MultiService Forum
VoLTE Interoperability Event 2011

MSF VoLTE Interoperability Event 2011

Multivendor testing in global LTE
& IMS Networks

Backed By

GSMA

Host Sites

中国移动通信 CHINA MOBILE 移 动 信 息 专 家

vodafone

Gold Sponsors

GENBAND

HUAWEI

ZTE中兴

Silver Sponsors

ALEPO

amdocs

cisco

tellabs

Abstract

This white paper provides a summary of the Voice over LTE (VoLTE) Interoperability 2011 event which took place from September 12th – 30th, 2011. The event was organised by the Multi-Service Forum (MSF) and backed by the GSMA.

The event builds on the major success of the previous MSF LTE Interoperability Event that took place during March 2010 and reflects the industry's drive to continue to deliver major carrier driven events that benefit all its members in their quest to keep pace with an ever faster moving industry. The MSF VoLTE Interoperability 2011 event validated key network interfaces to support multi-vendor deployment strategies for LTE/EPC/IMS technology. The main objective was to validate the work of the GSMA as part of its global VoLTE initiative, focusing on Voice over LTE including Roaming and Interconnect, as specified in the GSMA's technical recommendations PRD IR.92 ("IMS Profile for Voice and SMS"), PRD IR.65 ("IMS Roaming and Interworking Guidelines"), and PRD IR.88 ("LTE Roaming Guidelines").

The GSMA technical recommendations are based on The Third Generation Partnership Project (3GPP) standards. 3GPP introduced the Evolved Packet Core to support LTE access with the IMS core network providing the application layer for which services (e.g. voice) may be deployed. The EPC and IMS core interact with the Policy and Charging Control (PCC) infrastructure to enable Quality of Service for the bearers.

The event was conducted in two host sites; the Vodafone Test and Innovation Centre in Düsseldorf, Germany and the China Mobile Research Institute Laboratory in Beijing, China.

The event demonstrated that the GSMA technical recommendations, based on the 3GPP specifications, for providing end to end VoLTE were mature and interoperable.

However some specific interoperability issues were discovered and will be considered for recommending potential updates to specifications where appropriate. In some cases, backwards incompatibility was observed between implementations of different versions of 3GPP specifications. Implementations that were not fully-compliant to the 3GPP specifications were found. Finally, in some cases it was difficult to re-configure the network components when testing different multi-vendor configurations.

It is important to identify and understand the factors that limit interoperability with commercially available equipment, from both a Vendors' perspective and an Operators' perspective. Vendors' benefit from identifying issues and improving products to become more commercially viable, and Operators need to be aware of any backwards incompatibility aspects to take into account for vendor selection and deployment strategy.

Events such as the MSF VoLTE Interoperability event highlight these issues and prove the validity of the MSF approach to achieving multi-vendor interoperability.

It is worth noting that the re-configuration issue is mainly related to the test network and the desire to test various different multi-vendor configurations. It is therefore not seen as a major issue for network deployments.

Highlights of the event included:-

- VoLTE calls were successfully completed within each host site (including MMTel services) as well as between the host sites to demonstrate network inter-connect.
- LTE Roaming between host sites was successfully demonstrated, utilizing dynamic policy control between home and visited networks employing DRA's (Diameter Routing Agents).
- Multi-vendor testing, a key component of all MSF IOT events, was conducted at each site, incorporating interworking between different vendors' UE, eNodeB, Sec-GW, EPC, IMS, MMTEL AS, DRA and PCC technology.
- The IMS Soft Clients interworked successfully with the LTE data dongle for LTE Attach and additionally with the IMS Core Network and MMTel AS to provide IMS services to the end user.
- LTE Handover was successfully demonstrated with S1 and X2 based handovers performed.
- Security Gateways (Sec-GW's) were utilized in the test network to enable secure communications between the eNodeB's and the EPC network.
- Robustness Testing was completed to demonstrate robustness of network nodes at the IP-level for the S-GW and P-GW, as well as SIP/UDP robustness for P-CSCF and I-CSCF.
- The use of Diameter Routing Agents enabled the simplification of diameter routing within the PLMN. DRA's were also shown to provide interworking between different transport layer protocols.

Contents

Executive summary p. 6

- The MultiService Forum (MSF) p. 6
- The VoLTE Interoperability Event p. 6
- VoLTE Architecture of the VoLTE Interoperability Event 2011 p. 6
- Optimised VoLTE Architecture of VoLTE Interoperability Event 2011 p. 9
- Key Objectives of the VoLTE Interoperability Event p. 12
- Key Statistics p. 13
- Key Results p. 13

Introduction p. 15

Part I: Participants and Planning p. 17

- Host Sites p. 18
  - Vodafone p. 18
  - China Mobile p. 18
- Vendor Participants p. 19
- Observing Companies / Organisations p. 23

Part II: LTE Interoperability Execution p. 24

- The Network Test Scenarios p. 26
- Test Scenario Validation p. 28
- Testing infrastructure support p. 28

Part III: Results and Issues p. 30

- Future Work p. 34

Appendix A: The Test Scenarios p. 35

- Basic Interoperability p. 35
- Security Gateway p. 39
- Roaming & Interconnect p. 40
- Handover p. 45
- Robustness p. 46

Appendix B: Interfaces Tested p. 52

Appendix C: The Benefits of MSF Membership p. 54

Appendix D: Participants in the VoLTE Interoperability Event p. 55

Executive Summary

The MultiService Forum (MSF)

The MSF is a global association with a membership that includes the world's leading Internet Protocol (IP) communications companies. The MSF promotes the testing of interoperability based on open standards within a defined end-to-end architecture.

The VoLTE Interoperability Event 2011

The VoLTE Interoperability Event 2011 was designed to test standards compliance of Long Term Evolution (LTE) , Evolved Packet Core (EPC), and IMS network scenarios in support of the provision of Voice over LTE (VoLTE). Such network scenarios are of interest to major Service Providers, and the event is intended to gauge standards maturity and vendor support for this technology. This event builds on the previous MSF LTE Interoperability Event which took place in March 2010 and provided the first global "real network" multi-vendor trial of the Evolved Packet Core infrastructure. This event is backed by the GSMA and seeks to validate a number of GSMA technical recommendations, namely:

- PRD IR.65 - IMS Roaming and Interworking Guidelines,
- PRD IR.88 - LTE Roaming Guidelines,
- PRD IR.92 - IMS Profile for Voice and SMS.

Interoperability testing was conducted in 2 labs; the Vodafone Test and Innovation Centre in Düsseldorf and the CMCC Research Lab in Beijing. The two labs were interconnected via a VPN. Conducting the tests in two interconnected labs made it possible to test more vendor combinations, and also allowed realistic testing of important roaming and interconnect scenarios.

A total of 89 test cases were written across 4 test scenarios. The test scenarios were as follows:

- Basic Interoperability,
- Roaming & Interconnect,
- Handover,
- Robustness testing.

VoLTE Architecture of the VoLTE Interoperability Event 2011

The VoLTE architecture allows users to connect to the network via the LTE high-speed wireless infrastructure and access voice services provided by a Multimedia Telephony (MMTel) Application Server on an IMS framework. This allows access to the applications and services that todays sophisticated user's demand, while providing the necessary Quality of Service management and mobility functions.

The basic intra-PLMN VoLTE architecture is shown in the Figure below:

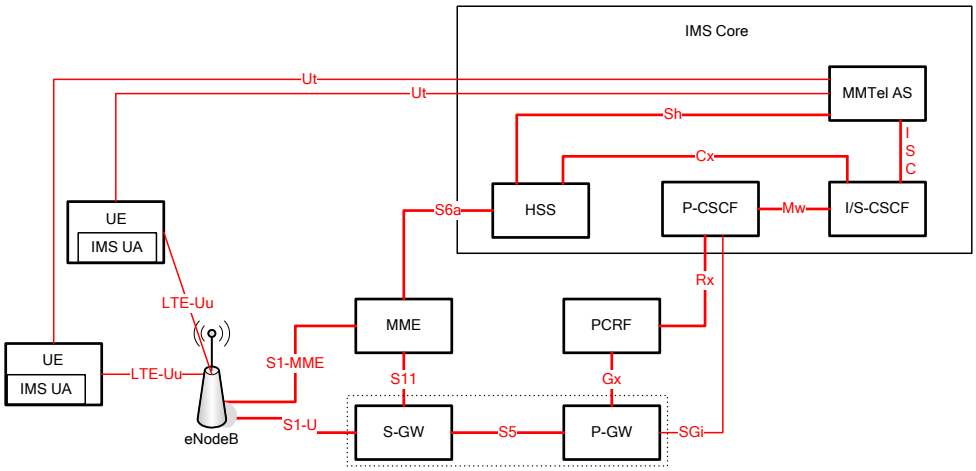

Figure 1. Basic Intra-PLMN VoLTE Architecture

NOTE: The Gm interface (UE to P-CSCF) is a focus for testing although not explicitly shown in the above figure.

- **UE (User Equipment)**. The User Equipment that is used to connect to the EPS, and is an LTE capable UE accessing EPC via the LTE-Uu radio interface.

- **eNodeB.** The evolved RAN (E-UTRAN) consists of a single node, the eNodeB that interfaces with the UE. The eNodeB hosts the Physical (PHY), Medium Access Control (MAC), Radio Link Control (RLC), and Packet Data Convergence Protocol (PDCP) layers that include the functionality of user-plane header-compression and encryption. It also offers Radio Resource Control (RRC) functionality corresponding to the control plane. It performs many functions including radio resource management, admission control, scheduling, enforcement of negotiated UL QoS, cell information broadcast, ciphering/deciphering of user and control plane data, and compression/decompression of DL/UL user plane packed headers.

- **MME (Mobility Management Entity)**. The Mobility Management Entity (MME) is the key control-node for the LTE access-network. It is responsible for idle mode UE tracking and paging procedures including retransmissions. It is involved in the bearer activation / deactivation process and is also responsible for choosing the S-GW (see below) for the UE at the initial attach and at time of intra-LTE handover involving Core Network node relocation. It is responsible for authenticating the user (in conjunction with the HSS). The NAS (Non-Access Stratum) signalling terminates at the MME which is also responsible for the generation and allocation of temporary identities to the UEs. The MME validates the permission of the UE to camp on the service provider's PLMN (Public Land Mobile Network) and enforces UE roaming restrictions. The MME is the termination point in the network for ciphering/integrity protection for NAS signalling and handles security key management. Lawful interception of signalling is also a function provided by the MME. The MME provides the control plane function for mobility between LTE and 2G/3G access networks and interfaces with the home HSS for roaming UEs.

- **S-GW (Serving Gateway).** The S-GW routes and forwards user data packets, while also acting as the mobility anchor for the user plane during inter-eNodeB handovers and as the anchor for mobility between LTE and other 3GPP technologies (terminating S4 interface and relaying the traffic between 2G/3G systems and PDN GW). For idle state UE, the S-GW terminates the DL data path and triggers paging when the DL data arrives for the UE. It manages and stores UE contexts and performs replication of the user traffic in case of lawful interception. It is likely that the S-GW and P-GW functions would be realized as a single network element.

- **P-GW (Packet Data network Gateway).** The P-GW provides connectivity between the UE and external packet data networks, it provides the entry and exit point of traffic for the UE. A UE may have simultaneous connectivity with more than one P-GW for accessing multiple Packet Data Networks. The P-GW performs policy enforcement, packet filtering for each user, charging support, lawful interception and packet screening. The P-GW also acts as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX or DSL. It is likely that the S-GW and P-GW functions would be realized as a single network element.

- **PCRF (Policy Charging and Rules Function).** The PCRF provides policy control decisions and flow based charging controls. The PCRF determines how a service data flow shall be treated in the enforcement function (P-GW in this case) and ensure that the user plane traffic mapping and treatment is in accordance with the user's profile.

- **HSS (Home Subscriber Server).** The HSS is a network database that holds both static and dynamic data elements related to subscribers. The HSS provides user profile information to the MME during user authentication.

- **P-CSCF (Proxy Call Session Control Function).** The P-CSCF is the initial point of contact for session signaling for the IMS-enable VoLTE UE. The P-CSCF behaves as a SIP proxy by forwarding SIP messages the UE and the IMS Core Network, maintains the security associations between itself and the VoLTE UE, incorporates the Application Function aspect of PCC to enable binding of the IMS session with the bearer for applying dynamic policy and receiving notifications of bearer level events.

- **I/S-CSCF (Interrogating/Serving Call Session Control Function).** The I-CSCF is the contact point within an operator's network for all connections destined to a user of that network. On IMS Registration, it interrogates the HSS to determine which suitable S-CSCF to route the request for registration. For Mobile Terminating calls, it interrogates the HSS to determine which S-CSCF the user is registered on.
  The S-CSCF provides session set-up, session tear-down, session control and routing functions. It generates records for billing purposes for all sessions under its control, and invokes applications using Application Servers. The S-CSCF acts as SIP registrar for VoLTE UE's that the HSS and I-CSCF assign to it. It queries the HSS for the applicable subscriber profiles and handles calls involving these end points once they have been registered. The S-CSCF uses subscription information to determine the appropriate onward routing for calls originating through it.

- **MMTel AS (Multimedia Telephony Application Server).** The MMTel AS is an IMS Application Server providing support for multimedia telephony services as defined by 3GPP e.g. supplementary service functionality.

Optimised VoLTE Architecture of VoLTE Interoperability Event 2011

In addition to the above VoLTE Architecture, functions that secure communications between access and core network and functions that optimise the routing of Diameter messages were included in the test scenarios. These are discussed in detail below.

Diameter Routing

LTE and IMS networks require the exchange of information among network elements for each subscriber data, voice, video, IM or other type of SIP session. More specifically, subscriber and session authentication, authorization, location, charging and quality of service (QoS) information must be exchanged among HSS, PCRF, MME, CSCF and other elements within a single service provider's network. This information must also be exchanged between visited and home networks for roaming subscribers. Diameter is the IP signalling protocol that supports this policy information exchange in all-IP networks.

The Diameter Routing Agent defined by 3GPP and GSMA, is a new network element that controls Diameter signalling, enabling the seamless communication and control of information between network elements within LTE or IMS networks and across LTE network borders. A DRA reduces the mesh of Diameter connections that negatively impacts network performance, capacity and management.

As LTE networks grow with new elements, the resulting provisioning and routing updates in a very interconnected network element, is costly in two dimensions: it increases OPEX and it slows down growth. DRA's are needed to:

- Reduce processing load on Diameter elements from having to handle too many SCTP and TCP transport layer connections
- Distribute and load balance traffic to effectively use existing Diameter agent capacity
- Prevent element overload and service interruption
- Simplify the provisioning and troubleshooting of connectivity between core Diameter elements
- Enforce business logic through AVP-driven routing as well as manipulation of Diameter AVPs
- Interwork transport protocols and IP version between core Diameter elements
- Ensure seamless interworking among Diameter interfaces at the transport and application layers.
- Provide security mechanisms at the network edge by utilising IPSec encryption, Denial-of-Service protection, Network topology hiding, etc.

Security in LTE Networks

LTE has been developed from an architectural point of view as well as industry de-facto deployments to run over Next Generation Networks: All-IP transport capability built on the Internet Protocol family of standards and giving rise to separate domains of security when implementing end-end networks.

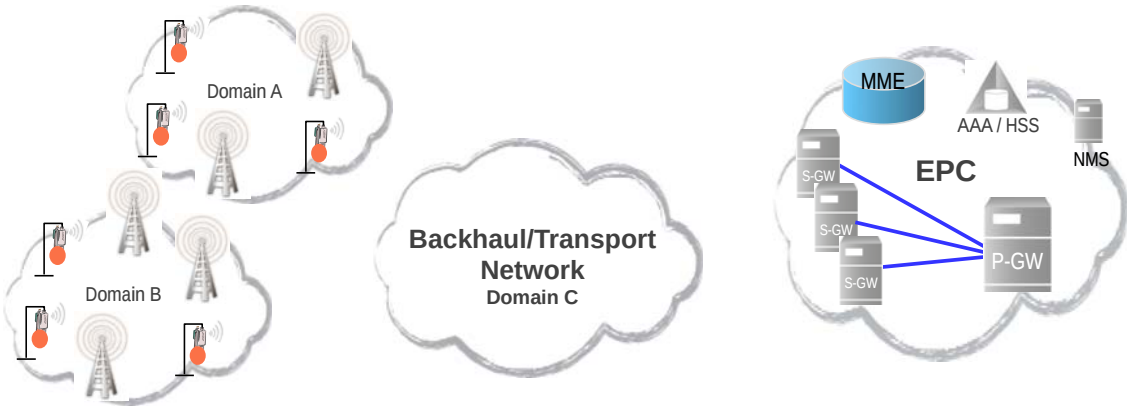

Figure 2. Architecture Domains of Security in a typical LTE deployment

Unlike previous technologies such as Circuit-Switched PDH/SDH and Packet-Switched ATM transport networks, IP protocols in their own right do not authenticate customer premises or remote site equipment (such as Base Stations) with their core network components, and vice-versa, in the same way that SS7 did and so this gives rise to potential security threats such as "man in the middle" and denial of service attacks. In particular, but not exclusively, such attacks to the control/signaling and operations and maintenance planes can have disastrous impact on network stability, not to mention exploit fraud opportunities.

As an additional requirement, very often LTE network providers will need to procure backhaul connectivity from Base Station sites, Femto & Pico Cells from 3rd-party providers and would wish to secure the data (signaling, O&M and data plane) from snooping or interception which could be used for gathering intelligence for example on traffic volumes and transactions being processed.

A Security Gateway (Sec-GW) acts as the “Inter Domain Police” between each of the domains of security: The RAN, the backhaul and the EPC. For non-Trusted integration to the EPC, the Sec-GW can also protect other access networks such as Wi-Fi and is capable of delivering the following functions:

- Network attachment authentication and authorization from site equipment
- Separation and specific QoS treatment of the different planes within LTE , namely S1-MME (signaling and control), Operations and Maintenance, S1-U (data) and X2 (handover)
- Aggregation function for eNodeB, Pico and Femto Cells requirement the same security functions (authentication, authorization)
- Encryption of sensitive data and control planes, e.g. S1-MME and O&M

The Sec-GW is used to originate and terminate secure associations between those components that are “under threat” or where security risks exist. IPsec tunnels are

established both inside the home network (Zb) and between home and visited networks (Za) with pre-shared security keys, which can take a number of different formats. 3GPP TS 33.210 mandates that the IPsec tunnels enforce traffic encryption, for added protection, according to the parameters exchanged between the two parties during tunnel setup.

For the home network it is envisaged that the security gateway will be used to secure S1-MME, S1-U and X2 interfaces to the eNodeB.

An EPC Core is typically owned by an individual mobile operator and therefore is considered secure. Similarly the LTE air interface is encrypted (secure) between the User Equipment and an eNodeB. Across the LTE access backhaul network encryption of Network Access Stratum (NAS) signalling is performed between the User Equipment (UE) and the MME. This maintains the security of NAS signalling between the UE and the EPC core. However, encryption of user data from the UE is terminated at the eNodeB. This obviously presents a security risk for user-plane data between the Serving Gateway (S-GW) deployed in a secure site and the remote eNodeB's.

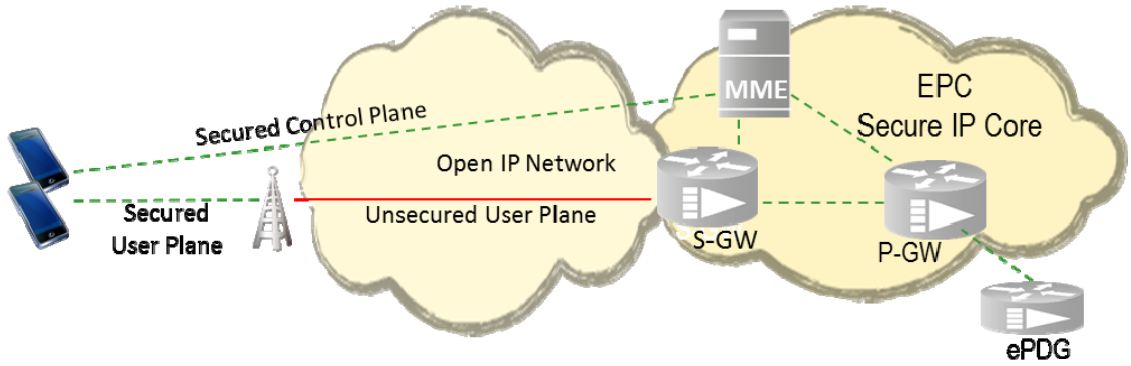

Figure 3. Identifying the Security Risk in LTE Network

Un-encrypted user data is subject to being tapped or "sniffed" within an open / shared backhaul network, as well as at the eNodeB interface (particularly in physically unsecured deployments such as in-building eNodeB's), therefore there is a potential for cyber-attacks, such as Denial of Service, on eNodeB's and S-GW's (e.g. from a device placed at the eNodeB site or within the access backhaul site masquerading as an eNodeB or S-GW).

Optimised VoLTE Architecture

The Figure below shows the optimised intra-PLMN VoLTE Architecture incorporating Sec-GW and DRA technology.

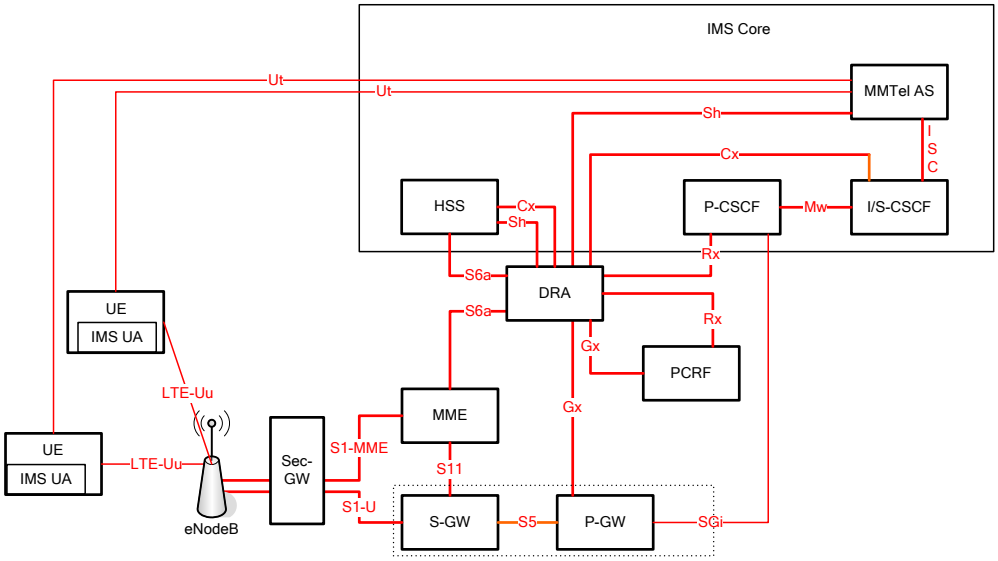

Figure 4. Optimised Intra-PLMN VoLTE Architecture

NOTE: The Gm interface (UE to P-CSCF) is a focus for testing although not explicitly shown in the above figure.

Key Objectives of the VoLTE Interoperability Event 2011

It is vital that operators have confidence in the multi-vendor interoperability of EPC and IMS components as a solid basis for VoLTE before volume deployment can begin. Demonstrating this capability in action was a key overarching objective of the VoLTE Interoperability Event 2011. The following equipment types (and associated vendor instances) participated in the event:

- In Germany, the equipment types included UE (3), eNodeB (2), MME (5), S-GW (5), P-GW (5) , PCRF (5), HSS (4), IMS Core (4), MMTel AS (3), P-CSCF (6), DRA (4), IBCF (4) and Security GW (1).

- In China, the equipment types included UE (2), eNodeB (1), MME (1), S-GW (2), P-GW (2), PCRF (1), HSS (1), IMS Core (1), MMTel AS (1), P-CSCF (1), DRA (1) and IBCF (1).

In addition, the VoLTE Interoperability Event 2011 was designed to:

- Validate the maturity of EPC network interfaces to enable multi-vendor support.
- Demonstrate that an EPC network can manage session control with an applied Quality of Service for default and dedicated bearers.

- Validate the maturity of IMS network interfaces to enable multi-vendor support,
- Demonstrate the support for user roaming between different networks.
- Validate VoLTE and MMTel services for both home registered and roaming UEs,
- Validate VoLTE and MMTel services over an interconnect between IMS networks,
- Demonstrate the LTE Handover capability
- Demonstrate the Robustness capability of EPC network nodes

Key Statistics

The VoLTE Interoperability Event 2011 was held from September 12th – 30th, 2011, at two major Service Providers labs; China Mobile Research Institute Laboratory in Beijing, China and Vodafone Test and Innovation Centre in Düsseldorf, Germany.

Over 65 network components from 19 participating vendors were tested by 60 test engineers using approximately 200 pages of test plans during this 15-day event.

The test scenarios incorporated a total of 89 test cases. Taking account of different vendor combinations, the 89 test cases resulted in a total of 561 scheduled tests being defined. Of the 561 defined tests, a total of 204 were executed of which 163 tests were successfully completed and 41 failed. In those cases where defined tests were not run, it was due to a combination of lab configuration limitations, equipment limitations or lack of time. Appendix A gives a detailed summary of the test results.

Key Results

- VoLTE calls and supplementary services, based on GSMA recommendations, are a viable solution for providing voice services for LTE access, including for Roaming and Interconnect scenarios.
- This test event showed basic interoperability between the different nodes in a multi-vendor configuration.
- The IMS Soft Clients interworked successfully with the LTE data dongle for LTE Attach and additionally with the IMS Core Network and MMTel AS to provide IMS services to the end user.
- Interaction with service layer (IMS and MMTel AS) was successfully demonstrated, with binding of Quality of Service to EPC bearers utilising Policy and Charging Control (PCC), providing relevant QoS for signalling and voice on the default bearer and dedicated bearers respectively.
- Diameter routing within the PLMN was greatly simplified by utilizing Diameter Routing Agents. DRA's were also shown to provide interworking between different transport layer protocols. Diameter Roaming interfaces S6a and S9 were routed successfully across the network interconnect via Diameter Routing Agents.
- IPSec security between eNodeB and MME/S-GW can be achieved utilizing a Sec-GW with complete transparency to signaling and media and no impact to other network elements.

- GTP protocol and S9 protocol proved to be mature and stable with no issues identified.
- The event showed that implementations based on different versions of the 3GPP Release 8 specifications are not fully interoperable, as there are backward incompatible protocol versions (observed for Gx and Rx interfaces)
- By using a commercial layer2 and above traffic capture and monitoring system with multiple connections points in to the System Under Test (SUT), the End2End packet path of the testing was greatly enhanced by capturing the path of packets through various Network Elements (NE's) such that packets from various parts of the system could be analysed by the commercial test tools – thus greatly aiding the interoperability effort as well as results analysis after the completion of the event.
- The commercial test tools used provided uncompromising visibility to all End to End procedures allowing rapid analysis and the ability to test the robustness of the various networks nodes.

Introduction

The VoLTE Interoperability Event 2011 test environment was based on:

1. Proving multivendor interoperability of Evolved Packet Core network nodes;
2. QoS control as an essential underpinning for services using PCC architecture and binding to the application layer in IMS;
3. Proving multivendor interoperability between IMS network nodes;
4. Proving VoLTE, including MMTel services via EPC and IMS, including interaction with the PCC architecture;
5. Roaming between EPC capable networks, including proving VoLTE and MMTel services for the roaming UE,
6. Proving VoLTE, including MMTel services, via the interconnect between IMS networks,
7. Intra-LTE Handover.
8. Robustness testing of EPC network nodes;

Publishing the results of the VoLTE Interoperability Event 2011 provides valuable feedback to the industry as a whole. Based on tests carried out in real world networked scenarios, specific feedback was also provided to the Standards Development Organization (SDO) community and to GSMA.

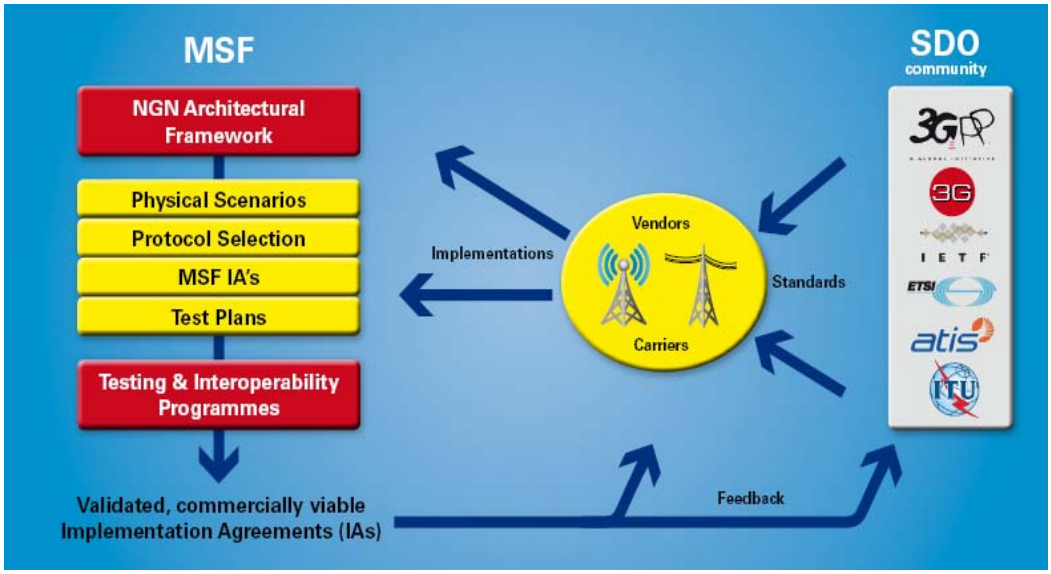

Figure 5. The results from the testing and interoperability programs are fed back to the relevant standards bodies, i.e. there is a virtual circle.

The key relationship between the MSF and relevant standards bodies is illustrated in Figure 5. As can be seen, there is a virtuous circle between testing based on the MSF architectural framework and IA's, and the feedback provided to the SDOs.

This white paper is organized into three parts and four appendices. In Part I, the planning that went into the VoLTE Interoperability Event 2011 is discussed. Part II discusses the three-week event, while Part III discusses the key results obtained from the VoLTE Interoperability 2011 Event.

Appendix A provides more details on the test scenarios; Appendix B highlights the interfaces that were tested, Appendix C discusses the benefits of MSF membership and Appendix D provides a brief resume of the participating companies.

Part I: Participants and Planning

The VoLTE Interoperability Event 2011 involved a diverse group of IP communications professionals whose common goal was to test the current capabilities of LTE and EPC products operating in real world Service Provider environments. In particular, the event focussed on Voice over LTE (VoLTE) via 3GPP LTE/EPC technology based on GSMA technical recommendations, which were endorsed by the MSF. The MSF developed a number of testing scenarios to validate core network interfaces in multi-vendor deployment scenarios for VoLTE.

This testing allows vendors to improve their products, Service Providers to accelerate their service deployment strategies, and the MSF to identify standards shortfalls to the appropriate SDO's.

A three-week test event involving two inter-networked lab sites, 19 vendors, over 60 participants, 65 network components and 200+ pages of test plans requires careful planning. A committee of 5 people, along with numerous volunteers, spent over 12 months preparing for the event.

Planning for the VoLTE Interoperability Event 2011 began in September 2010 by identifying scenarios and tests for the event. The scope of the event is defined in the Testing Scenarios document MSF- VoLTE-SCN-001-FINAL which is publicly available at http://www.msforum.org/techinfo/approved.shtml. A total of 5 scenarios were initially defined covering VoLTE, Roaming & Interconnect, non-LTE access to EPC, Handover and 3GPP Self-Organising Networks (SON). Each of the 5 main scenarios included a number of sub-scenarios. A sixth scenario was subsequently added to cover robustness testing. Test plans were developed for the majority of the identified sub-scenarios. During event planning, it became clear that commercial equipment was unlikely to be available with the functionality required for all test scenarios. Effort was thus focussed on the highest priority tests, and in some cases it was decided to postpone the writing of some test cases. This White Paper will therefore only detail the test scenarios that were executed during the VoLTE Interoperability Event 2011.

Inter-lab testing was a key objective of the VoLTE Interoperability Event 2011 with testing focussing on tests where inter-lab connectivity reflected real world deployment scenarios (i.e. roaming and interconnect). In addition, the initial activity focused on testing permutations of vendor-provided EPC technology within each lab. Given the complexity of the event and to help prioritize demand, the VoLTE Planning Committee developed a test schedule to maximise inter-vendor testing and vendor participation for all sessions. In particular, due to the large amount of equipment in the Vodafone site, it was decided to split the equipment between two logical sites which enabled parallel testing sessions at the Vodafone site as well as running roaming and interconnect tests between the two logical sites. Access to both the SUT and the NE's was provided by VSS Monitoring's intelligent tap solutions. This was facilitated with multiple connection points in to the network itself and on both the ingress and egress ports of several key functional nodes. Trace analysis and test equipment supplied by JDSU and EXFO received the monitored traffic flow from the intelligent taps and provided insight and analysis in to the operation of the network and the underlying interoperability of the actual NE's themselves. HP Quality Centre tool was employed as the results recording tool.

Test planning, host site selection, preparation and network interconnectivity all needed to be completed before the start of testing. Regular VoLTE Planning Committee meetings were held and vendor participation calls kept the participants informed of the preparation progress and their needed inputs and activities. Preparation activities peaked two weeks before the VoLTE Interoperability Event 2011 started, as participant engineers arrived at the host sites to ensure that the components were installed so that testing could commence on time. The two week set up period also encompassed a level of pre-testing, whereby connectivity and configuration between vendors equipment was performed.

Host Sites

Vodafone and CMCC provided host sites in Germany and China respectively, thereby allowing the various tests and scenarios to be deployed in an environment that replicates a live global network. Testing was structured to enable both intra-site and inter-site testing and a test schedule was devised to enable structured testing to be performed at each site as well as co-ordinating activity between the two sites for the roaming and interconnect scenarios.

The two host sites were:-

Vodafone provided the host site at the Test and Innovation Centre in Düsseldorf, Germany. The availability of the other site in China provided the opportunity for the VoLTE Interoperability Event 2011 to prove "real-life" roaming and interconnect scenarios. In addition, due to the amount of equipment in the Düsseldorf lab, it was decided to partition the lab into two logical labs and split the equipment between the two logical labs.

China Mobile provided the host site at the CMCC Research Lab in Beijing, China. The VoLTE Interoperability Event 2011 allowed China Mobile to establish a test network with the other host-site and establish ”real-life” roaming and interconnect scenarios.

Vendor Participants

Nineteen vendor companies participated in the VoLTE Interoperability Event 2011

The network equipment vendors were:

The Network protocol and call-flow analysis test equipment vendors were:-

The Robustness testing equipment was provided by:

The Test environment infrastructure & Traffic monitoring equipment was provided by:

Tables 1 and 2 show the components provided by the vendor participants at the Düsseldorf and Beijing sites respectively.

Vendor	LTE UE	eNodeB	Sec GW	MME	S-GW	P-GW	PCRF	HSS	P-CSCF	IMS Core	MMTel AS	DRA	IBCF	Test Eqpt
ALU				X	X	X	X							
Acme Packet									X			X	X	
Alepo							X					X		
Amdocs (Bridgewater)							X	X						
Cisco				X	X	X			X	X				
Codenomicon														X
D2 Tech	X													
Exfo														X
Genband											X		X	
Huawei								X	X	X	X		X	
JDSU														X
IPneo	X													
Metaswitch									X				X	
Samsung		X		X	X	X			X	X				
Stoke			X											
Tellabs				X	X	X								
Traffix												X		
ZTE	X	X		X	X	X	X	X	X	X	X	X		

Table 1. The VoLTE Interoperability vendor participants in the Vodafone host-site in Düsseldorf, Germany.

Vendor	LTE UE	eNodeB	MME	S-GW	P-GW	PCRF	HSS	P-CSCF	IMS Core	MMTel AS	DRA	IBCF	Test Eqpt
ALU		X	X	X	X	X	X						
Acme Packet								X			X	X	
CMCC	X								X	X			
D2 Tech	X												
JDSU													X
Tellabs				X	X								
Note:- The elements tagged in tagged as “CMCC” are other vendor elements already in the CMCC lab and which are being used in the VoLTE IOT event.													

Table 2. The VoLTE Interoperability vendor participants in the China Mobile host-site in Beijing, China.

.

Observing Companies / Organizations

MSF rules permit non-vendor companies to attend its interoperability events as observers. For the VoLTE Interoperability Event 2011, invitations were extended to MSF non-vendor members, GSMA members and partner fora/organizations. The following companies/organisations attended the VoLTE Interoperability Event 2011 as observers:-

Part II: The VoLTE Interoperability Event 2011 Execution

The VoLTE Interoperability Event 2011 involved two major Service Providers, one based in China, and the other in Europe. The test scenarios involved the connection of the host labs via an IP Security (IPSec) Virtual Private Network (VPN). The IPSec VPN tunnel was established and maintained to provide full connectivity between the two sites for the duration of testing. The previous successful LTE Interoperability Event had used IPSec VPN tunnels and thus the same technique was selected for the VoLTE IOT 2011 event.

The use of a flexible VPN also allowed each site to give participating vendors remote access to their equipment during the event. This was an important capability because it allowed vendors to complement onsite staff with personnel at home locations. The ability to support secure access from remote locations enhances flexibility and reduces cost for vendors.

Figure 6 presents a high-level diagram of the test environment used for the Vodafone Düsseldorf host-site.

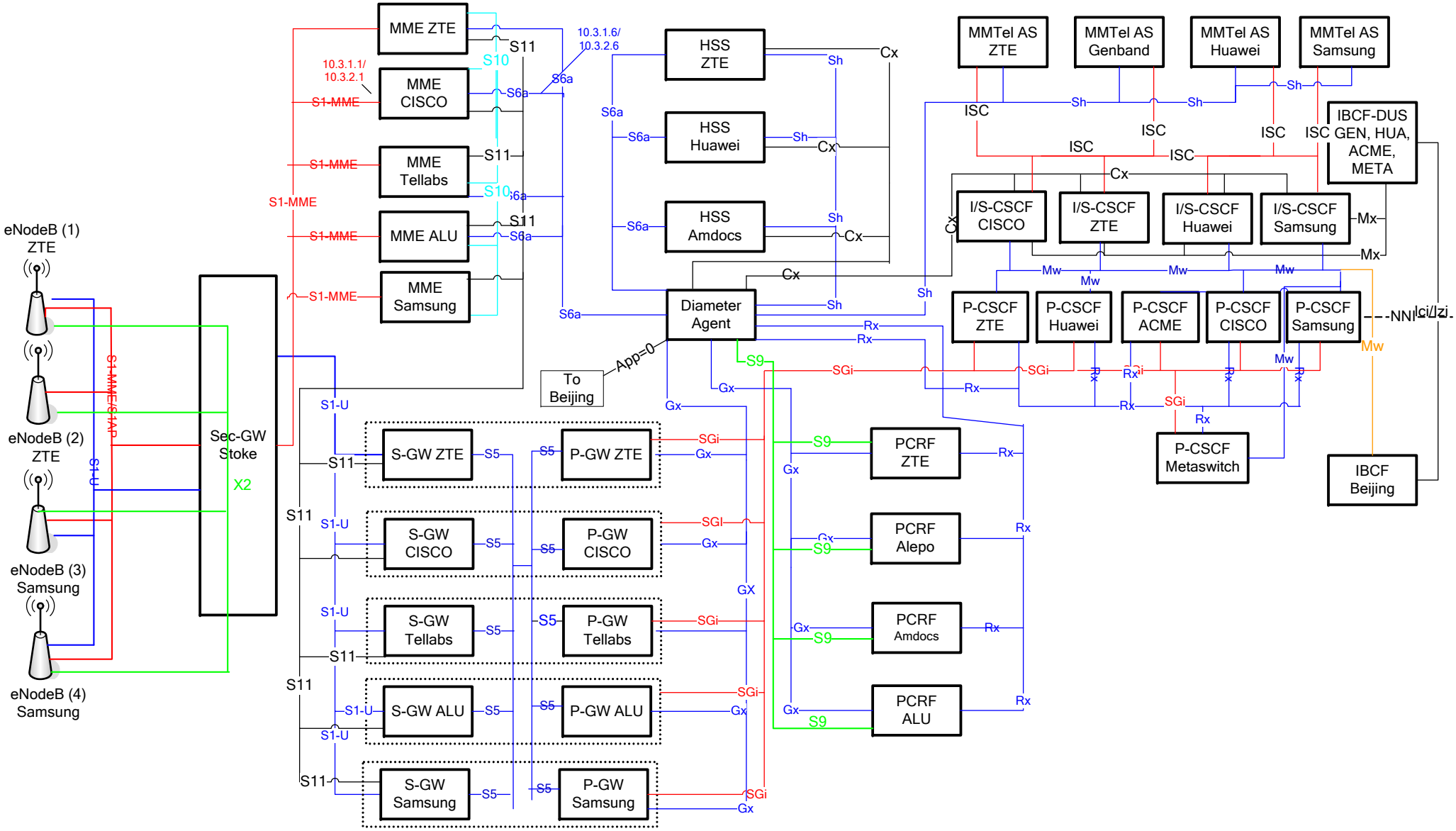

Figure 6. Test environment used for the Vodafone Düsseldorf host-site

Figure 7 presents a high-level diagram of the test environment used for the China Mobile, Beijing host-site.

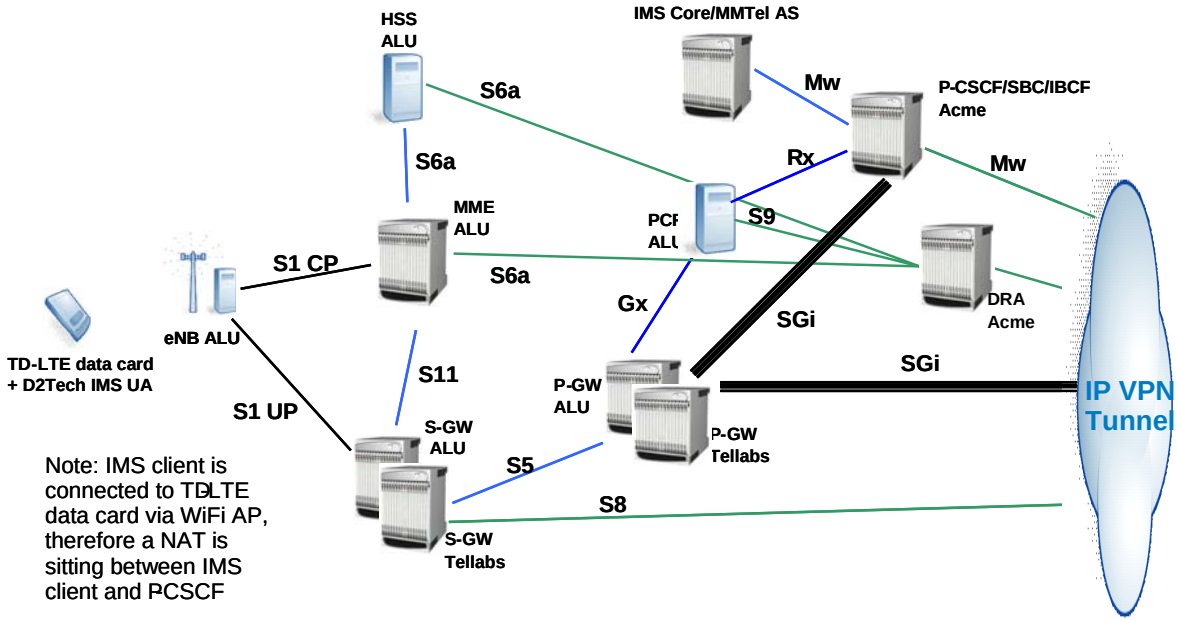

Figure 7. Test environment used for the China Mobile Beijing host-site

The Network Test Scenarios

Figure 8 is a high-level view of the EPC framework. The EPC network provides capabilities to attach multiple access technologies into a single core network infrastructure. These include LTE, legacy wireless access technologies (2G/3G), non-3GPP wireless access and fixed access. The common infrastructure provides a converged way to access a common service layer (e.g. Internet, IMS) and apply a consistent method of Quality of Service management and mobility management.

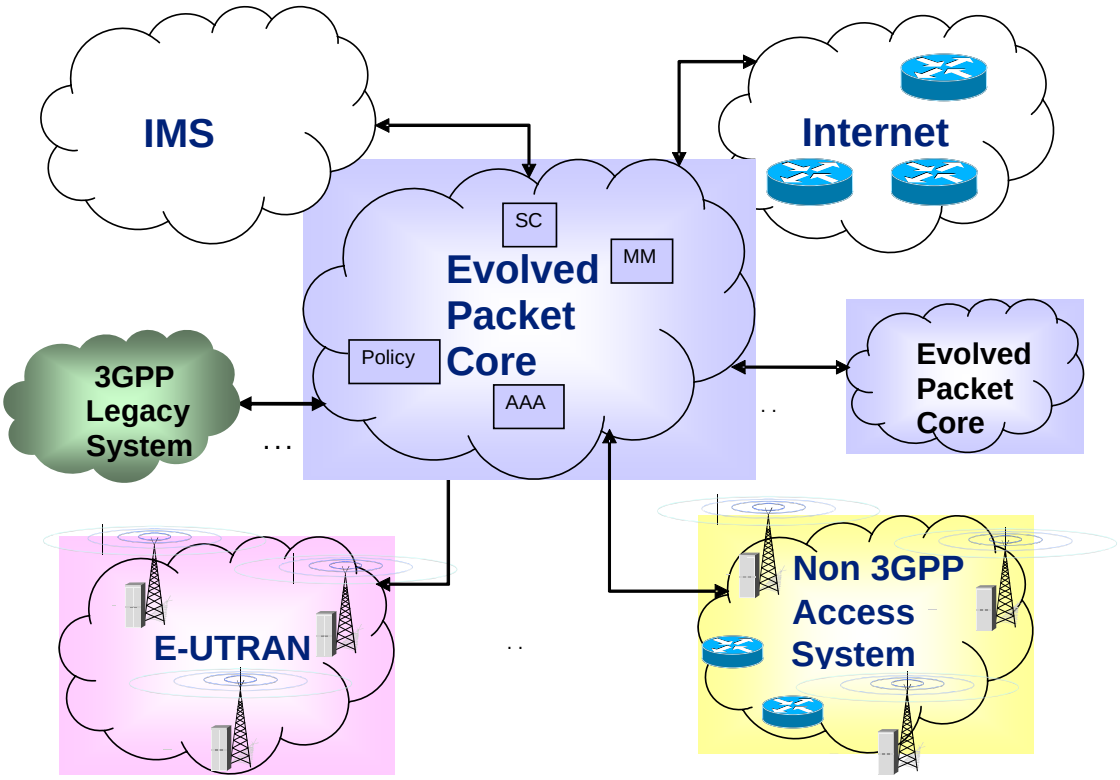

Figure 8. The Evolved Packet Core

The Evolved Packet Core can be accessed using all mainstream wireline and wireless access technologies, for connection to the application/service layer (e.g. IMS, Internet).

This high-level architecture formed the basis of the scenarios for the VoLTE Interoperability Event 2011. These scenarios were:

- Basic Interoperability:
  - VoLTE (Attachment/Detachment of an LTE capable UE to the Evolved Packet Core via an eNodeB and creation/deletion of a default bearer with related Quality of Service applied utilising PCC architecture, IMS Registration, IMS Session establishment and teardown utilising a dedicated bearer with related Quality of Service applied utilising PCC architecture and MMTel Service Configuration and usage).
- Roaming & Interconnect:
  - Roaming with Local Breakout in visited network (Visited P-CSCF) incorporating Attachment/Detachment of an LTE capable UE, IMS Registration, IMS Session establishment and teardown and MMTel Service Configuration and usage).
  - Interconnect between two UEs in their respective home PLMNs incorporating IMS Session establishment and teardown and MMTel Service usage.

- Handover:
    - S1 and X2 based Handover between eNodeB's.
- Robustness:
    - Core network traffic between S-GW, P-GW and IMS Core Network nodes.

These scenarios are discussed in more detail in Appendix A.

Test scenario validation

JDSU

The JDSU Signalling Analyzer solution, in a multi-user setup, was used to validate the completed test scenarios at both the Vodafone and China Mobile sites. This multi-user setup provided the participants of the Interoperability Event a real-time end to end view of the test scenarios as they were being executed.

The Signalling Analyzer provides support for the requirements outlined in GSMA IR.92 specifications for delivering Voice services over LTE (VoLTE).

The Signalling Analyzer provided a number of key capabilities:-

- End to End EPC and IMS Core Network Sub-System Visibility
- Real-Time Multiple Interface end to end Call Session Correlation and Measurements
- Real-time control-plane and user-plane correlation
- Access to common data source (probe) with the ability to perform independent functions/operations
- LTE/SAE security - EPS real time NAS Encryption deciphering
- Generic file sharing of the test scenarios results (both in JDSU proprietary format and Wireshark .pcap format)

The Signalling Analyzer supports an extensive set of LTE/EPC/2G/3G/IMS CN interfaces and is able to validate the outcome of each test case in real-time. After the validation of each individual test scenario the trace file was saved for possible future reference and traceability.

EXFO

The EXFO solution was used to validate the completed test scenarios at the Vodafone site.

Testing infrastructure support

VSS Monitoring

VSS Monitoring provided the Distributed Traffic Capture System as a traffic capture monitoring system. All packets generated during the event passed through the VSS Monitoring equipment and could then be passed on as appropriate to other elements (including the signalling analyser test tools). In this way, all traffic was properly segregated and all participants protected from having their packets snooped by other participants to whom there was no direct information exchange.

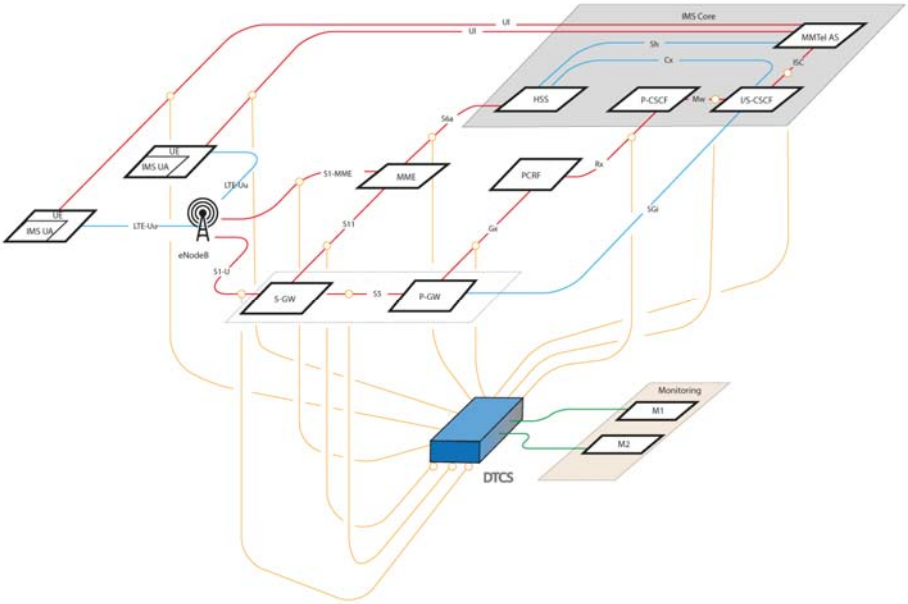

Figure 9. Monitoring system showing various connection points to the test network

VSS Monitoring also has the capability to provide the Test Acceleration System which enables the interoperability test equipment to be connected to the VSS Monitoring equipment. The introduction of the TAS would mean one pass at the physical cabling and the test network configuration. The re-configuration to provide the myriad of different combinations of network element setups, is realised by software configuration of the tool rather than having to physically re-cable and re-configure the complex network settings.

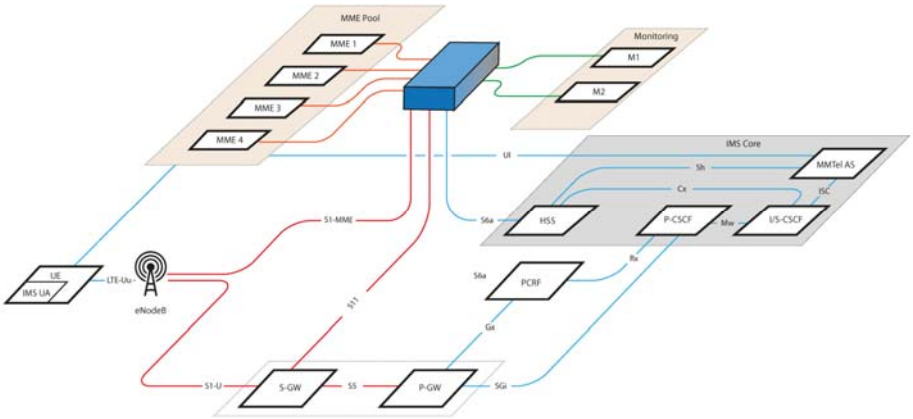

Figure 10. Example of how TAS could be deployed to speed up testing

Part III: Results and Issues

The event demonstrated that the GSMA technical recommendations, based on the 3GPP specifications, for providing end to end VoLTE were mature and interoperable. The event proved that VoLTE is a viable solution for providing voice services over LTE access technology, and can be deployed with roaming and interconnect functionality to provide equivalent service as CS-based voice services today.

Utilisation of Diameter Routing Agents provided optimisation of diameter routing within the core network and across the interconnect between network operators.

The inclusion of a Security Gateway provided a mechanism for secure communications between the eNodeB and Evolved Packet Core network with transparency for signalling and media.

However some issues were discovered and feedback may be provided to the relevant standards organizations where appropriate. In some cases, backwards incompatibility was encountered between implementations of different versions of 3GPP specifications (specifically Gx and Rx interfaces). Problems were also encountered with implementations that were not fully-compliant to the 3GPP specifications. Finally, in some cases it was difficult to re-configure the network components when testing different multi-vendor configurations.

The extensibility mechanism standardised by 3GPP for the Diameter-based interfaces has been utilised to provide a level of granularity only per 3GPP Release for the Gx and Rx interfaces. This reduces the level of interoperability of implementations that use different versions within the same 3GPP Release.

Implementations should implement all mandatory aspects of protocol interfaces in order to achieve full-compliancy and achieve maximum interoperability.

The re-configuration issue is mainly related to the test network and the requirement to test numerous different multi-vendor configurations, so it is not seen as a major issue for network deployments. While it may not be an issue once a network is operational and stabilized, it is however an issue during long cycle of testing and initial roll-out which justify the need for some interworking capabilities both at signaling (SIP/Diameter) and transport layers to ease those processes.

Though essential standards are reasonably mature, Service Providers will need to take care to clearly specify which version of the Release 8 specifications they are deploying. Events such as the MSF LTE Interoperability event highlight such difficulties and prove the validity of the MSF approach to achieving multi-vendor interoperability.

It is anticipated that backwards compatibility issues will be resolved as all nodes and interfaces are aligned to the 3GPP Release 9 and will be backwards compatible with this baseline release. The accuracy of this claim may be validated at subsequent Interoperability events.

Basic Interoperability:

In this scenario, intra-network testing utilised a single VoLTE architecture created using components from different vendors. Testing included LTE attachment and detachment from the network, SIP registration (to IMS), SIP session establishment,

SIP session teardown, MMTel Service Configuration across the Ut interface, and MMTel Service usage as specified by GSMA IR.92.

This test scenario demonstrated that VoLTE calls and supplementary services, based on GSMA IR.92, are a viable solution for providing voice services for LTE access. Testing consisting of equipment from different infrastructure vendors worked properly over the applicable 3GPP standardized interfaces.

It was shown that the IMS Soft Clients interworked successfully with the LTE data dongles for LTE Attach and additionally with the IMS Core Network and MMTel AS to provide IMS services to the end user.

Diameter routing within the PLMN was greatly simplified by utilizing Diameter Routing Agents. DRA's were also shown to provide interworking between different transport layer protocols.

IPSec security between eNodeB and MME/S-GW can be achieved utilizing a Sec-GW with complete transparency to signaling and media and no impact to other network elements.

Although basic interoperability was achieved, it was noted that implementations based on different versions of the Rel-8 Rx and Gx interfaces are not backwards compatible. Some implementations were discovered not to be fully compliant to 3GPP specifications, with missing mandatory functionality on various interfaces.

Appendix A provides more details on the test results.

Roaming & Interconnect:

The Roaming test scenario represents the test architecture where two subscribers, of the same Operator, perform an end to end call whilst one subscriber is in the HPLMN and the other is roaming in a VPLMN. The roaming subscriber attaches in the visited network where local breakout is applied, a Visited P-CSCF and home IMS services as defined in GSMA IR.65 and IR.88.

The Interconnect test scenario is where two subscribers, of different operators, perform an end to end call whilst in their respective PLMN's as defined in GSMA IR.65.

Roaming

This test scenario was designed as an inter-site test with the subscriber roaming in a 'visited network'. The LTE UE, eNodeB, MME, SGW, PGW and V-PCRF were physically in the visited network whilst the H-PCRF and HSS were physically located in the Home Network. Whilst the IMS Core was configured in the home network, the P-CSCF was configured in the Visited Network. This roaming model aligns with GSMA specifications IR.65 and IR.88.

The focus of these tests was to verify the roaming interfaces between the H-PLMN and V-PLMN required for roaming with VoLTE. Specifically the utilisation of a Diameter Routing Agent for routing Diameter messages between the MME in the visited network and the HSS in the home network with S6a and between the visited PCRF to home PCRF interaction across the S9 interface. Additional roaming aspects are the PCC interaction in the visited network (Rx and Gx interfaces) and the SIP interconnect between the P-CSCF in the visited network to the Session Border Controller in the home network.

This scenario tests LTE attachment and detachment of the visiting UE as well as IMS registration, IMS session establishment & teardown MMTel Service Configuration, and MMTel Service usage; as specified in GSMA IR.92, IR.65 and IR.88.

This test scenario demonstrated that the VoLTE architecture is a viable solution for providing voice services for LTE access for a user whilst in a roaming network. The testing consisted of equipment from different infrastructure vendors, and worked properly over the applicable 3GPP standardized interfaces.

The Diameter Roaming interfaces of S6a and S9 were routed successfully across the network interconnect via Diameter Routing Agents. It was shown that the S9 interface proved to be mature and stable for installing PCC and QoS rules.

IMS Registration was successful when the user was roaming validating the connectivity of a roaming UE to a home IMS Core Network (via a P-CSCF in a visited network to an SBC in the home network).

Although basic interoperability was achieved, it was noted that some implementations were discovered not to be fully compliant to 3GPP specifications, with missing mandatory functionality on various interfaces.

Appendix A provides more details on the test results.

Interconnect

This test scenario tests IMS session establishment, IMS session teardown plus MMTel Service Configuration, and MMTel Service usage for LTE UEs registered in their respective home PLMNs and interacting across the Ici/Izi reference points. Compliance against GSMA PRD IR.65 was tested.

This test scenario demonstrated that the VoLTE architecture is a viable solution for providing voice services for LTE access between users on different PLMN's. The testing consisted of equipment from different infrastructure vendors, and worked properly over the applicable 3GPP standardized interfaces.

Although basic interoperability was achieved, it was noted that some implementations were limited in how they performed the routing of SIP messages, i.e. based on IP Address only rather than IP Address and port number.

Appendix A provides more details on the test results.

Handover:

This test scenario was designed to validate the different handover cases. The primary focus included Intra-Radio Access Technology handover for LTE; including S1-based handover, X2-based handover, and MME/SGW relocation.

The focus of testing for this scenario was to demonstrate handover between LTE access (S1-based, X2-based, MME/SGW Relocation).

X2-based handover tests were successfully executed with a level of basic interoperability achieved.

S1-based Handover and SGW/MME relocation were successfully executed with a level of basic interoperability achieved.

SGW/MME Relocation could not be tested due to only one MME being available and therefore MME Relocation could not be performed.

Appendix A provides more details on the test results.

Robustness:

Robustness testing is based on the systematic creation of a very large number of protocol messages (tens or hundreds of thousands) that contain exceptional elements simulating malicious attacks. This method provides a proactive way of assessing software robustness, which, in turn, is defined as *"the ability of software to tolerate exceptional input and stressful environment conditions"*. A piece of software which is not robust fails when facing such circumstances. A malicious intruder can take advantage of robustness shortcomings to compromise the system running the software. In fact, a large portion of the information security vulnerabilities reported in public are caused by robustness weaknesses. Robustness problems can be exploited, for example, by intruders seeking to cause a denial-of-service condition by feeding maliciously formatted inputs into the vulnerable component. Certain types of robustness flaws (e.g., common buffer overflows) can also be exploited to run externally supplied code on the vulnerable component.

The following robustness testing was performed during the event:-

- Robustness testing for core network traffic between S-GW, P-GW and IMS Core Network nodes.

The objective was to test the robustness of the LTE and IMS core network order to ensure that the Core network is robust against malformed traffic sent by malfunctioning or badly interoperating Core elements or UE's. Malfunctioning Core elements could send anomalous data to other surrounding elements, affecting overall network stability. The goal is that the LTE and IMS network can handle anomalous traffic that is sent intentionally or unintentionally by other elements.

The S-GW testing was done with IPv4 robustness testing of the IP implementation within the module. The expectation of this test was a very clean result with no major failures as the IPv4 stack is one of the most tested network element.

The P-GW testing was done with IPv4 robustness testing of the IP implementation within the module. The expectation of this test was a very clean result with no major failures as the IPv4 stack is one of the most tested network element.

The IMS core network testing focused on testing the two elements P- and I-CSCF. These elements were tested through SIP UAS and IPv4 plain UDP test tools. The expected outcome was that there would be some issues with the SIP implementations.

The test results imply that there are potential issues in the network. Further testing is needed to fully characterize and address these issues. This is especially important in the S-GW and P-GW components and their IPv4 deployments. Since IPv4 is one of the most tested protocols there shouldn’t be any major issues within it and as these two components are the ones that face the customer and the Internet thus they are the components receiving the first impact of all the traffic and failures.

The IMS core is a bit more secure and it can be made more secure through filtering the traffic that reaches the components. The filtering can be done on malformed SIP packets but occasionally the filtering fails or hasn't been implemented at all. Thus SIP deployments should be mainly tested that they can manage the proper packets that they are likely to receive and make sure that the IMS core can handle the different

issues without causing issues to the end users trying to access or gain services through the IMS core.

Appendix A provides more details on the test results.

Future Work

Interest has been expressed on continuing work in this area by way of a future MSF VoLTE Interoperability Event.

The focus of such an event may initially be on the test cases that were not able to be executed in this event. These are as follows:-

- Non-LTE Access via S4-SGSN
- Non-LTE Access via legacy SGSN
- 2G/3G handover via S4-SGSN
- 2G/3G handover via legacy SGSN
- Automatic Neighbour Relation/Self Organising Networks

In addition, there are additional potential features that could also be part of a future IOT event:-

- SRVCC,
- SMS over IP
- Emergency Call,
- Network Interconnect via IPX
- RCS/RCSe
- non-3GPP access
- Performance Measurements

The timeframe of any future IOT event would be dependent on availability of UEs and network nodes supporting the required functionality as well as Service Provider interest in seeing such functionality tested in a multi-vendor environment.

Appendix A: The Test Scenarios

This appendix provides a detailed description of each of the test scenarios and presents the test results on a per-lab, per-scenario basis. When presenting the results, the following category types are defined to define the results of the test cases in the VoLTE Interoperability Event:-

- **Passed –** Test case was scheduled to be run and Passed the criteria defined within the Test Plan
- **Failed –** Test case was scheduled to be run and Failed the criteria defined within the Test Plan
- **Not Run –** Test Case was scheduled to be run, however due to lack of time this was not possible
- **N/A –** Test Case was identified to be not applicable to be scheduled (e.g. duplication of test case functionality)
- **Restricted –** Test Case was scheduled to be run, however due to issues with configuration or other limitations (UE and equipment restrictions) it was not possible.

Basic Interoperability - VoLTE

This test scenario demonstrated the attachment and detachment from the network, IP-CAN session establishment, SIP registration (to IMS), SIP session establishment/termination, and invocation/configuration of MMTel Services.

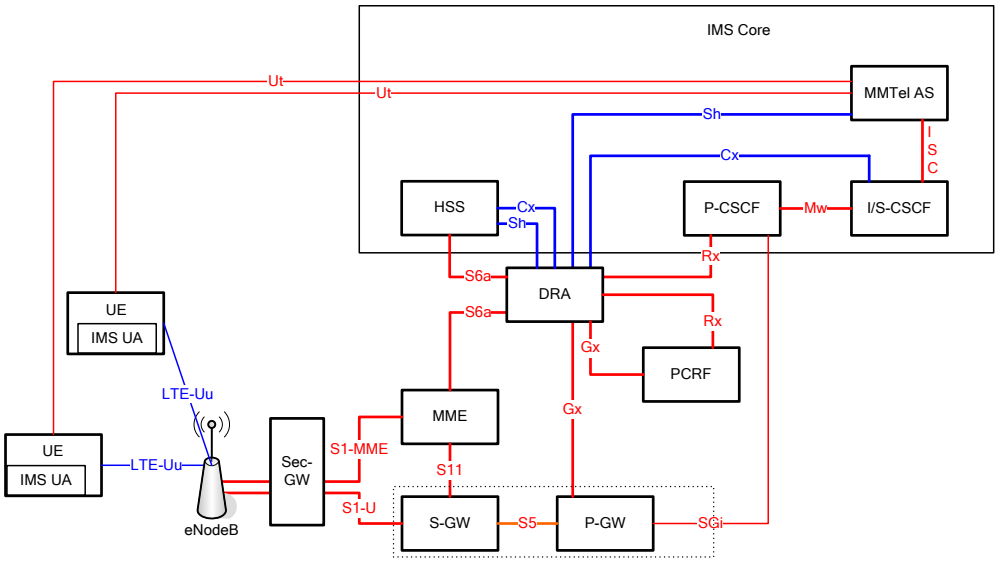

Figure 11 Test Configuration – Basic Interoperability VoLTE.

NOTE: The Gm interface (UE to P-CSCF) is a focus for testing although not explicitly shown in the above figure.

The network architecture for VoLTE Basic Interoperability is shown in Figure 11 above. The interfaces for which interoperability were tested are shown in red (i.e. S1-MME, S1-U, S5, S11, S6a, Gx, Rx, Gm, Mw, ISC, and Ut).

Test Objectives

1. To demonstrate the ability to perform UE Attach (IP-CAN Session Establishment) and UE Detach (IP-CAN Session Tear Down). This covers inter-working between eNodeB-EPC, between the EPC elements, MME-HSS and P-GW-PCRF for creation of a default bearer for IMS Signalling.

2. To demonstrate the ability to perform UE IMS Registration, and IMS Voice Session Establishment, IMS Voice Session Termination as defined by GSMA IR.92. This covers inter-working between UE, IMS Core Network, MMTel AS and PCC for creation of a dedicated bearer for voice.

3. To demonstrate the ability to perform MMTel Service Configuration over the Ut reference point for an attached UE.

4. To demonstrate inter-working between the UE, IMS Core and IMS-AS for MMTel Service usage as defined by GSMA IR.92.

5. To demonstrate the ability to provide a secure transport mechanism between the eNodeB and EPC elements utilising the Sec-GW to provide an IPSec tunnel.

6. To demonstrate the ability to provide an optimised solution for routing of Diameter messages within the core network utilising the DRA functionality.

Test Results and Observations

The Basic Interoperability – VoLTE test plan defined 28 basic test cases. By pairing different vendors' equipment in the various network configurations, the basic test cases were expanded to 224 test case instances scheduled in the Vodafone Düsseldorf lab, and 112 test case instances scheduled in the CMCC Beijing lab. The Vodafone Düsseldorf lab configuration included connections to one HSS and one S-GW located in the CMCC Beijing lab.

The following table summarizes the VoLTE test results.

No Run	Passed	N/A	Failed	Restricted	Total	Lab
69	32	28	8	87	224	**Düsseldorf**
0	76	0	12	24	112	**Beijing**

Table 3. Basic Interoperability – VoLTE Test Results

The "No run" test cases were largely due to lack of time to execute those test cases.

The "N/A" test cases were due to duplication of test scope already specified in other test cases.

The "Failed" test cases were largely due to backwards incompatibility between implementations of different versions of 3GPP specifications, implementations that were not fully-compliant to the 3GPP specifications, and the difficulty in re-

configuring the network components when testing different multi-vendor configurations.

The “Restricted” test cases were due to missing functionality that did not enable the test case to be executed.

Basic Interoperability – VoLTE demonstrated:-

- Multi-vendor interoperability of UE, eNodeB, Sec-GW, EPC, IMS/MMTEL, DRA and PCC technology.
- VoLTE calls and supplementary services, based on GSMA IR.92, are a viable solution for providing voice services for LTE access.
- The IMS Soft Clients interworked successfully with the LTE data dongle for LTE Attach and additionally with the IMS Core Network and MMTel AS to provide IMS services to the end user.
- GTP protocol proved to be mature and stable with no issues identified.
- Diameter routing within the PLMN was greatly simplified by utilizing Diameter Routing Agents. DRA's were also shown to provide interworking between different transport layer protocols.
- IPSec security between eNodeB and MME/S-GW can be achieved utilizing a Sec-GW with complete transparency to signaling and media and no impact to other network elements.

Several issues were encountered during the test execution of Basic Interoperability - VoLTE:

- PCC Issues
  - On Gx and Rx interfaces, it was discovered that some implementations do not implement the Supported Features AVP. On both Rx and Gx interfaces, a Mandatory Supported Feature is introduced per 3GPP Release (e.g. Rel8). However it was discovered that Release 8 compliant implementations were not implementing this functionality. This resulted in an error code being returned to the originator of the message, with resultant Gx and Rx commands being rejected. The sender may optionally fall-back to an earlier 3GPP Release of the interface, however this would have resulted in Release 7 behavior.
  - Backwards incompatibility between different versions of the same 3GPP Release was discovered on the Rx interface. Between version 8.4.0 and 8.6.0 of the Rx interface, backwards incompatible changes were introduced when the Specific-Action AVP was modified to introduce new events. As the Rx interface Supported Features introduces mandatory features per 3GPP Release, it lacks the granularity that is required to enable backwards compatibility between implementations based on the two different versions.
  - Mandatory AVP's were missing on the Gx and Rx interfaces in some implementations. The Bearer-Control-Mode and QoS-Information were missing on some implementations of the CCA of the Gx interface.

Precedence, Allocation-Retention-Priority and Rating-Group were missing on some implementations of the RAA of the Gx interface. The Auth-Application-ID was missing on some implementations of the AAR on the Rx interface.

  - Triggering of relevant Gx and Rx messages (CCR/AAR) were not performed by some implementations of P-GW and P-CSCF respectively. This results in lack of appropriate QoS being applied on the EPC bearer, and no session binding being performed in the PCRF between the IMS and EPC bearer.

- IMS Issues
  - On the Cx interface, it was discovered that an HSS implementation did not implement the Supported Features AVP. For Release 8 compliant implementations, a mandatory Supported Feature (Alias Indication) is standardized. Non support of this mandatory Supported Feature results in an error code being returned to the S-CSCF, with the SAR/SAA command being rejected – IMS Registration fails. The sender may optionally fall-back to an earlier 3GPP Release of the interface, however this would have resulted in Release 7 behavior.
  - The Sh interface was not supported on all implementations of HSS and MMTel Application Server. Whilst the Sh interface is optional, as user service information may be stored locally on the MMTel AS, it was discovered that some implementations of MMTel AS require the Sh interface to store user service information in the HSS. Without the support of the Sh interface, there is an interoperability issue between MMTel AS and HSS for some vendor combinations.
  - The Ut interface was not supported on all MMTel AS's in order to provide supplementary service configuration. Note that this is mandatory within GSMA PRD IR.92.
  - The Cx interface UAR/UAA command was found to fail in one configuration due to an incorrect implementation in the I-CSCF related to the setting of the Proxy-Bit in the command header. The Proxy-Bit is mandated to be set in both the request and answer messages, but was not being set by the I-CSCF.
  - 3rd Party Registration requests were not being sent by all implementations of S-CSCF to the MMTel AS. The 3rd party Registration is required to register the user on the MMTel AS and its availability for supplementary services.
  - The tests showed that there are ambiguities in the specifications for user authentication across the Ut interface. Specifically, it is not specified whether the username should be input as “user@domain” or simply as “user”. Similarly, it is not specified whether username and password should be case sensitive, or case insensitive.

- EPC Issues
  - Fragmentation issues were seen when the MTU size exceeded that specified by 3GPP for e.g. 1500 octets in the transport network, providing

a link MTU value of 1358 octets to the MS as part of the IP configuration information from the network. During the IOT event, it was necessary to also reduce the size of the SIP INVITEs (e.g. by reducing the number of codecs being offered).

- Transport Issues
  - SCTP was not initially supported by all DRA's, TCP was the transport protocol supported. 3GPP Diameter interfaces are based on SCTP for the transport protocol. This was resolved during the 3 week test period with SCTP being implemented.
  - The SCTP solution of one of the HSS's did not support dynamic local port allocation.
- Difficulty was experienced when re-configuring the network components for testing the different multi-vendor configurations. The issue is mainly related to the test network configuration and the desire to test various different multi-vendor configurations; it is not seen as a major issue for network deployments.

Security Gateway Testing

There are two modes in which IPSec tunnels can be established, both making use of IKE:

- Network-Network / Lan2Lan whereby static IP addresses are used, for the establishment of the tunnel during the authentication/authorization phase. Either end of the tunnel can initiate the process.
- Client-Server, whereby the customer premises equipment, typically the Femto gateway, is the only node allowed to setup tunnels. The additional advantage of the client-server model is that IP addresses can be allocated dynamically from a pool of addresses or by allocation from a DHCP server via the Sec-GW. The scalability of client-server mode can in theory be much larger (10x) but this has to be balanced with the total amount of traffic /throughput to be processed as the two requirements are related at least for peak operation.

Both of these were in use within the MSF VoLTE IOT and a single Sec-GW was used to serve both vendors/types of eNodeB's.

The tunnel establishment protocol is the “Internet Key Exchange” protocol or IKE. IKE presently has version 1 and version 2. The Sec-GW used within the MSF was able to support both but the only version supported by the eNodeB suppliers at this event was IKE v1.0. In summary, as with any newer versions, is that IKE v2.0 provides additional flexibility and security, for example support for NAT traversal, dead peer detection and Extensible Authentication Protocol (EAP) whilst IKE only support pre-shared keys.

The following table summarizes the Sec-GW test results.

Security Gateway Procedures			
Procedure	Tested	Result	Notes/Issues encountered
Tunnel (IKE) creation, including cookies	Yes	Passed	Minor issue with IP addressing subnet mask (changed eNodeB physical address subnet mask from /16 to /24)
Tunnel tear down	Yes	Passed	
Tunnel (Child SA) creation	Yes	Passed	
SA Rekeying Child SA rekey	Yes Yes	Passed Passed	Complete test with only one eNodeB vendor, time constraints restricted full testing with other.

Table 4. Sec-GW Test Results

Tests were executed based on IKE v1.0 and using client-server ("sessions") configuration, similar to Femto-cell deployment: eNodeB only can initiate IPsec setup, with ability to have dynamic IP address allocated from a pool of IP addresses held by the SSX. Tunnels were established successfully and operated for 2.5 days with no issues

Tests were executed based on IKE v1.0 and using lan2lan ("network-network") configuration, suitable for macro base station deployment, large traffic pipes. eNodeB or Sec-GW can initiate IPsec setup, with static IP addressing. Tunnels were established successfully and operated for 2 weeks with no issues.

Roaming & Interconnect

This test scenario demonstrates roaming (i.e. LTE attachment and detachment, IMS registration, IMS session establishment/teardown, MMTel Service configuration and MMTel Service usage for roaming UEs) and interconnect (IMS session establishment/teardown and MMTel Service usage between 2 LTE UEs registered in their respective home PLMNs).

This scenario was broken down into two sub-scenarios that are further detailed.

Roaming

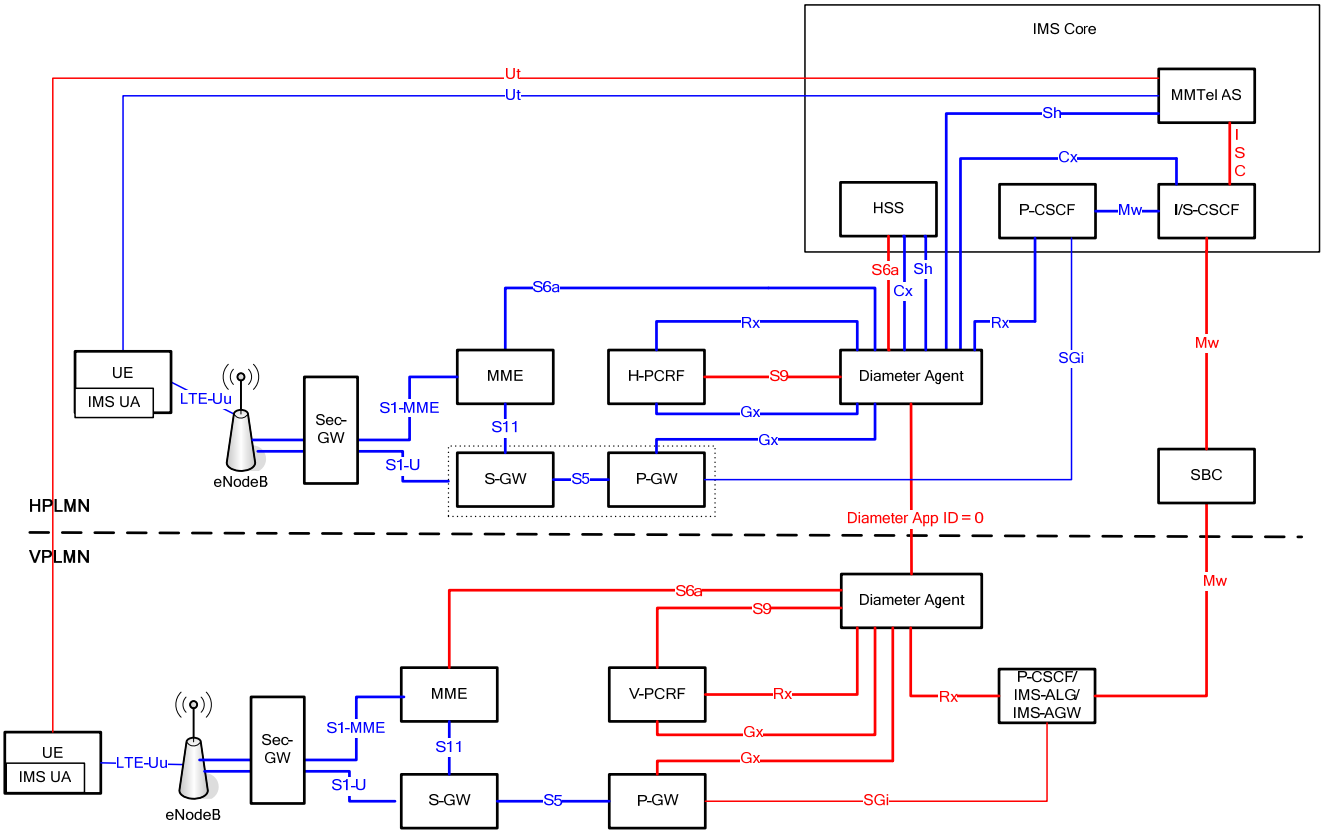

Figure 12. Test Configuration for Roaming

NOTE: The Gm interface (UE to P-CSCF) is a focus for testing although not explicitly shown in the above figure.

The network architecture for the Roaming test scenario is shown in Figure 12 above. The interfaces for which interoperability were tested are shown in red (i.e. S6a, S9, Rx, Gx, Mw, Gm, Ut and ISC).

<u>Objectives</u>

1. To demonstrate roaming with the UE in a Visited Network (i.e. eNodeB, MME, S-GW, P-GW, V-PCRF and P-CSCF in the VPLMN and the HSS, H-PCRF and IMS core in the HPLMN). Specifically, the ability to perform interworking between the MME and PCRF in the VPLMN with the HSS and PCRF in the HPLMN respectively, and the PCRF and P-CSCF in the visited network by performing UE Attach (IP-CAN Session Establishment) and UE Detach (IP-CAN Session Tear Down). Thus validating the Diameter roaming interfaces and DRA functionality for S6a and S9 as defined by GSMA IR.88.

2. To demonstrate UE IMS Registration, and IMS Voice Session Establishment, IMS Voice Session Termination as defined by GSMA IR.92, whilst roaming in a visited network.

3. To demonstrates the ability to perform MMTel Service Configuration over the Ut reference point for an attached UE, whilst roaming in a visited network.

4. To demonstrate inter-working between the UE, IMS Core and IMS-AS for MMTel Service usage as defined by GSMA IR.92, whilst roaming in a visited network.

Testing Results and Observations

The Roaming test plan defined 27 basic test cases. However, due to lack of time and available MMTel Application Servers, the IMS supplementary service test cases were not executed, and therefore the focus was on 5 basic test cases. By pairing different vendors' equipments in the various network configurations, the 5 basic test cases were expanded to 45 test case instances scheduled in both the Vodafone Düsseldorf and CMCC Beijing labs.

The following table summarizes the test results.

No Run	Passed	N/A	Failed	Restricted	Total	Lab
16	7	0	2	0	25	**Düsseldorf**
14	2	0	4	0	20	**Beijing**

Table 5. Roaming Test Results

The "No run" test cases were largely due to lack of time to execute those test cases, and MMTel Application Servers not being available.

The "Failed" test cases were due to implementations that were not fully-compliant to the 3GPP specifications and the difficulty in re-configuring the network components when testing different multi-vendor configurations.

Roaming demonstrated:-

- Successful LTE Attach and LTE Detach was performed demonstrating the Diameter Roaming interfaces of S6a and S9 were routed successfully across the network interconnect via Diameter Routing Agents.
- The S9 interface proved to be mature and stable for installing PCC and QoS rules. No issues were identified.
- IMS Registration was successful when the user is roaming validating the connectivity of a roaming UE to a home IMS Core Network (via a P-CSCF in a visited network to an SBC in the home network).

Issues were encountered during the test execution of Roaming:

- Mandatory Event-Trigger AVP with value of UE_IP_ADDRESS_ALLOCATE within the CCR on the Gx interface was not understood by one instance of a PCRF. This resulted in the CCR being rejected and the LTE Attach failing.
- The optional "warning header" within the Authentication Header was not understood by one of the UE's. This resulted in failure of IMS Registration.
- Due to time limitations and lack of MMTel AS's, no testing related to VoLTE calls and supplementary services could be performed.

- Difficultly was experienced when re-configuring the network components for testing the different multi-vendor configurations. The issue is mainly related to the test network configuration and the desire to test various different multi-vendor configurations, it is not seen as a major issue for network deployments.

Interconnect

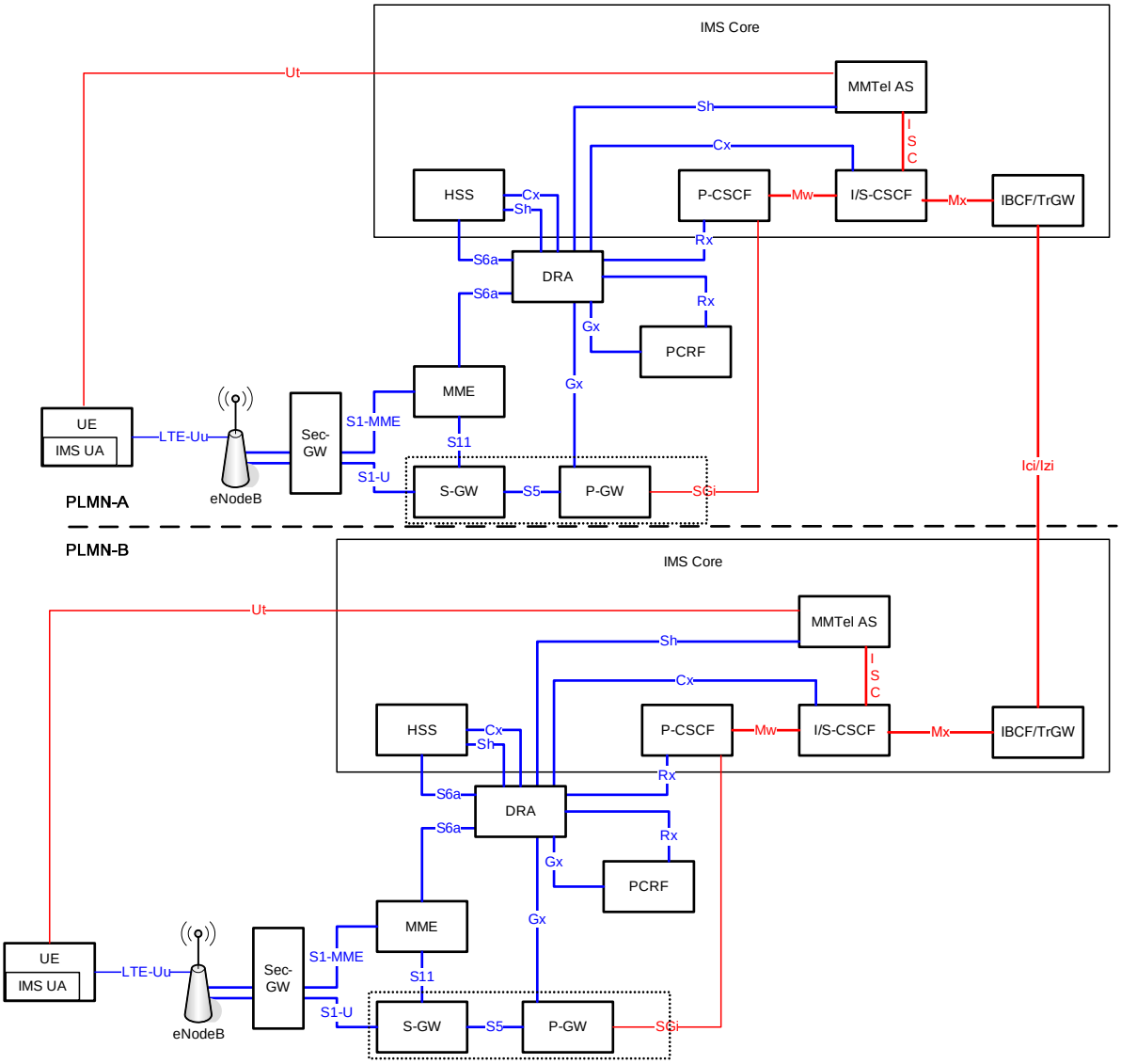

Figure 13. Test Configuration for Interconnect

NOTE: The Gm interface (UE to P-CSCF) is a focus for testing although not explicitly shown in the above figure.

The network architecture for Interconnect is shown in Figure 13 above. The interfaces for which interoperability were tested are shown in red (i.e. Mw, Mx, Gm, Ut, ISC and Ici/Izi).

Objectives

1. To demonstrate interconnect between two UE's registered in their respective home PLMN's. Specifically, the ability to perform interworking between the IBCF/TrGW's in the respective PLMN's validating the Ici/Izi interfaces and GSMA IR.65.

2. To demonstrate IMS Voice Session Establishment and IMS Voice Session Termination as defined by GSMA IR.92 and IR.65, with voice sessions established with a subscriber in a different PLMN.

3. To demonstrate the usage of MMTel Services as defined by GSMA IR.92, across a network-to-network-interconnect validating Ici/Izi.

Testing Results and Observations

The Interconnect test plan defined 20 basic test cases. However, due to lack of time and available MMTel Application Servers, the IMS supplementary service test cases were not executed, and therefore the focus was on 2 basic test cases By pairing different vendors' equipments in the various network configurations, the basic test cases were expanded to 106 test case instances scheduled in both the Vodafone Düsseldorf and CMCC Beijing labs.

The following table summarizes the test results.

No Run	Passed	N/A	Failed	Restricted	Total	Lab
19	6	0	1	0	26	**Düsseldorf**
72	8	0	0	0	80	**Beijing**

Table 6. Interconnect Test Results

The "No run" test cases were largely due to lack of time to execute those test cases, and MMTel Application Servers not being available.

The "Failed" test cases were due to implementations that were not fully-compliant to the 3GPP specifications and the difficulty in re-configuring the network components when testing different multi-vendor configurations.

Interconnect demonstrated:-

- VoLTE calls, based on GSMA IR.92 and IR.65, are a viable solution for providing voice services for LTE access between Mobile Network Operators.
- Multi-vendor interoperability of IBCF/TrGW's was achieved.

Issues were encountered during the test execution of Interconnect:

- Routing of SIP messages was only based on IP Address but not port number in one of the IBCF's. In implementations that contain P-CSCF, I-CSCF and S-CSCF within the same physical node, the IP Address is common, and the port number is utilized to distinguish between the different functional nodes. Therefore routing SIP messages only on IP Address, causes SIP messages

to be routed to the incorrect destination, resulting in IMS voice calls not being established.

- Due to time limitations and lack of MMTel AS's, no testing related to MMTel supplementary services could be performed.
- Difficultly was experienced when re-configuring the network components for testing the different multi-vendor configurations. The issue is mainly related to the test network configuration and the desire to test various different multi-vendor configurations; it is not seen as a major issue for network deployments.

Intra-LTE Handovers

This test scenario demonstrates LTE-LTE handover, both with registered terminals and with active sessions.

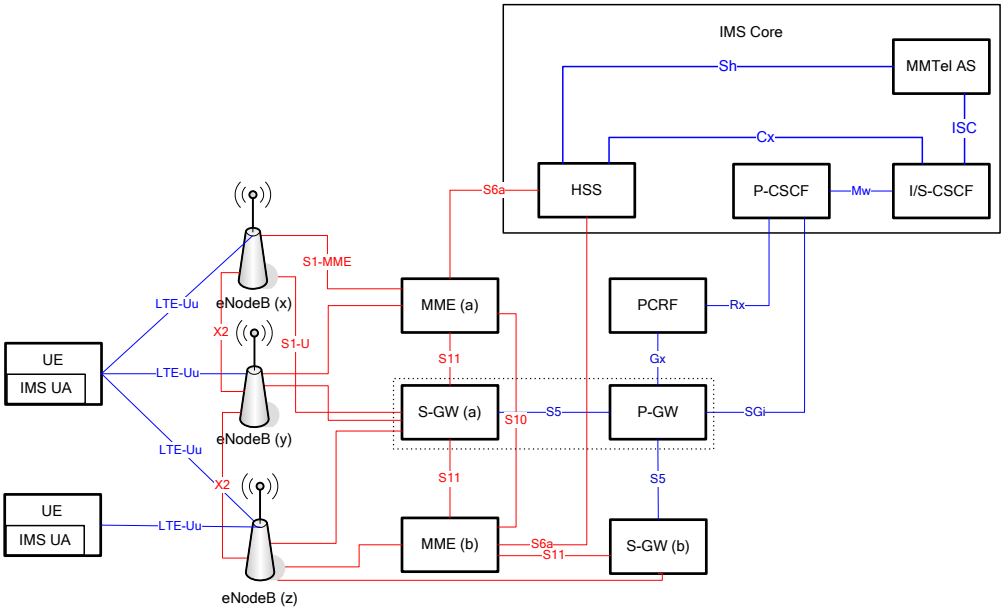

Figure 14. Test Configuration for Intra-LTE Handover

The network architecture is shown in Figure 14 above. The interfaces for which interoperability were tested are shown in red (i.e. S1-MME, S1-U, S10, S11, and S6a).

<u>Test Objectives</u>

1. To demonstrate handover of registered UEs, including those involved in active sessions, intra-LTE including between eNBs, MME re-location and S-GW re-location.

<u>Testing Results and Observations</u>

The Intra-LTE test plan defined 9 basic test cases. By pairing different vendors' equipments in the various network configurations, the basic test cases were expanded to 36 test case instances in the CMCC Beijing lab.

The following table summarizes the test results.

No Run	Passed	N/A	Failed	Restricted	Total	Lab
0	24	0	0	12	36	**Beijing**

Table 7. Intra-LTE Handover Test Results

The “Restricted” test cases were due to only one MME being available and therefore MME Relocation could not be performed.

Intra-LTE Handover demonstrated:-

- The interoperability between eNB and EPC is verified
- Multi-vendor eNB environment is not available for this scenario due to lack of other eNB vendors

Robustness

This test scenario demonstrated the usage of robustness testing in a LTE context and provided an overview of protocol implementation level vulnerabilities. The robustness test tool was physically located in the Düsseldorf lab and target equipment in the Beijing lab was tested remotely via use of the VPN.

The focus was mainly on the components that interact and effect the end user directly, the components tested within this environment where the S-GW, P-GW and IMS Core Services (I-CSCF, P-CSCF and S-CSCF). The test scenario did limit the protocol scope also to three main protocols (IPv4, UDP and SIP) due to the limitations in time and possible interoperability issues. Although this limitation was done it is suggested that the vendors taking part of this event would also include testing of the other core protocols in LTE networks mainly GTPv2 and SCTP.

This scenario was broken down into three sub-scenarios that are detailed below (S-GW Robustness, P-GW Robustness, and IMS Robustness). A common test configuration was used in all cases as shown below.

As an outcome of this testing it was noticeable that issues were found within all components, which from end user and provider perspectives raises some concerns in two ways were end users cannot gain access to the services and providers will lose revenues through this.

Robustness testing configuration

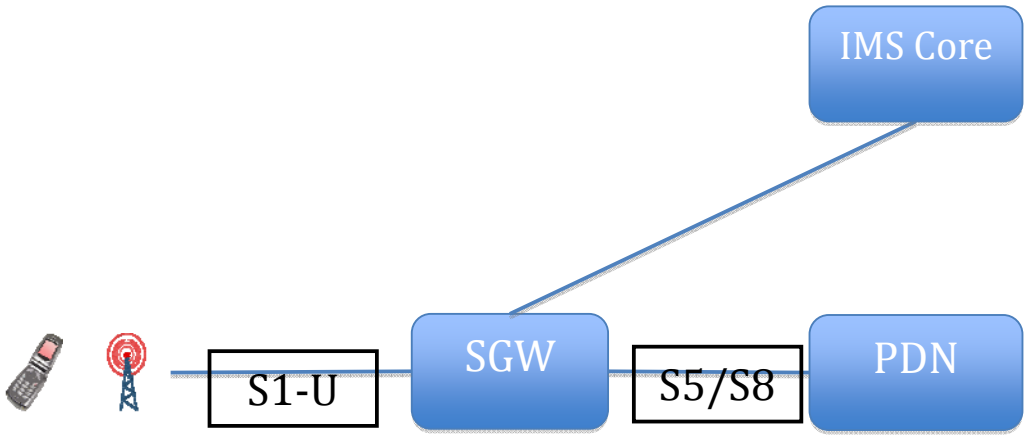

Figure 15. Test Configuration for Robustness

Definitions for Robustness results

No Interoperability contains that the test target allowed the test cases to come through but there were some failures within the configuration between the test target and test system. Most issues related to the fact that the user or callee was not recognized.

Full Interoperability means that the test target contained all the necessary information that allowed the test system to confirm all the settings without possible failures

Not Available means that the target system was not available for testing during the event due to other constraints.

Denial-of-Service is the amount of time the test target was out of communication. This was validated through sending first an anomalized request and then a valid request. If the test target failed to reply to the valid request then the test system records a failure and Denial-of-Service timer starts. The denial of service time represents the maximum amount of time the system was unavailable with one test case out of all the failed cases.

Fail/Pass criteria. Within the MSF test scenarios test target got a pass verdict if there was no failures detected. Fail is recorded if the test target has even one failed case this is because to limited time in the test event thus regression testing or failed case analysis was not done within this test event with the Vendors.

Robustness testing of the S-GW

The objective was to test the robustness of the LTE core network when traffic originates from the end user. The goal is that the LTE network can handle anomalous traffic that is sent intentionally or unintentionally by the end user equipment. Thus the testing equipment will be simulating end user in the network configuration in figure 15.

The S-GW testing was done with IPv4 robustness testing of the IP implementation within the module. There were five vendors that had provided their solutions to this network component. Out of the five vendors, four were available for robustness

testing. The expectation of this test was a very clean result with zero to few failures as the IPv4 stack is one of the most tested network element.

It should be noted that UDP and IPComp failed to Interoperate with all the solutions (RFC 3173), thus these were left out on this scenario.

This test contained the default test case amount from the tool that would represent 21% coverage of potential test cases that can be generated through the tool.

Below is a list of the vendors and the results:

Test Configuration	**Verdict**	**Result**	**Notice**
1	Pass	0 fails	
2	Fail	1 fail	1.5s Denial of Service time
3	Fail	8670 fails	11.5s Denial of Service time
4	Fail	1 fail	11.5s Denial of Service time
5	Inconclusive	N/A	Not Executed

Table 8. S-GW Robustness Test Results

Robustness testing of the P-GW

The objective was to perform robustness testing for the S11 interface in order to ensure that the Core network is robust against malformed traffic sent by malfunctioning or badly interoperating Core elements. Malfunctioning Core elements could send anomalous data to other surrounding elements, affecting overall network stability.

The P-GW testing was done with IPv4 robustness testing of the IP implementation within the module. There were five vendors that had provided their solutions to this network component. Out of the five vendors testing was executed on all five, but one P-GW was physically the same machine as the S-GW thus it was not retested within this test scenario. The expectation of this test was a very clean result with zero to few failures as the IPv4 stack is one of the most tested network element.

It should be noted that UDP and IPComp failed to Interoperate with all the solutions (RFC 3173), thus these were left out on this scenario.

This test contained the default test case amount from the tool that would represent 21% coverage of potential test cases that can be generated through the tool.

Below is a list of the results:

Test Configuration	**Verdict**	**Result**	**Notice**
1	Pass	0 fails	
2	Fail	3 fails	1.5s Denial of Service time

3	Skipped		Same device as SGW
4	Fail	1 fail	11.6s Denial of Service time
5	Fail	2 fails	1.8s Denial of Service time

Table 9. P-GW Robustness Test Results

Robustness testing of the IMS Core

The objective was to perform robustness testing for the SIP and UDP interfaces in order to ensure that the IMS Core network is robust against malformed traffic sent by malfunctioning or badly interoperating Core elements. Malfunctioning Core elements could send anomalous data to other surrounding elements, affecting overall network stability.

Within the IMS core the tests focused on testing the two elements P- and I-CSCF. These elements were tested through SIP UAS and IPv4 plain UDP test tools. The expected outcome was that there would be some issues with the SIP implementations but it should be noted that full Interoperability was not achieved with all the vendors and this might have an effect of the test outcomes by giving better results through dropping packets that are coming from a not known host.

The test scenario with SIP UAS represented 5% test coverage of the potential maximum test cases that can be generated through the tool. It should be noted that one vendor requested the tests to be stopped and their test coverage at the time of cancellation would represent 2.65% coverage. This scenario was only for the Options-Sequence within SIP with possibility to test another 19 different sequences. This means the test coverage is below 1% within the MSF VoLTE test event.

The UDP test scenario had 29% test coverage of the potential maximum test cases that could be generated through the tool.

For the P-CSCF and I-CSCF testing, four of the five test configurations were available for I-CSCF testing, and five out of ten test configurations were available for P-CSCF testing. Both P- and I-CSCF were tested utilizing SIP and UDP test tools. Generally the results were what were expected with some failures without any major Denial of Service time but as combined with the low coverage it should be noted that this requires further evaluation to be done before a comprehensive answer can be given.

Below is a list of the results:

I-CSCF Test Configuration (SIP)	**Verdict**	**Result**	**Notice**
1	Fail	1 fail	No full Interoperability
2	Fail	13 fails	0.5s Denial of Service time. Full Interoperability
3	Inconclusive	N/A	Not available
4	Inconclusive	N/A	No Interoperability

Table 10. I-CSCF SIP Robustness Test Results

I-CSCF Test Configuration (UDP)	Verdict	Result	Notice
1	Fail	78 fails	
2	Inconclusive	N/A	No Interoperability
3	Pass	0 fails	
4	Inconclusive	N/A	No Interoperability

Table 11. I-CSCF UDP Robustness Test Results

Below is a list of the results for the P-CSCF:

P-CSCF Test Configuration (SIP)	Verdict	Result	Notice
1	Fail	14 fails	33.7s Denial of Service time, full interoperability
2	Inconclusive	N/A	Not available
3	Fail	460 fails	3.6s Denial of Service time
4	Fail	1883 fails	11.6s Denial of Service time
5	Fail	12 fails	0.5s Denial of Service time
6	Inconclusive	N/A	No interoperability
7	Inconclusive	N/A	No Interoperability
8	Inconclusive	N/A	Not available
9	Inconclusive	N/A	No Interoperability
10	Fail	1 fail	0.5s Denial of Service time

Table 12. P-CSCF SIP Robustness Test Results

P-CSCF Test Configuration (UDP)	Verdict	Result	Notice
1	Pass	0 fails	
2	Inconclusive	N/A	No Interoperability
3	Inconclusive	N/A	No Interoperability
4	Inconclusive	N/A	No Interoperability

5	Pass	0 fails	
6	Inconclusive	N/A	No interoperability
7	Pass	0 fails	
8	Pass	0 fails	
9	Inconclusive	N/A	No Interoperability
10	Pass	0 fails	

Table 13. P-CSCF UDP Robustness Test Results

Robustness Tests Observations

There are two main scenarios that can be viewed through the testing results: a) a person with malicious intent willingly wants to bring down the network with anomalous packets or b) there is a component issue within the network and starts to send malformed packets which has a direct effect on the quality of the services within the network.

The test results imply that there are issues in the network protocol deployments that need to be tested further to validate these results. The priority is to focus on the S-GW and P-GW components and the IPv4 implementations within them. These components are facing the end user and potentially the Internet thus making them susceptible to attacks or malformed traffic.

The IMS core is more secure and it can be made even more secure through filtering the traffic that reaches these components. Filtering can be done to target specifically on malformed SIP packets but in cases where the filtering fails or it hasn't been implemented at all the SIP deployments within the IMS-core should be tested and make sure that the IMS core can handle the potential malicious packets without causing issues to the end users trying to access or gain services through the IMS core.

Robustness Tests Conclusion

Based on the results seen through the robustness testing it is quite obvious that further testing in the network components is needed since there are issues found. There is a clear importance of verifying IPv4 robustness is verified as a first priority issue since it will be in the core of the whole solution thus if it fails the whole network will become unusable for the end users. This creates loss of revenue for the operators and then annoyance towards the end users as they cannot reach the services needed.

Appendix B: Interfaces Under Test

The following is a set of references for the interfaces tested in the VoLTE Interoperability Event 2011 :

- LTE-Uu (UE – eNodeB)
  3GPP TS 36.300 (E-UTRAN protocol)

- S1-MME (UE – MME)
  3GPP TS 24.301 (Non Access Stratum)

- S1AP (eNodeB-MME)
  3GPP TS 36.413 (S1 Application Protocol)

- S1-U (eNodeB - S-GW)
  3GPP TS 29.281 (GTPv1-U)

- X2 (eNodeB – eNodeB)
  Signaling 3GPP TS 36.423 (X2 Application Protocol).

  User Plane 3GPP TS 29.281 (GTPv1-U)

- S3 (S4 SGSN – MME)
  3GPP TS 29.274 (GTPv2-C)

- S4 (S4 SGSN – S-GW)
  Control Plane 3GPP TS 29.274 (GTPv2-C).

  User Plane 3GPP TS 29.281 (GTPv1-U).

- S5 (S-GW - P-GW)
  User Plane 3GPP TS 29.281 (GTPv1-U)

  Control Plane 3GPP TS 29.274 (GTPv2-C)

- S6a (HSS – MME)
- 3GPP TS 29.272 (Diameter)

- S6b (P-GW – 3GPP AAA)
  3GPP TS 29.273 (Diameter)

- S6d (HSS – S4 SGSN)
  3GPP TS 29.272 (Diameter)

- S8 (S-GW – P-GW)
  User Plane 3GPP TS 29.281 (GTPv1-U)

  Control Plane 3GPP TS 29.274 (GTPv2-C)

- S9 (PCRF – PCRF)
  3GPP TS 29.215 (Diameter).

- S10 (MME – MME)
  3GPP TS 29.274 (GTPv2-C).

- S11 (MME – S-GW)
  3GPP TS 29.274 (GTPv2-C)
- S12 (UTRAN – S-GW)
  3GPP TS 29.281 (GTPv1-U, utilized for direct tunnel model).
- Gx (PCRF – P-GW)
  3GPP TS 29.212 (Diameter).
- Rx (PCRF - IP Application [P-CSCF for IMS])
  3GPP TS 29.214 (Diameter).
- Gr (SGSN – HSS)
  3GPP TS 29.002 (MAP)
- Gn (SGSN – MME / SGSN – P-GW)
  Control Plane 3GPP TS 29.060 (GTPv1-C)

  User Plane 3GPP TS 29.281 (GTPv1-U)
- Gm (UE – P-CSCF)
  3GPP TS 24.229 (IMS SIP)
- Mw (x-CSCF – x-CSCF)
  3GPP TS 24.229 (IMS SIP)
- ISC (S-CSCF – AS)
  3GPP TS 24.229 (IMS SIP)
- Ut (UE – AS)
  3GPP TS 24.623 (XCAP)
- SGi (EPC based PLMN and another packet data network)
  3GPP TS 29.061 (IP)

Appendix C: The Benefits of MSF Membership

The MSF is a global association of service providers, system suppliers, test equipment vendors, and users committed to developing and promoting open-architecture, multiservice Next Generation Networks. Founded in 1998, the MSF is an open-membership organization whose members are drawn from the world's leading IP communications companies. Historically, the MSF developed Implementation Agreements (IAs), promoting worldwide compatibility and interoperability of network elements, and encouraging input to appropriate national and international standards bodies. However, this role has become less of a focus as a standard architecture has emerged and protocol profiles are being defined in other SDOs and industry fora (e.g. 3GPP). The MSF primarily focuses on running IOT events to facilitate the deployment of next-generation multi-service networks, driven by its member needs. In addition, in 2009, the MSF decided to complement its established biennial Global MSF Interoperability (GMI) events by more targeted test events focused on critical and timely issues associated with deployment of IP communications. The VoLTE Interoperability Event 2011 is the third test event of this nature. For a history of MSF IOT events as well as information on planned upcoming IOT events, see http://www.msforum.org/interoperability/GMI.shtml.
.

The advantages of MSF membership include:

- Access to more than ten years of ground-breaking industry work with input from key service providers and vendors,
- The experience of some of the world’s leading scientists and engineers,
- The opportunity to leverage the external talent pool active in the MSF to more efficiently implement a validated architecture built on industry-standard protocols,
- The ability to validate product implementations in industry-leading interoperability events.

In addition, service providers and equipment vendors that actively participate in MSF IOT events learn how multivendor next-generation products and networks will interoperate in the real world. That information translates into several financial benefits:

- Reduced time to market for deployment of interoperable solutions,
- Decreased costs and resources to resolve interoperability issues,
- Improved protocol documentation through facilitating clarifications in the tested standards via feedback to the appropriate SDOs ,
- Thoroughly evaluated architectural framework for cooperatively designing end-to-end networking solutions.

The MSF's IOT program is designed to facilitate implementation of NGNs and to deliver the Forum’s mission statement that “We make Next Generation Networks work”. MSF IOTs validate products in the latest standards-based architectural framework using network deployment scenarios that are meaningful to Service Providers.

Appendix D: The Participants

This appendix provides a brief resume of the participant companies in the LTE Interoperability Event:-

Acme Packet

Acme Packet (NASDAQ: APKT), the leader in session delivery network solutions, enables the trusted, first-class delivery of next-generation voice, data and unified communications services and applications across IP networks. Our Net-Net product family fulfills demanding security, service assurance and regulatory requirements in service provider, enterprise and contact center networks. Based in Bedford, Massachusetts, Acme Packet designs and manufactures its products in the USA, selling them through over 200 reseller partners worldwide. More than 1,525 customers in 107 countries have deployed over 14,000 Acme Packet systems, including 90 of the top 100 service providers and 36 of the Fortune 100. For more information visit www.acmepacket.com.

Alcatel-Lucent

The long-trusted partner of service providers, enterprises, strategic industries and governments around the world, Alcatel-Lucent is a leader in mobile, fixed, IP and Optics technologies, and a pioneer in applications and services. Alcatel-Lucent includes Bell Labs, one of the world's foremost centres of research and innovation in communications technology.

With operations in more than 130 countries and one of the most experienced global services organizations in the industry, Alcatel-Lucent is a local partner with global reach.

The Company achieved revenues of Euro 16 billion in 2010 and is incorporated in France and headquartered in Paris.

For more information, visit Alcatel-Lucent on: http://www.alcatel-lucent.com, read the latest posts on the Alcatel-Lucent blog http://www.alcatel-lucent.com/blog and follow the Company on Twitter: http://twitter.com/Alcatel_Lucent.

Alepo

Alepo provides core network & business management solutions across next generation services and technologies, including LTE, WiMAX, Wi-Fi and Femto, as well as gateways into legacy technologies like UMTS, GSM, CDMA2000. With over 15 years of experience working directly with leading telecommunications service providers to bring the latest technologies and services to market quickly and cost-effectively, Alepo's innovation and expertise spans real-time policy & charging, fixed mobile convergence, packet core evolution, device management, mobile data offloading, carrier Wi-Fi hotspots and more.

www.alepo.com

twitter.com/AlepoUSA

facebook.com/AlepoUSA

Amdocs

Amdocs is the market leader in customer experience systems innovation. The company combines business and operational support systems, service delivery platforms, proven

services, and deep industry expertise to enable service providers and their customers to do more in the connected world. Amdocs' offerings help service providers explore new business models, differentiate through personalized customer experiences, and streamline operations. A global company with revenue of approximately $3.0 billion in fiscal 2010, Amdocs has over 19,000 employees and serves customers in more than 60 countries worldwide. Amdocs completed the acquisition of Bridgewater Systems in August 2011 and now offers Bridgewater's industry leading network and subscriber control solutions as part of the Amdocs Data Experience Solution Business Unit. For more information, visit Amdocs at www.amdocs.com.

Cisco

About Cisco

Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Today, networks are an essential part of business, education, government and home communications, and Cisco Internet Protocol-based (IP) networking solutions are the foundation of these networks.

Cisco hardware, software, and service offerings are used to create Internet solutions that allow individuals, companies, and countries to increase productivity, improve customer satisfaction and strengthen competitive advantage. The Cisco name has become synonymous with the Internet, as well as with the productivity improvements that Internet business solutions provide. At Cisco, our vision is to change the way people work, live, play and learn.

Cisco's Mobile Internet Technology Group, MITG, is responsible for helping mobile operators manage the deluge of mobile data and migrate to next generation networks. This group provides the most intelligent, high-performance IP mobile networks enabling customers to deliver rich multimedia services. MITG solutions provide seamless integration and migration across a range of 2.5G, 3G, and 4G wireless radio access technologies with the highest quality and reliability.

Codenomicon

Codenomicon, the first commercial venture to utilize fuzzing technology to allow Customers gain visibility into potential vulnerabilities. Codenomicon solutions can be used in software security testing and network management situations. With Codenomicon's proactive security testing software and situation awareness tools you can discover and react to the problems at the earliest possible moment.

Proactive security testing. Codenomicon Defensics is a proactive testing solution for finding and mitigating both known and unknown vulnerabilities in software even before deployment, improving application and network security. In the core of the solution is fuzz testing, a method where invalid input are fed to the system under test to expose vulnerabilities.

www.codenomicon.com/defensics

Situation awareness. The management of critical infrastructure requires making fast and informed decisions. Thus, it is essential to acquire relevant information, and understand the relationship between individual events. The problem is that there is too much information available, making it extremely challenging to separate significant facts from irrelevant data. Codenomicon's situation awareness tools help with collecting, automatic filtering and

visualizing the information, and alerting stakeholders in real time, allowing you to make the right decisions.

www.codenomicon.com/clarified

Codenomicon's solutions are used by top governments and leading software companies, operators, service providers and manufacturers to secure critical networks and to provide robust and reliable products and services.

D2 Technologies

D2 is the recognized leader in converged IP communications software for devices used in next-generation networks such as 4G LTE and WiMAX. Manufacturers and service providers rely on D2 software to deliver carrier-grade IP communications across any network (WiFi, WiMAX, LTE, cellular, broadband, PSTN), service (voice, video, IM chat, SMS, presence/status, etc.) and system (IP PBX, UC, carrier, OTT, social network, etc.) for a broad range of fixed and mobile devices. From processing billions of VoIP minutes each month to adding enhanced IP communications for Android™, learn how D2 software is converging communications at www.D2Tech.com or follow the company on Twitter @D2Tech.

Exfo

EXFO (NASDAQ: EXFO, TSX: EXF) is among the leading providers of next-generation test and service assurance solutions for wireless and wireline network operators and equipment manufacturers in the global telecommunications industry. The company offers innovative solutions for the development, installation, management and maintenance of converged, IP fixed and mobile networks — from the core to the edge. Key technologies supported include 3G, 4G/LTE, IMS, Ethernet, OTN, FTTx, and various optical technologies (accounting for an estimated 35% of the portable fiber-optic test market). EXFO has a staff of approximately 1800 people in 25 countries, supporting more than 2000 telecom customers worldwide.

For more information, visit www.EXFO.com.

Genband

About GENBAND

GENBAND is a global leader of IP infrastructure solutions, enabling enterprise, service and content providers around the world to evolve communications networks through IP innovation. The Company offers market-leading Switching, Applications, Networking and Service solutions, with products deployed in over 600 customer networks spanning more than 80 countries. GENBAND is headquartered in Frisco, Texas, and has operations in 50 countries. To learn more, visit us on the web at www.genband.com.

GENBAND, the GENBAND logo and icon are trademarks of GENBAND.

Huawei

Huawei is a leading global information and communications technology (ICT) solutions provider. Through our dedication to customer-centric innovation and strong partnerships, we have established end-to-end advantages in telecom networks, devices and cloud computing.

We are committed to creating maximum value for telecom operators, enterprises and consumers by providing competitive solutions and services. Our products and solutions have been deployed in over 140 countries, serving more than one third of the world's population.

Huawei's vision is to enrich life through communication. By leveraging our experience and expertise in the ICT sector, we help bridge the digital divide by providing opportunities to enjoy broadband services, regardless of geographic location. Contributing to the sustainable development of the society, economy, and the environment, Huawei creates green solutions that enable customers to reduce power consumption, carbon emissions and resource costs.

IPNeo

IPneo provides innovative solutions that bring tomorrow's IP technologies to the hands of today's users. Focusing on IP Multimedia Subsystem (IMS), IPneo delivers standardized client software solutions enabling rich communication capabilities for end- users. IPneo client solutions pave the way for operators and OEMs to quickly attain their goals towards a convergent All-IP-Network in order to leverage the end-user satisfaction and to drive new streams of revenues easier than ever before.

At IPneo we value the growing needs for IP-based applications. Therefore, we provide our customers with a set of IMS features/APIs for RCS and VoLTE, that are all fully compliant with the IMS standards, quality-proven through a series of Inter-operability tests, and seamlessly portable to the leading handset equipment and mobile operating systems including: Android, iOS, and Windows Phone 7.

JDSU

JDSU (NASDAQ: JDSU; and TSX: JDU) innovates and markets diverse technologies that enhance the way people experience the world every day. We enable fast, high-quality communications, secure financial transactions, reliable consumer electronics, green energy, differentiated brands and a host of other solutions. We provide these solutions through three business segments: Communications Test and Measurement, Communications and Commercial Optical Products, and Advanced Optical Technologies. To learn more about JDSU, please visit www.jdsu.com and www.jdsu.tv and follow us on JDSU Perspectives, Twitter, Facebook and YouTube.

Metaswitch

Metaswitch Networks powers over 600 network operators worldwide and is a leading provider of the technologies and solutions that are empowering the migration of communications networks to open, next-generation architectures. For over 30 years, Metaswitch has been innovating solutions to simplify communications, add next-gen functionality and services, while addressing the challenges of converging networks and devices.

Samsung

Samsung Electronics Co., Ltd. is a global leader in semiconductor, telecommunication, digital media and digital convergence technologies with 2010 consolidated sales of US$135.8 billion. Employing approximately 190,500 people in 206 offices across 68 countries, the company consists of nine independently operated business units: Visual Display, Mobile Communications, Telecommunication Systems, Digital Appliances, IT Solutions, Digital

Imaging, Memory, System LSI and LCD. Recognized as one of the fastest growing global brands, Samsung Electronics is a leading producer of digital TVs, semiconductor chips, mobile phones and TFT-LCDs. For more information, please visit www.samsung.com.

Stoke

About Stoke, Inc.

Stoke is the mobile industry's only transformation platform, delivering future-focused thinking and solutions for 3G and 4G mobile broadband infrastructures. Stoke enables mobile operators, through the application of Business-Crossover™ thinking, to overcome limitations inherent in legacy approaches and architectures, helping them tackle the new realities of 3G mobile data service delivery today and successfully navigate their transition to 4G services platforms tomorrow. For more information, visit www.stoke.com.

Tellabs

Tellabs innovations advance the mobile Internet and help our customers succeed. That's why 43 of the top 50 global communications service providers choose our mobile, optical, business and services solutions. We help them get ahead by adding revenue, reducing expenses and optimizing networks.

Tellabs Smartcore® 9100 series is a purpose-built mobile packet core platform offering unmatched performance with integrated network intelligence. So you can deploy smart HSPA, LTE and WiMAX networks that optimize network resources, deliver new revenue generating services and monetize the mobile Internet.

Traffix Systems

Traffix Systems was born in the wake of the telecommunications industry's adoption of the Diameter signaling protocol as the preferred signaling protocol to enable the users to connect, move, use and pay for network resources and services in next-generation architecture such as LTE, IMS and HSPA+.

While acclaimed for its high bandwidth and the promise of exciting new data services, LTE introduces substantial core network complexity due to the addition of many more network elements, advanced services and new policy and charging schemes. Operators own the task of managing all this complexity, the most challenging of which occurring in the Diameter control plane.

Since 2005, the Traffix's team of experienced telecommunications experts has focused on solutions for the Diameter control plane with a portfolio of Diameter products including a Diameter Gateway, Diameter Load Balancer and Diameter Router.

With the adoption of HSPA+, IMS and LTE as the technologies of choice for mobile data and Diameter as the underlying signaling protocol, there is an increasing need for carrier-grade, Diameter signaling products. Traffix's products fulfill these needs, as well as each and every operator challenge for seamless and cost-effective signaling related to connectivity, scalability, routing, failover management and overload control, security and message normalization and visibility, performance monitoring and troubleshooting.

In 2011, Traffix announced a market-first: The Signaling Delivery Controller (SDC), a single platform consolidating fully-featured solutions of a Diameter Gateway, Diameter Load Balancer and Diameter Router to deliver a truly convergent solution. With its SDC technology, Traffix has set the industry benchmark for Diameter signaling solutions.

In addition to Diameter, the SDC supports a multitude of additional protocols, e.g. SS7, RADIUS, GTP', LDAP, HTTP, JMS. This makes it an attractive solution when interaction with legacy equipment is required.

With much of the groundwork already completed, Traffix strives to bring to market evolutionary signaling products that enable intelligent and simplified network control, management and advanced subscriber context awareness for operators to unleash the full potential of their 4G networks.

For more information, please visit www.traffixsystems.com or write info@traffixsystems.com.

VSS Monitoring

VSS Monitoring is the world leader in Network Intelligence Optimization, providing a visionary, systems-approach for optimizing and scaling the connectivity between network switching and the entire network intelligence ecosystem of analytics, inline security, and WAN acceleration tools. For more information, visit www.vssmonitoring.com.

ZTE

ZTE is a publicly-listed global provider of telecommunications equipment and network solutions with the most comprehensive product range covering virtually every sector of the wireline, wireless, service and terminals markets. The company delivers innovative, custom-made products and services to over 500 operators in more than 140 countries, helping them to meet the changing needs of their customers while achieving continued revenue growth. ZTE's 2010 revenue led the industry with a 21% increase to USD10.609 billion. ZTE commits 10 percent of its revenue to research and development and takes a leading role in a wide range of international bodies developing emerging telecoms standards. A company with sound corporate social responsibility (CSR) initiatives, ZTE is a member of the UN Global Compact. ZTE is China's only listed telecom manufacturer, publicly traded on both the Hong Kong and Shenzhen Stock Exchanges (H share stock code: 0763.HK / A share stock code: 000063.SZ). For more information, please visit www.zte.com.cn.