tek Signals
073, 7th Fl., GIBCA BLDG
Khalifa St., AUH, UA E.
www.teksignals.com

اتصالات
etisalat

ALBEDO Telecom
R. Turró, 100 - Barcelona - 08005
Chalfont St Peter - Bucks - SL9 9TR
www.telecom.albedo.biz

Triple Play Service Performance Test System

System to provide an Integrated Multiplay Test System (IMTS) to evaluate the Performance and Quality of Voice, High Speed Internet and IPTV services delivered over converged IP/Ethernet infrastructures and GPON access networks.

ALBEDO TELECOM is pleased to provide this information in response to ETISALAT request for proposal and quotation (RFP) for managing its Triple Play network.

Presentation

This proposal for System to provide an integrated test solution to evaluate the performance of Voice, High Speed Internet and IPTV services is presented by TEKSIGNALS and ALBEDO Telecom and the support of Malden, IXIA and Rohde&Schwarz.

- *ALBEDO* Telecom: Manufacturer with 30 years experience in telecommunications, test, measurement and monitoring, ALBEDO has clients in more than 25 countries. Many solutions have been pioneered by this company as the we designed the first PDH tester in the world, or the first handheld testers for SDH, ATM, and MPEG / TS2. Today ALBEDO designs test equipment and systems while consulting / integration services for VoIP and IPTV and unified networking.
- *Teksignals* sets standards as a professional consultancy in the fields of Broadcasting, Telecommunications, Test & Measurements, Multimedia, Education, Instrumentation and Professional Systems. Teksignals is truly an innovator and leader in the integration of performance and different technologies. The expertise gained have given the firm a strong local and international client base and a “can do well” reputation. Teksignals believes their industry has no boundaries and they are continually striving to develop and implement new and unprecedented practical design solutions.
- *IXIA*: Manufactures highly scalable solutions generate, capture, characterize, and emulate network and application traffic, establishing definitive performance and conformance metrics of network devices or systems under test. Ixia's Triple Play test systems address the growing need to test voice, video, and data services and network capability under real-world conditions. Ixia's test systems utilize a wide range of industry-standard interfaces, including Ethernet, SONET, ATM, and wireless connectivity.
- *ROHDE & SCHWARZ*. Rohde & Schwarz is the largest manufacturer of electronic test and measurement equipment in Europe. Our T&M instruments and systems are setting standards worldwide in research, development, production and service. We are the key partner of industry and network operators for all measurement tasks in the field of analog and digital communications.
- *MALDEN*. Malden delivers reference speech quality measurement systems to the telecommunications community. With carefully designed interfaces to VoIP, mobile, satellite and wireline networks, our products are used to define and confirm performance standards all over the world. Malden products are used for product evaluation, benchmarking, SLA verification, IP equipment developers and regression testing.

Introduction

This document describes the major uses and features of ALBEDO's Triple Play Service Performance Test System which is built integrating network elements and solutions from IXIA, MALDEN, R&S, TECNALIA and ALBEDO. Our goal is to provide ETISALAT with the right solution to test, monitor and troubleshoot their voice, video and data applications that will improve ATISALAT Triple Play service fulfillment, service quality, service assurance and service optimization.

The Integrated Multiplay Test System

This Multiplay Test System is an integral solution to evaluate the performance of Voice, High Speed Internet, and IPTV services in actual Network Conditions. It is also capable of testing the IP Converged and Transport network, while verifying the FTTH access network. This System it is also capable to Emulate Triple Play services through generation and analyzing the services on GPON, CPE routers, PLC, Coax, and STB.

ALBEDO Overview

ALBEDO is a company based in Barcelona, Spain (European Union). Our two main businesses are: (1)manufacturer of Telecom Test and Diagnostics instruments and systems for telcos and OEMs; and (2) as consultant and integrator for VoIP and IPTV monitoring services delivered over unified networking and new generation access technologies.

At the Consulting and Integration business, we design test & monitoring solutions for a highly quality, resilient IPTV, VoD, VoIP, HSI architectures. We use probes, servers and testers capable that are of emulate IPTV servers and software for compression and Video on Demand (VOD) and Streaming Video content. We can replicate accurately the actual VoIP scenarios to execute approval and acceptance procedures in optimal conditions, while verifying the quality of the phone service.

Our triple play (voice, video and data) converged network test solutions focus on Standard and High Quality services deployed over multi-vendor IP networks using state-of-the-art hardware and software to IP technologies. The IP stream can be unicast or multicast onto the network backbones maintaining Quality of Service (QoS). The result is to achieve excellence Quality of Experience (QoE) keeping in Triple Play services jitter free, low loss and minimal latency end-to-end.

We look forward to work with ETISALAT to provide a best in class solution to verify and assure the quality for your converged infrastructure and Multiplay services.

Sincerely,

Jose M Caballero
General Manager
ALBEDO Telecom
jose.caballero@albedo.biz
+34 637 410 299

Table of Contents

1. INTRODUCTION

This document describes an Integrated Test System consisting of generators of traffic, measurement probes, standard network elements, a network impairments generators at IP layer and at physical level. The system also includes a GPON analyzer option to measure also in the FTTH access network.

This system is test solution capable of generating Voice, Video, TV, P2P, Data traffic in the same way as ETISALAT contribution network and customer applications. There is the possibility of adding perturbations in different ways from traffic generators to control the IP network impairments such as delay, jitter, loss, etc. to characterize and test any Service Under Test (SUT) such as Voice/TV/Video/ Data, in actual network conditions.

The system allow the verification of network elements and their compliance capabilities with the Multiplay system of ETISALAT. Some are: IP phones, STB, IPTV, PC and components for interconnection (wireless, coax, PLCs).

One important point to highlight is that all elements could be automated to become part of test plans that can be managed in a simple and centralised way.

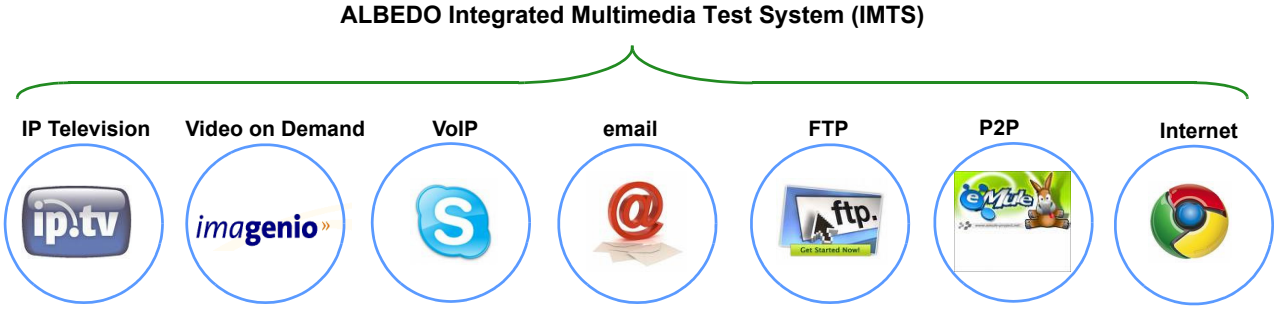

Figure 1. *Multiplay services that can be fully verified in the ALBEDO Multiplay Test System.*

Highlighted Features

This Multiplay Test System includes a series of facilities, equipment and optional services to provide an optimal solution, scalable and effective safeguards need to evolve with complete ability to create new tests and trials expected in future.

- Standard and scalable architecture, integration of new connectivity features, new services (ie VoIP), new test suite, new access networks.
- Testing places scalable from 4 to 16 ports. The proposed frame can have two cards.
- QoE metrics in audio and video applications, including MDI, MOS MOS audio and video. In addition, generic compute QoS metrics (delay, jitter, packet loss).
- Support RFC 2544, RFC 2889, RFC 3511 and RFC 3918 standard test devices with standard tests for Ethernet / IP, IP Multicast tests and specific tests for NAT routers and firewalls.
- Net.Storm is a simple, fast, hardware based Ethernet/IP network emulator that provides the ability to generate common network effects such as packet loss, duplication, delay, congestion, packet errors and bandwidth limitations. It is designed to offer sufficient capabilities and performance to reproduce a wide range of network behaviors up to 1 Gbps rates with accuracy always better that 1 ms.

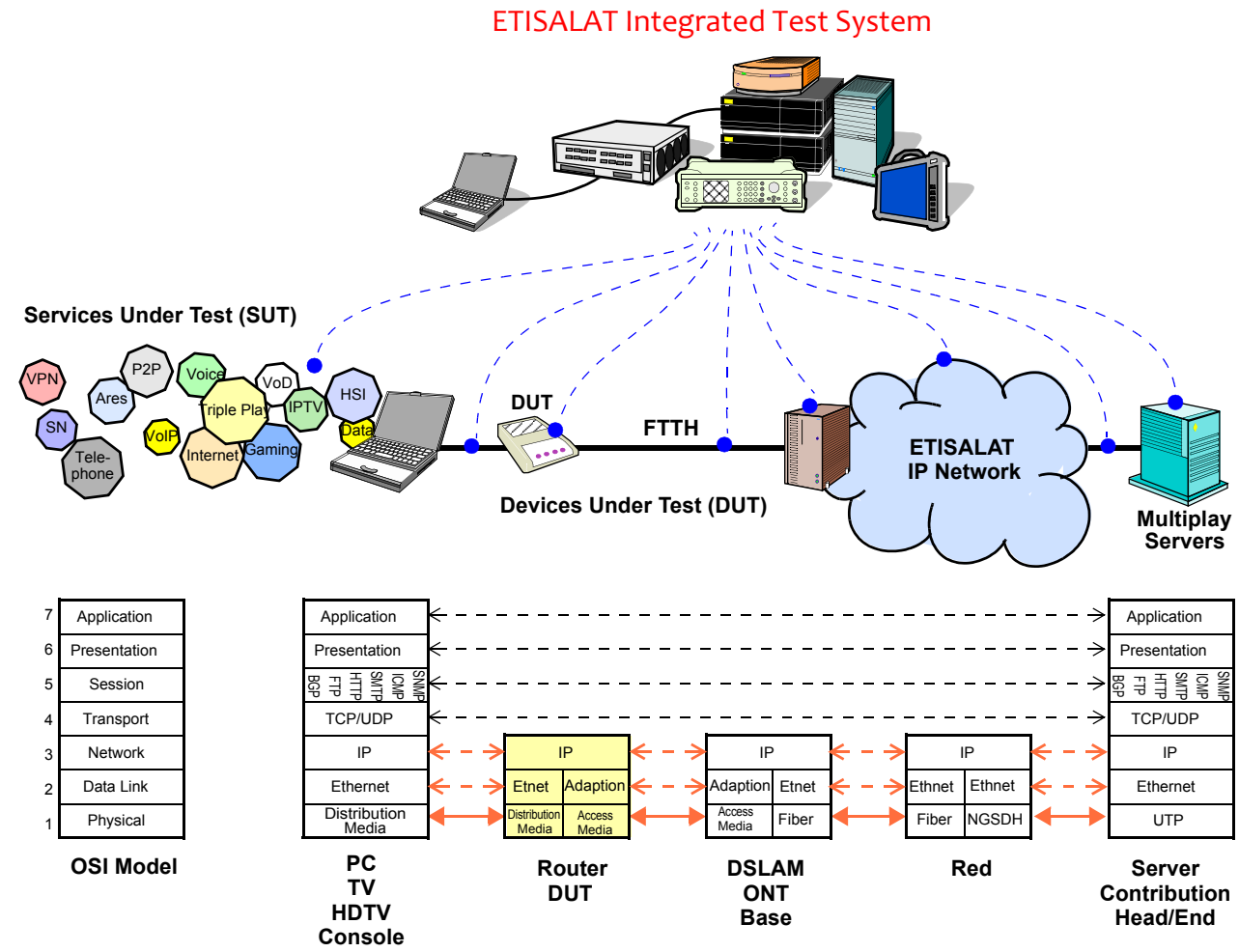

Figure 2. *The model of seven levels of telecommunications allows the router, not have to analyse the payload of the IP frames, or what is the same, never engages with the upper levels of protocols or applications.*

Options

This system has several alternatives to be extended:

- Application Replay. This is an application that can play back previously captured traffic, stored in a format widely accepted by industry (PCAP). This application transforms the Integrated Test System in an Open Solution capable to support virtually any application used by the subscriber.
- Simulation of disturbances in the network subscriber. Including those that occur in elements such as wireless (Wi/Fi), Coax and Powerline (PLC). For each of the modalities of interconnection network subscriber ALBEDO may also offer predefined test suites (also known as test plans).

Acceptance and Conformance Test Suite

The second family of options is a range of test suites developed by ALBEDO Telecom intended for the Acceptance and Approval of equipment for IPTV or VoIP such as routers, STB and other terminals, that could be implemented systematically in the test:

- Test suite for video coaxial transmitters

- Test Suite for the approval of PLC equipment (see Annex B)
- Test Suite for the selection of video transmitters (see Annex B)
- Suite of tests to ensure quality of VoIP equipment (see Annex B)
- Compliance test suite VoIP equipment (see Annex C)
- Suite of tests to ensure quality of network equipment and terminals IPTV
- Verification test suite IP, DNS, Server error (see Appendix C)

2. ARCHITECTURE

The Integrated Test System is made up of several subsystems. Each has specific functions:

- *Generator / Analyzer*: This part of the Test System performs two distinct functions. On one side is responsible for emulating the user traffic in the most realistic way and the other acts as a probe for evaluating traffic after passing through the Service under Test (SUT) or the Device under Test (DUT). The core of this subsystem is the application of Ixia IxLoad.
- *Subsystem I - Network Services Simulation:* It will provide the connectivity, switching and emulation services that usually provide IP networks, specifically those provided by the ETISALAT network, including authentication, IP address allocation and domain name service. Some of the protocols from the application itself will emulate IxLoad (DHCP server, DNS server) and others such as access via PPPoE be made by a dedicated server.

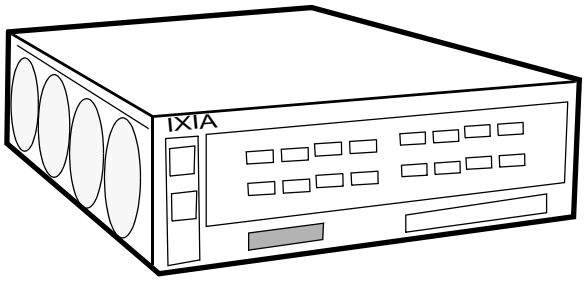

Figure 3. *XM2 chassis is the platform which is built platform subsystems test generation and simulation of networks. It is scalable up to 32 ports.*

- *OPTIONAL:* The network subsystem can take care to generate impairments that may occur in the operator's network and affect the quality of services. Disturbances such as delays (constant or variable according to a given distribution probability), duplication of packets, packet loss and reordering of packets

OPTIONAL

- *Subsystem II - Subscriber Network Simulation*: The most important part of this subsystem is the physical simulation which is used to interconnect the communication equipment of the subscriber network. In the simplest case, the interconnection is done via Ethernet interfaces but there are other possibilities that require more extensive testing. For example WiFi, PLC or interconnection via coaxial cable. Some network services commonly available in the networks of subscribers (eg. DHCP server).

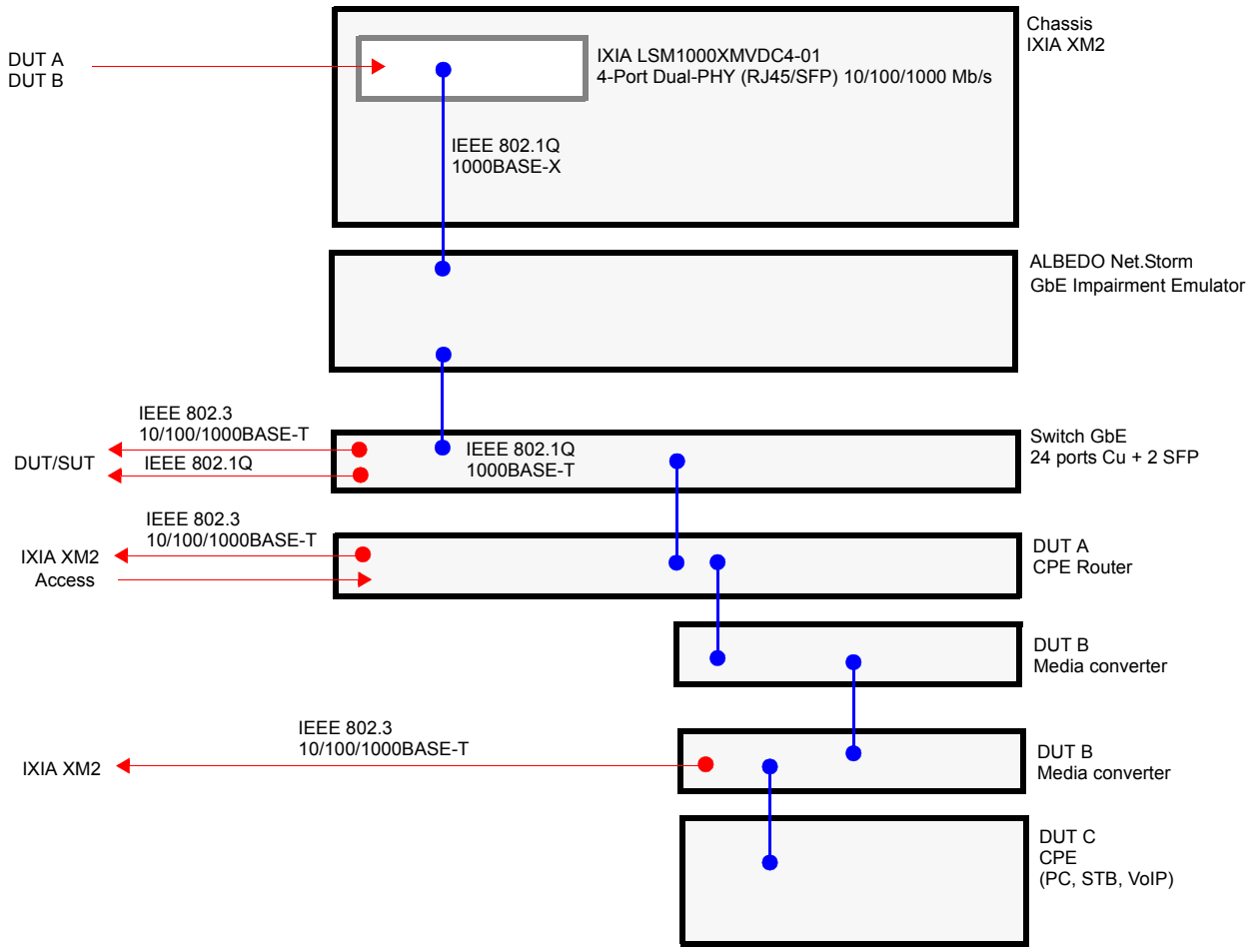

Figure 4. *Block diagram of some elements of the Integrated Multimedia Test System (IMTS).*

3. SIMULATION ETISALAT NETWORK AND SUBSCRIBER

The Integrated System Test verifies network and the Multiplay services such as IPTV or VoIP particularly in the case of a failure or bad quality is not determined the cause if it is on the network or device that is being evaluated. The System is a known and 100% controlled environment. The simulation of ETISALAT network and the subscriber, involves the generation of traffic, often a client / server, which is not in itself proof traffic but at the same time it is essential to ensure that evidence can function correctly. For example, it is necessary to allow the Implemented network to authenticate users and provide IP addresses because otherwise never get to test traffic transmitted.

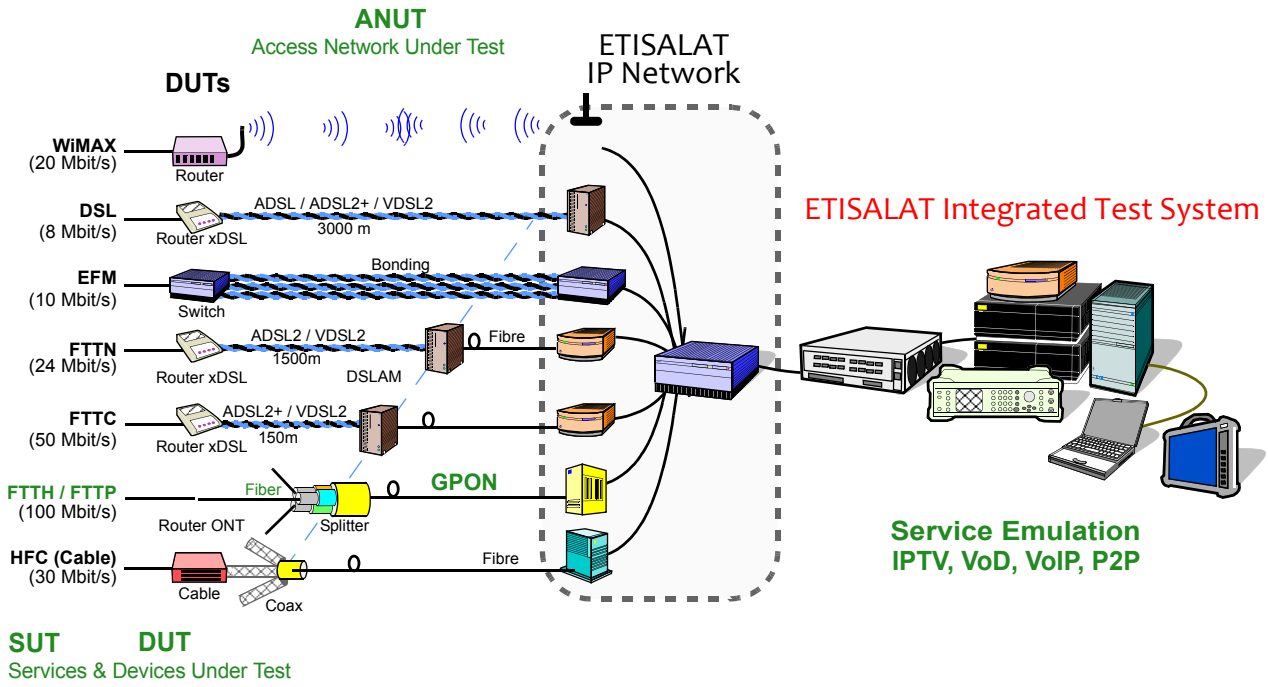

Figure 5. *It is also possible to Implement ETISALT network in order to verify the quality of the services and access network*

PPPoX

The base configuration of the Integrated Test System offers the ability to authenticate the subscriber routers and assign IP addresses on the network using PPPoE.

It also offers advanced testing protocols for access to PPPoE and PPPoA to characterize in detail the behavior of the DUT / SUT. Once established the session, the Integrated Test System allows the injection of user traffic on them and measure quality parameters. Proficiency testing are supported, latency associated with DUT / SUT.

The optional item described also includes the ability to Implement the L2TPv2 protocol (RFC 2661) and L2TPv3 (RFC 3931).

Table 11.
Technical specifications of the PPP simulator sessions.

PPP	• Full PPP stack • Support for PPPoE, PPPoA and PPPoEoA • IPv4 and IPv6 sessions • DHCP support • VLAN and stacked VLAN (QinQ) support • ATM: LLC and VC Multiplexed encapsulation over AAL5 • Full session control (setup and teardown rates, total session count, flapping, retry attempts, multiple sessions per VLAN or ATM VPI/VCI) • LCP link control, IPCP network control and NCP address control • Access Concentrator selection • Authentication: PAP and CHAP (MD5) with unique user names and passwords • Keep-alive responses and requests • Domain groups used to direct access to network port traffic
Traffic Generation	• Stateless and stateful traffic generation over established sessions/tunnels • Stateless Layer 4 traffic flows with configurable protocol (TCP, UDP) and variable source/destination port numbers • Full QoS control per traffic stream using DSCP, IP Precedence or IPv6 Traffic Class/Flow labels • Full bi-directional source to destination traffic flow, with variable data rates • Fixed, incrementing, or mixed frame sizes • IMIX mode allowing individual rates assigned to up to 5 different frame sizes • Frame rate control in frames per second or percentage of line rate • IEEE 802.1q VLANs and stacked VLANs (QinQ) - full range of 4,095 IDs
Relevant Standards	• RFC 1332 (IPCP) • RFC 1334 (PAP) • RFC 1570 (LCP Extensions) • RFC 1661 (PPP) • RFC 1994 (CHAP) • RFC 2364 (PPP over AAL5) • RFC 2516 (PPPoE) • RFC 2661 (L2TP) • IEEE 802.1q (VLANs)

DHCP

The Integrated Test System allows the emulation of a DHCP server (item 925-3148). The server is a fully integrated with the test system so that it can be managed together and allows the extraction of detailed statistics.

Through this server, DHCP clients can connect directly to the Test System for those tests where needed. Examples could include performance testing of STBs for IPTV or, IP phones without the need of the subscriber router. The DHCP server will also be useful in case ETISALAT wants to verify the operation of DHCP protocol access in place of PPP. In the latter case, the DHCP client would be the subscriber router.

On the other hand it is also possible to Implement one or more DHCP clients (Item 925-3300) and send traffic once established test sessions. This is needed to Implement the user traffic in the user's network via a subscriber router.

DNS

The Integrated System Test Implements DNS traffic generated by both clients and servers (Item 925-3300). Thus, all tests can be performed with maximum likelihood because the domain names resolved to IP addresses and statistics (especially latency) include delays resulting from DNS requests and responses.

Table 12.
DHCP server simulator specifications.

Features	• IPv4, IPv6 • Multiple servers per port • Configuration of starting pool address and number of IPs per pool and scope mask • Per-scope configuration of gateway/router and DNS server • Configurable timers for lease • Server IP and MAC address • VLAN and QnQ support per server • First pool IP and pool count • Default lease time (s) • Maximum lease time (s)
Relevant Standards	• RFC 2131 (DHCP)

Table 13.
DHCP client simulator specifications.

Commands	• DHCP DISCOVER, REQUEST, DECLINE, REJECT and INFORM
Options	• Pad (0) • Subnet Mask Value (1) • Time Offset in Seconds from UTC (2) • Router addresses (3) • DNS Server addresses (6) • Hostname string (12) • DNS domain name of the Client (15) • Interface MTU Size (26) • All Subnets are Local (27) • Broadcast Address (28) • Perform Mask Discovery (29) • Perform Router Discovery (31) • ARP Cache Timeout (35) • Vendor Specific Information (43) • Requested IP Address (50) • IP Address Lease Time (51) • Overload "sname" or "file" (52) • DHCP Message Type (53) • DHCP Server Identification (54) • Parameter Request List (55) • DHCP Error Message (56) • DHCP Maximum Message Size (57) • DHCP Renewal (T1) Time (58) • DHCP Rebinding (T2) Time (59) • (Vendor) Class Identifier (60) • Client Identifier (61) • User Class Information (77) • DHCP Relay Agent (82) • End (255)
Features	• Support for BOOTP • Ability to configure option 82 relay agent emulation with sub-options circuit-id and remote-id • Ability to emulate trusted network element in networks containing DHCP relay agents • Support to configure DHCP options (mandatory and informational)

Table 13.
DHCP client simulator specifications.

Collected Statistics	• DHCP DHCPDISCOVER Response Time • DHCP DHCPREQUEST Response Time • DHCP DHCPREQUEST (SELECTING) Response Time • DHCP DHCPREQUEST (INIT-REBOOT) Response Time • DHCP DHCPREQUEST (RENEWING) Response Time • DHCP DHCPREQUEST (REBINDING) Response Time • DHCP DHCPINFORM Response Time • DHCP BOOTREQUEST Response Time • DHCP Total Commands Sent • DHCP Total Commands Succeeded • DHCP Total Commands Failed • DHCP Total Commands Failed (NAK Received) • DHCP Total Commands Failed (Timeout) • DHCP Total Commands Failed (Error) • DHCP Total Commands Retransmitted • DHCP Total Responses Matched • DHCP Total Responses Mismatched

Table 13.
DHCP client simulator specifications.

	• DHCP DHCPDISCOVER Commands Sent • DHCP DHCPDISCOVER Commands Succeeded • DHCP DHCPDISCOVER Commands Failed • DHCP DHCPDISCOVER Commands Failed (Timeout) • DHCP DHCPDISCOVER Commands Failed (Error) • DHCP DHCPDISCOVER Commands Retransmitted • DHCP DHCPDISCOVER Responses Matched • DHCP DHCPDISCOVER Responses Mismatched • DHCP DHCPREQUEST Commands Sent • DHCP DHCPREQUEST Commands Succeeded • DHCP DHCPREQUEST Commands Failed • DHCP DHCPREQUEST Commands Failed (NAK Received) • DHCP DHCPREQUEST Commands Failed (Timeout) • DHCP DHCPREQUEST Commands Failed (Error) • DHCP DHCPREQUEST Commands Retransmitted • DHCP DHCPREQUEST Responses Matched • DHCP DHCPREQUEST Responses Mismatched • DHCP DHCPREQUEST (SELECTING) Commands Sent • DHCP DHCPREQUEST (SELECTING) Commands Succeeded • DHCP DHCPREQUEST (SELECTING) Commands Failed • DHCP DHCPREQUEST (SELECTING) Commands Failed (NAK Received) • DHCP DHCPREQUEST (SELECTING) Commands Failed (Timeout) • DHCP DHCPREQUEST (SELECTING) Commands Failed (Error) • DHCP DHCPREQUEST (SELECTING) Commands Retransmitted • DHCP DHCPREQUEST (SELECTING) Responses Matched • DHCP DHCPREQUEST (SELECTING) Responses Mismatched • DHCP DHCPREQUEST (INIT-REBOOT) Commands Sent • DHCP DHCPREQUEST (INIT-REBOOT) Commands Succeeded • DHCP DHCPREQUEST (INIT-REBOOT) Commands Failed • DHCP DHCPREQUEST (INIT-REBOOT) Commands Failed (NAK Received) • DHCP DHCPREQUEST (INIT-REBOOT) Commands Failed (Timeout) • DHCP DHCPREQUEST (INIT-REBOOT) Commands Failed (Error) • DHCP DHCPREQUEST (INIT-REBOOT) Commands Retransmitted • DHCP DHCPREQUEST (INIT-REBOOT) Responses Matched • DHCP DHCPREQUEST (INIT-REBOOT) Responses Mismatched • DHCP DHCPREQUEST (RENEWING) Commands Sent • DHCP DHCPREQUEST (RENEWING) Commands Succeeded • DHCP DHCPREQUEST (RENEWING) Commands Failed • DHCP DHCPREQUEST (RENEWING) Commands Failed (NAK Received) • DHCP DHCPREQUEST (RENEWING) Commands Failed (Timeout) • DHCP DHCPREQUEST (RENEWING) Commands Failed (Error) • DHCP DHCPREQUEST (RENEWING) Commands Retransmitted • DHCP DHCPREQUEST (RENEWING) Responses Matched • DHCP DHCPREQUEST (RENEWING) Responses Mismatched • DHCP DHCPREQUEST (REBINDING) Commands Sent • DHCP DHCPREQUEST (REBINDING) Commands Succeeded • DHCP DHCPREQUEST (REBINDING) Commands Failed • DHCP DHCPREQUEST (REBINDING) Commands Failed (NAK Received) • DHCP DHCPREQUEST (REBINDING) Commands Failed (Timeout) • DHCP DHCPREQUEST (REBINDING) Commands Failed (Error) • DHCP DHCPREQUEST (REBINDING) Commands Retransmitted • DHCP DHCPREQUEST (REBINDING) Responses Matched • DHCP DHCPREQUEST (REBINDING) Responses Mismatched • DHCP DHCPDECLINE Commands Sent • DHCP DHCPDECLINE Commands Send Failed • DHCP DHCPRELEASE Commands Sent • DHCP DHCPRELEASE Commands Send Failed

Table 13.
DHCP client simulator specifications.

	• DHCP DHCPINFORM Commands Sent • DHCP DHCPINFORM Commands Succeeded • DHCP DHCPINFORM Commands Failed • DHCP DHCPINFORM Commands Failed (Timeout) • DHCP DHCPINFORM Commands Failed (Error) • DHCP DHCPINFORM Commands Retransmitted • DHCP DHCPINFORM Responses Matched • DHCP DHCPINFORM Responses Mismatched • DHCP BOOTREQUEST Commands Sent • DHCP BOOTREQUEST Commands Succeeded • DHCP BOOTREQUEST Commands Failed • DHCP BOOTREQUEST Commands Failed (Timeout) • DHCP BOOTREQUEST Commands Failed (Error) • DHCP BOOTREQUEST Commands Retransmitted • DHCP BOOTREQUEST Responses Matched • DHCP BOOTREQUEST Responses Mismatched • DHCP Total Number of DHCPOFFER Messages • DHCP Number of DHCPOFFER Messages Ignored • DHCP Total Number of DHCPACK Messages • DHCP Number of DHCPACK Messages Ignored • DHCP Total Number of DHCPNAK Messages • DHCP Number of DHCPNAK Messages Ignored • DHCP ICMP Echo Messages Received • DHCP ICMP Echo Reply Messages Sent • DHCP ARP Request Messages Received • DHCP ARP Reply Messages Sent • DHCP Valid IP Addresses Received • DHCP Duplicate IP Addresses Received • DHCP User Count • DHCP Total Transaction • DHCP Number of Active Leases • DHCP Number of Leases Expired • DHCP Number of Clients Awaiting IP Address from Server • DHCP Total Bytes Transmitted • DHCP Total Bytes Received • DHCP Total Bytes Transmitted and Received
Relevant Standards	• RFC 2131 Dynamic Host Configuration Protocol • RFC 3046 DHCP Relay Agent Information Option

In the transactions associated with the DNS protocol are collected and stored statistics associated with the operation of the protocol in DUT / SUT. As in the other services Implemented in the Integrated Test System, the server / client DNS is fully integrated and managed in conjunction with other elements and devices

Table 14.
DNS technical specification.

Version	• DNSv4
IP Support	• IPv4, IPv6
Emulation	• Client and Server
Queries	• A, AAAA, CNAME, SOA, NS, MX, PTR
Features	• UDP and TCP transport • Option to use multiple zones and unique/non-unique resource records • Ability to import named configurations to DNS serve re

Table 14.
DNS technical specification.

Client Statistics	• DNS Total Queries Sent • DNS Total Queries Successful • DNS Total Queries Retried • DNS Total Queries Failed • DNS Total Queries Failed (Format Error) • DNS Total Queries Failed (Server Failure) • DNS Total Queries Failed (Name Error) • DNS Total Queries Failed (Not Implemented) • DNS Total Queries Failed (Refused) • DNS Total Queries Failed (Other) • DNS Total Queries Failed (Timeout) • DNS Total Queries Failed (Aborted) • DNS (Type A) Queries Sent • DNS (Type A) Queries Successful With Match • DNS (Type A) Queries Successful Without Match • DNS (Type A) Queries Failed • DNS (Type CNAME) Queries Sent • DNS (Type CNAME) Queries Successful With Match • DNS (Type CNAME) Queries Successful Without Match • DNS (Type CNAME) Queries Failed • DNS (Type MX) Queries Sent • DNS (Type MX) Queries Successful With Match • DNS (Type MX) Queries Successful Without Match • DNS (Type MX) Queries Failed • DNS (Type PTR) Queries Sent • DNS (Type PTR) Queries Successful With Match • DNS (Type PTR) Queries Successful Without Match • DNS (Type PTR) Queries Failed • DNS (Type NS) Queries Sent • DNS (Type NS) Queries Successful With Match • DNS (Type NS) Queries Successful Without Match • DNS (Type NS) Queries Failed • DNS (Type SOA) Queries Sent • DNS (Type SOA) Queries Successful With Match • DNS (Type SOA) Queries Successful Without Match • DNS (Type SOA) Queries Failed • DNS Total Bytes Transmitted • DNS Total Bytes Received • DNS Bytes • DNS Throughput • DNS Transactions • DNS Transaction Rate • DNS Simulated Users • DNS Total Queries Received • DNS Total Queries Responded Successfully • DNS Total Queries Failed • DNS Total Queries Failed (Format Error) • DNS Total Queries Failed (Server Failure) • DNS Total Queries Failed (Name Error)

Table 14.
DNS technical specification.

Server Statistics	• DNS Total Queries Failed (Not Implemented) • DNS Total Queries Failed (Refused) • DNS Total Queries Failed (Other) • DNS (Type A) Queries Received • DNS (Type A) Queries Responded Successfully • DNS (Type A) Queries Failed • DNS (Type CNAME) Queries Received • DNS (Type CNAME) Queries Responded Successfully • DNS (Type CNAME) Queries Failed • DNS (Type MX) Queries Received • DNS (Type MX) Queries Responded Successfully • DNS (Type MX) Queries Failed • DNS (Type PTR) Queries Received • DNS (Type PTR) Queries Responded Successfully • DNS (Type PTR) Queries Failed • DNS (Type NS) Queries Received • DNS (Type NS) Queries Responded Successfully • DNS (Type NS) Queries Failed • DNS (Type SOA) Queries Received • DNS (Type SOA) Queries Responded Successfully • DNS (Type SOA) Queries Failed • DNS Total Bytes Transmitted • DNS Total Bytes Received • DNS Total Bytes Transmitted and Received
Relevant Standards	• RFC 1034 • RFC 1035 • RFC 1123 • RFC 1886

4. TRAFFIC GENERATION/ANALYSIS

One of the characteristics of the Integrated Test System is the ability to Implement the traffic generated by users and network elements in a way that is as close as possible to the actual situation but in a totally controlled to ensure repeatability of the measurements. On the other hand, as a Test System tool, the Integrated Test System is able to obtain statistics at the reception test traffic and perform various tests and measures that characterize the performance of the DUT / SUT.

The core of both generator and the measuring probe consists of Ixia's IxLoad product. IxLoad software is installed on a single Ixia XM2 chassis. The application module installed on the XM2 is the LSM1000XMVDC4-01 that has four Gigabit Ethernet ports, RJ-45 or SFP. The interface used to schedule generation to meet the IEEE 802.1Q standard, i.e. Ethernet frames with VLAN tags. In this way, you can distribute traffic between different VLANs test and switches in the network subsystem independently.

The union of the generator and analyzer on a single computer offers numerous advantages. These make use of the same time base at both ends of transmission. This feature is important when trying to evaluate metrics to-end delay as specified in RFC 2679 (A One-way Delay Metric for IPPM).

IxLoad is characterized by the potential to generate different types of traffic in a very flexible way. Can be Implemented clients and web servers (HTTP and HTTPS), FTP, P2P (eDonkey, BitTorrent...), telephony and IP video telephony, VoD, IPTV and other applications. To this must be attached to the possibility of combining different types of traffic for complex test scenarios using different encapsulated data.

The performance metrics are specific to each type of traffic but some, such as those associated with latency, are repeated in several types of evidence.

P2P traffic (OPTIONAL)

P2P traffic generation is supported natively by the Integrated Test System (Item 925-3143) for most common protocols. This includes both BitTorrent and eDonkey).

Table 15.
Technical specifications of the P2P Traffic Generator

IP Support	• IPv4, IPv6
Protocols	• BitTorrent, eDonkey
Emulation	• Initiator peer, responder peer or both
Features	• Realistic P2P protocol simulation • Extensive library of predefined P2P traffic flows • Supports detailed measurement statistics and real-time graphs • Scales to thousands of peers, generating 800 Mb/s of P2P traffic per Gigabit Ethernet port • Choose from a library of P2P flow definitions for each protocol • Each traffic flow defines traffic with a different set of properties, such as the direction (upload, download or bidirectional to download), the amount of data transferred, the data size unit, and other properties.
Objectives	• Number of peers • Throughput • Concurrent connections • Connections per second • Transactions per second

Table 15.
Technical specifications of the P2P Traffic Generator

Statistics	• Peer Count • Concurrent Sessions • Connection Rate • Transaction Rate • Initiator Total Bytes Sent Rate • Initiator Total Bytes Received Rate • Initiator Total Throughput • Responder Total Bytes Sent Rate • Responder Total Bytes Received Rate • Responder Total Throughput • Connection Requests Sent • Connection Requests Successful • Connection Requests Failed • Active Connections • Connection Requests Received • Connections Accepted • Connections Failed • Initiator Total Bytes Sent • Initiator Total Bytes Received • Initiator Total Bytes Sent and Received • Responder Total Bytes Sent • Responder Total Bytes Received • Responder Total Bytes Sent and Received • Total Transactions Initiated • Total Transactions Successful • Total Active Flow • Total Flow Initiated • Total Flow Succeeded • Total Flow Failed • Total Flow Failed Error • Total Flow Failed Timeout • Total Flow Failed Mismatch • Control Flow Transmission Initiated • Control Flow Transmission Succeeded • Control Flow Transmission Failed • Control Flow Transmission Failed (Error) • Control Flow Transmission Failed (Timeout) • Control Flow Reception Initiated • Control Flow Reception Succeeded • Control Flow Reception Failed • Control Flow Reception Failed (Error) • Control Flow Reception Failed (Timeout) • Control Flow Reception Failed (Mismatch)
	• Data Flow Transmission Initiated • Data Flow Transmission Succeeded • Data Flow Transmission Failed • Data Flow Transmission Failed (Error) • Data Flow Reception Initiated • Data Flow Reception Succeeded • Data Flow Reception Failed • Data Flow Reception Failed (Error Data) • Flow Reception Failed (Timeout)

Constantly are appearing new applications based on P2P techniques, these applications are not based on any standard. Therefore, P2P applications are always difficult to test. The solution is to use Application Replay (item 925-3142). This is a feature of the Integrated Test System that allows playback of a stream of IP data previously captured.

To recreate the previously captured session is not enough to reproduce the data stored mechanically. Replay Application has been designed to play both ends of the communication if necessary and take into account the rules of TCP / IP during playback. Thus, the Integrated Test System can be extended to support new protocols not provided in principle. This method is especially efficient then those protocols not covered by any standards can be easily recreated with maximum likelihood.

Table 16.
Application Replay Specifications (OPTIONAL).

IP Support	• IPv4
Emulation	• Peers - initiator, responder or both
Features	• Create bi-directional traffic simultaneously • Industry's only solution that replicates user-specified traffic at varying levels of performance. • Emulates application traffic alongside other IxLoad-emulated traffic (HTTP, VoIP, IPTV,...) • Supports detailed measurement statistics and real-time graphs. • Supports conditional statistics (per-IP, per-VLAN, per-User), per-flow statistics, and latency statistics support • Override responder port derived from the capture during replay • Select point in PCAP file to be begin playback from • Configure filters for initiator and responder IP and ports • Concurrent flow support to simulate users initiating more than one flow at one time • Validate Per-flow and Latency statistics with the advanced statistics option • Verify content of payload against expected payload • Verify length of payload against expected length
Objectives	• Peer count • Throughput • Concurrent connections • Connection rate • Transaction rate
Global statistics	• AppReplay Application Peer Count • AppReplay Connection Rate • AppReplay Concurrent Sessions • AppReplay Transaction Rate • AppReplay Initiator Total Bytes Sent/sec • AppReplay Application Initiator Total Bytes Received/sec • AppReplay Initiator Total Throughput • AppReplay Responder Total Bytes Sent/sec • AppReplay Responder Total Bytes Received/sec • AppReplay Responder Total Throughput

Table 16.
Application Replay Specifications (OPTIONAL).

	• AppReplay Connection Requests Sent • AppReplay Connection Requests Successful • AppReplay Connection Requests Failed • AppReplay Connection Requests Received • AppReplay Connections Accepted • AppReplay Connections Failed • AppReplay Active Connections • AppReplay Total Transactions Initiated • AppReplay Total Transactions Successful • AppReplay Total Flow Replays Initiated • AppReplay Total Active Flow Replays • AppReplay Total Flow Replays Succeeded • AppReplay Total Flow Replays Failed • AppReplay Total Flow Replays Failed Error • AppReplay Total Flow Replays Failed Timeout • AppReplay Total Flow Replays Failed Mismatch • AppReplay Initiator Total Bytes Sent • AppReplay Initiator Total Bytes Received • AppReplay Initiator Total Bytes Sent and Received • AppReplay Responder Total Bytes Sent • AppReplay Responder Total Bytes Received • AppReplay Responder Total Bytes Sent and Received • AppReplay Segment Transmission Initiated • AppReplay Segment Transmission Succeeded • AppReplay Segment Transmission Failed • AppReplay Segment Transmission Failed (Error) • AppReplay Segment Transmission Failed (Timeout) • AppReplay Segment Reception Initiated • AppReplay Segment Reception Succeeded • AppReplay Segment Reception Failed • AppReplay Segment Reception Failed (Error) • AppReplay Segment Reception Failed (Timeout) • AppReplay Segment Reception Failed (Mismatch)
Per flow statistics	• Connection Requests Successful • Active Connections • Total Transactions Successful • Initiator Total Bytes Tx • Initiator Total Bytes Rx • Initiator Total Bytes Tx and Rx • Responder Total Bytes Tx • Responder Total Bytes Rx • Responder Total Bytes Tx and Rx • Connection Requests Sent • Connection Requests Failed • Connection Requests Received • Connections Accepted • Connections Failed • Total Transactions Initiated • Total Flow Replays Initiated • Total Active Flow Replays • Total Flow Replays Succeeded • Total Flow Replays Failed • Total Flow Replays Failed Error • Total Flow Replays Failed Timeout • Total Flow Replays Failed Mismatch • Total Flow Replays Aborted • Total number of flow replays aborted for any reason.

Table 16.
Application Replay Specifications (OPTIONAL).

	• Control Flow Transmission Initiated • Control Flow Transmission Succeeded • Control Flow Transmission Failed • Control Flow Transmission Failed Error • Control Flow Transmission Failed Timeout • Control Flow Reception Initiated • Control Flow Reception Succeeded • Control Flow Reception Failed • Control Flow Reception Failed Error • Control Flow Reception Failed Timeout • Control Flow Reception Failed Mismatch • Inter Segment First Response Latency (for Initiated Flows) • Inter Segment First Response Latency (for Responded Flows) • Inter Segment Last Response Latency (for Initiated Flows) • Inter Segment Last Response Latency (for Responded Flows) • Session Life Time (for Initiated Flows) • Session Life Time (for Responded Flows)

HTTP / HTTPS Navigation

Another characteristic of the Integrated Test System is the ability to Implement one or more transactions HTTP / HTTPS implementing the activity of web users. Both the server and the client can be tested, nevertheless in cases when ETISALAT wants to use an external HTTP server only customers could be tested. It would be possible to even measure the performance parameters such as server response time.

The ability to customize both, client requests and responses of users, is virtually unlimited. It supports HTTP cookies and redirection can be loaded pages and user defined on the server Implemented.

Table 17.
Web navigation specifications.

Version	• HTTP 1.0, HTTP 1.1
IP Support	• IPv4, IPv6
Emulation	• Client and Server
Features	• Supports HTTP pipelining, cookies and HTTP redirection • Supports proxy server commands • Supports decompression on HTTP clients • Supports Content-MD5 integrity check • Supports Chunked Encoding processing on HTTP clients • Option to use multiple TCP connections per user • User realism with control of HTTP commands using transaction aborts and *Think* times • User defined pages on HTTP server • Supports sequence generators that easily create large numbers of user sessions with unique credentials • Configurable TOS and DSCP bit settings • Configurable HTTP headers for each request • Inspection of data payloads for user-specified text • Option for HTTP servers to listen on multiple TCP ports • User-configurable HTTP server page responses • Support for customizing response code, page size, cookies and page content on servers • Detailed metrics such as average server response times and total transaction times in addition to HTTP state level and HTTP response code statistics • Per-URL statistics

Table 17.
Web navigation specifications.

Commands	• GET, POST, HEAD, PUT and DELETE
Web browsers	• Microsoft Internet Explorer 5/6, Mozilla, Firefox, Safari and Custom
Client Statistics	• HTTP Simulated Users • HTTP Concurrent Connections • HTTP Connections • HTTP Transactions • HTTP Bytes • HTTP Requests Sent • HTTP Requests Successful • HTTP Requests Failed • HTTP Requests Failed (Write) • HTTP Requests Failed (Read) • HTTP Requests Failed (Bad Header) • HTTP Requests Failed (4xx) • HTTP Requests Failed (400) • HTTP Requests Failed (401) • HTTP Requests Failed (403) • HTTP Requests Failed (404) • HTTP Requests Failed (408) • HTTP Requests Failed (4xx other) • HTTP Requests Failed (5xx) • HTTP Requests Failed (505) • HTTP Requests Failed (5xx other) • HTTP Requests Failed (Timeout) • HTTP Requests Failed (Aborted) • HTTP Aborted Before Request • HTTP Aborted After Request • HTTP Session Timeouts (408) • HTTP Sessions Rejected (503) • HTTP Transactions Active • HTTP Users Active • HTTP Bytes Sent • HTTP Bytes Received • HTTP Cookies Received • HTTP Cookies Sent • HTTP Cookies Rejected • HTTP Cookies Rejected - (Path Match Failed) • HTTP Cookies Rejected - (Path Domain Failed) • HTTP Cookies Rejected - (Cookiejar Overflow) • HTTP Cookies Rejected - (Probabilistic Reject) • HTTP Connect Time (ms) • HTTP Time to First Byte • HTTP Time to Last Byte • HTTP Responses Received With Match • HTTP Responses Received Without Match • Content-Encoded Response Received • Content-Encoded Responses Decode Successful • Content-Encoded Responses Decode Failed • Unrecognized Content-Encoding Received • Per-URL Average Compression Ratio • Deflate Content-Encoding Received • Deflate Content-Encoding Decode Successful • Deflate Content-Encoding Decode Failed • Deflate Content-Encoding Decode Failed Checking Error • Deflate Content-Encoding Decode Failed Data Error • Deflate Content-Encoding Decode Failed Decoding Error

Table 17.
Web navigation specifications.

	• Gzip Content-Encoding Received • Gzip Content-Encoding Decode Successful • Gzip Content-Encoding Decode Failed • Gzip Content-Encoding Decode Failed \u2013 Checking Error • Gzip Content-Encoding Decode Failed \u2013 Data Error • Gzip Content-Encoding Decode Failed \u2013 Decoding Error • Identity Content-Encodings Received • Identity Content-Encoding Received • Identity Content-Encoding Decode Successful • Identity Content-Encoding Decode Failed • Identity Content-Encoding Decode Failed \u2013 Checking Error • Identity Content-Encoding Decode Failed \u2013 Data Error • Identity Content-Encoding Decode Failed \u2013 Decoding Error • Chunked Transfer-Encoded Responses Received • Chunked Transfer-Encoding Decode Successful • Chunked Transfer-Encoding Decode Failed • Content-MD5 Response Received • Content-MD5 Check Successful • Content-MD5 Check Failed • Custom-MD5 Response Received • Custom76. Custom-MD5 Check Failed • MD5 Check Successful
Server Statistics	• HTTP Requests Received • HTTP Requests Successful • HTTP Requests Failed • HTTP Requests Failed (404) • HTTP Requests Failed (50x) • HTTP Requests Failed (Write Error) • HTTP Sessions Rejected (503) • HTTP Session Timeouts (408) • HTTP Transactions Active • HTTP Bytes Received • HTTP Bytes Sent • HTTP Cookies Received • HTTP Cookies Sent • HTTP Cookies Received with Matching Server ID • HTTP Cookies Received with Nonmatching Server ID
Relevant Standards	• RFC 1945, Hypertext Transfer Protocol - HTTP/1.0 • RFC 2616, Hypertext Transfer Protocol - HTTP/1.1 • RFC 2246, The TLS Protocol Version 1.0

Another feature of the Integrated Test System is the ability to verify the characteristics and performance metrics described there are SSLv2.0 based connections, and TLS v1.0 SSLv3.0 allowing detailed characterization of HTTPS transactions.

The Integrated Test System also supports sophisticated methods of discharges, such as jDownloader. For non-standard option that some were not supported natively by the web traffic simulator could be used as described Replay Application to generate the traffic and check the performance of the DUT.

IP Telephony

The Integrated Test System, in its basic configuration, can also generate IP calls using the most popular signaling protocols such as SIP (item 925-3502).

It supports both audio calls and video calls. The audio / video traffic is encoded using the RTP and reports associated to each call quality are created including performance metrics (packet loss, delay, jitter) and VoIP specific (MOS) (Item 925-3106).

Table 18.
Specifications of the Traffic Simulator, Telephony / SIP based IP Video Telephony.

Features	• UDP and TCP Transport • Support for IP video phone to emulate voice calls with video • MOS scores reported on a per call basis • Support for user-defined authentication and registration parameters • Support for sequence generators to easily create large number of VoIP calls using unique user credentials • Ability to use audio files as payload in a voice session • Ability to create realistic and complex call flows • Support for path confirmation using synthetic data or DTMF tones • Statistics reported on an average and for each call • Emulate jitter buffers in packets or duration in ms • Ability to adjust the size of the jitter buffer in real-time • Customizable SIP header order • Option to create specific rules to control handling of SIP messages • Option to configure SIP User Agent Server for Stateless operation
Emulation	• SIP User Agent (UA) emulation with signaling and RTP media
Codecs	• G.711, G.729A, G.729B, G.726, G.723.1
Client Statistics	• SIP calls initiated • SIP calls completed • SIP calls active • SIP INVITE client transactions initiated • SIP INVITE client transactions succeeded • SIP INVITE client transactions failed • SIP INVITE client transactions failed (TIMER B) • SIP INVITE client transactions failed (TRANSPORT ERROR) • SIP INVITE client transactions failed (TRANSACTION TIMEOUT TIMER) • SIP INVITE client transactions failed (5xx) • SIP NON-INVITE client transactions initiated • SIP NON-INVITE client transactions succeeded • SIP NON-INVITE client transactions failed • SIP NON-INVITE client transactions failed (TIMER F) • SIP NON-INVITE client transactions failed (TRANSPORT ERROR) • SIP INVITE requests sent • SIP ACK requests sent • SIP BYE requests sent • SIP REGISTER requests sent • SIP INVITE messages retransmitted • SIP NON-INVITE requests retransmitted • SIP INVITE requests unexpected • SIP ACK requests unexpected • SIP BYE requests unexpected • SIP CANCEL requests unexpected • SIP UNKNOWN messages unexpected • SIP UNKNOWN requests unexpected

Table 18.
Specifications of the Traffic Simulator, Telephony / SIP based IP Video Telephony.

	• SIP 1xx responses expected • SIP 1xx responses unexpected • SIP 2xx responses expected • SIP 2xx responses unexpected • SIP 3xx responses expected • SIP 3xx responses unexpected • SIP 4xx responses expected • SIP 4xx responses unexpected • SIP 5xx responses expected • SIP 5xx responses unexpected • SIP 6xx responses expected • SIP 6xx responses unexpected • RTP Bytes Sent • RTP Packets Sent • RTP Tx Jitter (ns) • RTP Tx Packets Dropped • RTP Dropped Packets • RTP Bytes Received • RTP Packets Received • RTP Payload Bytes Received • RTP Bad Packets Received • RTP Lost Packets Received • RTP Mis-ordered Packets Received • RTP Duplicate Packets Received • RTP Jitter Min • RTP Jitter Max • RTP Packets With Jitter Up To 1ms • RTP Packets With Jitter Up To 3ms • RTP Packets With Jitter Up To 5ms • RTP Packets With Jitter Up To 10ms • RTP Packets With Jitter Up To 20ms • RTP Packets With Jitter Up To 40ms • RTP Packets With Jitter More Than 40ms • RTP DTMFs Detected • RTP Good DTMF Sequences Detected • RTP Bad DTMF Sequences Detected • RTP Packets Dropped By Jitter Buffer • RTP MOS Average Instant • RTP MOS Worst Instant • RTP MOS Best Instant • RTP MOS Worst • RTP MOS Best • RTP MOS Average Per Call • RTP MOS Worst Per Call • RTP MOS Best Per Call • RTP Calls With Continuous Path Confirmation • RTP Calls With Interrupted Path Confirmation • RTP Calls Without Path Confirmation • SIP Bytes Transmitted • SIP Bytes Received • SIP Signaling UDP Packets Transmitted • SIP Signaling UDP Packets Received • RTP Path Confirmation Status • RTP MOS • RTP Worst MOS • RTP Best MOS

Table 18.
Specifications of the Traffic Simulator, Telephony / SIP based IP Video Telephony.

	• RTP Bytes • RTP Packets • RTP Bad Packets • RTP Lost Packets • RTP Missorder Packets • RTP Duplicate Packets • RTP Packets With Jitter Up To 1ms • RTP Packets With Jitter Up To 3ms • RTP Packets With Jitter Up To 5ms • RTP Packets With Jitter Up To 10ms • RTP Packets With Jitter Up To 20ms • RTP Packets With Jitter Up To 40ms • RTP Packets With Jitter More Than 40ms • RTP Average Jitter (ns) • RTP Min Jitter (ns) • RTP Max Jitter (ns) • RTP DTMFs Detected • RTP Good DTMF Sequences Detected • RTP Bad DTMF Sequences Detected • RTP Packets Dropped By Jitter Buffer
Server Statistics	• SIP calls received • SIP calls completed • SIP calls active • SIP INVITE server transactions received • SIP INVITE server transactions succeeded • SIP INVITE server transactions failed • SIP INVITE server transactions failed (TIMER H) • SIP INVITE server transactions failed (TRANSPORT ERROR) • SIP NON-INVITE server transactions received • SIP NON-INVITE server transactions succeeded • SIP NON-INVITE server transactions failed • SIP NON-INVITE requests retransmitted • SIP REGISTER Requests sent • SIP 1xx responses expected • SIP 2xx responses expected • SIP 3xx responses expected • SIP 4xx responses expected • SIP 5xx responses expected • SIP 6xx responses expected • SIP 300-699 responses retransmitted • SIP INVITE requests expected • SIP ACK requests expected • SIP BYE requests expected • SIP 1xx responses sent • SIP 1xx responses unexpected • SIP 2xx responses sent • SIP 2xx responses unexpected • SIP 3xx responses sent • SIP 3xx responses unexpected • SIP 4xx responses sent • SIP 4xx responses unexpected • SIP 5xx responses sent • SIP 5xx responses unexpected • SIP 6xx responses sent • SIP 6xx responses unexpected

Table 18.
Specifications of the Traffic Simulator, Telephony / SIP based IP Video Telephony.

	• SIP INVITE requests unexpected • SIP ACK requests unexpected • SIP BYE requests unexpected • SIP CANCEL requests unexpected • SIP UNKNOWN requests unexpected • SIP UNKNOWN messages unexpected • RTP Bytes Sent • RTP Packets Sent • RTP Tx Jitter (ns) • RTP Tx Packets Dropped • RTP Dropped Packets • RTP Bytes Received • RTP Packets Received • RTP Payload Bytes Received • RTP Bad Packets Received • RTP Lost Packets Received • RTP Missordered Packets Received • RTP Duplicate Packets Received • RTP Jitter Min • RTP Jitter Max • RTP Packets With Jitter Up To 1ms • RTP Packets With Jitter Up To 3ms • RTP Packets With Jitter Up To 5ms • RTP Packets With Jitter Up To 10ms • RTP Packets With Jitter Up To 20ms • RTP Packets With Jitter Up To 40ms • RTP Packets With Jitter More Than 40ms • RTP DTMFs Detected • RTP Good DTMF Sequences Detected • RTP Bad DTMF Sequences Detected • RTP Packets Dropped By Jitter Buffer • RTP MOS Average Instant • RTP MOS Worst Instant • RTP MOS Best Instant • RTP MOS Worst • RTP MOS Best • RTP MOS Average Per Call • RTP MOS Worst Per Call • RTP MOS Best Per Call • RTP Calls With Continuous Path Confirmation • RTP Calls With Interrupted Path Confirmation • RTP Calls Without Path Confirmation • SIP Bytes Transmitted • SIP Bytes Received • SIP Signaling UDP Packets Transmitted • SIP Signaling UDP Packets Received • RTP Path Confirmation Status • RTP MOS • RTP Worst MOS • RTP Best MOS • RTP Bytes • RTP Packets • RTP Bad Packets • RTP Lost Packets • RTP Missorder Packets • RTP Duplicate Packets

Table 18.
Specifications of the Traffic Simulator, Telephony / SIP based IP Video Telephony.

	• RTP Packets With Jitter Up To 1ms • RTP Packets With Jitter Up To 3ms • RTP Packets With Jitter Up To 5ms • RTP Packets With Jitter Up To 10ms • RTP Packets With Jitter Up To 20ms • RTP Packets With Jitter Up To 40ms • RTP Packets With Jitter More Than 40ms • RTP Average Jitter (ns) • RTP Min Jitter (ns) • RTP Max Jitter (ns) • RTP DTMFs Detected • RTP Good DTMF Sequences Detected • RTP Bad DTMF Sequences Detected • RTP Packets Dropped By Jitter Buffer
Relevant Standards	• RFC 3261, SIP: Session Initiation Protocol • RFC 2327, SDP • RFC 2976, The SIP INFO method • RFC 3262, Reliability of Provisional Responses in Session Initiation protocol (SIP) • RFC 3264, An Offer/Answer Model with the Session Description Protocol (SDP) • RFC 3265, Session Initiation Protocol (SIP)-Specific Event Notification • RFC 3311, The Session Initiation Protocol (SIP) UPDATE Method • RFC 3515, The Session Initiation Protocol (SIP) Refer Method • RFC 3428, Session Initiation Protocol (SIP) Extension for Instant Messaging • RFC 3966, The tel URI for Telephone Numbers • RFC 3550, RTP: A Transport Protocol for Real-Time Applications • RFC 3551, RTP Profile for Audio and Video Conferences with Minimal Control • RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals • RFC 3389, Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)

In addition to the features described that apply to the SIP signaling protocol, the Test System supports other signalling forms such as Skinny (Item 925-3503), H.323 (Item 925-3504) H.248/MEGACO (item 925-3505). For each of these protocols, there is an specific support of metrics that characterize its performance.

Unicast and Multicast Video

The Integrated Test System can generate flows of multicast video traffic suitable for IPTV applications (item 925-3105). Unicast video applications suitable for video services on demand (VoD) are also supported natively by the Integrated Test System (Item 925-3104). As in other applications, both servers are tested IPTV / VoD and customers.

It support most common codecs today, including MPEG-2, MPEG-4, H.264 and WM9. The video programs can be both standard definition (SD) and High Definition (HD).

Among the metrics of interest include the MDI, QoS statistics, video MOS, EPSNR and latency parameters in channel changing (zapping delay) associated with IGMP and MLD protocols. In VoD applications latency statistics in the channel change are being replaced by latency play / pause associated with the protocol RTSP.

With the aim of maximizing the ability to make measurements on video signals are included in the basic Test System setup options required for advanced analysis of video quality. In the video advanced statistical metrics include MOS-V absolute and MOS-V relative. For both, include means computed for all packets from the start of flow and interval statistics can be initialized by the user.

Table 19.
Technical specifications of the IPTV traffic simulator.

Features	• Mix IPTV, voice and data traffic in the same test • Support for RTP/UDP or UDP for video transmission • Near wire-speed video transmission with very low jitter • Channel change performance testing with latency measurements on a per-subscriber basis • Support for interleaving multicast and VoD commands on client • Support for user-specified video files or synthetic data using IxLoad servers • Channel viewing sequences such as sequential, concurrent and random for user-realism • Channel viewing profiles based on statistical distribution models for prime-time emulation • Support for channel switch delay emulation • Customizable client headers • Configurable TOS and DSCP bit settings • Video quality metrics to measure both transmission quality using MDI and perceptual video quality • Video quality metrics on a per-subscriber basis • Per video stream statistics such as jitter, latency, loss, bit rates • MPEG level statistics on number of I, B and P frames received per video stream • Support for jitter buffer emulation to model and characterize STB behavior • Emulation of video on demand (VoD) subscribers • Emulation of high-performance VoD servers • Real-time streaming protocol (RTSP) over IPv4 and IPv6 network • RTP media streams over raw UDP and RTP/UDP transport
Video Codecs	• MPEG2, MPEG4, H.264 and others over MPEG2-TS streams • MPEG4, H.264 and WM9 • Support for native MPEG4 transport of High definition streams • Support for single-program (SPTS) and multi-program transport streams (MPTS)
Client Statistics	• Active Multicast Channels • Multicast Channels Requested • Multicast Requests Successful • Multicast Requests Failed • VoD Streams Played • IGMP Queries Rcvd • IGMP Reports Sent • IGMP Leaves Sent • MLD Queries Rcvd • MLD Reports Sent • MLD Leaves Sent • Join Latency • Leave Latency • Channel Switch Latency • RTSP Bytes Sent • RTSP Bytes Received • RTSP Packets Sent • RTSP Packets Received • RTSP Presentations Active • RTSP Presentations Playing • RTSP Presentations Paused • RTSP Presentations Requested • RTSP Presentation Requests Successful • RTSP Presentation Requests Failed • RTSP DESCRIBE Sent • RTSP SETUP Sent • RTSP PLAY Sent • RTSP PAUSE Sent • RTSP TEARDOWN Sent • RTSP DESCRIBE Successful • RTSP SETUP Successful • RTSP PLAY Successful • RTSP PAUSE Successful

Table 19.
Technical specifications of the IPTV traffic simulator.

	• RTSP TEARDOWN Successful • RTSP DESCRIBE Failed • RTSP SETUP Failed • RTSP PLAY Failed • RTSP PAUSE Failed • RTSP TEARDOWN Failed • Average Play latency • Average Pause latency • Video Simulated Users • Frame Stats Disabled • Quality Metrics Disabled • Total Bytes Rcvd • Total packets Rcvd • Total Loss • Unexpected UDP Packets Received • RTP Packets • Global Jitter • Jitter less than 50 us • Jitter between 50 - 100 us • Jitter between 100 - Overload Packets Dropped • Total RTP Packets Lost • Total Out Of Order RTP Packets Rcvd • Total Duplicate 500 us • Jitter between 500 us - 2 ms • Jitter between 2 - 5 ms • Jitter between 5 - 10 ms • Jitter greater than 10 ms • Inter Packet Arrival Time between 0 - 2 ms • Inter Packet Arrival Time between 2 - 5 ms • Inter Packet Arrival Time between 5 - 10 ms • Inter Packet Arrival Time between 10 - 25 ms • Inter Packet Arrival Time between 25 - 50 ms • Inter Packet Arrival Time between 50 - 100 ms • Inter Packet Arrival Time between 100 - 200 ms • Inter Packet Arrival Time between 200 - 500 ms • Inter Packet Arrival Time greater than 500 ms • Active • Stream Name • Transport • Video Codec • Stream Bit Rate • MDI-DF • MIN MDI-DF • MAX MDI-DF • AVG-MDI-DF • MDI-MLR • Bytes • I Frames Rcvd • P Frames Rcvd • B Frames Rcvd • Packets • Loss • Jitter • Inter Pkt Arrival Time • Min Inter Pkt Arrival Time • Control Sent

Table 19.
Technical specifications of the IPTV traffic simulator.

	• Max Inter Pkt Arrival Time • Packet Latency (ns) • Min Packet Latency (ns) • Max Packet Latency (ns) • Join Latency (ms) • Join Latency (ns) • Leave Latency (ms) • Channel Switch Latency • Channel Gap Duration • Channel Overlap Duration • Data Rcvd • RTP Packets Lost • RTP Packets Out of Order • Jitter Buffer Packets Accepted • Jitter Buffer Packets Early • Jitter Buffer Packets Discarded • Jitter Buffer Packets Discarded (Underrun) • Jitter Buffer Packets Discarded (Overrun) • MOS_V • Video Service Quality • Gap Video Service Quality • Burst Video Service Quality • Burst Count • Avg Gap Len (Pkts) • Avg Burst Len (Pkts) • Degradation (Loss) • Degradation (Discard) • Degradation (Video Codec) • Current Jitter Buffer Packets Accepted • Current Jitter Buffer Packets Discarded • Current JB Packets Lost • Current Video Service Quality • Unicast Bytes • Unicast Packets • Multicast Bytes • Multicast Packets • Unicast Join Latency • Multicast Join Latency • D-A overlap • A Server Channel Requested • A Server Requests Successful • A Server Requests Failed • D Server Requested • D Server Requests Successful • D Server Requests Failed • D Server Requests Failed - Control • D Server Requests Failed - Data • V Server Requested • V Server Requests Successful • V Server Requests Failed • Active D Server Playing • Active V Server Playing • Active V Server Paused • Active A Server Streams

Table 19.
Technical specifications of the IPTV traffic simulator.

Server Statistics	• Total Streams Playing • No of Multicast Streams Playing • No of VoD Streams Active • No of VoD Streams Playing • No of VoD Streams Paused • No of Multicast Streams Played • No of VoD Streams Played • Total Streaming Bit Rate • Multicast Streams Bit Rate • VoD Streams Bit Rate • RTSP Presentations Received • RTSP Presentations Successful • RTSP Presentations Failed • RTSP Bytes Sent • RTSP Bytes Received • RTSP Packets Sent • RTSP Packets Received • RTSP Play Latency (ms) • RTSP Commands Received • RTSP DESCRIBE Received • RTSP SETUP Received • RTSP PLAY Received • RTSP PAUSE Received • RTSP TEARDOWN Received • RTSP Response Codes Sent (2xx) • RTSP Response Codes Sent (3xx) • RTSP Response Codes Sent (4xx) • RTSP Response Codes Sent (5xx) • RTSP Response Codes Sent (6xx-1xxx) • Total Bytes Sent • Total Packets Sent • Tx Jitter (ns) • Tx Packets Dropped • V Server requests Received • V Server requests Successful • V Server requests Failed • V Server requests Failed - Bandwidth • V Server requests Failed - Port Overload • V Server requests Failed - Other Reasons • D Server requests Received • D Server requests Successful • D Server requests Failed • D Server requests Failed - Bandwidth • D Server requests Failed - Port Overload • D Server requests Failed - Other Reasons • Active A Server Streams Playing • Active D Server Streams Playing • Active V Server Streams • Active V Server Streams - Playing • Active V Server streams - Paused
Relevant Standards	• RFC 2326 - Real Time Streaming Protocol (RTSP) • RFC 3550 - RTP: A Transport Protocol for Real-Time Applications • RFC 3376 - Internet Group Management Protocol, Version 3 • RFC 4445 - A Proposed Media Delivery Index (MDI) • RFC 2250 - RTP Payload Format for MPEG1/MPEG2 Video • RFC 2327 - SDP: Session Description Protocol

The MOS-V on the perceptual quality is estimated considering the effects of encoding processes, the impact of disruptions to the IP layer and the effectiveness of recovery mechanisms used by the transmission system. However, do not take into account the image size, resolution, frame rate or scanning method (interlaced or progressive).

Some video formats offer better quality than other intrinsically. For example the quality of a coded signal in HD is higher than the one in SD, one with a frame rate of 60 Hz is more than a 30 Hz and a 1080p format is better than one with 1080i or 720p. The Absolute MOS-V takes into account these factors and considered in the calculation of quality.

In addition to the metric MOS-V, the video analytic provides bandwidth statistics, metrics specific to Tables I, P and B, analysis of MDI, and EPSNR.

Table 20.
Advanced Analysis of Video Traffic.

Video and Bandwidth Information (per Stream)	• Video Codec: The video CODEC type for the video stream. • Frame Rate: The video frame rate, in frames per one thousand seconds. e.g. 29,970 equals 29.97 frames per second. • Frame Width: The video frame image width, in pixels. • Frame Height: The video frame image height, in pixels. • Average Video Bandwidth (kbps): The average video bandwidth, measured over the interval, excluding transport packet header overhead and error correction/retransmission. • Peak Video Bandwidth (kbps): The peak video bandwidth, measured during a 1-second window, excluding transport packet header overhead and error correction/retransmission.
Absolute and Relative MOS (per Stream)	• Average Absolute MOSV: Absolute MOS for the video stream, averaged over the statistics Update Interval configured on the video client Statistics Options tab. • Average Relative MOSV: Relative MOS for the video stream, averaged over the statistics Update Interval configured on the video client Statistics Options tab • Average Absolute MOSA: Absolute MOS for the audio stream, averaged from stream start to the current time. • Average Absolute MOSAV: Audio/video (multimedia) MOS for the stream, averaged from stream start to the current time. • Interval Absolute MOSV: Absolute MOS for the video stream, averaged over the statistics Update Interval configured on the video client Statistics Options tab. • Interval Relative MOSV: Relative MOS for the video stream, averaged over the statistics Update Interval configured on the video client Statistics Options tab.
Frame Statistics (per Stream)	• I Frames Rcvd: A count of the number of stream video Iframes received during the interval configured on the video client Statistics Options tab. • P Frames Rcvd: A count of the number of stream video P-frames received during the interval configured on the video client Statistics Options tab. • B Frames Rcvd: A count of the number of stream video B-frames received during the interval configured on the video client Statistics Options tab. • I Frames Impaired: A count of the number of stream video Iframes that were impaired during the interval configured on the video client Statistics Options tab. • P Frames Impaired: A count of the number of stream video P-frames that were impaired during the interval configured on the video client Statistics Options tab. • B Frames Impaired: A count of the number of stream video B-frames that were impaired during the interval configured on the video client Statistics Options tab. • Inter I Frame Gap: The average I-frame inter-arrival jitter, in milliseconds. The inter-arrival jitter is computed relative to the expected arrival time based on the frame rate.
Scene Analysis (per Stream)	• Scene Detail Level: The instantaneous amount of detail, expressed on a scale of 0 (little detail) to 100 (maximum detail). • Scene Motion Level: The instantaneous amount of motion, expressed on a scale of 0 (no motion) to 100 (continuous motion). • Scene Panning Level: The instantaneous amount of panning, expressed on a scale of 0 (no panning) to 100 (continuous panning).

Table 20.
Advanced Analysis of Video Traffic.

Transport Metrics (per Stream)	• MPEG2 TS Loss: Number of MPEG-2 Transport Stream packets lost. • MDI-DF: Media Delay Index \u2013 Delay Factor experienced on stream. • MDI-MLR: Media Delay Index - Media Loss Rate experienced on stream. • PPDV: The instantaneous Packet-to-Packet Delay Variation (RFC3550), in milliseconds, sampled at the end of the interval configured on the video client Statistics Options tab.
Jitter Buffer (per Stream)	• JB Packets Rcvd: The number of stream transport packets received by the jitter buffer. • JB Packets Lost: The number of stream transport packets lost in the network. • JB Packets Discarded: The number of stream transport packets discarded by the endpoint due to late arrival.
Video Description (per User)	• Codec Type: The video CODEC type for the video stream. • GOP Structure: The GOP structure expressed as a series of 'I', 'B', 'P' characters describing the frame type series in the structure. • Avg GOP Length: The average GOP length, in frames. • Avg Inter I Frame Gap (Frames): The average gap, in frames, between I frames (excluding the I-frames) • Frame Width: The video frame image width, in pixels. • Frame Height: The video frame image height, in pixels. • Frame Rate: The video frame rate, in frames per one thousand seconds \u2013 e.g. 29,970 equals 29.97 frames per second. • RTP Clock Rate: Clock rate used for RTP connection. • Video PID: Package Identifier used on video stream. • Audio PID: Package Identifier used on audio stream.
MOS (per User)	• Average Absolute MOS V: he average absolute video stream MOS over the stream duration. • Average Relative MOS V: The average relative video stream MOS over the stream duration. • Average MOS A: The average audio stream MOS over the stream duration. • Average MOS AV: The average audio/video stream MOS over the stream duration. • Interval Absolute MOS V: The absolute stream instantaneous video MOS sampled at the end of the interval configured on the video client Statistics Options tab. • Interval Relative MOS V: The relative stream instantaneous video MOS sampled at the end of the interval configured on the video client Statistics Options tab. • EPSNR (ATIS): The Estimated Peak Signal to Noise Ratio (PSNR) calculated according to ATIS specifications.
Frame Statistics (per User)	• I Frames Rcvd: The number of video I-frames received. • I Frames Impaired: The number of video I-frames impaired by packet loss or discard. • P Frames Rcvd: The number of video P-frames received. • P Frames Impaired: The number of video P-frames impaired by packet loss or discard. • B Frames Rcvd: The number of video B-frames received. • B Frames Impaired: The number of video B-frames impaired by packet loss or discard. • SI Frames Rcvd: The number of video SI-frames received. • SI Frames Impaired: The number of video SI-frames impaired by packet loss or discard. • SP Frames Rcvd: The number of video SP-frames received. • SP Frames Impaired: The number of video SP-frames impaired by packet loss or discard. • I Frame Pkts Rcvd: The number of transport packets received containing video I-frame information. • I Frame Pkts Lost: The number of transport packets lost containing video I-frame information. • I Frame Pkts Discarded: The number of transport packets discarded due to late arrival containing video I-frame information. • P Frame Pkts Rcvd: The number of packets received containing video P-frame information. • P Frame Pkts Lost: The number of transport packets lost containing video P-frame information. • P Frame Pkts Discarded: The number of transport packets discarded due to late arrival containing video P-frame information. • B Frame Pkts Rcvd:The number of packets received containing video B-frame information. • B Frame Pkts Lost: The number of transport packets lost containing video B-frame information. • B Frame Pkts Discarded The number of transport packets discarded due to late arrival containing video B-frame information.

Table 20.
Advanced Analysis of Video Traffic.

Stream and Frame Bandwidth (per User)	• Avg Video Bw (Kbps: The average video bandwidth, measured during a one second window, excluding transport packet header overhead and error correction/retransmission. • Peak Video Bw (Kbps): The peak video bandwidth, measured during a one second window, excluding transport packet header overhead and error correction/retransmission. • Avg Audio Bw (Kbps): The average audio bandwidth, measured during a one second window, excluding transport packet header overhead and error correction/retransmission. • I Frame Avg Video Bw (Kbps): The average bandwidth of I-frame transport packets received, in bits/second. • I Frame Peak Video Bw (Kbps): The maximum bandwidth of I-frame transport packets received, in bits/second. • P Frame Avg Video Bw (Kbps): The average bandwidth of P-frame transport packets received, in bits/second. • P Frame Peak Video Bw (Kbps): The maximum bandwidth of P-frame transport packets received, in bits/second. • B Frame Avg Video Bw (Kbps): The average bandwidth of B-frame transport packets received, in bits/second. • B Frame Peak Video Bw (Kbps): The maximum bandwidth of B-frame transport packets received, in bits/second.
Frame and Packet JItter (per User)	• Frame Inter Arrival Jitter (ms): The average frame inter-arrival jitter, in milliseconds. The inter-arrival jitter is computed relative to the expected arrival time based on the frame rate. • I Frame Inter Arrival Jitter (ms): The average I-frame inter-arrival jitter, in milliseconds. The inter-arrival jitter is computed relative to the expected arrival time based on the frame rate. • PPDV (ms): The stream transport Packet-to-Packet Delay Variation (RFC3550), in Q4 fixed-point milliseconds. • PPDV (ms): The maximum stream transport Packet-to-Packet Delay Variation (RFC3550), in Q4 fixed-point milliseconds.
Jitter Buffer (per User)	• JB Packets Rcvd: The number of stream transport packets received. • JB Packets Lost: The number of stream transport packets lost in the network. • JB Packets Discarded: The number of stream transport packets discarded by the endpoint due to late arrival.
Scene Analysis (per User)	• Scene Detail Level: The instantaneous amount of detail, expressed on a scale of 0 (little detail) to 100 (maximum detail). • Scene Motion Level: The instantaneous amount of motion, expressed on a scale of 0 (no motion) to 100 (continuous motion). • Scene Panning Level: The instantaneous amount of panning, expressed on a scale of 0 (no panning) to 100 (continuous panning).

Table 20.
Advanced Analysis of Video Traffic.

Global Video Quality Statistics	• I Frames Rcvd: The number of video I-frames received. • P Frames Rcvd: The number of video P-frames received. • B Frames Rcvd: The number of video B-frames received. • I Frames Impaired: Number of I-frames impaired due to packet loss or discards. • P Frames Impaired: Number of P-frames impaired due to packet loss and/or discards. This does not include frames impaired due to error propagation through temporal reference. • B Frames Impaired: Number of B-frames impaired due to packet loss and/or discards. This does not include frames impaired due to error propagation through temporal reference. • Avg Current Absolute MOS V: Absolute MOS for all the video streams, averaged from stream start to the current time. • Avg Current Relative MOS V: Relative MOS for all the video streams, averaged from stream start to the current time. • Avg Current MOS AV: Audio/video (multimedia) MOS for all streams, averaged from stream start to the current time. • Avg Current MOS A: Absolute MOS for all the audio streams, averaged from stream start to the current time. • Avg Complete Absolute MOS V: Absolute MOS for all completed video streams, averaged across all streams. • Avg Complete Relative MOS V: Relative MOS for all completed video streams, averaged across all streams. • Avg Complete MOS AV: Audio/video (multimedia) MOS for all completed streams, averaged across all streams. • Avg Complete MOS A: Audio MOS for all completed streams, averaged across all streams. • Avg Interval Absolute MOS V: Absolute MOS for all video streams, averaged over the statistics Update Interval configured on the video client Statistics Options tab. • Avg Interval Relative MOS V: Relative MOS for all video streams, averaged over the statistics Update Interval configured on the video client Statistics Options tab.
Global Video Bandwidth Statistics	• Avg Video BW: The average video bandwidth, in bits/second, measured over the interval, excluding transport packet header overhead and error correction/retransmission. • I Frame Avg Video BW: The average bandwidth of I-frame video content transmitted, in bits/second. • P Frame Avg Video BW: The average bandwidth of P-frame video content transmitted, in bits/second. • B Frame Avg Video BW: The average bandwidth of B-frame video content transmitted, in bits/second.

5. VoIP Traffic Generation and Analysis Subsystem

The Traffic Generation and Analysis Subsystem (TGAS) provides test traffic when needed and performs different kinds of analysis of traffic generated by the own TGAS or other Test System subsystems. The TGAS is able to generate an analyses both signalling (SIP) and packetized voice (G.711, G.729,... over RTP).

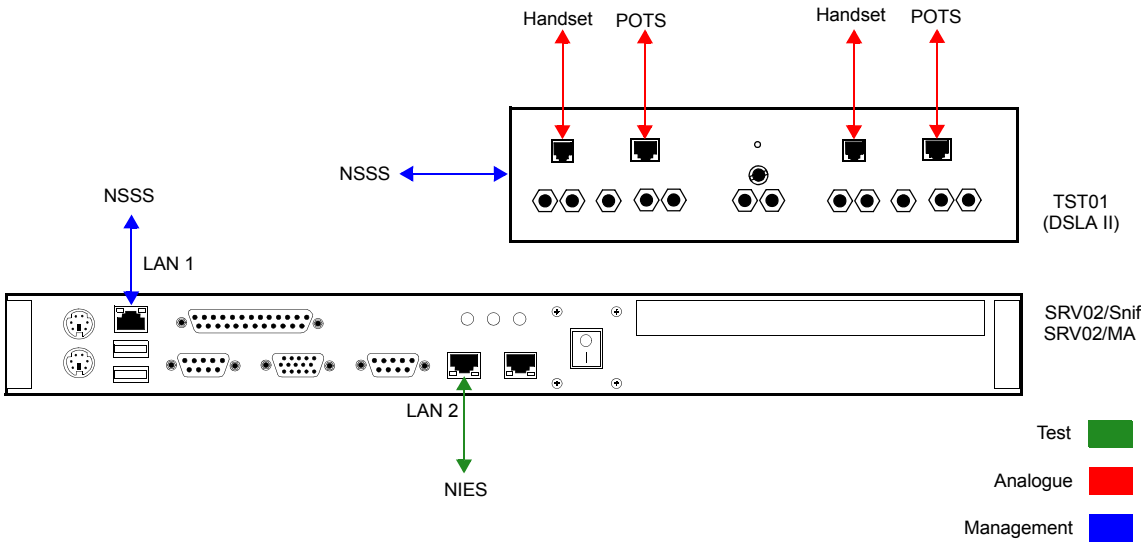

Figure 6. *The TGAS is made up by two different devices, the TST01 generates different kinds of test analogue audio signals. The SRV02/MA is a software installed in the SRV02 that generates ana analyses test VoIP signals.*

The TGAS is made up of different software and hardware components:

- *DSLAII*: The Digital Speech Level Analyzer (DSLA) II provides a pair of stable, high quality analogue interfaces to test any device able to generate telephone speech signals such as (but not limited to) VoIP telephones. The DSLA II can either replace the whole customer premises equipment or just the telephone handset. The first setup is suitable to test network performance and the second one is the best suited to check end-to-end quality provided by the network and the end user equipment. The DSLA provides two RJ-11 and two RJ-22 ports. The RJ-11 ports are needed when the whole telephone is going to be replaced by the test set and the RJ-22 can be used when it is wanted to keep the telephone in the network but the handset is going to be replaced by the test equipment. The DSLA II provides an Ethernet management interface that enables the equipment to interact with other test or management devices.
- *VN*: The Virtual Node (VN) is the IP counterpart of the DSLA II. The VN generates packetized speech signals and signalling on demand. The VN can send/receive signals to/from remote VoIP devices or testers such as the DSLA II. The VN is a software that is installed in the SRV02 and it does not require any specific configuration.
- *MultiDSLA*: The MultiDSLA manages tests and collects result data from all the DSLA II and VN installed in the network. It can also be used for result post-processing and graphical presentation, report generation and test scheduling. The MultiDSLA also provides basic signalling analysis of SIP calls between the test devices and the DUT. The MultiDSLA is a software installed in the SRV02.
- *SIPp*: This is SIP generation/analysis tool developed by Hewlett-Packard and currently distributed free of charge and available for download from the Internet. SIPp is able to generate almost any custom SIP message and emulate complex protocol transactions. SIPp is based on a powerful scripting language specially designed for flexible generation of custom SIP messages. Usage of SIPp has been kept to the minimum

possible. Transactions based on real SIP devices such as the VGW01 or reference VoIP phones is preferred to the synthetic transactions generated with SIPp. However, SIP has been used when the Test System devices exhibit a not-standard or buggy behavior. All scripts needed to work with SIPp are provided and the way they are used is addressed in detail in every test where they are used.

- *Sniffers*: SIP signalling and other complementary protocols (DNS, DHCP,...) can be analyses by means a traditional IP sniffer. Sniffers capture the traffic they see in the network and presents the contents in a structured way. The IP traffic sniffer installed in the TGAS will not normally be used in the acceptance suite. IP packet analysis will be performed by the VGW01. This is the preferred method because the VGW01 has some packet contents display modes that is well suited for message oriented protocols like SIP. Other two sniffers are used in the Test System, *ngrep* for packet capture in the Test System console and *WireShark* for the SRV02. Both are free and can be downloaded and installed from the Internet.

  All the testing tools mentioned are installed in two different boxes, the TST01 (DSLAII) and the SRV01 (VN, MultiDSLA, WireShark). Both the TST01 and the SRV01 are connected to the management VLAN (VLAN 103) in the NSSS and furthermore, the SRV01 LAN 2 interface is connected to the NIES to enable controlled impairment emulation over the test traffic.

Digital Speech Level Analysis

A remarkable feature of the TGAS is that all possible voice analysis if performed at the speech level. That means that IP packets are not directly involved in such analysis and only the speech that results from the encoding and transmission processes is used for testing. This, has two important advantages:

- Coding and decoding processes are all taken into account in the measure results. All from the IP packet segmentation, reassembly and buffering to analogue voice-band signal amplification is considered by the testing procedure. This would not be possible with the more simple packet-based analysis performed by other testing tools.
- Any speech signal, and not only VoIP signals are suitable for the testing. This includes speech signals generated by cellular telephones (GSM, UMTS,...), fixed line POTS/ISDN telephones or VoIP services over wireless links (IEEE 808.11 for example). Although there is no specific test in the acceptance suite to check performance of these devices, it is straightforward and cost less to extend the already defined QoE tests to some or all these devices.

  Most of the tests described in the acceptance suite require close collaboration between the TGAS and the other subsystems that made up the Test System. In a typical setup for a VoIP telephone, the telephone handset is replaced with the TST01. The TST01 provides RJ-22 ports that are commonly used for connections between the handset and the telephone (but other ways to connect the DUT to the TST01 are also possible). The DUT (the VoIP telephone) encodes the audio received from the TST01 and delivers the corresponding VoIP packets to the Test System network. The DUT also receives VoIP packets coming from the Test System, decodes them and forwards them to the TST01 for speech level analysis. The packets received/sent by the DUT are routed by the NSSS (usually through the NIES) to other Test System devices like the SRV02 where they can be processed by software like the VN.

  All the information collected by the TST01 or the SRV02/VN is delivered to the MultiDSLA for post-processing. To report results to the MultiDSLA, the TST01 uses the management Ethernet interface and the VN uses the same IP network that it uses to send/receive test data. In the particular case of the Test System, the VN and the MultiDSLA are installed in the same machine and therefore no physical IP link needs to be created between them.

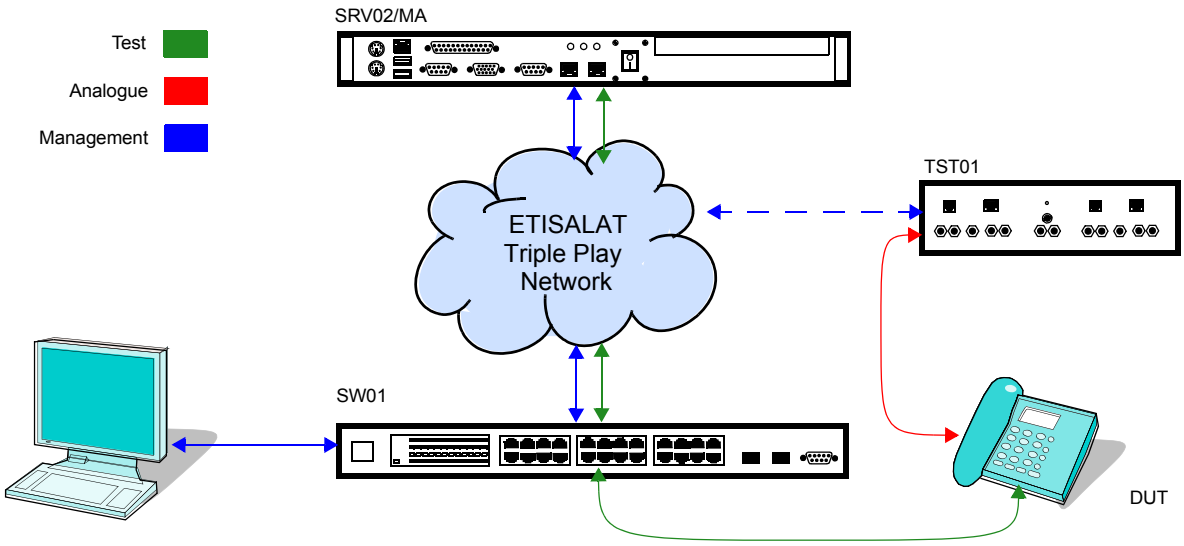

Figure 7. *Typical test setup that makes use of the TGAS.*

In the acceptance Test System, the MultiDSLA is provided with a simple configuration for a VN interface (VN 1) and two DSLA interfaces (DSLA 1 and DSLA 2). The former corresponds with the VN installed in the SRV02. The DSLA interfaces are the DSLA Channel A and Channel B. Tests of the acceptance suite always use the DSLA Channel 1 (DSLA 1 node).

The information processed by MultiDSLA is available from the Test System console by means a remote desktop connection established through the management VLAN.

Traffic Sniffers

The TGAS uses to different sniffers, *WireShark* and *ngrep* but none of them is the preferred sniffing tool. Most of the tests of the acceptance suite use the SIP sniffer provided by the VGW01 in the NSSS. *WireShark* and *ngrep* are only used when for some reason the VGW01 sniffer cannot be used.

- *WireShark*: is a widely distributed software. It is free of charge and it can be installed over Linux or Windows platforms. It is installed in the SRV01 in the Test System. It is mainly used to monitor the activity of the DNS server and their clients. The detailed usage of this tool is described in the test suite.
- *ngrep*: is a command line tool for Linux. It is in fact installed in the system console. (not in the TGAS). This sniffer is well suited to capture message-based protocols like SIP. It is used when the VGW01 is replaced by SIPp to generate highly customized signalling. In this case *ngrep* analyses the SIP transactions between SIPp and the DUT. The *ngrep* tool requires administrator rights to be used. Details about usage of *ngrep* is given within the acceptance suite.

SIPp Scripts

SIPp is a tool for generation and analysis of custom SIP signalling and media. SIPp is useful when it is wanted to generate uncommon SIP messages or even messages containing controlled errors in SIP headers and payloads. All messages that cannot be generated by the Test System in any way, are generated with SIPp. SIPp is not in-

stalled in the TGAS, it is a software that has to be compiled and installed in the system console. The SIPp version that has been used for the Test System is a CVS version (*sipp.2009-07-29.tar.gz*). The software has to be compiled from the source files. Support for authentication and PCAP play has to be selected before starting the compilation process:

```
[user@host~] make pcapplay_ossl
```

More details about compilation and installation procedures, along with usage description and applications of this tool is found in the documentation.

SIP is based in an scripting language based on the XML standard. That means that SIPp scripts are XML files with an special syntax suited for SIP message generation, manipulation an analysis. The Test System includes all the scripts necessary to run all the tests included in the acceptance suite. Some of the scripts have been designed with a particular test in mind and others are more general and can be used in several tests.

- *incomingcall-180nosdp.xml*: This script is for the test 8382-01. It generates a *180 Ringing* message without SDP payload during a SIP transaction. In this script SIPp acts as the UAS while de DUT is the UAC.
- *incomingcall-180sdp.xml*: This script is for the test 8383-01. It generates a *180 Ringing* message with an SDP payload during a SIP transaction. In this script SIPp acts as the UAS while de DUT is the UAC.
- *incomingcall-183nosdp.xml*: This script is for the test 8380-01. It generates a *183 Session Progress* message with SDP payload during a SIP transaction. In this script SIPp acts as the UAS while de DUT is the UAC.
- *incomingcall-183sdp.xml*: This script is for the test 8381-01. It generates a *180 Ringing message* without an SDP payload during a SIP transaction. In this script SIPp acts as the UAS while de DUT is the UAC.
- *incomingcall-with-proxiauth.xml*: Implements a proxy-authentified INVITE. In this script, SIP is the UAS and the DUT is the UAC. It is worth noting that the script does not really authenticates the UAC. It generates the message any proxy would issue to authenticate users but it does not implement the authentication algorithm. This is however enough for the purposes of the test.
- *incoming-register-noauth.xml*: This is an script that accepts and replies registration requests from remote SIP devices. In this script, SIPp is also the UAS and the DUT the UAC.
- *outgoingcall-with-reinvite.xml*: This script calls a remote SIP device and starts a media session and before the end of the media session finishes it attempts to issue a re-INVITE message. In this script SIP is the UAC and the remote device is the UAS. This script is to be used in test 11490-01 (session refresh).
- *register-with-authentication.xml*: This script attempts to register SIPp in a remote SIP registrar. The script will reply to a register authentication request from the registrar with a correct response to authentication challenge. In the authentication script, SIPp acts as the UAC and the registrar is the UAS.

Remote Access

Access to the SRV01 and the software installed in this server is performed from the system console through the *rdesktop* tool already described in previous sections. Access to the TST01 is indirectly done by means rdesktop and the MultiDSLA software installed in the SRV01.

6. PERFORMANCE TESTING LAYER 2 / LAYER 3

In addition to its ability to test the traffic of one or more users Integrated Test System provides the ability to generate traffic generated layer 2 or layer 3 to stress the DUT / SUT and verify its operation in extreme load conditions. Specifically, we support the tests defined in RFC 2544, RFC 2889 (Item 928-0102), RFC 3511 (Item 928-0203) and RFC 3918 (item 928-0243).

The RFC 2544 is a standard widely used to characterize the performance of network elements. RFC 2544 tests supported by the Integrated Test System is the Back to Back, Frame Loss, Latency and Throughput.

Table 21.
Description of the parameters supported in RFC 2544 tests

Back to Back Test	*The Back to Back test determines the maximum time that the DUT can receive and forward without frame loss. Frames are sent at a user-specified rate, generally the maximum theoretical rate based on the speed of the port. The results of the test show the number of back-to-back frames obtained for each frame size and the average and total back-to-back frames for all the trials. Frames can be MAC only, IPv4 or IPv6. Results include total back to back frames without loss for each frame size.*
Frame Loss Test	*The Frame Loss test determines how many frames the DUT loses at various frame rates. The number of frames to transmit is specified along with the initial transmit rate, and the percentage decrease in the frame rate (the Granularity parameter) for each iteration. Frames can be MAC only, IPv4, IPv6 (with or without Extension Headers) or IPv4/IPv6 mixture. Results include frame loss at various rates for each frame size.*
Latency Test	*The Latency test determines the latency of the DUT. In the Latency test, frames are transmitted for a fixed duration. Frames are transmitted and tagged with timestamps. Latency is calculated by subtracting the transmit timestamp from the receive timestamp. Frames can be MAC only, IPv4, IPv6 (with or without Extension Headers) or IPv4/IPv6 mixture. Results include latencies for each frame size and the average latencies for all the trials.*
Throughput Test	*The Throughput test determines the maximum rate at which the DUT receives and forwards frames without any frame loss. Frames are initially sent at a user-specified rate and a binary search algorithm is used to obtain a rate at which the DUT does not lose frames. Frames can be MAC only, IPv4, IPv6 (with or without Extension Headers) or IPv4/IPv6 mixture. Results include: throughput rates in frames per second obtained for each frame size.*

Table 22.
RFC 2544 test (OPTIONAL)

ID	*MAC*	*IPv4*	*IPv6*
Back to back	*X*	*X*	*X*
Frame Loss	*X*	*X*	*X*
Latency	*X*	*X*	*X*
Throughput	*X*	*X*	*X*

RFC 2889 is an extension to RFC 2544. It applies to DUT / SUT using Ethernet framing. Many of the tests defined by RFC 2889 apply only to multi items.

Table 23.
Description of the parameters supported in RFC 2889 tests (OPTIONAL)

Address Cache Size Test	*The Address Cache Size test uses a binary search to determine the size of the address table for each port or for an entire switch. Beginning at half the size of the initial user-specified table size, frames are transmitted at a user-specified frame rate to see if the DUT has properly learned all of the addresses. If no frame loss and no flooding is detected, the address table size is increased and the test is repeated in a binary fashion until the address table size is determined. Results include maximum number of MAC addresses supported by DUT.*

Table 23.
Description of the parameters supported in RFC 2889 tests (OPTIONAL)

Address Rate Test	*The Address Rate test determines the maximum no drop rate by transmitting frames with multiple addresses based on the initial table size at the user-specified frame rate. The number of frames received on each receive port is counted and the receive rate calculated. The rates are compared and a binary search algorithm is used to calculate the address learning rate of the DUT. Results include address learning rate of DUT.*
Broadcast Rate Test	*The Broadcast Rate test determines the maximum rate at which the DUT receives and forwards broadcast frames without any loss of frames. A binary search algorithm is used to obtain a rate at which the DUT does not lose frames within an acceptable rate window. The results of the test show the throughput rates obtained for each frame size. Results include broadcast throughput rate per packet size.*
Back Pressure Test	*The Back Pressure test determines the congestion control back-pressure exerted when multiple ports are transmitting to a single port in order to overload the port. The results of the test show the number of received frames, number of collision frames and the percent loss of frames obtained for each frame size. Results include collision frames, receive frames, percent frame loss.*
Head of Line Blocking Test	*The Head of Line Blocking test determines the added delay on an non-congested output interface whenever frames are received from an input interface which is also attempting to forward frames to a congested output interface. The results of the test show the number of received frames, number of collision frames and the percent loss of frames obtained for each frame size.* *Results include collision frames, receive frames, percent frame loss.*
Frame Error Filtering Test	*The Frame Error Filtering test determines if the DUT correctly filters frames with certain types of errors such as undersized frames, oversize frames, CRC errors, fragments, alignment errors and dribble errors. The results of the test show the type of error transmitted, the number of transmit frames, inter-frame gap and the number of frames in error for each frame size. Results include type of error, IFG, number of frames in error.*
Fully Meshed Test	*The Fully Meshed test determines the total number of frames that the DUT can handle when it receives frames on all of its ports. The results of the test show the total number of frames transmitted from all the ports and the total number of frames received on all the ports, and the percent loss of frames obtained for each frame size. Dual-mesh capability that supports two separate sets of ports running independently. Results include percent frame loss, average latency, frame loss.*
Many to Many Mesh Test	*The Many to Many Mesh test determines the frame loss from the total number of frames transmitted from all the ports and the total number of frames received on all the ports. There are two types of many-to-many mesh tests available: round-robin and peak load. Dual-mesh capability that supports two separate sets of ports running independently. Results include frame loss, average latency.*
Many to One Throughput Test	*The Many to One Throughput test determines the maximum rate at which the DUT receives and forwards frames from many interfaces to one interface without any loss of frames. A binary search algorithm is used to obtain a rate at which the DUT does not lose frames within an acceptable rate window. The results of the test show the throughput rates obtained for each frame size. Results include throughput per frame size.*
One to Many Throughput Test	*The One to Many Throughput test determines the maximum rate at which the DUT receives and forwards frames from one interface to many interfaces without any frame loss. A binary search algorithm is used to obtain a rate at which the DUT does not lose frames within an acceptable rate window. This window is the rate within one inter-frame gap of the initial transmit rate. The results of the test show the throughput rates obtained for each frame size.* *Results include throughput per frame size.*
Partially Meshed Test	*The Partially Meshed test determines the maximum throughput of the DUT by sending frames from multiple transmit ports to multiple receive ports in a mesh fashion, where the transmit ports do not receive and the receive ports do not transmit. Results include throughput per frame size.*

Table 24.
Support for RFC 2889-based testing

ID	MAC	IPv4	IPv6
Address Cache Size	*X*		
Address Rate	*X*		
Broadcast Rate	*X*		
Back Pressure	*X*	*X*	*X*
Head of Line Blocking	*X*	*X*	*X*

Table 24.
Support for RFC 2889-based testing

Frame Error Filtering	*X*		
Fully Meshed	*X*	*X*	*X*
Many to Many Mesh	*X*	*X*	*X*
Many to One Tput	*X*	*X*	*X*
One to Many Tput	*X*	*X*	*X*
Partially meshed	*X*	*X*	*X*

Contrary to what happens with the standards RFC 2544 and RFC 2889 RFC 3 918 is applicable only when the DUT / SUT is IP. Specifically, the RFC 3918 measures the performance of multicast processing performed by the DUT / SUT. This includes support for IGMP and performance and overall treatment is done in multicast groups.

Table 25.
Description of the parameters supported in RFC 3918 tests

Accumulated Test	*The Accumulated test determines the DUT's throughput when clients join a large number of groups at a certain rate. The test stresses the DUT by forcing it to rapidly update its IGMP/MLD group cache and then forward traffic to all the groups. This test functions in a similar way to the Distributed test, but differs from it in that each receive port joins every group, resulting in the same multicast traffic going out multiple ports. Results include frame loss per group.*
Aggregated Test	*The aggregated test measures a DUT\u2019s ability to maintain IP multicast traffic throughput when a fixed number of clients joined via IGMP/MLD are re-distributed among fewer subnets. To simulate this, the test reduces the number of ports it transmits to while keeping the number of clients fixed. This test uses a one-to-many traffic map and requires at least four ports; one to transmit and three to receive. Results include frame loss, leaked frames per group.*
Burdened Group Join Delay Test	*This interaction test determines how long it takes a DUT to register multicast clients to a new group or to a group that already exists in the DUTs forwarding table, while forwarding meshed traffic as an interacting factor. This test uses two maps: a one-to-many traffic map for multicast traffic as in the other tests (it is a manual map) and, a many-to-many traffic map for the unicast traffic as burdening traffic (it has to be fully meshed so this is an automatic map). Results include transmit and receive frames per port, Group join delay time (minimum/maximum and average values), burden rate, number of burden ports.*
Burdented Latency Test	*This interaction test measures the DUTs ability to forward multicast traffic with acceptable latency while forwarding meshed traffic as an interacting factor. The test differs from the Latency test in that it forces the DUT to perform extra processing of packets while multicast traffic is being forwarded for latency measurements. This test uses two maps: a one-to-many traffic map for multicast traffic as in the other tests (it is a manual map) and, a many-to-many traffic map for the unicast traffic as burdening traffic (it has to be fully meshed so this is an automatic map). Results include Frame loss per port, transmit and receive frames per port, average latency per multicast group address, burden rate, number of burden ports, average latency per multicast group address.*
Distributed Test	*The Distributed test determines the DUT\u2019s ability to forward traffic to the correct multicast clients on a per-port basis. In this test, each receive port IGMP/MLD joins a different set of multicast groups. The test sends validation traffic to all the groups to calculate the throughput. This test functions in a similar way to the Accumulated test, but differs from it in that each receive port joins a different set of groups, resulting in different streams of multicast traffic going out different ports of the DUT. Results include frame loss, leaked frames.*
Group Capacity Test	*The Group Capacity test determines the maximum number of multicast groups that a DUT can register, using IGMP/MLD, and forward multicast frames to. This test requires at least two ports; one to transmit and one to receive, and uses a one-to-many traffic map. Results include group capacity counts.*
Group Join Delay Test	*The Group Join Delay test determines how long it takes a DUT to register multicast clients. The test measures the elapsed time between the time a DUT receives a group of IGMP/MLD Join requests and the time the multicast clients begin receiving traffic for the groups they joined. The test can optionally increase or decrease the frame rate to record how different frame rates affect the delay between joining a group and receiving traffic. This test requires a minimum of four ports; one to transmit, at least two to receive, and one to act as the timing port which allows the test to derive timing information for the validation traffic. Results include join delay per group.*

Table 25.
Description of the parameters supported in RFC 3918 tests

Group Leave Delay Test	*The Group Leave Delay test determines how long it takes a DUT to remove a client from its multicast table. The test measures the elapsed time between the time a DUT receives a group of IGMP/MLD Leave requests and the time the multicast clients stop receiving traffic for the groups they left. The test can optionally increase or decrease the frame rate to record how different frame rates affect the delay between leaving a group and the cessation of traffic. This test requires a minimum of four ports; one to transmit, at least two to receive, and one to act as the timing port which allows the test to derive timing information for the validation traffic. Results include leave delay per group.*
Latency Test	*The Latency test measures the average latency of multicast frames sent to clients on multiple subnets (ports). The Latency test reveals how much processing overhead the DUT requires, on average, to forward multicast frames. This test differs from the Min Max Latency test in that it transmits special tagged frames and records only their latency, while the Min Max Latency test calculates the average latencies of all the frames it sends. Results include latency per group.*
Mesh Test	*The Mesh test measures the DUTs throughput per port while it is receiving and forwarding frames on all its ports. This test is similar to the RFC2889 Fully Meshed test, except that this test uses multicast frames.* *This test requires a minimum of three ports. This test uses a many-to-many traffic map; each port transmits to, and receives from, all other ports. Results include frame loss.*
Throughput NDR Test	*The Throughput No Drop Rate test allows you to calculate the maximum DUT throughput for IP Multicast traffic using either a binary search or a linear search, and to collect Latency and Data Integrity statistics. This test differs from the others in the suite in that it supports PIM and IGMP/MLD and is considered the most flexible test in the suite. Results include NDR throughput, latency, data integrity.*
Mixed Class Throughput Test	*The Mixed Class Throughput test measures a DUTs throughput when it is receiving and forwarding a mixture of unicast and multicast frames simultaneously on multiple ports. For the unicast traffic, the test uses a one-to-one traffic map. For the multicast traffic, the test uses a one-to-many map and requires at least three ports. Results include throughput, frame loss.*
Scale Group Test	*The Scale Group Test determines a DUTs multicast throughput using a fixed quantity of traffic and increasing or decreasing the numbers of the multicast groups the traffic is sent to. This test can reveal how rapidly the DUTs multicast throughput increases or decreases based on the number of groups it is transmitting to. This test uses a one-to-many traffic map requiring a minimum of three ports. Results include throughput, frame loss.*
Tunneling Throughput Test	*This test determines the multicast throughput when a DUT or a set of DUTs interfaces are acting as tunnel endpoints. Throughput represents the highest rate at which the DUT receives and forwards frames with loss lower than or equal to the specified value for loss tolerance. In this test, encapsulation or tunneling refers to a packet that contains an unsupported protocol feature in a format that is supported by the DUT. A one-to-many traffic mapping is used, with a minimum of two ports required. This test supports only one traffic map which means that only one transmit port must be set. Results include Originating Frame Size, Offered Frames, Tx Frames/Rx Port, Rx Frames, Frame Loss (%), Forwarding Rate (%Tx Line).*

Table 26.
RFC 3918 tests

ID	*MAC*	*IPv4*	*IPv6*
Accumulated	*n.a.*	*X*	*X*
Aggregated	*n.a.*	*X*	*X*
Distributed	*n.a.*	*X*	*X*
Group capacity	*n.a.*	*X*	*X*
Group Join Delay	*n.a.*	*X*	*X*
Group Leave Delay	*n.a.*	*X*	*X*
Latency	*n.a.*	*X*	*X*
Mesh	*n.a.*	*X*	*X*
Burdened Group Join Delay	*n.a.*	*X*	*X*
Mixed Class Throughput	*n.a.*	*X*	*X*
Scale Group	*n.a.*	*X*	*X*
Tunneling Throughput	*n.a.*	*X*	*X*

Table 26.
RFC 3918 tests

Throughput NDR	*n.a.*	*X*	*X*
Burdened Latency	*n.a.*	*X*	*X*

RFC 3511 applies to firewalls and NAT devices that perform translations or NAPT. They are characterized aspects of great importance when the DUT is a subscriber router. For example, the maximum number of TCP connections supported, the maximum rate of TCP connection establishment and processing of fragmented IP datagrams.

Table 27.
Description of the parameters supported in RFC 3511 tests.

Denial of Service Handling Test	*The Denial of Service Handling test determines the effect of a denial of service attack on a DUT TCP connection establishment rate. The iterative process of the cMax. TCP Connection Establishment Rate is running with the denial of service attack enabled and disabled. The difference between results is the effect of the denial of service attack on the DUTs performance. The DoS attack exploits the TCP three way handshake mechanism by sending TCP SYN attack segments. Results include maximum TCP connection rates per port.*
Illegal Traffic Handling Test	*To characterize the behavior of the DUT/SUT when presented with a combination of both legal and illegal traffic. Illegal traffic does not refer to an attack, but traffic which has been explicitly defined by a DUT access control list to drop the illegal traffic flow. The test uses a Max HTTP Transaction Rate test, but mixes legal and illegal traffic in a user definable percentage. Results include maximum HTTP transaction rates per port.*
IP Fragmentation Handling Test	*The IP Fragmentation Handling test sends packets which have been fragmented due to crossing a network that supports a smaller MTU (Maximum Transmission Unit) than the actual IP packet. This fragmentation may require the firewall to perform re-assembly prior to the rule set being applied. This test will focus on determining how the additional processing associated with the re-assembly of the packets has on the forwarding rate of the DUT/SUT. This test employs two types of traffic: HTTP 1.1 as non-fragmented traffic and UDP/IP fragmented packets. Results include average transfer rate of non-fragmented transactions and number of requests sent and received.*
IP Throughput Test	*The Throughput NDR test uses network layer traffic (stream based) to determine the maximum packet No Drop Rate that can pass through the device or system under test. A binary search with multiple iterations is used to determine this maximum. Multiple packet sizes can be configured. Results include total packets transmitted and received, frame loss, and a packets per second rate.*
Latency Test	*The Latency test is used determine and compare the latency of both connectionless network layer traffic and HTTP application layer traffic. Latency is measured for each type of traffic so that comparisons can be made. In addition, line rate and packet sizes can be configured. Results include the maximum and average latency per port.*
TCP Connections Capacity Test	*The TCP Connections Capacity test determines the maximum total number of TCP connections the device or system under test can support. The test uses a binary search routine that begins with an initial number of attempted concurrent connections, if successful the test iterates by doubling the concurrent attempted connections until the maximum number of successful connections no longer meets the search tolerance that has been defined. Results include the maximum number of concurrent connections per port.*
HTTP Maximum Transaction Rate Test	*The HTTP Maximum Transaction Rate test uses a binary search routine to determine the maximum transaction rate for an HTTP requested object traversing the firewall. To achieve it a set of http client(s) are configured to initiate simultaneously connections to the http server(s). Results include attempted/maximum/average transaction rates per second and total HTTP requests and responses received.*
HTTP Transfer Rate Test	*The HTTP Transfer Rate test determines the transfer rate of HTTP requests per second traversing the device or system under test. A definable number of clients are configured along with a Requests per Connection value and an object size. The test calculates the aggregate transfer rate in bits per second. Results include Transfer Rate (bits/sec), and HTTP requests sent and received.*
TCP Maximum Connections Rate Test	*The TCP Maximum Connections Rate test finds the maximum TCP connection establishment rate the DUT can handle. To validate the connections, the application performs http transactions from the configured client networks to the server networks. The test employs an iterative search algorithm to determine the maximum rate and the attempted connection rate is varied from iteration to iteration. Results include attempted and actual connection rate (TCP connections/sec.), HTTP requests/responses completed, and total bytes sent and received.*

Other Services and Protocols

Other protocols supported in the base configuration are TCP Integrated Test System (Item 925-3300), Telnet (Item 925-3300), SSH (Item 925-3112), RADIUS (Item 925-3113) and TFTP (item 925-3138), FTP (Item 925-3300), WAP (Item 925-3144).

Table 28.
Traffic generation in RFC 3511 tests

ID	*HTTP*	*Binary Search*	*Connection Oriented*	*Connectionless*
DOS Handling test	*X*	*X*	*X*	-
Illegal Traffic Handling test	*X*	*X*	*X*	-
IP Fragmentation test	*X*	-	*X*	*X*
IP Throughput test	-	*X*	-	*X*
Latency test	*X*	-	*X*	*X*
TCP Connection Capacity test	*X*	*X*	*X*	-
HTTP Max. Transaction Rate test	*X*	*X*	*X*	-
HTTP Transfer Rate test	*X*	-	*X*	-
HTTP Max. Connection Rate test	*X*	*X*	*X*	-

7. IP Network impairments Generation

Network Impairments Generation

Application traffic it is always subject to a series of disturbances that degrade it. These disturbances often result from congestion-related phenomena.

The Integrated Test System includes ALBEDO Net.Storm. This device can generate disturbances in the IP / Ethernet layer at speeds of up to 1 Gbit/s over electrical and optical interfaces. Among the disturbances supported include:

- Constant delay, variable from uniform distribution, exponential distribution variable, delay associated with a shaping filter (shaping). The equipment can be adjusted to force the order of the frames or to vary according to the programmed delay statistics
- Deterministic packet loss (single event, variable burst length), random loss with a configurable rate, based on a Gilbert-Elliot model of two states. Also supports the shaping filter emulation (policing).
- Packet error rate deterministic or random with configurable
- Duplication at a deterministic or random rate defined by user

Another important feature is the ability Net.Storm set filters so that the perturbations are only applied to some of the traffic or even apply different rates to different fractions of disruption of traffic. Filters can be based on MAC addresses, IP addresses, protocol, DSCP, VLAN or port TCP / UDP.

Simulation of actual networks conditions

NetStorm generates those perturbances typical of IP and Carrier Ethernet to test applications, devices and protocols that should be tolerant with packet delay, jitter, loss, duplication, reordering, error and bandwidth variations.

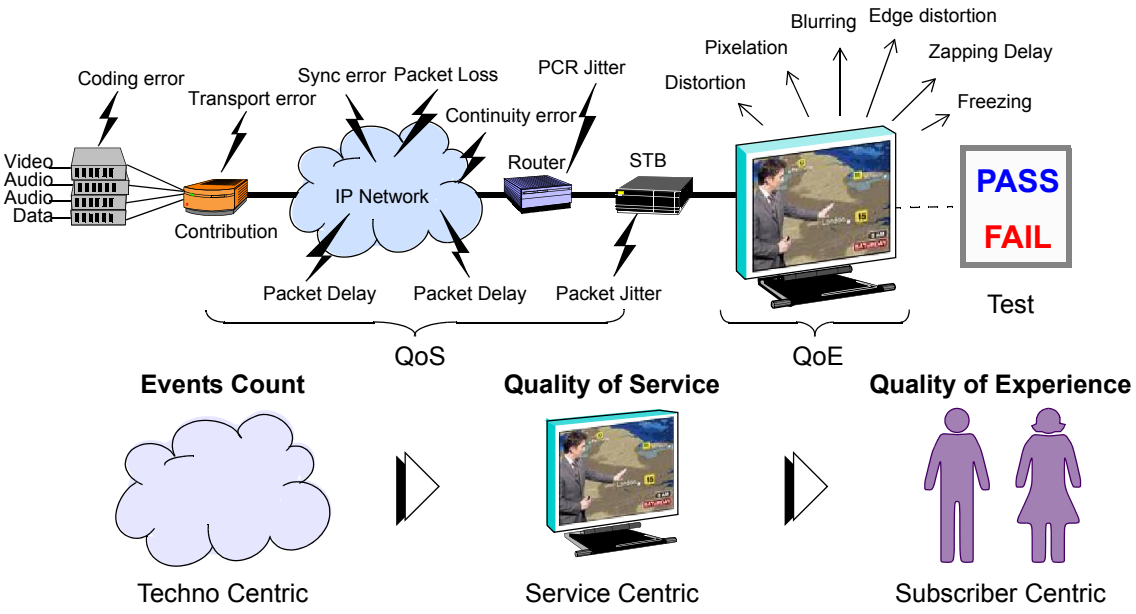

Figure 8. *Disruptions can occur anywhere on the network and determine the quality of the network service (QoS) that affect the experienced quality (QoE).*

The diversity of underlying technologies, and the adaptive behavior of applications requires more sophisticated testing technologies. NetStorm facilitates the verification of new applications, services and nodes through emulation of the real nature of IP networks. NetStorm enables engineers to model and modify arbitrary performance dynamics including packet delay, jitter, bandwidth limitations, congestion, packet loss, errors and duplication on live IP packets.

The degradation will be used to test the response of the services and also terminals using a signal that can be manipulated its delay, jitter, packet loss and other events. The effects of degradation is measured later and its effects will be measurable in the quality metrics used for this purpose as TR 1001 209, Video MOS, MDI and other.

Figure 9. *ALBEDO Net.Storm is an independent and connectable to any point in the network with Ethernet interface. It comes in two formats, carrier-class rack as a hand-held battery-operate.*

Conformity procedures

The process followed to accept a device (DUT) or system (SUT), or solve a problem of implementation has always been an important task, but when the new solution is based on the IP protocol formal verification of the solution becomes essential.

IP networks are ubiquitous, heterogeneous, and are now capable of delivering any type of traffic quality IP connections can vary in terms of bandwidth, latency, error rate and loss rates, and these results are usually asymmetric (up / downstream). Moreover, the dynamics of QoS can vary widely, due to congestion at peak times, and routing failures.

QoS requirements

Applications must make a more intelligent use of available network resources just as the proper conduct of the DUT / SUT can not be defined in simple deterministic and adaptive protocols that can interact in a way that is not easily detectable or predictable.

Net.Storm

NetStorm solution addresses this growing diversity of the network and to emulate real traffic conditions and thus to test nodes, protocols and terminals used in the new IP applications. NetStorm is largely independent of all systems and nodes. It is also effective and very accurate since the disturbances generated are based on hardware so it has full capacity to emulate any system Ethernet / IP and common network generate effects such as packet loss, duplication, delay, congestion, packet errors and bandwidth limitations.

It is designed to provide sufficient capacity and performance play a wide range of network behavior up to 1 Gbps with accuracy rates always better than 1 ms. When operating at the Ethernet layer NetStorm can emulate the critical features from end to end performance imposed by the core routers and switches support for any underlying network.

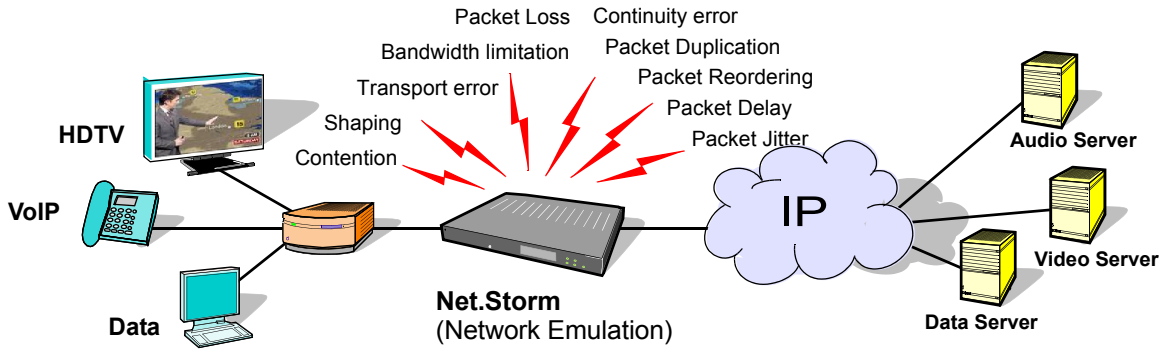

Figure 10. *ALBEDO Net.Storm is the selected network impairments generator that allows to Implement the network*

Hardware Performance

NetStorm is inserted between two Ethernet segments pass-thru mode, while in bi packet transfer. The configuration of the emulation can be set independently for 16 separate streams that can be filtered by several criteria including MAC, IP, TCP / UDP or user of the mask.

The result is a realistic simulation and controlled 100% of those obtained under real conditions WAN networks that have been detected in living. The same conditions are capable of being reproduced in order to observe the behavior of applications such as VoIP, IPTV, VoD, these nodes we gateways, routers and set top boxes, and link protocols such as SIP, MEGACO, H.323, and criticism and access networks.

(Find out more info in ALBEDO.Net.Storm.pdf)

8. TESTING AT THE GPON ACCESS NETWORK

When quality degrades until certain level and testing results tell that the Contribution, Transport and CPE network are in good shape then is the moment to verify if the FTTH access network is the cause of the problems. After the making an analysis of the network and users' computers come to the conclusion that the problem is in GPON access network.

The analysis of the FTTH network is made by means of GPON tester capable to be connected at any point of the access network supporting testing suites to verify elements such as ONT, OLT and Splitters and, in addition, capable to drop and send the user Triple Play traffic to be ana lysed including VoIP, IPTV and HSI.

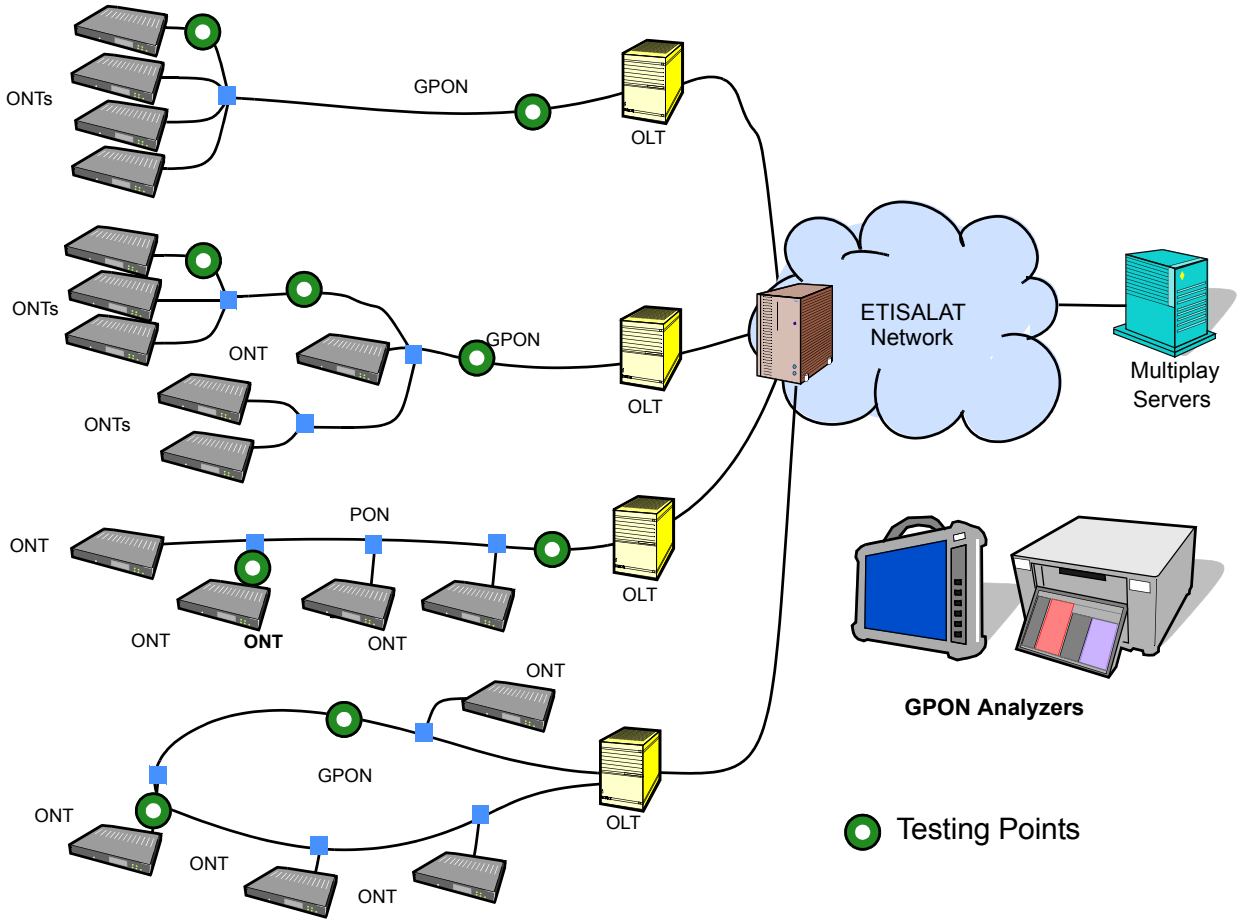

Figure 11. *Any GPON topologies that could be used by ETISALAT can be analysed with GPON 4000.*

Some of the functionalities of the GPON 4000 are explained herein below.

Real time user traffic extraction

GPON analyzer extracts decrypted user traffic in real time and at Ethernet layer. This traffic is made available at the 10/100/1000BaseT interface for its monitoring and upper layer analysis by external network analyzing tools and/or other application tools. Its hardware decoder fully supports AES automatic decryption combined with FEC encoding

Service regeneration and QoS Evaluation

GPON analyzer can regenerate services established over a PON network. i.e. Multicast video can be sniffed & reassembled in real time and watched on GPON analyzer screen. This feature is perfect to evaluate QoS and QoE of configured services over a PON.

Problems in PON and GPON networks

With the aim of reducing the ONTs price it is important that any OLT is capable to interact with any ONT regardless its manufacturer. However, GPON has a number of intrinsic characteristics that could make difficult the interoperability among manufacturers:

- Commercial implementations from earlier versions of the standard.
- Problems during the activation process.
- Misinterpretation of the standard.
- OMCI, a very broad standard.
- Heterogeneity among operators.

Furthermore, the structure of a PON network is a fiber that is divided over using optical power dividers or splitters. At this point it appears the concept of *degree of splitting*" defined as the number of divisions that suffers the fiber to reach an ONT. The degree of splitting indicates that the percentage of optical power arriving to an ONT. Attenuation in a GPON circuit can be very high due to the sum of fibre splitting, connectorization (Insertion loss), fusion splice, and distance in the fiber, and thus, some of the network active elements operate under stress conditions.

All these factors imply a great challenge in the deployment of GPON networks.

Transparent analysis and Capture

The GPON 4000 transparently analyze traffic within a FTTH network. Moreover, its automatic calibration and built-in touch screen into a high performance chassis, makes it possible with just one click to have a full capture of GPON network traffic.

The capture can be very long (e.g. 30 minutes) and exportable to be used out of the GPON equipment.

Network analysis and evaluation

The analysis software interprets the captured data and translates it into a graphical and categorized format that can be easily used for in-depth analysis of GPON protocol compliance, interoperability evaluation, bandwidth assignments and field deployment troubleshooting.

Applications

Interoperability is a significant requirement of the industry to gain confidence on the of Gigabit-capable Passive Optical Networks (GPON). Moreover, lack of maturity of this technology has moved the ITU-T focus on verifying correct deployments at the OMCI[1] Implementers' guide. As often happens with standards, OMCI was written with a lot of compromises and facilities, then when it come to interoperability, issues rise.

In other words, GPON analyzer is a tool for engineers planning the deployment of FTTH networks. This instrument will help them not only to run Interoperability test, but also for product certification, diagnose and troubleshooting. It is the best tool in market to verify TR-156 / TR-167 compliance of GPON networks.

World leader operators and manufacturers all over the world are already using GPON analyzer to perform:

- Verification of
- Interoperability Test between different ONT / OLT vendors
- FTTH Deployment
- Maintenance and Troubleshooting
- Assessment of compliance of OLT / ONU / ONT
- Analysis of GPON protocols from the Ethernet

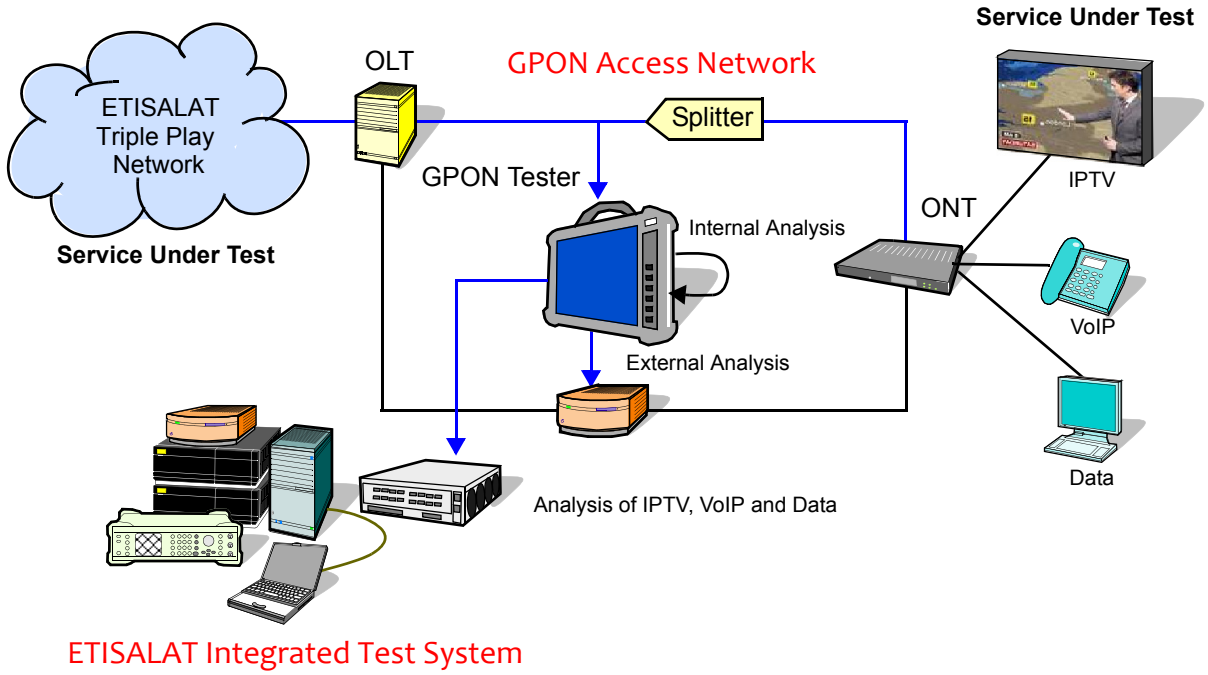

Figure 12. *Albedo GPON analyser can capture and analyse traffic in real time and can drop data for further analysis with other applications and instruments.*

1. OMCI: Optical Network Termination (ONT) Management and Control Interface

9. PHYSICAL MEDIA DISTURBANCES (OPTIONAL)

This test is intended to execute acceptance test of CPE equipment such as routers and STB connected by means of Wi-Fi, PLC or Coax under physical media perturbances.

Test Requirements

In an ideal situation the Integrated System Test should be performed in stressful conditions coaxial Media, PLC and WiFi to be held in Faraday cages in the Test System using attenuators and RF generators.

In ALBEDO are convinced that it is sufficient with only one disturbance generator that can be used for any of the physical transmission media including Coaxial, PLC, UTP, or Wireless. The only difference is the fact that the disturbance should to be conducted or radiated (depending on the media), and therefore only involves using a cable or antenna, connectors and adapters for each medium of transmission.

Figure 13. *Signal Generator to 6GHz is the source of problems sorting and Faraday cage bag format for entering the DUT. This system comes complete with accessories such as antennas, couplers and cables that allow for verification testing and tolerance in a totally controlled environment.*

We understand the difficulty of having all these facilities are highly specialized as available only to specialized laboratories and disposal. For the Integrated Test System to realize a subset of the tests proposed (see Annex 2).

The equipment under test is placed in a suitcase as the CMW-Z10/-Z11 which has a useful range up to 6 GHz frequency that exceeds the range needed to generate interferences in the bands of GSM, UMTS, DVB, WiFi, WLAN, Bluetooth ® and GPS interference are to be tested. The suitcase has a Double N interface where you connect the generator and antenna interference generation. The DUT, such as a router, is installed inside the bag and passes through a wall is connected to the network to remain in service.

In all cases the engineer selects the test to run, program the level of interference with the proper parameters and observes the consequences of disturbances in the levels of quality (TS2, IP, MOS, MDI, etc.) of the signal with digital information.

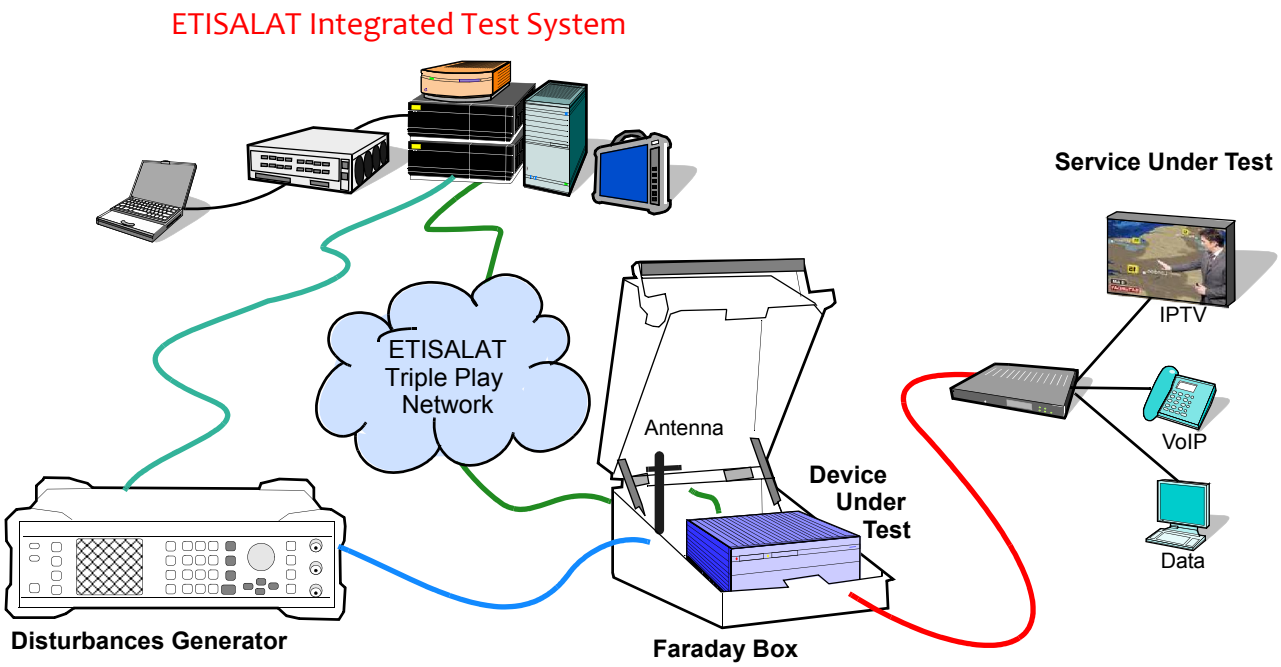

Figura 14. *An interfering signal in the frequency band in which you want to create disturbance in the physical environment. The equipment being measured (DUT) is inserted into the suitcase of Faraday. If it were a router, as the case illustrated in Figure, first access network to the test system and on the other client computers using the appropriate physical environment Coax, UTP or PLC. In the case of WiFi transmitter and receiver must be placed inside the Faraday Box.*

Automatic control

In the case of disturbances of the physical medium of transmission, the test system must be prepared to grow by incorporating automatic control of new elements involved in this function that have GPIB interface for remote control, and has conventional Ethernet interfaces (TCP / IP) and USB.

Testing of PLC system

In these trials will be necessary the following scenarios:

- Without disturbance
- Interference between PLC produced on other frequencies in the same medium (frequency narrowband PLC)
- Interference between PLC supported by the team due to other signals that share the medium (frequency narrowband PLC, PLC frequency bandwidth used by other teams)

WiFi Testing Systems

In these trials will be necessary to teste the following scenarios:

- Without disturbance.
- Disturbances in the air due to obstacles between transmitter and receiver.

- Disturbances in the air environment due to radiated signals at frequencies of GSM transmission standard, WiFi, DVB-T and other sources of interference to 6GHz

  The air attenuation will be minimal, if receiver and transmitter are in front and avoid radiated and conducted electromagnetic interference.

Tests for Coaxial transmission systems

In these trials will be necessary to teste the following scenarios:

- Without disturbance.
- Disturbances in the middle coaxial produced on other signals that share the medium (digital terrestrial television frequencies).
- Disturbances in the middle coaxial supported by the team due to other signals, they share the medium (digital terrestrial television frequencies).

  There is no need any verification disturbing other differences from that of digital terrestrial television, because such shocks are checked in the harmonized standard EN 301 489-01 V1.6.1.

10. CONTROL, MANAGEMENT AND AUTOMATION (OPTIONAL)

The Integrated Test System provides automation capabilities based on Ixia's Composer software (item 931-3003). Once developed a test for the Integrated System Test Composer allows it to be repeated as many times as desired with minimal human intervention.

Composer is an interactive development environment that allows users to develop scripts using multiple devices (including himself DUT / SUT) and measuring equipment simultaneously. Users can develop their own tests by capturing session, using available procedures or by entering commands directly in the script.

Another key feature of Composer is the ability to analyze logs generated by the DUT and execute scripts to proactively depending on the content of these logs.

Table 29.
Key features of Ixia Composer

Test IDE	*Provides a working environment that simplifies the test development process.*
Multi-vendor test authoring	*Provides a unified scripting environment that coordinates and synchronizes test steps. Composer tracks the commands executed in the different test tools and DUTs and replays them as a script in the desired order.*
Open architecture framework	*An open architecture framework that can accept command plug-ins developed by other vendors. Plug-ins can be easily added to the framework to extend and enhance the user's ability to control and script interactions with other test vendors' tools.*
Comprehensive Ixia application support	*Complete coverage of the Ixia portfolio of products including IxNetwork, IxLoad, IxAutomate, IxChariot and many more. Test Composer has the broadest list of supported applications and the deepest level of command support of any product in the industry.*
Live interactive capture/replay	*Create a test by simply entering commands in one or more live sessions connected directly to the DUT and/or test tool, then craft the captured sequence into an automated test or procedure that can be used by many tests.*
Passive DUT Monitoring	*Configure live sessions to passively monitor session logs and consoles for various messages, such as errors or warnings, and then take proactive steps to flag the errors and optionally recover from the errors. Supported sessions include SNMP and SYSLOG among others.*
Customizable Report Generation	*Automatically generate test reports as part of the test execution. The report can include any number of tables, graphs, images and text. A table of contents is automatically generated based on the content added by the test. The report content and format can be tailored dynamically by the test in real time.*
Built-in CSV file analyzer	*Easily read and analyze CSV files as part of the automated test. Many test tools produce output in CSV formats. The CSV Analyzer can read these files in, extract relevant data, and even aggregate the data for analysis. Then use the data to determine success or failure of the test automatically.*
Shared Test Resources	*Create a variety of shared resources like procedures and device profiles that allow the test team to leverage their work among the different test cases and make those test cases more portable.*
Full-featured debugger	*A debugging environment that shortens the time between creating and debugging a test. The debugger has a full set of features, including breakpoints, execution progress indicators, variable watches, global and session logging streams for diagnosing failures within the test.*
Simplified test development process	*A unique combination of capturing live interactions with the devices and test tools plus the full flexibility of a script editor and debugger.*

Annex A. SUPPLIER STATEMENT OF COMPLIANCE

Below is a summary of the status of compliance of various conditions specified by the customer for the Integrated System Test specified in the preceding sections.

GPON Analyzer.

Table 30.
GPON network analyzer as per the attached compliance sheet and specification and general requirements.

ID	Description	Country Origin Make
1	GPON network analyzer	Spain (European Union)

Voice Services

Table of compliance.

Table 31.
Performance Monitoring of various VoIP and FAX protocols and voice codec.

ID	Description	Compliance
1	H.323	YES
2	MGCP	YES
3	H.248 (MEGACO)	YES
4	SIP	YES
5	T.38	YES
6	void	n.a.
7	void	n.a.
8	G.726	YES
9	G.728	YES
10	G.729	YES
11	G.722 HD	YES
12	G.711	YES
13	Clear Mode	YES

Table 32.
Monitor and report all voice related performance parameters including service availability.

ID	Description	Compliance
14	No dial tone	YES
15	Busy	YES
16	Unreachable called party	YES
17	Sound loss	YES
18	DTMF transmission issue	YES
19	One way speech	YES
20	Dropped call	YES
21	Clipping	YES
22	Noise level	YES

Table 32.
Monitor and report all voice related performance parameters including service availability.

23	*End to end delay*	*YES*
24	*One way delay*	*YES*
25	*Dial tone delay*	*YES*
26	*Capture and analyze signalling and speech (RTP) path during voice calls*	*YES*

IPTV Service

Table of compliance.

Table 33.
Performance Monitoring of various IPTV services including Multicast and Unicast TV (SDTV, HDTV, MPEG2, MPEG4, and video on demand-VoD) Monitor and report all the performance related parameters including Service availability.

ID	*Description*	*Compliance*
27	*IGMP v1 / v2 / v3*	*YES*
28	*MPEG frames*	*YES*
29	*IGMP performance*	*YES*
30	*IGMP / MLD Querier*	*YES*
31	*MLD v1 v2*	*YES*
32	*Error Screens*	*YES*
33	*Black Out*	*YES*
34	*Frozen image*	*YES*
35	*Macro Blocks*	*YES*
36	*No sound*	*YES*
37	*Concurrently monitor multiple TV channels and provide alarm / report for service degradation*	*YES*

Table 34.
Monitor and report Picture quality.

ID	*Description*	*Compliance*
38	*Video MOS*	*YES*
39	*Blockiness*	*YES*
40	*Blur*	*YES*
41	*Jerkiness*	*YES*
42	*Video error screen capture*	*YES*
43	*Frame loss rate (FLR)*	*YES*
44	*Tiling*	*YES*
45	*Color Pixelation*	*YES*
46	*Slice Losses*	*YES*
47	*Channel Overlap*	*YES*

Table 35.
Monitor and report Audio quality.

ID	*Description*	*Compliance*
48	*Audio MOS*	*YES*

Table 35.
Monitor and report Audio quality.

49	*Bandwidth*	*YES*
50	*Loudness*	*YES*
51	*Saturation*	*YES*
52	*Audio Capture with video*	*YES*
53	*Fidelity*	*YES*
54	*Frequency response*	*YES*
55	*Signal to noise ratio*	*YES*
56	*Total Harmonic distortion (THD)*	*YES*

Table 36.
Monitor and report VoD analysis

ID	*Description*	*Compliance*
57	*Channel changing and menu browsing*	*YES*
58	*Channel Change Time*	*YES*
59	*VoD access time*	*YES*
60	*EPG access time*	*YES*

Table 37.
Monitor and report the Network analysis during testing off IPTV service.

ID	*Description*	*Compliance*
61	*MPEG-TS based on ETSI TR 101.290, ETSI TR 102.034*	*YES*
62	*MDI*	*YES*
63	*Backbones and service platform response time*	*YES*
64	*Packet loss*	*YES*
65	*Gap loss*	*YES*
66	*Jitter*	*YES*
67	*Packet Discard Rate (PDR)*	*YES*
68	*Connection Success Rate (CSR)*	*YES*
69	*Out of order Packets*	*YES*
70	*IGMP Join Leave Latency*	*YES*

HSI Service

Table of compliance.

Table 38.
Performance Monitoring for service availability of PPP sessions.

ID	*Description*	*Compliance*
71	*PPP successful session status*	*YES*
72	*Failed sessions with reason for failure*	*YES*
73	*DNS resolution failure*	*YES*
74	*TCP connect failure*	*YES*
75	*Servers and applications errors*	*YES*
76	*Authentication errors*	*YES*
77	*Time out*	*YES*

Table 38.
Performance Monitoring for service availability of PPP sessions.

78	*Integrity Check*	*YES*
79	*Web surfing*	*YES*
80	*HTTPS*	*YES*
81	*FTP*	*YES*
82	*Streaming media*	*YES*
83	*HTTP file download performance*	*YES*
84	*FTP file upload and download performance*	*YES*
85	*Messaging services with SMTP*	*YES*
86	*POP3*	*YES*
87	*IMAP4*	*YES*
88	*Time to send and receive emails*	*YES*
89	*Message transit time*	*YES*
90	*Measurement of the impact of firewall and antivirus for receiving messages*	*YES*
91	*DNS*	*YES*
92	*Telnet*	*YES*

Backbone testing

Table of compliance. . .

Table 39.
Backbone testing Analysis.

ID	*Description*	*Compliance*
93	*TCP*	*YES*
94	*UDP*	*YES*
95	*ICMP*	*YES*
96	*Hops*	*YES*
97	*Delay*	*YES*
98	*Packet Loss*	*YES*
99	*Jitter*	*YES*
100	*DNS Analysis*	*YES*
101	*Capability to do RFC-based benchmarking methodologies for Layer2 and Layer3*	*YES*

Table 40.
Testing of Network Traffic Access.

ID	*Description*	*Compliance*
102	*Spanning Tree*	*YES*
103	*VLAN*	*YES*
104	*DHCP*	*YES*
105	*QoS*	*YES*
106	*IPv4/IPv6*	*YES*
107	*Routing*	*YES*
108	*IEEE 802.1ad (Qin Q) tagging*	*YES*
109	*IPsec*	*YES*

Table 40.
Testing of Network Traffic Access.

110	*PPPoE*	*YES*
111	*IGMP*	*YES*
112	*SSL*	*YES*
113	*IPSec*	*YES*
114	*IPv6 functionalities*	*YES*
115	*IPv6 support for the 1Gig / 10 Gig interfaces*	*YES*
116	*DHCPv6*	*YES*
117	*Multicast for IPv6*	*YES*
118	*MLD (Multicast Listener Discovery Protocol)*	*YES*
119	*PIMv6*	*YES*

Table 41.
Monitor and Report.

ID	*Description*	*Compliance*
120	*Packets in order*	*YES*
121	*Dropped frames*	*YES*
122	*re-ordered frames*	*YES*
123	*late and duplicate frames*	*YES*
124	*In and Out-of-Sequence frames*	*YES*
125	*Latency modes like FIFO (bit forwarding devices per RFC 1242) LILO (forwarding delay per RFC 4689) and LIFO (store and forward devices per RFC1242)*	*YES*
126	*Latency, avrg, min, max, and short term avg, first/last frame arrival timestamp*	*YES*
127	*TCP/UDP checksum*	*YES*
128	*Frame CRC*	*YES*
129	*Embedded CRC*	*YES*
130	*PRBS bit errors*	*YES*
131	*FCS Errors*	*YES*
132	*IP checksum*	*YES*
133	*Total, Average, Minimum and Maximum Jitter*	*YES*
134	*Total, Average, Minimum and Maximum Interarrival time*	*YES*

Annex B. ALBEDO TELECOM SIP/VOIP TEST SUITE[2] (OPTIONAL)

This is one of the options for extension of the Triple Play Monitoring System. This suite lets you run the tests for approval and acceptance of VoIP terminals. The certification protocol described in this document enables testing of VoIP user equipment such as IP telephones or ATAs. The currently defined tests can be classified in the following groups (see Table 42.):.

Table 42.
Group of the test suite.

Class	Type	Purpose
IP - VOIP -General	*Conformance*	*They check basic features of the devices under test (DUTs) such as the capability of remote management through a web interface or the keypad directly attached to the device.*
IP - General	*Conformance*	*This family includes tests to verify features related with IP but not specifically with IP telephony. Support of DHCP or DNS protocols are examples.*
IP - VOIP - SIP	*Conformance*	*These tests check that the DUT is able to generate SIP signaling messages with a correct syntax and if they can decode and understand SIP messages received from remote entities.*
IP - VOIP - QOS	*Performance*	*This family checks that the DUT offer good voice quality under different conditions, including different types of network degradations.*

he QOS test family is general enough to allow verification of any telephone and not only VoIP telephones. Specifically, the Test System enables QoS verification and testing of POTS, ISDN or cell telephones under some not restricting conditions. On the other hand, it has to be noted that the Test System is prepared (or at least it can be configured) to enable testing of VoIP network equipment such as voice gateways proxies and other devices. However, in this case, it would be necessary to modify the test suite. Something similar can be said about H.323 VoIP devices. Either the Test System subsystems are independent of the actual VoIP signalling protocol or they support both SIP and H.323 signalling. The test suite, however, is suited only for SIP devices. It would be necessary to define from scratch a new IP- VOIP - H323 family for H.323 devices.

The following table (see Table 43.) reproduces de contents of the test suite along with a short summary with the purpose of every individual test

Table 43.
SIP/VoIP test suite.

Number	Test ID	Class	Name
0001	*8348-01*	*IP - VOIP - General*	*Management with keypad*
0002	*8432-01*	*IP - VOIP - General*	*Web management*
0003	*8433-01*	*IP - VOIP - General*	*Remote management*
0004	*8351-01*	*IP - General*	*Default settings*
0005	*8352-01*	*IP - General*	*Dynamic IP assignment*
0006	*11430-01*	*IP - General*	*DNS communication with dynamic IP*
0007	*11397-01*	*IP - General*	*DNS communication with dynamic IP (primary DNS server fails)*
0008	*11431-01*	*IP - General*	*DNS communication with dynamic IP (both DNS servers fail)*
0009	*11433-01*	*IP - General*	*DNS communication with static IP*
0010	*11432-01*	*IP - General*	*DNS communication with static IP (primary DNS server fails)*
0011	*11434-01*	*IP - General*	*DNS communication with static IP (both DNS servers fail)*
0012	*11345-01*	*IP - General*	*Port assignment procedure*
0013	*8357-01*	*IP - VOIP - SIP*	*REGISTER method (register without authentication)*

2. ALBEDO suite to test the acceptance and compliance of VoIP terminal.

Table 43.
SIP/VoIP test suite.

Number	Test ID	Class	Name
0014	10719-01	IP - VOIP - SIP	REGISTER method (register with authentication)
0015	8359-01	IP - VOIP - SIP	REGISTER method (unregister without authentication)
0016	10720-01	IP - VOIP - SIP	REGISTER method (unregister with authentication)
0017	11346-01	IP - VOIP - SIP	INVITE method (successful outgoing call)
0018	11347-01	IP - VOIP - SIP	INVITE method (successful incoming call)
0019	11488-01	IP - VOIP - SIP	INVITE method (outgoing call to a busy line)
0020	11489-01	IP - VOIP - SIP	INVITE method (incoming call to a busy line)
0021	11490-01	IP - VOIP - SIP	INVITE method (session refresh)
0022	11348-01	IP - VOIP - SIP	INVITE method (outgoing call hold)
0023	11349-01	IP - VOIP - SIP	INVITE method (line pickup after hold)
0024	11491-01	IP - VOIP - SIP	INVITE method (incoming call hod)
0025	11350-01	IP - VOIP - SIP	INVITE method (3 parties call, join calls)
0026	11492-01	IP - VOIP - SIP	INVITE method (3 parties call, join outgoing call)
0027	-	IP - VOIP - SIP	INVITE method (proxy authentication)
0028	11351-01	IP - VOIP - SIP	BYE method (internal phone ends call)
0029	11493-01	IP - VOIP - SIP	BYE method (external phone ends call)
0030	11494-01	IP - VOIP - SIP	CANCEL method (incoming call)
0031	11668-01	IP - VOIP - SIP	CANCEL method (outgoing call)
0032	11353-01	IP - VOIP - SIP	REFER method (blind call transfer)
0033	11352-01	IP - VOIP - SIP	REFER method (call transfer)
0034	11495-01	IP - VOIP - SIP	URI composition depending on register server port
DELETED	8378-01	IP - VOIP - SIP	RTP with codec G.729
DELETED	8379-01	IP - VOIP - SIP	RTP with codec G.711A
0035	8380-01	IP - VOIP - SIP	183 Session Progress message reception without SDP
0036	8381-01	IP - VOIP - SIP	183 Session Progress message reception with SDP
0037	8382-01	IP - VOIP - SIP	180 Session Progress message reception without SDP
0038	8383-01	IP - VOIP - SIP	180 Session Progress message reception with SDP
0039	11704-01	IP - VOIP - QOS	Clarity measurements introducing no perturbation
0040	11705-01	IP - VOIP - QOS	Clarity measurements introducing perturbations
0041	11706-01	IP - VOIP - QOS	Clarity measurements introducing no perturbation
0042	15766-01	IP - VOIP - QOS	Delay measurements introducing no perturbation
0043	15767-01	IP - VOIP - QOS	DMTF tone measurement introducing no perturbation
0044	15768-01	IP - VOIP - QOS	Signal loss introducing no perturbation
0045	12397-01	IP - VOIP - QOS	Clarity measurements introducing perturbations
0046	15769-01	IP - VOIP - QOS	Delay measurements introducing perturbations
0047	15770-01	IP - VOIP - QOS	DMTF tone measurements introducing perturbations
0048	15771-01	IP - VOIP - QOS	Signal loss introducing perturbations

Varios dispositivos de montaje en rack permitirán emular diferentes sistemas de red, cada uno con un propósito específico:

The Test System system has been specifically designed to perform the mentioned tests but it was also taken into account several possible future extensions like for example the attachment of a custom access network (like for example DSL or WiFi), or video generation/analysis subsystem.

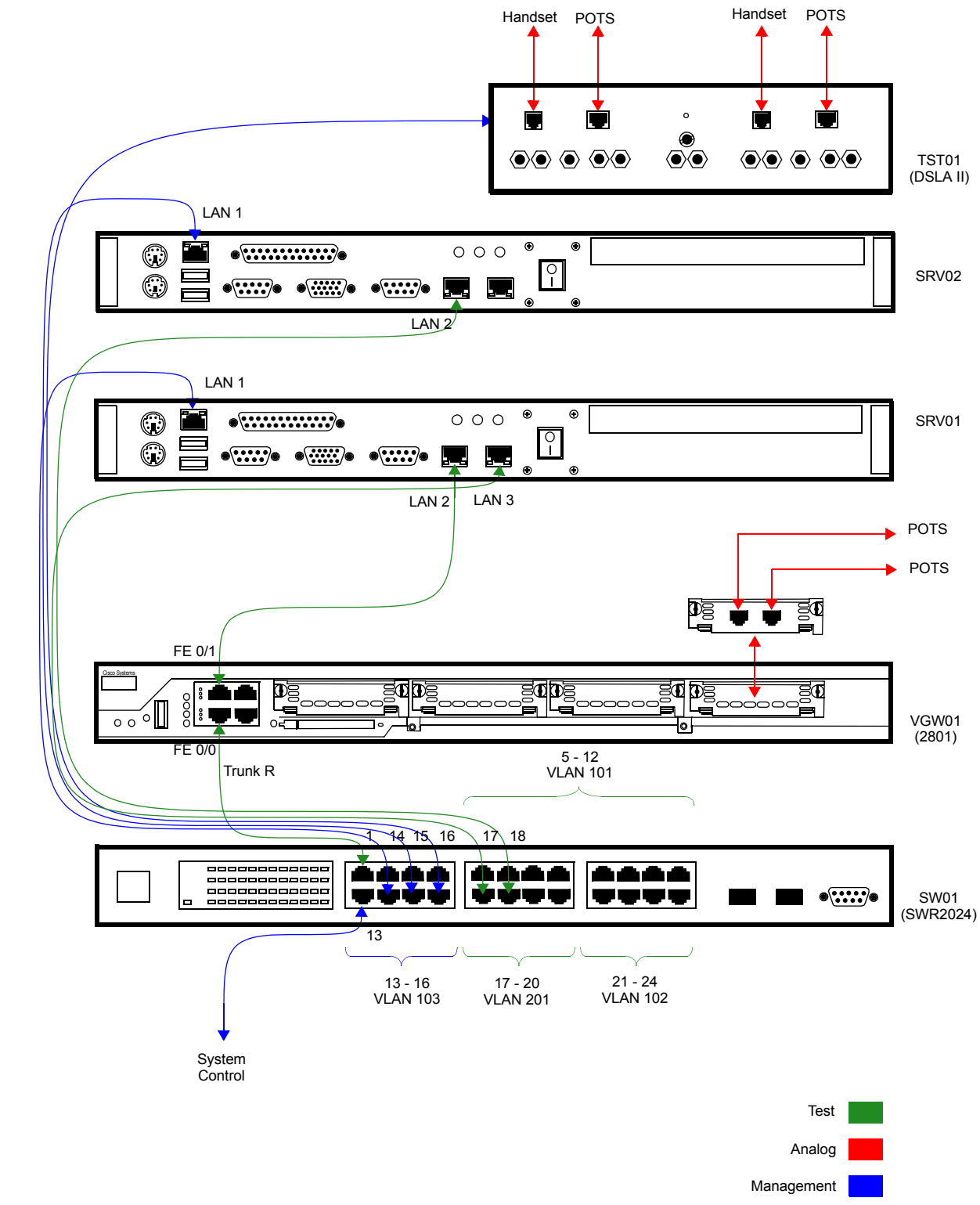

Figure 15. *ALBEDO Integrated VoIP Lab to execute conformity and acceptance test procedures for VoIP terminals, PBX and systems.*

The certification and acceptance Test System is made up by various rack-mountable devices. These devices emulate different network systems. There are three differentiated subsystems in the certification Test System, each with an specific purpose:

- *Network Services Simulation Subsystem (NSSS)*: Implements all the services commonly found in IP networks such as domain name service, address assignation, routing and others. At the same time, it provides access ports to test devices and other test Test System subsystems.
- *Network Impairment Emulation Subsystem (NIES)*: It generates controlled network impairments such as packet loss, delay, packet reordering and others. This subsystem is based in a software installed in a dedicated server.
- *Traffic Generation and Analysis Subsystem (TGAS)*: Devices attached to this subsystem are in charge of generating voice test signals, either as analogue audio or packetized media, and analyses the media signal. The most important measurement carried out by this subsystem is the clarity or MOS, that rates the quality of the voice signal with a number between 1 (for bad) and 5 (for good).

Although the testing Test System emulates most of the features and defects of most public or private IP networks, it does not pretend to be an exact reproduction of a service provider IP network. Switching and transmission equipment that are commonly included in the provider network have been replaced by simpler devices like the ones that are usually included in enterprise networks. These equipment include most of the functionality also offered by service provider equipment but they operate at lower bit rates. Including carrier class devices to the Test System would make it more expensive without adding new really important features and in any case these elements would always be used under their possibilities.

Physical interfaces that probably would made up the provider network will be replaced by simple Ethernet interfaces as well. The Test System network is an electrical Ethernet network operating at 100 Mb/s. However, connection of external devices is extended to 1 Gb/s Ethernet both over electrical or optical interfaces.

(More info: ANNEX.VoIP.Test.pdf)

Annex C. TRAINING, SUPPORT AND MAINTENANCE

1. ALBEDO Telecom will carry out the installation, configuration and complete overhaul of the solution in the Operator Facility.
2. ALBEDO Telecom will carry out personnel training in technology Operator and Test System use.
3. Telecom ALBEDO funded for a year, without charge, all queries on the system after delivery.
4. ALBEDO Telecom guarantees the system for one year free of charge.

   (More info: ANNEX.TRIPLE.PLAY.BOOK.ETISALAT.pdf)

Annex D. README

List of Documents for the ETISALAT RFP GPON Network Analyzer.

DOCUMENTS FOR THE PROPOSAL

- 1.MAIN.IMTS.GPON.ETISALAT.pdf (central document)
- 2.MAIN.COMPLIANCE.ETISALAT.pdf
- 3.MAIN.GPON.QUOTATION.ETISALAT.pdf

BROCHURES

- 4.BROCHURE.ALBEDO.Net.Storm.pdf
- 5.BROCHURE.IXIA.ixautomate_multicast.pdf
- 6.BROCHURE.IXIA.ixautomate_rfc_3511.pdf
- 7.BROCHURE.IXIA.ixautomate_rfc_benchmarking.pdf
- 8.BROCHURE.IXIA.ixload_overview.pdf
- 9.BROCHURE.IXIA.optixia_xm2.pdf
- 10.BROCHURE.IXIA.test_conductor_composer.pdf
- 11.BROCHURE.R&S.GENERADOR.SMB100A.pdf
- 12.BROCHURE.R&S.CMW-Z10.pdf
- 13.BROCHURE.MALDEN.DSLA.pdf
- 14.BROCHURE.GPON4000.pdf

ANNEX

- 15.ANNEX.VoIP.Lab.br.pdf
- 16.ANNEX.TRIPLE.PLAY.BOOK.ETISALAT.pdf
- 17.ANNEX.ABOUT.ALBEDO.pdf

CONTACT

Jose M Caballero
jose.caballero@albedo.biz
ALBEDO Telecom
+34 637 410 299

ALBEDO Telecom

ALBEDO Telecom designs, manufactures, and delivers solutions that enable Telecom organizations of all sizes to test, measure, troubleshoot, monitor, and migrate mission critical networks and multiplay applications.

On local segments and across distributed networks, ALBEDO enable Organizations, Installers, Operators, Service Providers and Suppliers to quickly check the health of Network Architectures, Service Agreements (SLA), IP Quality (QoS), or fix any issue.

Your Business Partner

Results. ALBEDO Telecom helps the industry to make the most of the investment on infrastructure.

Expertise. ALBEDO Telecom engineers and consultants provide industry leading knowledge in IPTV, VoIP, Carrier-Ethernet, Sync-Ethernet, SDH, and WDM / OTN to address the unique needs of customers.

Integration. ALBEDO Telecom integrates disparate telecom technologies and applications, facilitating new business efficiencies.

Agility. ALBEDO Telecom increases the ability of customers to respond quickly to new market opportunities and requirements.

Coverage. ALBEDO Telecom offers solutions that facilitates the migration and the roll-out to new architectures.

ALBEDO Telecom

the Path to Excellence

Ramón Turró, 100 - Barcelona - 08005 - Sp
Chalfont St Peter - Bucks - SL9 9TR - UK
www.telecom.albedo.biz

aims

+ UNDERSTAND causes of telecom interoperability issues
+ EXPERIENCE the best quality in unified networking
+ ASSESS different hardware, firmware, and software solutions
+ LEARN from experts by means of professional services and consultancy