FLUKE networks

Application Note

Troubleshooting with the power of Multi-Segment Analysis

Introduction

Your network is the foundation for all of your business connections. Whether salespeople are looking up customer information in the CRM, or employees are exchanging email, or Accounting is paying invoices via SAP, the network and its applications are crucial for business to get done. To guarantee the responsiveness demanded by today's computer savvy user, IT Professionals must be able to visualize the data as it travels through locations, and be able to isolate and solve problems quickly.

Today's networks connect multiple business locations. In the past, if you suspect that there was a response time issue, you may capture traffic at the client and server side at the same time using two protocol analyzers. You were then faced with the challenge of looking at both trace files to locate the bottleneck. With Fluke Networks, those files can then be merged to take advantage of ClearSight Analyzer's unique multi-segment ladder diagram function.

Multi-segment analysis lets you view connections end-to-end to see how transactions propagate, as they travel through your network. It has the ability to correlate data that has been collected on up to four segments. This makes finding bottlenecks or other problems faster and more efficient.

ClearSight Analyzer provides detailed real-time analysis for many important network applications, including Oracle and MS SQL databases, POP, SMTP, and Exchange email, VoIP applications such as H.323, SIP and Cisco's Skinny, and many more. For each supported application type, ClearSight Analyzer detects servers and flows, providing real-time analysis and statistics that enable you to troubleshoot network problems as they occur. You can view information for a specific flow, for a specific server, or for an application type as a whole. For each detected flow, ClearSight Analyzer rebuilds and displays the interactions and transactions between a client and server, using a network ladder diagram and including the associated delta and relative timing. For some application flows such as databases, e-mail, and file transfers, ClearSight Analyzer even rebuilds the content flow as the end user sees it. This helps detect unauthorized application access, abnormal data patterns, and application level errors.

There are several examples of where this could be extremely beneficial, including:

- Application server access is either slow or intermittent
- Database is running slowly
- Network is busy
- User can't send email

This paper will examine the best way to experience the power of the ClearSight Analyzer's visualization of a single conversation throughout a multi-segment network.

Troubleshooting in a Multi-Segment environment

Because there are so many components involved in troubleshooting a multi-segment network, it is difficult to find out where the problem lies. The problem could be in the client, server, network, or application. The ability to merge multiple trace data files for up to four network segments, and watch the flow of the data between them, makes problem identification easier and more efficient, thus lowering Mean Time To Resolution (MTTR).

Steps to Analyze an issue in a Multi-segment network

1. Placement of the analyzer
2. Monitor and capture traffic
3. Extracting packets to trace file
4. Create merged trace files
5. View and analyze the combined flow

Troubleshooting with the power of Multi-Segment Analysis

1. Placement of the analyzer

The key to multi-segment analysis is to capture the data as it travels throughout the network. An analyzer must be placed at each collection point. The data is captured onto each analyzer, then consolidated to one analyzer and merged into a single trace file.

For this paper, accessing a terminal server has been intermittently slow for a client. The stations are on separate floors at the corporate headquarters, and indifferent VLANs. To troubleshoot the issue, a Network Time Machine that has ClearSight Analyzer build-in was placed on the client's segment, while another was positioned on the server's segment, while another was positioned on the server's segment. The system clocks of both analyzers are synchronized to an Internet Time Server through the use of Network Time Protocol (NTP) to make it easier to align the traces.

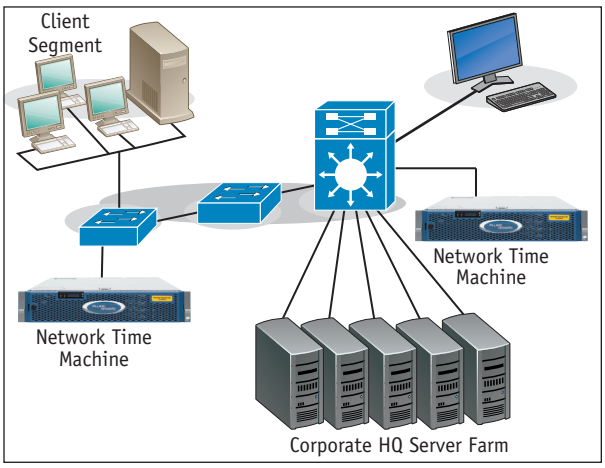

Figure 1: Example Network with Analyzer Placement

2. Monitor and capture traffic

The Network Time Machine began monitoring the network as soon as the application was opened, updating its displays with statistics and information related to the network layer connections and application flows on the network. An application flow is a set of packets that performs a specific function, such as a Get or a Post command to a web server, sending or receiving an email message, resolving a domain name, or making a phone call. Depending on the nature of the transaction, flows may consist of as little as two or as many as thousands of packets.

During monitoring, Network Time Machine does not save data to the capture buffer. Instead, it gathers statistics and alerts you to problems and issues on the network. We can see that Telnet is flowing across the segment in the initial screen **(see Figure 2)**. A capture may be started after capture filters are created to focus on the issues found while monitoring or packet can be continuously stream-to-disk at Gigabit per second rate to record(s) when intermittent event with unknown characteristic is being investigated..

Figure 2: Network Time Machine's Initial Screen

3. Extracting packets to trace file

Once data has been captured on each segment, we want to extract only those traffic/packets that represent the problem that we want to address. User can specify by time period and user defined filter condition to extract the packet of interest from the stored record. NTM has an Atlas function that provides flow base statistic information so that users can identify the IP flow of interest with rich performance statistics and decide what packets to export to trace file. They can then give the trace file a unique file name, so it can be easily recognized when multi-segment analysis is needed, or directly send to the on-board ClearSight Analyzer for analysis.

4. Create merged trace files

Once the trace files have been transferred to a single machine, they can be merged into a single trace file. Network Time Machine will process the merged trace file in such a way that transactions involving more than one segment can be displayed. Network Time Machine tracks flows for applications according to the source IP address and port number. If the same IP address/port pair appears on more than one segment within a suitably short time interval, Network Time Machine will automatically create a combined flow.

To merge two or more trace files, choose the files that you would like to merge **(see Figure 3)** and add them to a new file. Files from up to four segments may be added. For example, an analyzer could be placed on the client's segment, after the firewall between the client and router, after the firewall between the last router and server, and on the server's segment.

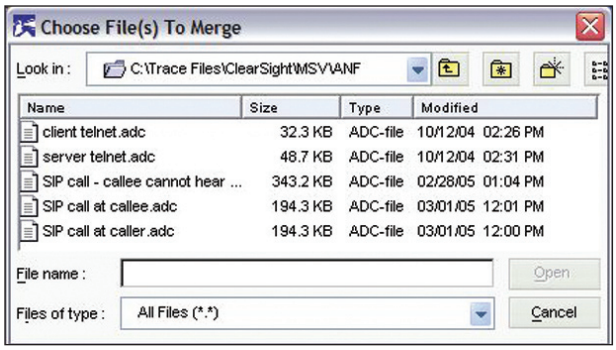

Figure 3: File>Merge>Add Dialog Box

If the Capturing Appliance (such as the NTM) were not synchronized to an external time server, an adjustment factor may be added. To obtain the value for the adjustment, note the time stamp for the first packet in the conversation flow in each trace file and use the difference between them minus the network latency. Taking the average response to a series of ICMP Ping requests will provide the value for the network latency.

Continue the process until you have gathered all the files that you want included. Merge the files, and save the new trace file under a new name. The new merged trace file can now be opened in the Network Time Machine.

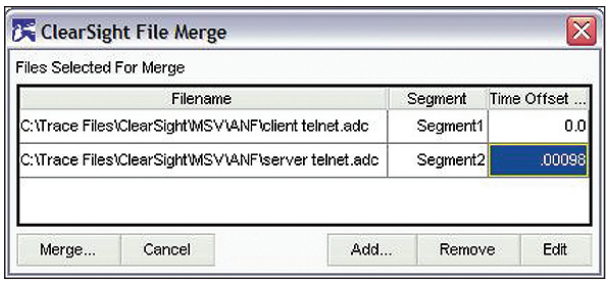

Figure 4: Time Offset

5. View and analyze the combined flow

To view combined flows, open the trace file that contains multi-segment data. The Combined Flows pane will list all of the flows that have been recognized as combined flows, for all active applications in the trace file. If you select an individual flow, the multi-segment ladder view will appear in the Conversation tab of the Statistics pane **(see Figure 5)**.

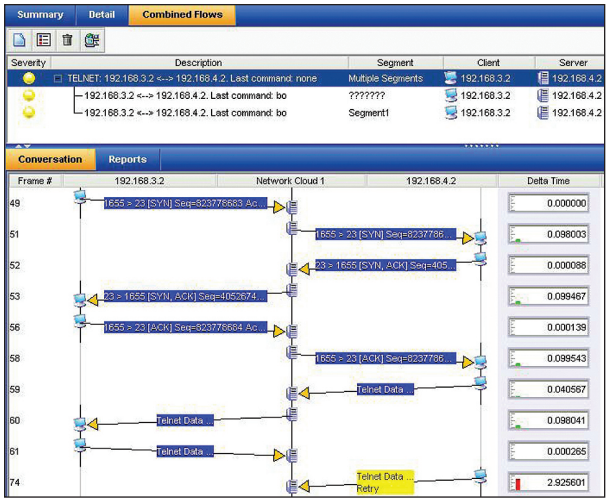

Figure 5: Combined Flow

We can see that packet 61 was sent by the client, but never received by the server. Since the missing packet also contained the acknowledgement for packet 60, the server retransmits in packet 74 after it times out. Notice the large Delta time for the retransmission, it is almost 3 seconds. That is certainly enough latency to cause the user to complain. This pattern continues throughout the flow, with packets being dropped on both sides. By being able to see that the packets are being sent, but never received, we can isolate this as a network issue. Statistics on the intermediary switches should be queried to see which one is dropping the packets.

Adjusting the timeout factor for Telnet would also have an enormous impact on this transaction. Each time a packet was dropped, the client or server waited seconds to retransmit. To see the effect this has on total transaction time, performance related statistics can be viewed in the Reports Tab. This report clearly shows that the majority of the transaction time was at the client **(see Figure 6)**. Network latency was only 2.54%, but the two retransmissions for the client and one for the server added more than 2 seconds each to the process. Having the additional documentation in such a clear and visual format makes isolating the bottleneck and communicating the information to the stakeholders faster and more efficient.

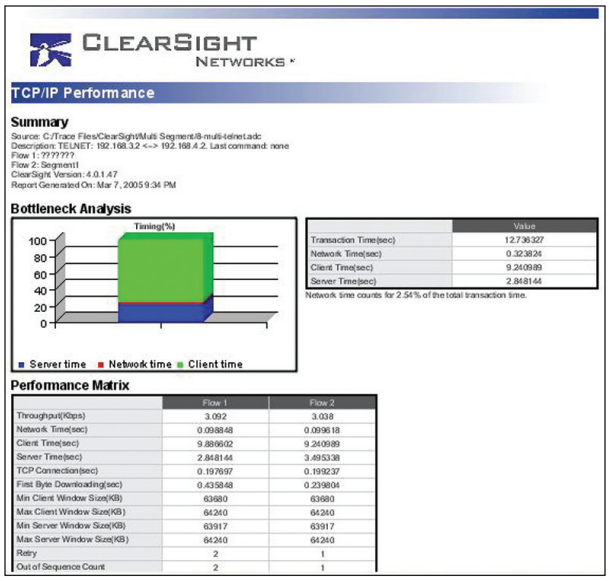

Figure 6: TCP/IP Performance Report

Summary and conclusion

Networks are becoming more complicated every day, and the demands placed upon them are only exceeded by the expectations of the users. Every network environment consists of a wide variety of components. When one of these components fails, malfunctions, or is inefficient, it impacts a variety of network functions. The key is to be able to locate the specific issue, whether it is the client, server, network, or application. This is always a challenge, but becomes even more of a challenge when trying to locate the offender in a multi-segment environment.

The key to troubleshooting in this environment is to have an analyzer that can let you consolidate traffic in more than one place at a time…Network Time Machine is the answer!

Terminology

CRM	Customer Relationship Management
HTTP	Hypertext Transfer Protocol
POP	Post Office Protocol
RTP	Real Time Protocol, used to transmit voice or video in a VoIP call.
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
VLAN	Virtual Local Area Network

About Fluke Networks

Fluke Networks provides innovative solutions for the installation and certification, testing, monitoring and analysis of copper, fiber and wireless networks used by enterprises and telecommunications carriers. The company's comprehensive line of solutions provide network installers, owners, and maintainers with superior vision, combining speed, accuracy and ease of use to optimize network performance. Headquartered in Everett, Washington, the company distributes its products in more than 50 countries. More information can be found by visiting Fluke Networks' Web site at: **www.flukenetworks.com** or by calling (800) 283-5853.

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. 05/2010 3790749A D-ENG-N