

What is a Protocol Analyzer?

With the evolution of today's advanced LAN and WAN networks, everything about the protocol analyzer has changed except the name. Originally designed many years ago to monitor single-protocol proprietary WAN circuits operating at 9600 bits/s or less, early protocol analyzers were little more than capture and decode boxes. Because early WAN circuits were usually single-protocol environments, making use of the decoded frames was left to the user.

Today's protocol analyzers must be able to decode multiple protocols simultaneously at speeds undreamed of 10 years ago. Along with the detailed protocol decodes, the analyzer must monitor the network and provide details on a number of different statistics, events and error conditions. The current breed of protocol analyzers provides an overall view of network performance and utilization as well as specific details on individual users and applications.

Protocol analyzers offer some advantages over other technologies: real-time analysis, problem resolution, and performance analysis for network planning and identification of specific issues that may be overlooked by RMON Probes or network management platforms.

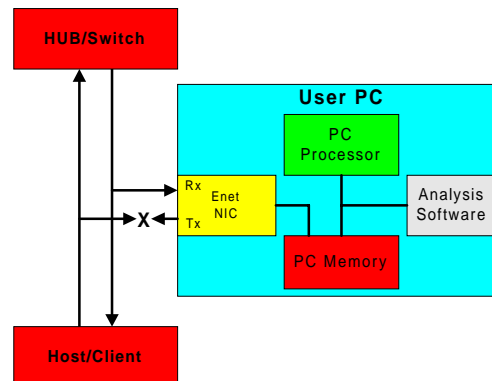
With prices ranging from several hundred to tens of thousands of dollars, anyone thinking about buying a protocol analyzer is faced with many choices. Choosing the right product for your needs may take some investigation but is not impossible. Arming yourself with the right information can ensure that you make the right choice the first time.

Software LAN Analyzers

At the low end of the LAN analyzer scale are the software analyzers. Costs are kept low by designing software that loads on the user's PC and runs under a standard operating system with an off-the-shelf LAN interface card. Recent advances in PC power and LAN chipset performance make software analyzers viable in many low to moderately utilized networks.

For Ethernet and Token Ring applications, the user needs a NIC that supports *Promiscuous Mode*. This feature allows all frames on the network segment to be passed by the NIC to the PC for processing and analysis. Without promiscuous mode capabilities, the NIC itself would filter out frames because of their destination MAC addresses, rendering the analysis of little or no use.

Because the software is loaded on the user's PC, it is actually the PC that is performing all analysis functions. The processing power of the PC, amount of memory, NIC capabilities and amount of LAN traffic all have an impact on the performance of a software analyzer.



The Software Analyzer functional block diagram shows the reason it can only work on broadcast type half duplex networks.

If the LAN is heavily utilized, there is a possibility that a software analyzer may not “see” all of the packets on the network. This is because the PC processor must process every packet. Imagine a 166 MHz processor trying to keep up with thousands of frames per second on a 100 Base-T Ethernet circuit while running Windows® 95. With a high-performance PC and LAN card, results can be surprisingly good on a low to moderately utilized network without excessive numbers of frames per second.

Decode Analysis: Analyzing the protocol details

Many software analyzers do not provide great depth of decode analysis. This is not the fault of the analyzer but an effort to keep cost low. Understanding and making use of the information provided by decode engines is not an everyday skill. Having the information available when calling for support, however, can be very valuable. Always look for a powerful decode engine even if you feel you don’t currently need the depth of detail provided.

Monitoring utilization and providing statistics is another capability of quality software analyzers. This can be quite useful for performing LAN traffic analysis. Generally software analyzers will provide information on general traffic patterns without getting into great detail. Look for units that display not only the amount of IP, IPX and HTTP traffic, but also those that provide detailed information on traffic patterns and protocols.

Filtering: Narrowing down the problem zone

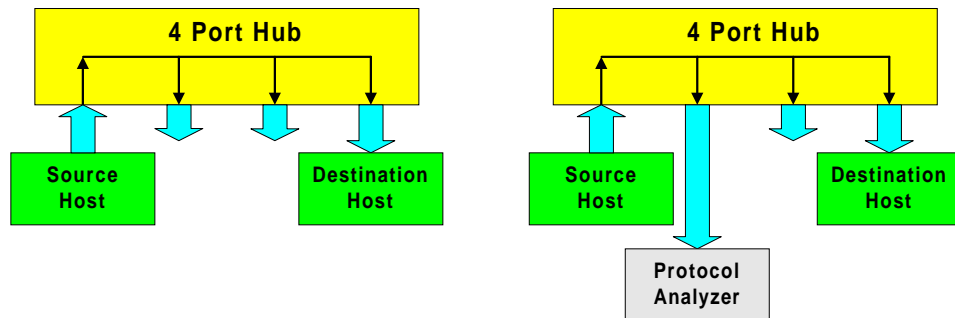
To help narrow the focus for troubleshooting specific problems, a user may want to set a filter. This can allow only specific frames to be captured. For example, you may only need to see frames to and from a specific workstation. With a software analyzer, every frame must be brought into the PC and evaluated with respect to your filter settings. At that point, a decision is made to save the frame or discard it. This type of filtering is dependent upon the PC and tends to be processor-intensive. On a high-utilization 100Base-T network, some missed frames should be expected.

Monitoring Limitations: Half duplex and full-duplex issues

One limitation common to software analyzers is the inability to operate in full-duplex mode. For many users this is not a problem, and if the connection to the network is available through a hub port, then half duplex is probably adequate.

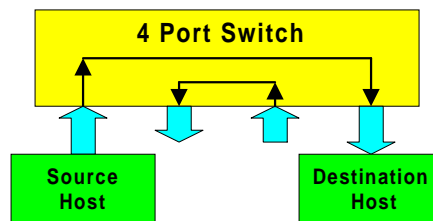
Switched Ethernet environments, on the other hand, pose problems for half-duplex software analyzers.

As can be seen in the figure below, the classic “Ethernet Hub” method provides easy connection for software analyzers. With hubs, all frames entering the hub are transmitted to all ports attached to the hub. This means that the protocol analyzer can be attached to any open port of the hub and still be assured of seeing all data entering the hub.



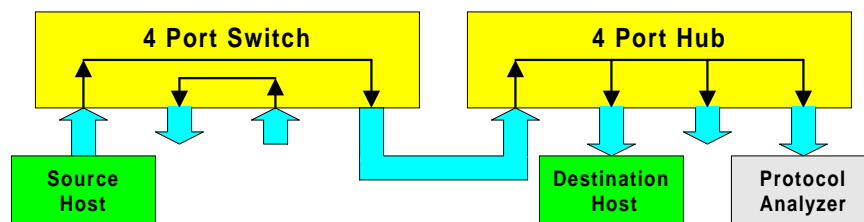
Ethernet hubs are broadcast devices allowing easy connection of protocol analyzers

Complications can arise when Ethernet switches are employed in the network. Unlike the shared media broadcast approach of the hub, Ethernet switches are intelligent devices. By “learning” the addresses of devices connected to each port, they pass the frames only between the required ports. This leaves other ports free and does not flood every port with every packet as hubs do.



Ethernet switches do not broadcast data out all ports

One way to get around this problem is to connect a hub to the port of the switch you want to monitor, as shown. Whenever possible, you should try to insert the hub on the least utilized switch port connecting two devices. Switch ports connected to clients generally have less traffic than ports connected to servers.



Connecting software analyzers to Ethernet switches may be done with a hub. This type of connection may not work in some full duplex environments.

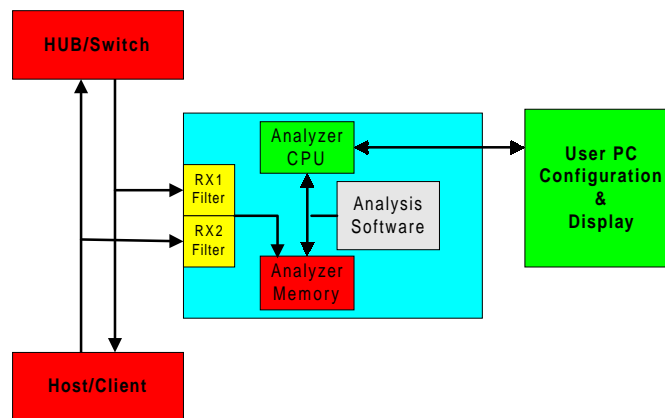
Some software analyzers offer special NICs. These can be PCI, PCMCIA or Cardbus types. Generally these cards provide improvements in monitoring specific conditions, such as collisions, when compared to “off-the-shelf NICs”. These optional cards should not be confused with true hardware analyzers, as the PC is still required for capture and analysis.

Hardware LAN Analyzers

When very high performance with extensive protocol and traffic details are required, the hardware analyzer is the tool to have. Hardware analyzers use custom-designed hardware circuitry combined with special software to ensure high performance when monitoring and capturing data. Hardware analyzers employ special processors dedicated to capturing and analyzing the network data. Unlike their software cousins, hardware analyzers are not dependent upon the PC processor for capture and analysis performance.

Hardware Filtering: High-performance filters

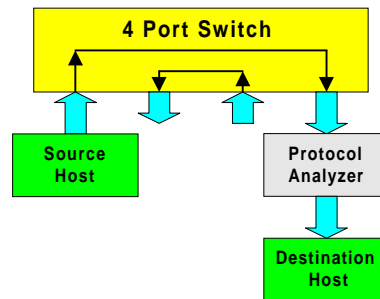
Hardware analyzers contain special circuitry that can be set up to filter in or filter out specific frames based upon user-defined characteristics. This special circuitry eliminates the need to have processor-interrupt cycles involved in the frame-examination process and reduces or eliminates the chance of missing desired frames on heavily utilized networks. This type of filter capability is referred to as “hardware filtering.”



Hardware analyzer functional block diagram

Specialized Functions: Time-saving features

Another key feature of quality hardware analyzers is their ability to monitor full-duplex Ethernet circuits. Many circuits, in particular switched Ethernet environments, can only be monitored with a “dual receiver” hardware analyzer. This full-duplex capability doesn’t prevent attaching them to standard hub ports.



Connecting pass through cable hardware analyzers to Ethernet switches and hubs requires no special equipment.

Because of the specialized hardware, users can often obtain specialized applications to expand the capabilities of the analyzer. These may include long-term monitoring applications and expert systems that will operate “real time” on the network. When looking to purchase a hardware analyzer, look at the options available. You may not need them today, but needs change with technology and paying a little more now for a unit that can grow with your network may be a wise investment.

Some hardware analyzers can also support multiple-segment analysis. This is a method of monitoring more than one segment of a network at a time. For example, both the LAN and WAN side of a router can be monitored to analyze the traffic passing through the router. When you run into problems with routing, switching or application timing issues, it may help to resolve the problem if multiple analyzers can be used to ensure packets are being routed or switched correctly without excessive network or device transit delay.

Architectures: Design concepts

Hardware analyzers come in two basic types. The first is a self-contained unit with all interface cards and controls (keyboard, screen, etc.) in one piece. This has the advantage of being a self-contained, one “box” device, but it may lack some flexibility. With an “*all in one package*,” there are limits to what you can do with the product. It becomes difficult to upgrade the unit and newer technologies may not be adapted to the unit easily. Distributed applications also require the entire unit to be placed on site.

The second type of hardware analyzer is the stand-alone “box” or “pod” that connects to a PC. This has the advantage of letting you use your current laptop to control the analyzer. Captured information is saved to your PC’s hard drive and can be looked at later without having to set up the test equipment. It also makes it easy to export information you have gathered to applications residing on the laptop for the purpose of generating reports or e-mailing captured information.

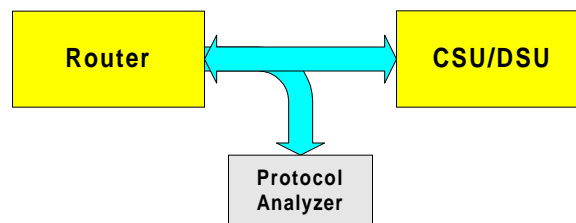
Another advantage of the stand-alone hardware analyzer is cost. A manufacturer of hardware analyzers with the PC built in is in the position of spending time and money developing a PC when a better one at much lower cost is probably available off the shelf. If your company uses a standard laptop and gets volume discount pricing, you may save money going with an external hardware analyzer.

There are manufacturers that make internal NICs that operate as hardware analyzers. These usually take the form of PCI cards and contain a processor and

other hardware dedicated to performing analysis. This does not mean that all PCI-based analyzers are hardware. The true difference between hardware and software analyzers is a function of where and how the data is collected and processed.

WAN Analyzers

Because of the way a WAN works, there are no true software WAN analyzers. By its very nature, a WAN circuit is bi-directional. This means that both the DCE and the DTE have one transmitter and one receiver. In addition, specialized interface requirements are broad for WAN applications, with many speeds and termination types to consider. To monitor traffic in both directions, the analyzer must be able to monitor both the transmit and receive directions, and that requires two receivers. The most common method of attaching a WAN analyzer is with a “Y” cable.



Typical method of connecting a WAN analyzer is with a “Y” cable

When monitoring traffic, WAN analyzers should be able to handle the various types of encapsulations your network uses. This includes PPP, frame relay, SDLC, etc. Remember that your network may change, so be sure your analyzer can accept the needed enhancements required to keep it current.

One important feature to look at when considering a WAN analyzer is compatibility with a LAN analyzer. Buying products that share the same design concepts and work well together will prove a wise choice. Your current needs may be for a WAN analyzer, but in the future your network needs may require you to add a LAN analyzer. By choosing equipment that works together as a team, the combined analysis capabilities of the pair can be greater than the sum of the parts. Look for common tools such as protocol decode applications and consistent graphs and charts used on both the LAN and WAN analyzer.

Distributed Analyzers

Distributed analyzers are designed to provide analysis at key points throughout the network. Available in both hardware and software versions, the idea is to place analyzers on various segments and control them from a remote location. Distributed analyzers come in software and hardware versions for LAN and hardware versions for the WAN.

With software analyzers, it is often acceptable to place the analyzer “agent” in a user PC and let the analyzer software run in the background when needed. This allows the MIS department to connect and run the analyzer as needed. The number of distributed agents in a network can range from a few to hundreds depending upon the needs of the user.

When selecting the PC for the agent, there are things to keep in mind. Select a PC that will not be turned off. Some users will install a PC dedicated to running the agent on the network. This allows access and eliminates the chance of the user altering the configuration in such a way as to stop the agent. There will also be some improvement in performance if no other applications are being run concurrently with the agent.

Hardware analyzers require the user to place the units at various locations throughout the network. Hardware analyzers are often used to run regular baselining and monitoring as well as analysis. This allows the MIS department to connect and take a look at the current state of the network and compare it to historical data collected over time. With this information, trends in network utilization can be monitored and addressed before they become problems.

If you are going to distribute hardware analyzers, be sure to investigate how you attach and control the unit. While many users connect through the LAN, it is always good to have a dial-up connection. A distributed analyzer that you cannot connect due to a network outage won't be of much help.

A distributed hardware analyzer should support a method of segment switching. By employing matrix switches, the user can connect the analyzer to multiple hub and switch ports and remotely select which port to monitor. This eliminates the need to buy multiple analyzers. Matrix switches are available for supporting all forms of LAN and WAN circuits.

Many users opt for a combination of hardware and software analyzers in a distributed system. This often takes the form of distributed hardware analyzers placed on critical segments, such as a backbone Ethernet or ATM circuit or a frame relay WAN circuit. This is augmented with distributed software analyzers loaded on PCs connected to less critical Ethernet segments. Be sure that the key applications, such as protocol decode engines, operate in the same way for both your hardware and software analyzers.

Software analyzers are often loaded on a number of users' PCs on key segments throughout the network, while hardware analyzers are located near routers and switches in equipment rooms. This is a cost-effective way to provide individual segment analysis at low cost while placing the power of hardware analyzers where they will be of the most benefit.

What's Right For You?

Picking the right analyzer for your network and your needs starts with what you hope to learn from the analyzer. If you need basic LAN monitoring and troubleshooting capabilities, the software analyzer may be the right choice. Hardware LAN analyzers are more complex to set up and operate but provide large amounts of information that network experts deal with on a regular basis. If you are not this type of power user, the complexity and detail of information may not be of help to you. The software analyzer, with its simplicity and ease of use, might be a better choice.

If you are looking at a software analyzer, make sure there are some options available to improve the power of your analyzer. Users often start out with the basic software analyzer components loaded on a laptop they take with them from site to site. After becoming more familiar and comfortable with the tools, they

find they could benefit from additional capabilities, such as a more powerful expert analysis application. With some software analyzers, there is no ability to add these features and the user must replace the entire tool for increased power.

If you are responsible for LAN segments distributed over a large area, the distributed software analyzer may cut down on travel time. A report of slow application response from a user can be investigated from your desktop by attaching to an agent on the segment in question. With low-cost agents distributed around the network, complaints of unacceptable performance can quickly be analyzed and the root cause identified. When network changes are considered, the network can evaluate current performance and determine the impact of adding new users or applications to a segment.

Hardware LAN analyzers are true power-user tools. A quality hardware analyzer provides tremendous amounts of information about the network and is best for tracking usage and protocol distribution on high speed, high utilization segments and backbones. With their transmit capabilities, they can be used to test WAN and LAN circuits for errors as well as commission new circuits. These are the tools of the professional responsible for network turn-up, maintenance, analysis and troubleshooting.

Something often overlooked is expert analysis systems. A 100Base-T Fast Ethernet circuit can easily generate 20,000 frames in one second. This volume of traffic can overwhelm the user trying to capture and analyze it. While filtering for specific types of frames can help, a quality expert system can examine volumes of data. This is especially useful when the interaction between different applications is causing problems. Remember: the object is to identify and resolve problems. A good expert system makes you an expert, but does not require you to be an expert to use it.

Portability is another important consideration. Think about where you plan to use your analyzer. Some analyzers will never leave a building, so issues of size and weight are less important. If you will be traveling with your analyzer, however, consider how it will go through airports and fit in your car.

Many users have a laptop computer they use on a daily basis. If you get an analyzer with a built-in PC, you now have two PCs to carry. When you are running across a parking lot on a rainy day, the last thing you need is 50 pounds of equipment slung over your shoulder.

If you plan to generate reports or import the gathered information into other documents, be sure your analyzer supports these functions. This is important when trying to send captured information to technical support or a help desk. By converting the captured data into a standard format, the intended recipient does not need to have the same analyzer software loaded on their PC.

Perhaps a mix of software and hardware analyzers would suit your needs. This allows multiple users to have relatively low-priced software analyzers with hardware analyzers on hand when the power or application requires.

What Does WWG Offer?

Wavetek Wandel Goltermann offers a range of network analysis equipment. From the LinkView PRO™ software analyzer to the Domino® family of

hardware analyzers, we make a product to fit your current need and allow it to grow with your network. Our products support LAN from 10 Mbit to Gigabit Ethernet, WAN from RS232 to HSSI, and a full range of ATM tools, in portable field service units or distributed systems.

Software Analyzers

All software analyzers listed below include Examine™ for protocol decoding. Files captured using LinkView® are fully supported in Mentor™ for expert analysis.

LinkView PRO with Examine™ is an economical software analyzer. Designed for field service and MIS departments, it will work with a variety of NICs and provide a range of information to identify problems and monitor usage on your LAN.

LinkView PRO™ Distributed extends the power of LinkView by allowing software agents to be placed in PCs. Around the building or around the world, you have visibility into network segments with the click of a mouse.

LinkView PRO™ Collision Expert comes in either a PCI or 32-bit Cardbus NIC designed to identify collisions on Ethernet networks. Field-service engineers can benefit from this extra capability when troubleshooting high-utilization Ethernet networks. The 32-bit NIC is a high-performance 10/100 card that improves the monitor and capture performance of LinkView.

Hardware Analyzers

Domino hardware analyzers are connected to, and controlled by, just about any Windows®-based PC. Combinations of up to eight Domino analyzers can be connected to a single PC and run simultaneously. With multiple-Domino stacks, the captured information is time synchronized for true multisegment analysis. Like the software analyzers above, Domino hardware analyzers use Examine for protocol decoding.

DominoPLUS™ is a single portable chassis with plug-in interface modules that reduces the cost of supporting multiple network technologies. More than 20 LAN/WAN & ATM interfaces are supported on nine different plug-in modules.

- **DominoFE™** is a 10/100 Fast Ethernet hardware analyzer module for the DominoPLUS chassis. Capable of operating in full- and half-duplex mode, it can work with Ethernet switch mirror ports and hub ports or can be placed in-line for backbone applications
- **DominoHSSI™** is a plug-in module for the DominoPLUS chassis. Supporting speeds up to 52 Mbit/s, DominoHSSI provides a solution for high-speed WAN analysis. Supported interfaces on this single module include HSSI, V.35, V.36, V.11, X.21, RS-449 and RS-530.
- **DominoATM®** is a series of plug-in modules for the DominoPLUS chassis. With speeds from DS1/E1 to OC-3/STM-1, DominoATM provides the users with an economical way of adding ATM support to their WAN and LAN analyzers.

DominoLAN® is a combination 10 MB Ethernet and 4/16 MB token ring network analyzer. With support for a number of different media types, it provides hardware analysis capabilities at a low price. Full Mentor™ expert analysis and Wizard™ baselining support is provided.

DominoGigabit® is a Gigabit Ethernet network analyzer that uses industry-standard GigaBit Interface Connector (GBIC) modules. This allows a single chassis to support single mode and multi-mode with the simple change of plug-in interface modules. Capable of full-line rate, full-duplex operation, the DominoGigabit analyzer is the industry leader in this emerging technology.

DominoWAN® is intended for WAN circuits with speeds up to 2 Mbit/s. Four plug-in modules are available to support a wide variety of WAN interface modules.

- **T1 interface module** supports full T1 as well as FT1 and Primary Rate ISDN.
- **E1 interface module** supports full E1 as well as FE1 and Primary Rate ISDN.
- **BRA interface module** supports S/T interface Basic Rate ISDN. Support of U interface BRI is available with the addition of the IUM-10.
- **V series interface module** supports V.36, V.35, V.24, V.11, RS-232, RS-449, RS-530, X.21

Examine™ is the most powerful decode engine in the networking industry. Able to decode through all 7 layers of the OSI reference model, Examine currently identifies over 900 different protocols and provides detailed decodes for more than 350 of those protocols. A built-in quick-filter allows the user to quickly focus the display to include only frames that meet user-defined criteria. As a common component of all WWG software and hardware analyzers, Examine meets the needs of the most demanding professionals in the industry.

Mentor™ is recognized as the leader in expert analysis systems for the networking industry. Mentor can operate offline with capture files from LinkView and Domino. Additionally, it will operate in real time on DominoLAN and DominoWAN analyzers. Mentor can be tailored to look for problems related to a specific network or application-related symptom. To find problems related to packet transport issues, multiple-segment analysis is also supported.

Wizard™ is a full-featured baselining tool designed to work with DominoLAN, DominoWAN and DominoFE. Wizard allows the user to customize and generate color reports through a series of charts and graphs that provide an in-depth analysis of the state of the network over the monitor period. By entering a schedule for the monitor period, long term monitoring is possible. (Example: Monday through Friday 7 a.m. until 6 p.m. is possible)

DominoServer™ is designed for distributing any Domino or stack of Domino analyzers. From a browser-based interface, a user can connect to multiple DominoServer remote-access devices and control stacks of Domino analyzers. Distributed Domino analyzers can be removed from the stack and taken to a site for use and then returned to distributed service. DominoServer provides Mentor and Wizard as well as full support for LAN/WAN and ATM matrix switching.