Network Analysis - FAQs

What is a Protocol Analyzer?

Protocol analyzers capture conversations between two or more systems or devices. A protocol analyzer not only captures the traffic, it also decodes (interprets) the traffic. Decoding allows you to view the conversation in English, as opposed to binary language. A sophisticated protocol analyzer will also provide statistics and trend information on the captured traffic. Protocol analyzers provide information about the traffic flow on your LAN, from which you can view device-specific information. Unlike SNMP-based management consoles, protocol analyzers are device independent.

How will a protocol analyzer be useful to me?

A protocol analyzer is the only tool that shows you exactly what is happening on your LAN. Once a problem is isolated and recorded, there can be no denying which vendor, or which system is the cause.
For example, if your TCP/IP sessions are "hanging," a protocol analyzer can show which system sent the last packet, and which system failed to respond. If you are experiencing slow screen updates, a protocol analyzer can display delta time stamps and show which system is waiting for packets, and which system is slow to respond. In an NT environment, a protocol analyzer can show runaway traffic (broadcast or multicast storms) and its origin, system errors and retries, and whether a station is sending, trying to send, or only seeming to communicate. You will get information that is otherwise unavailable, which results in more efficient troubleshooting and better LAN health.

Do I have to be a protocol expert to use a protocol analyzer?

Definitely not. While protocol analyzers can be used by network developers to view the exact contents of a network conversation, a modern protocol analyzer with a graphical user interface provides many other types of information beyond the bits and bytes of the actual protocols. Being able to see which device or system failed to respond is usually enough information to pinpoint the problem and focus your attention on that piece of the puzzle. As you may have experienced, network troubleshooting can be full of hours of wasted time chasing a theory that turns out to be misdirected. If a protocol analyzer helps you save just one wild goose chase, it is money well spent. Protocol analyzers also provide many statistical and real time trend statistics that help for management justification of new hardware.

What kind of information will a protocol analyzer provide to help troubleshoot or maintain the overall health of my LAN?

Protocol Analyzers should provide three main sources of information about your LAN traffic.

- Network Statistics about traffic flow, station health and network or station line errors. This information helps identify trends and general conditions that may signal an unexpected network problem condition, or a load issue that is causing slowdowns. Additionally if you are considering adding a switch, the statistical traffic breakdown can show how best to implement the new switch. If you currently have a switch installed, statistical analysis can show if your switch is configured correctly and your ports are supporting a balanced load of LAN traffic.
- Packet Capture and Decode displays LAN traffic (packets) decoded into specific function and sub-function for LAN or protocol problem isolation. Being able to view the specific packet-by-packet conversion can show exactly what is happening during a system-to-system communication, both when things are functioning correctly and when things are not.
- Trending Information displays historical usage data over days, weeks, months or even years. This information provides a historical perspective on any new problem, and can show trends that may indicate a potential problem before it happens.

Examples of Network Statistics troubleshooting applications

- Viewing frame errors can show if a LAN slowdown is because of excess CRC or alignment errors. Once the error rate is determined to be above normal, viewing errors by station will show which stations are sending the error packets, and let you focus your attention to the source of the problem.
- Protocol Statistics displays the percentage of your LAN bandwidth that a particular protocol is using. This helps determine efficient segmentation, and allows for problem isolation based on application or server type.
- Station Statistics shows the traffic generation by each station, server, bridge, router and the percent of the total bandwidth each station is using. With this information, you can determine who is using your bandwidth and what stations or devices are using more bandwidth than expected. For example, if one station is sending 40% of the total data sent this could indicate either a faulty network adapter (multiple retries) or simply a device that consumes more network bandwidth than expected. In either case, having a protocol analyzer allows you to take the appropriate action based on facts, not guesswork.
- Packet Capture and Decode allows you to capture traffic in real time and record and view the decoded information. Packet decodes show you conversations between workstation and host, between workstations or between hosts. This information helps in any problem situation by showing you exactly what is happening and when, and exactly which device is doing what.

Some example problem situations where a protocol analyzer's information is indispensable

- Host sessions are "hanging" - packet capture and decode will show which system sent the last packet and which system failed to respond. This helps pinpoint which device - host or workstation - is causing the problem.
- Problematic network printing - an analyzer answers the question: ``Did the station send the job or does it just look as though it was sent?
- Can't log in - Packet Capture can display login negotiations, retransmits and response times to determine where the problem is, and where to focus your attention.

Do protocol analyzers use SNMP?

Typically not. SNMP products provide device specific information, where protocol analyzers obtain all their information by examining the traffic on the LAN. For example, an SNMP collection utility could not provide session delta time stamps for a Unix telnet session, nor can SNMP provide bandwidth utilization statistics directly. Example SNMP statistics would include how many packets came in or went out of a router, a print server's IP address, or a predefined trap generated by a network printer for ``out of paper''. SNMP products are a good complement to any protocol analyzer.

Can an analyzer see all of the segments of my network (can a protocol analyzer work over a WAN)?

No. Protocol analyzers can only view and collect traffic from the segment where the analyzer is located. To capture and analyze traffic from another segment (local multi-segment LAN or remote WAN), a distributed or mutli-segment analyzer is required. Distributed analyzers offer similar functionality to a standard (non-distributed) analyzer, displaying multiple diagnostic windows, each representing a segment on your LAN - all from a single management station. Typically, distributed analyzers consist of a software based management station and ether software or hardware based probes allowing an administrator to ``view'' any segment that hosts a probe.

Is a protocol analyzer useful in a switched environment?

Yes. Using a protocol analyzer in a switched environment is common, and can provide both global port balancing information (using station statistics) and specific conversation troubleshooting information (using packet capture and decode). In most switched environments using an analyzer is as simple as placing the tool on a server to collect access and conversational data to and from that server. Placing the analyzer on a ``downstream'' hub can show if the hub's users are correctly placed to maximize the aggregate throughput of the switch. Most switches allow for port tapping to direct any port's traffic to the port where the protocol analyzer is installed.