
On Gigabit Analysis System Performance and System Requirements

WildPackets regularly receives questions from customers asking, "What is the capture rate for GigaPeek?" Before answering that question, one must first understand the gigabit analysis environment both in terms of its possibilities and limitations, as well as with respect to how vendors approach this market.

To understand gigabit analyzer performance, it is important to understand the nature of gigabit network segments and the architecture of different network analysis "systems". This paper will pose a series of questions that relate to the performance of the different components of an analysis system and will provide perspective and an answer for each. Prospective buyers should request an answer to each of these questions from each protocol analyzer vendor when comparing tools.

Gigabit Ethernet analysis equipment falls into two distinct categories. The first category includes analyzers that utilize proprietary hardware designed to capture 100% of packets at line rate speed. Analyzers that fall into this sub-category include the Sniffer Portable, Sniffer DSS, Sniffer s6040, and WildPacket's Gigapeek NX. The second category includes analyzers that utilize off-the-shelf network interface cards (NICs). These products may include a custom driver or use the existing NDIS driver. Analyzers that fall into this category include Network Instruments Observer product, and EtherPeek NX. EtherPeek NX, for example, can work with SysKonnnect, Intel, or any standard 10/100/1000 NIC to capture data. Observer uses a standard SysKonnnect NIC with some driver modifications.

First, let's delineate the difference between these two approaches. Each offers a trade off between cost, features, and performance. Using an off-the-shelf NIC is typically the least expensive approach to gigabit network analysis. Products that support the native NDIS drivers can capture data off gigabit segments without modification. This means they support 10/100 as well as Gigabit, including both fiber and copper Gigabit segments. Further, these products can take advantage of Ethernet switches' port mirror functionality to perform full duplex analysis using only a half-duplex stream. In other words, the switch handles merging the two streams inherent in a full duplex segment, and passes the data out the mirror port in one stream so that a standard Ethernet analysis product like EtherPeek NX can capture the data using an off-the-shelf NIC. Note that this system cannot perform full duplex gigabit analysis or line rate speed, since a port mirror has throughput limitations.

Some vendors, have therefore, enhanced the capability of the standard NDIS driver by merging the streams in the driver itself. This approach allows you to use an off-the-shelf NIC for full-duplex analysis in-line using a tap, rather than through a port mirror.

The proprietary hardware approach can offer several advantages depending on the system setup. Typically, custom analysis cards filter and slice packets on the card, allowing for higher performance during capture and analysis. The cards also support hardware-based time-stamping, which is critical to accurate merging of the two data streams. Finally, some solutions using customized hardware offer the same flexibility as NIC solutions by supporting both copper and fiber, and the ability to be used both in-line and with port-mirroring.

Finally, we need to clearly define the terms related to analyzer system performance. When vendors refer to capture rate, they mean how fast the hardware is pulling packets off the wire. By analysis, they mean how fast the software can process the packets received from the capture. It is important to understand that just because a vendor provides hardware that can capture all the packets, it does not mean that their software can process all the packets.

What is the gigabit ethernet analyzer performance?

Capture Rate

- Solutions utilizing custom hardware will capture 100% of packets at "line rate" of full duplex Gigabit network segments. Solutions using off-the-shelf NICs with customized drivers might capture at full line rate. Solutions using off-the-shelf NICs and standard NDIS drivers, by definition cannot exceed 50% of line-rate, since they can only capture half-duplex.
- All solutions with custom hardware or custom NDIS drivers can only capture at full-line rate until the point the memory buffers on the hardware are full.

Analysis Rate

- While most vendors claim "real-time" analysis, most solutions only pass the packets to the software for analysis after the memory buffers on the hardware are full. In other words, one starts the capture, the capture stops when the buffer is full, then the packets are quickly passed to the software for analysis.
- GigaPeek NX is the only analyzer we know of that can not only capture until the buffers are full, but also capture and analyze and decode the packets in true real time, even after the memory buffers are full! We call this sustained real-time analysis.
- Hardware filtering and packet slicing are also key to the analysis rate. If the hardware does not support onboard filters, your analysis rate is not optimal. Why is this? Say you have a gigabit segment running at 10% utilization and 64 MB hardware buffers. If you were to capture this data, your buffers would fill up in a little over five seconds. If you are able to provide filters on the card, however, to reduce the amount of traffic relevant for analysis to 50% of the utilization, you double the amount of packets you capture.
- Here is another example. Say you are using GigaPeek NX for sustained real-time analysis. Say the network is running at 60% utilization. (You have a serious problem on your hands.) With GigaPeek NX, you can still analyze this segment, in real-time, while sustaining capture, by applying filters and packet slicing.

What is the capture and analysis rate of GigaPeek NX?

- GigaPeek NX captures full-duplex gigabit at full line-rate.
- GigaPeek NX performs hardware filtering and packet slicing at full line rate.
- GigaPeek NX performs quasi-real-time analysis until the hardware buffers are full at full line-rate.
- Exclusive: GigaPeek NX performs sustained real time analysis at 5-30% traffic rate. This is equivalent, for example, to full line rate with 70-95% traffic reduction using hardware filters and slicing. The range is dependent upon the type of capture and analysis being performed, as well as by the system hardware running GigaPeek NX.

How big is GigaPeek NX's on-board memory buffer?

GigaPeek NX GAC card has an onboard buffer of 64MB per channel. The buffer of standard NICs depends on the card. They Sysconnect 98xx cards have 1 MB per channel.

How does packet size relate to analysis performance?

If a network consisted of all one packet size it would be a simple matter to duplicate network behavior in the lab and produce performance numbers. The reality is that many different packet sizes are present on a real-world network. In the lab, however, we have determined that

small packets (64-bytes) require more work to process on a continuous basis than do maximum size packets (1518-bytes).

Will a faster host computer improve analysis performance?

Up to a certain point. Memory, CPU, and bus performance all affect how fast packets can be processed. There is a limit to packet processing as stated above, however, beyond which increasing host system performance will not affect. WildPackets offers both minimum system requirements and recommended system requirements. The type of system you will need depends on the type of analysis you wish to do, the utilization on the gigabit segments, and your budget.

How does the real world compare to the test lab in terms of gigabit segment utilization?

We have been using our Gigabit analysis tools in the field, for on-site consulting, since early in 2003. We have sent our engineers to numerous customer sites to perform real-world testing of the products. Our findings are that we have not found any networks with sustained segment data rates of greater than 500 Mbps (.5 Gigabits/second). There are situations in which bursty traffic may momentarily exceed this, but it appears that the reality of the situation allows sufficient time for removal of the packets from the card's on-board buffer with no subsequent packet loss.

Why do many analyzer vendors report "100% capture rate" for Gigabit Ethernet?

It's common to hear a vendor indicate that their analyzer provides a 100% capture at full line rate. WildPackets GigaPeek and EtherPeek NX with a Gigabit Ethernet NIC also support a 100% capture rate in this context. When a vendor says this, they're referring to the acquisition of packets into their card's on-board buffer and does not guarantee that the packets will ever make it to the analysis software. GigaPeek NX is the only analyzer we know of that can analyze data in a sustained fashion beyond the limits of the buffer.

How do I determine what I need?

The questions below are designed to help you choose the appropriate solution.

- Do you need to analyze in-line analysis or via a port mirror?

Remember, most switches today offer port mirroring. This capability merges streams from full duplex segments and streams the data out the port mirror. This is a very effective way to perform full duplex GB analysis. There are limitations to analyzing via a port mirror, however. The throughput of a port mirror is by definition, one half of full duplex gigabit. VLAN tags are stripped and in general, there is a lack of flexibility inherent in configuring port mirrors.

- How does utilization rate effect the type of solution I should choose?

If your switch doesn't support port mirroring, you will, of course, need an in-line gigabit analyzer and a tap. There is no hard and fast rule, but you probably need a custom card when utilization rates exceed 10%. The custom card that has hardware based timestamping, channel aggregation, packet slicing and filtering, allows you to optimize analysis no matter what the utilization rate.

- Why should I care about timestamping ?

For full duplex analysis, timestamping is critical. The merging of the two streams of full duplex segments is based on the packet timestamp, so it is critical that the timestamps are as

precise as possible, occur on hardware, and that the two channels are accurately synchronized. Inaccurate timestamping will lead to spurious analysis.

WildPackets Professional Services

WildPackets offers a full spectrum of unique professional support services, available on-site, online or through remote dial-in service.

WildPackets Academy

WildPackets Academy provides the most effective and comprehensive network and protocol analysis training available, meeting the professional development and training requirements of corporate, educational, government, and private network managers. Our instructional methodology and course design centers around practical applications of protocol analysis techniques for Ethernet and 802.11 wireless LANs.

In addition to classroom-taught Network Analysis Courses, WildPackets Academy also offers:

- Web-Delivered Training
- On-site and Custom Courseware Delivery
- The (T.E.N.) Technology, Engineering, and Networking Video Workshop Series
- On-site and Remote Consulting Services
- Instruction and testing for the Network Analysis Expert (NAX™) Certification

For more information about consulting and educational services, including complete course catalog, pricing and scheduling, please visit www.wildpackets.com/services. NAX examination and certification details are available at www.nax2000.com.

Live Online Quick Start Program

WildPackets now offers one-hour online Quick Start Programs on using EtherPeek NX/ EtherPeek and AiroPeek NX/AiroPeek, led by a WildPackets Academy Instructor. Please visit www.wildpackets.com for complete details and scheduling information.

About WildPackets, Inc.

Since 1990, WildPackets has built affordable and easy to use network analysis tools. Our customers rely on WildPackets tools to help them design, maintain, troubleshoot, and optimize their networks. For information about our company, its products and partners, please see our website at www.wildpackets.com. See the WildPackets Academy site, www.wildpackets.com/services, for information on courses and Professional Services offerings. WildPackets' Network Analysis Expert (NAX) Certification Program details can be found at www.nax2000.com.

WildPackets, Inc.
1340 Treat Blvd., Suite 500
Walnut Creek, CA 94597
925-937-3200
www.wildpackets.com

