Athens - Greece
www.ote.com

R. Turró, 100 - Barcelona - 08005
www.telecom.albedo.biz

IMS Acceptance and Verification System

Architecture and Procedures to execute Acceptance and Approval testing on the IMS network to be deployed in OTE

This document gives to OTE the configuration of a comprehensive Laboratory or System stating the parts and complemented with a budgetary price of each part of the test system. The parts of the ALBEDO solution may be hardware (HW), software (SW), and also the service to set up, customize and document the procedures to be executed.

OTE Requirements

IMS equipment will be installed in about 12 sites in the OTE network including Athens (in the basement of the Headquarters Building of OTE), Thessaloniki (the second biggest city of Greece in North Greece), and in 10 other sites in other cities of Greece.

In order to carry out the acceptance testing of the IMS network that will be installed in the network of OTE throughout Greece (as described above), the test system should be able to have a call generator that will be able to generate n x 5.000 simultaneous SIP calls with IMS extensions. Ideally, call generator as necessary in order to stress the network according to the calls load that is desirable.

The acceptance test will be carried out in a similar way to those performed to accept digital exchanges. It will be necessary to install *probes* in selected sites in the network of OTE. These probes will be part of the test system. It is calculated that will be necessary 3 or 4 probes.

Certification of customer terminals

User equipment shall be approved according to OTE specs by means of a testing suite that will result in a PASS/FAIL criteria. This procedure will be stationary in the Labs building of OTE in Athens and will be used for testing IMS terminal equipment (SIP user agents).

The requirements concerning the system to be bought by OTE sent us on February 1st. are those that are supposed to be the difficult ones for the potential suppliers. The system should also provide SIP testing capabilities.

Scalability

This document define also state the scalability of the whole system in terms of:

1. **Capacity,** more call generators, number of simultaneous calls, remote probes.
2. **Functionality**, test suite for IMS, acceptance suite for terminal, interconnectivity tests.

Certain test suites may be also offered as optional items, in any case ALBEDO is going to suggest the upgradeability of the solution to other functionalities while describing the hardware and software that may be necessary and their relevant budgetary cost.

Loopback

This capability is desirable where this is possible in order to allow OTE to carry out measurements from a central position without the need to send specialized personnel in the site where the equipment under test is.

SIP - IMS Test Suite

Functionalities specified are going to be describe in a bundle way. A number of groups are going to be defined to characterize them and giving a budgetary price for each separate group whenever is possible.

Open Solution

The whole system is totally modular and vendor independent which means that every single element can be substituted by an alternative vendor if necessary, including the genuine ALBEDO elements. Direct consequence of this design decision is to have an Open and scalable solution that does not depend on one single provider. We have selected the best element to better match OTE requirements.

An interesting consequence is that the Acceptance IMS system will allow OTE to write its test suites for related applications to be added to those specifically designed by ALBEDO Telecom.

Datasheet

- SIP/IMS terminal emulation (SIP/UDP and SIP/TCP and RTP traffic)
- SIP/IMS server/proxy emulation (selectable SIP and RTP port)
- SIP header manipulation
- A number of embedded basic testing scenarios, ready for execution (functional and conformance testing)
- Editor (GUI, or scripting language) for self-creation of additional testing scenarios
- Load/stress testing
- QoS capability (MOS, PESQ, R-factor)
- IMS features/protocols (authentication, Diameter, TLS, IPsec, XCAP)
- Tracing capabilities (MSCs display and message analysis) existing on the central system as well as on the distributed probes
- Windows or Linux OS and system calls support

The probes are requested to support

- SIP/IMS terminal emulation (and RTP traffic)
- Be centrally and remotely manageable
- Local tracing and statistics capabilities to interact/co-operate with the central system for end-to-end QoS measurements

1. INTRODUCTION

It can be said that IP and the Internet have the effect of moving the value of telecommunications services from the network to the end equipment and thus, IP make it difficult for network operators to obtain high return to their investments. Network operators are facing the risk of becoming mere "bit pipe" administrators. Today, telcos are seeing how their network becomes a commodity but they are unable to find an alternative to IP converged networks due to two reasons:

1. They can not ignore the success of IP services. Being in the IP market is a must for them.
2. They must keep operating expenditure and capital expenditure as low as possible to be competitive. Today this can only be made through a single multiservice IP network.

The solution that the telecommunications industry has proposed to keep the value of IP-centric network operators is the IP Multimedia Subsystem (IMS). In other words, IMS is a way to keep applications user-centric in a network-operator-centric business model. IMS is a session control subsystem based on IP, SIP, SDP, and other protocols, specifically designed for provision of multimedia services through high variety of access networks. As well as session control, IMS provides subscriber profile management, charging mechanisms and bearer and QoS resource allocation for media transmission.

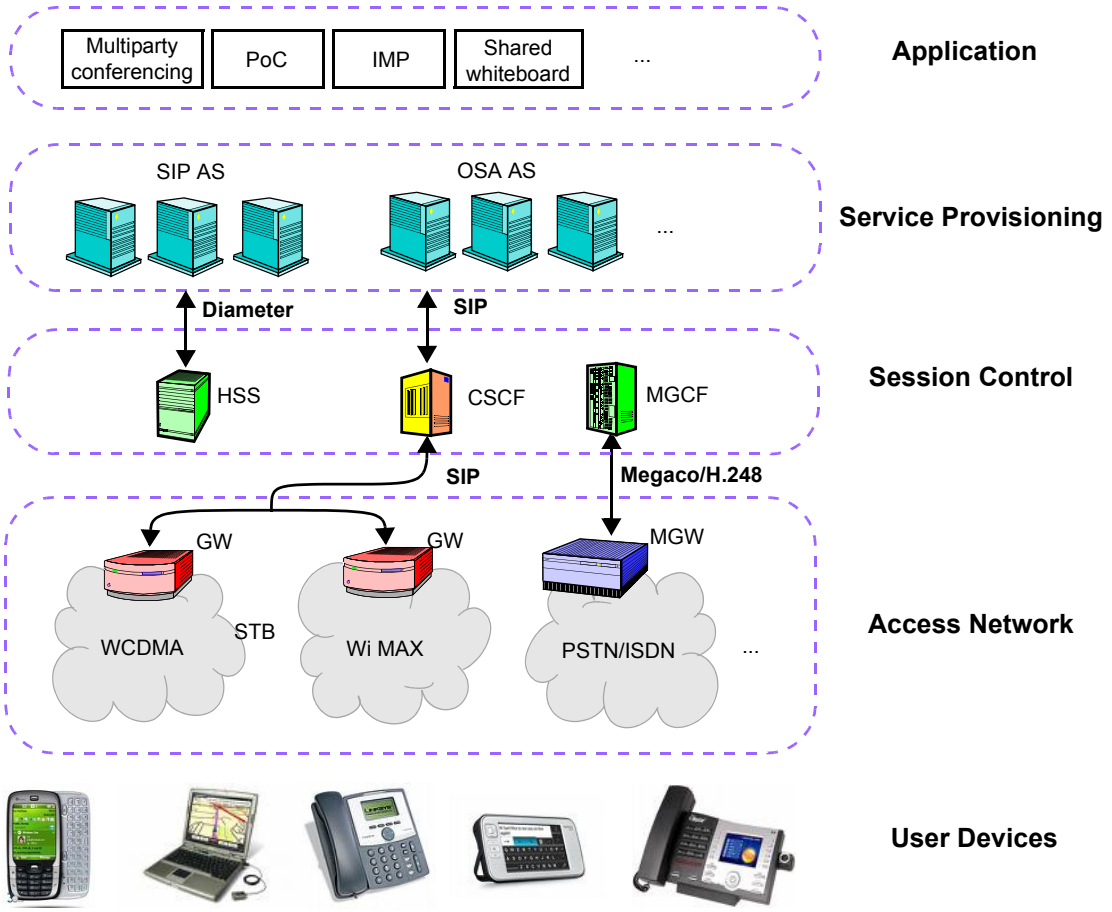

Figure 1. *IMS layered architecture from the application servers to the user devices.*

IMS was introduced in 3GPP specifications Release 5 in June 2002. The initial IMS specification was enhanced in Releases 6 and 7 and it is still an active standardization area. IMS brings together the IETF and the 3GPP worlds. Currently, the organization that releases IMS standards is the 3GPP but most of the IMS protocols are largely based on IETF RFCs.

Session Control

The key components of the IMS architecture are the Call Session Control Function (CSCF) and the Home Subscriber Server (HSS). Together, these components control how users access to the services in a highly versatile and customizable environment. The power of IMS is manifested through the great variety of user terminals that potentially could log on in the IMS capable network through many types of access mechanisms. Supported user equipment include mobile phones but also Personal Digital Assistants (PDAs), computers, VoIP phones, gaming consoles and many others. These devices must support the IPv6 protocol stack and run SIP user agents. Supported access networks are:

- *Wireline networks* based on Digital Subscriber Loop (DSL), Passive Optical Network (PON), Data Over Cable Service Interface Specifications (DOCSIS) or Ethernet.
- *Cellular mobile networks* including WCDMA, cdma2000, GSM and GPRS
- *IEEE wireless networks* including Wi-Fi and WiMAX.

Applications potentially available for IMS subscribers is large as well. Some example applications are video telephony, Push to talk over Cellular (PoC), Instant Messaging and Presence (IMP), shared whiteboards, multiparty conferencing, interactive gaming, and many others. IMS is capable of performing advanced session control over these applications on different ways:

- *Customizing the application depending on the user equipment or the access network*. For example the network could reduce the signal bit rate wherever the access network provides limited bandwidth to the subscriber or resize the image in a video telephony application when the video is displayed in the small screen of a mobile phone.
- *Modifying sessions in accordance with user preferences*. For example, some subscribers may want to configure their mobile phones to switch to Wi-Fi mode in the office and 3G mode in the car or the street. Other users may want to display the video signal in a video conference only when they have wireline access in order to optimise bandwidth usage.
- *Allowing roaming users to access to services located in the home network from the visited network*. An example of this situation is a user accessing to an IPTV channel provided in this home network from a remote network.

The outstanding features of IMS makes it a key requirement for FMC and effective IP-centric, quadruple play services rollout.

2. *Gm* Interface Testing

The Gm interface, as defined by the IMS 3GPP standards interconnects the user equipment (UE) and the IMS core. Acceptance of the UE requires emulation of the network side of the *Gm*, represented by the Call Session Control Function (CSCF). On the other hand, acceptance of the equipment installed in the IMS core requires emulation of the UE.

The conformance testing laboratory is able to generate calls and sessions, with the proper IMS header additions and modifications, across any SIP based IMS interface. Net.IMS allows the user to update and modify the underlying protocol state machine to adjust to changing IMS standards, interoperability, and negative testing situations. Diverse codec support make it useful for media testing in both fixed and cellular-based IMS networks and ideal for Fixed Mobile Convergence applications.

The complete test suite for IMS enables full verification of virtually any procedure defined for *Gm* interface, including discovery, authentication, call origination and termination, etc. The predefined test suite for IMS signalling verification over the Gm interface includes about 170 tests organized in 27 classes.

These families are described in Table 1. These classes are customizable. The test operators may decide to leave out of the suite test families not relevant or not yet implemented in their network. It is also possible to define new tests or customize the existing tests to the test operator demands with great flexibility.

Table 1. *Acceptance test suite for the Gm interface.*

Class	*Type*	*Purpose*
IP - IMS - CSCF - GENERIC	Conformance	Generic tests for the CSCF: - Basic user equipment registration - Basic call origination and reception
IP - IMS - CSCF - PLUGFEST	Conformance	Basic tests for the CSCF: - Basic call without authentication - Basic call IMS to PSTN - Re invite to update media stream
IP - IMS - CSCF - QOS	Conformance	QoS signalling in the CSCF - SIP establishment with QoS - GPRS procedures to guarantee the QoS
IP - IMS - CSCF - REGNONHIDING	Conformance	Registration tests for the CSCF without hiding the subscriber identity: - Registration tests - Re-Registration tests - Deregistration tests
IP - IMS - CSCF - SINONHIDING	Conformance	Session initiation tests for the CSCF without hiding the subscriber identity: - Incoming call tests - Outgoing call tests - PSTN termination tests
IP - IMS - CSCF - TERMNONHIDING	Conformance	Call termination tests for the CSCF without hiding the subscriber identity: - Termination error tests - Call establishment failure tests
IP - IMS - CSCF - SRNONHIDING	Conformance	Session release tests for the CSCF without hiding the subscriber identity: - User equipment initiated session release tests - Network initiated session release tests
IP - IMS - CSCF - MSNONHIDING	Conformance	Session management tests for the CSCF without hiding the subscriber identity: - Call on hold tests - Privacy request tests - Session redirection tests - Session transfer tests
IP - IMS - CSCF REGHIDING	Conformance	Registration tests for the CSCF hiding the subscriber identity: - Registration tests - Re-Registration tests - Deregistration tests

Table 1. *Acceptance test suite for the Gm interface.*

Class	*Type*	*Purpose*
IP - IMS - CSCF - SIHIDING	Conformance	Session initiation tests for the CSCF hiding the subscriber identity: - Call tests - Configuration hiding tests
IP - IMS - CSCF - TERMHIDING	Conformance	Call termination tests for the CSCF hiding the subscriber identity: - Termination error tests - Call establishment failure tests
IP - IMS - CSCF - SRHIDING	Conformance	Session release tests for the CSCF hiding the subscriber identity: - User equipment initiated session release tests - Network initiated session release tests
IP - IMS - UE - ETSI24228 - QOS	Conformance	QoS signalling in the user equipment
IP - IMS - UE - ETSI24228 REGNONHIDING	Conformance	Registration tests for the user equipment without hiding the subscriber identity: - Registration tests - Re-Registration tests - Deregistration tests
IP - IMS - UE - ETSI24228 SINONHIDING	Conformance	Session initiation tests for the user equipment without hiding the subscriber identity: - Incoming call tests - Outgoing call tests
IP - IMS - UE - ETSI24228 MSNONHIDING	Conformance	Session management tests for the user equipment without hiding the subscriber identity: - Session redirection tests - Session transfer tests
IP - IMS - UE - ETSI24228 SIHIDING	Conformance	Session initiation test for the user equipment hiding the subscriber identity
IP - IMS - ETSI34229 - T3GPPTSPDPCONTEXTACT	Conformance	Packet data protocol context activation tests
IP - IMS - ETSI34229 - T3GPPTSPCSCFDISC	Conformance	P-CSCF Discovery procedure: - Discovery over IPv4 tests - Discovery over IPv6 tests
IP - IMS - ETSI34229 - T3GPPTSREGISTRATION	Conformance	ETSI TS 34 229 registration procedure tests
IP - IMS - ETSI34229 - T3GPPTSAUTHENTICATION	Conformance	ETSI TS 34 229 authentication procedure tests
IP - IMS - ETSI34229 - T3GPPTSSUBSCRIPTION	Conformance	ETSI TS 34 229 subscription procedure tests
IP - IMS - ETSI34229 - T3GPPTSNOTIFICATION	Conformance	ETSI TS 34 229 notification procedure tests
IP - IMS - ETSI34229 - T3GPPTSCALLCONTROL	Conformance	ETSI TS 34.229 call control procedure tests: - Testing resource reservation in IMS calls - Testing IMS calls with preconditions
IP - IMS - ETSI34229 - T3GPPTSSIGCOMP	Conformance	ETSI TS 34.229 signalling compression tests.
IP - IMS - ETSI34229 - T3GPPTSEMERSERVICE	Conformance	ETSI TS 34.229 emergency call service testing.
IP - IMS - ETSI34229 - T3GPPTSMISC	Conformance	ETSI TS 34.329 miscellaneous tests

We define four different test setups (Figure 2). Some of them can be used for testing the network *Gm* interface and some others are for the user *Gm* interface. Setups C and D contain the service provider access network within the system under test.

This network (an the IMS core as well) may contain real or synthetic user traffic. While scenarios A and B are probably the most appropriate for equipment acceptance, set-ups C and D can be used at later stages of network deployment and bringing into service.

Table 2. *Test classes that apply to every test scenario.*

Class	*Setup A*	*Setup B*	*Setup C*	*Setup D*
IP - IMS - CSCF - GENERIC	**Yes**	No	**Yes**	No
IP - IMS - CSCF - PLUGFEST	**Yes**	No	**Yes**	No
IP - IMS - CSCF - QOS	**Yes**	No	**Yes**	No
IP - IMS - CSCF - REGNONHIDING	**Yes**	No	**Yes**	No
IP - IMS - CSCF - SINONHIDING	**Yes**	No	**Yes**	No
IP - IMS - CSCF - TERMNONHIDING	**Yes**	No	**Yes**	No
IP - IMS - CSCF - SRNONHIDING	**Yes**	No	**Yes**	No
IP - IMS - CSCF - MSNONHIDING	**Yes**	No	**Yes**	No
IP - IMS - CSCF REGHIDING	**Yes**	No	**Yes**	No
IP - IMS - CSCF - SIHIDING	**Yes**	No	**Yes**	No
IP - IMS - CSCF - TERMHIDING	**Yes**	No	**Yes**	No
IP - IMS - CSCF - SRHIDING	**Yes**	No	**Yes**	No
IP - IMS - UA - ETSI24228 - QOS	No	**Yes**	No	**Yes**
IP - IMS - UA - ETSI24228 REGNONHIDING	No	**Yes**	No	**Yes**
IP - IMS - UA - ETSI24228 SINONHIDING	No	**Yes**	No	**Yes**
IP - IMS - UA - ETSI24228 MSNONHIDING	No	**Yes**	No	**Yes**
IP - IMS - UA - ETSI24228 SIHIDING	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSPDPCONTEXTACT	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSPCSCFDISC	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSREGISTRATION	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSAUTHENTICATION	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSSUBSCRIPTION	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSNOTIFICATION	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSCALLCONTROL	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSSIGCOMP	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSEMERSERVICE	No	**Yes**	No	**Yes**
IP - IMS - ETSI34229 - T3GPPTSMISC	No	**Yes**	No	**Yes**

Only a subgroup of the 27 defined test classes makes sense for every test scenario. The correspondence between test setups and classes is described in table 2

3. AUTHENTICATION, AUTHORIZATION, ACCOUNTING TESTING

Authentication, Authorization, and Accounting (AAA) are three related terms that can be defined as follows:

- *Authentication* is the act of verifying the identity of an entity like for example the subscriber of a service provided by a network or a remote server that requests an specific network resource.
- *Authorization* is the act of determining whether a service subscriber or any other requesting entity will be allowed to access to a resource provided a network or a server.

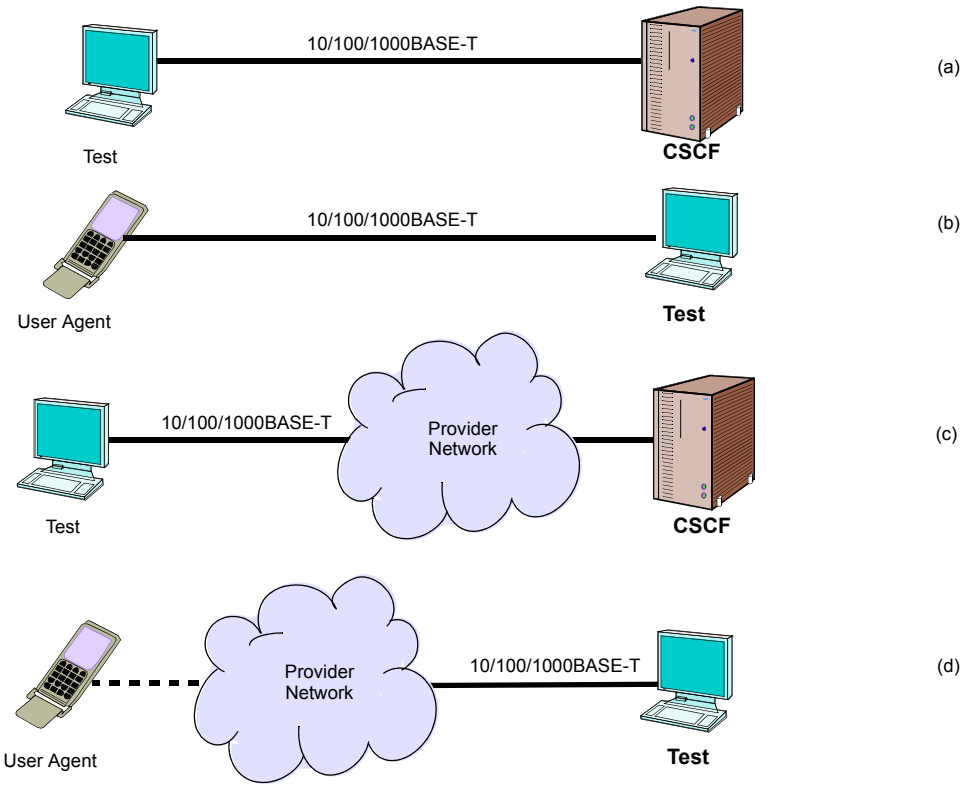

Figure 2. *Tests scenarios for verification of the Gm interface (a) Setup A, checks the Gm-Network interface, (b) Setup B, checks the Gm-User interface, (c) Setup C, similar to scenario A but it integrates the provider access network within the system under test, (d) Setup D, similar to scenario B but it integrates the provider access network within the system under test.*

- *Accounting* is the act of collecting information of a resource usage for the purpose of capacity planning, auditing, billing or cost allocation

  Within the IMS, AAA information exchange is performed by the Diameter protocol. Specifically, Diameter is the basis of the *Cx* interface that allows information exchange between the HSS and different types of CSCFs. Other interfaces within the IMS network based on Diameter are the *Dx* and the *Sh*. Our solution can be used for all three (Cx, Dx, Sh) interfaces and it is compliant with the following standard set:

- **RFC 3588** Diameter
- **RFC 4005** Diameter Network Access Server Application
- **RFC 4006** Credit Control
- **RFC 4740** Diameter Session Initiation Protocol (SIP) Application
- **ETSI TS 129 228 V7.3.0** (Cx, Dx)
- **ETSI TS 129 229 V7.3.0** (Cx, Dx)
- **ETSI TS 129 328 V6.12.0** (Sh)
- **ETSI TS 129 329 V6.12.0** (Sh)
- **3GPP2 X.S0013-005-A** (Cx)
- **3GPP2 X.S0013-006-A** (Cx)
- **3GPP2 X.S0013-010-A** (Sh)

- **3GPP2 X.S0013-011-A** (Sh)
- **ETSI TS 129 209 V6.1.0** (Gq)

The solution we provide also comes with a predefined test suite. All tests have are compliant and have been approved by the ACATS-Forum.

4. MEDIA TESTING

Quality in voice applications is usually specified in term os the Mean Opinion Score (MOS) or other objective rating schemes. In practical applications there are two important quality rating groups:

- Quality rating with reference: They rate the media quality by compared the degraded signal with a known reference. These methods use to be accurate but they are computanionally expensive and require a reference signal that is not available in some testing environments. Currently, the most important representative of this family is the PESQ algorithm, defined in standard ITU-T P.862.
- Quality rating without reference: They rate the media quality without reference signal. They for example are able to rate the signal quality of life voice. They are usually less accurate than parametric models and some require less computer power as well. The most important quality rating model without reference model is the E-Model, defined in ITU-T recommendation G.107.

The media analyzer that we include in the laboratory for IMS provides ratings for voice applications both with and without reference by means the PESQ and the E-model.

In conjunction with signaling testers and traffic generators, the media generator provides the RTP voice and video components and quality analysis. The API provides full control of RTP and RTCP, including payload and error injection. The media generator provides QoS metrics including delay, loss, out of order, de-jitter buffer simulation as well as an objective performance score using the MOS scale for audio and video media. PESQ analysis is also available as option. The media generation features the following:

- Full RTP, RTCP & sRTP audio analysis
- IPv4 and IPv6
- Audio includes G.711, G.729, G.723, GSM 6.10, Speex, iLBC, ...
- Import payload from Wireshark
- Path validation with unique verification sequences
- Echo cancellation testing
- Objective performance scoring for each stream, P.862 PESQ as option
- Text-To-Speech (TTS) synthesis for IVR & path labelling
- In-band DTMF and RFC 2833 support
- Scalable across several machines
- Query and view quality analysis results via the virtual desktop
- Export results as CSV
- IMS traffic generation with IPSEC support

To simulate the environment in which the devices to be tested will have to work, the laboratory implements network impairment emulation and synthetic background traffic generation.

Table 3. *Acceptance test suite for IMS.*

Class	*Type*	*Purpose*
IP - IMS - VOIP - QOE	Performance	Voice clarity testing without perturbations
IP - IMS - VOIP - QOEPERTURBATION	Performance	Voice clarity testing with perturbations
IP - IMS - VOIP - QOESTRESS	Performance	Voice clarity testing in presence of background voice traffic

By means impairment emulation, the laboratory operators can test and learn how the IMS network elements and the user equipment behaves under controlled degradation. Some possible degradation sources that can be configured are the following:

- Deterministic delay
- Uniform jitter
- Exponential Jitter
- Percentage of packet loss
- Percentage of packet duplication

On the other hand, the synthetic traffic generator enables generation of many call/session profiles across numerous protocols simultaneously, allowing it to simulate a wide variety of real and unusual traffic patterns (see the *Call Generation* section)

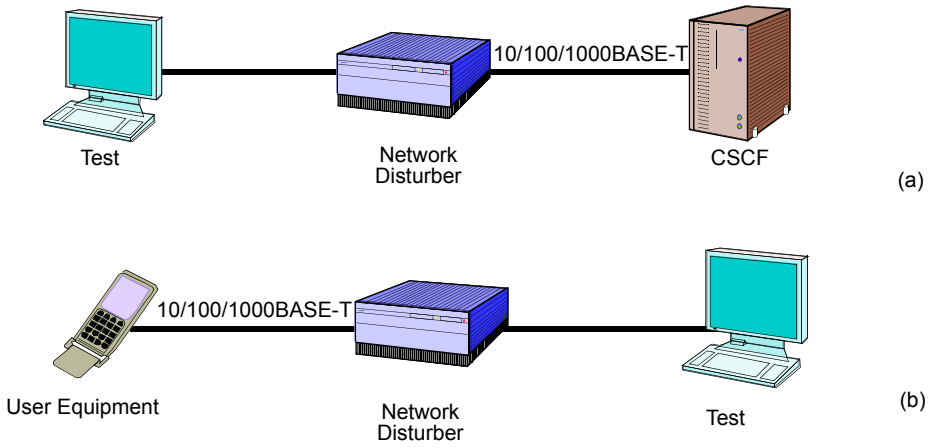

Figure 3. *Extra test scenarios for media quantity verification: (a) Setup E, checks the network end of the Gm interface with custom network impairments. (b) Setup F, is similar to setup E but it is adapted to check the user-Gm interface.*

To check media quality in the IMS network, we define three specific test classes, one for quality of experience (QoE) without impairments, the second for QoE testing introducing controlled impairments in the network and the third one measures QoE with traffic generated by the synthetic traffic generator (see Table 3).

In order to check properly the QoE, it is necessary to define two extra test scenarios (setups E and F) operating with the network impairment generator. The new test scenarios are defined in Figure 2.

Table 4. *Test classes that apply to every setup.*

Class	*Setup A*	*Setup B*	*Setup C*	*Setup D*	*Setup E*	*Setup F*
IP - IMS - VOIP - QOE	No	No	**Yes**	**Yes**	**Yes**	**Yes**
IP - IMS - VOIP - QOEPERTURBATION	No	No	No	No	**Yes**	**Yes**
IP - IMS - VOIP - QOESTRESS	**Yes**	**Yes**	**Yes**	**Yes**	No	No

As it happens with the signalling test classes, not all media testing classes make sense for every test setup. Correspondence between test setups and classes is illustrated in Table 4.

5. IMS Call Generation

The Net.IMS call generator verifies that products and voice applications perform precisely as designed with advanced capabilities for VoIP and IMS testing, signaling and media functionality, real world test scenarios and the ability to emulate realistic user behavior provides a robust SIP support, IMS UE emulation, full IPv6 support, and flexible signaling engine make it ideal for testing IMS networks and devices at any stage of the life cycle.

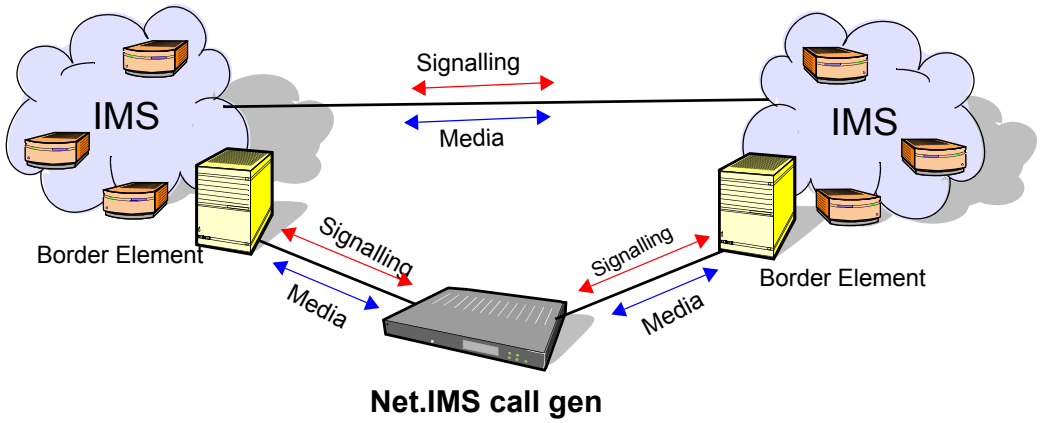

Figure 4. *Net.IMS call gen can generate numerous call/session profiles across numerous protocols simultaneously, allowing it to simulate a wide variety of real and unusual traffic patterns.*

The call generation capability to be included in the IMS laboratory includes the following capabilities:

- Stress and feature tester
- Supports transmission of well and poorly constructed SIP packets (configurable length payload, too long, too short packets):
- Up to 8,000 endpoints
- Up to 1,000 upper-layer MSUs per second
- Static or DHCP address allocation

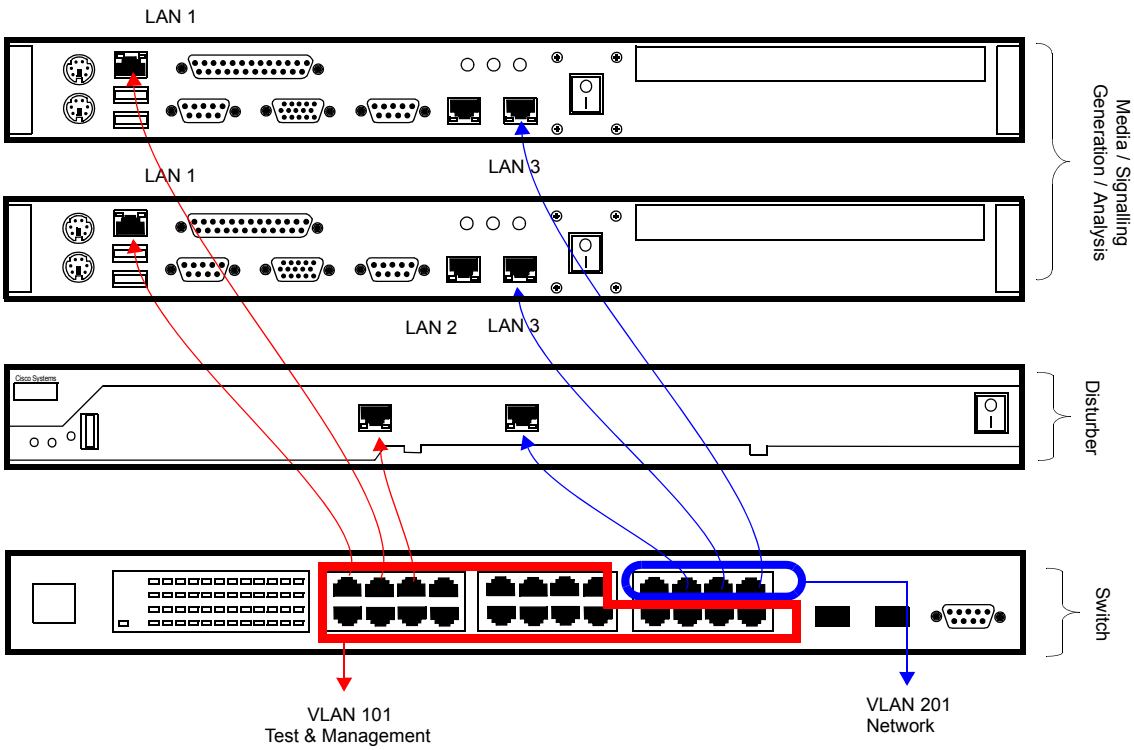

Figure 5. *Preliminary block diagram for the IMS laboratory.*

- IPv4 and IPv6 options supported
- Configurable MD5/AKA Registration
- Send upper-layer protocol data towards system under test
- Statistics and logging including successful / failed registration / call attempts
- Email alerts
- Client, Server and Client-Server (loopback) traffic modes
- Audio RTP/R TCP generation and analysis

6. TEST SYSTEM ARCHITECTURE

The test laboratory is provided as a rack mounted solution made up of different elements, each of them with an specific function:

- Ethernet Switch: Provides connectivity to the laboratory. It enables connection of different kinds of devices, and connection of the laboratory to the IMS network.
- Disturber: Generates custom impairments under controlled conditions as requested by the laboratory operators. Perturbations can be added separately in each transmission direction. This element has two network interfaces and the perturbations are generated between these two interfaces.
- Media / Signalling generation and analysis: The generation and analysis provides test traffic when needed and performs different kinds of analysis of traffic on this test traffic or traffic received from the network or device under tests. Signalling testing and media testing (including stress testing) are provided in two different hardware pieces.

Server Hardware

Software components for the laboratory are installed in high-performance Windows-based servers. The hardware platform can be customized to meet all the required testing needs. It's compact form-factor fits into an industry standard 19" rack for permanent installations. The server specifications are listed below:

- Intel® Pentium® 4 3.0GHz processor
- Windows® XP SP2
- 2GB Ram
- 120GB HD
- CD-ROM drive
- 2 Network Interface Cards (Ethernet 10/100bT)
- 2 full-length PCI slots (extendable)
- 250W Power Supply
- VGA
- 2 USB Ports

7. THE NETWORK DISTURBER

Simulation of Real Networks

IP networks are subject to degradations for different reasons. A key is congestion. The nodes of the Network Service Providers (NSP) support quality of service (QoS) allowing them to some extent mitigate the effects of congestion. Coding schemes and terminal equipment must also be designed so that the impact of congestion effects as small as possible. For example, IPTV set-top boxes and IP phones incorporate buffers that absorb the effects of delay variation without losing data. This minimizes the degradation of service experienced by subscribers.

The production subsystem degradations will be used to test the response of the elements to a signal that is under delay, delay variation, packet loss and other events. The effects of degradation will be measured later in the subsystems of generation / analysis of IMS/SIP calls.

Conformance Procedures

The process followed to accept a device, test a protocol, or troubleshoot an application has always been a important task, but when the new solution is based on the IP protocol stack, then a formal verification of the solution becomes essential.

IP networks are everywhere, and very diverse indeed, and now are capable to carry any type of traffic. IP connections may vary a lot in bandwidth, latency, and error and loss rates, and often are asymmetric. Moreover QoS dynamics can fluctuate widely, because of the congestion in peak hours, failures and routing.

QoS demands

The demands that applications make of networks vary widely as well, often relying on near-real-time characteristics that differ fundamentally from the best-effort delivery typically provided by current networks. Applications and protocols in consequence increasingly employ adaptive mechanisms to make more intelligent use of available network resources. But these, too, present new testing challenges: the correct behavior of adaptive STBs cannot be defined statically or often even in any simple deterministic fashion; and adaptive protocols at different levels or in different systems may interact poorly with each other in ways not easily detectable while testing in isolation.

NetStorm

ALBEDO Telecom has designed NetStorm to address this growing diversity of network hardware and software, and to provide a controlled, reproducible environment for testing nodes, protocols and terminals used in the new IP applications. NetStorm 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 behavior up to 1 Gbps rates with accuracy always better that 1 ms. By operating at the Ethernet layer NetStorm can emulate the critical end-to-end performance characteristics imposed by core routers and carrier switches and by any underlying network technology.

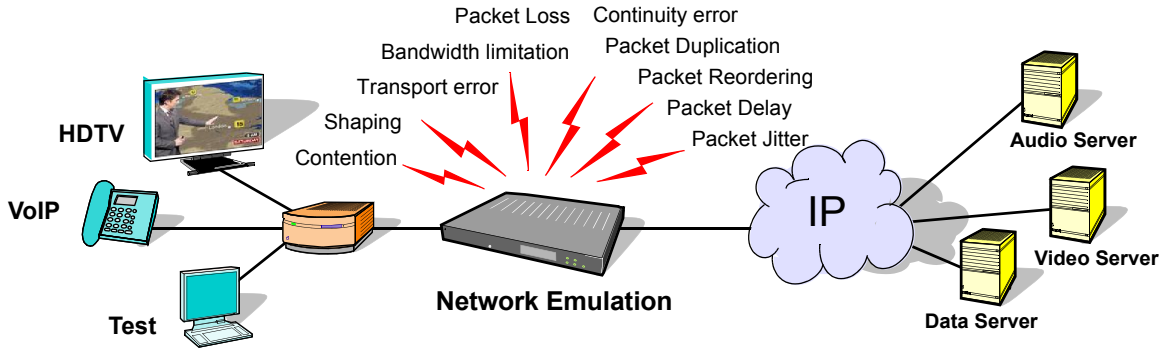

Figure 6. *ALBEDO Net.Storm is the selected network impairments generator that allows to simulate the network*

Hardware Performance

NetStorm is inserted between two Ethernet segments in pass through mode while operating in bidirectional packet transfer mode. The emulation settings can be defined independently for 16 separate flows that can be filtered by several criteria including MAC, IP, TCP/UDP or User Mask.

The result is a realistic and 100% controlled simulation of those conditions obtained of actual WAN networks that have been detected at the live. The same conditions are able to be reproduce in order to observe the behavior of applications such as VoIP, IPTV, VoD; nodes such us gateways, routers or set top boxes; and protocols such as SIP, MEGACO, H.323; and critical links and access networks.

Key Features

The overall QoE depends not only on the packet loss or jitter time pattern but also on the content, the encoding and dejitter buffering strategies. With NetStorm, all of this impairments and more can be generated to address a reliable performance verification.

- High performance appropriate for TV head-end, Video servers or Massive VoIP calls.
- Configurable, either deterministic or random, time delays can be inserted
- FEC errors, IP checksum errors
- Users can place errors within IP protocols or edit the Ethernet/IP fields.
- Impairments ITU-T Y.1541.
- Detailed event log window with per flow viewing of the events.
- Controlled impairments per specific traffic flows

NetStorm has the ability to replicate complex network dynamic by means of modifying Bandwidth and QoS parameters. NetStorm is now a useful tool in IP equipment manufacturers, R&D departments, Network Operators, ISP and Triple Play service providers that use this tool for a wide variety of projects.

8. SIP/VoIP TEST SUITE (OPTIONAL)

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:.

Table 5. *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.

The QOS test family is general enough to allow verification of any telephone and not only VoIP telephones. Specifically, the laboratory enables QoS verification and testing of POTS, ISDN or cell telephones under some non restricting conditions. On the other hand, it has to be noted that the laboratory 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 laboratory 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 reproduces de contents of the test suite along with a short summary with the purpose of every individual test:

Table 6. *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)
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

Table 6. *SIP/VoIP test suite.*

Number	*Test ID*	*Class*	*Name*
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

The laboratory 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.

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

- *Network Services Simulation Subsystem* (NSSS): Simulates 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 laboratory 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 analog audio or packetized media, and analyse 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 laboratory 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 laboratory 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 laboratory network is an electrical Ethernet network operating ta 100 Mbit/s. However, connectivity is extended to 1 Gb/s Ethernet both over electrical or optical interfaces.

The downside is that you can get to be the case that any of the services or features provided by network provider are not available in enterprise-class elements. This could be the case for example the server side of the PPPoE protocol, used by some service providers to authenticate clients on the network and provide IP addresses. In this case, opt for these services simulate the architecture of a PC or take them directly from the provider network by connecting to a WAN laboratory.

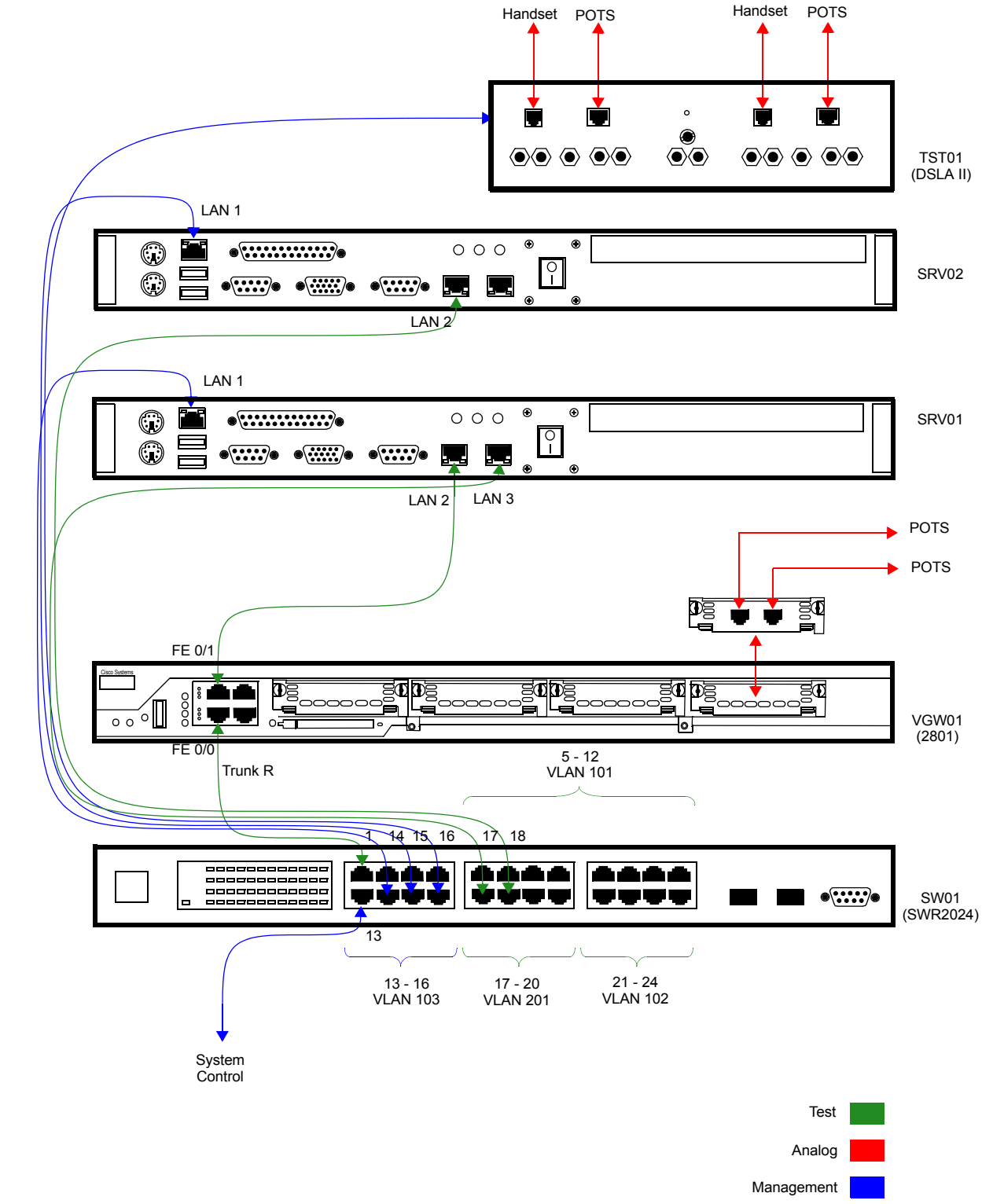

Figure 7. *This figure represents the laboratory network.*

9. NETWORK SERVICES SIMULATION SUBSYSTEM

The test laboratory is designed to be autonomous, that means that it implements all services normally provided by IP networks but without the support of any external network. Services provided by the IP laboratory include IP address assignation, domain name service, network address translation, SIP device registration and SIP call routing. The network services simulation subsystem (NSSS), is in charge of the emulation of these services. This subsystem is made up of the following components:

- *Ethernet Switch (SW01)*: Provides connectivity to the VoIP laboratory. It enables connection of different kinds of devices, including control consoles and test devices like VoIP phones. This component is implemented by a Linksys SRW2024 switch with 24 electrical and 2 optical Gigabit Ethernet interfaces.
- *Voice Gateway (VGW01)*: This device, implemented by a Cisco 2801 router is at the same time a router that forwards traffic between the laboratory IP networks and a voice gateway that delivers traffic to/from POTS telephones and SIP devices.
- *Domain Name Service (SRV02/DNS)* server: Provides name resolution to the subsystems of the laboratory, including the devices under test.

10. TRAINING AND DOCUMENTATION

ALBEDO Telecom will carry out the complete installation of this IMS solution in Athens.

ALBEDO Telecom will carry out the training to OTE staff on the technology and in the use of the laboratory and the system itself.

ALBEDO Telecom will support during one year, free of charge, all the queries regarding the system once delivered.

consulting + network auditing + maintenance + laboratory troubleshooting + architectonic

ALBEDO Telecom

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

On local segments and across distributed networks, ALBEDO enable Organizations, Installers, Operators, Service Providers and Suppliers to quickly check the health of your architecture, verify SLA, or find and fix problems.

Your Business Partner

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

Expertise. ALBEDO Telecom trainers, auditors, engineers and consultants provide industry-leading knowledge to address the unique needs of customers.

Integration. ALBEDO Telecom integrates disparate telecom resources and applications, realizing 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
Avenida Europa, 30 - Madrid - 28023
www.telecom.albedo.biz

aims

+ UNDERSTAND causes of telecom interoperability issues
+ EXPERIENCE the best QoS in unified networking
+ ASSESS different solutions for hardware and firmware design
+ LEARN from telecom experts by means of network auditing and consultancy