White Paper

Why You Should Consider a Hardware Based Protocol Analyzer?

Software-only protocol analyzers are limited to accessing network traffic through the utilization of mirroring. While this is the most convenient and versatile way of accessing network traffic, this paper will explore its constraints and how those restrictions can significantly hinder the ability to accurately access all the relevant network traffic. Additionally, the use of typical Network Interface Cards (NICs) by software only protocol analyzers keeps them from having sufficient performance to analyze or capture network traffic beyond minimal utilization levels.

Fluke Networks' protocol analysis cards with its multiple interfaces provide the unique capability of being able to merge label and multiple streams of network traffic. ClearSight Analyzer built-in to every Network Time Machine is able to merge up to four trace files, align them in a multi-segment ladder-view, and maintain that alignment through the use of their protocol analysis cards that can time-stamp packets with an accuracy of 20 ns or less.

FLUKE networks

Table of contents

Overview

Software-only protocol analyzers are limited to accessing network traffic through the utilization of mirroring. While this is the most convenient and versatile way of accessing network traffic, this paper will explore its constraints and how those restrictions (losing all frames that exceed 50% of a full-duplex frame rate, mirrored frames being delayed when the CPU utilization is too high, switches rebooting when they run out of memory, filtering out MAC frames with errors) can significantly hinder the ability to accurately access all the relevant network traffic. Protocol analysis cards, being a hardware-based solution, can take advantage of port mirroring where it makes sense, but also access network traffic using full-duplex TAPs, which avoid all the limitations of port mirroring.

Additionally, the use of typical Network Interface Cards (NICs) by software only protocol analyzers keeps them from having sufficient performance to analyze or capture network traffic beyond minimal utilization levels. Furthermore, they lack the ability to employ precision time-stamping, which can result in their indicating problems that aren't really there.

Fluke Networks' protocol analysis cards provide the unique capability of being able to merge multiple streams of network traffic and view them in a multi-segment ladder-view in real-time. The ClearSight Analyzer build-in to each Network Time Machine is able to merge up to four trace files, align them in a multi-segment ladder-view, and maintain that alignment through the use of their protocol analysis cards that can time-stamp packets with an accuracy of 20 ns or less.

Why Consider a Hardware Based Protocol Analyzer?

Although software only protocol analyzers are a useful resource, downloadable and inexpensive, protocol analysis cards[1] specifically designed for the unique rigors of protocol analysis are worth their higher cost.

One of the reasons to consider protocol analysis cards is that software only protocol analyzers are limited to analyzing network traffic using port mirroring[2]. Such cards can take advantage of port mirroring's convenience and versatility when it makes sense, but they can also avoid its limitations by using full-duplex Test Access Points (TAPs.)

A full-duplex link is a point-to-point connection between two devices, such as a host and a switch, two switches, and a router and a switch.[3] In this case, the transmit pair (channel) and receive pair (channel) can operate simultaneously at the rate of the medium (see Figure 1)

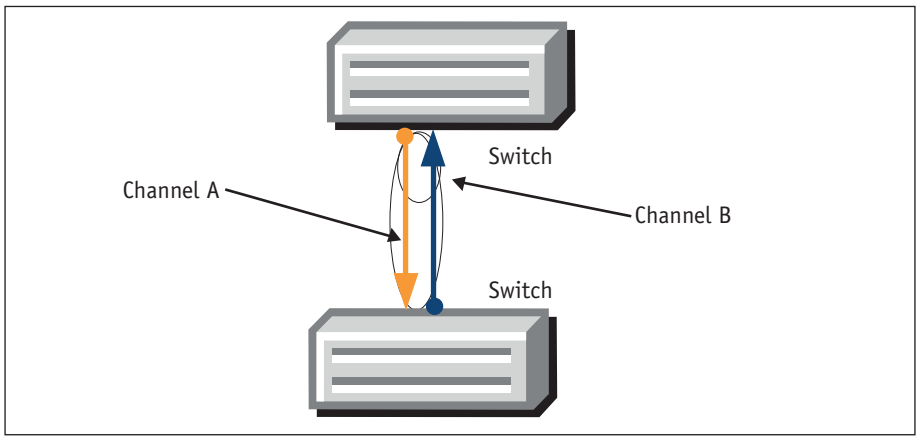

Figure 1

[1] The phrase "protocol analysis card" is used in the generic sense to describe the physical card itself and its driver. To help simplify this paper, it will not distinguish between those features that are provided by the protocol analysis card's driver, verses the features provided by the protocol analysis card itself since a driver is designed to work with only one specific make and model card.

[2] Technically, hubs can also be used by software only analyzers. However, the ubiquitous presence of switches, the performance disadvantages of hubs, and that many "hubs" sold today are actually switches renders the availability of this option mute.

[3] A half-duplex link is a connection to a shared medium, such as a host or router to a hub. In this case, the transmit pair and the receive pair operate by taking turns accessing the medium.

Since both channels operate at the rate of the media, a full-duplex link can handle twice the rate of the media. In other words, a full-duplex Fast Ethernet link can support up to 200 Mb/s, and a full-duplex Gigabit Ethernet link can support up to 2,000 Mb/s. In contrast, half-duplex links don't use channels and are therefore limited to rate of the media, i.e., 100 MB/s or 1,000 MB/s. Mirroring (a.k.a. SPAN for Switched Port Analyzer) can use one of two methods to copy traffic from a link on the switch to a network monitoring device, such as a protocol analyzer. The first method uses only one channel of a full-duplex link between the switch and the analyzer. (see Figure 2) The second method uses a half-duplex link where the receive pair on the switch is turned off.[4] The reason why the monitor port's receive channel or receive pair are turned off is to prevent the possibility of routing or bridging loops, and to prevent the possibility of confusing servers or workstations by the analyzer re-transmitting traffic.

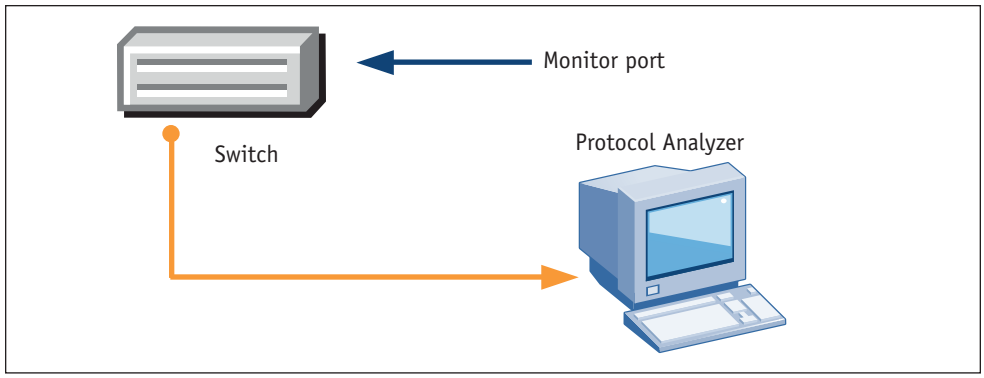

Figure 2

Consider a full-duplex link where both channels have a bandwidth utilization of 75%. For Fast Ethernet that would be an aggregate of 150 Mb/s; for Gigabit Ethernet 1,500 Mb/s. If that link were mirrored to a protocol analyzer, 1/3 of the traffic would be dropped at the switch, never reaching the protocol analyzer. For Fast Ethernet that would be a loss of 50 Mb/s. For Gigabit Ethernet that would be a loss of 500 Mb/s.

Two pieces of equipment are required to avoid dropping frames when a full-duplex link exceeds 50% utilization: a full-duplex TAP and a full-duplex protocol analyzer. When a full-duplex protocol analyzer connects to a full-duplex TAP, traffic is copied from each channel and is transmitted to the protocol analyzer over a corresponding cable. (See Figure 3)

A full-duplex analysis link is different from a typical full-duplex network link in two ways: the analyzer is receiving traffic over both channels, and each channel uses its own cable. A typical network interface card (NIC) has only a single port that is used to establish a typical full-duplex network link, and it is not designed to receive traffic over both channels. These features only come with a protocol analysis card specifically designed for full-duplex analysis.

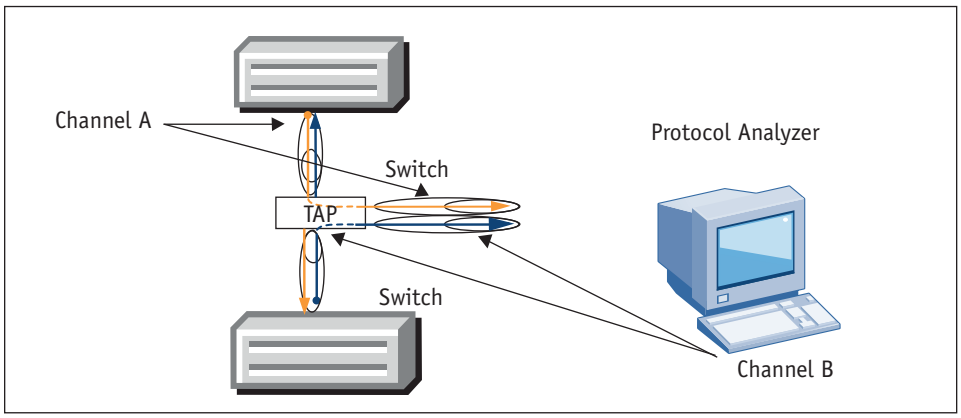

Figure 3

[4] Half-duplex links use "contention". Full-duplex links do not. Contention listens for traffic before transmitting and allows for collisions, both of which can reduce the performance of the link. As a result, monitor ports that use only one channel of a full-duplex link tend to have better performance than monitor ports that use a half-duplex link.

Switch Resources

A second reason to consider protocol analysis cards is that port mirroring uses extra CPU cycles and memory on a switch. The main purpose of a switch is to forward packets between network links. If the switch's CPU utilization gets too high, it will only forward packets to the monitor port when it has extra CPU cycles, since port mirroring is a lower priority task. When this happens it can create false-positives when monitoring time-sensitive protocols, such as falsely indicating jitter (sometimes referred to as phantom-jitter) in an RTP stream[5]. Additionally, if the switch's memory utilization gets too high, the switch will reboot. Using a TAP avoids the need to monitor these resources when troubleshooting a problem[6].

MAC Errors

A third reason to consider protocol analysis cards is that software only protocol analyzers are significantly limited in their ability to analyze and capture frames with MAC errors.

Most of today's switches[7] discard frames that have MAC errors because the information in the frame is no longer reliable and to prevent them from disrupting network services. Nonetheless, frames with MAC errors can still cause problems with the behavior of the link on which they are occurring or with the behavior of applications running over it. Additionally, old switches still in use may not filter them out. So, it is still important to be able to analyze and capture these frames.

It is rare when a software only analyzer can be of useful here. If the monitoring port on the switch is filtering them out, these frames will never get to the analyzer. If the switch is old and does forward these frames, the software only analyzer will need to come with special drivers that enable it to analyze and capture these frames. As a result, when it becomes necessary to look for frames with MAC errors, it is necessary to employ cards that are specifically designed to analyze and capture these kinds of frames through full-duplex analysis.

As a result of the above reasons, while port mirroring is convenient, it should only be used when traffic will not spike above 50% of a full-duplex link, when the switch has ample CPU cycles and memory available, and when MAC errors have otherwise been ruled out. Unlike software only analyzers, protocol analysis cards are not constrained by these limitations as they can also use a full-duplex TAP.

Performance

A forth reason to consider protocol analysis cards is that software only protocol analyzers cannot analyze and capture all the frames of a highly utilized link, where a card specifically designed for this task can.

It is common for a typical NIC to perform well for client-server forms of communications (e.g., web surfing, file exchanges, email, database queries, etc.), but perform poorly under the unique demands of protocol analysis.

When performing protocol analysis, typical 10/100 NICs start dropping frames when network utilization reaches between 20% and 30%. For Gigabit Ethernet that performance barrier is 7% to 9%.

Utilization can easily reach over 70% even though normal utilization is low. Additionally, it is easy these spikes to occur and go undetected. This is because network trending tools average numbers to the intervals that they're plotting, effectively leveling off any spikes.

[5] RTP (Real-Time Protocol) is used in VoIP communications.

[6] Either an aggregation TAP or a full-duplex TAP can be used here, though concerns about network bandwidth utilization will still be relevant when using an aggregation TAP.

[7] There are two kinds of switches: "cut-through" and "store and forward". Cut-through switches only read the destination address of a frame before forwarding it. As a result, the switch can quickly forward frames, but it can also forward problem frames that can bring a network to a stand-still. Store and forward switches read the whole frame. As a result, they will identify any frame that has a problem with it and drop it, preventing it from propagating through the network. Originally, cut-through switches were popular for performance reasons. However, as switch technology matured with the increased use of ASICs (Application-Specific Integrated Circuit), store and forward switches can now perform as well as cut-through switches. As a result, almost all switches sold today are store and forward switches.

For example, if your utilization charts are making a plot mark every hour, the performance is averaged over an hour; if the plots are every second, then it is averaged over a second. A second may not seem like a long time to average utilization, but frames at gigabit speeds take between .608 and 12.24 microseconds (millionth of a second) to transmit[8]. Hence, between 81K and 1.6M frames can be transmitted in a second, more than enough time to spike over 70% utilization and settle down for an average of 5% over the duration of the second. As a result, the trending tool would never identify that spike. And if this is true over the span of a second, then it is all the more true over the course of an hour.

Also, an error condition known as jabbering[9] may use up all network resources effectively bringing a server to a stand-still or choking a network aggregation link.[10] Being able to analyze which interface is jabbering in such circumstances is essential to resolving this condition quickly.

To ensure that all frames are analyzed and captured during spikes or sustained periods of high utilization, a card that is specially designed to support high utilization must be used.[11]

Time-Stamping

A fifth reason to consider protocol analysis cards is their ability to accurately time-stamp frames in hardware as they are analyzed and/or captured.

There are two ways to time-stamp frames, in hardware and in software. Hardware time-stamping is used by cards specifically designed for network testing and is done on the card as the frame enters it. If the card is properly designed for network testing, then it should have double-digit nanosecond accuracy.

Software time-stamping is used by a software only protocol analyzer. Before the frame can be time-stamped by the application it has to traverse the card and the card's driver. Time-stamping frames in software can typically have a timestamp accuracy of one microsecond, but it can have fluctuations of "tens of microseconds" between frames if the system has other processes that are demanding resources. Since an entire frame takes between .608 and 12.24 nanoseconds to transmit, a variation of "tens of microseconds" (e.g., 20 microseconds) can equal the time it takes to transmit over 30 frames.

Just as insufficient CPU resources in a switch can create false-positives, the variation that is found in software time-stamping can also create false-positives when troubleshooting network problems such as phantom-jitter in an RTP stream, stealing time from isolating real problems.

Fluke Networks protocol analysis cards have a time-stamp resolution of 20 nanoseconds or less.[12]

Besides the above reasons to consider protocol analysis cards that apply to all protocol analyzers, there are additional reasons to consider the Network Time Machine that has the Fluke Networks protocol analysis cards and the ClearSight Analyzer's function included.

[8] For 64-byte and 1518-byte frames, respectively.

[9] Informally, an error in which a faulty device continuously transmits corrupted or meaningless data onto a network; Formally, a condition wherein a station transmits for a period of time longer than the maximum permissible packet length.

[10] e.g., a NIC can "get stuck" repeatedly transmitting a single packet with a small interpacket gap to a specific host across the network.

[11] It should also be noted that certain factors of a PC platform can inhibit the ability of a high performance protocol analysis card. These factors can include, but are not limited to BIOS, chip set, bus speeds, system CPU, and system RAM.

[12] This does not pertain to protocol analysis cards that are only 10/100 or are PCMCIA/PC-Cards.

Real-Time Multi-Segment Analysis

A sixth reason to consider Fluke Networks' protocol analysis cards is their ability to perform Real-Time Multi–Segment Analysis.

With the Fluke Networks' protocol analysis cards, the Network Time Machine with its build-in ClearSight Analyzer has the ability to correlate data between multiple network segments in real-time. Real-Time Multi-Segment Analysis lets you view connections end-to-end, to see how transactions are propagating through the network. This makes it easier to see where there may be bottlenecks or other problems.

To illustrate this point, consider a common use of protocol analysis, the elimination of finger pointing: is the problem caused by the client, by the server, or by the infrastructure (routing/switching)? For example, if a client sends a proper request to the server and the server never responds or takes excessively long to respond, the problem is with the server. Likewise, if the server sends a proper message to the client and expects a response in return, and the client never responds or takes excessively long to respond, the problem is with the client. If the network is dropping the frames or introducing the significant delays, then the problem is with the network. ClearSight Analyzer's Ladder-View can provide the visibility needed to see quickly and easily what's going on.

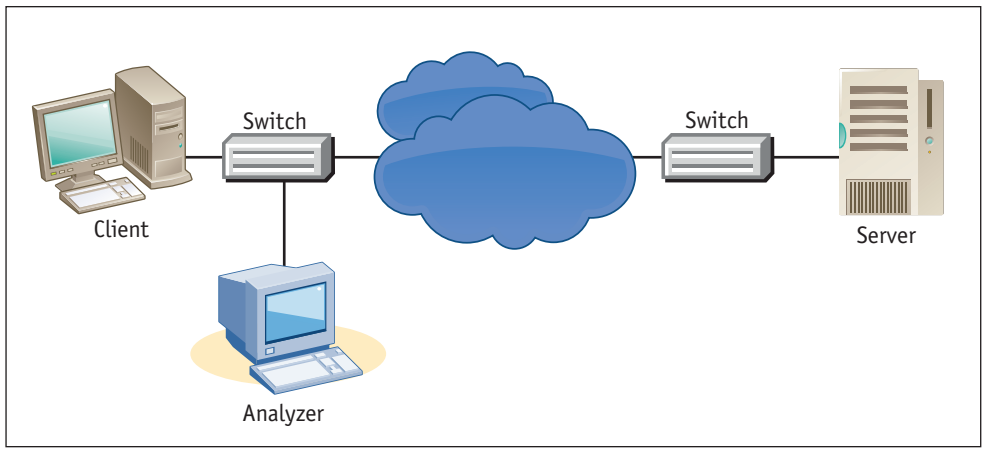

Figure 4

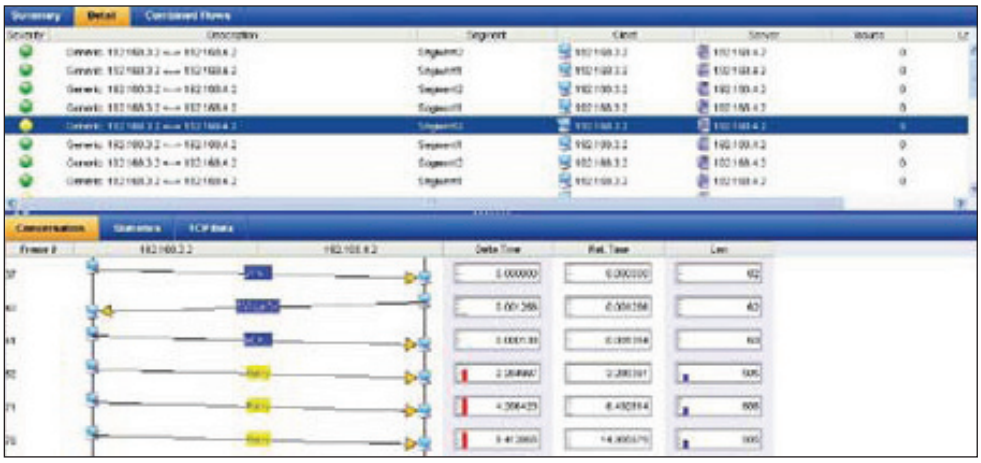

Figure 5

Consider the following scenario. A user is complaining of a hanging application. An analyzer is connected to the switch that the client is directly connected to. Upon analysis it is obvious that the client is not getting the response to a request it has made. (See Figures 4 and 5)

However, it is not obvious what is causing the problem. Is the server not responding or is the network dropping the frames? In order to answer this question, another analysis session needs to be performed at the other end. (See Figures 6 and 7)

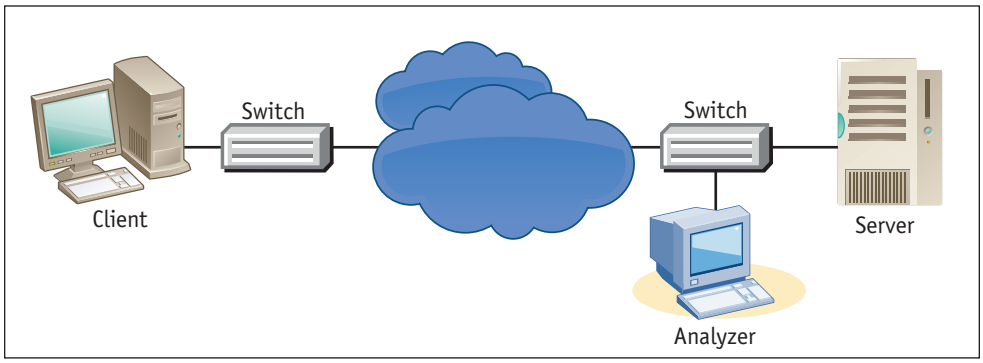

Figure 6

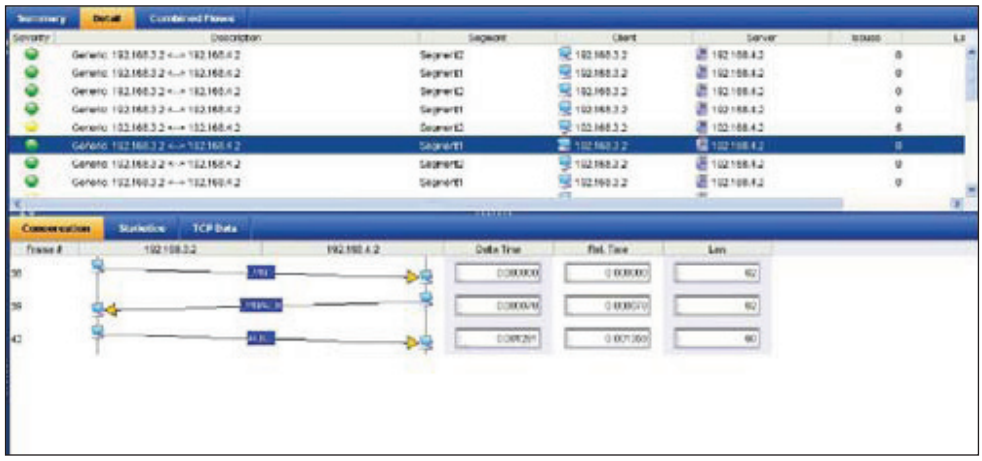

Figure 7

Since there are no retry frames from frames 52, 71, 76, 97, and 130, it is obvious that the network is the cause of the problem. However if Real-Time Multi-Segment Analysis is employed, then in only one analysis session the problem is made obvious and is more intuitive. (See Figures 8 and 9)

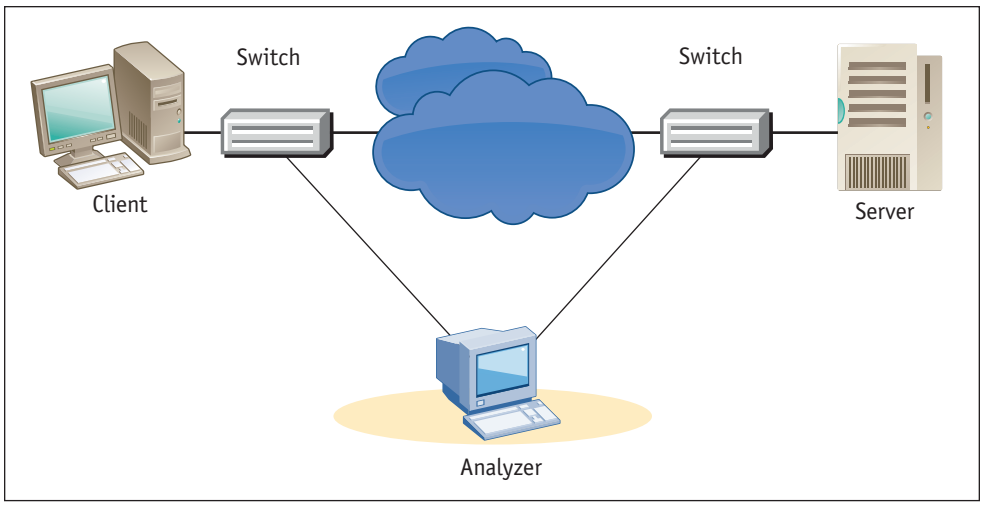

Figure 8

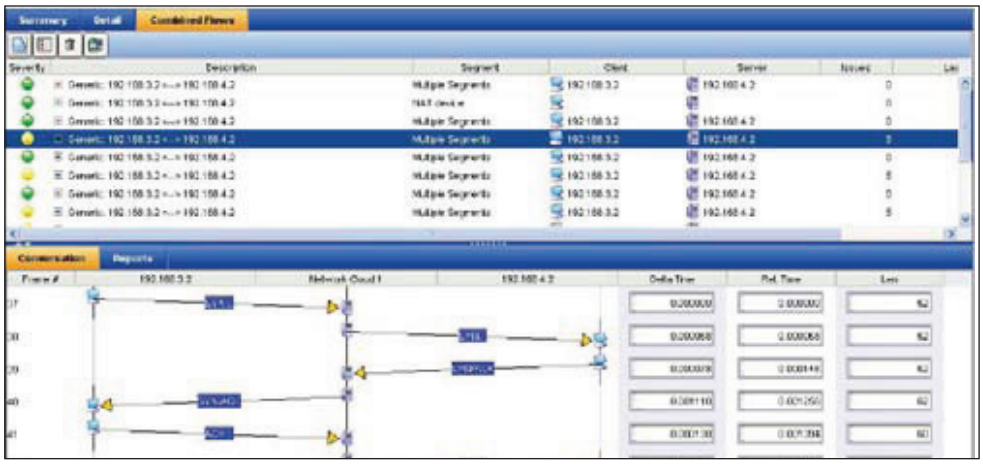

Figure 9

Additionally, as is the case with ClearSight Analyzer's regular ladder-view, each rung of a Multi-Segment ladder-view has a corresponding Delta and Relative Time measurement. If the problem was with delayed responses or with network delay, such issues would be made clear by the Delta Time[13] column, where vertical colored bars highlight excessive delays. A pattern of delay being introduced by a particular network element would indicate a need for performance tuning that element.

Post-Capture Multi-Segment Analysis

A seventh reason to consider Fluke Networks' protocol analysis cards is the ability to maintain the alignment of merged trace files when performing Post-Capture Multi-Segment Analysis. When Real-Time Multi-Segment Analysis is not practical, ClearSight Analyzer has the ability to correlate data between up to four segments when merging trace files. (See Figure 10)

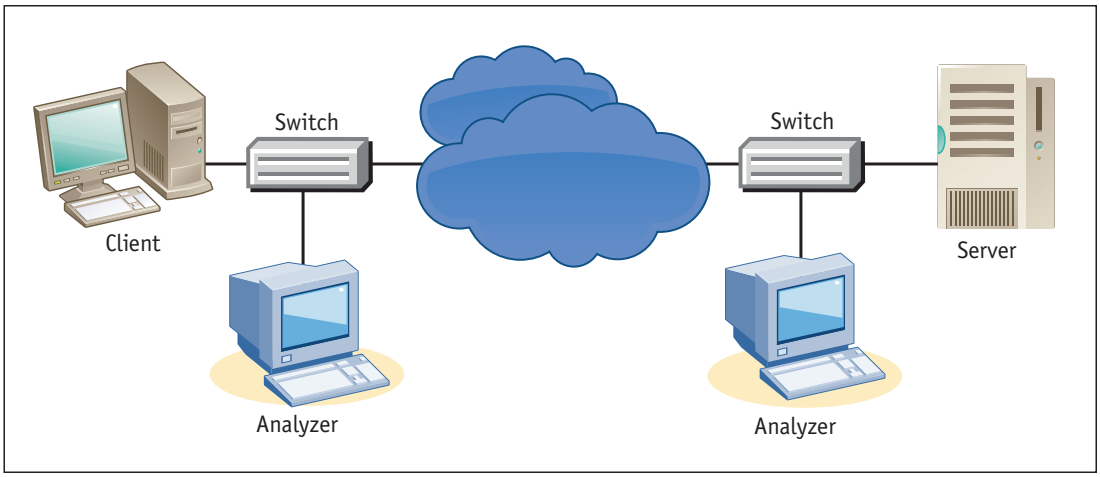

Figure 10

[13] Delta Time is the time between the indicated frame and the frame that preceded it

Merging trace files is simple and intuitive. To bring up the Merge dialog, select the menu options File, Merge. Select the files you want to merge and click **(Auto Sync)**. ClearSight Analyzer will automatically align the trace files without the need to synchronize the actual analyzers.[14] Save and then open the merged files and see the same Multi-Segment interface from Real-Time Multi-Segment Analysis.

Additionally, in Post-Capture Multi-Segment Analysis there is the ability to align traces taken from the public and private side of a Network Address Translator (NAT). Analyzing problems spanning both sides of a NAT are particularly difficult in that not only do they have different addressing, but they maintain independent sessions. (See Figure 11)

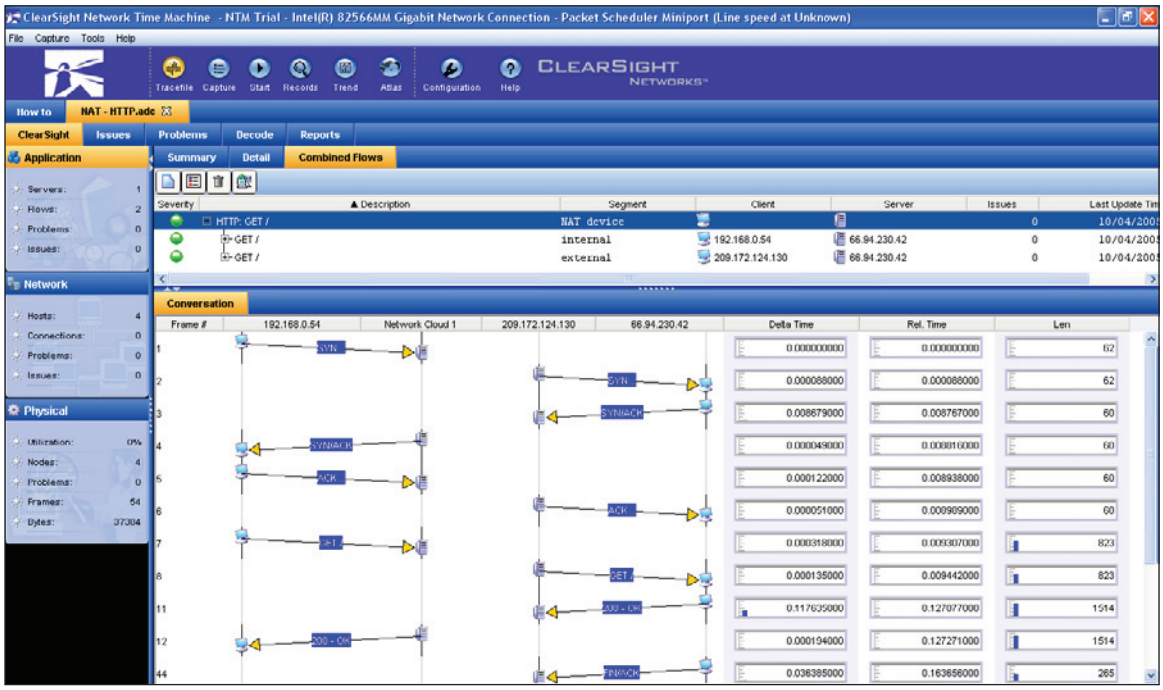

Figure 11

The need for protocol analysis cards when using Post-Capture Multi-Segment Analysis is that accurate time-stamps on the frames are needed to maintain the alignment of the trace files. As discussed previously in the Time-Stamping section, typical NICs do not support hardware time-stamping, and the variations that are part of software time-stamping can have a significant impact during the course of capturing a trace files. This variation can cause the alignment to be lost. The same kind of accuracy that is needed to prevent phantom-jitter in an RTP stream is also needed to maintain the alignment of merged files, being: double-digit nanosecond resolution. Only a card specifically designed and manufactured for network testing will be capable of this kind of time-stamp resolution.

As previously mentioned, Fluke Networks' protocol analysis cards have a time-stamp resolution of 20 nanoseconds or less.[15]

ClearSight Analyzer will merge trace-files captured from other protocol analyzers provided that they export their trace files to industry standard trace-files formats. If those protocol analyzers use protocol analysis cards that have a time-stamp accuracy of double-digit nanosecond resolution, then ClearSight Analyzer will be able to maintain alignment of the merged trace-files just as if it were using its own cards.

[14] Network Timing Protocol (NTP) synchronizes network elements to 100 milliseconds (0.100), and as such it is not suitable for synchronizing analyzers. There are only two mechanisms that have sufficient time resolution to properly synchronize analyzers, a connection to a stratum clock or a connection to a GPS.

[15] This does not pertain to protocol analysis cards that are only 10/100 or are PCMCIA/PC-Cards.

Summary

Protocol analysis cards avoid the limitations that are inherent with software only analyzers. They can perform full-duplex analysis, avoiding the limitations of port mirroring (losing all frames that exceed 50% of a full-duplex frame rate, mirrored frames being delayed when the CPU utilization is too high, switches rebooting when they run out of memory, filtering out MAC frames with errors), though they can take advantage of it when it is appropriate to do so. Protocol analysis cards have the performance needed to analyze and capture all frames even under heavy loads, and they use hardware based time-stamping which ensures that any jitter detected is real.

Fluke Networks' protocol analysis cards together with the ClearSight Analyzer provide the unique capability of being able to merge multiple streams of network traffic and view them in a multi-segment ladder-view in real-time. Finally, protocol analysis cards (Fluke Networks' or third party that can time-stamp to double-digit nanosecond accuracy) enable ClearSight Analyzer to maintain the alignment of a merged files comprising up to four trace files.

These are seven reasons why protocol analysis cards are worth the extra money, and why you should consider them.

Contact Fluke Networks: Phone **800-283-5853** (US/Canada) or **425-446-4519** (other locations). **Email: info@flukenetworks.com**.

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 06/2010 3790708A D-ENG-N