Troubleshooting with the Power of Multi-Tier 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 applications are increasingly complex. Unlike the older two-tier client-server model, most first tier clients need only a Web browser to access their applications. The second-tier Web server makes the translations necessary to forward the requests to a back-end application server, most commonly a database. The database server responds to the Web server, which again makes the translations necessary to forward the response to the client. To complicate matters, an additional tier may be inserted before the database to perform load balancing. While this multi-tier model has many benefits, it makes troubleshooting slow performance even more challenging.

The ClearSight Analyzer equips IT Professionals with the ability to see the multiple conversations correlated together, making isolating bottlenecks straightforward. No longer is time wasted pointing fingers and guessing whose fault it may be; by visualizing each tier as a combined flow, you can now see where latency and inefficiencies exist.

ClearSight Analyzer provides detailed real-time or post-capture 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.

This paper will detail the best way to experience the power of the ClearSight Analyzer's visualization of a single transaction throughout a multi-tier network.

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-Tier Environment

Because there are so many components involved in troubleshooting a multi-tier network, it is difficult to find out where the problem lies. The problem could be in the client, network, front end or back end server, or application. The ability to correlate data from up to four tiers, 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-Tier Network

1. Placement of the Analyzer
2. Monitor the Applications
3. Combine the Flows
4. View the Combined Flow

Troubleshooting with the Power of Multi-Tier Analysis

1. Placement of the Analyzer

The key to multi-tier analysis is to understand how the data flows for a transaction. This paper will examine an example sales query. Using a browser, a user on the client segment can see the sales for previous day. The user then fills in a form to request the information per store. These requests are sent to the Web server which then translates those requests into a query to the Microsoft SQL server. The MS SQL server responds to the Web server, which then sends the data back to the client in HTTP, so the client's screen populates with the information.

If an analyzer is placed at each tier, the requests and responses will be duplicated in the trace file. When capturing in a multi-tier environment, capture at every other tie. In this example, the traffic sent to and from the Web server's port was copied to the analyzer's port.

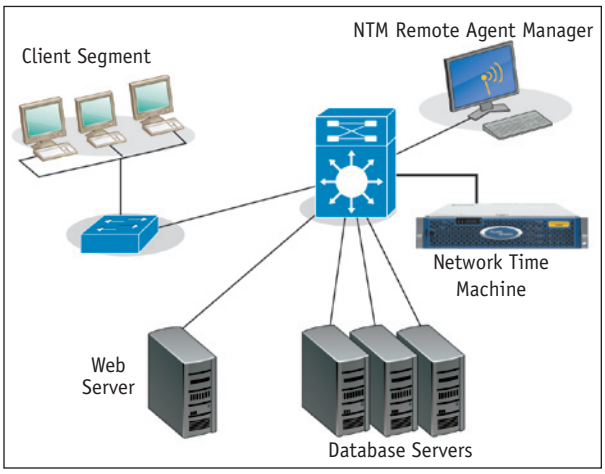

Figure 1: Example Network with Analyzer Placement

2. Monitor the Applications

The Network Time Machine that has ClearSight Analyzer build-in begins monitoring the network as soon as the application is opened, updating its displays with statistics and information related to the network layer connections and application flows on the segment. An application flow is a set of packets that performs a specific function, such as a Get or a Post on 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 few 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 HTTP and MS SQL are flowing across the segment in the initial screen **(see Figure 2)**. In case we need to refer back to the packet data, a capture was started. Often the issue in database transactions is how the query is formulated. Having the capture as a reference can make it easier for the Database Developer to isolate inefficient code.

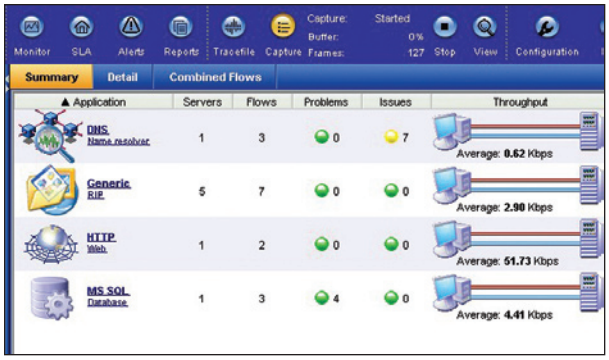

Figure 2: Network Time Machine's Initial Screen

Easy to Use Interface

To view the flows, simply click on either HTTP or MS SQL to move to the Detail pane **(see Figure 3)**. The information is available in real-time both in Monitor and Capture modes. The Detail ladder diagram shows the delta time between the client's requests and the Web server's response. The delta times are very high. Seeing the back-end database process will help determine if the bottleneck is truly the Web server's fault.

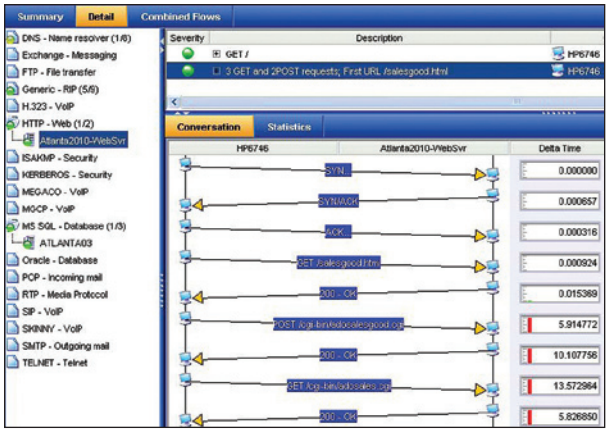

Figure 3: Ladder Diagram for HTTP

3. Combine the Flows

Once data has been captured on each segment, it must because there are no matching port numbers for Network Time Machine to base the combined flow upon, we will have to add the flows together manually. For VoIP conversations,

Network Time Machine uses the port numbers negotiated between the caller and gateway to allocate the RTP flow to the call setup flow automatically.

We created a new combined flow called Sales Query, and can now add each tier's conversation to the new flow. First the HTTP conversation was added, then the MS SQL query each with a right-click **(see Figure 4)**. Notice the substantial delta times for the database server's responses.

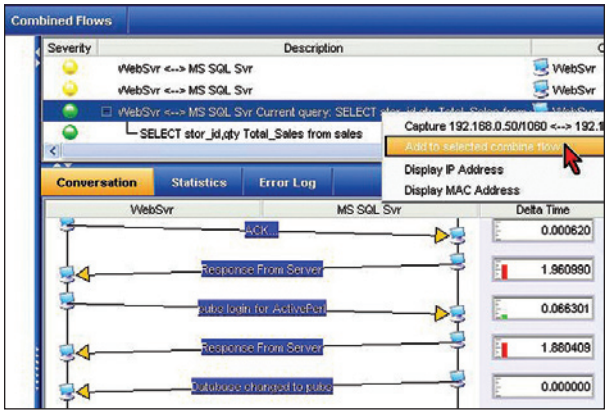

Figure 4: MS SQL Flow

4.View the Combined Flow

Once the flows are combined, the entire transaction can be viewed in one ladder diagram and analyzed. In this example, there is an assortment of issues. Notice the large delta times between the client's POST request and the Web server's synchronization (SYN) to the database server. It took almost 6 seconds for the Web server to translate the HTTP POST to an SQL query, and then initiate the conversation with the database server. The database is not without latency either; observe the delta times between the requests and responses. We will have to forward the queries to the Database Developer to see if they can be optimized. We can eliminate the network as a bottleneck. However, notice the trivial delta times for some of the frames. Using this picture saves countless hours of finger pointing, and facilitates determination and resolution of the problem.

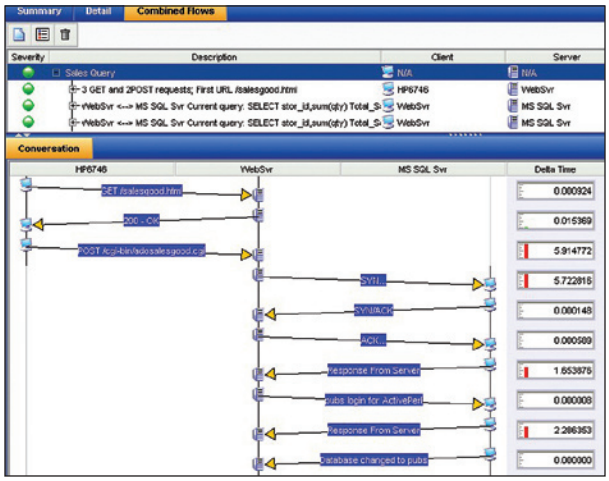

Figure 5: Combined Sales Query Flow

In all of the examples so far, all of the investigation has been in real-time. The power of multitier analysis is available in post capture as well. After all of the traffic has been captured, and once the data is displayed, Network Time Machine can be configured to automatically combine the flows based on IP address. Up to four tiers with five stations can be united **(see Figure 6)**. If data has been captured for a station that is not part of the transaction, the flow can be further refined based on well-known application or dynamic port number. Once the settings are applied and saved, Network Time Machine will display the combined flow automatically.

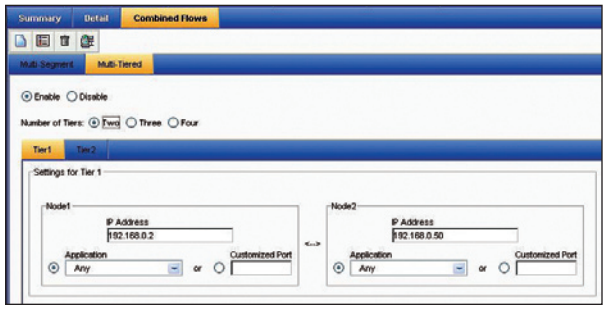

Figure 6: Auto-Combine Flows

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-tier 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
VoIP	Voice over Internet Protocol

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 Network SuperVision™ 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. 06/2010 3790751A D-ENG-N