JDSU

Application Note

Packet Capture and Expert Troubleshooting with the JDSU T-BERD®/MTS-6000A

By Barry Constantine

Introduction

As network complexity grows, network provider technicians require the ability to troubleshoot problems within the various layers of the Transmission Control Protocol/Internet Protocol (TCP/IP) stack. Previously, the capability to capture and decode network packets was a feature found only in high-end protocol analyzers and required the corresponding network expertise to use such complex tools.

The ideal network field tool should provide both network installation and troubleshooting capabilities. Additionally, the troubleshooting capabilities should be easy enough for less experienced technicians to use, yet provide the advanced capabilities for experienced network engineers. Advantages of a dual-purpose field installation tool are:

- Increased workforce productivity: Installation technicians can use the dual-purpose field tool for initial turn-up/basic troubleshooting, and network engineers can remotely access the field tool for advanced troubleshooting
- Reduced test set costs: Eliminates the need to purchase dedicated (and expensive) protocol analyzers for occasional use

This application note describes the new workflow enabled by the T-BERD®/MTS-6000A Multi-Services Application Module (MSAM) with the Packet Capture and J-Mentor options. Technicians can perform packet capture decodes directly on the T-BERD/MTS-6000A user interface with the industry-standard open-source tool Wireshark (protocol decoder). The J-Mentor option allows less experienced technicians to troubleshoot basic network problems with its embedded packet capture diagnostic capabilities.

Another key feature of the T-BERD/MTS-6000A is the capture file format. It stores captures natively in standard packet capture (PCAP) format, eliminating the need for time-consuming post-capture conversion.

Traditional Turn-Up Testing Workflow

Using the T-BERD/MTS-6000A MSAM as part of traditional Layer 2/Layer 3 (L2/L3) installation (i.e., RFC 2544), Tier 1 technicians can verify end-to-end connectivity, measure bit error rate (BER), and determine whether throughput, utilization, frame loss, packet jitter, and round-trip delay (RTD) characteristics meet service level agreements (SLAs). Instead of requiring a dedicated troubleshooting test set such as a protocol analyzer, the T-BERD/MTS-6000A MSAM can also be used to troubleshoot during deployment and in operational networks.

Using Packet Capture to Conduct Basic Troubleshooting

In the ever-changing Ethernet and Internet Protocol (IP) world, providers must be able to troubleshoot problems at all layers of the stack quickly, cost-efficiently, and reliably. Troubleshooting basic network issues can become time-consuming. Frequently IP connectivity problems occur when first attaching a host to a network, including test instruments. When installation tests fail (i.e., RFC-2544, TCP testing, etc.), technicians can spend a significant amount of time adjusting IP stack settings and pinging, etc., which often results in higher costs for providers.

Similarly, conducting service-oriented network installation requires more advanced troubleshooting capabilities. Troubleshooting IP networks effectively requires line rate packet capture capabilities at wire speeds to 10 GigE. Few if any field testers can perform capture and decode even at 1 Gb/s, and are virtually non-existent at 10G line rate. The T-BERD/MTS-6000A MSAM from JDSU offers powerful filter and packet capture at all Ethernet line rates (10 Mb/s to 10 GigE). It is important to capture all the packets on the link to ensure retrieval of all important information. Once information has been captured, it can be viewed directly on the unit using the popular open source network analysis tool Wireshark to display the packet decodes.

Viewing Packets Directly on the T-BERD/MTS-6000A using Wireshark

Once the packets are captured, technicians typically must carry additional equipment in the field to decode and conduct analysis. The T-BERD/MTS-6000A provides capture and decode analysis using Wireshark directly on the test set; and it also allows for export of the packet capture (pcap) files for expert analysis. Using the integrated packet capture and decode provided on the test instrument itself greatly simplifies the troubleshooting process. Tier 3 technicians can remotely access the unit with a standard web browser and analyze the data or perform additional testing capabilities to resolve the problem.

Using J-Mentor to Automate Troubleshooting

Wireshark is an extremely powerful open-source protocol analyzer but requires a knowledgeable/senior staff member to troubleshoot many problems, which led JDSU to create a post-capture Expert Engine called J-Mentor that includes embedded network engineering best practices. This easy-to-navigate Expert Analysis tool provides graphs, charts, and tables to expedite diagnosis of network issues. With the J-Mentor expert diagnostic tool, technicians can use the T-BERD/MTS-6000A to resolve common network issues because the tool provides recommendations for further isolation and resolution.

Troubleshooting with Wireshark versus J-Mentor

Applications such as Wireshark often require technicians to carry a laptop computer to transfer files and to perform packet decodes. Often Tier 3 technicians are called in to perform the analysis or to run additional, more complicated tests. These extra steps incur further costs for providers. A considerably more cost-effective approach is to offer Tier 1 technicians an easy-to-use testing device that features Tier 3 testing expertise and analysis and eliminates the need for additional equipment, such as a laptop computer. Also, while packet decodes are useful, actually diagnosing the network problems remains difficult.

The following screen shots compare Wireshark analysis with J-Mentor. Note that the Wireshark example in Figure 1 has several menu items and requires an advanced level of expertise to debug; whereas, the screen shown in Figure 2 demonstrates the simplicity of the J-Mentor analysis tool. Technicians can quickly see the network layer where a suspected problem is detected and click for details about the diagnosis and receive recommendations for resolution.

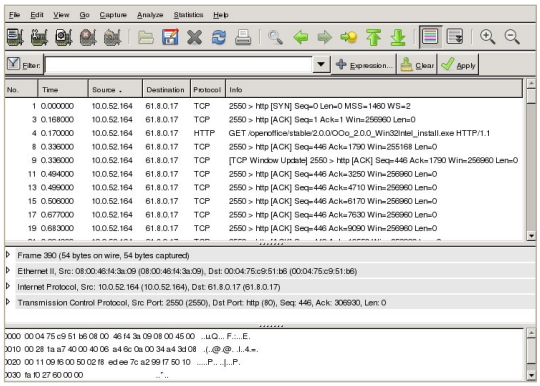

Figure 1. Wireshark screen shot for comparison

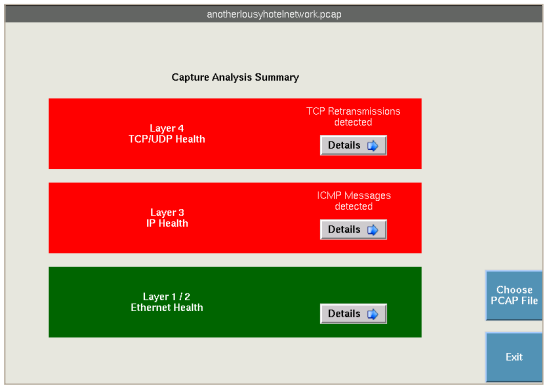

Figure 2. Example of a Capture file "health screen" with J-Mentor

Simple User Interface and Intuitive Diagnostics

Using the T-BERD/MTS-6000A with J-Mentor, technicians can view a simple network dashboard for Layers 1-4 that includes relevant graphs and tables complete with problem identification and recommendations.

Technicians can select the capture file to analyze and receive summary statistics for the packet capture file as shown in Figure 3.

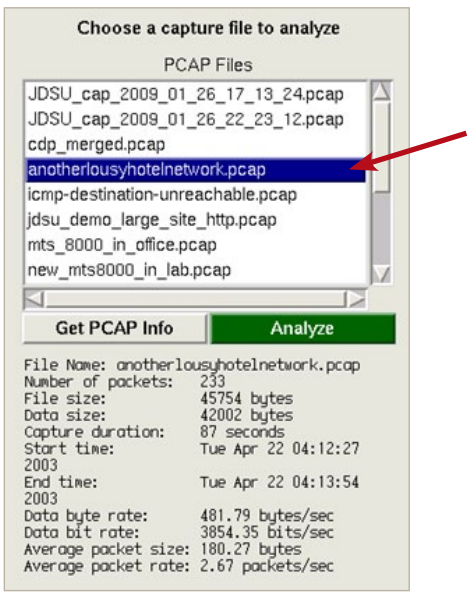

Figure 3. Choosing a capture file to analyze

After selecting the Analyze function, J-Mentor provides a simple dashboard results screen that quickly highlights the problem layers in the capture file and provides details if users want to drill down into the diagnostics as Figure 4 shows.

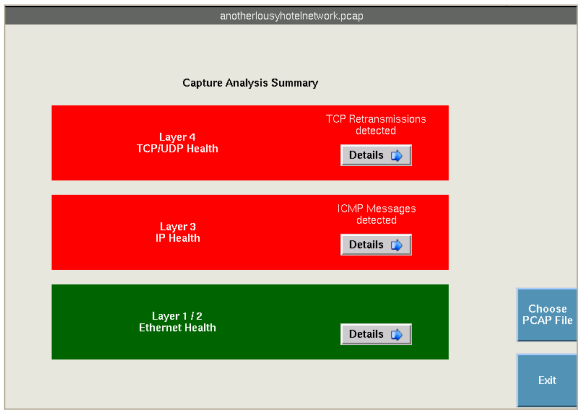

Figure 4. J-Mentor Dashboard Results Screen

Half-Duplex Port Detection

Half duplex port issues remain a cause for significant problems. The J-Mentor analysis option automatically detects switch advertisement messages and provides a list of Source MAC addresses, similar to those shown in Figure 5 below, that advertise Half-Duplex settings during the packet capture timeframe. The test set eliminates the need to filter or decode complex advertising protocols letting technicians focus on the problem ports with the click of a mouse.

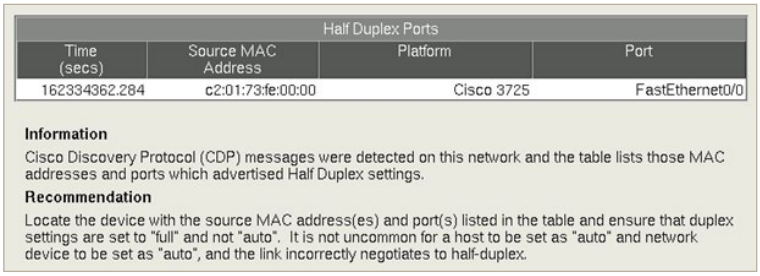

Figure 5. J-Mentor Half-Duplex Testing Results

TCP/IP Retransmissions

For applications that use TCP as the Layer 4 protocol (versus User Datagram Protocol, UDP), packet loss manifests itself in the form of TCP retransmissions. J-Mentor automatically detects retransmission issues and provides both a graph and table to diagnose the source(s) that are encountering the retransmissions. Figure 6 shows a network experiencing serious retransmission issues with the blue line indicating network utilization plotted along the red line showing retransmissions.

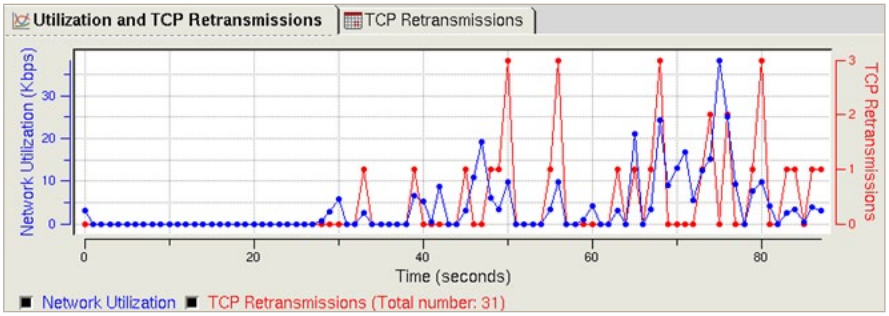

Figure 6. Graph Showing Network Utilization vs Retransmissions

The table in Figure 7 clearly shows the source(s) of the retransmissions along with an explanation of the possible problems. It also provides clear troubleshooting next-steps and recommendations.

TCP Retransmissions

Conversation	Source IP Address	Destination IP Address	Retransmissions
1	161.58.73.170	172.17.8.66	2
2	172.17.8.66	161.58.73.170	23
3	207.46.249.61	172.17.8.66	2
4	172.17.8.66	207.46.249.61	4

Information

This table identifies the IP Source Addresses that are experiencing TCP retransmissions. When TCP retransmissions are detected, this could be due to downstream packet loss (toward the destination side). It could also indicate that there is a half duplex port issue.

Recommendation

Check the port settings between the Source IP and the device it is connected to; verify that the half duplex condition does not exist. Further sectionalization can also be achieved by moving the analyzer closer to the Destination IP; determine if retransmissions are eliminated to isolate the faulty link(s).

Figure 7. TCP Retransmission Table

IP Top Talkers

Users who frequently send and receive large files are commonly known as "bandwidth hogs" or Top Talkers. Testers often search for these users because they are frequently the source of potential issues in poorly performing networks. J-Mentor provides a list like that shown in Figure 8 of the Top Talkers detected within the packet capture file along with the number of bytes and frames for each.

IP Converstaions

Source IP Address	Destination IP Address	Frames S <- D	Bytes S <- D	Frames S -> D	Bytes S -> D	Total Frames	Total Bytes
172.17.8.66	161.58.73.170	71	7249	104	19848	175	27097
207.46.249.61	172.17.8.66	28	4914	17	8187	45	13101
172.17.8.66	4.2.2.1	4	639	4	311	8	950
208.38.50.34	172.17.8.66	4	555	2	369	6	924

Figure 8. List of Top Talkers

Packet Capture Modes

This section summarizes the network access modes supported by the T-BERD/MTS-6000A for packet capture applications.

Single Port Termination Mode

IP connectivity problems such as incorrect IP stack setting and unresolved Address Resolution Protocols (ARPs) can occur during end-to-end Ethernet/IP installations. To troubleshoot these links, technicians can use the testers at each end in Terminate Mode to capture packets up to 10GigE from a single test port, using the T-BERD/MTS-6000A as an endpoint or host. The unit simultaneously generates typical throughput test traffic, or RFC 2544 and other application layer tests such as HTTP, FTP, and stateful TCP, at Layers 2 or 3 (IP). It also captures packets on the link, such as J-Proof protocol packets, or CDP and STP. J-Proof is a JDSU term used for packets that prove network connectivity.

Figure 9 shows an example of troubleshooting during end-to-end Ethernet service installation.

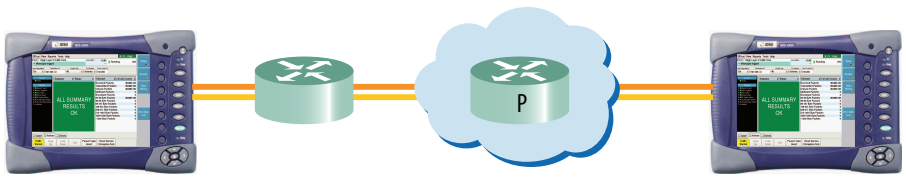

Figure 9. Troubleshooting end-to-end Ethernet service installation

Passive Monitoring from a Single Port

Connecting the T-BERD/MTS-6000A to a mirror or spare test port on a switch or router enables the monitoring and capturing traffic up to 10GigE. Figure 10 shows the unit configured for this type of monitoring and testing. Technicians can then analyze the captured packets natively on the test set using Wireshark, or they export them to a USB stick for further offline decode analysis.

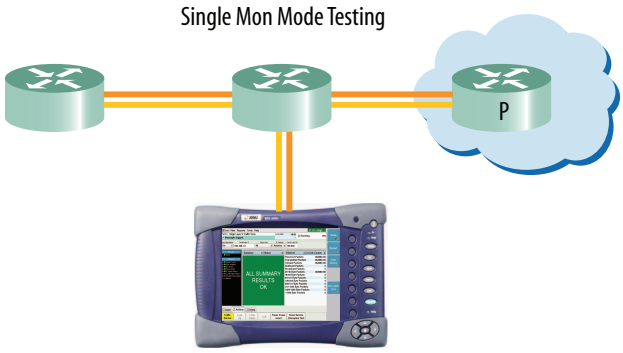

Figure 10. T-BERD/MTS-6000A monitors traffic forwarded by a router/switch mirror port or network tap

In-Line Monitoring Using Two Ports

Using the In-line Monitor Mode the T-BERD/MTS-6000A acts as a tap between two network elements, which is useful when a mirror port is unavailable or when higher confidence is desired to capture all packets, as network devices may drop packets in Port Mirror Mode. In this mode, the maximum line rate is 1G using the dual 1G test ports on the unit. Figure 11 shows the T-BERD/MTS-6000A using two ports in In-line Monitoring Mode.

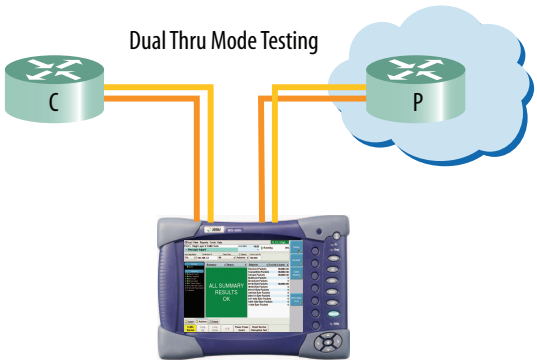

Figure 11. The T-BERD/MTS-6000A testing in dual Through Mode

Conclusion

Carrier Ethernet IP field networks present challenges to network providers and those who troubleshoot during installation or when experiencing operational problems. Those who can perform capture and decode analysis at wire speeds up to 10 GigE have the edge over their competitors. Few tools on the market today offer this capability; however, one easy-to-use tester offers capture and decode capabilities as well as expert analysis critical to the application. The T-BERD/MTS-6000A provides best practices testing capabilities in one powerful unit that makes complex testing procedures simple enough for less experienced technicians to function like a specialized pro. They can now troubleshoot basic network issues in significantly less time. It also enables advanced network staff to use the same tool for complex troubleshooting tasks and can be accessed remotely. The T-BERD/MTS-6000A provides everything technicians need to isolate and resolve Ethernet or IP problems in the field using in-depth capture and decode capabilities.

Test & Measurement Regional Sales

NORTH AMERICA
TEL: 1 866 228 3762
FAX: +1 301 353 9216

LATIN AMERICA
TEL: +1 954 688 5660
FAX: +1 954 345 4668

ASIA PACIFIC
TEL: +852 2892 0990
FAX: +852 2892 0770

EMEA
TEL: +49 7121 86 2222
FAX: +49 7121 86 1222

WEBSITE: www.jdsu.com/test

 30162943 000 1209 PACKETCAP6000.AN.TFS.TM.AE December 2009