

Troubleshooting LANs with Network Statistics Analysis

Introduction

This application note is one in a series of local area network (LAN) troubleshooting papers from JDSU Communications Test and Measurement. Troubleshooting LAN issues covers a wide array of network problems and diagnostic scenarios that may include:

- evaluating network utilization over the course of a business day by link, virtual LAN (VLAN), or subnet
- detecting excessive broadcast or multi-case traffic
- finding “bandwidth hogs”
- understanding what protocols are present on the network (and determining whether they should be)
- identifying the “top-talkers” on the link—the IP devices that are consuming the most capacity
- experiencing application performance issues (slow web server response time or intermittent unavailability of an e-mail server).

Before network troubleshooting can begin, one must have a clear understanding of network test access. Testing tools used for network analysis and troubleshooting scenarios must be able to monitor the network traffic being tested. The most common means for monitoring a network is using the built-in port mirroring capabilities of a network device, such as the switch/router or to install a special “tap” device between the devices being analyzed, such as those between an application server and database server. Figures 1 and 2 show each test access mode for analyzing traffic between a switch and a router.

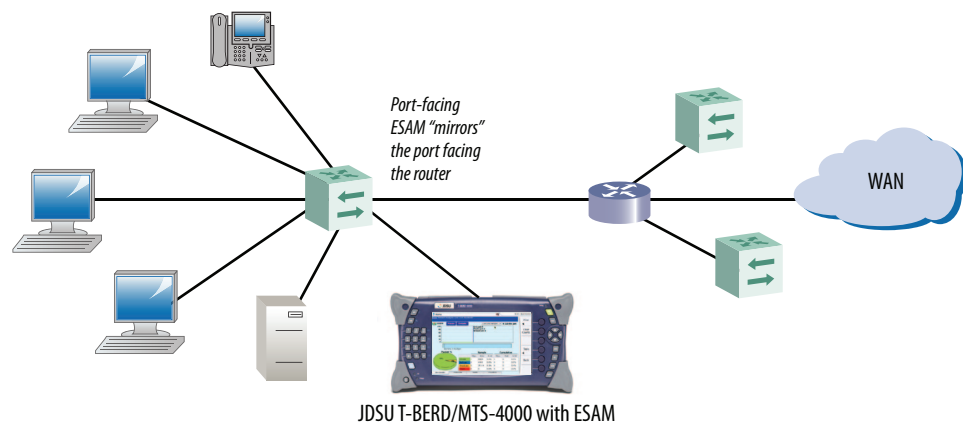


Figure 1: Test access via port mirroring

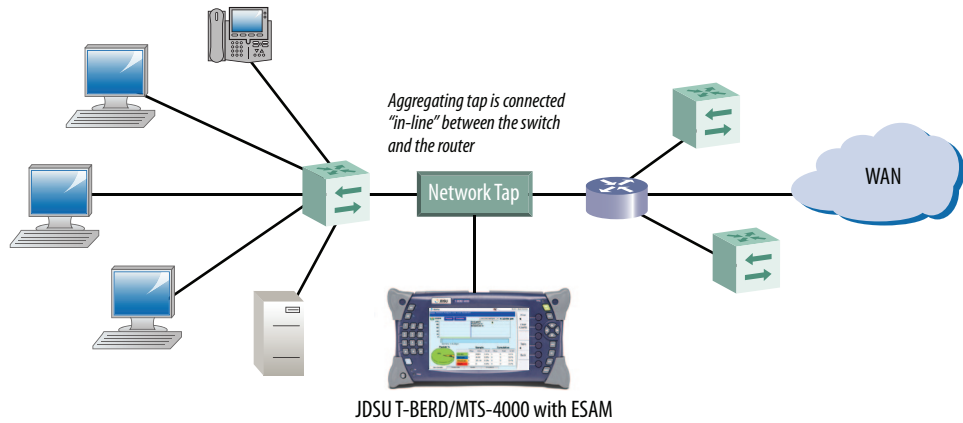


Figure 2: Test access with a network tap

In the port mirroring test access mode shown in Figure 1, the T-BERD®/MTS-4000 Enterprise Services Application Module (ESAM) is connected directly to a spare switch port (10M/100M/1000M) that is configured to copy all traffic to and from the port facing the router to the spare port. Because a mirror port can copy traffic from both directions out a single port, it will drop frames if full-duplex link utilization exceeds 50 percent. Aggregating taps perform similarly as they funnel both directions of traffic out of a single port. Likewise, if the full-duplex link utilization exceeds 50 percent, it also drops frames. Some aggregating taps have internal buffers that allow them to compensate for bursts above 50 percent.

As a general rule, port mirroring is the preferred approach as there are generally spare switch ports and no interruption to production traffic is required to install the tap.

The following table provides a summary of each test access mode:

Item	Port Mirroring	Aggregating Network Tap
Disruptive to network operation	No. A port mirror command does not interrupt normal production traffic.	Yes. Must install network taps during off-hours or as part of the production installation on critical network links.
Handle full line rate traffic	Handles up to 50-percent traffic utilization before dropping packets. Port mirroring may not be able to "keep up" on busy network links.	Handles traffic up to 50-percent utilization before dropping packets. Aggregating taps with buffers can compensate for bursts above 50 percent. A good network tap will not drop any production traffic, but may drop duplex traffic (on heavily loaded links) because the duplex traffic is combined into a single test access port.
Pass Layer 1 and Layer 2 Errors	No.	Depends on the tap. Some pass errors, some do not.
Require network device administrative privileges	Yes. Console access to the network device is required to enable port mirroring.	No.
Cost	Usually free, because most switches have a spare port.	Reputable 1000Base-T taps can cost \$1000+.

The following sections summarize a practical approach to conducting network analysis using the JDSU ESAM for the T-BERD/MTS-4000.

Network Analysis Workflow

There is no single method for analyzing network issues and yet there are some best practices that experts use in their day-to-day troubleshooting activities. Figure 3 shows the JDSU proposed network analysis workflow.

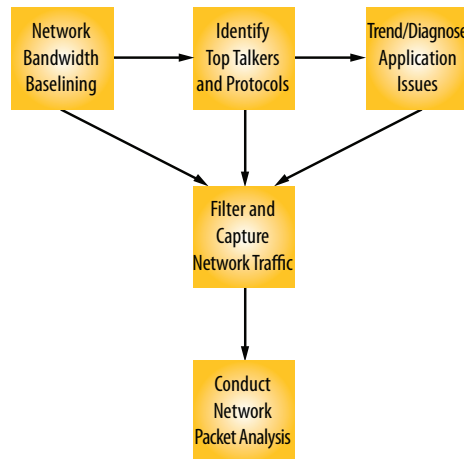


Figure 3: Best practices Network Analysis workflow

The following briefly describes each step in the workflow.

1. **Network Bandwidth Baselineing:** Baselineing network utilization over a period of time, such as over the course of a business day, is a valuable first step because it provides insight into general bandwidth consumption at different times of the day. With graphically trended views of network utilization, users can easily detect utilization spikes and determine if they are due to excessive broadcast or multicast traffic. Baselineing by VLAN or subnet can clearly identify network bandwidth usage by application service or remote offices.
2. **Identify Top Talkers and Protocols:** After baselineing the network utilization, the next step is determining who or what is consuming the network bandwidth. This step requires easy-to-understand tables and charts that display such items as Internet Protocol (IP) top talkers and top protocols.
3. **Trend and Diagnose Application Issues:** Applications have many unique communication characteristics, and it is impossible to isolate problems with standard counters such as top IP talkers and standard protocol counts, such as Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). To troubleshoot tough application problems, users must configure custom filters/counters that can look deep inside the packet and detect application-specific events. For example, receiving a failed Database response “Item not found” where using a custom deep packet inspection counter can trend and troubleshoot the application problem.
4. **Filter and Capture Network Traffic:** At any of the steps listed above, users must conduct content-sensitive packet captures. For example, to identify an IP Top Talker and simply select it as a capture filter. The JDSU ESAM provides a simple capture filter user interface for the more common filter scenarios and also provides advanced deep packet inspection (DPI) filters that can search within the payload of packets.
5. **Network Packet Analysis:** The JDSU ESAM conducts analysis of the capture files directly using the popular open source software Wireshark. The ability of the test tool to perform expert analysis and diagnose common network problems within the packet file is also essential.

This application note covers network analysis Steps 1-3 in detail and briefly covers Steps 4 and 5. A separate application note in the series is devoted to the topics of capture filtering and analysis (Steps 4 and 5).

Network Bandwidth Baselineing

Baselineing network utilization over a period of time, such as the course of a business day, is a valuable first step because it provides insight into general bandwidth consumption at different intervals.

Connecting the ESAM to either a port mirror or tap access point enables graphical display of network utilization as Figure 4 shows.

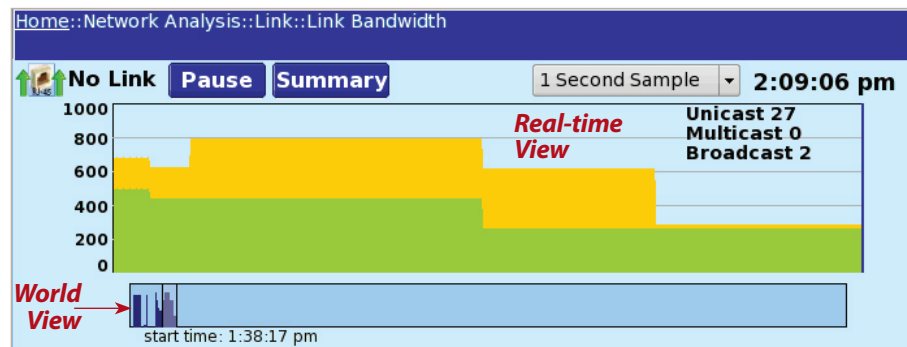


Figure 4: Network trending, Link utilization view

The ESAM can chart the network utilization over the course of an 8-hour business day and provides both the world view and a zoomed-in real-time view. The world view offers a great view of the entire trended time period to detect potential issues. While the real-time view allows users to select a period of time from the world view and zoom in on the problem area.

This case reveals the occurrence of excessive broadcast traffic, possibly indicating that a legacy device remains connected to the network that is consuming link bandwidth.

In addition to trending the total utilization a very beneficial practice is baselineing by VLAN or subnet to clearly identify network bandwidth usage by service or remote offices.

Enterprise networks use VLANs and IP subnets to prioritize and organize services and/or departments within the corporate LAN. The use of VLANs and subnets vary; however, several common examples are listed below:

- Assign voice over IP (VoIP) traffic to a common VLAN with higher priority over default data traffic
- Use VLANs to group an office by department in order to isolate broadcast and multi-cast traffic from one department to another
- Use IP subnets per each remote office, making it possible to study site bandwidth usage within the main office campus or data center

Figures 5 and 6, respectively, demonstrate the ability to view network utilization by VLAN or subnet using the ESAM network trending view.

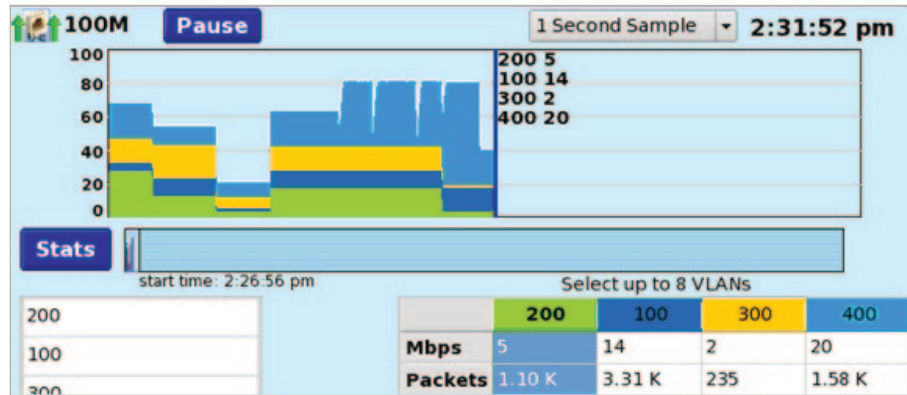


Figure 5: Network trending VLAN view

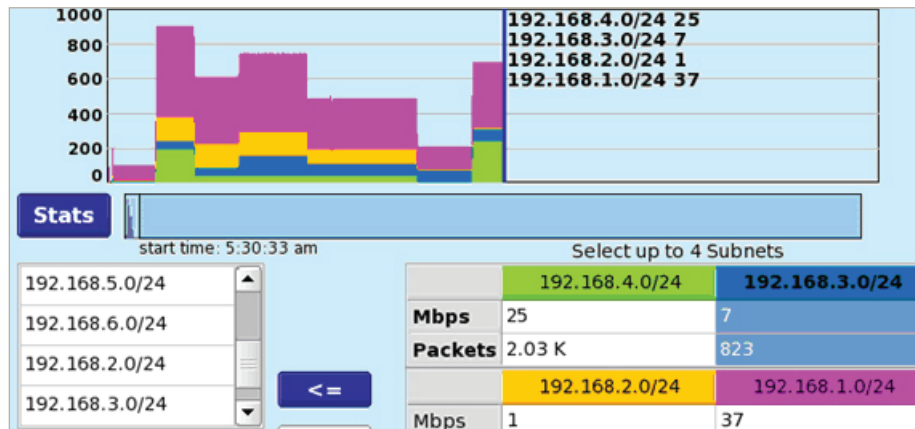


Figure 6: Network trending Subnet view

In these graphs, technicians can view the usage by VLAN or subnet to study usage trends and make decisions about service or site bandwidth upgrades.

Identification of Top Talkers and Protocols

After baselining the link utilization, the next step is determining who or what is consuming the link bandwidth. At this step in troubleshooting problems, technicians must identify the top IP talkers and protocols in terms of network bandwidth consumption, such as HTTP, file transfer protocol (FTP), or SMTP. The ESAM user interface makes viewing top talkers and protocols easy, as Figures 7 and 8 show.

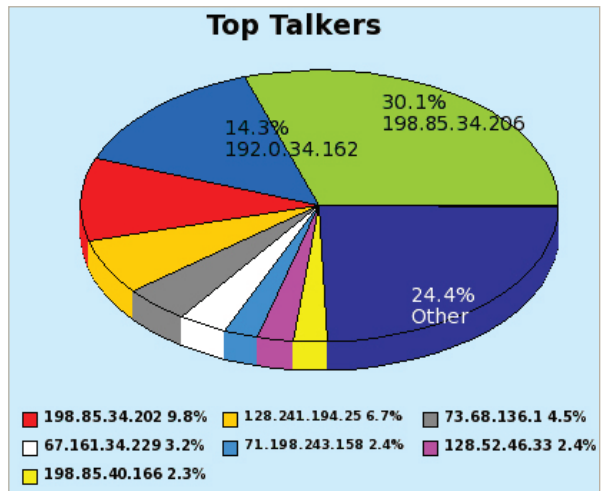


Figure 7: Top Talkers

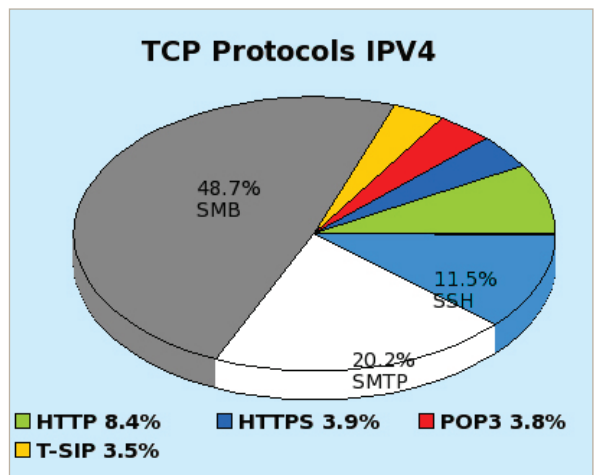


Figure 8: Top Protocols

Looking at the Top Hosts view, it is easy to see that 198.185.34.206 is consuming 30 percent of the overall link bandwidth. It is also noticed that the Microsoft file sharing protocol (SMB) is consuming nearly 49 percent of the network bandwidth.

With this information, the network troubleshooter can drill into the specific IP bandwidth hog (198.185.34.206) and conduct a packet capture. This can be accomplished by simply clicking on the 198.185.34.206 portion of the pie chart and the pop-up window appears, as shown in Figure 9.

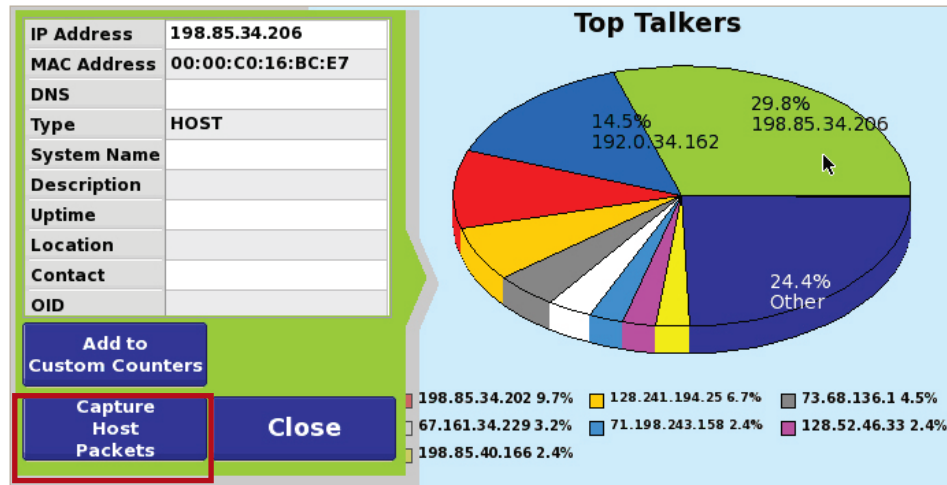


Figure 9: Context-sensitive capture filter of Top Talkers

Simply clicking “Capture Host Packets” in the pop-up window will automatically apply a filter and the user can view the captured packets directly on the ESAM user interface using Wireshark, as shown in Figure 10.

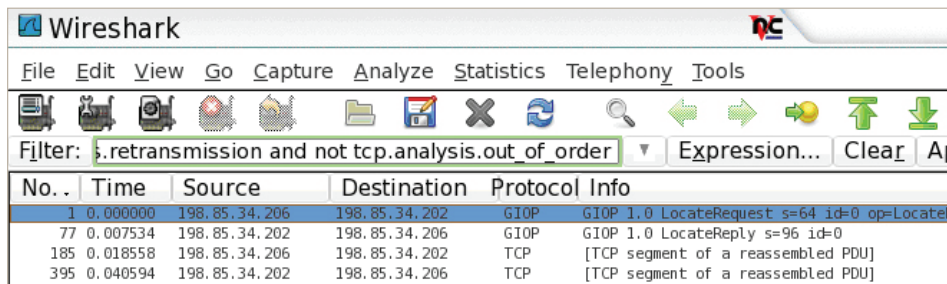


Figure 10: IP Top Talker capture viewed with Wireshark on the JDSU ESAM

The network statistics workflow enabled the troubleshooter to:

- quickly understand network usage over time
- determine if broadcast/multicast traffic was a major consumer of bandwidth
- study network traffic over time according to VLAN and subnet usage
- drill into top talkers and top protocols
- isolate top talker to “one-click” filter and view in Wireshark

The finer aspects of packet capture, filtering, and analysis are covered in a separate JDSU application note that is part of this series entitled **Troubleshooting LANs with Wirespeed Packet Capture and Expert Analysis**.

One other very useful diagnosis technique is to examine fundamental network counts for a variety of common protocols and message types to determine how many Internet Control Message Protocol (ICMP) messages exist versus Address Resolution Protocol (ARP) frames, jabbers, and Cyclical Redundancy Check (CRC) errors.” Conducting this type of analysis can prove very complex with a simple packet capture device. However, the JDSU ESAM provides more than 25 built-in standard counters that provide a very concise view of the common, interesting protocols as shown in Figure 11.

Home::Network Analysis::Link::Built-in Wire Speed Counters							
	Name	Packets	Bytes		Name	Packets	Bytes
1	Total Packets RX	11.2 M	8.4 G	16	IP-V6	0	0
2	Total Packets TX	0	0	17	Multicast	0	0
3	L2 Broadcast	19965	5.9 M	18	ICMP	0	0
4	L3 Broadcast	16220	5.6 M	19	TCP	0	0
5	VLAN IP-V4	0	0	20	TCP (win size=0)	0	0
6	VLAN IP-V6	0	0	21	UDP	0	0
7	802.2	1791	134 K	22	IGMP	0	0
8	IP-V4	11.1 M	8.4 G	23	CRC errors	5	644
9	Multicast	0	0	24	RUNT Frames	0	0
10	Fragments	11.1 M	8.4 G	25	JABBER Frames	0	0
11	with options	0	0	26	ARP request	3742	249 K
12	ICMP	0	0	27	ARP reply	0	0
13	TCP	11.1 M	8.4 G				
14	TCP (win size=0)	4368	280 K				
15	UDP	16223	5.6 M				

Highlight Changes

Figure 11: JDSU ESAM wirespeed protocol counters

These Wirespeed protocol counters provide a “Highlight Changes” feature that makes it much easier for the network troubleshooter to spot rapidly changing counts. These types of statistics are very beneficial to more advanced troubleshooters who have a good feel for what is normal on the network.

Trend and Diagnose Application Issues

Applications have many unique communication characteristics making it impossible to isolate problems with standard counters like top IP talkers and standard protocol counts, such as HTTP, SMTP, and others. To troubleshoot tough application problems, users must configure custom filters/counters that can look deep inside the packet and detect application-specific events.

For example, users complain that database queries timeout requiring them to restart their database application periodically throughout the day. A network assessment of the backend database server shows that network utilization is only 20 percent even during peak hours. Perhaps the database system is causing errors itself under higher user load; however, the network is (of course) always under suspicion.

Conducting packet captures would be literally like trying to find the “needle in the haystack” considering the volume of users. Applications such as databases usually produce some type of response code when an error occurs. In our example, the database administrator provided information that the following query response occurs in the event of such an error:

“Response code 327: Unknown search name”

It is beneficial to trend the network packets based on custom fields, but often the fields are not part of the header but deep within the packet. In this scenario, DPI techniques are the appropriate means for troubleshooting this problem. DPI examines payload within the packet payload (as opposed to simply looking at the header). The JDSU ESAM is equipped with advanced DPI technology.

In this case, the ESAM must first be configured with a custom DPI filter. Note that these filters can also be used as custom counters, so the number of Errored response events can be counted as well as filtered for capture. This example demonstrates the use of the DPI filters as trending counters.

First, create the custom filters for the normal Database Response and Request messages. The request and response are similar and Figure 12 shows the Database Request filter.

Item	Value
Filter Name	Database_Request
Filter By IP Address	None
Filter By MAC	None
Filter By Port	None
Filter by VLAN	None
Payload 1 Setting	Search Payload
Payload 1 String	Select_from_Names

Figure 12: Configure a DPI filter for Database Request

Similarly, configure the Data Error Response filter as shown in Figure 13.

Item	Value
Filter Name	Database_Error
Filter By IP Address	None
Filter By MAC	None
Filter By Port	None
Filter by VLAN	None
Payload 1 Setting	Search Payload
Payload 1 String	Response_Code_327:Unknown_se...
Payload 2 Setting	Ignore

Figure 13: Configure a DPI filter for Database Error

Once these filters are configured, the database server can be monitored at various times of the day to compare total Database Requests/Responses to Database Errored messages, as shown in Figure 14.

	Name	Packets	Bytes
1	Database_Request	244944	349 M
2	Database_Response	244944	349 M
3	Database_Error	405	510 K

Figure 14: Database statistics over a 1-hour busy time period

The 244,944 Database Requests and Response occurred with 405 Errors. While the number of Errors may seem insignificant, it is supposed to be zero. At other times of the day with light database usage, such as early in the morning, this same test yielded a similar number of requests (over a longer duration) and indeed with zero errors.

This example clearly shows the power of custom counters on a live network. These counters can be assigned standard Ethernet, IP and Protocol values, and more importantly DPI-based payload counters that enable powerful application level statistical analysis and diagnosis.

Conclusion

Troubleshooting LAN network issues cover a wide array of network problem and diagnostic scenarios. Typical network problems covered in this application note included:

- evaluating utilization over the course of a business day by link, VLAN, or subnet
- detecting excessive broadcast or multi-case traffic
- finding “bandwidth hogs”
- understanding what protocols are present on the network (and determining whether they should be)
- experiencing application performance issues (slow web server response time, intermittent unavailability of an email server)

Each of these network problems is complex to solve and requires an efficient troubleshooting methodology and easy-to-use LAN test tool that provides detailed network statistical analysis.

The JDSU ESAM for the T-BERD/MTS-4000 provides a workflow-based interface that “walks” the user through the best practices approach to solving a multitude of network problems. Figure 15 shows the JDSU T-BERD/MTS-4000 platform with ESAM interface (and an optional fiber probe scope). Figure 16 shows the workflow-based user interface.



Figure 15: JDSU T-BERD/MTS-4000 with ESAM



Figure 16: ESAM workflow-based user interface

The JDSU ESAM for the T-BERD/MTS-4000 provides comprehensive LAN testing capabilities with these features:

- Layer 1-7 protocol capture and expert analysis
- network connectivity
- network discovery
- a full range of physical media tests
- a workflow-based user interface
- a modular platform with many options:
 - VoIP phone emulation
 - OPM/VFL
 - fiber inspection probe with automated pass/fail
 - WiFi testing
 - OTDR modules

Through its workflow-based intuitive user interface, the ESAM provides physical media tests including speed-certification of electrical Ethernet cabling, network connectivity tests, discovery, wirespeed deep-packet statistics, and wirespeed protocol capture and expert analysis using unique, in-depth JDSU J-Mentor capabilities. In addition, the ESAM is part of the modular JDSU T-BERD/MTS-4000 platform allowing additional options that include VoIP emulation, Wireless Fidelity (WiFi) testing, IP video testing, optical power meters (OPMs), visual fault locators (VFLs), digital fiber inspection probes, and optical time domain reflectometers (OTDRs). Test connectivity can be obtained either electrically via a 10/100/1000 RJ45 Ethernet jack or via a small form-factor pluggable (SFP) for optical Ethernet.

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/esam
---	--	---	---	--