JDSU Network Analyzer Software
Technical Overview

Key Benefits

- **Reduces OpEx by avoiding unnecessary dispatches and reducing mean time to repair (MTTR) from days to minutes**
- **Greatly improves visibility at the edge when integrated with PacketPortal™**
- **Increases average revenue per user (ARPU) by eliminating premises visits and solving problems faster from a central location**
- **Provides affordable access on a massive scale with powerful real-time monitoring and analysis**
- **Analyzes and troubleshoots across virtually any network with pervasive on-demand monitoring**
- **Narrows QoE/QoS-affecting packet and ATM cell-based issues to a specific location**

Applications

- Advance protocol analysis
- Wireline solution for LAN and WAN
- IPTV, VoD, and VoIP QoE analysis
- Advanced mobile network analysis solution for 2/2.5/3/4G technologies

JDSU Network Analyzer software lets network professionals maintain and optimize voice, data, and video services quickly over next-generation networks and decreases operational costs by enabling testing any technology, over any interface, anywhere by anyone.

Network Analyzer protocol-analysis software, in conjunction with the Distributed Network Analyzer (DNA), 10 Gigabit/Gigabit Ethernet blade hardware, and the revolutionary PacketPortal solution provides an expert network testing and troubleshooting solution that supports real-time measurements in LAN, WAN, and ATM environments. In addition, this solution can be deployed so that network monitoring and troubleshooting activities can be coordinated from a single, centralized location.

Network Analyzer software runs on a standalone PC or on the DNA platform. Several additional elements complement the Network Analyzer solution such as Report Center, Telephony Network Analyzer, Instrument Manager, and File Translator.

JDSU® PacketPortal™
E N A B L E D
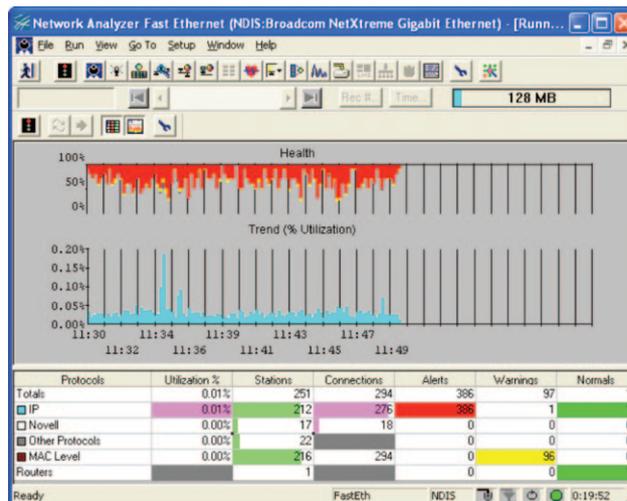
Figure 1. Network Analyzer software provides expert commentators for network performance advice and problem resolution

2

Network Analysis and Troubleshooting Solutions Overview

The JDSU Network Analyzer is one of the key software applications that runs on the scaleable Network Analysis and Troubleshooting Solutions platform. This platform provides the foundation of advanced protocol analysis. Take advantage of extensive diagnostic capabilities for troubleshooting and optimizing voice, video, and data networks, as well as 2/2.5/3/4G mobile networks.

The DNA hardware platform brings greater power for collecting and analyzing real-time data over multiple technologies such as Ethernet, ATM, POS, Frame Relay, IPv6, MPLS, VoIP, IPTV, LTE, HSDPA, HSUPA, UMTS, CDMA 2000, and GPRS.

The scaleable DNA hardware platform provides the foundation of advanced protocol analysis architecture for fixed and mobile network applications. Couple the hardware with Network Analyzer and you have a powerful wireline solution for LAN and WAN networks; couple the DNA platform with the Triple Play Analyzer for IPTV, VoD, and VoIP QoE analysis. Similarly, use the hardware in conjunction with Signaling Analyzer to create an advanced mobile network analysis solution for 2/2.5/3/4G technologies.

Network Analyzer software   Triple Play Analyzer software   Signaling Analyzer software

Distributed Network Analyzers

Figure 2. Combine your DNA platform hardware with Signaling Analyzer software for mobile network testing, with Network Analyzer software for fixed wireline network testing, and with Triple Play Analyzer software to test next-generation VoIP

3

Network Analyzer Solution Components

Network Analyzer software

J6840A	Network Analyzer software
J6865A	Network Analyzer 10 GigE Blade Interface software
J6839A	Network Analyzer Software Professional Edition

Add-on licenses

J6844A	VoIP Telephony Network Analyzer
J6848A	Report Center
J6825A	Inverse Multiplexing for ATM (IMA) and Multi-Link WAN Technologies license
J6835A	NDIS server
J6765A	Network Analyzer RFC2544 LAN benchmarking
J6766A	MPLS analysis
J5425A	Switch advisor

Data acquisition platform

J6801B	DNA
J6802B	DNA MX
J6803B	DNA PRO
J6872A	10 Gigabit/Gigabit Ethernet Blade Interface

Utilities

File translator	Time sync Data File Merge Utility

4

Network Analyzer Solution Components

The J6840A Network Analyzer has extensive capabilities including:

- It is the base software for controlling the DNA family of products.

- It runs on PCs as a software analyzer, using off-the-shelf NDIS network interface cards (NICs) as measurement interfaces for LAN (10/100/1000 Mb/s Ethernet, Token Ring and FDDI). For example, the 10/100 PC Cards (PCMCIA cards) found in most PC laptops can be used as the test interface for monitoring the LAN network traffic, even while this card is simultaneously providing the network connection for the PC.

- It is the client software and GUI for accessing the J6835A Network Analyzer NDIS Server running on another PC.

- It provides off-line analysis, allowing previously captured and saved LAN and WAN data from any Network Analyzer hardware platform, JDSU Advisor or NDIS-based NIC, to be re-analyzed using the full features available on-line for captured data.

- It includes file translator to allow analysis from a variety of industry standard formats.

Network Analyzer is pre-loaded and runs on the embedded PC in the J6802B and J6803B platforms. It is also shipped on the DVD media with the J6801B DNA, together with a single-use license key to enable the software on a PC/laptop. License keys plus manuals and DVD media for running the software on additional PCs can be purchased as the J6840A Network Analyzer software product. For example, a second engineer can control an existing DNA from their PC, with the purchase and installation of J6840A. The engineer can also use the software to perform LAN testing with an NDIS-based NIC, or perform offline analysis of previously captured LAN or WAN data.

5

Network Analyzer Solution Components

J6865A Network Analyzer 10 GigE/GigE Blade Interface software

The J6865A Network Analyzer software is required to use the J6872A 10 Gigabit/Gigabit Ethernet Blade Interface acquisition and analysis hardware in order to:

- capture and analyze 100% of the traffic at 10 G
- perform full Network Analyzer measurements.

J6839A Network Analyzer Software Professional Edition

The J6839A Network Analyzer Software Professional Edition is a lighter version of Network Analyzer, designed for non-distributed real-time analysis on a standard PC. It has all of the capabilities of the J6840A Network Analyzer, except for Distributed Network Analyzer LIM (Line Interface Module) control.

It has the following capabilities:

- it runs on PCs as a software analyzer, using off-the-shelf NDIS network interface cards (NICs) as measurement interfaces for LAN (10/100/1000 Mb/s Ethernet, Token Ring and FDDI). For example, the 10/100 PC Cards (PCMCIA cards) found in most PC laptops can be used as the test interface for monitoring the LAN network traffic, even while this card is simultaneously providing the network connection for the PC.
- it provides off-line analysis, allowing previously captured and saved LAN and WAN data from any Distributed Network Analyzer hardware platform, JDSU Advisor or NDIS-based NIC, to be re-analyzed using the full features available on-line for captured data.

Network Analyzer software comparison

	J6840A Network Analyzer software	J6839A Network Analyzer Software Professional Edition	J6865A Network Analyzer 10 GigE/ GigE Blade Interface software
Offline analysis	LAN/WAN/ATM	LAN/WAN/ATM	LAN/WAN/ATM
Controls analyzer HW	Yes	No	Yes
Can be used with NDIS Server J6835A	Yes	Yes	Yes
Install footprint	850 MB	110 MB	950 MB

6

Network Analyzer Software Detailed Specifications

Features

Network Analyzer offers multiple capabilities, particularly when used with the Network Analyzer hardware platforms. The following information describes these features.

Flexible and unified approach lets you:

- test over LAN and WAN interfaces with identical network and higher-layer measurement features and user experience
- analyze MPLS for troubleshooting converged networks
- analyze with specialized hardware and off-the-shelf NDIS PC-Card NICs
- solve network problems quickly and effectively with the Expert Analyzer
- anticipate network problems using performance statistics and vitals
- analyze critical full-duplex server or backbone links
- obtain thorough information with comprehensive network statistics
- decode 500+ protocols across all seven layers
- test in IPv4 and IPv6 (or mixed IPv6 and IPv4) environments
- navigate easily with the graphical user interface
- run all the powerful measurements of the Network Analyzer, including the Expert Analyzer, on your own PC using Network Analyzer Software off-line analysis.

Guided troubleshooting lets you:

- get continuous feedback on key network issues
- identify problems by severity to prioritize troubleshooting
- isolate faults quickly without extensive protocol knowledge, using drill-down sequences
- stream decoded data to external storage with Run-Time Store to Media
- get extensive online Help to explain problems and recommend solutions.

**Network Analyzer Software
Detailed Specifications**

Features (continued)

Information for understanding network issues lets you:

- select only the required data with flexible capture and display filters
- focus on troubleshooting the network and not on configuring the instrument with the auto-encapsulation mechanism. This includes support for GRE and GTP tunneling. Automatic detection with measurements are reported on the highest IP layer.
- understand traffic patterns with Connection Statistics
- identify MAC and network nodes through use of Node Discovery
- export statistics to the Report Center for long-term trend analysis and more in-depth analysis

Advanced lower-layer Capabilities lets you:

- monitor line vitals on all WAN/ATM interfaces
- perform ATM analysis on a wide range of interfaces up to 622 Mbps, including the eight-port E1/T1 ATM analysis and inverse multiplexing, and on the sub-rate tributaries of channelized STM-4/OC-12 and STM-1/OC-3
- auto-discover and perform analysis on over 1024 ATM virtual channels that have been reassembled (AAL-2 and AAL-5) in real time simultaneously on any ATM interface or tributary (cell mode analysis is also available)
- perform packet over SONET/SDH (PoS) analysis up to 622 Mbps
- collect multiple statistics per DLCI on all discovered Frame Relay virtual channels or per VPI.VCI on over a thousand ATM virtual channels (in SAR mode or cell mode) simultaneously
- perform policing and graph 1-Point CDV on up to 1024 ATM virtual channels simultaneously with other measurements on all interfaces except the eight-port E1/T1 multi-port LIM
- estimate suitable ATM traffic contracts on up to 1024 ATM virtual channels simultaneously
- generate LAN traffic on 10/100/1000 Mbps and 10 GE
- generate AAL-5 segmented higher layer and cell-based traffic on all ATM interfaces (except IMA and ATM25) up to 622 Mbps
- analyze over V-series and HSSI interfaces
- analyze HDLC, PPP and ISDN.

Network Analyzer Software Detailed Specifications

Features (continued)

Advanced measurements to solve problems quickly

Network Analyzer has a wide range of specialized capabilities that will help you solve network problems.

Over the next few pages, the following capabilities are described in detail:

- **Expert Analyzer** graphs utilization and health over time and provides summary information on connections, protocols and network events of interest.
- **Data Filtering** allows you to focus on the important data and make efficient use of the capture buffer.
- **TCP Connection Analysis** lets you analyze TCP connections and quickly identify delay and retransmission issues.
- **Multi-segment jitter, latency, and packet** loss identifies the source of packet degradation across multiple segments in a network.
- **RTSM**, run-time store to media allows post-analysis forensics on captured traffic.
- **Encapsulation Discovery** allows the analyzer to find the higher layer data regardless of the lower layer encapsulation including support for tunneled GRE or GTP traffic.
- **Protocol Commentator** provides a detailed list of network events on connections and on nodes.
- **Protocol Statistics** provide a detailed view of the active protocols on the network, including utilization statistics, number of errors and average frame size.
- **Node Discovery** provides a list of node physical addresses, names, network addresses and events that have occurred on each node.
- **Baselining** lets you see how the network is changing over time.
- **Protocol Vitals** provide a list of every node on the network, showing utilization and data link layer (DLL) errors.
- **Connection Statistics** provide a detailed view of every active connection including the protocols used and the problems encountered.
- **Protocol Decodes** display the contents of every packet on the network in summary, detailed or hex format.
- **IPv6 Protocol Analysis** is fully supported and available for all measurements and analysis.
- **LMI Statistics and Commentator** track statistics on the LMI channel in a Frame Relay network and identify anomalies in protocol behavior.
- **ATM VPI.VCI statistics and Frame Relay DLCI statistics** provide detailed statistics on a per VC and per port basis. Compliance to service level agreements is easily seen.
- **ATM policing** shows why data errors are occurring in ATM networks.
- **ATM Usage Expert** analyzes ATM traffic to determine what would be a suitable traffic contract for each virtual channel in terms of PCR, SCR, CDVT and MBS.
- **Active Tests** allow you to generate traffic, copy from buffer for edit and playback, PING, and ARP.

9

Expert Analyzer

No matter what your traffic level is, Network Analyzer transforms data into meaningful diagnostic information, constantly monitoring the traffic on your network. The Expert Analyzer reduces thousands of frames to a handful of significant events. It watches continuously for router misconfigurations, slow file transfers, inefficient window sizes, connection resets, and many other problems. It does this for each protocol stack you have running (including IPv6); all in real time as events actually occur.

- Alert events indicate a serious network problem, such as "zero time to live" in IP.
- Warning events highlight a configuration or performance problem in the network, such as "connection refused" in Oracle, then list all possible reasons for the refusal.
- Normal events give information on normal network transactions, such as "OSPF router identified" and provide statistics on the IP and MAC addresses as well as the number of OSPF routers identified.

An additional drill-down capability enables you to focus on the data, discover the source of the problem and find a recommended solution.
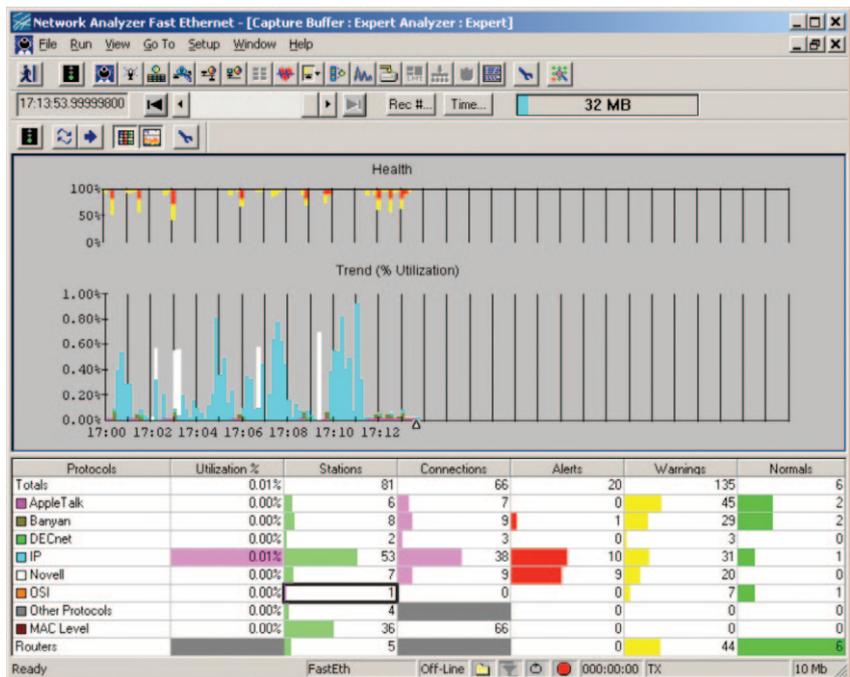
Figure 11. Expert Analyzer summarizes network conditions in a simple screen, with drill-down capabilities for major details

Network Analyzer Software Detailed Specifications

Data Filtering

The J6801B DNA, J6802B DNA MX, J6803B DNA PRO, and J6872A 10 Gigabit/ Gigabit Ethernet Blade Interface support two types of data filtering to assist in troubleshooting and analyzing the large quantities of data generated on a high-speed link: capture and display filters. Hardware-based capture filters allow the user to specify which data the instrument should store in the capture buffer or analyze in real-time. Software-based display filters let the user specify which captured frames should be shown on the display.

The acquisition system used in the J6801B DNA, J6802B DNA MX, J6803B DNA PRO and J6872A 10 Gigabit/Gigabit Ethernet Blade Interface allows 100% of all data via any interface to be captured (full-duplex), regardless of the link speed, link utilization, or errors; the specialized hardware will catch everything. Often, the data of interest occurs rarely; even large capture buffers can fill quickly, particularly from higher rate interfaces. The data acquisition system has sophisticated hardware capture filters so that capture memory is used with maximum efficiency, avoiding the capture of vast amounts of data of no interest. These capture filters consist of 32 simultaneous hardware protocol filters (each 256 bytes wide) and are in addition to hardware filters in the LIMs that can also filter traffic by ATM VPI.VCI labels. These capture filters operate on all data entering the acquisition system, whether or not the data is to be captured or analyzed in real-time. One measurement that operates on data before capture filtering is the Protocol Vitals measurement.

Any number of hardware filters may be active at the same time; multiple active filters are logically ORed. Network Analyzer allows you to set up filters by frame attributes. For example, when filtering LAN traffic, filters can be specified to filter frames with a bad frame check sum (FCS), runts (collisions), jabbers, dribbles, or the data portion of the packet. When filtering by data, up to 64 bytes may be specified in the data field following the MAC source and destination addresses as filter criteria or network layer for IP filters.
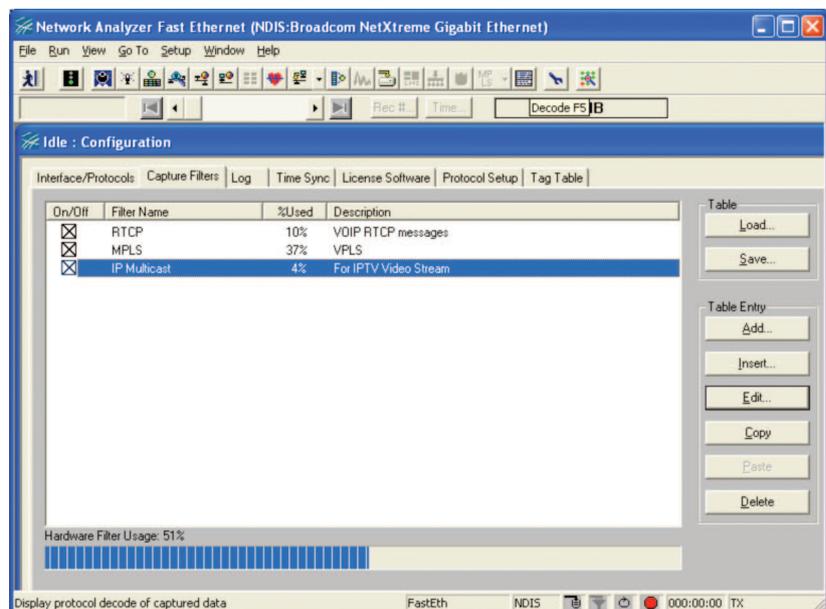
Figure 12. See only the data of interest with extensive filtering for voice, data and IPTV protocols

**Network Analyzer Software
Detailed Specifications**

TCP Connection Analyzer

Easily analyze TCP connections and quickly troubleshoot and identify TCP connection issues. With this measurement, you can examine TCP flow control, messaging, response times, window sizes, retransmissions, payload statistics, and other TCP characteristics. This is an off-line measurement performed on captured data.

The statistics shown for each TCP connection are:

- average acknowledgement response times
- total packets sent from a port (host)
- total bytes sent from a port (host)
- average bytes per packet sent from a port (host)
- bytes per second sent from a port (host)
- good bytes per second sent from a port (host). That is, the portion of the connection bandwidth sent from a port that is not associated with retransmitted packets.
- retransmitted bytes per second sent from a port (host). That is, the portion of the connection bandwidth associated with retransmitted packets.
- the number of retransmitted packets
- the number of retransmitted bytes
- graph of response time from source and destination
- graph of window size
- graph of retransmissions.

Figure 13. Use the TCP connection analyzer to quickly identify TCP connection issues

Multi-segment jitter, latency, and packet loss

Quickly identify degradation points across a network. Use the IP multi-segment jitter measurement to detect and report jitter, packet loss and latency across multiple Network Analyzer data capture files from a distinct communication path across a network. This measurement supports IP, ICMP, TCP, UDP and RTP networks. This is an off-line measurement performed on multiple capture files.

Measurements include:

- total jitter (min, max, and average) in each direction
- network jitter (min, max, and average) in each direction
- source jitter (min, max, and average) in each direction
- packet loss in each direction
- latency (min, max, and average) in each direction.
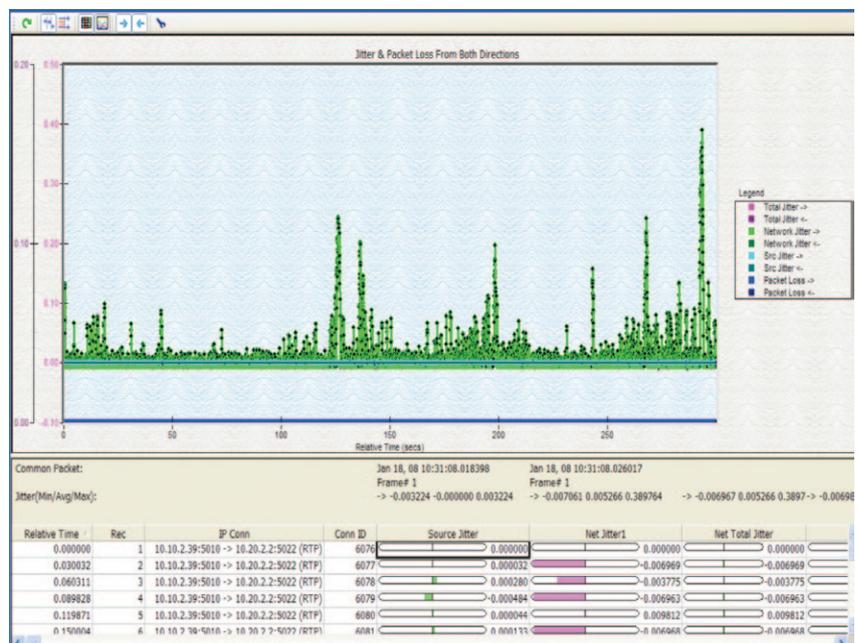
Figure 14. Identify IP multi-segment jitter, latency and packet loss

Run-time store to media

Do you need to collect and analyze traffic over extremely long periods or have an intermittent problem that is hard to capture? The DNA platform lets you collect and analyze data over long periods by utilizing unique data streaming capabilities. In run-time store to media (RTSM) mode, the instruments streams data in run-time through external ports for post analysis and troubleshooting.

The J6801B DNA, J6802B DNA MX and J6803B DNA PRO can stream to media up to 55 Mbps using the Control and Sync port. By utilizing a dedicated gigabit Ethernet port, the J6801B DNA and J6803B DNA PRO can stream up to 150 Mbps.

13

**Network Analyzer Software
Detailed Specifications**

Encapsulation discovery

Network Analyzer takes care of handling tunneled or encapsulated LAN traffic. Sophisticated algorithms discover the encapsulation used on the link under test and will configure the system for you. Simply type in the IP address or the application you want to filter on and the software will take care of the encapsulation that the network devices are using. You can also define a filter based on the discovered encapsulation. GRE and GTP tunneling is supported. All measurements and analysis are done at the highest IP level.

Protocol commentators

At the heart of Network Analyzer is a series of "commentators", which perform real-time protocol state-following analysis of frames to detect anomalous protocol events. These events are logged and linked to the corresponding captured frames, making it easy for you to scroll through the capture buffer to see the events that led up to an anomalous event and then drill down into the event itself. Commentators for many different protocol families, including IPv6 and VoIP, are included.

One of the most important capabilities of the protocol commentators is the ability to detect potential problems in the network, and provide a suggestion of what to do to solve the problem, in addition to an explanation of the actual problem and technology behind it. You do not have to be a network expert to detect, understand, and troubleshoot problematic networks.
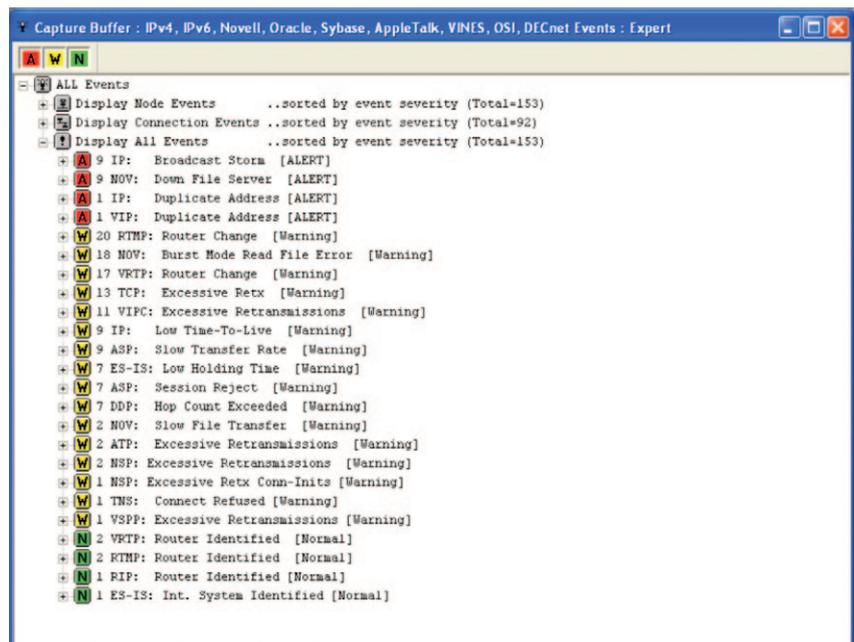
Figure 15. Commentators allow you to automatically detect problematic issues in the network and obtain possible solutions to the problems

14

Network Analyzer Software Detailed Specifications

Protocol statistics

To help understand variations of frame length and protocol usage over time, protocol and frame length statistics are gathered simultaneously for the network layer and the major protocol stacks. Network Analyzer displays these statistics in both tabular and pie chart format, showing percentage utilization or frame length distribution by protocol. Ethernet, Frame Relay, and reassembled ATM frame lengths are displayed in the following categories:

- < 64 bytes
- 64….127 bytes
- 128….255 bytes
- 256….511 bytes
- 512….1023 bytes
- 1024….1518 bytes
- > 1 518 bytes

The data is displayed in a tabular or graphical format and can be viewed by Hub/Node, DTE/DCE or LN/EQ activities depending on the link-layer technology used, to provide:

- % utilization
- total number of frames and bytes
- frames and bytes per second
- DLL (data link layer) errors
- errors per second
- average frame length.

The statistics can be logged to disk and may be exported in CSV format or JDSU Network Analyzer file format. This data can then be used to generate professional-quality reports with the J6848A Report Center software.
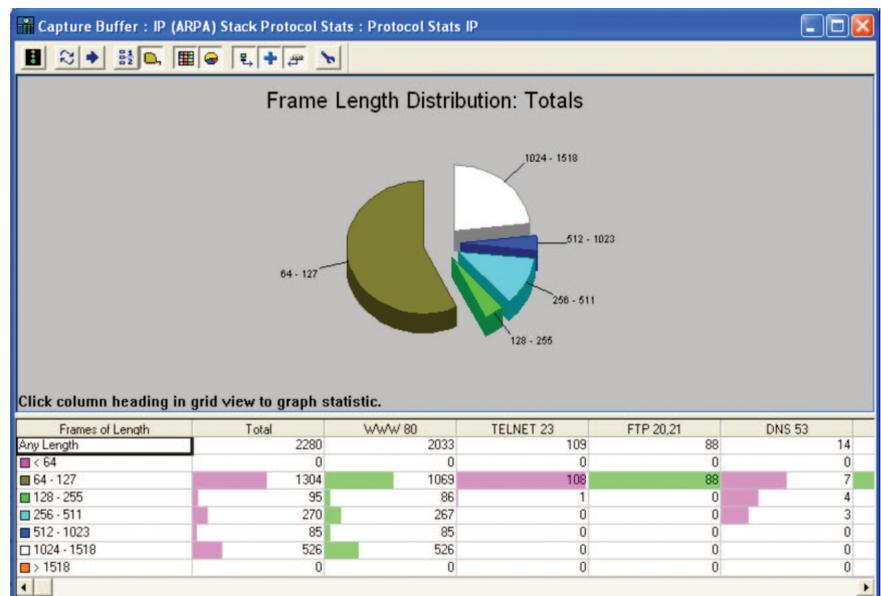
Figure 16. Frame Length by protocol is one of the multiple ways to view the information

Frames of Length	Total	WWW 80	TELNET 23	FTP 20,21	DNS 53
Any Length	2280	2033	109	88	14
< 64	0	0	0	0	0
64 - 127	1304	1069	108	88	7
128 - 255	95	86	1	0	4
256 - 511	270	267	0	0	3
512 - 1023	85	85	0	0	0
1024 - 1518	526	526	0	0	0
> 1518	0	0	0	0	0

Node discovery

Maintaining an up-to-date list of network nodes is key to managing many network problems as they occur. Network Analyzer provides an open node list that is automatically incremented as new discoveries are made by the node discovery algorithm. The node list shows MAC or bridged WAN addresses, network addresses and node names. Node Statistics reports use the station and server node names extensively, making node identification easier and faster. As a result, the Network Analyzer software provides useful clues to solving network problems.

Network Analyzer Software Detailed Specifications

Baselining

Network Analyzer lets you collect statistical information over long periods and export it to the J6848A Report Center software to generate management-level reports. Armed with these reports, you can easily identify network trends and plan for future network requirements. The two most important measurements for this feature are the Protocol Vitals and the Connection Statistics measurements.

Protocol Vitals

While the analyzer is decoding data, it is also gathering important information from the network. These network performance statistics can be accessed with just a click of the mouse button and may be viewed simultaneously with the decoded data. The Protocol Vitals measurement provides a statistical picture of the lower layers and the various protocol stacks to show cumulative data and trends over time. You can use these statistics to identify problems or assist in optimizing your network configuration.

Figure 17. Protocol Vitals allow you to examine traffic before and after applying filters

The Protocol Vitals measurement is one of the fundamental measurements in the system.

- It gives you a real view of the network, even if capture filters are active.
- The measurement collects a wealth of protocol-specific information on various protocols like ATM, Ethernet, Frame-Relay, IPv4, IPv6, Apple Talk, IPX, OSI etc., plus line status (WAN/ATM interfaces).
- You can select the information you want to graph without having to stop or restart this or any other measurement. This selection makes it easy to identify correlated data patterns like broadcast frames versus routing packets versus Frame-Relay frame-rate, etc.
- The measurement monitors thresholds that you can easily set dynamically to detect intermittently occurring events automatically and stop the capture process for further analysis, even if the system is running unattended.

The Protocol Vitals measurement graphs current and maximum utilization in real-time and provides current, average, peak and cumulative values in tabular format of the following parameters:

**Network Analyzer Software
Detailed Specifications**

Protocol Vitals (continued)

LAN	Pre-filter utilization (%)
	Post-filter utilization (%)
	Pre-filter frames
	Post-filter frames
	Pre-filter runts
	Post-filter runts (good FCS)
	Pre-filter local collisions
	Post-filter jabbers (good FCS)
	Pre-filter late collisions
	Post filter jabbers (bad FCS)
	Pre-filter remote collisions
	Post-filter dribbles
	Pre-filter remote late collisions
	Post-filter broadcast frames
	Pre-filter mis-aligned frames
	Post-filter multicast frames
	Pre-filter frames (bad FCS)
WAN (Frame Relay only)	Forward explicit congestion notification (FECN)
	Backward explicit congestion notification (BECN)
	Discard eligibility (DE)
ATM	Physical Layer Line Status (interface dependent)
	Utilization (%)
	Total idle/unassigned cells
	Total assigned cells received
	Total frames received (AAL-2 and AAL-5)
	Total cells indicating a single bit header (HEC) error
	Total cells indicating detected multi-bit header (HEC) errors
	Total cells indicating congestion experienced
	Total cells with CLP=1 (low priority)
	Total reassembled AAL-2 or AAL-5 frames with trailer CRC-32 errors
	Loss of cell delineation (LCD)
	Total bridged frames (LAN over ATM)
	Total bridged broadcast frames (LAN over ATM)
	Total bridged multicast frames (LAN over ATM)
	WAN (common to Frame Relay, HDLC/SDLC, sync PPP)
	Physical layer line status (interface dependent)
	Utilization (%)
	Total frames
	Total bridged frames (LAN over WAN)
	Total bridged broadcast frames (LAN over WAN)
	Total bridged multicast frames (LAN over WAN)
	Total octets
	Throughput (kbps)
	Aborted frames
	Short frames
	FCS errors

**Network Analyzer Software
Detailed Specifications**

Connection Statistics

Users report many network prob-
lems in terms such as, "I cannot
connect to a printer" or "the connec-
tion to the network is very slow." To
resolve these kinds of problems, you
need to view the activity on a partic-
ular station or specific connection.
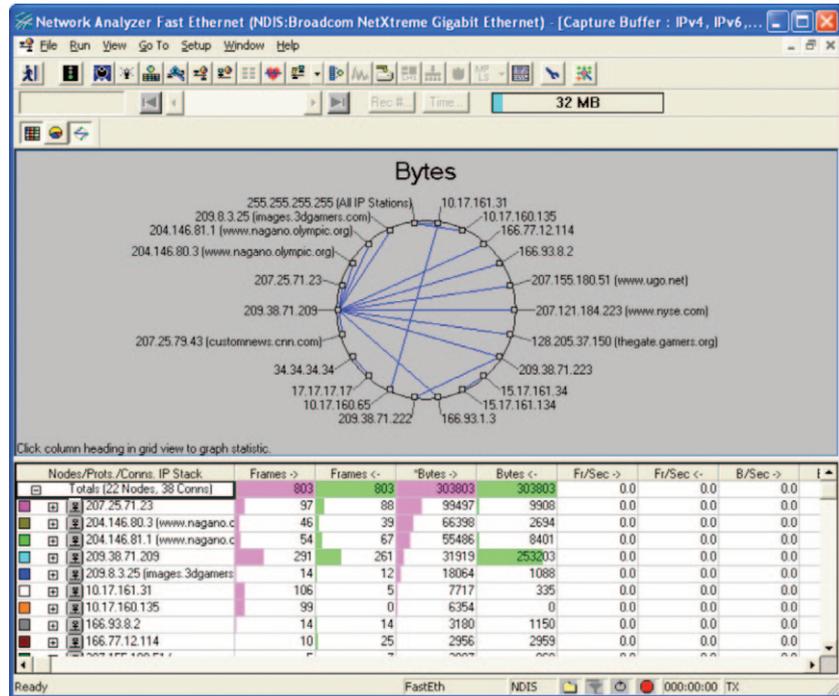
Figure 18. Obtain visibility of group of conversation by node, protocol, connection, etc.

To see who is using the bandwidth and how the bandwidth is used, Network Analyzer
provides numerous connection statistics. By simply clicking on a busy node, you will
see immediately to whom the node is talking most often and what protocol is used.

The display shows by column:

- total frames and bytes to or from a node
- frames or bytes per second to or from a node
- utilization to or from a node
- total retransmissions to or from a node
- retransmissions per second to or from a node
- low window to or from a node
- source or destination port.

You can even differentiate between data sent or received by a device by simply using
the Hub/Node, DTE/DCE or Ln/Eq buttons. Moreover, this measurement provides
even more data than it appears at first glance. You can easily customize the view of how
the information is displayed by using the right-mouse-click context menu and choos-
ing one of the pre-defined filters, views, or drill-down functions. If needed, you can
filter the data shown by the protocol decode with one click or get a comprehensive list
of all Alerts and Warnings generated by any node/station you select. IPv6 is fully sup-
ported by Connection Statistics.

18

**Network Analyzer Software
Detailed Specifications**

Protocol Decodes

Many problems can be solved with the Expert Analyzer without viewing the details of each frame. However, when needed, more than 500 protocol decodes are available to help interpret the protocols as they appear on the network. A detailed display shows the field-by-field protocol decode for every frame, while the summary display provides a single-line display of the key fields. A hexadecimal display provides the correlation with the detailed data display. For a complete list of decodes, please contact your JDSU Technologies representative.
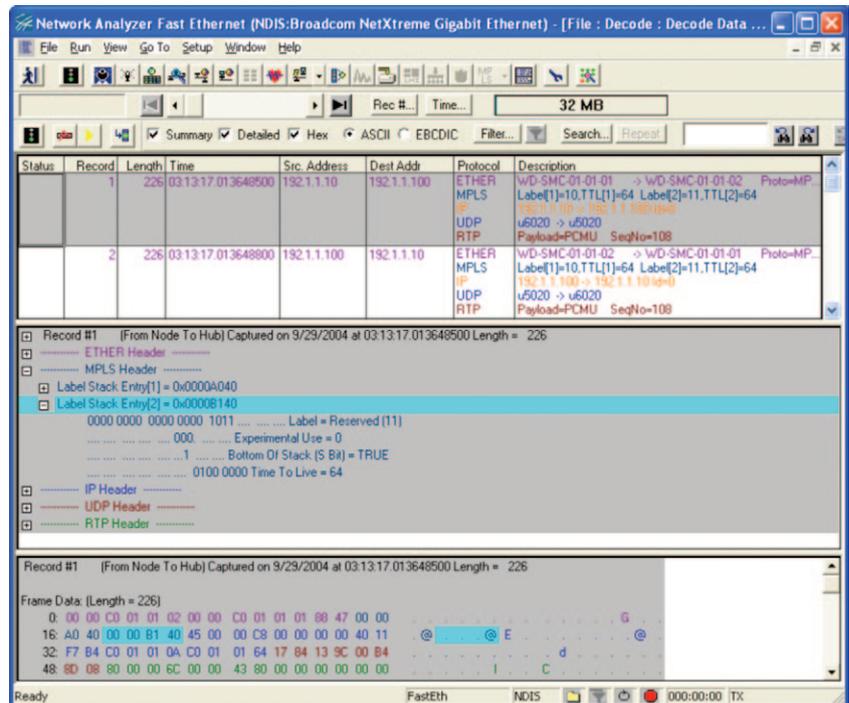
Figure 19. Visualize the packet data information in several ways: summary, detailed, or hex mode

Network Analyzer software provides 7-layer decodes of all major protocols, including SIP, IPTV, MPLS, IEEE 802.1p, 802.1Q and 802.3x. Protocol decodes have a built-in protocol follower that will flag errors as they occur.

**Network Analyzer Software
Detailed Specifications**

IPv6 protocol analysis

The Network Analyzer has extensive capabilities for IPv6 networks:

- Expert Analyzer and Commentators for IPv6 protocol families, including VoIP, help to quickly identify root causes of problems

- advanced measurements supporting IPv6 include Connection Statistics, Protocol Statistics, and Node Discovery

- extensive capture and display filters for IPv6 protocol families and station addresses, including IPv4 to IPv6 tunneling

- VoIPv6 measurements and diagnostics, including MOS values.

LMI Statistics and Commentator

The LMI Statistics measurement in the analyzers is used to track statistics on the LMI channel on a Frame Relay network. Every LMI frame is analyzed and the statistics are guaranteed to be 100% accurate. The Commentator feature lets the user know normal, warning and alert events, quickly and easily. Typical events are Sequence Number Errors, N391 Errors, T392 Errors, Invalid LMI Frames, and Link Down.

Figure 20. Varieties of normal, warning, and alert events are supported in the LMI Commentator

20

Network Analyzer Software Detailed Specifications

ATM VPI.VCI statistics and Frame Relay DLCI statistics

When ATM or Frame Relay interfaces are in use, the Network Analyzer automatically collects statistics on each of up to 1024 virtual channels. Statistics are collected in real-time before hardware filtering takes place. Statistics are collected per port and per virtual channel (except where inappropriate). This measurement can be run from data already captured but in this case, of course, any hardware capture filters will affect what statistics are gathered.
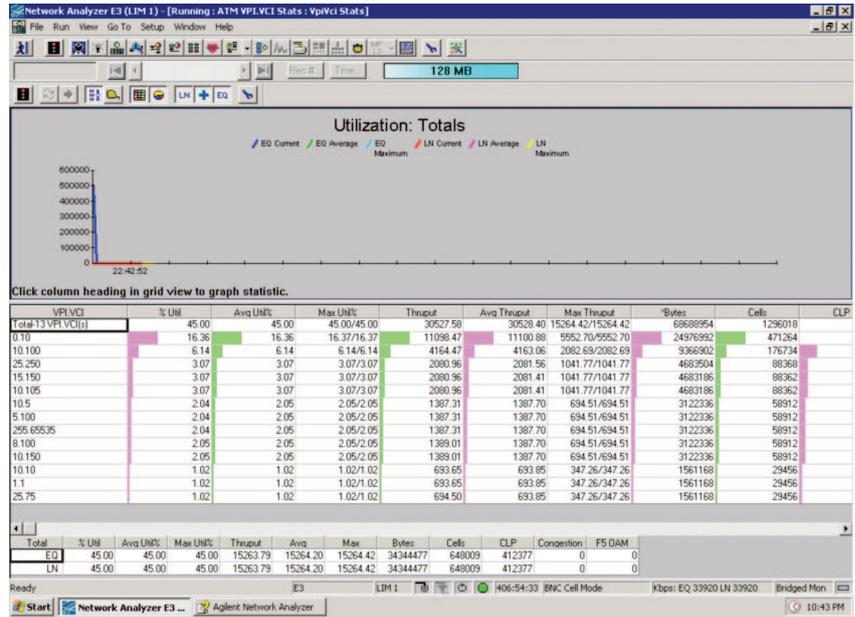
Figure 21. ATM VPI.VCI statistics identify network performance issues at a glance

ATM Statistics (cell mode), per VC and per port, unless otherwise stated	Total Cells – The total cells since the start of the run or last reset
	Total HEC – The total cells with header errors (per port only)
	Total Cell Loss Priority – The total cells with CLP set since the start of the run or last reset
	Total Congestion – The total cells with Congestion set since the start of the run or last reset
	Total F5 OAM Cells – The total F5 OAM cells since the start of the run or last reset
ATM Statistics (frame mode), per VC and per port, unless otherwise stated	AAL indication – Indicates 2 (AAL-2), 5 (AAL-5) or 0 (other/unknown) per VC
	Total HEC – Total cells with header errors (per port only)
	Total F5 OAM Cells – Total F5 OAM cells since the start of the run or last reset
	Total Frames – Total reassembled PDUs since the start of the run or last reset
	Total CRC Errors – Total AAL-5 PDUs with CRC errors since the start of the run or last reset
	Total Cell Loss Priority – Total AAL-5 PDUs with CLP set in at least one cell in the PDU since the start of the run or last reset
	Total Congestion – Total AAL-5 PDUs with Congestion set in at least one cell in the PDU
Frame Relay statistics, per VC and per port	Total Frames – Total frames since the start of the run or last reset
	Total Discard Eligible – Total frames with DE set since the start of the run or last reset
	Total Forward Explicit Congestion Notification – Total frames with FECN set since the start of the run or last reset
	Total Backward Explicit Congestion Notification – Total frames with BECN set since the start of the run or last reset

**Network Analyzer Software
Detailed Specifications**

ATM policing

The policing measurement operates in real-time with all ATM-capable LIMs up to 622 Mbps, including IMA and ATM channelized sub-rates of the J6810B SDH/SONET LIM. In all cases, policing is performed on up to 1024 virtual circuits simultaneously. Virtual circuits are auto discovered and the measurement is performed in hardware prior to hardware-based AAL-2/AAL-5 reassembly, so it works in cell mode or frame mode. It can be used simultaneously in real-time with other measurements such as the VPI.VCI statistics and, in frame mode, with higher layer analysis. The measurement can also be used to post-process data from the capture buffer or from file (cell mode only).

The following traffic service configurations are supported:

CBR.1/DBR/UBR.1	GCRA (1/PCR0+1, CDVT0+1), no tagging
VBR.1/SBR1	GCRA (1/PCR0+1, CDVT0+1)
	GCRA (1/SCR0+1, BT0), no tagging
VBR.2/SBR2	GCRA (1/PCR0+1, CDVT0+1)
	GCRA (1/SCR0, BT0), no tagging
VBR.3/SBR3	GCRA (1/PCR0+1, CDVT0+1)
	GCRA (1/SCR0, BT0), tagging

ATM VPI.VCI provides results in a table format. Configuration of the traffic contract parameters can be performed globally, in ranges of VPI.VCI or individually per VPI.VCI. The configuration can be saved and restored from file.
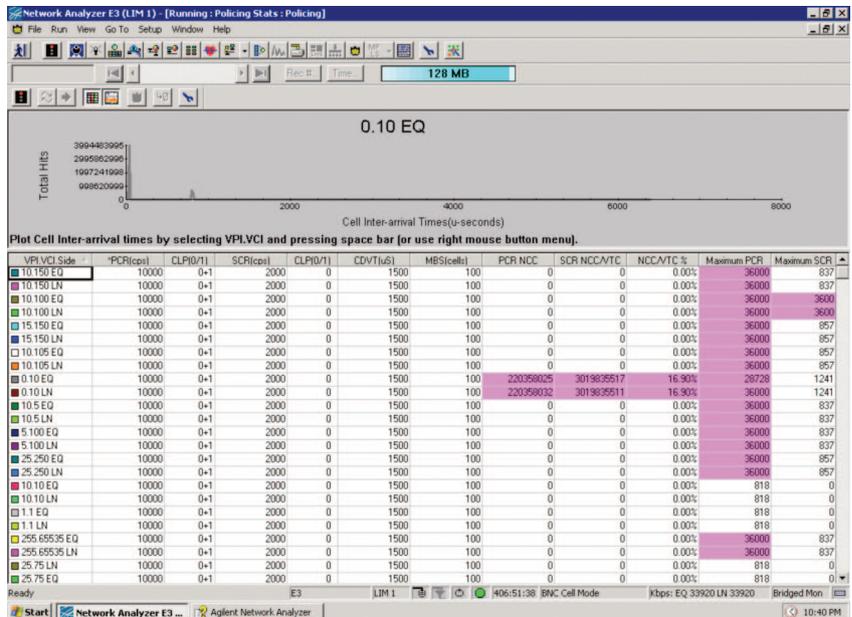
Figure 22. ATM policing verifies service level agreement contracts

**Network Analyzer Software
Detailed Specifications**

ATM Usage Expert

The network has traffic contracts set up to protect it from excessive traffic and the danger of congestion. However, how close is your traffic to the contract limits? This useful measurement is able to derive suitable traffic contracts for actual constant/deterministic bit rate (CBR/DBR) and variable/statistical bit rate (VBR/SBR) traffic by post-processing data from the capture buffer. The estimated traffic contracts can be subsequently applied to live real-time policing analysis on the same virtual circuit in cell mode or frame mode to confirm that this is a suitable traffic contract over the longer term.

1-Point CDV graphing

A side effect of the policing measurement is the ability to graph 1-point cell delay variation (that is, CDV observed at a single point). The graph is derived from the data collected per virtual channel of cell inter-arrival times. For each virtual channel, the measurement keeps multiple bins of accumulated counts of inter-arrival times that occur within the ranges covered by these bins. The graph can be plotted as a distribution of hits against inter-arrival times or hits against cells/second. As a non-intrusive passive measurement on live traffic, this is particularly useful for observing the behavior of CBR/DBR traffic where CDV can impact the quality of service of the emulated circuit being carried in the virtual channel. This measurement is performed simultaneously with other policing measurements and a graph of any policed virtual circuit can be displayed at any time.

**Network Analyzer Software
Detailed Specifications**

Active tests: traffic generation and packet editing

Built into the Network Analyzer software is a powerful traffic generator to add advanced traffic generation and intelligent packet or capture file-editing capabilities. Ideal for installation testing and for manufacturing test and support organizations, it provides the tools you need to thoroughly test, simulate and troubleshoot a network device or problem. Network Analyzer provides intelligent packet and capture buffer file editing for full 7-layer customization of data to be transmitted. While you specify frame rate, burst count, or percent utilization, the software automatically calculates inter-packet gaps for various traffic loads, calculates the checksum and generates a CRC.

You can quickly configure Network Analyzer to generate a single packet such as an ARP or PING to troubleshoot a production network and verify connectivity or to generate a series of packets to saturate a test network and test new equipment and configurations before network deployment.

The multitasking capabilities of Network Analyzer let you monitor the network while the traffic is generated including:

- perform active stimulus/response tests to troubleshoot a production network
- test new equipment or configurations before deploying them in the network
- generate higher layer traffic over any Ethernet interface up to 10 G or any ATM interface (except IMA and ATM25) up to 622 Mbps – AAL-5 segmentation is performed automatically. ATM cell mode generation is also available.

For ATM, the user is allowed to create either a set of cells, or a set of frames for transmission onto a network.

For each frame or cell in a transmit set, users have the option to:

- start with pre-defined templates (IP frames or cells), or
- start with frames or cells previously captured on ATM networks, or
- create their own frames or cells.

In ATM cell mode, templates are available for the creation of AAL-5 cell sequences and F4 and F5 ATM layer OAM cells. If the VPI.VCI is 0.0, templates for F1 and F3 physical layer OAM cells or IMA ICP/filler cells are available.

In ATM frame mode, the traffic generator frame builder allows AAL-5 frames and ATM cells to be built. If cells are selected, the choice is the same as for cell mode above but if frame mode is selected, the frame will be encapsulated (RFC2684/RFC1483-routed) and AAL-5 segmented appropriately.

ICMP Echo (Ping)

This active measurement is currently available for LAN and ATM. LAN Ping operates via any of the 10/100/1000 and 10 GE interfaces and ATM Ping operates via any of the ATM interfaces except IMA.

The user can specify the source and destination IP addresses, the number of ICMP data bytes, the time-out period, and in the case of ATM, the VPI.VCI value and encapsulation method.

Measurement logging

Measurement logging is available to store test results in a disk file. You can select logging for all the open measurements from a common dialog box. Data may be logged in one of two formats, CSV and Network Analyzer *.dat. All data are stored into files that can easily be opened by the J6848A Report Center software or the Network Analyzer application.

J6844A Telephony Network Analyzer

The Telephony Network Analyzer simplifies and expedites the resolution of quality and signaling problems in IP telephony networks. It provides simple and precise diagnostics of VoIP QoS through non-intrusive measurements, including the voice quality measurement known as mean opinion scores (MOS). It also provides simplified troubleshooting of call signaling and control through embedded expert analysis of VoIP protocols. The Telephony Network Analyzer supports testing over LAN and WAN networks as part of the JDSU Network Analysis and Troubleshooting solutions.

This powerful tool offers advanced VoIP signaling and service quality troubleshooting capabilities including:

- non-intrusive voice quality measurements using breakthrough predictive MOS technology for passive voice clarity MOS scoring
- VoIP analysis on MPLS and IPv6 networks
- simple analysis that exposes the impairments to voice quality
- RTCP and RTP voice session sorting and prioritization for easy drill-down to problem areas
- H.323, MGCP and SIP commentators with CDR completion statistics
- precise measurements of IP network performance for VoIP services
- diagnostics for troubleshooting and identifying problems at the root cause.
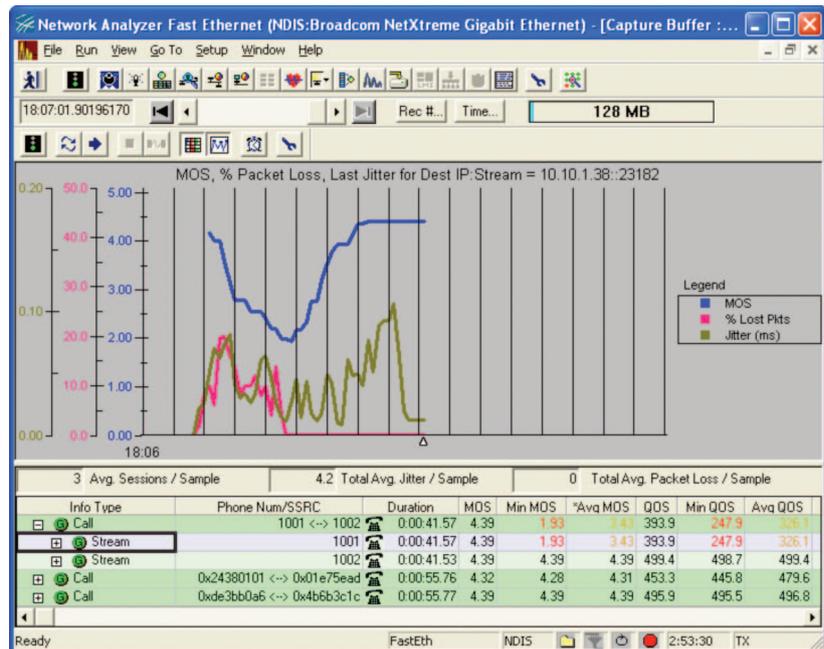
Figure 3. Telephony Network Analyzer provides MOS and network impairments over time that affect the quality of service

Network Analyzer Solution Components

Add-on Licenses (continued)

J6848A Report Center

The JDSU Report Center helps network professionals to visualize, analyze, document, and present vast arrays of network data with ease and flexibility. Report Center merges network data collected with the JDSU Network Analyzer into a common database for further analysis. The use of this high quality, high-resolution data is unique to Report Center, and results in a level of network analysis previously unattainable with conventional tools.
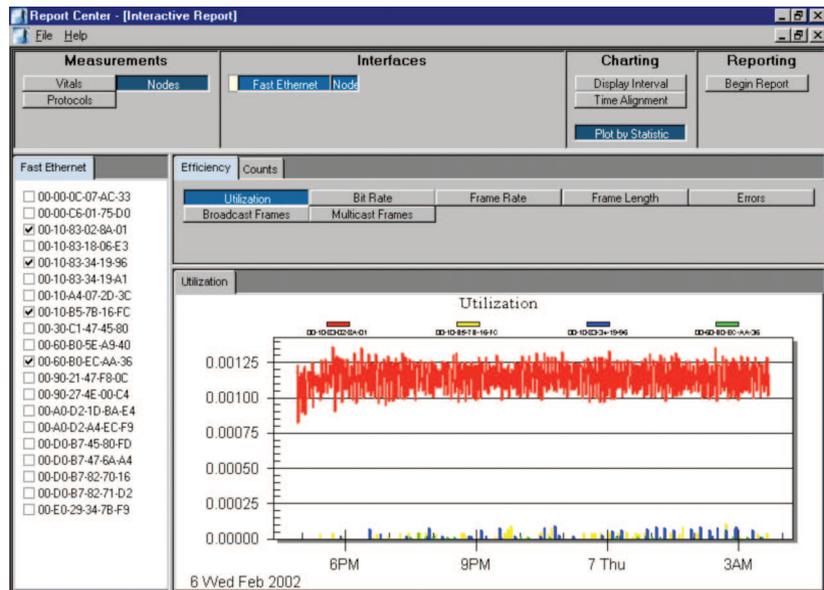
Figure 4. Report Center: automate reports for network characterization, troubleshooting and reporting

J6825A Inverse Multiplexing for ATM (IMA) and Multi-Link WAN Technologies

The J6825A license for the J6824A Eight-port E1/T1 LIM enables software for Inverse Multiplexing for ATM (IMA), multi-link Frame Relay, multi-link PPP and multi-link HDLC on the Network Analyzer's eight-port E1/T1 LIM.

Re-aggregated IMA traffic is analyzed in the same way as other ATM LIMs, with cell mode and frame mode (AAL-2/AAL-5 reassembly) available, plus other ATM analysis features.

J6835A Network Analyzer NDIS server

J6835A Network Analyzer NDIS server is a software agent process that is able to connect to a NDIS-based NIC and capture data in promiscuous mode, performing various analysis tasks. Measurements on 10/100/1000 Mbps or 10 GE, Token Ring or FDDI NICs are supported. This server is accessed from the Network Analyzer software client and does not contain an analysis GUI.

J6765A RFC2544 Gigabit and 10/100 Ethernet benchmarking

The RFC2544 Gigabit and 10/100 Ethernet benchmarking software license enables active performance benchmarking for Gigabit and 10/100 Ethernet devices and LANs. Measurements include throughput, latency, frame loss, and back-to-back frames without loss, all for varying frame sizes per IETF RFC2544.

This RFC2544 measurement enables fast and efficient benchmarking of network devices to certify and troubleshoot network installations. Testing is enabled using the J6830A 10/100 BaseTX, J6831A 10/100 Base FX, and J6832A Gigabit Ethernet LIMs.

Network Analyzer Solution Components

Add-on Licenses (continued)

J6766A MPLS analysis

Network Analyzer captures and decodes MPLS signaling and data protocols in real-time and at full-line rate. The analyzer can diagnose and decode MPLS accordingly with RFC2547bis among other MPLS standards.

Network Analyzer can filter single or up to six MPLS stack labels. Network Analyzer creates a table of Label Switched Paths (LSPs) present in the network and measures the vital statistics of the VPN in real time. It also quickly creates a graphical visualization. VoIP over MPLS performance is analyzed on the filtered traffic to indicate performance and trouble spots for a specific label-switch path or VPN.

The J6766A MPLS Analysis software keeps track of the different class priorities in an MPLS network specified by the experimental and QoS bits. In addition, the measurement analyzes the MPLS payload and detects the DiffServ priorities of the IP packet transported by an MPLS frame.

Key MPLS measurements include:

- MPLS CoS analysis
- DiffServ analysis
- routing and MPLS decodes
- MPLS protocol filtering
- LSP statistics
- VoIP performance on VPNs.
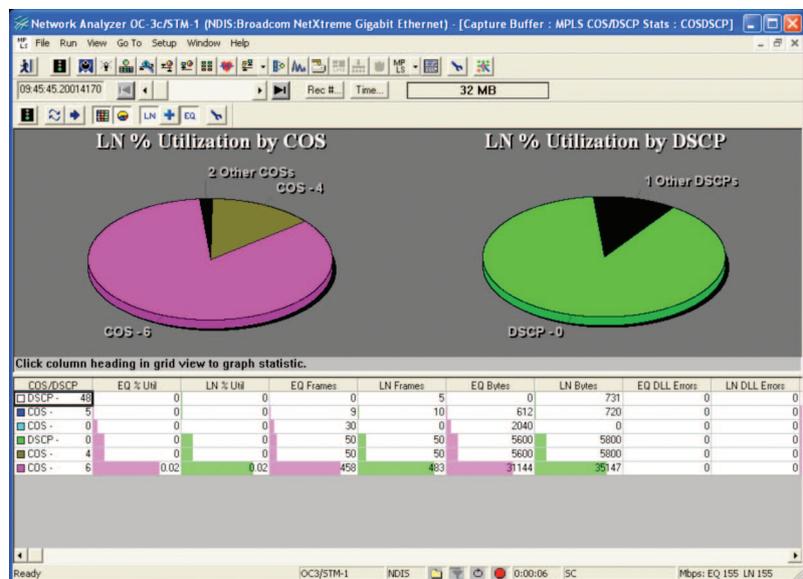
Figure 5. Easy to view traffic levels by MPLS Class of Service and IP DSCP

J5425A Switch Advisor

The Switch Advisor provides the capability to trend switch port utilization and other vital statistics. It allows the user to monitor a suspect WAN link and any other management information base (MIB) supported device simultaneously to correlate problems between the two. The user can discover switches and other MIB-supported devices via user-directed search or can directly enter the device management IP address and graphically view current port utilization levels. The Switch Advisor sends SNMP messages over an Ethernet connection and gathers MIB data including utilization, packet information, and errors.

27

Network Analyzer Solution Components

Data Acquisition Platforms

JDSU® PacketPortal™

E N A B L E D

PacketPortal

PacketPortal is a distributed packet acquisition and selective packet forwarding system that can capture traffic from points in a network and forward it to a TPA and other Ethernet-based applications for analysis. Enhanced SFP optical transceivers called SFProbes give PacketPortal enhanced network visibility normally reserved for taps or span ports which are directly connected to monitored devices.

PacketPortal lets you collect data throughout the entire network, from the edge to the core, by leveraging existing SFP ports and network cabling to inspect, filter, and forward traffic. PacketPortal reduces the need for separate network monitoring infrastructure by taking advantage of the network capacity already in place. PacketPortal provides access to network, service, and application data in near realtime.

The PacketPortal system consists of the following major components:

- SFProbe — installed in network switch and router ports in place of normal SFPs. SFProbes capture traffic based on filters and forward it across the network to PREs.
- Packet routing engine (PRE) — aggregates captured traffic from SFProbes and distributes it to analysis applications.
- System manager (SM) — provides a graphical user interface for command and control of SFProbes and PREs.
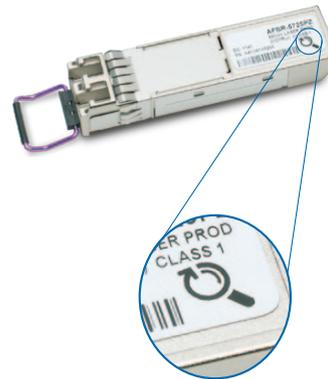
The JDSU SFProbe PacketPortal-enabled logo

Network Analyzer Solution Components

Data Acquisition Platform (continued)

For detailed information on the DNA Hardware Platform, please consult the JDSU Distributed Network Analyzer Data Sheet (P/N 5988-4176EN).

J6801B DNA

The J6801B DNA achieves its small form factor by excluding an integrated PC. You can control a DNA locally or remotely from a separate PC. One or more DNAs can be added to create multi-port systems. Like the DNA MX and DNA PRO, the DNA includes an acquisition system and accommodates line interface modules. Under this configuration, the J6840A Network Analyzer runs on a PC and connects to a DNA to acquire data from the network under test.

Figure 6.

J6802B DNA MX

The J6802B Distributed Network Analyzer MX is a transportable and rackmountable protocol acquisition and analysis solution. When deployed into the network under test, use DNA MXs to perform distributed measurements at different points in your network. An embedded version of the J6840A Network Analyzer runs in the integrated PC of the J6802B. In addition, remote Network Analyzer software can access and control the DNA MX via Instrument Manager.

Figure 7.

Network Analyzer Solution Components

Data Acquisition Platform (continued)

J6803B DNA PRO

The J6803B DNA PRO offers the most advanced feature set in the DNA portfolio. You can control the analyzer from a PC, locally or remotely. The analyzer hosts the J6840A Network Analyzer for full protocol analysis and network testing. It supports Run-Time Store to Media (RTSM) up to 150 Mbps. Like the DNA MX, Network Analyzer is accessed using a remote session. The hardware includes a built-in controller and a removable hard disk drive. The use model of the DNA PRO is as a portable analyzer for local or remote troubleshooting.

Figure 8.

J6872A 10 Gigabit/Gigabit Ethernet Blade Interface

The J6872A 10 Gigabit/Gigabit Ethernet Blade Interface provides advanced packet capture and processing for high speed Ethernet networks. This full-length, full-height PCI Express[*] interface card provides full 10 G capture, extensive filtering, and network key performance indicators to solve more network problems quickly. Install it in a PC or Server for full 10 GE per second Ethernet analysis.

Figure 9.

Network Analyzer Solution Components

Access and Management of DNAs

Secure Web browser control

The DNA PRO and DNA MX can be controlled using a Windows® web browser from a standard PC. There is no need to have any Network Analyzer software installed on the client PC. Additionally, if the wireless option for the DNA PRO is present, this platform can be controlled from a WiFi-capable laptop, notebook or PDA (personal digital assistant).

Network Analyzer Instrument Manager

Network Analyzer Instrument Manager is a software application that is used to control several remote J6803A DNA PRO or J6802B DNA MX platforms, with or without attached J6801B DNAs. These DNAs are seen as extra interfaces on the DNA PRO or DNA MX platforms.

Instrument Manager lets you:

- discover all DNA PRO or DNA MX on a local subnet and discover any attached DNAs
- add a DNA PRO or DNA MX from discovered list (instruments beyond the local subnet must be added by IP address)
- allow a remote session to the desktop using remote desktop protocol (RDP)
- update software on multiple DNA PROs and/or DNA MXs simultaneously
- display instrument status – up (reachable)/down (not reachable)/locked (to a user)
- configure DNA PROs and DNA MXs (assigning hostnames, changing OS passwords, etc.)
- configure DNAs
- get DNA status information such as LIM type and whether the DNA is in use.

Figure 10. Access and manage your DNAs remotely using Instrument Manager

Network Analyzer Solution Components

Network Analyzer Utilities

File Translator

File Translator is an included utility that converts LAN, WAN, and ATM packet trace files between different brands of protocol analyzers, including PCAP files.

Example uses for File Translator include:

- use the Expert system on files from other analyzers
- share trace files with other analyzer users or tech support
- convert trace files for training purposes
- reduce a trace file size by converting to the same format using the "frame slicing" option

Time sync Data File Merge utility

Network Analyzer includes a time-synchronized Data File Merge utility to enable multi-port analysis for up to 10 ports. This utility can merge up to 10 data files collected on different ports of the same technology (for example, 10 Ethernet ports or 10 STM- 4/OC-12 ports) into one data file.

This combination of data sources provides visibility into traffic collected at different points in the network in one aggregated and time-synchronized view. With the Data File Merge utility, searching for a problem on a widely distributed network becomes a quick and easy task.

NORTH AMERICA	LATIN AMERICA	ASIA PACIFIC	EMEA	WEBSITE: www.jdsu.com/test
TEL: 1 866 228 3762	TEL: +1 954 688 5660	TEL: +852 2892 0990	TEL: +49 7121 86 2222	
FAX: +1 301 353 9216	FAX: +1 954 345 4668	FAX: +852 2892 0770	FAX: +49 7121 86 1222	