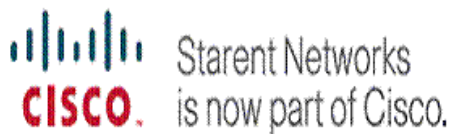




MultiService Forum

MSF LTE Interoperability

Multivendor testing in global Evolved Packet Core Networks



Empowered by Innovation



Abstract

This white paper provides a summary of the MultiService Forum's (MSF) Global LTE Interoperability event which took place from March 15-30, 2010.

The LTE Interoperability Event is designed to test standards compliance of Evolved Packet Core network scenarios of interest to major Service Providers, and to gauge vendor support for this technology. Building on the success of previous Global MSF Interoperability (GMI) events, the LTE Interoperability event provided the first global "real network" multi-vendor trial of the Evolved Packet Core infrastructure.

Incorporating the Evolved Packet Core defined within the Third Generation Partnership Project (3GPP) Release 8 (R8) standards, the MSF architecture introduced new access tiles to support LTE access and non-3GPP (specifically eHRPD) access to EPC. The IMS core network provided the application layer for which services may be deployed, and the binding of Quality of Service utilizing the Policy and Charging Control (PCC) for the bearer.

The event demonstrated that most of the defined LTE/EPC interfaces were mature and interoperable; however limited backwards compatibility between different implementations of 3GPP Release 8 specifications did create some issues. The fact that 3GPP does not require backward compatibility is a known limitation, but it is important to understand that this is limiting interoperability with commercially available equipment. Service providers will need to factor this into vendor selection. Highlights of the event included:-

- Sessions were successfully established via LTE access to EPC, with creation of default and dedicated bearers with appropriate Quality of Service applied.
- An end-to-end IMS Voice over LTE session was also successfully demonstrated,
- Access to the EPC via a simulated eHRPD access was successfully tested.
- Handover between LTE and eHRPD,
- Roaming was successfully tested.

Though the essential standards are reasonably mature, the implementation of early versions of the standards within several of the available implementations of network nodes highlights the problems that can arise due to non-backwards compatibility between 3GPP releases. It is also clear that early implementations have focused initially on development of LTE access to EPC and that support for legacy access (2G/3G) to EPC is somewhat behind. Events such as the MSF LTE Interoperability event highlight these issues and prove the validity of the MSF approach to achieving multi-vendor interoperability.

Contents

Executive summary	p. 4
The MultiService Forum (MSF)	p. 4
The LTE Interoperability Event	p. 4
Key Objectives of the LTE Interoperability Event	p. 4
Key Statistics	p. 6
Key Results	p. 6
Introduction	p. 7
Part I: Participants and Planning	p. 9
Host Sites	p. 9
Vodafone	p. 10
China Mobile	p. 10
Vendor Participants	p. 10
Part II: LTE Interoperability Execution	p. 12
The Five Network Test Scenarios	p. 13
Test Scenario Validation	p. 15
Part III: Results and Issues	p. 16
Future Work	p. 22
Appendix A: The Five Test Scenarios	p. 24
Scenario 1 – Basic Attachment	p. 24
Scenario 2 – Roaming	p. 28
Scenario 3 – non-LTE Access	p. 32
Scenario 4 – Handover	p. 36
Scenario 5 – Robustness	p. 40
Appendix B: Interfaces Tested	p. 45
Appendix C: The Benefits of MSF Membership	p. 46
Appendix D: Participants in the LTE Interoperability Event	p. 48

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 established Global MSF Interoperability (GMI) events are now being complemented by more technically focused test events. The LTE Interoperability Event being is the first example of a focused test event of this nature.

The LTE Interoperability Event

The LTE Interoperability Event is designed to test standards compliance of Evolved Packet Core network scenarios of interest to major Service Providers, and to gauge vendor support for this technology. Building on the success of previous Global MSF Interoperability (GMI) events, the LTE Interoperability event provided the first global "real network" multi-vendor trial of the Evolved Packet Core infrastructure.

Extending the IMS compliant MSF R4 architecture, the MSF defined:

1. LTE Access Tile based on Third Generation Partnership Project (3GPP) Release 8 (R8) Evolved Packet Core standards, and
2. eHRPD Access Tile based on Third Generation Partnership Project (3GPP) Release 8 (R8) Evolved Packet Core standards,

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 scenarios.

A total of 95 test cases were written across 5 scenarios. The scenarios were as follows:

- Scenario 1 – Basic Interoperability,
- Scenario 2 – Roaming,
- Scenario 3 – non-LTE access to the EPC,
- Scenario 4 - Handover,
- Scenario 5 – Robustness testing.

Key Objectives of the LTE Interoperability Event

The Evolved Packet Core (EPC) provides a comprehensive architecture that allows users to connect to the network via the LTE high-speed wireless access. This allows access to the applications and services that today's sophisticated users demand, while providing the necessary Quality of Service management and mobility functions.

The Evolved Packet Core has the following components:

- The Mobility Management Entity (MME) which is the heart of the control plane and session management functions. It also manages complex features such as resource allocation and bearer control for multiple nodes and gateways.
- The Serving Gateway (SGW) which routes data packets through the access network;
- The Packet Data Network Gateway (PGW) which acts as the on-ramp and off-ramp to the Internet and other IP networks; and
- The Home Subscriber Server (HSS), 3GPP AAA (Interworking), and Policy Controller (PCRF) which together form the central control point and include the main repository for subscriber information. They also provide authorization, authentication and critical accounting functions for services, enable interworking between LTE and non-3GPP networks for a seamless subscriber experience, and apply policies to manage network resources, applications, devices, and subscribers.

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

- In Germany, the equipment types included UE (1), eNodeB (1), MME (3), SGW (3), PGW (3), PCRF (2), HSS (2), 3GPP AAA (1), HSGW (1) & IMS Core (1).
- In China, the equipment types included UE (1), eNodeB (1), MME's (4), SGW (4), PGW (4), PCRF (2), & HSS (2).

In addition, the LTE Interoperability Event 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.
- Demonstrate the support for user roaming between different networks.
- Demonstrate support for access to EPC networks via legacy access technology (e.g. 2G/3G)
- Demonstrate support for access to EPC networks via eHRPD access technology
- Demonstrate the Handover capability between the following access technologies:
 - LTE access - LTE access
 - LTE access - 2G Access
 - LTE access - 3G Access
 - LTE access - eHRPD Access
- Demonstrate the Robustness capability of EPC network nodes

Key Statistics

The LTE Interoperability Event was held from March 15-30, 2010, and involved two major Service Providers; China Mobile in Beijing and Vodafone in Düsseldorf.

Over 40 network components from 8 participating vendors were tested by 50 test engineers using approximately 300 pages of test plans during this 12-day event.

The five physical scenarios incorporated a total of 95 test cases. Taking account of different vendor combinations, the 95 defined tests resulted in a total of 550 scheduled tests being defined. Of the 550 defined tests, a total of 253 were executed of which 234 tests were successfully completed and 19 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

- This test event showed that basic interoperability is achievable between the different nodes from the vendors participating in this event.
- Successful testing of Roaming Interfaces and Protocols (Diameter S6a, GTPv2 S8) was achieved between the labs in Germany and China.
- 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 (especially observed for GTPv2)
- This event was scheduled quite early in the vendor implementation cycle and therefore not all specified features were supported in vendor products (e.g. MME pooling). In particular, the limitations on the UE side (e.g. GERAN/UTRAN and eHRPD) and the interworking with legacy systems are not fully implemented in currently available products.
- The tested UE's (USB dongles) were stable, and provide an appropriate UE for interoperability events.
- Interaction with service layer (e.g. IMS) was successfully demonstrated, with binding of Quality of Service to EPC bearers utilising Policy and Charging Control (PCC)
- End to End IMS Voice calls were achieved over LTE Access,
- eHRPD testing was performed and handover was achieved between LTE and eHRPD,
- The commercial test tools used provided uncompromising visibility to all End2End procedures allowing rapid analysis (JDSU) and the ability to test the robustness of the various networks nodes (Codenomicon).

Introduction

The LTE Interoperability Event 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) Access to EPC via legacy technology (2G/3G) and non 3GPP technology (eHRPD) – including Handover between LTE and legacy access.
- (4) Roaming between EPC capable networks
- (5) Robustness testing of EPC network nodes

Publishing the results of the LTE Interoperability Event 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.

The key relationship between the MSF and relevant standards bodies is illustrated in Figure 1. 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.

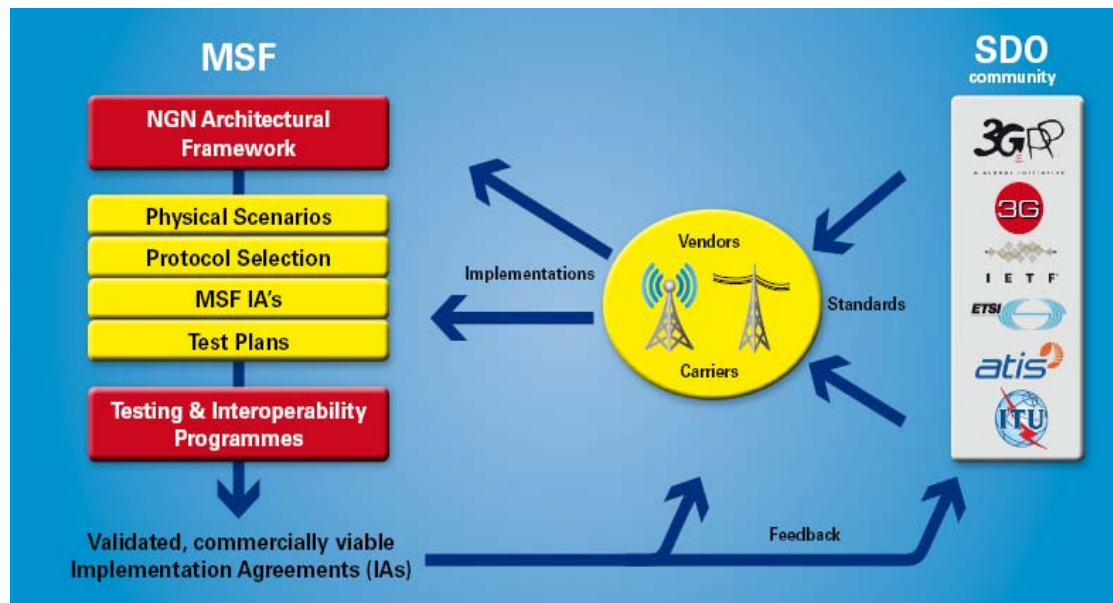


Figure 1. The results from the testing and interoperability programs are fed back to the relevant standards bodies, i.e. there is a virtuous circle.

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

Appendix A provides more details on the five 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 LTE Interoperability Event 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. This testing allowed 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 two-week test event involving two inter-networked lab sites, 8 vendors, over 50 participants, 40 components and 290+ pages of test plans requires careful planning. A dedicated committee of 9 people, along with numerous volunteers, spent over 18 months preparing for the event.

Planning for the LTE Interoperability Event began in January 2009 by identifying scenarios and tests for the event. The scope of the event is defined in the Physical Scenarios document MSF-EPS-LTE-SCN-002-FINAL which is publicly available at <http://www.msforum.org/techinfo/approved.shtml>. A total of 4 scenarios were initially defined covering basic interoperability, roaming, non-LTE access and handover. Each of the 4 main scenarios included a number of sub-scenarios. A fifth 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 focussed on the highest priority tests, and in some cases it was decided to postpone the writing of the test cases. The deferred test cases will be completed before a phase 2 test event is held.

Inter-lab testing was a key objective of the LTE Interoperability Event, but the initial activity focused on testing permutations of vendor-provided EPC technology within each lab. Testing between labs focused on tests where inter lab testing reflected real world deployment scenarios (e.g. roaming). Given the complexity of the event and to help prioritize demand, the LTE Planning Committee developed a test schedule acceptable to all participants. The HP Quality Centre tool was used as a scheduling tool.

In addition to test planning, host site selection, preparation and network interconnectivity needed to be completed before the start of testing. Biweekly LTE Planning Committee meetings were held and a number of vendor participation calls kept the participants informed of the preparation progress and their needed inputs and activities. Preparation activities peaked the week before the LTE Interoperability Event started, as participant engineers arrived at the host sites to ensure that the components were installed so that testing could commence on time.

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. In the LTE Interoperability Event, however, there were no subscribers; instead engineers made extensive use of test tools and emulation to actively monitor product performance and track, identify and fix issues.

Testing was structured to enable both intra-site and inter-site testing, with each host site first carrying out testing against up to five scenarios in isolation before carrying out collaborative networked testing with the other lab.

Vodafone

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 LTE Interoperability Event to prove "real-life" roaming and nomadic scenarios that would not be possible in single lab test events. The Vodafone site was able to demonstrate multi-vendor interoperability of EPC elements, and successfully utilised an IMS service layer to provide dynamic creation of a dedicated bearer via PCC for an end-to-end voice session. In addition, eHRPD access was verified with specific interest from Verizon who were in attendance on-site.

China Mobile

China Mobile provided the host site at the CMCC Research Lab in Beijing, China. The LTE Interoperability Event allowed China Mobile to establish a test network with the other host-site and establish a "real-life" roaming and nomadic environment. The China Mobile site was able to demonstrate multi-vendor interoperability of EPC elements utilising the Policy and Charging Control infrastructure to bind in Quality of Service management,.

Vendor Participants

Eight companies participated in the LTE Interoperability Event:

- The network equipment vendors were Alcatel Lucent, Bridgewater Systems, Cisco/Starent Networks, Huawei Technologies, NEC, and the ZTE Corporation.
- The test equipment vendors were JDSU (network protocol and call-flow analysis – formerly part of Agilent’s Network Solutions Division recently acquired by JDSU) and Codenomicon (network protocol simulator).

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

Vendor	LTE UE	eNodeB	MME	SGW	PGW	PCRF	HSS	3GPP AAA Server	IMS Core	Access Simulator (eHRPD)	H-SGW	Robustness Test Suite	Test Equipment
JDSU													X
Bridgewater Systems						X	X	X					
Starent/Cisco			X	X	X				X	X	X		
Codenomicon												X	
NEC			X	X	X								
ZTE	X	X	X	X	X	X	X						

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

Vendor	LTE UE	eNodeB	MME	SGW	PGW	PCRF	HSS	IMS Core	Access Simulator (eHRPD)	H-SGW	Robustness Test Suite	Test Equipment
JDSU												X
Alcatel-Lucent			X	X	X	X						
Starent/Cisco			X	X	X							
Codenomicon											X	
Huawei	X	X	X	X	X		X					
ZTE			X	X	X	X	X					

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

Part II: The LTE Interoperability Event Execution

The LTE Interoperability Event involved two major Service Providers, one based in China, and the other in Europe. The test scenarios involved the connection of the host labs: connected using 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.

Figure 2 presents a high-level diagram of the test environment used for the Vodafone Düsseldorf host-site.

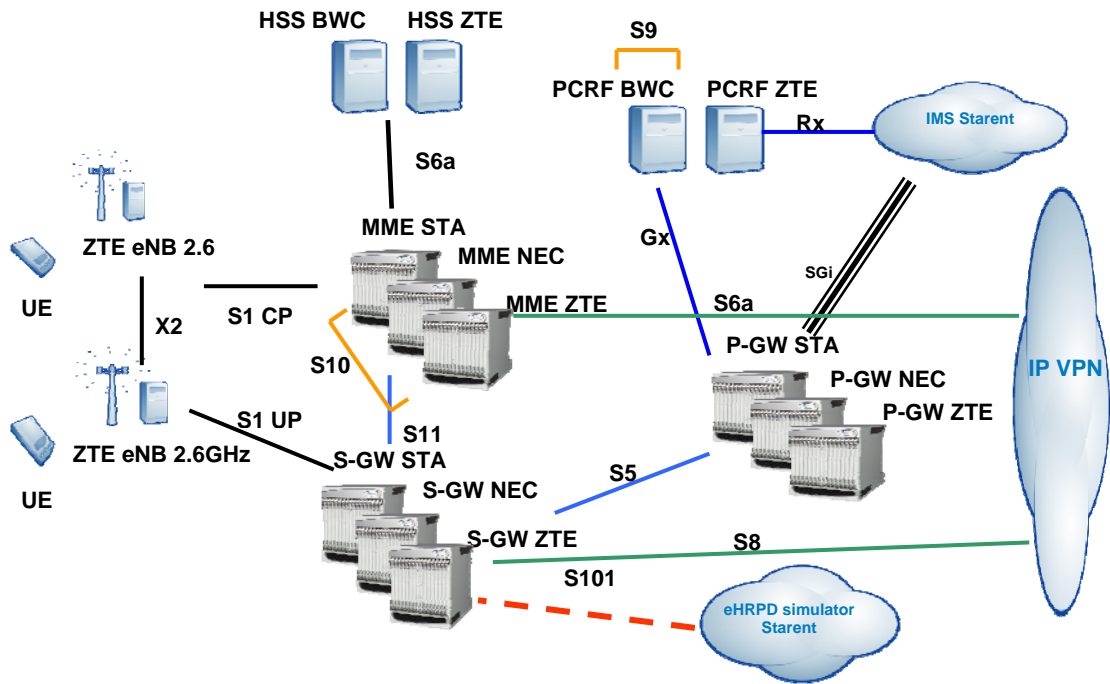


Figure 2 is a high-level view of the Vodafone, Düsseldorf test environment.

Figure 3 presents a high-level diagram of the test environment used for the China Mobile, Beijing host-site.

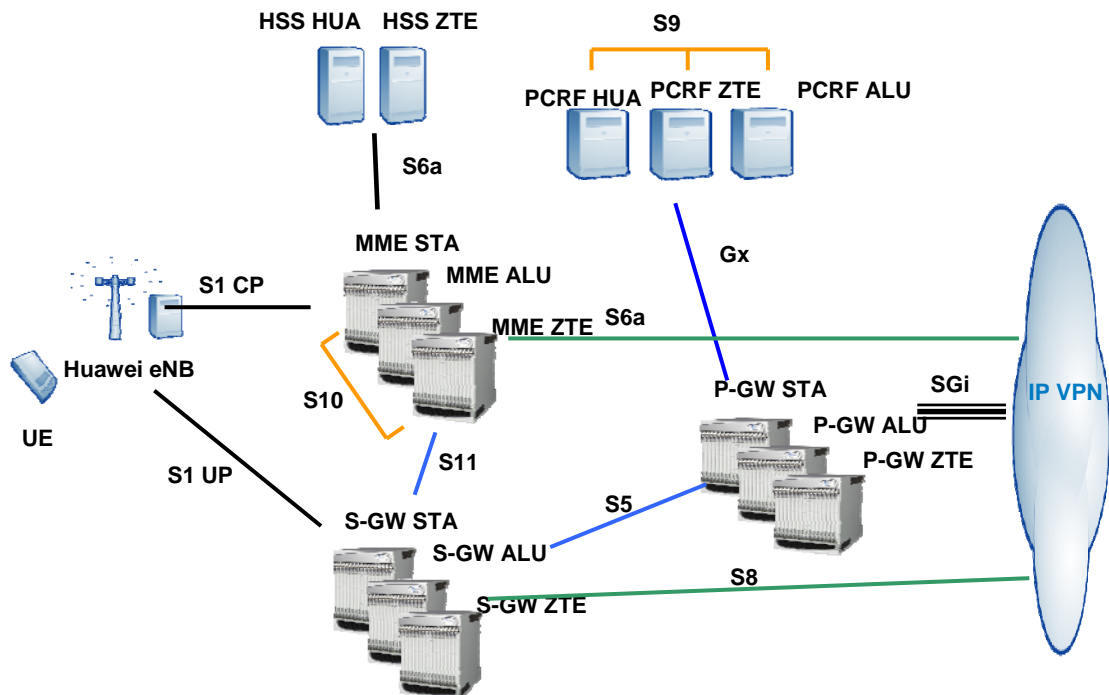


Figure 3 is a high-level view of China Mobile, Beijing test environment.

The LTE Interoperability network used a different technical solution to that of most previous MSF test events. For the initial events, connectivity was provided using dedicated leased lines between each of the sites, with core routers enabling interconnection. This provided a highly reliable infrastructure, but it had two key disadvantages: it was very expensive, and it did not provide the flexibility possible with VPNs. GMI2008 tried a new technique, using VPN tunnels instead of dedicated leased lines. This was highly successful, and the LTE Interoperability Event used the same technique.

The use of a flexible VPN provided important advantages. It 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.

The Five Network Test Scenarios

Figure 4 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 (e.g. eHRPD), 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.

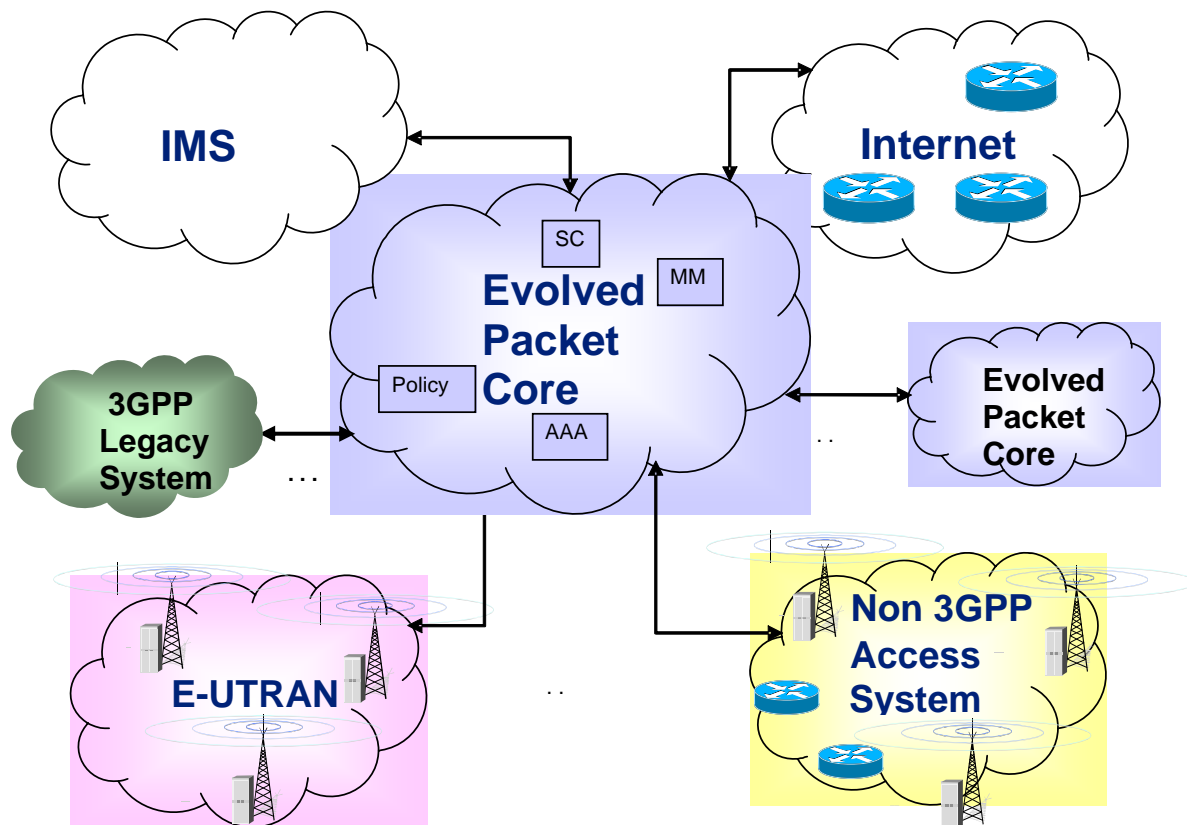


Figure 4 shows how the Evolved Packet Core can be accessed using all mainstream wireline and wireless access technologies, for connection to the application/service layer (e.g. IMS, Internet).

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

- Scenario 1 - Basic Interoperability – focused on three main areas
 - Attachment of an LTE capable UE to the Evolved Packet Core via an eNodeB and creation a default bearer with related Quality of Service applied utilising PCC architecture. Tracking Area Updates, IMS Session establishment utilising a dedicated bearer with related Quality of Service applied utilising PCC architecture were also tested.
 - MME Pooling
 - SGW Selection
- Scenario 2 – Roaming:
 - Roaming with Home Routed Traffic
 - Roaming with Local Breakout in visited network (Home P-CSCF)
 - Roaming with Local Breakout in visited network (Visited P-CSCF)
- Scenario 3 – non-LTE Access to EPC:
 - Legacy wireless access technology (2G/3G) with legacy SGSN
 - Legacy wireless access technology (2G/3G) with S4-SGSN

- Non-3GPP access technology; both trusted (eHRPD) and non-trusted (fixed)
- Scenario 4 - Handover:
 - S1 and X2 based Handover between eNodeB's.
 - Inter-RAT Handover between LTE and legacy wireless technology (2G/3G)
 - Handover between LTE and non-3GPP wireless technology (eHRPD)
- Scenario 5 - Robustness:
 - SGW and PGW testing of receiving malformed GTPv2 packets
 - SGW and PGW testing of receiving malformed PMIP packets

These scenarios are discussed in more detail in Appendix A.

Test scenario validation

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 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 interfaces and is able to validate the outcome of the test case in real-time. After the validation of each individual test scenario the trace file was saved for possible future reference and traceability.

Part III: Results and Issues

During the event it was observed that most of the defined interfaces were mature and interoperable, however the lack of backwards compatibility between different versions of 3GPP Release 8 specifications did cause some issues. Some vendors implemented early versions of the Release 8 specification (based on March 2009), and these early versions were not fully interoperable with equipment based on the latter versions of Release 8 specifications (June 2009).

Sessions were successfully established via LTE access to EPC, with creation of default and dedicated bearers with related Quality of Service applied. An end-to-end IMS Voice over LTE session was also successfully demonstrated, as well as access to the EPC via a simulated eHRPD access and handover between eHRPD and LTE. Roaming was also successfully tested.

Though essential standards are reasonably mature, the implementation of early versions of the standards within network nodes highlights the non-backwards compatibility issue. Service Providers will need to take care to clearly specify which version of the Release 8 specification they are deploying. It is also clear that implementations have focused initially on development of LTE access to EPC and that legacy access (2G/3G) to EPC is somewhat behind. 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 newly agreed baseline of 3GPP Release 8 Dec-2009. In addition, the view is that 3GPP Release 9 will be backwards compatible with this baseline release. The accuracy of this claim may be validated at subsequent Interoperability events.

Scenario 1 – Basic Interoperability:

In this scenario, intra-network testing utilised a single EPC architecture created using components from different vendors. Testing included attachment and detachment from the network, Tracking Area Update, IP-CAN session establishment, SIP registration (to IMS), SIP session establishment, MME pooling and SGW Selection. This was broken down into three sub-scenarios listed below.

Scenario 1a – Basic Interoperability with basic network configuration:

This scenario demonstrated that basic interoperability in a LTE network consisting of equipment from different infrastructure vendors worked properly over the applicable 3GPP standardized interfaces. The demonstrated functionality includes UE registration with the network, data session establishment and termination, as well as UE tracking area update. In addition, the testing also successfully demonstrated the following IMS interworking:

- IMS UA Registration via LTE UE – including interacting with PCC to allow the service layer to be notified of change of default bearer status.
- IMS Session Establishment/Termination between IMS UA's on two LTE UE's – including interacting with PCC to dynamically creating a dedicated bearer with associated Quality of Service

Although basic interoperability was achieved, it was noted that implementations based on different versions of the Rel-8 GTPv2 protocol are not backwards compatible (i.e. March 09 and June 09).

Scenario 1b – Basic Interoperability with MME Pooling

This scenario extended the basic architecture in order to demonstrate MME Pooling and test the interoperability of the pooling function. Although test plans were completed to cover this specific scenario, the MME pooling function was not yet supported by the eNodeB and MME vendors. It is therefore concluded that it is too early to test MME Pooling as the implementations are not yet ready for this feature.

Scenario 1c – SGW Selection

This scenario extended the basic architecture in order to demonstrate SGW Selection and to test the interoperability of the selection function. LTE Attachments were performed with different multi-vendor configurations, thus concluding that basic interoperability of SGW Selection was successfully achieved.

Scenario 2 - Roaming:

This scenario focussed on the different roaming scenarios between Düsseldorf and Beijing. This included the home routed traffic model and the local breakout model with both home and visited operator applications. Testing included attachment and detachment from the network, IP-CAN session establishment, SIP registration (to IMS), and SIP session establishment. This scenario was broken down into the following 3 sub-scenarios.

Scenario 2a – Home Routed Traffic

This scenario was configured as an inter-site test with the subscriber roaming in a 'visited network'. The LTE UE, eNodeB, MME, and SGW were physically in the visited network whilst the PGW, PCRF, HSS were physically located in the Home Network. The testing included the attachment and detachment from the UE in the visited network to the home network. No issues were raised during the tests between Beijing and Düsseldorf in the multi-vendor configuration and therefore interoperability was successfully achieved.

Further testing included the SIP registration (to IMS) and SIP session establishment. As the IMS Core was only present in the Düsseldorf site, and the UE simulator in the Beijing site could not support an IMS User Agent, all related IMS tests were performed within the Düsseldorf lab which was configured as two separate networks. These tests were also successfully executed.

Scenario 2b – Local Breakout (Home Network P-CSCF)

This 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. The IMS Core, including P-CSCF, was configured in the home network.

The focus of these tests was to verify the PCRF interaction across the S9 interface. Test plans were completed to cover this scenario; however as support of the S9

interface within the PCRF nodes was not available the tests could not be executed. It is concluded that it is too early to test the S9 interface as the implementations of PCRF's are not yet ready for this feature.

Scenario 2c – Local Breakout (Visited Network P-CSCF)

This 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.

The focus of these tests was to verify the PCRF interaction across the S9 interface and interaction between the PCRF and P-CSCF in the visited domain over the Rx interface. Test plans were completed to cover this scenario; however as the support of the S9 interface within the PCRF nodes was not available the tests could not be executed. It is concluded that it is too early to test the S9 interface as the implementations of PCRF's are not yet ready for this feature.

Scenario 3 – non-LTE Access to EPC:

This scenario was designed to validate the use of a range of non-LTE access technologies that can be used to connect to the Enhanced Packet Core. The design focussed on the 'legacy' 3GPP access types (e.g. 2G and 3G) that are used to access the Evolved Packet Core. In addition the non-3GPP access technologies, trusted (eHRPD) and non-trusted (fixed) were also designed to access the Evolved Packet Core.

In the early planning stages it was recognized that initial product developments were likely to focus on access via the EPC Mobility Management Entity (MME), with support for other access technologies being deferred till later product releases. As a result, testing priority was given to LTE access. However, the testing scenarios for alternative access technologies were left in the test plan in anticipation of a potential phase 2 interoperability event.

This scenario is broken down into the following 4 sub-scenarios.

Scenario 3a - Non-LTE Access (via S4-SGSN)

The focus of testing for this scenario was to access the EPC over legacy 2G/3G wireless networks via an S4 SGSN.

Based on discussions with vendors, it emerged that S4-SGSNs were not mature enough in their development for testing in time for this interoperability event. The initial focus for product development has been on MME's. These test plans were thus postponed. However, this is seen as an important area, and it is expected that products will be available in time for a possible phase 2 interoperability event.

Scenario 3b - Non-LTE Access (via Release 8 Legacy SGSN)

The focus of testing for this scenario was to access the EPC over legacy 2G/3G wireless networks via Release 8 Legacy SGSN.

Based on discussions with vendors, it emerged that Release 8 Legacy SGSNs were not mature enough in their development for testing in time for this interoperability event. The initial focus for product development has been on MME's. These test

plans were thus postponed. However, this is seen as an important area, and it is expected that products will be available in time for a possible phase 2 interoperability event.

Scenario 3c - Non-LTE Access (via non-3GPP Access)

The focus of testing for this scenario was to access the EPC over non-3GPP access technologies. This scenario included trusted non-3GPP access (e.g. Femto cell) as well as non-trusted non-3GPP access (e.g. WiFi).

The full test plan for this interoperability event included both non-LTE and non-3GPP access technologies. However, it was determined that this sub-scenario was of relatively low priority and thus the test plans were postponed. This sub-scenario could be tested in a future phase 2 interoperability event.

Scenario 3d – Non LTE eHRPD Access.

This scenario focussed on validating IP-CAN Session Establishment and IMS Registration and Session Establishment from an eHRPD access technology using S2a, Gxa, STa and S6b interfaces. This involved the following core network components – HSS, 3GPP AAA, MME, and HSGW. Only one HSS and 3GPP AAA Server provided support for this scenario.

The test cases for IP-CAN Session Establishment were successfully executed, Further testing, including IMS UE Registration and Session Establishment, were not executed due to limitations of the test environment and time constraints. In conclusion the basic interoperability for non-LTE access via eHRPD was successfully demonstrated.

Scenario 4 - Handover:

This 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. Secondly, the handover mechanism between LTE and 'legacy' 3GPP access types (e.g. 2G and 3G) was designed to be tested. Finally, the non-3GPP access technologies (trusted – eHRPD) were also designed to be tested for handover to/from LTE.

In the early planning stages it was recognized that initial product developments were likely to focus on access via the EPC Mobility Management Entity (MME), with support for other access technologies being deferred till later releases. As a result, testing priority was given to LTE access. However, the testing scenarios for alternative access technologies were left in the test plan in anticipation of a potential phase 2 interoperability event.

This scenario is broken down into the following 3 sub-scenarios.

Scenario 4a - Handovers (Intra-LTE, 2G/3G via S4-SGSN)

The focus of testing for this scenario was two-fold:-

1. Demonstrate handover between LTE access (S1-based, X2-based, MME/SGW Relocation).
2. Demonstrate handover between LTE access and legacy 2G/3G wireless access with an S4- SGSN.

X2-based handover tests were successfully executed, although there were some limitations in the configuration of the test environment limiting the execution of some tests due to difficulty in triggering the correct radio conditions.

S1-based Handover and SGW/MME relocation were successfully executed with a level of basic interoperability achieved. However issues were raised with GTPv2 due to backwards incompatibility of implementations based on different 3GPP Release 8 versions (March 2009 – June 2009). These were as follows:-

- S11 interface (MME to SGW) - Indication Flags are not set by the MME
- S10 interface (MME to MME) – Forward Relocation Request message (invalid length of AUTN parameter in MM Context)

Based on discussions with vendors, it emerged that S4- SGSNs were not mature enough in their development for Interoperability Testing in time for this interoperability event. The initial focus for product development has been on MME's. However, this is seen as an important area, and it is expected that products will be available in time for a possible phase 2 interoperability event.

Scenario 4b - Handovers (2G/3G via Release 8 Legacy SGSN)

The focus of testing for this scenario was to demonstrate handover between LTE access and legacy 2G/3G wireless access with Release 8 Legacy SGSN.

Based on discussions with vendors, it emerged that Release 8 Legacy SGSNs were not mature enough in their development for testing in time for this interoperability event. The creation of these test plans was thus postponed. The initial focus for product development has been on MME's. However, this is seen as an important area, and it is expected that products will be available in time for a possible phase 2 interoperability event.

Scenario 4c - Handovers (non-3GPP eHRPD Access)

This scenario focussed on validating the eHRPD to LTE Handover mechanism. This involved the following components – HSS, 3GPP AAA, MME, HSGW. It was noted that only one HSS and 3GPP AAA Server were supported the related interfaces. However, these tests successfully demonstrated the non-optimized handover between LTE and eHRPD using GTPv2. As a result, the interoperability of the STa, S6a, S5, S8 and S11 interfaces was proven.

The remaining test cases, which were related to optimized handover and PMIP, could not be executed due to limitations of the test environment.

Scenario 5 - 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.

Six different sub-scenarios were developed for the LTE IOT event, covering the robustness testing of SGW and PGW:

- S5a – Robustness testing for SGW S11 using GTPv2
- S5b – Robustness testing for SGW S4 using GTPv2
- S5c – Robustness testing for PGW S5 using GTPv2
- S5d – Robustness testing for PGW S8 using GTPv2
- S5e – Robustness testing for PGW S5 using PMIP
- S5f – Robustness testing for PGW S8 using PMIP

Due to time constraints, only test scenario S5a, SGW S11 testing using GTPv2, was executed. SGW's from three different vendors were tested. Two SGW's were tested locally in Düsseldorf and 3rd one over VPN in Beijing site.

During the event, handling of malformed GTPv2-echo and GTPv2-create-session-request messages were tested against the all three SGW's.

Analysis of test run and issues detected

Test scenario 5a was partially passed. For all three SGW's, GTPv2-echo and GTPv2-create-session-request messages were executed, representing ~10% of total robustness test material available for S11 interface. Problems were identified in two SGW's. For both of the SGW's, vulnerabilities were related to processing of GTPv2-create-session-request while GTPv2-echo passed cleanly. This is most likely due to complexity of GTPv2-create-session-request compared to GTPv2-echo. This is typical for protocol level vulnerabilities, i.e. number of issues tends to increase with the increasing complexity. The found issues fall in two categories:

- Crashing of SGW due to vulnerabilities in parsing anomalous content in specific GTPv2 protocol fields. These issues lead to Denial of Service (DoS) situation and can be triggered with a single input message.
- DoS due to resource exhaustion. Problems in this category are caused by cumulative effect of multiple consequent input messages containing anomalous content. The exact nature of resource exhaustion in case of SGW was not fully analyzed, but a typical cause is memory exhaustion.

With the third SGW, half an hour downtime was observed on two occasions. Since this test was run remotely from Düsseldorf to Beijing, the reason could not be verified and may have been caused by network level connectivity problems.

As a general observation, it was noted that two days allocated for robustness testing was not sufficient. To mitigate this, a night run was added.

Scenario 5 Conclusions

LTE IOT event demonstrated that protocol level implementation problems can be identified and fixed with the robustness testing. While the IOT events can't

necessarily facilitate 100% test coverage due to time constraints, an overview of robustness and security issues is achieved. Expanding the testing for multiple interfaces allows vendors and operators to prioritize security related testing and development on interfaces that appear to be most vulnerable.

While robustness assessment is the main value of tests, some auxiliary results are also provided. Protocol message level interoperability is one of these. Robustness tester is not a conformance tester and therefore no conclusive verdicts can be given if a device fails to respond to a message sent by test tool. However, indications about the differences between devices can be observed. One valid interoperability bug, where device sent Echo replies to the wrong port, was identified during the testing. All the interoperability tests are based on valid messages/data sent by test tool.

Response times from the tested devices can also be estimated and compared with the robustness test tool.

Future Work

Interest has been expressed on continuing work in this area by way of a phase 2 MSF LTE Interoperability Event.

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

- Scenario 1b (MME Pooling),
- Scenario 2b (Local Break-out – Home P-CSCF),
- Scenario 3a (Non-LTE Access via S4-SGSN),
- Scenario 3b (Non-LTE Access via legacy SGSN),
- Scenario 3c (Non-LTE Access via non 3GPP access),
- Scenario 4a (2G/3G handover via S4-SGSN),
- Scenario 4b (2G/3G handover via legacy SGSN),
- Scenario 4c (eHRPD handover via S101 interface).

In addition, there are additional potential features that could also be part of a phase 2 LTE event:-

- Further S1/X2 interface testing (including Automatic Neighbour Relation/Self Organising Networks),
- Emergency Call,
- CS Fallback,
- Idle-mode signalling reduction,
- IMS Service Interaction,
- Location Services,
- Fixed broadband access to EPC

The timeframe of a phase 2 LTE 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 Five Test Scenarios

This appendix provides a detailed description of each of the 5 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 LTE 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)
- **Exempted** – Test Case was scheduled to be run, however due to issues with configuration or other limitations (UE and equipment restrictions) it was not possible.

Scenario 1 – Basic Interoperability

Scenario 1 demonstrated the attachment and detachment from the network, Tracking Area Update, IP-CAN session establishment, SIP registration (to IMS), SIP session establishment, MME pooling and SGW Selection.

This scenario was broken down into three sub-scenarios that are detailed below.

Scenario 1a – Basic Attachment

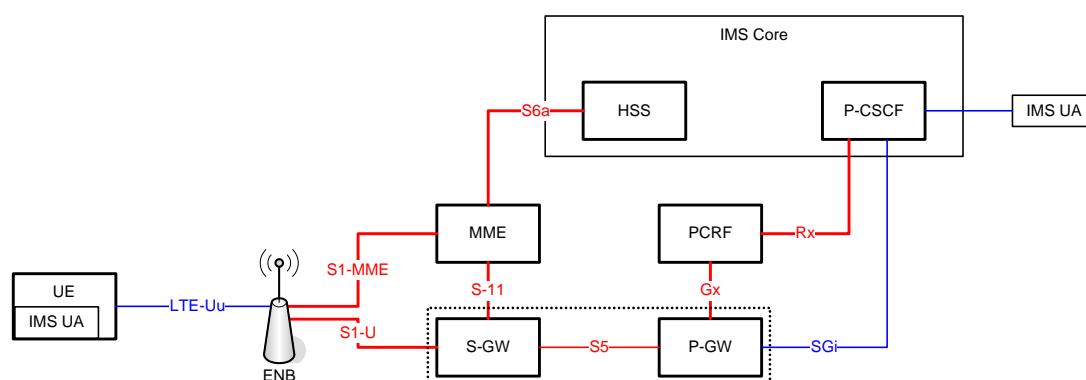


Figure 5 Scenario 1a Test Configuration- Basic Attachment.

The network architecture for scenario 1A is shown in Figure 5 above. The interfaces for which interoperability were tested are shown in red (i.e. S1-MME, S1-U, S5, S11, S6a, Gx and Rx). In some circumstances it was necessary to interoperate multiple of the interfaces together rather than in isolation.

Scenario 1a Objectives

1. Demonstrates the ability to perform interworking between an eNB provided by Vendor A and MME, S-GW and P-GW provided by Vendor B, by performing UE Attach (IP-CAN Session Establishment), Tracking Area Update and UE Detach (IP-CAN Session Tear Down)
2. Demonstrates the ability to perform interworking between an eNB and MME provided by Vendor A and S-GW, P-GW provided by Vendor B, by performing UE Attach (IP-CAN Session Establishment), Tracking Area Update and UE Detach (IP-CAN Session Tear Down)
3. Demonstrates the ability to perform Interworking between a MME provided by vendor A and a HSS provided by vendor B, by performing UE Attach (IP-CAN Session Establishment) and UE Detach (IP-CAN Session Tear Down)
4. Demonstrates the ability to perform Interworking between a S-GW provided by vendor A and a P-GW provided by vendor B, by performing UE Attach (IP-CAN Session Establishment) and UE Detach (IP-CAN Session Tear Down)
5. Demonstrates the ability to perform Interworking between a P-GW provided by vendor A and a PCRF provided by vendor B, by performing UE Attach (IP-CAN Session Establishment) and UE Detach (IP-CAN Session Tear Down)
6. Demonstrates the ability to perform Interworking between an IMS Core provided by vendor A and a PCRF provided by vendor B:
 - a. Via an LTE Attached UE performing an IMS Registration (IMS Session Registration)
 - b. Via an IMS registered LTE UE establishing an IMS Session (IMS Session Establishment - initiated by LTE side)
 - c. Via an IMS registered LTE UE terminating an IMS Session (IMS Session Tear Down - initiated by LTE side).
 - d. Via an IMS registered LTE UE establishing an IMS Session (IMS Session Establishment - initiated by Core side)
 - e. Via an IMS registered LTE UE terminating an IMS Session (IMS Session Tear Down - initiated by Core side)

Scenario 1a Test Results and Observations

The Scenario 1a test plan defined 20 basic test cases. By pairing different vendors' equipments in the various network configurations, the basic test cases were expanded to 113 test case instances scheduled in the Vodafone Düsseldorf lab, and 127 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 test results.

No Run	Passed	N/A	Failed	Exempted	Total	Lab
7	74	21	4	7	113	Düsseldorf
21	95	0	11	0	127	Beijing

Table 3 Scenario 1a 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 duplications of test cases already executed.

The “Failed” test cases were largely due to implementations based on different versions of the Rel-8 GTPv2 protocol which were not backward compatible

The “Exempted” test cases were due to difficulty in maintaining UE in Idle state.

Several issues were encountered during Scenario 1a test execution:

- Implementations based on different versions of the Rel-8 GTPv2 protocol are not backwards compatible (e.g. March 09 and June 09)
- One vendor expected the GTPv2 IEs in the order they are documented within the 3GPP TS 29.274 specification
- Missing link for the right coding of the PLMN-ID in the EUTRAN specification 3GPP TS 36.413 was detected.

Scenario 1a demonstrated that the basic interoperability between eNodeB and MME/S-GW, MME – S-GW, MME – HSS, S-GW – P-GW, P-GW – PCRF and PCRF and P-CSCF is working properly. Some problems were encountered with the different versions of the GTPv2 specifications.

Scenario 1b – MME Pooling

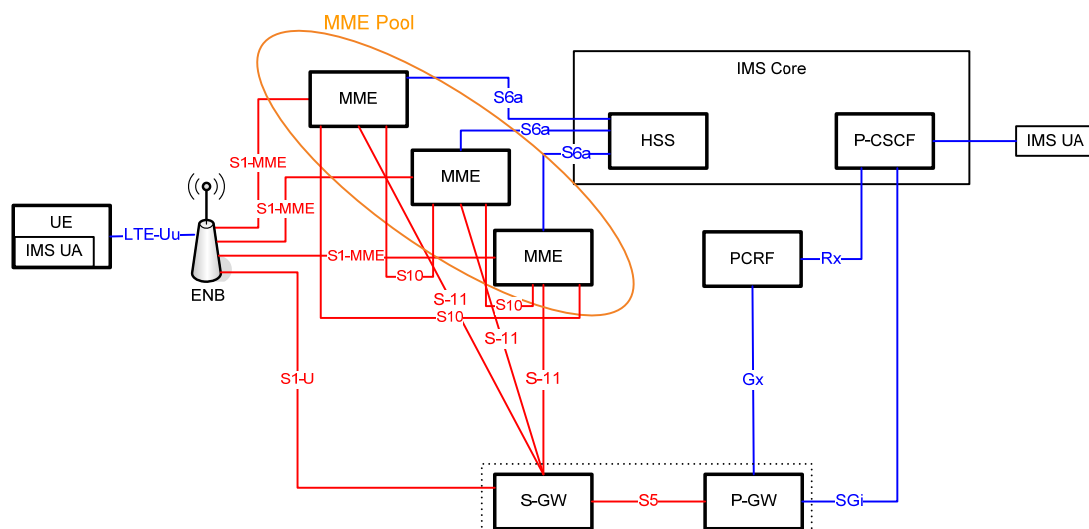


Figure 6 Scenario 1b Test Configuration- MME Pooling.

The network architecture for scenario 1b is shown in Figure 6 above. The interfaces for which interoperability were tested are shown in red (i.e. S1-MME, S1-U, S5, S11 and S10).

Scenario 1b Objectives

1. To demonstrate the ability to perform interworking between eNB, SGW and PGW provided to vendor A and more than one MME provided by vendor B (single vendor MME pool) by performing IP-CAN session establishment, IP-CAN session termination and IMS registration.
2. To demonstrate the ability to perform interworking between eNB, SGW and PGW provided to vendor A and more than one MME provided by multiple other vendors (multi vendor MME pool) by performing IP-CAN session establishment, IP-CAN session termination and IMS registration.

Scenario 1b builds on Scenario 1a, in that that the LTE UE Attach of scenario 1a requires the eNB selects the appropriate MME from the MME pool.

Scenario 1b Testing Results and Observations

The Scenario 1b test plan defined 3 test cases. All test cases are not applicable because the pooling function is not supported by eNB or MME Vendors.

Not Run	Passed	N/A	Failed	Exempted	Total
0	0	3	0	0	3

Table 4 Scenario 1b Test Results

Analysis of the Scenario 1b tests shows:

- Too early to test as implementations did not support this feature

Scenario 1c – SGW Selection

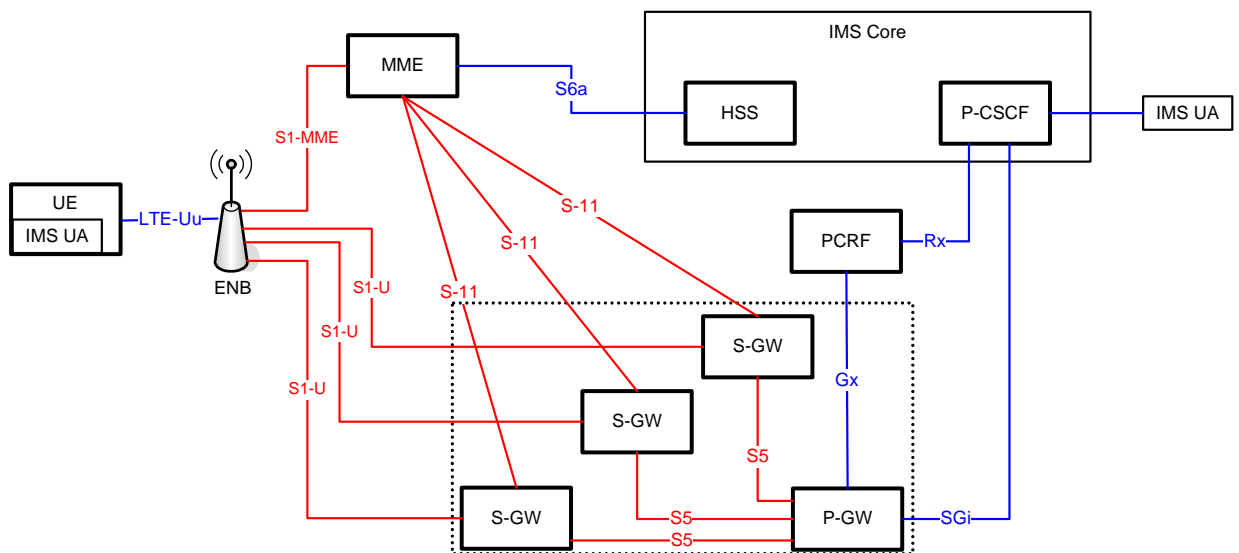


Figure 7 Scenario 1c Test Configuration- SGW Selection.

The network architecture for scenario 1c is shown in Figure 7 above. The interfaces for which interoperability were tested are shown in red (i.e. S1-MME, S1-U, S11 and S5).

Scenario 1c Objectives

1. To demonstrate the ability to perform interworking between eNB, MME and PGW provided to vendor A and more than one SGW provided by vendor B (single vendor SGW pool) by performing IP-CAN session establishment, IP-CAN session termination and IMS registration.
2. To demonstrate the ability to perform interworking between eNB, MME and PGW provided to vendor A and more than one SGW provided by multiple other vendors (multi vendor SGW pool) by performing IP-CAN session establishment, IP-CAN session termination and IMS registration.

Scenario 1c builds on Scenario 1a, in that that the LTE UE Attach of scenario 1a requires the MME selects the appropriate SGW from the SGW pool.

Scenario 1c Testing Results and Observations

The Scenario 1c test plan defined 6 test cases.

The Scenario 1c test plan defined 6 basic test cases. By pairing different vendors' equipments in the various network configurations, the basic test cases were expanded to 24 test case instances scheduled in the Vodafone Düsseldorf lab, and 23 test case instances scheduled in the CMCC Beijing lab.

The following table summarizes the test results.

No Run	Passed	N/A	Failed	Exempted	Total	Lab
4	14	0	0	6	24	Düsseldorf
23	0	0	0	0	23	Beijing

Table 5 Scenario 1c Test Results

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

The "Exempted" test cases were due to the IMS core not being accessible at that time.

Analysis of the Scenario 1c tests shows:

- No issue encountered so interoperability is given.

Scenario 2 – Roaming

Scenario 2 demonstrates the attachment and detachment from the network plus IMS registration for roaming UEs.

This scenario was broken down into three sub-scenarios that are detailed below.

Scenario 2a – Roaming (Home Routed)

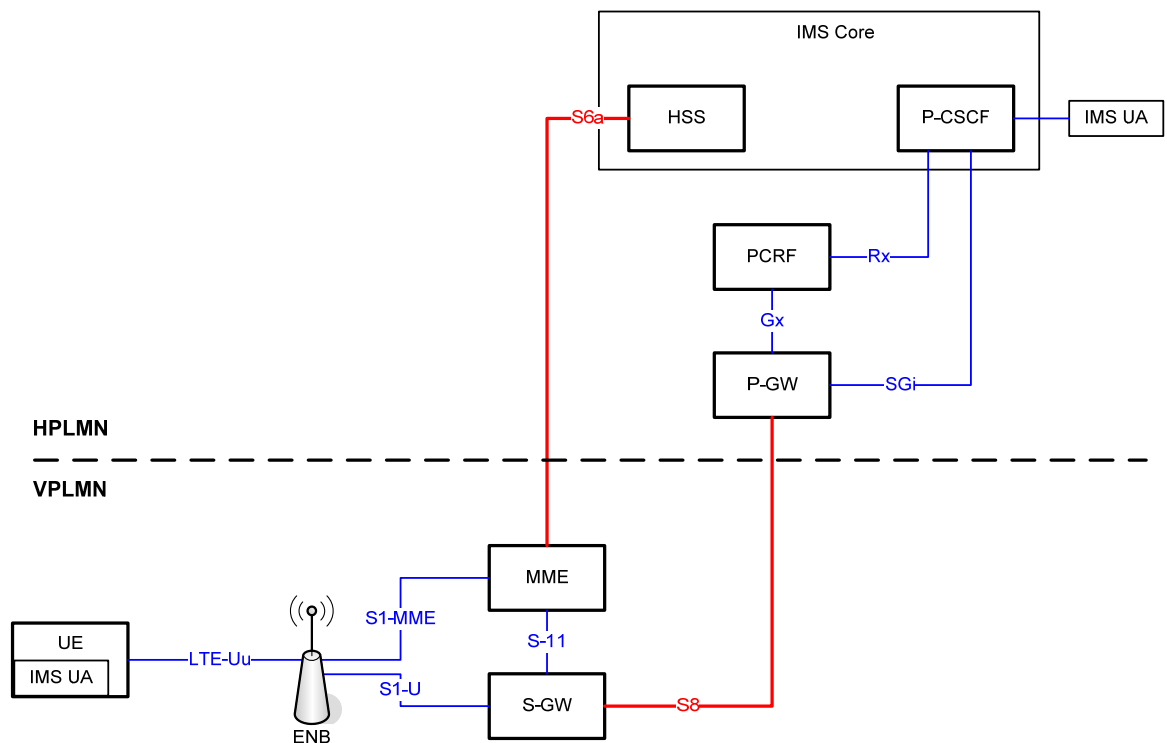


Figure 8 Scenario 2a (Home Routed)

The network architecture for scenario 2a is shown in Figure 8 above. The interfaces for which interoperability were tested are shown in red (i.e. S6a and S8).

Scenario 2a Objectives

1. To demonstrate roaming with the UE, eNB, MME and SGW in the VPLMN and the PGW, PCRF, P-CSCF and IMS core in the HPLMN. Specifically, the ability to perform interworking between MME and SGW in the VPLMN to the HSS and PGW in the HPLMN by performing IP-CAN session establishment, IP-CAN session termination and IMS registration.

Scenario 2a Testing Results and Observations

The Scenario 2a test plan defined 7 basic test cases. By pairing different vendors' equipments in the various network configurations, the basic test cases were expanded to 21 test case instances scheduled in the Vodafone Düsseldorf lab, and 40 test case instances scheduled in the CMCC Beijing lab.

The following table summarizes the test results.

No Run	Passed	N/A	Failed	Exempted	Total	Lab
0	21	0	0	0	21	Düsseldorf
20	8	0	0	12	23	Beijing

Table 6 Scenario 2a Test Results

The “No run” test cases were due to lack of time to execute those test cases.

The “Exempted” test cases were due to there being a configuration problem causing issues between the UE and the IMS core.

Analysis of the Scenario 2a tests shows:

- Notwithstanding the configuration problem, there was no issue encountered so interoperability was proven both within the different EPC cores and between the EPC cores and the IMS core.

Scenario 2b – Local Breakout (Home Network P-CSCF)

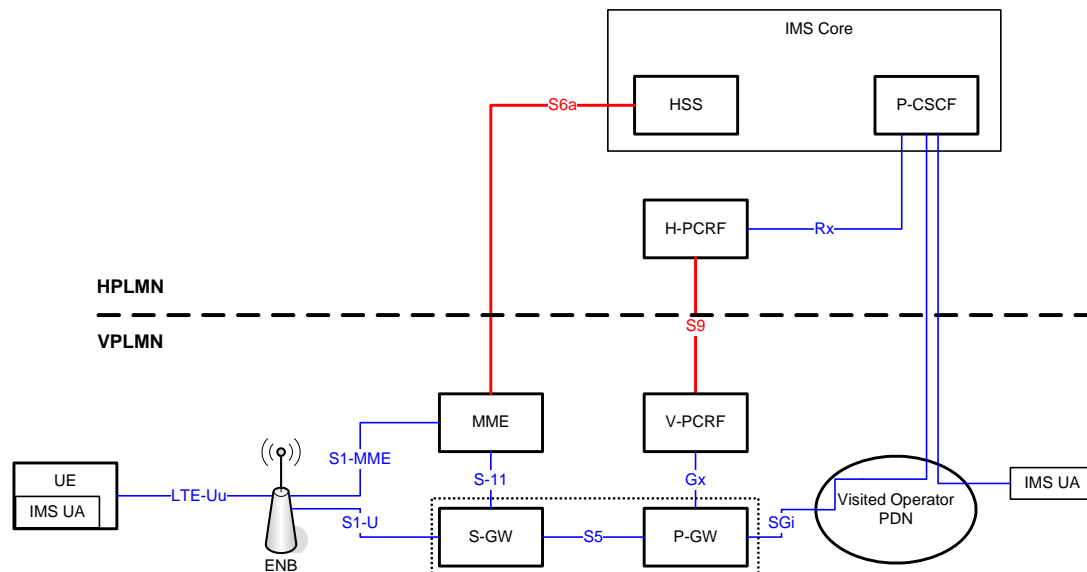


Figure 9 Scenario 2b – Roaming with local breakout

The network architecture for scenario 2b is shown in Figure 9 above. The interfaces for which interoperability were tested are shown in red (i.e. S6a and S9).

Scenario 2b Objectives

1. To demonstrate roaming with the UE, eNB, MME, SGW and PCRF in the VPLMN and the HSS, P-CSCF, PCRF and IMS core in the HPLMN. Specifically, the ability to perform interworking between MME and PCRF in the VPLMN to the HSS and PCRF in the HPLMN by performing IP-CAN session establishment, IP-CAN session termination and IMS registration.

Scenario 2b Testing Results and Observations

The Scenario 2b test plan defined 7 basic test cases. However, no test cases were scheduled due to there being only one IMS system available in the event.

The following table summarizes the test results in Düsseldorf.

Not Run	Passed	N/A	Failed	Exempted	Total
0	0	7	0	0	7

Table 7 Scenario 2b Test Results

Analysis of the Scenario 2b tests shows:

- Apart from the availability of only a single IMS core, the S9 interface was also not widely supported and so it was too early from an implementation point of view to test this scenario.

Scenario 2c – Local Breakout (Visited Network P-CSCF)

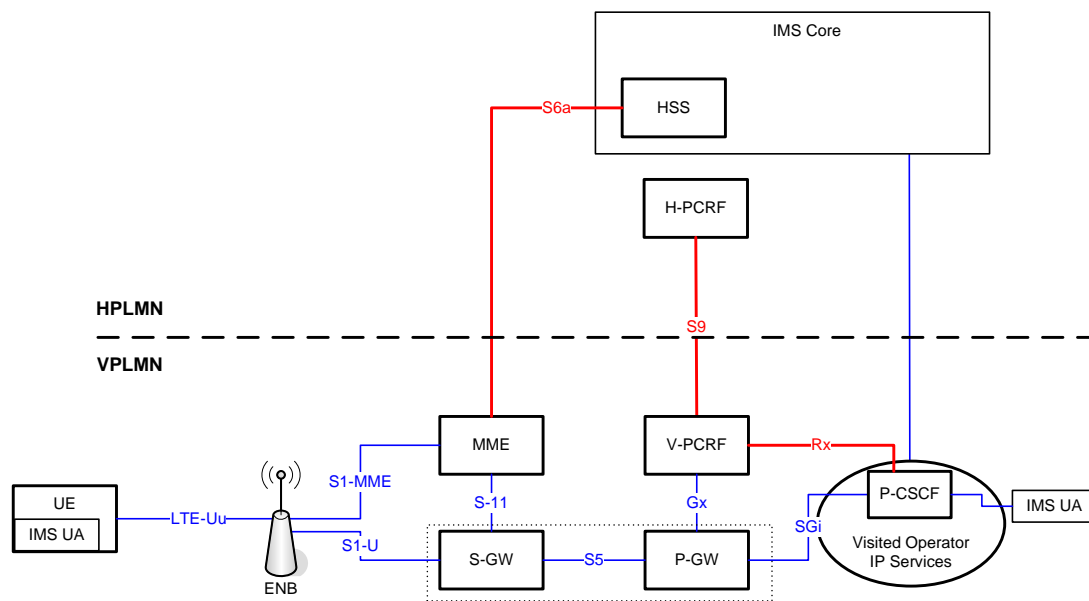


Figure 10 Scenario 2c – Roaming with local breakout (Visited P-CSCF)

The network architecture for scenario 2c is shown in Figure 10 above. The interfaces for which interoperability were tested are shown in red (i.e. S6a, S9 and Rx).

Scenario 2c Objectives

1. To demonstrate roaming with the UE, eNB, MME, SGW, PCRF and P-CSCF in the VPLMN and the HSS, PCRF and IMS core in the HPLMN. Specifically, the ability to perform interworking between MME and PCRF in the VPLMN to the HSS and PCRF in the HPLMN and the PCRF in the visited network to the P-CSCF by performing IP-CAN session establishment, IP-CAN session termination and IMS registration.

Scenario 2c Testing Results and Observations

The Scenario 2c test plan defined 5 basic test cases. By pairing different vendors' equipments in the various network configurations, the basic test cases were

expanded to 14 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	Exempted	Total	Lab
0	0	0	0	14	14	Düsseldorf
0	0	0	0	14	14	Beijing

Table 8 Scenario 2c Test Results

The “Exempted” test cases were due to these tests being of a lower priority to others and there being no IMS available at time periods when the tests could have been run. In addition, the S9 interface was not widely supported.

Analysis of the Scenario 2c tests shows:

- Too early to test as implementations did not support the S9 interface.

Scenario 3 – Non-LTE Access

Scenario 3 demonstrates the attachment and detachment to the EPC from non-LTE accesses.

This scenario was broken down into three sub-scenarios that are detailed below.

Scenario 3a – non-LTE 3G Access with S4-SGSN

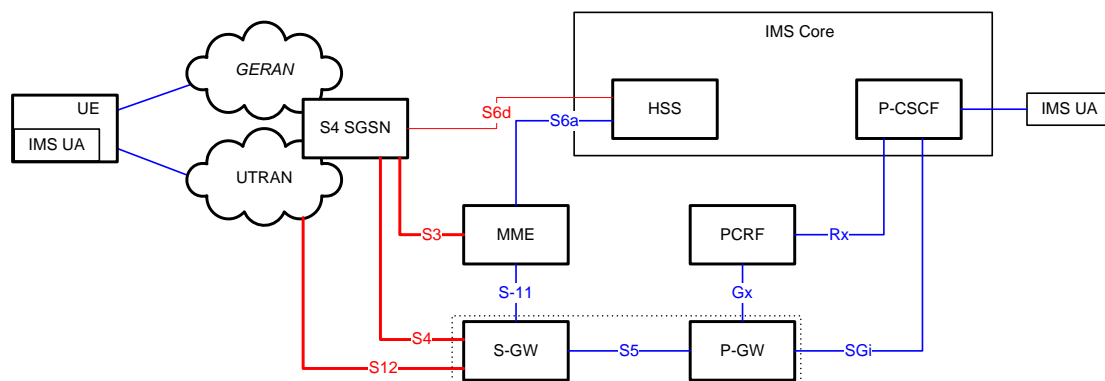


Figure 11 Scenario 3a – Non-LTE 3G Access with S4 SGSN

The network architecture for scenario 3a is shown in Figure 11 above. The interfaces for which interoperability were tested are shown in red (i.e. S6d, S3, S4 and S12).

Scenario 3a Objectives

1. To demonstrate the ability of a 3G UE, to attach to the EPC via a S4-SGSN and perform interworking between the S4-SGSN of one vendor with the EPC and IMS core of another vendor by performing IP-CAN session establishment, IP-CAN session termination, IMS registration and IMS session establishment and release.

Scenario 3a Testing Results and Observations

Due to time pressure in conjunction with there being no S4-SGSNs available in the timeframe, the test cases for this scenario were postponed. The focus has been on the development of MMEs with S4-SGSNs not yet being mature enough for interoperability testing.

Scenario 3b – non-LTE 3G Access with legacy SGSN

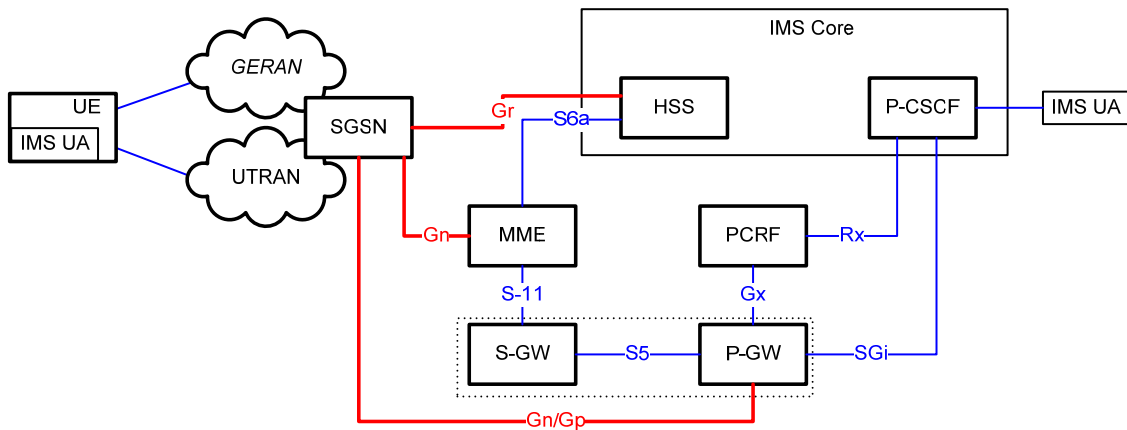


Figure 12 Scenario 3b – Non-LTE 3G Access with legacy SGSN

The network architecture for scenario 3b is shown in Figure 12 above. The interfaces for which interoperability were tested are shown in red (i.e. Gr, Gn and Gp).

Scenario 3b Objectives

1. To demonstrate the ability of a 3G UE, to attach to the EPC via a legacy SGSN and perform interworking between the legacy SGSN of one vendor with the EPC and IMS core of another vendor by performing IP-CAN session establishment, IP-CAN session termination, IMS registration and IMS session establishment and release.

Scenario 3b Testing Results and Observations

Due to time pressure in conjunction with there being no Release 8 legacy SGSNs available in the timeframe, the test cases for this scenario were postponed. The focus has been on the development of MMEs with Release 8 legacy SGSNs not yet being mature enough for interoperability testing.

Scenario 3c – non-LTE non-3G Access

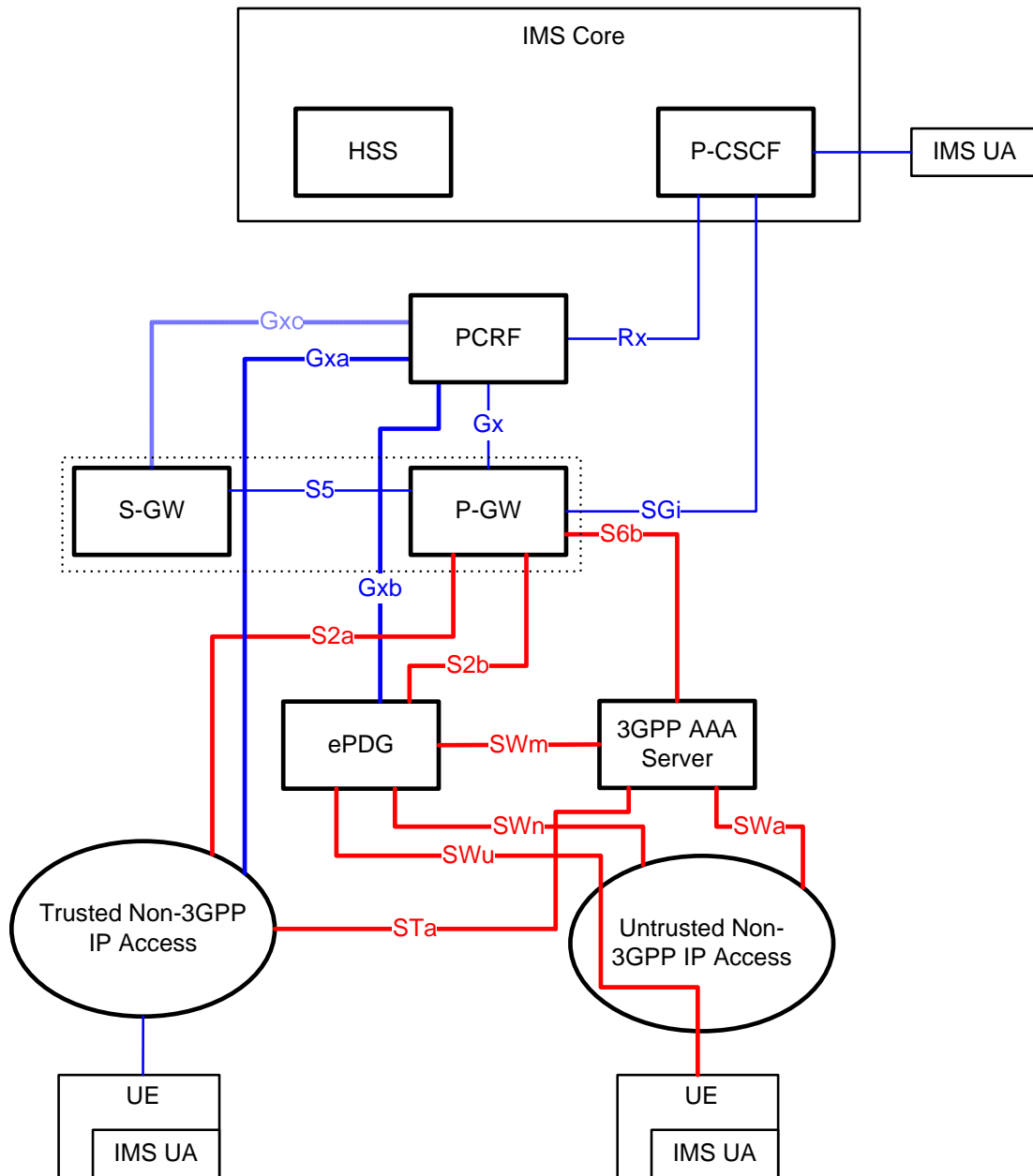


Figure 13 Scenario 3c – Non-LTE non 3G Access

The network architecture for scenario 3c is shown in Figure 13 above. The interfaces for which interoperability were tested are shown in red (i.e. STa, SWu, SWn, SWm, SWa, S2a, S2b and S6b).

Scenario 3c Objectives

1. To demonstrate the ability of a non-3G UE (both trusted and untrusted) to attach to the EPC and perform interworking between the PGW of one vendor with the ePDG and 3GPP AAA of another vendor by performing IP-CAN session establishment, IP-CAN session termination, IMS registration and IMS session establishment and release.

The following table summarizes the test results.

No Run	Passed	N/A	Failed	Exempted	Total	Lab
0	4	0	0	7	11	Düsseldorf

Table 9 Scenario 3d Test Results

Four of the test cases for IP-CAN Session Establishment were executed and passed. The “Exempted” test cases were due to a combination of time constraints together with limitations of the test environment.

Analysis of the Scenario 3d tests shows:

- Basic interoperability for non-LTE access via eHRPD was successfully demonstrated. No issues were found. .

Scenario 4 – Handover

Scenario 4 demonstrates handover, both with registered terminals and with active sessions.

This scenario was broken down into three sub-scenarios that are detailed below.

Scenario 4a – Handovers via S4-SGSN

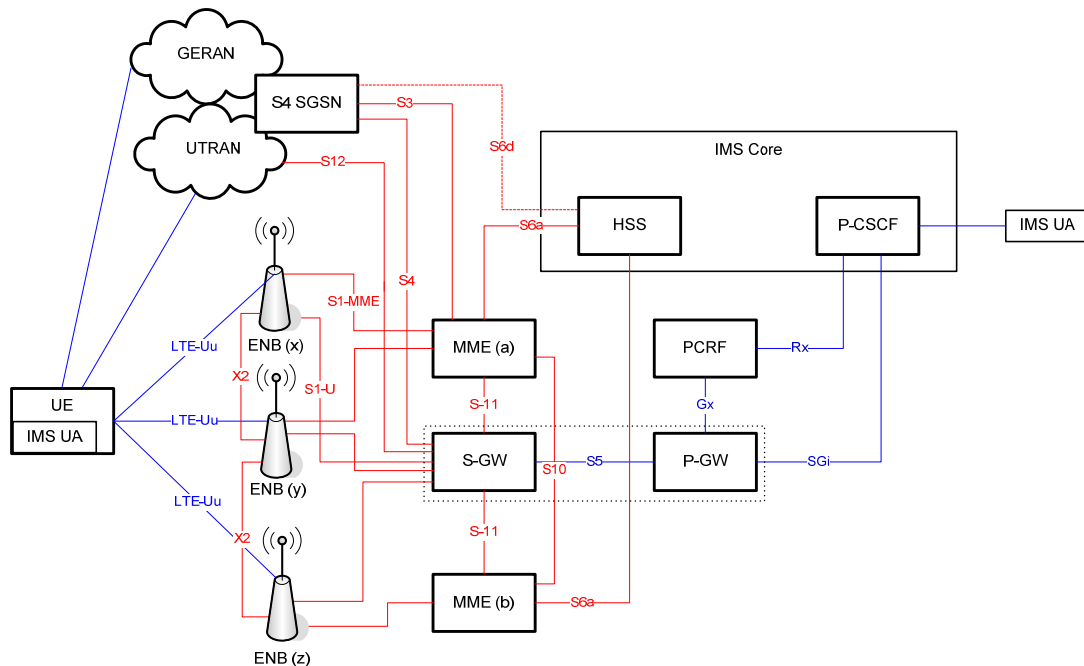


Figure 15 Scenario 4a Test Configuration- Handover via S4-SGSN

The network architecture for scenario 4a is shown in Figure 15 above. The interfaces for which interoperability were tested are shown in red (i.e. S1-MME, S1-U, S10, S11, S12, S6a, S3 and S4).

Scenario 4a Objectives

1. To demonstrate handover of registered UEs, including those involved in active sessions, both intra-LTE and between LTE and UTRAN/GERAN via a S4-SGSN.

Scenario 4a Testing Results and Observations

The Scenario 4a test plan defined 9 basic test cases. By pairing different vendors' equipments in the various network configurations, the basic test cases were expanded to 51 test case instances the Vodafone Düsseldorf lab and 75 test case instances in the CMCC Beijing lab.

The following table summarizes the test results.

No Run	Passed	N/A	Failed	Exempted	Total	Lab
17	12	0	4	18	51	Düsseldorf
0	0	0	0	75	75	Beijing

Table 10 Scenario 4a Test Results

The "Exempted" test cases were due to the lack of a S4-SGSN in either lab, the presence of a single eNB in the Beijing lab and the fact that one vendor did not wish to participate in this scenario.

The "Failed" test cases were due to a number of reasons:

- S11-1 failed between one MME and one S-GW as the S-GW expected the Indication Flags which are not set by the MME. PDN type is missing as GTPv2 March 2009 version requires the presence where the June 2009 version not.
- S1-MME i/f between one eNB and one MME; the handover request message from the MME to the eNB (UE) contained the wrong target S-GW IP address. It was targeting the old S-GW
- X2-4 failed as it was not possible to trigger the right radio conditions for the handover
- S10-1 between the one MME and another MME; first one MME send in invalid length for the AUTN parameter within the MM Context IE in the Forward Relocation Request. After patching the problem the same behaviour but another parameter within the MM Context IE occurred

The "No Run" test cases were due to lack of time.

Analysis of the Scenario 4a tests shows:

- It was too early in the development cycle for S4-SGSNs.
- Some problems encountered with different versions of GTPv2, but interoperability was successfully achieved.

Scenario 4b – Handovers via legacy SGSN

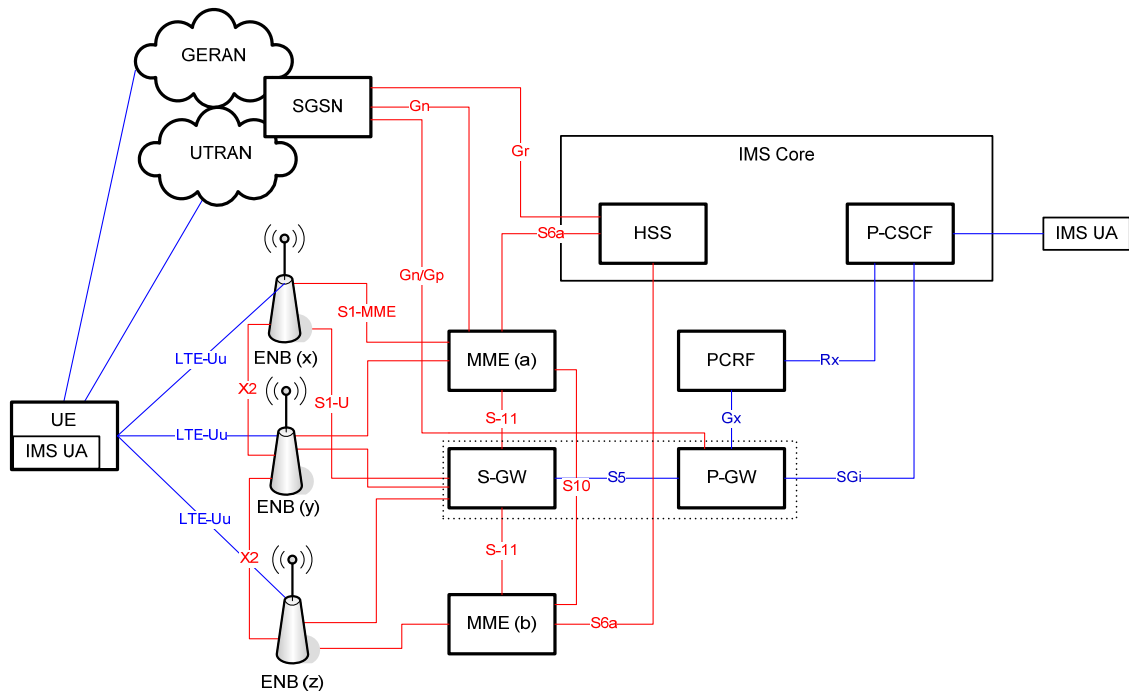


Figure 16 Scenario 4b Test Configuration- Handover via legacy SGSN

The network architecture for scenario 4b is shown in Figure 16 above. The interfaces for which interoperability were tested are shown in red (i.e. S1-MME, S1-U, S10, S11, S6a, Gr, Gn and Gp).

Scenario 4b Objectives

1. To demonstrate handover of registered UEs, including those involved in active sessions, both intra-LTE and between LTE and UTRAN/GERAN via a legacy SGSN.

Scenario 4b Testing Results and Observations

Due to time pressure in conjunction with this scenario being of relatively lower priority in conjunction with Release 8 SGSNs not being deemed sufficiently mature, the test plans for this scenario were postponed.

Scenario 4c – Handover to eHRPD Access

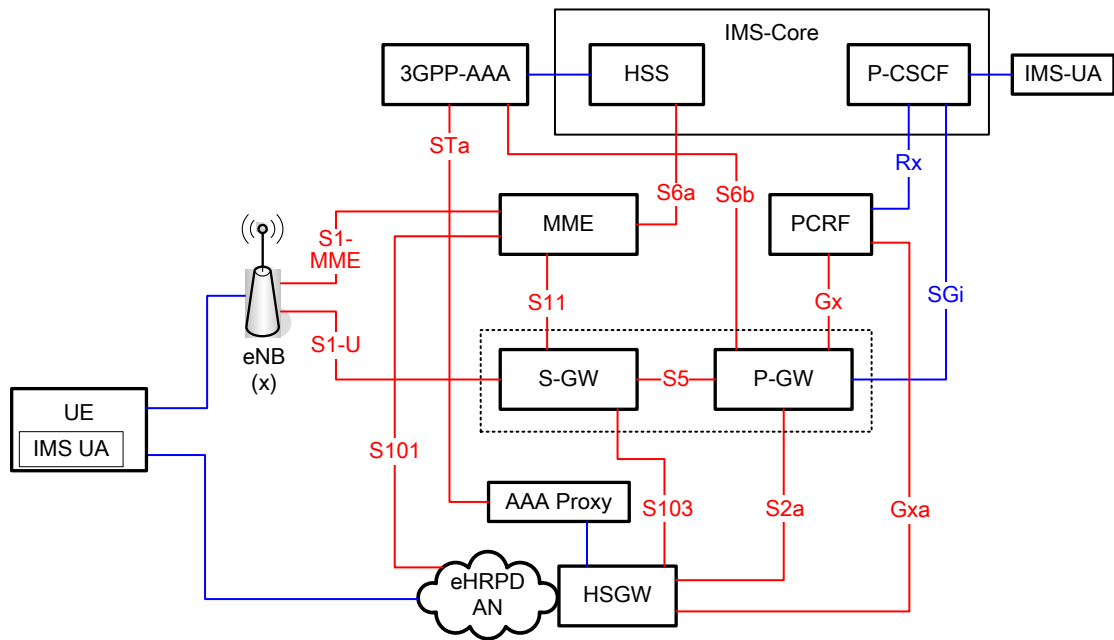


Figure 17 Scenario 4c Test Configuration- Non-LTE Access (eHRPD).

The network architecture for scenario 4c is shown in Figure 17 above. The interfaces for which interoperability were tested are shown in red (i.e. S1-MME, S1-U, S11, S6a, S6b, S2a, STa, S101, S5, S2a, Gx & Gxa).

Scenario 4c Objectives

1. To demonstrate handover of registered UEs, including those involved in active sessions, between LTE and eHRPD.

Scenario 4c Testing Results and Observations

The Scenario 4c test plan defined 21 basic test cases. By pairing different vendors' equipments in the various network configurations, the basic test cases were expanded to 25 test case instances the Vodafone Düsseldorf lab. Scenario 4c was not tested in the Beijing lab.

The following table summarizes the test results.

No Run	Passed	N/A	Failed	Exempted	Total	Lab
0	3	0	0	22	25	Düsseldorf

Table 11 Scenario 4c Test Results

The "Exempted" test cases were largely due to the S101 and PMIP interfaces were not supported by the equipment.

Analysis of the Scenario 4c tests shows:

- Non-optimized hand-over using GTPv2 was successfully demonstrated. As a result, the interoperability of the STa, S6a, S5, S8 and S11 interfaces was proven.

Scenario 5 – Robustness

Scenario 5 demonstrated the usage of robustness testing in 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. For this scenario, the definition of “Passed” means that the test was executed.

This scenario was broken down into six sub-scenarios that are detailed below.

Scenario 5a – Robustness testing for SGW S11 using GTPv2

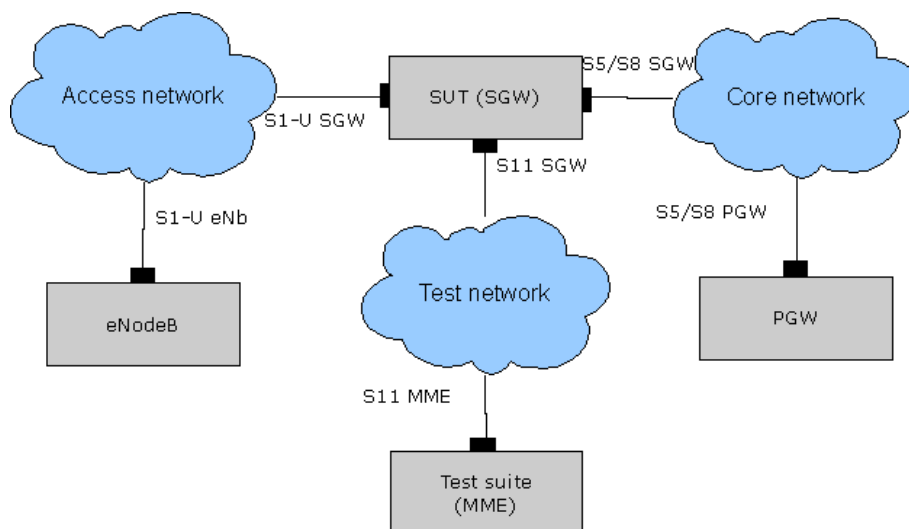


Figure 18 Scenario 5a Test Configuration- Robustness testing for SGW S11 interface.

Scenario 5a Objectives

Objective of scenario 5a was to assess the robustness of SGW S11 interface when processing GTPv2 protocol traffic.

Scenario 5a Testing Results and Observations

The Scenario 5a test plan defined 1 basic test case. By considering different vendors' equipments, the basic test cases were expanded to 2 test case instances in the Vodafone Düsseldorf lab and 1 test case instance in the CMCC Beijing lab.

The following table summarizes the test results.

No Run	Passed	N/A	Failed	Exempted	Total	Lab
0	2	0	0	0	2	Düsseldorf
0	1	0	0	0	1	Beijing

Table 12 Scenario 5a Test Results

Analysis of the Scenario 5a tests shows:

- Test scenario 5a was partially passed. For all three SGW's, GTPv2-echo and GTPv2-create-session-request messages were executed, representing ~10% of total robustness test material available for S11 interface. Problems were identified in two SGW's. For both of the SGW's vulnerabilities were related to processing of GTPv2-create-session-request while GTPv2-echo passed cleanly. This is most likely due to complexity of GTPv2-create-session-request compared to GTPv2-echo. This is quite typical for protocol level vulnerabilities: number of issues increases with the increasing complexity. The found issues fall in two categories:
 - Crashing of SGW due to vulnerabilities in parsing anomalous content in specific GTPv2 protocol fields. These issues lead to DoS situation and can be triggered with single input message.
 - DoS due to resource exhaustion. Problems in this category are caused by cumulative effect of multiple consequent input messages containing anomalous content. The exact nature of resource exhaustion in case of SGW was not fully analyzed, but typical example is memory exhaustion.
- On one SGW half an hour downtime was observed on two occasions. Since this test was run remotely from Düsseldorf to Beijing, reason could not be verified and may have been caused by network level connectivity problems.
- As a general observation, it was noted that the two days allocated for robustness testing was not sufficient. To mitigate this, an overnight run was added.

Scenario 5b – Robustness testing for SGW S4 using GTPv2

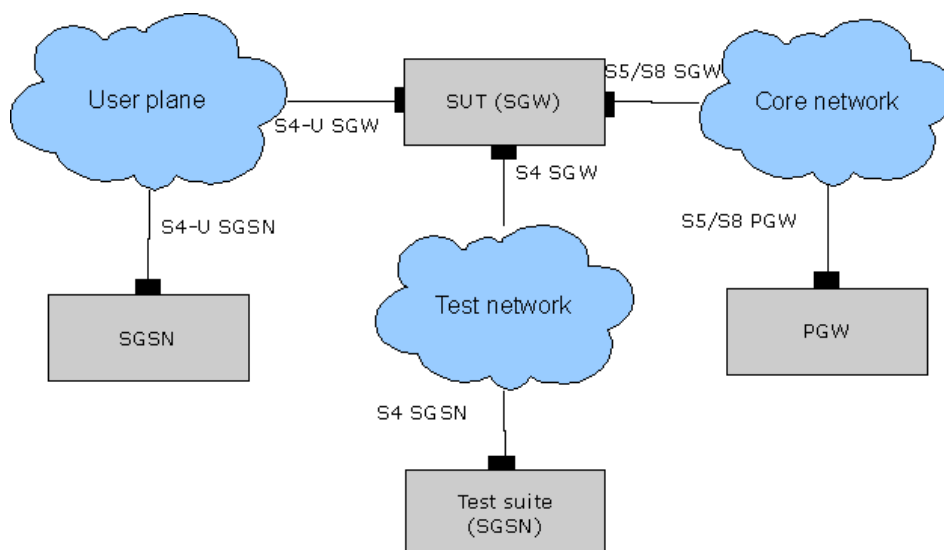


Figure 19 Scenario 5b Test Configuration- Robustness testing for SGW S4 interface.

Scenario 5b Objectives

Objective of scenario 5b was to assess the robustness of SGW S4 interface when processing GTPv2 protocol traffic.

Scenario 5b Testing Results and Observations

The Scenario 5b test was not executed due to time constraints.

Scenario 5c – Robustness testing for PGW S5 using GTPv2

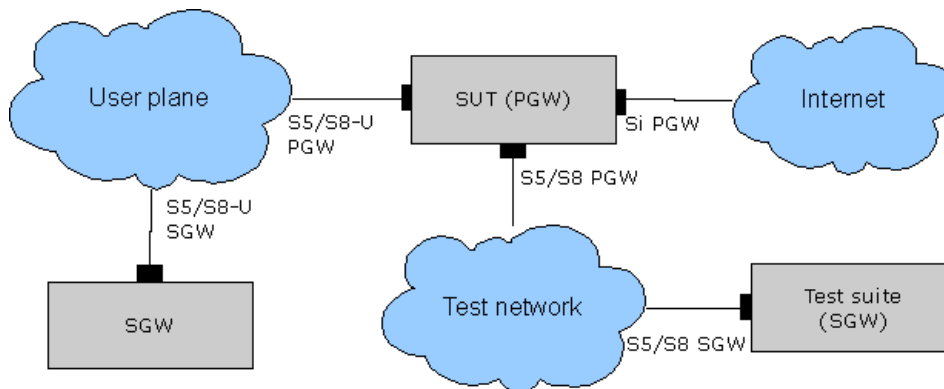


Figure 20 Scenario 5c Test Configuration- Robustness testing for PGW S5 interface.

Scenario 5c Objectives

Objective of scenario 5c was to assess the robustness of PGW S5 interface when processing GTPv2 protocol traffic.

Scenario 5c Testing Results and Observations

The Scenario 5c tests were not executed due to time constraints.

Scenario 5d – Robustness testing for PGW S8 using GTPv2

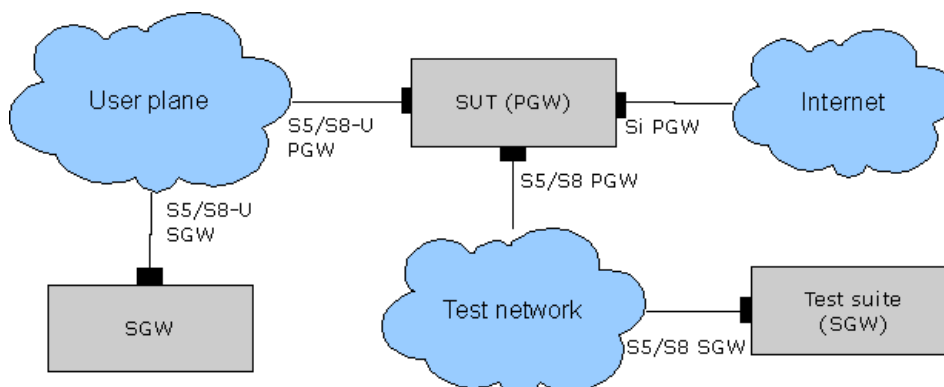


Figure 21 Scenario 5d Test Configuration- Robustness testing for PGW S8 interface.

Scenario 5d Objectives

Objective of scenario 5d was to assess the robustness of PGW S8 interface when processing GTPv2 protocol traffic.

Scenario 5d Testing Results and Observations

The Scenario 5d tests were not executed due to time constraints.

Scenario 5e – Robustness testing for PGW S5 using PMIP

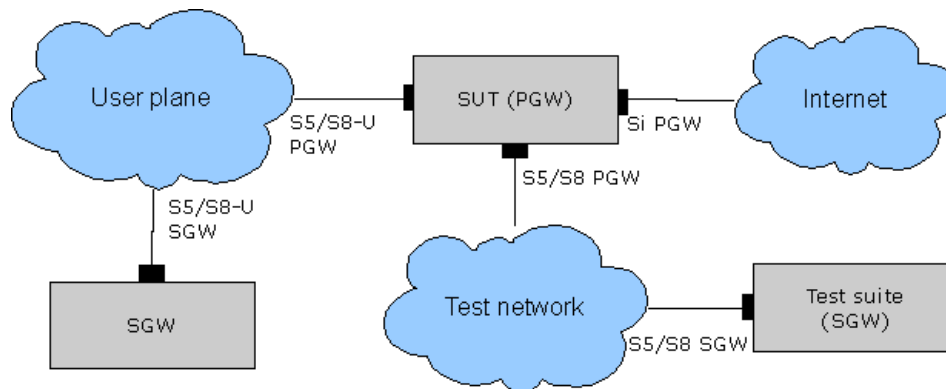


Figure 22 Scenario 5e Test Configuration- Robustness testing for PGW S5 interface.

Scenario 5e Objectives

Objective of scenario 5e was to assess the robustness of PGW S5 interface when processing PMIP protocol traffic.

Scenario 5e Testing Results and Observations

The Scenario 5e tests were not executed due to not having implementations available that supported PMIP.

Scenario 5f – Robustness testing for PGW S8 using PMIP

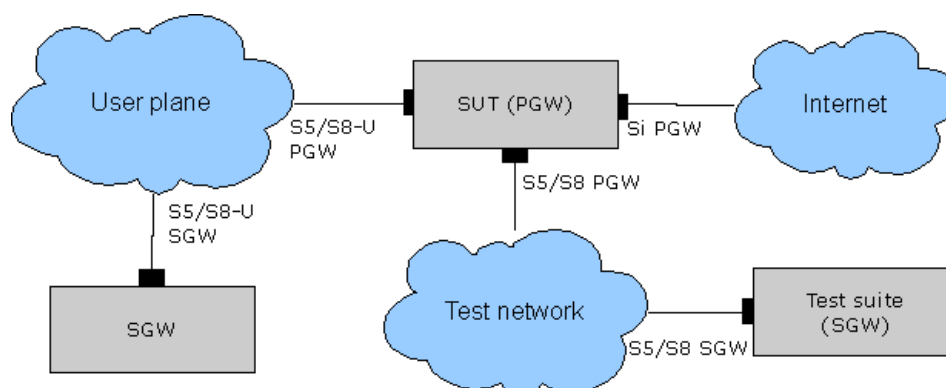


Figure 23 Scenario 5f Test Configuration- Robustness testing for PGW S8 interface.

Scenario 5f Objectives

Objective of scenario 5f was to assess the robustness of PGW S8 interface when processing PMIP protocol traffic.

Scenario 5f Testing Results and Observations

The Scenario 5f tests were not executed due to no PMIP implementations available..

Appendix B: Interfaces Under Test

Interface	specification
S1-MME (S1AP)	3GPP TS 36.413
S1-MME (NAS)	3GPP TS 24.301
S1-User Plane (GTPv1)	3GPP TS 29.281
S2a (PMIPv6)	3GPP TS 29.275
S2b (PMIPv6)	3GPP TS 29.275
X2-AP	3GPP TS 36.423
X2 –User Plane (GTPv1)	3GPP TS 29.281
S3 (GTPv2)	3GPP TS 29.274
S4 Control Plane (GTPv2)	3GPP TS 29.274
S4 User Plane (GTPv1)	3GPP TS 29.281
S5/S8 Control Plane (GTPv2)	3GPP TS 29.274
S5/S8 Control Plane (PMIPv6)	3GPP TS 29.275
S5/S8 User Plane (GTPv1)	3GPP TS 29.281
S6a (Diameter)	3GPP TS 29.272
S6b (Diameter)	3GPP TS 29.273
S6d (Diameter)	3GPP TS 29.272
S101 (GTPv2)	3GPP TS 29.276
S103 (GRE)	3GPP TS 29.276
Gxa (Diameter)	3GPP TS 29.212
S9 (Diameter)	3GPP TS 29.215
Gx (Diameter)	3GPP TS 29.212
Rx (Diameter)	3GPP TS 29.214
S10 (GTPv2)	3GPP TS 29.274
S11 (GTPv2)	3GPP TS 29.274
S12 (GTPv1)	3GPP TS 29.281
Gxc (Diameter)	3GPP TS 29.212
Gr (MAP)	3GPP TS 29.002
Gn (GTP)	3GPP TS 29.060
Gp (GTP)	3GPP TS 29.060
STa / Swa / Swm (Diameter)	3GPP TS 29.273

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. The MSF's activities include developing Implementation Agreements, promoting worldwide compatibility and interoperability of network elements, and encouraging input to appropriate national and international standards bodies.

MSF is a well-established forum with a balanced mix of service providers and vendors that integrates specific work from multiple standards into a holistic network and services architecture. The MSF architecture and solution framework combines legacy and next-generation services in a single unified network. Further, since all MSF participants implement the same baseline features and functions, members can eliminate the guesswork that technology development typically involves.

The advantages of MSF membership include:

- ✚ Access to more than ten years of groundbreaking 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 GMI 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 clarifications in the MSF IAs and standards process
- ✚ Thoroughly evaluated architectural framework for cooperatively designing end-to-end networking solutions

In 2007 the MSF introduced two important, complimentary programs:

- (1) The Next Generation Networks (NGN) Interoperability Test Bed provides the industry with a permanent test bed for testing emerging NGN interfaces
- (2) The MSF Certification Program provides vendor independent certification of critical NGN functionality.

Each program is a key element in a three-pronged strategy designed to facilitate implementation of NGNs and to deliver the Forum's mission statement that "We make Next Generation Networks work". GMI ties everything together by validating

products in the latest standards-based architectural framework using global 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:-

Alcatel-Lucent

Alcatel-Lucent (Euronext Paris and NYSE: ALU) is the trusted transformation partner of service providers, enterprises, strategic industries such as defense, energy, healthcare, transportation, and governments worldwide, providing solutions to deliver voice, data and video communication services to end-users. A leader in fixed, mobile and converged broadband networking, IP and optics technologies, applications and services, Alcatel-Lucent leverages the unrivalled technical and scientific expertise of Bell Labs, one of the largest innovation powerhouses in the communications industry.

The Alcatel-Lucent Ultimate Wireless Packet Core (UWPC) is scalable, service-aware, all-IP, high performance converged core for HSPA/UMTS and for LTE EPC. It is optimized for delivering both voice and multi-media rich wireless broadband. The Alcatel-Lucent UWPC is purpose-built to address the near term packet core renovations and expansion in upgrading the network to support next-generation of W-CDMA/HSPA+ as well as to address the more stringent requirements of LTE.

With operations in more than 130 countries and the most experienced global services organization in the industry, Alcatel-Lucent is a local partner with a global reach. Alcatel-Lucent achieved revenues of Euro 15.2 billion in 2009 and is incorporated in France, with executive offices located in Paris. For more information, visit Alcatel-Lucent on the Internet: <http://www.alcatel-lucent.com>, read the latest posts on the Alcatel-Lucent blog <http://www.alcatel-lucent.com/blog> and follow us on Twitter: http://twitter.com/Alcatel_Lucent.

Bridgewater Systems

Bridgewater Systems, the mobile personalization company, provides a modular portfolio of LTE Evolved Packet Core (EPC) solutions that enable mobile operators to manage mobile data applications, subscribers, and devices in real-time and deliver a dynamic personalized subscriber experience globally and across all wireless access networks. Specifically designed for the performance and capacity demands of mobile broadband networks with support for 3GPP Release 8 standards, Bridgewater's LTE EPC solutions include the Bridgewater Home Subscriber Server and the Bridgewater Policy Controller which supports Policy Charging Rules Function (PCRF), both anchored by Bridgewater's Subscriber Data Broker. Interworking with non-3GPP networks is supported by a 3GPP Authorization, Authentication, and Accounting (AAA) module.

Codenomicon

Codenomicon develops security and quality testing software, which allows users to quickly find and identify both known and previously unknown flaws before business-critical products or services are deployed. Their unique, targeted approach to the fuzz- and robustness testing of networked and mobile applications exposes more flaws and weaknesses than any other robustness testing platform or methodology. Companies rely on Codenomicon's solutions to mitigate threats, like Denial of Service (DoS) situations and Zero Day Attacks, which could increase liability, damage business reputation and cripple sales.

For the LTE/EPC protocol security- and robustness testing Codenomicon offers several protocol solutions, including GTPv2, GTPv1, PMIP, Diameter and all the underlying IP layers.

Codenomicon is a member of the SDL Pro Network. For more information, visit <http://www.codenomicon.com/>

Huawei

Established in 1988, Huawei Technologies is a high-tech enterprise which specializes in research and development (R&D), production and marketing of communications equipment, providing customized network solutions for telecom carriers in optical, fixed, mobile and data communications networks.

JDSU

JDSU (NASDAQ: JDSU; and TSX: JDU) enables broadband and optical innovation in the communications, commercial and consumer markets. JDSU is the leading provider of communications test and measurement solutions and optical products for telecommunications service providers, cable operators, and network equipment manufacturers. JDSU is also a leading provider of innovative optical solutions for medical/environmental instrumentation, semiconductor processing, display, brand authentication, aerospace and defense, and decorative applications.

JDSU recently acquired the Network Solutions Division (NSD) of Agilent Technologies, bringing together two of the strongest test and measurement teams worldwide to become the largest global provider of communications test solutions and a leader in the growing wireless market.

The addition of NSD brings products and services that support analysis, certification, monitoring, troubleshooting of mobile radio-access networks. NSD also has product marketing and development centers in Singapore and Beijing that, combined with existing JDSU offices, dramatically increase the JDSU marketing and development footprint in Asia. NSD products and technologies complement JDSU offerings and contribute to an outstanding end-to-end portfolio of wireless and wireline solutions.

More information is available at www.jdsu.com.

NEC Corporation

NEC Corporation is a leader in the integration of IT and network technologies that benefit businesses and people around the world. By providing a combination of products and solutions that cross utilize the company's experience and global resources, NEC's advanced technologies meet the complex and ever-changing needs of its customers.

NEC is recognized as a leading global LTE/EPC vendor through its selection and participation in LTE trials and commercial launch preparation around the world. NEC focuses on technology innovations and modernizing network by offering a competitive total as well as an End to End product line up. Our solution is based on LTE/EPC, IMS, transport products and other access technologies as well as innovative applications tailored for the operator networks in various regions. NEC aims to leverage its experience and achievement in the success of these activities and to maximize the company's contributions to the early commercialization of LTE.

NEC's vision is to be a leading global company leveraging the power of innovation to realize an information society friendly to humans and the earth.

Starent/Cisco

Starent Networks, now a part of Cisco, is a leading provider of infrastructure solutions that enable mobile operators to deliver multimedia services to their subscribers. The company has solutions that provide mobile operators with the functions and services needed for access, mobility management and call control in their networks. Through integrated

intelligence and high performance capabilities, these solutions also enhance subscriber management, billing and session policy enforcement. The company's products are capable of supporting a wide range of mobile wireless networks, such as CDMA2000, UMTS/HSPA, LTE, WiFi, and WiMAX. The solutions have been deployed in many of the world's most demanding mobile networks.

Cisco Systems is the worldwide leader in networking for the Internet. Cisco's networking solutions connect people, computing devices and computer networks, allowing people to access or transfer information without regard to differences in time, place or type of computer system.

ZTE

ZTE is a leading global provider of telecommunications equipment and network solutions. Founded in 1985, ZTE Corporation has been listed as an A-share company on the Shenzhen Stock Exchange since 1997. In December 2004, ZTE was successfully listed on the Main Board of The Stock Exchange in Hong Kong, becoming the first Chinese company to hold both A shares and H shares. Currently, ZTE is the telecom equipment provider with the most market capitalization and revenue in China's A share market.

ZTE has the widest and most complete product range in the world 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 achieve continued revenue growth and to shape the future of the world's communications. Besides its established cooperation with top Chinese telecoms players including China Mobile, China Telecom and China Unicom in China, the company also has developed long-term partnerships with industry-leading operators including France Telecom, Vodafone, Telstra, Telefonica, among others.

Moving forward, ZTE will continue its ongoing commitment in telecommunications field, aimed to be a world-class excellent enterprise in the near future.