Application Note: OneTouch™ AT / ClearSight™ Troubleshooting and Analysis Kit

While the OneTouch AT Network Assistant can solve most network problems quickly using its AutoTest and other features, in some cases trace file analysis is required to get to the root cause. Sometimes it's because an application problem is particularly complex, in others because it's the only way to prove to a third party that the problem isn't yours. In a recent Fluke Networks survey, customers reported performing packet analysis in 19% of problems.

Figure 1: OneTouch™ AT / ClearSight™ Troubleshooting and Analysis Kit

The OneTouch AT 3000 / ClearSight Analyzer bundle is designed to streamline the process of packet capture and analysis. The OneTouch AT is the fastest and easiest way to capture the packets you need to identify the problem; while the ClearSight Analyzer's unique application centric analysis provides an easy–to–understand view of application performance problems.

Packet Capture

When faced with the need to capture packets to troubleshoot an end user issue, a technician can choose between two common approaches. First, he can configure a mirror port in the switch. This involves logging into the switch, and changing the switch configuration to send copies of the packet stream to another port for capture by the analyzer. This requires access to the switch and significant expertise to get make sure the right packets are mirrored – and avoid making a mistake in the setup that could leave a large number of users without network access. For these reasons, most techs require assistance to set up mirror ports.

The second approach is to use a tap; a hardware device that connects in line with the user's PC and sends copies of the packets to the analyzer. Most techs don't carry taps, requiring a trip to get one, and finding a place to plug it in before capturing the traffic. Taps can also be instrumented into the network, but dealing with such a complex system presents issues similar to those of reconfiguring a switch.

Both approaches suffer from the fact that the problem may be gone by the time mirror ports or taps can be set up. Unfortunately, problems are very likely to come back, resulting in multiple calls to the help desk.

OneTouch AT's Built–In Tap

The OneTouch AT features a built in tap that makes it quick and easy to capture packets. Since it's physically connected between the user's PC and the network, it's already set up to catch the packets you're looking for. Acting as a passive device, it can't introduce any problems into the network while collecting packets.

Figure 2: OneTouch™ AT connection ports

While simple to use, the OneTouch AT provides sophisticated functionality not found in basic taps. Power over Ethernet is not only passed through, but is measured in real time. It supports both copper and fiber, without external transceivers. Full–duplex capture is supported, which would otherwise require an aggregating tap with buffering.

The OneTouch AT's 2Gb capture buffer is plenty for most single end user application issues. More efficient use of this space can be obtained by using the packet capture settings:

Figure 3: OneTouch™ sample of inline connections

Filter – Setting a filter allows the OneTouch to capture only a subset of the packets it sees. Filters may be set for: MAC or IP address, VLAN number, or IP Port. A NOT setting can be used to prevent the capture of certain packets, and IPv6 packets may also be filtered out.

Frame Slicing – This limits the capture the first "n" bytes of each frame, where n can be set to a range of values from 64 to 9,600. This conserves storage space by capturing only the important header information in the packets, which is all that is necessary for resolving timing and lost packet issues.

Connection – While inline mode is the easiest way to capture application traffic to and from a user having problems, the OneTouch AT also supports capture from either Port A Only, as well as Ports A and B which aggregates the two ports together. This last mode can be used to connect to an external full–duplex (dual–port) tap. AutoTest capture allows the OneTouch AT to capture the traffic generated by its own AutoTest for further testing server response without a user PC, and Wi–Fi mode allows capture of 802.11/a/b/g/n/ac traffic.

VoIP Capture – In this mode, in–line traffic is captured while call statistics including destination, length, and quality scores are displayed. Key parameters such as number of packets, errors, loss and jitter are shown. From these captures, the ClearSight Analyzer can generate call quality reports and even playback call content.

Accessing Capture Files

The OneTouch AT stores packet captures in PCAP format (easily readable by ClearSight and other common analyzers) on its removable SD memory cards. Transferring capture files to a PC may be done using the SD card, or for PC's without SD card readers, by copying the file to a USB memory device connected to the OneTouch AT. Files may also be downloaded using the OneTouch AT's remote control or cloud service through a wired or Wi–Fi management connection. This allows multiple captures to be acquired and downloaded to the PC without having to travel to the location of the tester. Since remote control is run through a separate connection it also provides full operation of the OneTouch AT, including capture settings, without adding its own traffic to the capture file.

ClearSight Analyzer

The award–winning ClearSight Analyzer (CSA) offers advanced application–centric monitoring and performance analysis, enabling enterprise Network Administrators and Engineers to maintain, diagnose, and resolve application and network performance issues in multi–protocol network environments. The ClearSight application analyzer supports the most commonly used protocols – both wired and Wi–Fi, and users can import Wireshark™ decodes to take advantage of the open–source community – making the ClearSight application analyzer the most versatile protocol analyzer in the market.

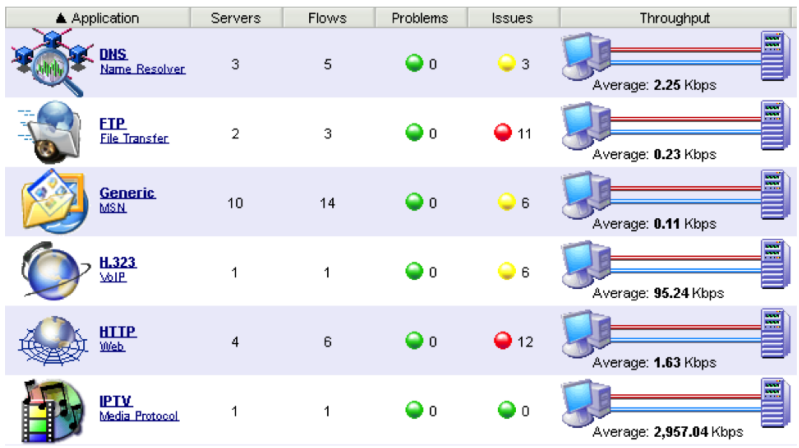

Figure 4: CSA analyzer screen

Application Centric Analysis

Through a simple and intuitive front page, CSA presents a comprehensive high–level overview of health of applications on your network. From that framework, you can drill down to gain access to more detailed information. As an example, you can display all the activity for HTTP application, then drill down to see activities on each server, and further down to the server flow to observe the actual media content of the flow. This unparalleled level of control and visibility speeds time to application problem resolution and minimize overall network downtime.

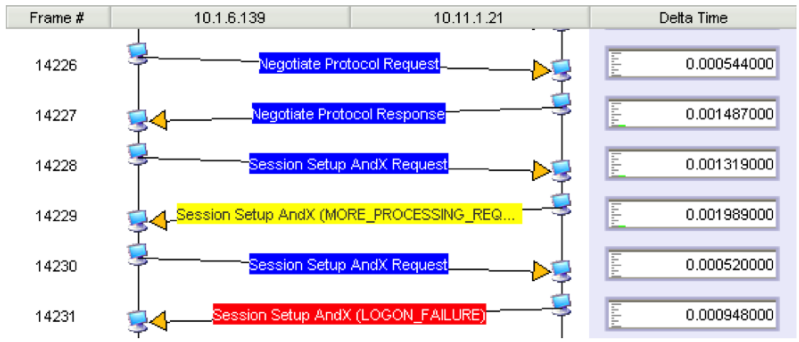

Figure 5: CSA network health overview screen

Content Playback

ClearSight Analyzer can recreate audio and video content from flows either during real–time monitoring or from a trace–file. In addition Exchange EMAIL, Fax over IP, Instant Messages and HTTP–base web pages can also be reconstructed. This is very valuable as proof of compliance violation or visualization of multimedia quality.

Ordering Information

Model Number	Description
1T–3000-CSA	OneTouch AT 1T–3000, plus ClearSight™ Analyzer Software on CD for decoding packet captures on a Microsoft Windows PC
GLD–1T3000	1 year of Gold Support for the 1T–3000 OneTouch AT Network Assistant
GLD–SW–1000	1 year of Gold Support Software Maintenance for CSA–1000
GLD3–1T3000	3 years of Gold Support for the 1T–3000 OneTouch AT Network Assistant
GLD–SW–1000–3YR	3 years of Gold Support Software Maintenance for CSA–1000