Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 80 (2002)

Heft: 3

Artikel: Testing the new networking paradigm

Autor: Coleman, Murray / Marti, Walter

DOI: https://doi.org/10.5169/seals-877188

Network Quality of Service Testing

Testing the new Networking Paradigm

The MD1230A Data Quality Analyser, Anritsu's answer to the need for testing network traffic engineering, the benchmarking of devices and virtual circuits, the establishment and verification of "Quality of Service" requirements and the maintenance of "Service Level Agreements".

MURRAY COLEMAN AND WALTER MARTI

Increasing corporate use of IP applications is placing new and greater demands on networks for service guarantees in both reliability and service quality. When your business depends on communication, you cannot afford a communications service that fails to deliver. The data networks of today simply do not currently offer any guarantees that service-level requirements can be met without some degradation at any time, day or night, irrespective of other users of the network.

There is a Change

IP networks are no longer the province of governments and research institutes, they are increasingly becoming a medium of choice for business communication. This type of use requires a new paradigm to support service-level agreements that guarantee a specified level of throughput and network reliability, irrespective of the usage level and individual network element failures. The methodology of "best effort" delivery network operations is no longer acceptable. There is a range of applications that operates across data networks, many of which do not have any strict service-level requirements, but are mission critical to Corporate Business Operations. Along with the growing importance of these data services, there is also a change in the types of applications that are available. The traditional range of non-real-time applications (e.g., e-mail and ftp) is being extended to include real-time interactive applications such as voice and video services.

A Testing Solution for Network

The Anritsu MD1230A Data Quality Analyser (fig. 1) is a comprehensive and complete testing solution for network quality of service levels. Its main strength lies in its ability to combine performance testing and network monitoring in the same unit, sharing the same interfaces. It accomplishes this test regime by being able to carry out a number of important tasks:

The unit possesses an Automatic Testing Programme that conforms to the RFC2544 benchmarking standards. This routine allows the determining of these network parameters:

- Throughput: The maximum traffic loading of a network before frames are lost.
- Latency: The time delay across the network.
- Frame Loss Rate: The frame loss characteristics of a network beyond the throughput threshold.
- Back-to-Back Frames: The capability of a network to handle bulk data transfer (i.e. a message with many fragments) Without losing frames and causing constant loop conditions.
- System Recovery: The capability of a system to recover from an overload condition caused by inputting 110% of the throughput threshold.
- System reset: The time it takes for the network to recover from hardware and software resets, as well as power outages.

These tests are carried out using a range of frame sizes from 64 byte to 1518 byte, or can be configured individually by the user. The duration of the test and the amount of repetitions can also be user configured for increased system stressing. The results are available in a printed format that shows the test configuration, a table of outputs and a graphical representation where appropriate (fig. 2). Currently the tests conform to the RFC 2544 requirement of using two independent ports to complete the test requiring two units to be used, one at each access point to the network. In a drive to make testing more efficient and easier to carry out, it is planned to upgrade the current

Fig. 1. Anritsu MD1230A Data Quality Analyser.

software early this year to allow single port bi-directional testing of a network. This will considerably simplify the testing process and benchmarking of system parameters. All MD1230A units are fully supported for software upgrades as part of the purchase contract.

Get a very clear Picture

This type of system benchmarking allows a network operator to have a very clear picture of his network's capabilities and limits, before starting to load client traffic and allocated quality of service levels as part of the "Service Level Agreement" process (fig. 3). If this testing regime does not produce the detail required then the MD1230A allows the network to be tested using customised data streams constructed by the user himself. Each testing port has the following capabilities:

– The constructing of up to 256 independent data streams.
– The distribution of each stream can be set to be continuous, continuous burst, or stand-alone configuration and the following parameters can be user configured:
  - Inter Stream Gap
  - Inter Frame Gap
  - Inter Burst Gap
  - Number of Frames per Stream
  - Number of Bursts per Frame

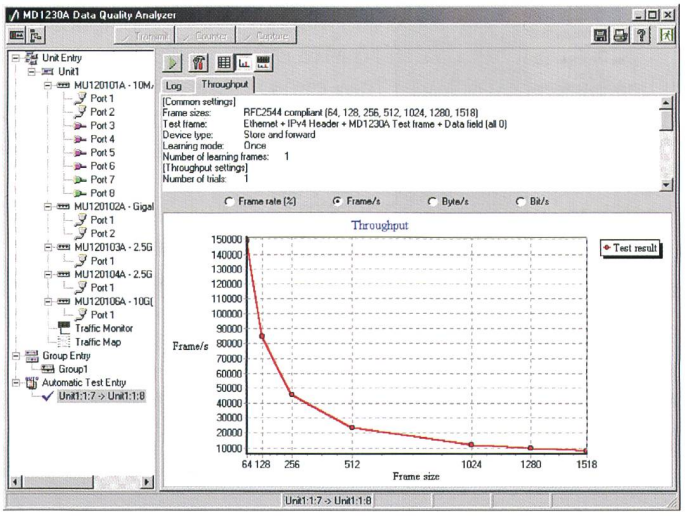
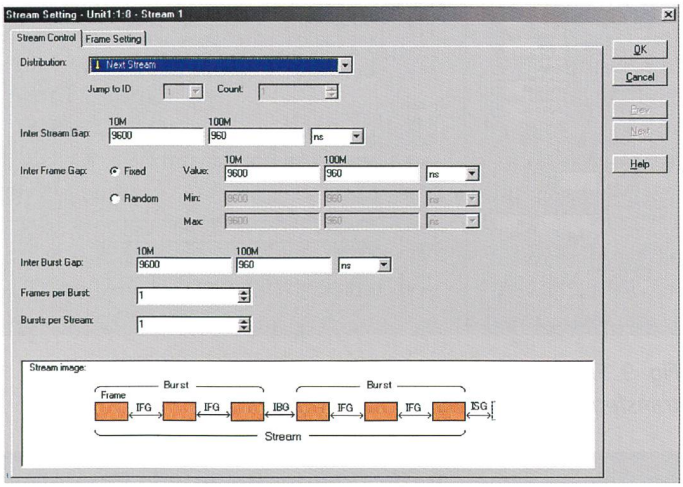


Fig. 2. The results are available in a printed format that shows the test configuration, a table of outputs and a graphical representation where appropriate.



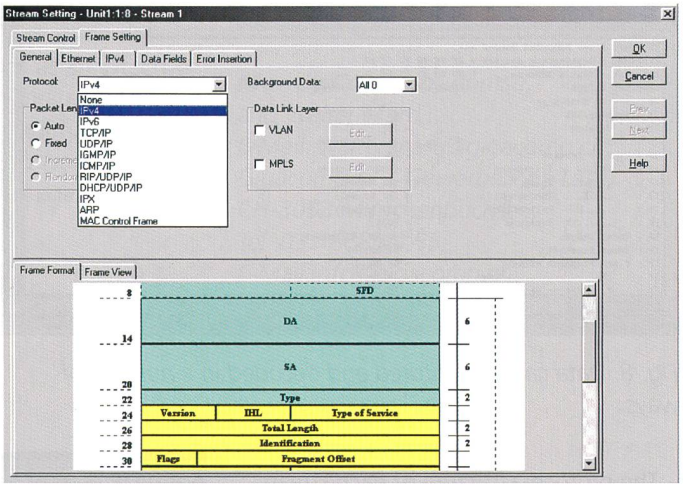


Fig. 3a and b. This type of system benchmarking allows a network operator to have a very clear picture of his network's capabilities and limits.

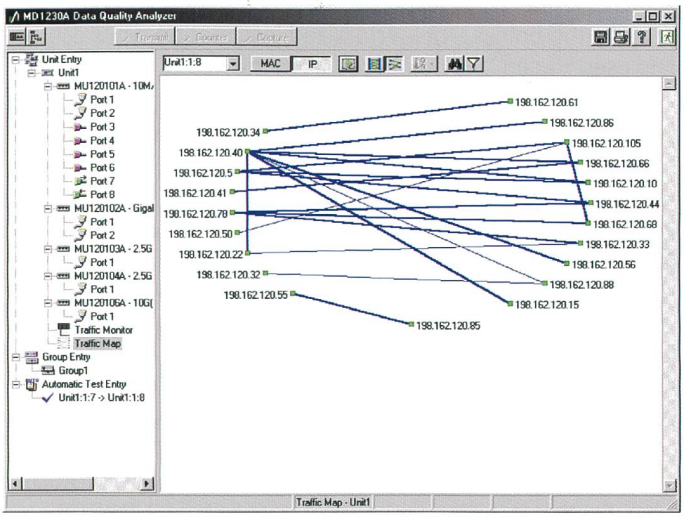


Fig. 4. Traffic mapping.

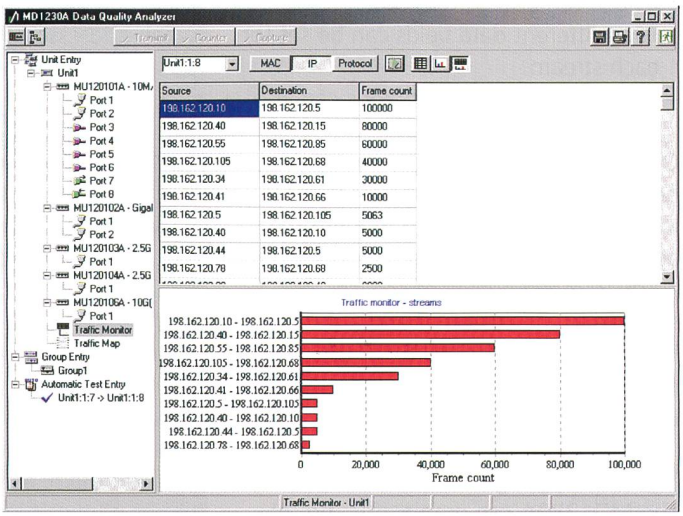


Fig. 5. Traffic monitoring.

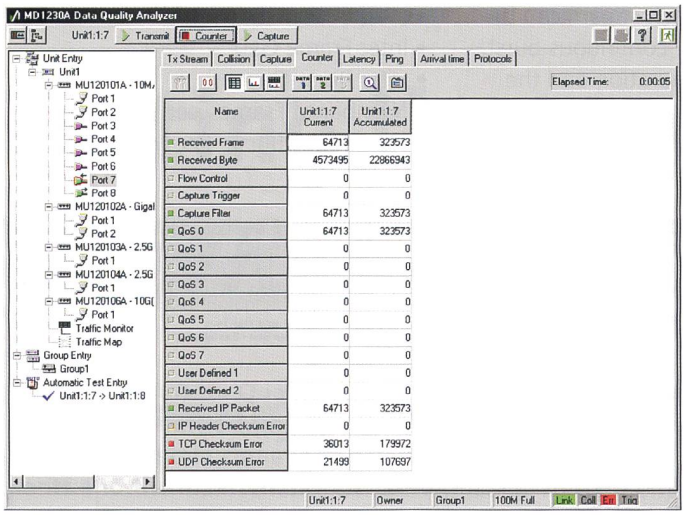


Fig. 6. Traffic counter feature.

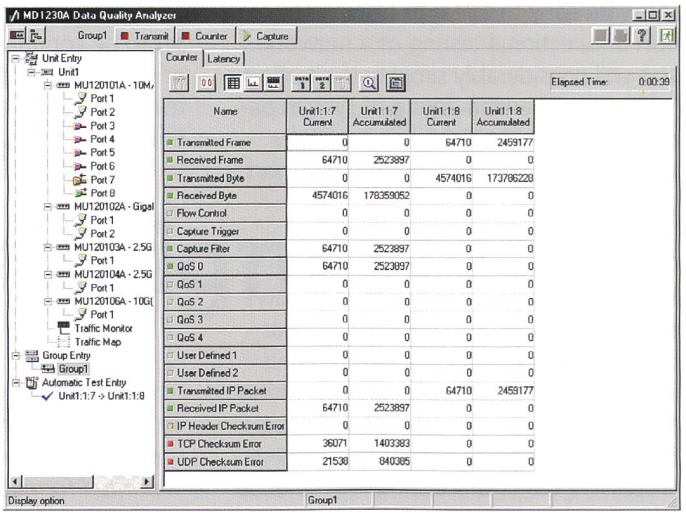


Fig. 7. The traffic counter feature has the ability to run a real-time graph function plotting two counters against an error condition.

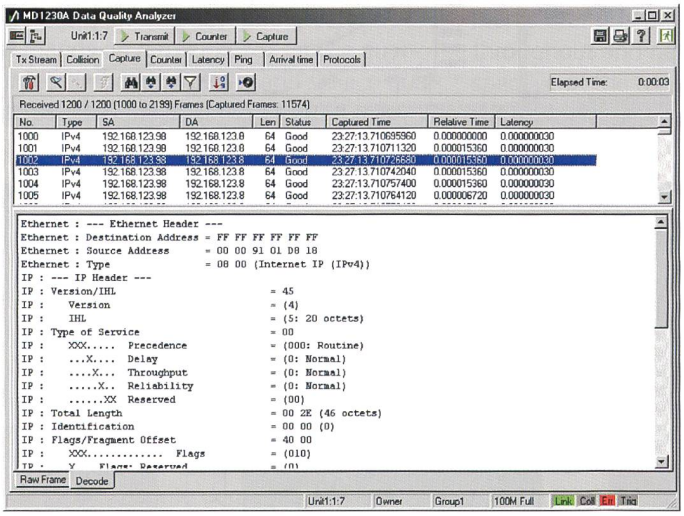


Fig. 8. Data can be captured and decoded in a number of ways.

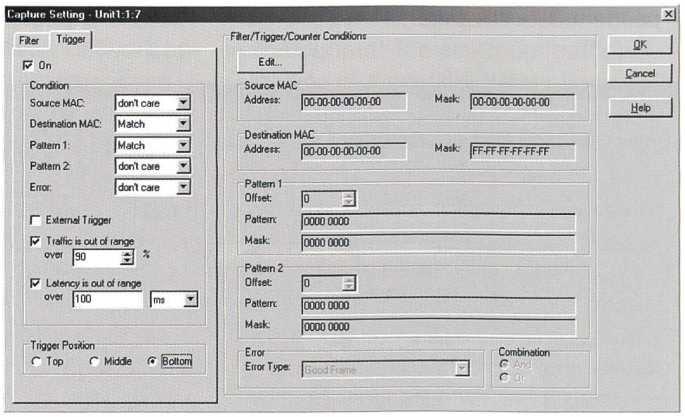


Fig. 9. Frames captured on a port can be quickly and easily transferred to the transmit side of any port.

– The protocol structure of each stream can be user configured to allow a wide range of layer 2, 3 and 4 protocols to be inserted into the frames. The frame length can also be user set.
– Four different data fields can be set for each stream.
– A number of error conditions can also be inserted.

Once a "Service Level Agreement" has been delivered to the end user the MD1230A can be used to monitor this agreement. This can be done both from a "guaranteed quality of service" perspective to the customer and a traffic level monitoring capability for the provider. The unit uses a number of features to monitor network traffic.

Traffic Mapping

The MD1230A can map traffic (fig. 4) on any of it ports and it can carry this out by IP or MAC address. This is a high-level tool that allows the network operator to see at a glance both easily and quickly the usage of his systems. This tool can highlight traffic increases between addresses by increasing the boldness and depth of the line used to connect them.

Traffic Monitoring

This feature takes the monitoring of the network into more detail and allows the system to be analysed by MAC or IP address, or by the type of protocol being used. This last instance will give an indication of the amount of control traffic present on the network. This feature gives a tabular and graphical display of the address pairs and the frame count between them, as well as the amount of frames of each type of protocol that is present (fig. 5).

Traffic Counter (to include Picture)

The traffic counter feature, which is present on every port, allows the network to be monitored in great detail and in real-time. A large number of characteristics, errors and information types can be monitored from this screen (fig. 6). Examples of these are:

– Received Frames
– Received Bytes
– Fragments
– FCS errors
– QoS Levels (both ToS and VLAN Tag)
– Received IP Frames
– IP Header Checksum Errors
– Transmitted Frames

Very important is the ability to set up to two user-defined counters per port (implemented in hardware). This gives full flexibility to monitor addresses, protocol types, error frames or even UDP/TCP port numbers (type of traffic) on the received

traffic flow. This can be used to monitor the amount of VoIP traffic on a network. This screen can also monitor the status of any capture filters or triggers that have been set over a prolonged testing period.
The traffic counter feature allows instantaneous real-time monitoring of both traffic levels, traffic types and quality of service indicators that will allow a network operator or a network user to ensure that service availability is both maintained and not exceeded. It will also give an early indication of any network problems by being able to monitor and report a wide range of fault conditions. It also has the ability to run a real-time graph function plotting two counters against an error condition. Additionally, the feature has the ability to group together separate testing ports across interfaces and test units (by remote operation). This gives the ability to monitor traffic as it flows across the network, pinpointing any trouble points quickly and easily (fig. 7).

Traffic Capture
The MD1230A has the capability to capture and decode any frames of interest on the network. Each port on each interface has its own independent capture capability and capture buffer. Data can be captured and decoded in a number of ways (fig. 8).

- 1. Capture of all data over a period of time (to the limit of the buffer) and the subsequent filtering of frames of particular interest.
- 2. Filtered capture of frames of interest. Filters can be set for Source and Destination IP and MAC addresses errors or two user-defined conditions. These are as flexible as the previously described user-defined counters. These filters can be set individually, as a logical "OR" function or a logical "AND" function.
- 3. Triggered data capture can be set using the same filter functions (implemented in hardware) and additionally by setting a traffic threshold or a latency threshold. This is a particularly useful tool when monitoring important high quality traffic levels. The trigger can be set to the top, middle or bottom of the capture buffer.
- 4. Additionally, frames captured on a port can be quickly and easily transferred to the transmit side of any port to be played back out over the network. This can be used as an effective faultfinding tool to recreate and simulate network problems during quiet periods without having to wait for them to manifest themselves again (fig. 9).

Network Interfaces
The MD1230A currently has the following range of network interfaces:

10 M/100 M Ethernet
- comes with 8 ports

1 Gb Ethernet
- comes with 2 ports and supports the full range of GBIC

2.5 G STM 16 (POS)
- comes with 1 port in both single and multi mode types

10 G STM 64 (POS)
- comes with 1 port in both single and multi mode types

Other interfaces may be available in the near future.
The MD1230A is the leading complete performance testing and network monitoring solution for data networks. It delivers system construction, verification and benchmarking, as well as being able to confirm traffic and network availability by effective, flexible and comprehensive network monitoring and analysis. 7

Murray Coleman, *Anritsu,*
and Walter Marti,
E-Mail: walter.marti@gigacomp.ch,
Gigacomp AG, Gewerbezone Lätti,
CH-3053 Münchenbuchsee,
Tel. 031 868 44 55,
E-Mail info@gigacomp.ch

Zusammenfassung

Das neue Vernetzungsparadigma testen

MD1230A Data Quality Analyser, die Antwort von Anritsu auf die Notwendigkeit des Testens von Network Traffic Engineering, des Benchmarkings von Geräten und Virtual Circuits, der Einführung und Verifizierung von Quality of Service-Anforderungen und der Wartung von Service Level Agreements. Zunehmende Nutzung von IP-Anwendungen durch Unternehmen stellt neue und grössere Anforderungen an Netze für Service-Garantien bezüglich der Zuverlässigkeit und Service-Qualität. Wenn das Geschäft von der Kommunikation abhängt, dann kann man sich keinen Kommunikationsdienst leisten, der seine Leistung nicht erbringt. Die heutigen Datennetze bieten gegenwärtig keine Garantien dafür, dass Service-Level-Anforderungen ohne eine gewisse Verschlechterung zu irgendeiner Tag- oder Nachtzeit erfüllt werden können, unabhängig von anderen Benutzern des Netzes.