J-Mentor
Packet Capture Expert–
Complexity Made Simple

Solution Description

Capture and Decode is a test option for the T-BERD®/MTS-6000A Multi Services Application Module (MSAM) that provides wire speed packet capture from 10 Mbps to 10 Gbps. It provides post-capture decode analysis for the experienced user by utilizing Wireshark directly on the test set and for the novice user by allowing the .pcap capture files to be exported and analyzed by a specialist. With the included J-Mentor expert diagnostic tool, common network issues are automatically detected and recommendations provided for further isolation and resolution.

Ordering Information

Included with:
1G Capture – CTLSCAPTURE (-U1)
10G Capture – CT10GCAPTURE (-U1)

Use Case

Troubleshooting Carrier Ethernet and IP field networks

Value Proposition

While Wireshark provides powerful packet decode and network debugging capabilities, it can be daunting for users with beginner-medium network troubleshooting experience. By integrating the best practices of senior network experts into the T-BERD/MTS-6000A, common network problems are automatically detected within the packet capture file. With this powerful troubleshooting assistant, the user is presented with a simple network dashboard (Layer 1-4) and provided with pertinent graphs, tables, etc., all with problem identification and recommendation. This provides field technicians the visibility into which layer of the network problems are occurring, allowing them timely fault isolation and correction.

Intended Audience

- Special Operations and Central Office technicians responsible for fault troubleshooting.
- Professional Services and Managed Service Engineers responsible for the maintenance, troubleshooting and evolution of end-customer access networks.
- Enterprise and Government network professionals responsible for circuit and network installation and fault analysis.
- Applications: Isolating and resolving Ethernet or IP problems in the field using in-depth capture and decode capabilities.

J-Mentor Feature/Benefit Summary

Feature	Description	Advantage	Benefit
Expert diagnosis of capture files	User is presented with simple interface to analyze capture files	Embed senior network expertise into the field tool	Reduce troubleshooting time of common network issues
Detect Half-duplex ports	Half-duplex port settings are a common cause of network performance issues	No need to filter / decode complex advertising protocols	User can hone in the problem port(s) with the click of the mouse
Detect IP Layer issues	ICMP messages can indicate unreachable ports and hosts	Automatically detects the "bad" ICMP messages	Identifies the unreachable host IP addresses and the last hop router
Identify Top IP Talkers	IP address pairs that are exchanging the most network traffic are the top talkers	The user does not need to be a Wireshark expert to identify top talkers	Top talkers is a key network statistic and helps track bandwidth hogs
TCP Layer expert analysis	TCP retransmission issues significantly affect network throughput	TCP retransmissions versus network utilization chart correlation	Identifies between which IP addresses TCP retransmissions are the occurring, which can cause poor network performance

Simple User Interface and Intuitive Diagnostics

Select the capture file to analyze and summary statistics are provided for the packet capture file.

After selecting the Analyze function, J-Mentor provides a simple dashboard results screen which quickly highlights the problem layers in the capture file and provides "Details" drill down into diagnostics

Use Case: Detect Half-duplex port

Half duplex port issues still are a cause of considerable headaches. Most networks advertise port settings: J-Mentor automatically detects these messages and provides a list of Source MAC addresses which advertised Half-Duplex setting during the packet capture time interval.

	Half Duplex Ports		
Time (secs)	Source MAC Address	Platform	Port
162334362.284	c2:01:73:fe:00:00	Cisco 3725	FastEthernet0/0

Information

Cisco Discovery Protocol (CDP) messages were detected on this network and the table lists those MAC addresses and ports which advertised Half Duplex settings.

Recommendation

Locate the device with the source MAC address(es) and port(s) listed in the table and ensure that duplex settings are set to "full" and not "auto". It is not uncommon for a host to be set as "auto" and network device to be set as "auto", and the link incorrectly negotiates to half-duplex.

Use Case: Identify IP Top Talkers

It is common to search for "bandwidth hogs" as a source of potential issues in poorly performing networks. J-Mentor provides a listing of the Top Talkers that were detected within the packet capture file along with the number of bytes and frames for each talker

	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

Use Case: Identify TCP Retransmission Issues

For applications that use TCP as the Layer 4 protocol (versus UDP), packet loss manifests itself in the form of TCP retransmissions. J-Mentor automatically diagnoses retransmission issues and provides both a graph and table to diagnose the source(s) that are encountering the retransmissions.
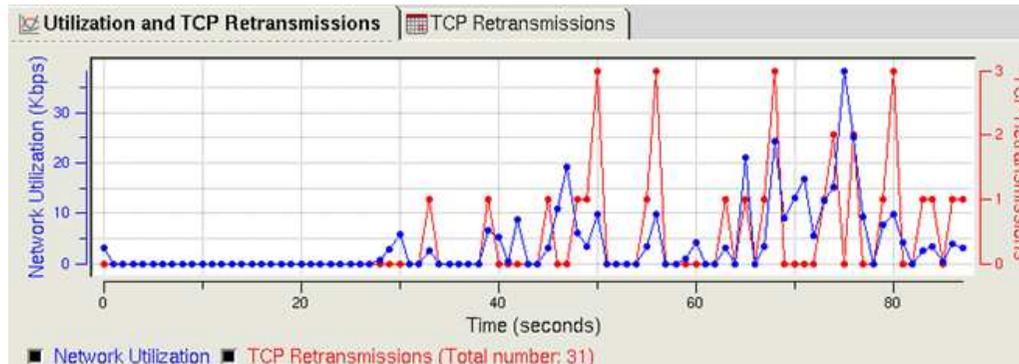
Network utilization (blue line) is plotted along with Retransmissions (red line) and in this example, the network is experiencing serious retransmission issues.

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

And the table clearly reveals the source(s) of the retransmissions, providing clear troubleshooting segmentation and next step recommendations

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).

FAQ

Q: What is Wireshark?
A: Originally named Ethereal, Wireshark is a network protocol analyzer (or packet Sniffer computer program) used for network troubleshooting and decode analysis.

Q: Why do customers need J-Mentor if they can use Wireshark?
A: Protocol analysis is a very complex skill and even senior folks can find Wireshark a daunting tool to master.   J-Mentor provides a best practices methodology to the protocol analysis workflow and is squarely aimed at troubleshooting / diagnosing problems. Lower experienced and advanced users will benefit from its "push button" diagnosis capability.

Q: Is this a software or hardware upgrade to existing units in the field?
A: Capture Decode is a software upgrade and J-Mentor is included with this option at no additional charge.

Q: Will J-Mentor grow in capabilities with future releases?
A: Yes. J-Mentor will evolve to include more of the best practice troubleshooting "rules" and even more complex diagnosis methods.