How to merge Trace Files with ClearSight™ Analyzer

Overview

Due to the complexity of today's networks, it's often difficult to pinpoint where problems occur. These problems may be caused by one or more network elements: network device (router, switch, firewall, etc.) client, server, or application. In addition, these elements may reside in different network segments. Viewing data from one segment provides only a local perspective. Viewing data from multiple segments becomes a challenge since correlation often proves too tedious and time consuming. With ClearSight Analyzer (CSA), this challenge is overcome by its ability to create a combined "ladder" diagram using trace files from up to four different network segments. IT Professionals will then be able to visualize data in proper perspective where the order of frames as they are generated, forwarded, received, processed, and replied to by the different network elements are taken into account.

How-to

This application note provides a methodology illustrating ClearSight Analyzer's Trace File Merge and Multi-Segment Analysis function. A general description of the function is given followed by a more detailed procedure.

A common first step in multi-segment analysis is to collect data from two or more (up to four) network segments and to save the data to respective trace files. The trace files may then be merged using the Trace File Merge function combined in CSA. The merged trace file will be displayed in a multi-segment view showing how and how fast packet transverse through each segment. The input trace files may be one of the following commonly used format: .adc, .enc, or .pcap format. The resulting merged trace files will be in .adc format for use with the ClearSight Analyzer (or Network Time Machine).

Steps to merge two or more Trace Files

1. Select Merge from the File menu. The ClearSight Analyzer Choose File(s) to Merge dialog box will appear.
2. Navigate to the location of the file(s) you want to include. Click or Ctrl-Click on the specific trace files. The result will be similar to Figure 1.

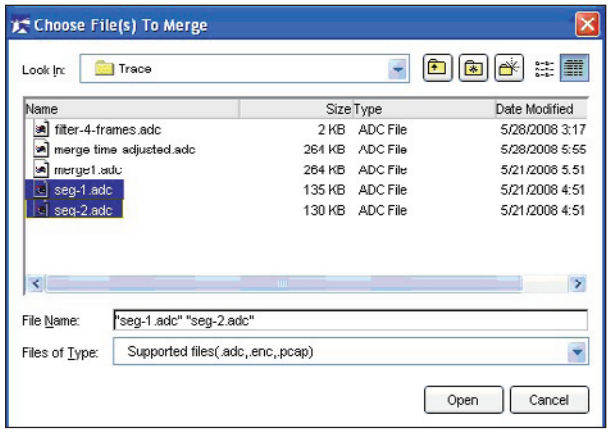

Figure 1: Choose Trace File(s) to Merge Dialog Box

3. Click Open. The ClearSight Analyzer File Merge dialog box will appear, with the file(s) you just selected included (see Figure 2). You can choose familiar names for the segments. To give a file a different segment name, double click in the Segment column for that file. Type in the new name or select a name from the drop-down list.

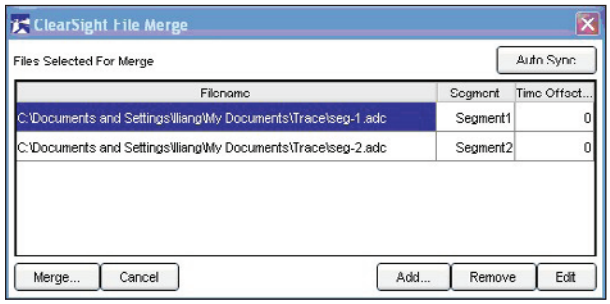

Figure 2: Trace Files Selected for Merge

How to merge Trace Files with ClearSight Analyzer

4. If the time stamp for the first packet is not the same in all the trace files, you can enter an adjustment factor for any file in the Time Offset (sec) column (see Figure 2). By clicking Auto Sync, ClearSight Analyzer can calculate Time Offset automatically IF there is TCP Connection (SYN, SYN/ACK, and ACK) frame sequence; otherwise, you need to calculate offset(s) time manually. An example of how to calculate the adjustment is shown in page 3.
5. Continue the process until you have gathered all the trace files that you want included. Up to four trace files may be specified. Then click the Merge button. The ClearSight Analyzer Save Merge To dialog box will appear (see Figure 3). Navigate to the location where you want to save the file, choose a name for the merged file, and click Save. The new merged trace file can now be opened in the ClearSight Analyzer.

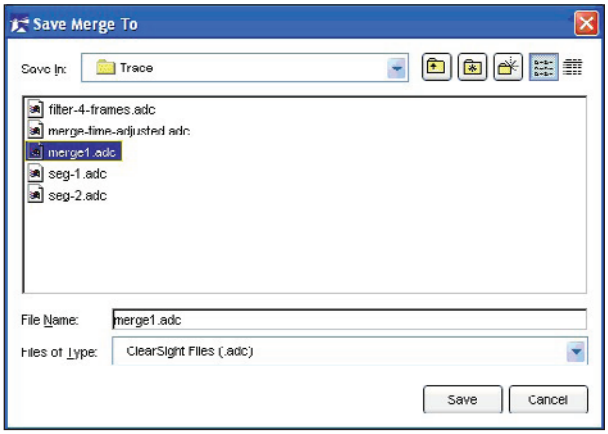

Figure 3: Save Merge To Dialog Box

Example on how to manually and calculate a time offset

In this section, how to calculate a time offset in detail. If there is TCP Connections (SYN, SYN/ACK, and ACK) frame sequence, CSA will calculate Time Offset automatically by clicking Auto Sync. However, you need to calculate time offset manually when there is no TCP Connection sequence.

1. Open the merge1.adc trace file. In our example, we select a MGCP-VoIP application from the Main pane of the Detail tab. Then we select one of these flows, and view the multi-segment ladder display in the Conversation tab of the Statistics pane (see Figure 4).
2. In the decode view, highlight 2 identical frames from 2 segments and check these frames on the left side (see Figure 5)
3. Right mouse click on the chosen frames and choose Filter Checked Frames as shown in Figure 6.

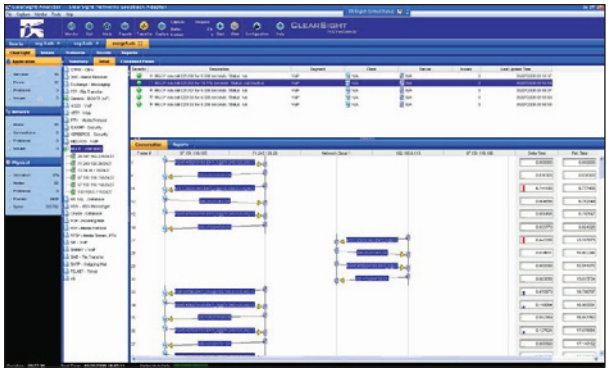

Figure 4: Ladder View for Merge1.adc Trace File

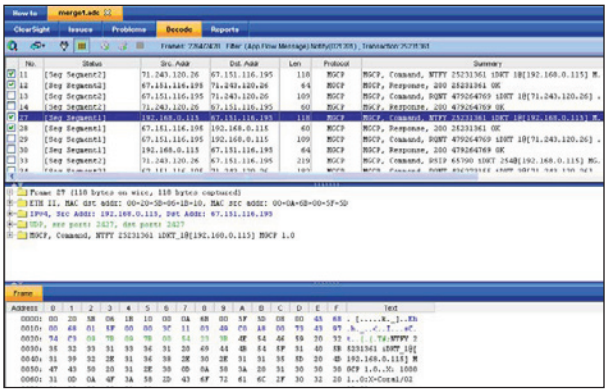

Figure 5: Decode View

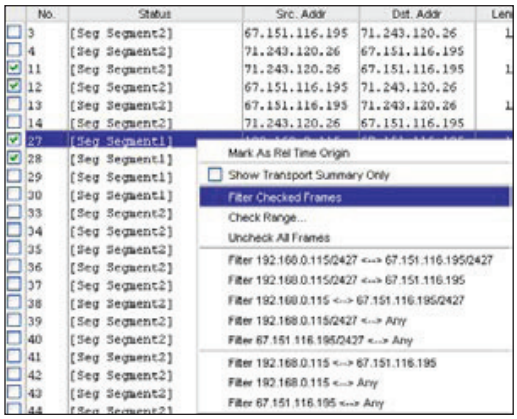

Figure 6: Filter Checked Frames

4. You will see 4 frames are filtered out as shown in Figure 7.These frames are saved into a new trace file. Filter-4-frames.adc, by clicking Save As from the File menu. The Save Filtered Packets dialog box will appear and you need to choose No in order to save filtered trace files (see Figure 8).
5. The filter-4-frames.adc will come up with only four frames as shown in Figure 9. Frames 1 and 2 belong to Segment 2, while frames 3 and 4 belong to Segment 1. The next step is to figure out the time offset between the two segments.

6. There are two timing values that we need to consider: relative time and delta time, as shown in Figure 9 and Table 1. The four frames listed with respect to their relatives times are shown in Figure 10. The primary goal is to align the central line of Frame 1 and 2 to the central line of Frame 3 and 4. A central line as shown in Table 1 is half of the Delta time between the two consecutive frames.

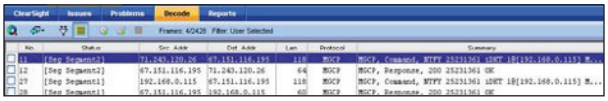

Figure 7: Filter Out Four Frames

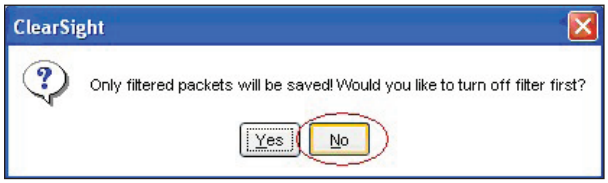

Figure 8: Save Filtered Packets

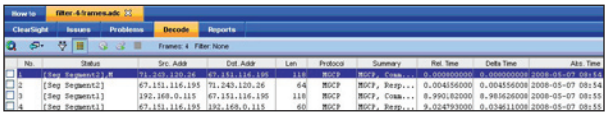

Figure 9: Filter-4-frames.adc

Calculate time offset

First, we align frame 1 to the t3 as shown in Figure 11. To align the central lines, we need to offset segment 2 by t6 – t5 = Δt4/2 - Δt2/2 (see Figure 12). Therefore, the correct time offset time to adjust Segment 2 to Segment 1 should be:

t = t3 + (Δt4 - Δt2) / 2 = 8.990182 + (0.034611 – 0.004556)/2 = 9.0052095

	Relative Time (sec)	Delta Time (sec)
Frame No. 1	t1 = 0	Δt1 = 0
Frame No. 2	t2 = 0.004556	Δt2 = t2-t1 = 0.004556
Frame No. 3	t3 = 8.990182	Δt3 = t3-t2 = 8.985626
Frame No. 4	t4 = 9.024793	Δt4 = t4-t3 = 0.034611
Central line of No.1 and No.2	t5 = Δt2 / 2	
Central line of No.3 and No.4	t6 = Δt4 / 2	

Table 1: Timing relationship between frames in trace files

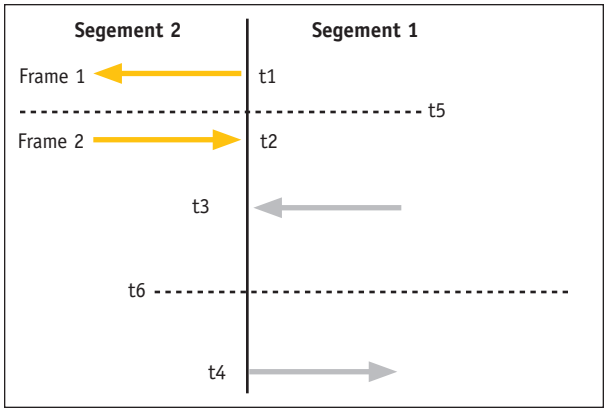

Figure 10: Original Four Filtered Frames

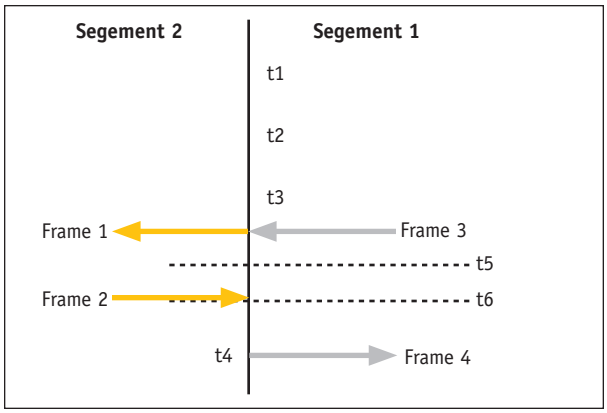

Figure 11: Move Segment 2 to t3 (Step 1)

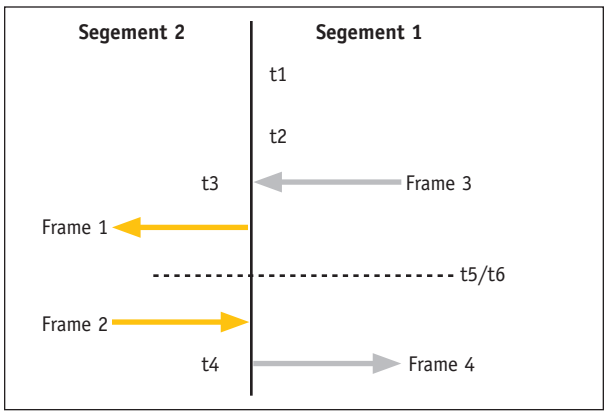

Figure 12: Move Segment 2 to the central of Segment 1 (Step 2)

Merge with the calculated time offset

Merge the original trace files again with the calculate time offset (see Figure 13). Then, we will get the new merged file shown in Figure 14.

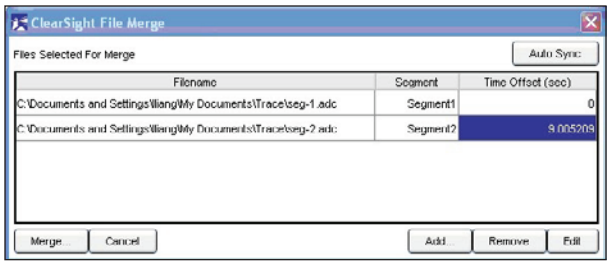

Figure 13: File Merge with the Correct Time Offset

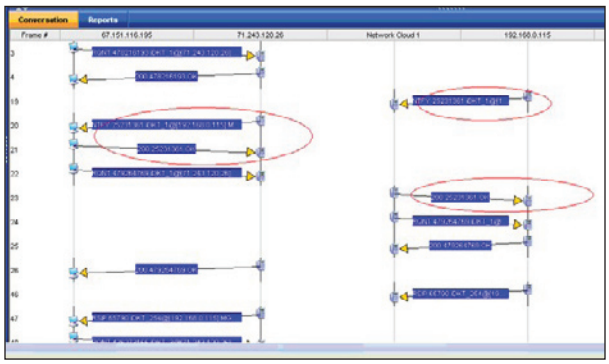

Figure 14: Merged Trace Files with Correct Offset

Summary

This application note has shown how to use file merge function by ClearSight Analyzer. How to merge trace files is explained step by step in this application note. Moreover, how to calculate time offset is discussed in this note and example on how to merge trace files is described in detail.

Readers are encouraged to extend the basic methodology in this paper to include additional file merge features such as combined VoIP flows, non-VoIP applications and other multi-segment functions.

Contact your nearest Fluke Networks Engineer to help you extend the methodology in this paper to help you to get the most benefit out of your ClearSight Analyzer and file merge functions.

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 3790785A D-ENG-N