysis" by allowing up to 30 percent of bandwidth to be streamed directly into physical system memory. This is obviously a problem when utilization spikes beyond 30 percent because critical information will be dropped.

Best Practice: For thorough and accurate real-time analysis, choose a capture card that streams directly to the buffer in physical system memory.

SFP-Based Technology

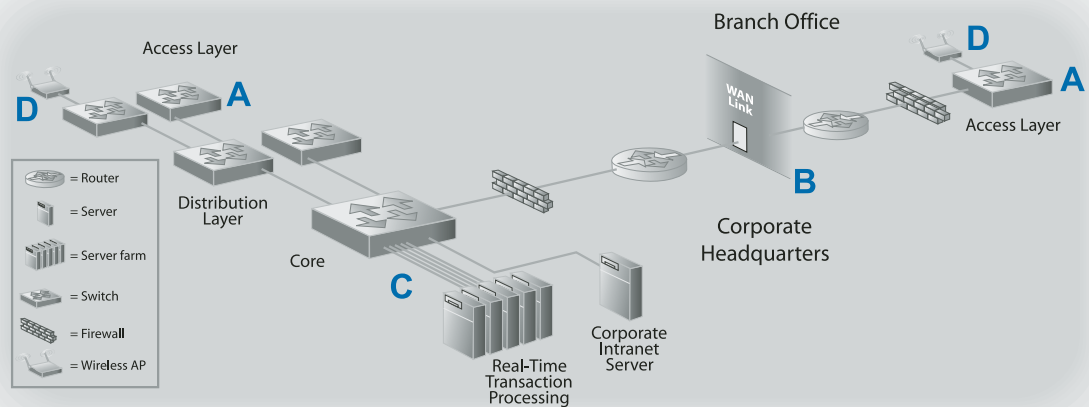
It is quite common for IT professionals to monitor multiple networks running on different media types. For flexibility in link analysis and monitoring, most gigabit analyzers include SFP (Small Form-Factor Pluggable)-based technology. SFPs are hot-swappable modules that can access different media types (Optical SX, LX, ZX, and Copper TX) and support varying data rates (10/100/1000). SFPs are an affordable alternative to purchasing multiple analyzers because the modules can be swapped out depending on the link under test. For example, if an analyzer currently monitors an optical SX link and a TX connection needs to be analyzed, the current SX-based SFP can be swapped out with a TX SFP.

Best Practice: Choosing an analyzer with integrated SFP-based technology is an efficient and affordable way to monitor links across various media types.

Ideal Points of Visibility

Even with the best gigabit capture technology, an analysis solution can only provide insight for the segments that are being monitored. That is why it is important to deploy capture technology strategically throughout the network. For example, if you are only capturing data on the edge of the network, you will never know what is happening at the core of the network, where the most vital information traverses. Therefore, deploy probes on high-traffic links, and those links that carry business-critical traffic. For more information on probe placement, download our whitepaper titled “Deploying Probes and Analyzers in an Enterprise Environment” at www.networkinstruments.com/products/white_papers.html.

Example Deployment



A) Ethernet Probe—An Ethernet probe connected to a switch’s SPAN port can show you top network users connected to that switch, help enforce corporate usage policies, and aid in troubleshooting station connections.

B) WAN Probe—A WAN probe deployed via a TAP on a WAN link can help to verify Service Level Agreements, monitor for intruders, and aid in troubleshooting branch office connections.

C) Trunk-Aware Probe—A trunk-aware probe deployed via TAPs on a trunk can show server, link, and application performance as well as aid in tweaking and troubleshooting trunk performance, and troubleshooting station connections.

D) Wireless Probe—A wireless probe helps to detect security threats so you can, detect and shut down rogue access points, and troubleshoot 802.11 connections.

But probe location is only half the solution. Because problems commonly extend beyond a single stream of data, and many networks support asymmetrical routing, it is important to have the ability to not only monitor data passing through individual links, but links in aggregate as well. Analyzers should support various SPAN sessions, full-duplex connections, and trunked links simultaneously. For example, if a capture card is configured with eight collection ports, you should be able to monitor two SPAN sessions, a two-link trunk, and a full-duplex link.

Best Practice: For complete visibility, install gigabit capture technology on highly utilized and business-critical links. Capture technology should also have the flexibility to analyze ports individually or in aggregate.

Conclusion

It is possible to make a complete and accurate analysis of gigabit links as long as the appropriate gigabit capture technology is implemented. Incomplete or inaccurate captures can skew data analysis, create false positives, and overlook problems that actually do exist. A gigabit capture card that provides a thorough report of network traffic will help to make better management decisions and keep IT professionals on top of the network.

Best Practices Reference Guide

Accessing Network Traffic	Rely on a TAP to access highly utilized or business-critical links. A switch's SPAN session and a port aggregator may be adequate for less critical, lower-utilized links.
Timestamping	For accurate timestamping across multiple gigabit links, rely on one card (one clock) with nanosecond resolution to timestamp all of the data.
Formatting the Raw Data	For analysis efficiency, choose a gigabit capture technology that can convert data into the native analyzer format on the capture card.
System Memory	For thorough and accurate real-time analysis, choose a capture card that streams directly to the buffer in physical system memory.
SFP-Based Technology	Choosing an analyzer with integrated SFP-based technology is an efficient and affordable way to monitor links across various media types.
Ideal Points of Visibility	For complete visibility, install gigabit capture technology on highly utilized and business-critical links. Capture technology should also have the flexibility to analyze ports individually or in aggregate.

Corporate Headquarters Network Instruments, LLC • 10701 Red Circle Drive • Minnetonka, MN 55343 • USA
toll free (800) 526-7919 • telephone (952) 358-3800 • fax (952) 358-3801 • www.networkinstruments.com

European Office Network Instruments • 7 Old Yard • Rectory Lane • Brasted, Westerham • Kent TN16 1JP • United Kingdom
telephone +44 (0) 1959 569880 • fax +44 (0) 1959 569881 • www.networkinstruments.co.uk

France, Italy and Spain Network Instruments • 1 rue du 19 janvier • 92380 Garches • Paris • France
telephone +33 (0) 1 47 10 95 21 • fax +33 (0) 1 47 10 95 19 • www.networkinstruments.fr

German Office Network Instruments • Allacherstrasse 189 • 80997 München
telephone +49 (89) 159 842-48 • fax +49 (89) 159 842-49 • www.networkinstruments.de