Application Note

Troubleshooting VoIP Problems with the Power of Multi-Tier and Multi-Segment Analysis

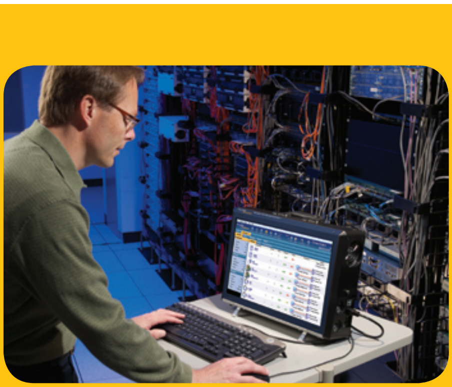
Introduction

In today's business environment, telephone calls are mission critical. For those who are either considering the leap to VoIP, or have already made it, the ability to monitor the quality of those calls is equally critical. Network latency, misconfigured hardware, and sluggish applications are simply unacceptable when it comes to voice calls and video conferences. An IT Professional needs to be equipped with the tools necessary to find issues before they are perceived by the users. Being able to visualize calls as they flow through the network is a requirement for quickly isolating and solving problems.

VoIP applications are increasingly complex. Unlike the older two-tier client-server model, VoIP phones first contact a Gateway or Server to locate the calling party, and then initiate the call with that party. While this multi-tier model has many benefits, it makes troubleshooting slow performance even more challenging.

Correlating both the call setup and actual call as a single flow is one of the most useful features in ClearSight Analyzer. Cumulating the two conversations together makes 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 also has the ability to capture the call at each location, and report on the call as it traveled through the network. Combining multi-tier analysis with multi-segment analysis, truly taps into the strength of ClearSight Analyzer.

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



About ClearSight™ Analyzer

ClearSight Analyzer provides detailed real-time analysis for many important network applications, including VoIP applications such as H.323, SIP, and Cisco's Skinny, Oracle, and MS SQL databases, POP, SMTP, and Exchange email, 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 server, for a specific flow, 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 VoIP calls, databases, email, 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.

Troubleshooting VoIP Problems

Because there are so many components involved in troubleshooting a multi-tier/multi-segment network, it is difficult to find out where the problem lies. The problem could be in the phone, network, gateway, 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/ Multi-Segment Network

1. Placement of the Analyzer
2. Capture Data
3. Save Data
4. Create Merged Trace files
5. View the Combined Flow

Troubleshooting with the Power of Multi-Tier Analysis

1. Placement of the Analyzer

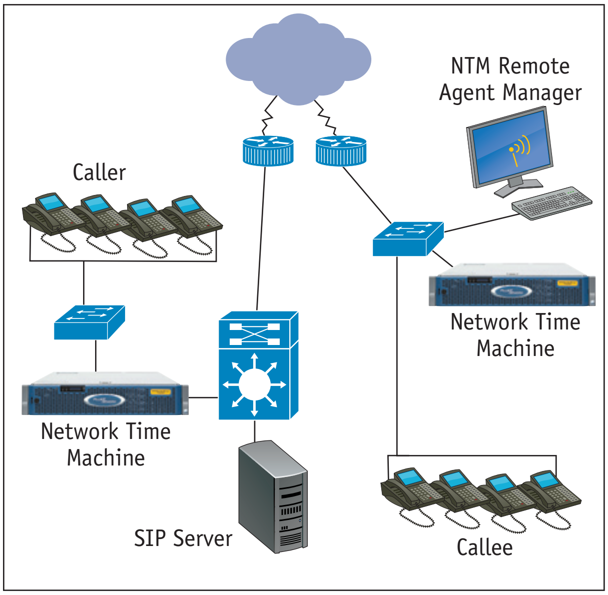
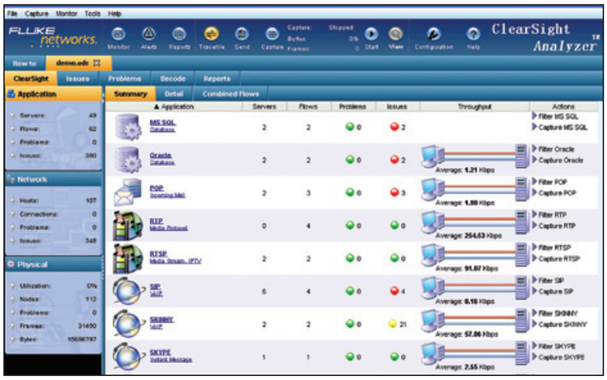


Figure 1: Sample VoIP Network

The key to multi-tier analysis is understanding how the data flows for a transaction. This paper will examine a SIP call. In the diagram above (see Figure 1), both parties use SIP phones. The Caller initiates the call with the SIP Server who forwards the invitation to the Callee. The Callee responds to the Server that it accepts the invitation, which the Server forwards to the Caller with the Callee's IP address information. The Caller can then send the voice RTP packets directly to the Caller. To see the conversation from all angles, the traffic from each phone is copied to an analyzer. In this way, we will be able to see both the conversation between the Caller and Server, and the Caller and Callee. By analyzing the traffic on the Callee's segment, we will be able to verify the receipt of all packets as well as their timings.

2. Capture Data

The Network Time Machine that has ClearSight Analyzer build-in began monitoring the network as soon as the application was opened, updating their 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 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 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 SIP is flowing across the segment in the initial screen (see Figure 2). A capture may be started at any time to have the data available for merging and future analysis.



Application

- Servers: 49
- Flows: 62
- Problems: 0
- Issues: 380

Network

- Hosts: 107
- Connections: 0
- Problems: 0
- Issues: 348

Physical

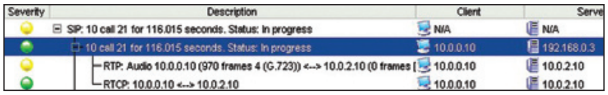
- Utilization: 0%
- Nodes: 112
- Problems: 0
- Frames: 31450
- Bytes: 15686797

▲ Application	Servers	Flows	Problems	Issues	Throughput	Actions
MS SQL Database	2	2	● 0	● 2		▶ Filter MS SQL ▶ Capture MS SQL
Oracle Database	2	2	● 0	● 2	Average: 1.21 Kbps	▶ Filter Oracle ▶ Capture Oracle
POP Incoming Mail	2	3	● 0	● 3	Average: 1.80 Kbps	▶ Filter POP ▶ Capture POP
RTP Media Protocol	0	4	● 0	● 0	Average: 254.53 Kbps	▶ Filter RTP ▶ Capture RTP
RTSP Media Stream, IPTV	2	2	● 0	● 0	Average: 91.87 Kbps	▶ Filter RTSP ▶ Capture RTSP
SIP VoIP	6	4	● 0	● 4	Average: 8.16 Kbps	▶ Filter SIP ▶ Capture SIP
SKINNY VoIP	2	2	● 0	● 21	Average: 57.86 Kbps	▶ Filter SKINNY ▶ Capture SKINNY
SKYPE Instant Message	1	1	● 0	● 0	Average: 2.55 Kbps	▶ Filter SKYPE ▶ Capture SKYPE

Figure 2: ClearSight Analyzer's Initial Screen

Easy to Use Interface

To view the SIP flows, simply click on SIP to move to the Detail pane. The information is available in real-time without yet requiring a capture of the packets. Since VoIP calls involve multiple protocols and stations, it is best to filter after the data is captured. Network Time Machine will combine the call setup, call control, and voice/video flows automatically in both Monitor and Capture (see Figure 3). Be sure to capture at both collection points at the same time.



Severity	Description	Client	Serve
●	⊟ SIP: 10 call 21 for 116.015 seconds. Status: In progress	N/A	N/A
●	⊟ 10 call 21 for 116.015 seconds. Status: In progress	10.0.0.10	192.168.0.3
●	RTP: Audio 10.0.0.10 (970 frames 4 (G.723)) <--> 10.0.2.10 (0 frames [	10.0.0.10	10.0.2.10
●	RTCP: 10.0.0.10 <--> 10.0.2.10	10.0.0.10	10.0.2.10

Figure 3: SIP Call in Real-Time

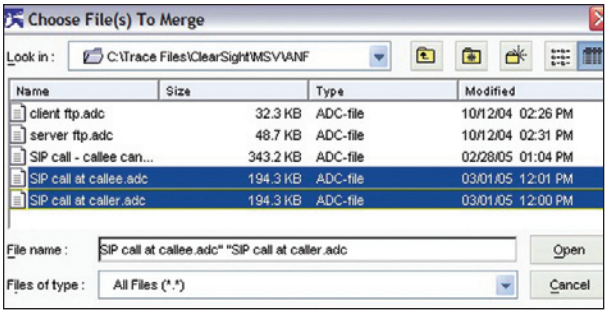
3. Save the Data

Once data has been captured on each segment, it must be saved. Give the trace file a unique file name, so it can be easily retrieved. Be sure to note in the trace file name where the analyzer was positioned.

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 4) 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.



Choose File(s) To Merge

Look in : C:\Trace Files\ClearSight\MSV\ANF

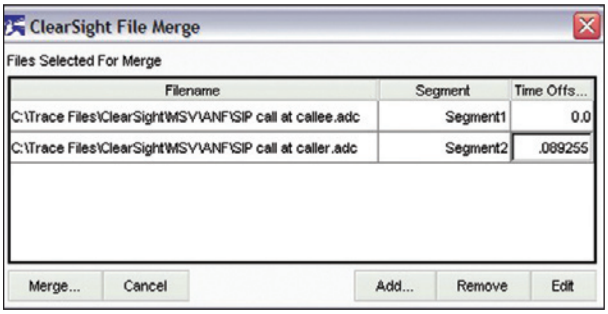
Name	Size	Type	Modified
client ftp.adc	32.3 KB	ADC-file	10/12/04 02:26 PM
server ftp.adc	48.7 KB	ADC-file	10/12/04 02:31 PM
SIP call - callee can...	343.2 KB	ADC-file	02/28/05 01:04 PM
SIP call at callee.adc	194.3 KB	ADC-file	03/01/05 12:01 PM
SIP call at caller.adc	194.3 KB	ADC-file	03/01/05 12:00 PM

File name : "SIP call at callee.adc" "SIP call at caller.adc"

Files of type : All Files (*.*)

Figure 4: File>Merge>Add Dialog Box

If the analyzers 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.



ClearSight File Merge

Files Selected For Merge

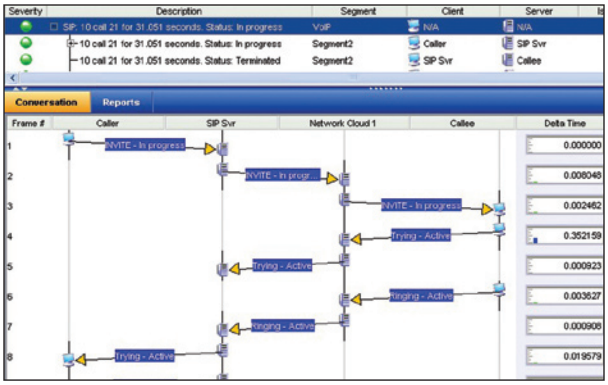
Filename	Segment	Time Offs...
C:\Trace Files\ClearSight\MSV\ANF\SIP call at callee.adc	Segment1	0.0
C:\Trace Files\ClearSight\MSV\ANF\SIP call at caller.adc	Segment2	.089255

Figure 5: Time Offset

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

5. View the Combined Flow

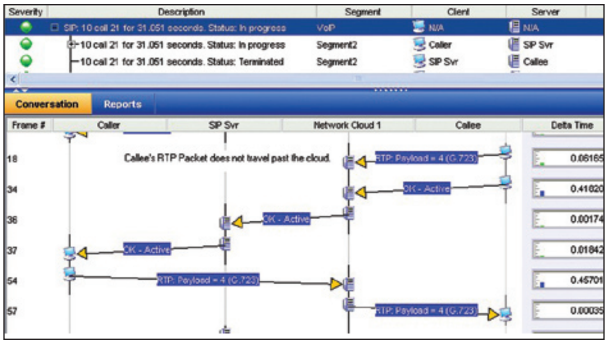
To view combined flows, open the newly created merged trace file. For VoIP calls, Network Time Machine does all of the work for you. The multiple tiers and multiple segments will be automatically combined and displayed in the Detail pane. If you select an individual flow, the multi-segment ladder view will appear in the Conversation tab of the Statistics pane (see Figure 6).



Severity	Description	Segment	Client	Server
●	SIP: 10 call 21 for 31.051 seconds. Status: In progress	VoIP	N/A	N/A
●	10 call 21 for 31.051 seconds. Status: In progress	Segment2	Caller	SIP Svr
●	10 call 21 for 31.051 seconds. Status: Terminated	Segment2	SIP Svr	Callee

Figure 6: Combined Flow

We can see that the call setup operated as expected. However, the Caller reported they could not hear the Callee. We will have to look further into the conversation. Once a call is established, we should see RTP packets. In frame 18, we can see that the Callee answered the call, but those packets did not reach the Caller's segment. Frame 54 shows that the RTP packets from the Caller's segment appear in the trace taken by the Callee, so we now know that RTP can travel only one way from Caller to Callee. The next step is to begin checking the routers on both segments to see where the packets are being dropped (see Figure 7).



Severity	Description	Segment	Client	Server
●	SIP: 10 call 21 for 31.051 seconds. Status: In progress	VoIP	N/A	N/A
●	10 call 21 for 31.051 seconds. Status: In progress	Segment2	Caller	SIP Svr
●	10 call 21 for 31.051 seconds. Status: Terminated	Segment2	SIP Svr	Callee

Figure 7: Identify the Missing RTP Packets

If additional analysis is required, performance related statistics appear in the Reports Tab. This report clearly shows that there were RTP packets missing from Segment 2 (see VoIP Report Samples on next page). 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.

Summary and Conclusion

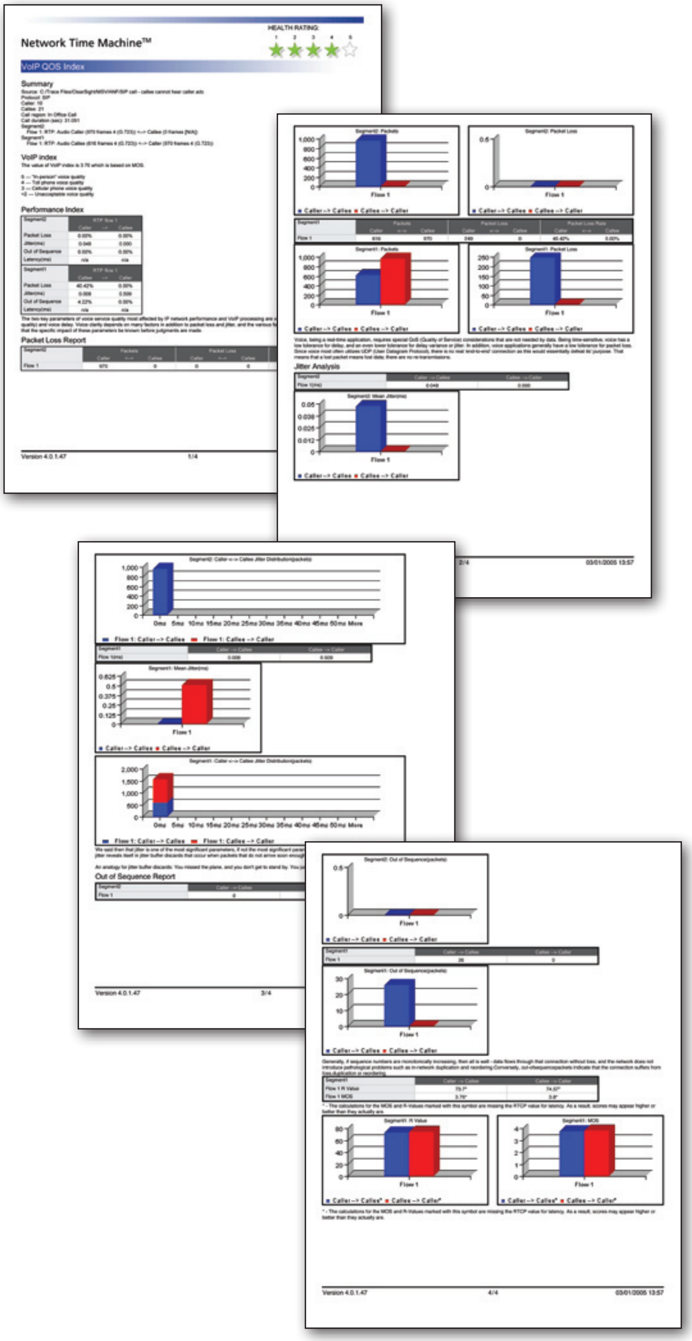
Networks are becoming more complicated every day, and the demands placed upon them are only exceeded by the expectations of the users. Every network environment consists of a wide variety of components. When one of these components fails, malfunctions, or is inefficient, it impacts a variety of network functions. The key is to be able to locate the specific issue, whether it is the phone, network, gateway, server or application. This is always a challenge, but becomes even more of a challenge when trying to locate the offender in a multi-tier/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
VoIP	Voice over Internet Protocol
Caller	The party who initiates the phone call
Callee	The party who is being called

VoIP Report Samples



TEquipment USA .NET
An Interworld Highway, LLC Company

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**.

©2010 Fluke Corporation. All rights reserved.
Printed in U.S.A. 06/2010 3790760A D-ENG-N