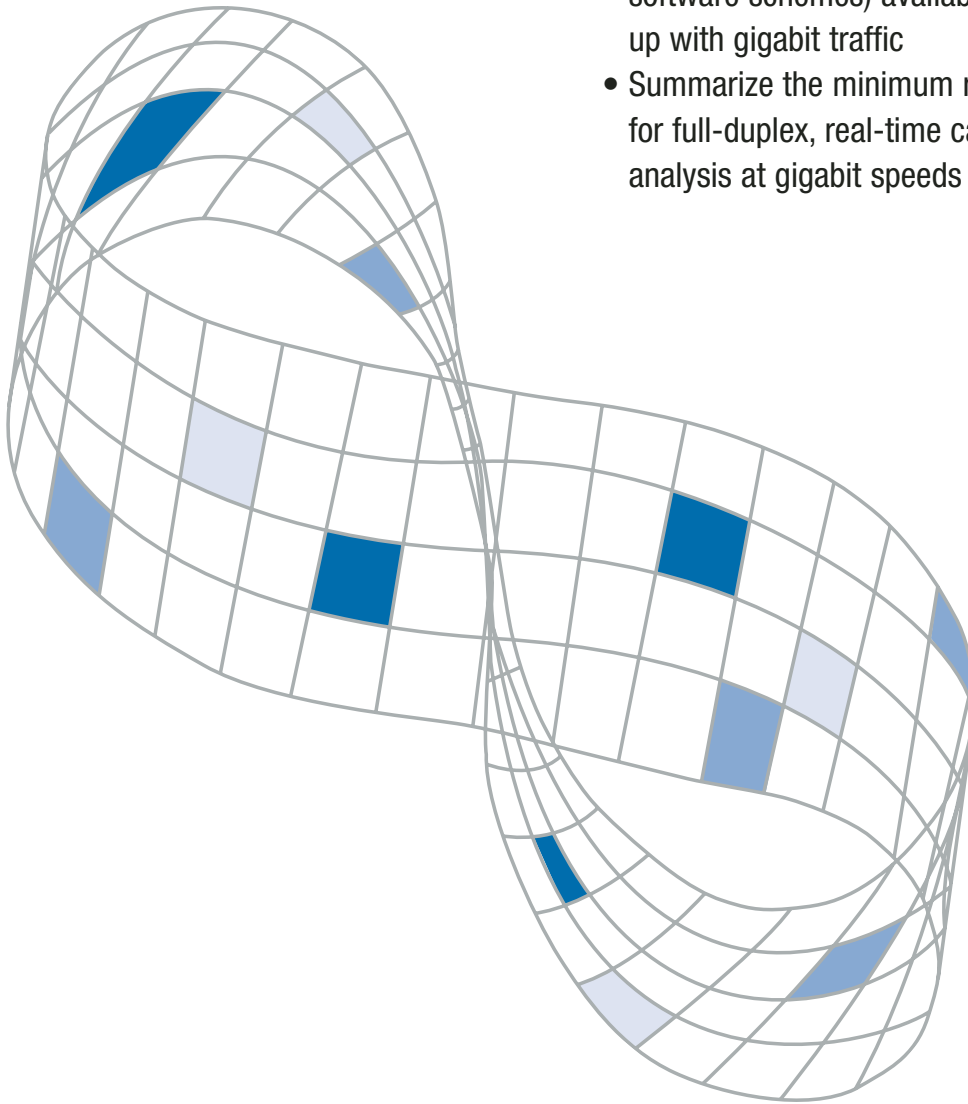


# Network Instruments Gigabit Capture Technology

Points to consider when choosing a gigabit analyzer

If you are in the market for a network analyzer that can keep up with your gigabit traffic, sorting through vendor claims and identifying the technologies required to manage the level of traffic at your site can be a daunting task. This paper will:

- Help you define throughput requirements for real-time gigabit network analysis
- Describe and examine the technologies (bus/card speed, buffers, and various software schemes) available to keep up with gigabit traffic
- Summarize the minimum requirements for full-duplex, real-time capture and analysis at gigabit speeds



## Gigabit Capture Technology: Defining Throughput Requirements

For low utilization gigabit networks, there are software-only solutions that can be combined with off-the-shelf gigabit network interface cards (NICs) to monitor the connection using a switch's analyzer port. Relying on the switch to process and redirect packets has a number of inherent limitations that you should be aware of:

- The switch's SPAN or monitoring port where the analyzer will be attached mirrors both sides of the full duplex gigabit link, transmitting the data stream out one side of a standard full-duplex switch interface. Although economical, the problem with this strategy is that as usage levels exceed 50% on each side of the full duplex gigabit link, the switch's analyzer port simply does not provide a big enough pipe for all the bits to pass through. The result is the switch will drop packets and thus the analyzer cannot provide valid analysis.
- In addition, SPAN port mirroring places an additional processing burden on the switch, which degrades its overall performance.

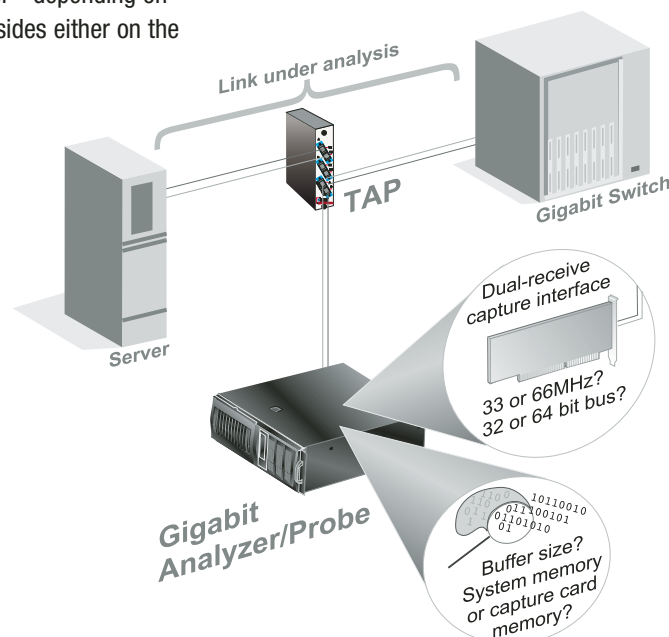
If gigabit network utilization is always less than the 1000Mb/sec total, an off-the-shelf gigabit adapter and a standard analyzer running on a switch's SPAN port is an adequate solution.

If utilization exceeds the 1000Mb/sec total offered by a switch SPAN port, a more robust solution is required. Most major players in the analyzer market offer one or more gigabit-specific hardware products. These solutions typically include capture hardware specifically designed for gigabit speeds coupled with a network Test Access Point (TAP).

## Anatomy of a Full-Duplex Gigabit Analyzer

Although the different gigabit analysis hardware solutions offered by various vendors vary widely in price and performance, they all share a number of common features:

- A network Test Access Point (TAP) - a device that passively captures both sides of the full-duplex link, and transmits a copy of the packets back to analyzer.
- A full-duplex dual-receive capture card - a special-purpose gigabit network interface card. Instead of the standard gigabit TX/RX ports, this card is designed to accept both sides of the full-duplex link from the TAP. Firmware software on the NIC timestamps and integrates the data streams into a coherent flow.
- A packet capture buffer - depending on the vendor, the buffer resides either on the capture card itself, or in system RAM.



## Not all Hardware Solutions are Created Equal

Beyond the broad similarities in the solutions that vendors are touting to overcome the challenges of gigabit analysis, products differ wildly in their claims and actual performance. A high price tag doesn't necessarily indicate the best performance. There are many items to consider before choosing a gigabit analyzer that can actually do the job. Looking at the three components of the solution independently will allow you to find the best solution for your needs.

### Network Test Access Point (TAP)

With TAPs, there is not much difference between one vendor and another's implementation of this basic technology. In fact, a few third-party manufacturers supply the same TAP hardware to multiple vendors.

### Full-duplex Dual-Receive Capture Card

With dual-receive capture cards, significant differences start to emerge. Network Instruments jointly developed a dual receive gigabit capture adapter with SysKonnect Corp. (now Marvel Corp.). Starting with an existing Marvel capture adapter, Network Instruments has re-written the firmware code, replaced a number of key chips on the adapter, and developed Windows drivers from scratch to support the new hardware and firmware.

Network Instruments' gigabit capture card outperforms competitive solutions from Network General (Sniffer products) and WildPackets (Peek and Omni products) by offering a number of key advantages.

Network Instruments capture adapter clocks at 66 MHz, and plugs into a 64-bit bus. The support of the 64bit, 66 MHz bus allows Network Instruments' products to stream gigabit traffic at wire speed to system memory rather than an onboard cache. Competing products (including Network General's Sniffer and WildPackets) capture cards clock at 33 MHz and plug into a 32-bit bus, depending on an on-board cache to store the collected data. These slower cards can not move data at the required speed for real-time analysis. For more information on why 64bit, 66Mhz based cards are a requirement for real-time gigabit capture, please see our white paper: [www.networkinstruments.com/assets/pdf/64BIT\\_capture\\_card.PDF](http://www.networkinstruments.com/assets/pdf/64BIT_capture_card.PDF)

### Packet Capture Buffer

The Network Instruments gigabit solution can stream gigabit traffic to a buffer residing in system memory in real-time, offering two very important performance advantages over other vendors' capture functionality.

First, it allows our solutions to utilize locked system RAM (up to 4 gigabytes) to either store captures, or for continuous capture using a circular buffer. A 4GB capture buffer equates to either a 14 second capture at wire speed, or a 14 second sliding window (using a circular buffer) to view problems or perform expert analysis. Competitive products are limited to capturing to the RAM on the capture adapter. In the case of Wildpackets, they use Xyratex-based capture cards ([www.xyratex.com](http://www.xyratex.com)) that have 64 megabytes per channel, or 128MB total. A buffer of 128MB equates to less than a second of capture.

Second, the WildPackets and Sniffer products cannot do wire speed real time analysis. WildPackets and Sniffer products are limited to capturing traffic to the capture card's onboard RAM. Once this RAM buffer is full, the capture process must be stopped to transfer the 128MB capture buffer to the analyzer for expert processing or further analysis. Because Network Instruments' gigabit products stream the traffic to system RAM in real time (no bus limitation as mentioned above) we can perform real-time capture and thus real-time expert analysis of gigabit traffic flows.

Vendors offering slow cards, narrow buses, and small capture buffers (such as Network General's Sniffer and WildPackets Gigabit products) may argue that filtering (in other words, capturing only pre-selected packets) and packet slicing (capturing only pre-selected portions of packets) overcome these fundamental limitations. But filter-based workarounds assume that you know in advance what you are looking for, which isn't always the case in troubleshooting situations. And in many forensic applications, you simply cannot discard any packets, as an unknown quantity of un-captured packets compromises the evidentiary value of what you did capture.

## Summary

A capture buffer located on the capture board, coupled with a narrow system bus or a slow clock rate (as provided by WildPackets and Network General) makes true real-time analysis impossible. The tiny onboard cache provided by these vendors mean that you won't be able to capture from a highly-saturated network for even a second without overflowing the buffer and dropping packets.

Network Instruments Gigabit Observer products are the most robust and scalable in that they combine a fast card and wide bus interface with a unique method of using up to 4GB of locked system memory to cache packets, making the packets immediately available for true real-time analysis.

Additionally, other vendor's arguments of capture speed versus analysis speed is simply a cover up for a substandard product. Network Instrument's gigabit products use a unique architecture that utilizes different processors and priorities for capture and analysis to insure both are done completely, and in real-time. Anything less is simply an excuse for inferior engineering.

### Putting it All Together

Only Network Instruments puts all of these pieces together into a system that can handle any traffic levels you might encounter on your gigabit network. Compare our specs to those of WildPackets and Network General, and it will become clear—where they offer hand waving equivocations, NI offers real performance engineered for the real world. Please visit our website to look at our comprehensive product line, which provides you with the same familiar user interface regardless of topology (10/100/1000 Ethernet, WAN, and WLAN) under analysis.

**Network Instruments, LLC** 8800 West Highway Seven, Fourth Floor, Minneapolis, MN 55426 telephone (952) 932-9899 fax (952) 932-9545

**Network Instruments** 7 Old Yard, Rectory Lane, Brasted, Westerham, Kent TN16 1JP United Kingdom telephone +44 (0) 1959 569880 fax +44 (0) 1959 569881

**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

© 2004 Network Instruments, LLC. All rights reserved. Network Instruments and the Network Instruments logo are trademarks or registered trademarks of Network Instruments, LLC.