BLACK BOOK
Long Term Evolution –
Evolved Packet Core Network
Your feedback is welcome

Our goal in the preparation of this Black Book was to create high-value, high-quality content. Your feedback is important to help guide our future books.

If you have comments regarding how we could improve the quality of this book, or suggestions for topics to be included in future Black Books, contact us at ProductMgmtBooklets@ixiacom.com.

Your feedback is greatly appreciated!
## Contents

- How to Read this Book ........................................................................................................................................... vii
- Dear Reader ......................................................................................................................................................... viii
- LTE Overview ...................................................................................................................................................... 3
- Nodes Overview ............................................................................................................................................... 13
- Concepts ............................................................................................................................................................... 17
- EPC Testing Challenges ..................................................................................................................................... 23
- EPC Test Cases .................................................................................................................................................. 25
- EPC Test Case: Throughput Test with High Control Plane (Signaling) Traffic ........................................... 27
- EPC Test Case: Constant BHCA ....................................................................................................................... 37
- EPC Test Case: Small Packets and Multiple Bearers ....................................................................................... 47
- EPC Test Case: Handovers ................................................................................................................................. 59
- EPC Test Case: eNodeB Plugin IDLE/Paging Procedure Using Subscriber Model ........................................ 73
- VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE ................................................. 85
- Wi-Fi Offload Test Case: Testing WAG/Wi-Fi Gateway in Isolation ............................................................... 110
- EPC Test Case: Single Radio Voice Call Continuity (SRVCC) with IR94 ...................................................... 122
- EPC Diameter Test Case: S6a Procedures for Attach and AVP Modification .............................................. 143
How to Read this Book

The book is structured as several standalone sections that discuss test methodologies by type. Every section starts by introducing the reader to relevant information from a technology and testing perspective.

Each test case has the following organization structure:

- **Overview**: Provides background information specific to the test case.
- **Objective**: Describes the goal of the test.
- **Setup**: An illustration of the test configuration highlighting the test ports, simulated elements and other details.
- **Step-by-Step Instructions**: Detailed configuration procedures using Ixia test equipment and applications.
- **Test Variables**: A summary of the key test parameters that affect the test’s performance and scale. These can be modified to construct other tests.
- **Results Analysis**: Provides the background useful for test result analysis, explaining the metrics and providing examples of expected results.
- **Troubleshooting and Diagnostics**: Provides guidance on how to troubleshoot common issues.
- **Conclusions**: Summarizes the result of the test.

Typographic Conventions

In this document, the following conventions are used to indicate items that are selected or typed by you:

- **Bold** items are those that you select or click on. It is also used to indicate text found on the current GUI screen.
- **Italicized** items are those that you type into fields.
Dear Reader

Ixia’s Black Books include network, application, and security test methodologies that will help you become familiar with new technologies and the key testing issues associated with them.

The Black Books are primers on technology and testing. They include test methodologies to verify device and system functionality and performance. The methodologies are universally applicable to any test equipment. Step-by-step instructions use Ixia’s test platforms and applications to demonstrate the test methodology.

Our library of Black Books includes twenty-two volumes that cover key technologies and test methodologies:

Volume 1 – Network Security
Volume 2 – Application Delivery
Volume 3 – QoS Validation
Volume 4 – Voice over IP
Volume 5 – Video over IP
Volume 6 – LTE Access
Volume 7 – LTE Evolved Packet Core
Volume 8 – Carrier Ethernet
Volume 9 – IPv6 Transition Technologies
Volume 10 – Converged Data Center
Volume 11 – Converged Network Adapters
Volume 12 – Network Convergence Testing
Volume 13 – Ethernet Synchronization
Volume 14 – Advanced MPLS
Volume 15 – MPLS-TP
Volume 16 – Ultra Low Latency (ULL) Testing
Volume 17 – Network Impairment
Volume 18 – Test Automation
Volume 19 – 802.11ac Wi-Fi Benchmarking
Volume 20 – SDN/OpenFlow
Volume 21 – Audio Video Bridging
Volume 22 – Automotive Ethernet

These Black Books are available in Ixia’s online Resources Library.

We are committed to helping our customers build and maintain networks that perform at the highest level, ensuring end users get the best application experience possible. We hope this Black Book series provides valuable insight into the evolution of our industry, and helps customers deploy applications and network services—in a physical, virtual, or hybrid network configurations.
Long Term Evolution - EPC

Core - Test Methodologies

This document covers the Long Term Evolution (LTE) wireless technology. The document presents a general overview of LTE technology market followed by a focused discussion on Evolved Packet Core (EPC) testing. It also includes multiple test cases based on Ixia’s IxLoad application. LTE Access is detailed in its own black book.
LTE Overview

The Third Generation Partnership Project (3GPP) conducted the Evolved UTRA and UTRAN study, finalized in September 2006, to define the long term evolution (LTE) of the 3GPP wireless access technology. A parallel study known as system architecture evolution (SAE) defined the evolution of the wireless core network.

Important objectives of LTE include:

- Reduced latency
- Higher data rates
- Faster connection times
- Improved system capacity
- Improved system coverage
- Reduced operator cost

To achieve these objectives, 3GPP defines a new radio interface and evolved radio access network architecture. LTE provides users with an always-on IP connectivity service.

SAE defines the evolved packet core (EPC) network architecture for LTE. The EPC simplifies connectivity with 3GPP and 3GPP2 technologies as well as Wi-Fi and fixed line broadband networks.

The LTE access network, which consists of base stations known as evolved Node Bs (eNode Bs), is known as the evolved universal terrestrial radio access network (E-UTRAN). The evolved packet system (EPS) consists of E-UTRAN combined with an EPC.

LTE Requirements and 3GPP Evolution

The 3GPP release 8 specifications define new requirements for LTE technology. Some of these requirements are:

- Scalable bandwidth
  - 1.4, 3.0, 5.0, 10.0, 15.0, and 20 MHz bandwidths in both uplink and downlink directions
- Operation in both paired and unpaired spectrum (FDD and TDD modes)
- Significantly increased peak data rates, scaled according to the size of the bandwidth allocation:
  - Downlink peak data rate of 300 Mbps with a 20 MHz downlink bandwidth when using a 4x4 multiple-input multiple-output (MIMO) antenna configuration
  - Uplink peak data rate of 75 Mbps with a 20 MHz uplink bandwidth when using a single-input single-output (SISO) antenna configuration
LTE Overview

- Uplink peak data rate of 150 Mbps with a 20 MHz uplink bandwidth when using multi-user MIMO

- Improved system performance
  - A two- to four-fold increase in performance in downlink bit rates compared with basic Release 6 system high speed downlink packet access (HSPDA) when using a maximum of two transmit antennas at the eNode B and two receive antennas at the user equipment (UE).
  - A two- to three-fold increase in performance in uplink bit rates compared with basic Release 6 system enhanced dedicated channel (E-DCH) when using a single transmit antenna at the UE and two receive antennas at the eNode B.

- Significantly reduced control plane latency
  - Transition time of less than 100ms from a camped state to an active state (excluding downlink paging delay and non-access stratum (NAS) signaling delay).

- Control plane capacity
  - At least 200 users per cell must be supported in an active state with spectrum allocations of up to 5 MHz and at least 400 users per cell with spectrum allocations greater than 5 MHz.

- Significantly reduced user plane latency
  - User plane latency of less than 5ms in an unloaded condition (a single user with a single data stream) and a small IP packet size (0 byte payload) calculated as the one-way transit time between the access network edge node and the UE at the IP layer in both the uplink and downlink directions.

- Interwork with other wireless technologies
  - GSM and UMTS
  - CDMA2000 1xRTT and high rate packet data (HRPD)

The 3GPP Release 9 specification baseline was set in the December 2009 specification release. Release 9 is now being adopted by eNode B manufacturers.

Key new features available in Release 9 are as follows:

- Multicast, MCH, eMBMS support
- Home eNode Bs, Femtocells and Picocells
- Emergency Bearer Services
- UE Positioning with Positioning Reference Signals
- Transmission Mode 8, a Beam Forming mode extending TM7 under 2x2 MIMO
- DCI Format 2B

Release 9 NAS protocol updates include messages for the following:
• Uplink/Downlink Generic NAS Transport
• Notification
• NF Capability
• LSC (Location Services)

Release 9 RRC protocol updates include messages for the following:
• Proximity
• UE Information
• MBMS
• SIBs 12,13
• UE CMAS

The evolution of 3GPP mobile technology for FDD and TDD modes is shown below.

<table>
<thead>
<tr>
<th>FDD evolution</th>
<th>TDD evolution</th>
<th>3GPP release</th>
<th>Network rollout year</th>
<th>Peak DL data rate</th>
<th>Peak UL data rate</th>
<th>Latency (round trip)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCDMA</td>
<td>TD-SCDMA</td>
<td>Release 99/4</td>
<td>2003/2004</td>
<td>384 kbps</td>
<td>128 kbps</td>
<td>150 ms</td>
</tr>
<tr>
<td>HSPA+</td>
<td>TD-HSUPA</td>
<td>Release 7</td>
<td>2008/2009</td>
<td>28 Mbps</td>
<td>11 Mbps</td>
<td>50 ms</td>
</tr>
<tr>
<td>LTE and HSPA+</td>
<td>TD-LTE and TD-HSPA+</td>
<td>Release 8</td>
<td>2010</td>
<td>LTE: 150 Mbps (2x2 MIMO and 20 MHz bandwidth) HSPA+: 42 Mbps</td>
<td>LTE: 75 Mbps; HSPA+: 11 Mbps</td>
<td>LTE: 10 ms</td>
</tr>
<tr>
<td>LTE Advanced</td>
<td>Study item initiated</td>
<td></td>
<td></td>
<td>High mobility: 100 Mbps Low mobility: 1Gbps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The LTE Market

Informa predicts a dramatic increase in the use of advanced mobile applications, such as mobile browsing and video, and predicts that mobile video traffic will grow by a factor of 30 by 2012. In fact, mobile video traffic could overtake voice traffic by 2011. Since the design, rollout, and operation of mobile networks has always been driven by voice, the future dominance of data traffic will have a significant impact on the design of future mobile networks.

In voice dominated networks, in the past revenue has closely been correlated with traffic, but in data dominated networks this relationship is not true because the value to application users is no longer proportional to data volume.

To remain profitable in data dominated networks, the per-bit cost must be reduced for operators, as shown in Figure 1. One way to do this is to optimize the network by moving from a voice traffic oriented architecture to a data traffic oriented architecture such as LTE.

Figure 1. Divergence between Traffic Volume and Revenue over Time (Source: Nokia Siemens Networks)

LTE promises to deliver the massive capacity required for the shift in mobile traffic patterns from voice to data and video at a lower cost compared to previous 3GPP technologies. Analysys Mason, in a study presented to the UMTS Forum in 2008, estimated that dual band 10 MHz (2x10 MHz) deployment of 10,000 eNode Bs would provide a significant increase in downlink capacity over a comparable 3GPP HSPA deployment, as shown in Figure 2. According to the Analysys Mason study, the cost per megabit could drop by a factor of three in going from HSPA (2x5 MHz) to LTE (2x5 MHz).
LTE offers a number of upgrade paths for operators of 3GPP and non-3GPP networks, as shown in Figure 3. LTE is the next step on the roadmap of 3GPP cellular systems that includes GSM, GPRS, EDGE, UMTS (WCDMA) and HSPA. LTE also fulfills the goal of harmonious coexistence with legacy circuit switched systems through the EPC, as shown in Figure 3.

Infonetics explains that the LTE infrastructure market is expected to grow at a compound annual growth rate of 56% to $5 billion by 2013, driven by E-UTRAN deployment during this period (see Figure 4). The market for E-UTRAN is expected to reach $4.7 billion by 2013, while the market for EPC is expected to reach $350 million by the same time.
In addition, according to Infonetics, the number of LTE subscribers could exceed 72 million by 2013, largely split between the Asia Pacific and North American regions. NTT Docomo, KDDI, Verizon Wireless, and AT&T are expected to deploy the technology during this time frame. Europe is expected to lag behind because it is deploying HSDA+ in the interim between HSDA and LTE, as shown in Figure 5.

Technical deployments of LTE are expected in the last half of 2009 and commercial offerings are expected between 2010 and 2012.
The Global Mobile Suppliers Association (GSA) conducted a study of LTE commitments worldwide. The study was released on August 26, 2009. The study shows growing support and commitment to LTE as the next broadband technology. Verizon Wireless and NTT Docomo are scheduled to introduce commercial LTE service in the U.S. and Japan, respectively, in 2009-2010 and 2010. In 2010, an additional eleven carriers are expected to launch LTE services in Canada, Japan, Norway, South Korea, Sweden and the U.S. According to the GSA study, it is anticipated that by the end of 2012 at least 31 carriers located in 14 countries will have launched LTE services.

**EPS Architecture**

Compared to the UMTS and GSM architectures that preceded it, LTE reduces the number of network elements and eliminates the circuit-switched domain. The LTE architecture defines the evolved packet system (EPS) as a combination of the IP-based core network and LTE access system. The EPS consists of the E-UTRAN and the EPC, as illustrated in Figure 6. The EPC is the LTE core network and the E-UTRAN is the LTE access network. The E-UTRAN consists of E-UTRAN Node B (eNode B) network elements.

The EPC contains the following components:

- **Mobility management entity (MME)**—terminates control plane signaling between the EPC and the UE as well as between the EPC and the E-UTRAN. The MME also contains bearer management functions and inter-core network mobility to other access networks such as UTRAN (UMTS) and GERAN (GSM) or to other MME.

- **Serving gateway (S-GW)**—a gateway that terminates the EPC user plane interface towards the E-UTRAN. For each UE associated with the EPS, there is a single S-GW.

- **Packet data network (PDN) gateway (PDN-GW)**—a gateway that terminates the user plane interface towards a PDN. There is a PDN-GW for each PDN accessed by the UE. The eNode B is a much more complex network element than its counterparts, the Node B in UMTS and the BTS in GSM, as it operates without a central controller (RNC or BSC).
functions of the central controller is performed by the eNode B itself in LTE, elevating the critical role of the base station in the LTE architecture.

An eNode B interconnects with other eNode Bs over the X2 interface and to the EPC over the S1 interface. The S1 interface is composed of the S1-MME control plane interface to the MME and the S1-U user plane interface to the S-GW. The Uu interface defines the radio interface between the eNode B and the user equipment (UE).

In the EPC the S5 (non-roaming) or S8 (roaming) reference point lies between S-GW and PDN-GW. The S11 interface reference point is defined between MME and S-GW.

QoS Control in the EPS

The units of QoS control in the EPS are the EPS bearer between the PDN-GW (sometimes denoted as P-GW) and the UE, and the E-UTRAN radio access bearer (E-RAB) between the S-GW and the UE. Each packet flow mapped to the same EPS bearer receives identical bearer-level packet forwarding treatment and is assigned the same QoS class. Provisioning of different packet forwarding treatments to different packet flows requires the establishment of separate bearers.

Each QoS class and UE IP address combination requires a separate bearer, and each UE IP address is associated with a single access point name (APN). The APN is a reference used to identify a PDN to which the UE may connect. The APN itself is a name that may be used in a DSN query to resolve the IP address of the appropriate PDN-GW. One bearer, known as the default bearer, remains established throughout the lifetime of the PDN connection. Additional EPS bearers, known as dedicated bearers, may be established to the same APN, but with different QoS classes, and are also associated with the same UE IP address. A single UE may connect to multiple APNs and hence may be assigned multiple UE IP addresses.

The indicator of QoS class throughout the EPS is the QoS Class Indicator (QCI). The QCI is a scalar that is associated to each individual bearer assigned to a UE. It establishes, for each network node, the QoS parameters and forwarding handling of the packets within each data flow. The delay budget, packet error loss rate and priority are all characteristics of a flow derived from the QCI associated bearer carrying the data flow. The 3GPP has defined the specific set of supported QCIs, and this QoS classes to be used in the EPS. These QCI values are shown in the following table.
The EPS supports the following types of bearer:

- **guaranteed bit rate (GBR)**
- **non-guaranteed bit rate (non-GBR)**

A GBR bearer is permanently assigned network resources at the time of its establishment or modification by the admission control functions resident in the EPS, for example the eNode B. If the traffic carried over a GBR bearer conforms to the QoS assigned to it, congestion related packet losses are expected to be rare. Congestion related packet loss on a non-GBR bearer, however, would not be unexpected.

<table>
<thead>
<tr>
<th>QCI</th>
<th>Resource Type</th>
<th>Priority</th>
<th>Packet Delay Budget</th>
<th>Packet Error Loss Rate</th>
<th>Example Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>2</td>
<td>100 ms</td>
<td>10-2</td>
<td>Conversational Voice</td>
</tr>
<tr>
<td>2</td>
<td>GBR</td>
<td>4</td>
<td>150 ms</td>
<td>10-3</td>
<td>Conversational Video (Live Streaming)</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>3</td>
<td>50 ms</td>
<td>10-3</td>
<td>Real Time Gaming</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>5</td>
<td>300 ms</td>
<td>10-6</td>
<td>Non- Conversational Video (Buffered Streaming)</td>
</tr>
<tr>
<td>5</td>
<td>Non-GBR</td>
<td>1</td>
<td>100 ms</td>
<td>10-6</td>
<td>IMS Signaling</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>6</td>
<td>300 ms</td>
<td>10-6</td>
<td>Video (Buffered Streaming) TCP-based (For example, www, e-mail, chat, ftp, p2p file sharing, progressive video, and so on.)</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>7</td>
<td>100 ms</td>
<td>10-3</td>
<td>Voice, Video (Live Streaming)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Interactive Gaming</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>8</td>
<td>300 ms</td>
<td>10-6</td>
<td>Video (Buffered Streaming) TCP-based (For example, www, e-mail, chat, ftp, p2p file sharing, progressive video, and so on.)</td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Nodes Overview

**eNodeB**

eNode B functions are summarized below:

- Radio resource management, including the following:
  - Radio bearer control
  - Radio admission control
  - Connection mobility control
  - Scheduling of uplink and downlink radio resources
- Data stream compression and encryption
- MME selection from an MME pool when the UE registers with the EPS
- Routing of user plane data to the assigned S-GW
- Scheduling and transmission of paging messages over the radio interface
- Scheduling and transmission of broadcast information over the radio interface
- Scheduling and transmission of earthquake and tsunami information (ETWS) over the radio interface
- Configuration of measurement reporting by the UE for mobility and scheduling
- Measurement of uplink radio signals

**MME**

The MME is a control entity that acts as the entry point into the EPC from the eNodeB. Only control plane interfaces and protocols are handled by the MME. It is responsible for:

- NAS signaling and security
- Signaling for iRAT handovers between LTE and 3G (via S3 the interface)
- Reaching the UE when the UE is in IDLE state
- Tracking area list management
- SGW and PGW selection
- Authentication and authorization
- Bearer management, including dedicated bearer establishment
- Lawful intercept
SGW

The Serving Gateway (SGW) is the termination of the user plane interface between the eNodeB and the EPC, as well as a control plane entity towards the MME. It handles both control plane and user plane functions. At any point in time, there is only one SGW serving one specific UE. The SGW is responsible for:

- User plane packet routing and forwarding
- Mobility anchor for inter-eNodeB handovers, as well as iRAT handovers between 3GPP networks
- Accounting for inter-operator charging

The SGW is sometimes incorporated with the PGW into one unit.

PGW

The Packet Data Network (PDN) Gateway (PDN-GW, or PGW) is the gateway between the EPC and the packet data network (PDN). All packets from the PDN destined towards UEs are routed by the PGW, and all packets from the UE are routed to the PDN by the PGW.

The PGW is responsible for:

- User plane packet routing and forwarding
- UE IP address allocation
- Per UE based packet filtering (DPI)
- Accounting for charging, including UL and DL service level charging
- UL and DL service level gating control and rate enforcement

PCRF

The policy and charging rules function (PCRF) is responsible for all policy in the EPS. For all UEs, it is responsible for dynamically installing policy rules in the PGW that determine the QoS and charging that is applied to all services for the UEs. These rules govern the parameters like maximum allowed bandwidth per bearer and per APN for the UE, as well as guide the charging of the services. The PGW is actually responsible for the policing of the rules, but the rules themselves are provided by the PCRF. Examples of policy rules are the allowed bandwidth over a bearer, the allocation of a dedicated bearer for a specific service to provide better QoS. The PCRF connects to the PGW using the Gx interface, and the Diameter protocol.

HSS

The HSS maintains the subscriber database. It is a stateful database, in the sense that when a UE is attached to the network and active, the HSS knows its state and location. It is also responsible for the authentication of the UEs. The HSS connects to the MME using the S6a interface, and uses the Diameter protocol.
OCS and OFCS

LTE charging is handled by the OCS and OFCS functions. The OFCS is responsible for offline charging, which is typically used for post-paid subscribers. The OCS is responsible for the online charging, which is used for pre-paid subscribers.

For offline charging, the SGW and PGW provide charging information to the OFCS based on the charging rules provided by the PCRF. These charging records can be based on volume of data, time using the service, and even other parameters like time of day and location. The OFCS then collects this charging information and creates charging records for each subscriber, which is forwarded to the billing service.

For online charging, operation is a little different. The PGW requests the OCS for credits as the subscriber performs actions. The OCS is aware of the subscriber’s credit. At a certain time, if the credit runs out, then the OCS responds negatively, and the service is then interrupted. Therefore, the OCS has a more real time focus to it than the OFCS.

Both the OCS and OFCS communicate with the EPC using the Diameter protocol.

SGSN

The SGSN provides 3G connectivity into the EPC. It provides control plane and user plane functionality, and therefore also implements packet routing and forwarding. The SGSN existed in the 3G UMTS system, and used to forward packets to/from the GGSN. Now, in LTE, it communicates to the SGW via the S4 interface.
Session creation and deletion

When a UE attaches to the LTE network (that is, it registers for service), a session is created. This session has an end to end meaning, in the sense that bearers are created over the air interface and throughout the EPS network. For EPC, it means that a default bearer (at a minimum) is created and maintained. This default bearer translates into a GTP-U tunnel. The main goal of a session is to provide IP connectivity to the UE, so during this procedure, an IP address is allocated to the UE.

For each APN connection that a UE establishes, a new session is created, and therefore a new default bearer. For each independent session, a distinct IP address is allocated to the UE.

When a UE detaches from an APN connection, or powers off, the sessions are deleted, and no IP connectivity is present.

TAU

A tracking area update (TAU) is a signaling (control plane) procedure that informs the network of the location of the UE. It can be triggered by a number of events, but is typically done when the UE moves from one tracking area to another one.

Idle and connected states

Typically, a UE is in connected state. It means that all bearers belonging to the UE are up and active, from end to end. However, if the UE has no activity for a certain duration of time, the network may put the UE in idle state. In idle state, the UE’s bearers are taken down over the air interface, as well as the bearers on the S1-U interface. However, even when in idle state, the S5/S8 bearers for the UEs remain active. Also, the UE keeps the allocated IP address during idle state.

Paging

When a UE is in connected state, any downlink (DL) packet destined to the UE is simply forwarded to it. However, if the UE is in idle state, the UE has no immediate IP connectivity because of the absent bearers on the air interface and the S1-U interface. In this case, a downlink packet destined for an idle state UE is buffered by the SGW, while the SGW invokes the paging procedure. The paging procedure has the goal of locating and informing the UE, and instructing it to transition to connected state, and re-establish all bearers. Once the UE is in connected state, the downlink packets buffered by the SGW can be forwarded to the UE.

Default and Dedicated bearers

A default bearer is created for each session. Each attached UE has at least one default bearer, but has one default bearer for each APN connection. A default bearer has a QoS setting which
is best effort. A UE can also have one or more dedicated bearers. Dedicated bearers are separate bearers that are characterized by a higher QoS. A specific QCI value (see table 2 above) is associated to the dedicated bearer, as well as values for average bandwidth and maximum bandwidth. Some dedicated bearers can also have a guaranteed bit rate. The goal is to deliver a better quality of experience for a specific service to a UE. The policy rules from the PCRF determine the allocation of a dedicated bearer to a UE, and are therefore under full control of the network operator. Examples of a service that would use a dedicated bearer is a video service offered by the operator and VoLTE. Dedicated bearers allow the operator to differentiate the service using QoS.

**Dual stack**

Connections to a PDN are normally IPv4 or IPv6. However, some PDNs support both IPv4 and IPv6. These PDNs are considered dual IP. When a UE connects to a dual IP PDN, it can obtain an IPv4 address and an IPv6 address, both of which can be used simultaneously. A UE that supports this ability is called a dual stack UE, which is also referred to as IPv4v6.

**Multi-APN**

Multi-APN refers to the capability of a UE to connect to multiple PDNs simultaneously. Each PDN is identified by the APN. Typically, subscribers are allocated a connection to the internet access APN, but VoLTE is implemented using a separate PDN (and therefore APN). A UE that can connect to both networks simultaneously supports multi-APN.

**Handovers**

A handover is the procedure where a UE’s air interface connection to the LTE network is transferred from one cell to another. The most common trigger for a handover is the fact that a UE moves in such a way as to degrade the radio connection being used. The UE scans other cells with a better radio connection, and then the network hands it over to the new cell.

**S1 Interface Protocol Stacks**

The S1 user plane interface (S1-U) is defined between the eNode B and the S-GW and provides non-guaranteed delivery of user plane PDUs between the two network elements. The user plane protocol stack is shown in Figure 7 and consists of the GPRS tunneling protocol user (GTP-U), UDP and IP protocols.
The S1 control plane interface (S1-MME) is defined between the eNode B and the MME. The S1 application protocol (S1-AP) is transported over the SCTP protocol, which runs over the IP protocol and provides reliable transport.

The S1-MME protocol stack is shown in Figure 8. The S1-AP protocol transports NAS messages between the UE and the EPC over the S1-MME interface.

**S11 interface**

**E-UTRAN Mobility**

Handover is a procedure handled by E-UTRAN that maintains a call while a user transitions from one cell to another. Handovers generally occur when the UE is near the edge of coverage and a failed handover often results in a dropped call. LTE only supports a very fast break-before-make hard handover procedure. In a break-before-make handover, the UE only has connectivity to a single cell at a time. The soft and softer make-before-break handover procedures used in UMTS systems are eliminated in LTE to simplify the procedures and reduce the need for extra radio and backhaul resources. LTE introduces the X2 interface that provides connectivity between source and target base stations during an intra-E-UTRAN handover. Introduction of the X2 interface reduces load on the EPC and makes the handover procedure faster, reducing the likelihood of failure.
Handover procedures are defined for UEs in the ECM-CONNECTED state. Several types of handover procedures are defined by LTE:

- Intra-eNode B handover between sectors of the same eNode B.
- Inter-eNode B handover between eNode Bs:
  - With MME relocation.
  - Without MME relocation, but with S-GW relocation.
  - With neither MME relocation nor S-GW relocation.
- E-UTRAN to UTRAN inter-radio access technology (inter-RAT) handover.
- UTRAN to E-UTRAN inter-RAT handover.
- E-UTRAN to GSM EDGE radio access network (GERAN) A/Gb mode inter-RAT handover.
- GERAN A/Gb mode to E-UTRAN inter-RAT handover.
- E-UTRAN to high rate packet data (HRPD) inter-RAT handover.
- E-UTRAN to cdma2000 1xRTT inter-RAT handover.

The inter-eNode B handover without MME and S-GW relocation is shown in Figure 9. The case illustrated assumes that IP connectivity is present between the S-GW and both source and target eNode Bs and also requires the presence of the X2 reference point between the eNode Bs. Part of the handover command information comes from the target eNode B and is passed to the UE by the source eNode B, which passes all information necessary to complete the handover to the UE. The UE then accesses the target eNode B using a contention-free RACH procedure, if a dedicated RACH preamble is available. During the execution of the handover procedure, user plane packets are forwarded from the source eNode B to the target eNode B. When the UE has connected to the target eNode B, downlink data that has been forwarded to the target eNode B is delivered to the UE.
Concepts

Figure 9. Inter eNode B Handover without MME Rel
EPC Testing Challenges

There are multiple dimensions that are important to test in the EPC. The EPC was designed to handle very large amounts of subscribers moving massive amounts of data. The most important aspects of EPC testing are listed below.

Subscribers

UMTS and HSPA technologies, in conjunction with the development of popular devices that take advantage of the possibilities of wireless data, have led to a rapidly increasing adoption of smartphones and wireless data usage. The worldwide amount of subscribers is growing at a much faster pace than new voice subscribers are. This growth will increase further with the impending deployment of LTE. The trend leads to a core network that must now handle vast amounts of subscribers simultaneously connected to the network. Current testing requirements range from 1 million to 7 million, for one single PDN-GW node. Loading subscribers is one of the most important testing aspects for the core network.

eNodeBs and MMEs

In addition to being able to handle vast amounts of subscribers, the EPC must also support a large amount of radio access network elements to allow for a large scale deployment economically. For LTE especially, NEMs have placed a high importance on being able to support very high counts of MMEs and eNode Bs connected and managed by the same EPC.

Data Throughput

The trend of increasing data adoption not only leads to higher amounts of subscribers, but it also leads to those subscribers using the data services much more than in the past. Furthermore, the applications enabled by ever increasing data rates coupled with fixed pricing models for data usage have encouraged subscribers to use their data plans much more freely. Video over a 3G connection is now commonplace. Current requirements for EPC testing range from 40 Gbps to over 120 Gbps.

Control Plane Load

In addition to the data plane load that the EPC is required to handle, it must also be able to accept all the control plane procedures that allow the data plane to be established, mobility events, QoS changes, and so on. The control plane load rate is critical dimension in all EPC test cases.

Small Packet Sizes

The average packet size in the EPC is approximately 600 octets, because of the nature of the required traffic models in a mobile environment. While testing for throughput objectives using larger packet sizes has value, it is necessary to be able to handle
smaller packet sizes, striving to achieve the same throughput values. This means that very high packet/second rate handling by the EPC nodes is expected, and must be tested. Sizes as low as 128 octets have been requested.

**Realistic Traffic Models**

The subscriber usage patterns witnessed in the field vary depending on the sophistication of the user, the applications used and the devices. For example, browsing the internet on a mobile device results in very different core network activity compared to watching a video. Web browsers typically download a page of about 250KB in size, pause a minute to read it, and then download another page. A video user generates a relatively constant stream of data to be handled quite differently. An EPC system test plan is not complete without a realistic usage, time and application model of the traffic. Configuring this into a test therefore becomes a critical ability and challenge for the test tool.

**Deep Packet Inspection (DPI)**

There are two levels of DPI that are tested in the EPC.

The first level is part of the 3GPP specifications for traffic handling: when dedicated bearers are used in the EPC, multiple traffic flows coming from and destined to the UE must be mapped onto the appropriate GTP-U bearers that are assigned to the UE. For example, suppose that a UE has two service data flows (SDFs): http and video on demand. Additionally, network policy has allowed this UE to establish a dedicated bearer for the video traffic. In the downlink direction (from network to UE), the PDN-GW must differentiate between both traffic types to map the http traffic to the default bearer, and map the video traffic to the dedicated bearer. This activity is done using DPI technology to recognize the traffic and map it correctly.

The second DPI application is the ability to manage the network traffic and perform policing on traffic types. This, and other related features are offered by the NEMs to the service providers as differentiated features of the EPC equipment. These features are very important, because traffic management is vital in a wireless environment, given the limited spectrum available. The DPI functionality developed by EPC manufacturers is quite sophisticated, and imposes very large requirements on the test equipment, mainly dealing with the ability to simulate vast amounts of different stateful applications, to large amounts of TCP connections.

**Combined Objectives**

The last category of test case, and the most challenging to support, consists of test cases that combine the objectives listed above into one massive test case. For example, the EPC must not only handle 60 Gbps of throughput, or 1 million subscribers, or 5000 GTP-C transactions/second. It must also support all of these dimensions at the same time: the throughput, the subscribers, and the control plane activity, at the same time. These types of tests take on an infinite number of personalities, because the combinations are endless.
EPC Test Cases

The EPC test cases are run using IxLoad. IxLoad surrounds the system under test, which consists of the SGW and PDN-GW, as shown in Figure 10. Optionally, a PCRF (Policy and Charging Rules Function) may be part of the system under test.

IxLoad simulates the MME using the GTP-C protocol on the S11 interface, and the eNodeB using the GTP-U protocol on the S1-U interface. The layer 7 traffic generated by IxLoad uses the S1-U interface, where the traffic is encapsulated in GTP-U bearers. On the right side of the network under test, using the SGi interface, IxLoad also simulates the network servers and peers. This interface does not use special wireless protocols, but rather uses straight UDP and TCP/IP.
EPC Test Case: Throughput Test with High Control Plane (Signalling) Traffic

Overview

The test case performs a dual objective: simulating high throughput while also having high control plane activity. GTP-c transactions represent the control plane activity for the S1-U/S11 interfaces. More precisely, the GTP-c acts on the S11 interface, between the MME and the SGW.

The control plane activity is simulated by having some of the subscribers constantly establishing sessions, performing a short user plane activity (http GET, in this case), and then terminating the session. These subscribers repeat this procedure constantly for the duration of the test.

The bulk of the throughput is simulated by the other group of subscribers, which is configured to establish a session, and perform continuous http GETs without terminating the session. They establish a session at the beginning of the test, and then maintain the same session for the duration of the test.

The reason for separating the subscribers like this is to optimize the usage of the port CPUs of the load modules. The subscribers performing high control plane activity are assigned to a group of port CPUs, while the other group of subscribers is assigned to another group of port CPUs.

By allowing the port CPUs to concentrate on either the throughput or control plane activity exclusively, the power of the CPUs is optimized for maximum traffic.

Objective

The test case is a system test case that has the dual objective of simultaneously generating high throughput user plane data and control plane activity.

Setup

The test case is set up as follows:

- 8 MME + eNodeB pairs, one per port CPU, with 1000 subscribers per pair each generating high throughput http traffic. These subscribers provide the high throughput part of the test.
- 4 MME + eNodeB pairs, one per port CPU, with 5000 subscribers per pair each subscriber establishing a session, downloading a small web page, and deleting the session repeatedly. These subscribers generate the high control plane traffic for the test. The lifetime feature is used to accomplish this setup.
- Multiple configuration parameters depend on the network under test, such as IP addresses for the MMEs and UEs, UE identifier parameters like IMSI and MSISDN, networking parameters, and so on. These parameters are typically obtained by knowing the network configuration.
Step by Step Instructions

1. Insert a new NetTraffic on the server side. Configure it to have a range of 12 IPs, using IP addresses that correspond to the network under test settings.

2. Add an HTTP server activity to the NetTraffic. The default settings can be used.

3. Insert a new NetTraffic on the client side. Select it to configure it, and delete the existing default IP stack by clicking Delete Stack.

4. Add the MME/eNB S11/S1-u stack from the Add Stacks > Wireless menu.

5. Select the User Equipment layer to configure the UEs (subscribers) for the test. The UE layer contains two sub-tabs that should be configured as follows:

   **UE Tab**

   The **UE** tab contains the following additional tabs:
**Basic sub-tab:**
Configure the Maximum Active UE Count value to match the test variables section.

**Identification sub-tab:**
Configure the appropriate values for IMEI, Software Version, IMSI and MSISDN. These values identify the subscription and equipment, and are usually provided by the customer, and must match the values configured in the system under test.

**Mobility sub-tab:**
Do not enable mobility for this test.

**Access Points tab**

![Access Points tab](image)

**Figure 13. Access Points tab**

The **Access Points** tab contains the following additional sub-tabs:

**Basic sub-tab:**
Configure the APN Name and corresponding PGW IP to match the values configured in the system under test. Leave the other values to default values.

**Default bearer sub-tab:**
The QoS values associated to the default bearer are configured here. Configure the QCI to a value of 8, and leave rest of the values to their default values.

**Timeline sub-tab:**
In the lifetime configuration, the user can define a precise duration for the subscriber. In this test, lifetime is not used. Leave the values to default values.
**PCO sub-tab:**

In the PCO configuration, user can enable sending the P-CSCF IP address discovery (IPv4 or IPv6) through PCO IE.

6. Select the **eNB S1-u** layer in the stack to configure the eNodeBs for the test. The e-NodeB layer contains two tabs.

![Figure 14. eNB S1-u Basic Tab](image)

**E-NodeB Tab**

The **E-NodeB** tab contains the following additional sub-tabs:

**Basic sub-tab:**

No change.

**Location sub-tab:**

Configure values that match the values from the network under test. The MNC and MCC values are typically selected to match the network’s values exactly. The Location Area Code, Routing Area Code, Service Area Code, Tracking Area Code and EUTRAN Cell Identifier values must match values configured in the network under test for the simulated Radio Access Network (RAN).

**ENodeBs Connectivity Tab**

This tab allows the configuration of the presence/absence of X2 interfaces between eNodeBs. No change is necessary.

7. Select the **MME S11** layer to configure the MMEs for the test. This layer contains two sub-tabs that should be configured as follows:
MME Tab

The MME tab contains 2 additional sub-tabs:

*Options sub-tab:*
Configure the SGW IP address. This is the main IP address to be used for all initial control plane messages destined to the SGW. The SGW may change this IP address during the course of the session signaling, but that is handled by IxLoad dynamically. Multiple IPs are supported, so if this is required by the configuration, increase the Count value to the appropriate value. Typically, this is left to 1. The UDP source port to be used by the MME for the GTP-c signaling can be configured using the Source UDP Port column. Configure the RAT Type column (Radio Access Technology) to EUTRAN, because this is an LTE test.

*Timers sub-tab:*
These are the GTP protocol timers and counters, which are set to the default values. There is no need to modify them.

DNS Tab

Configure the DNS settings, if needed. This is required in topologies where SGW and PGW IP addresses are resolved by using DNS NAPTR queries.

*Network Group Settings tab:*
No changes are needed.

8. Select the IP layer in the eNB S1-u stack. This IP layer corresponds to the eNodeBs for the test. For each range defined in the eNodeB settings, there is a corresponding range
automatically defined in the IP layer. Configure the appropriate IP range of eNodeBs corresponding to the configuration of the network under test. Configure the **Count** to a value of 8.

9. Select the IP layer in the MME stack. This IP layer corresponds to the MMEs for the test. For each range defined in the MME settings, there is a corresponding range automatically defined in the IP layer. Configure the appropriate IP range of MME corresponding to the configuration of the network under test. Configure the Count to a value of 8.

10. Click the Settings button for the network plugin. Configure the Interface Behavior selection to be Create interface with user, and select the Teardown interface with user checkbox. This action enables dynamic control plane mode.

11. Add an HTTP client activity to the NetTraffic. Configure it to have the previously configured HTTP server as a target. Configure one command in the command list: GET the 1024k.html file.

12. Click the Commands tab of the HTTP activity, and select the **APN** command. Make sure to clear the **Use Dedicated Bearer** checkbox. This action causes the http activity to run on the default bearer for each UE.
13. Add a new NetTraffic on the client side. This is the NetTraffic and subscribers responsible for the high control plane traffic. Follow the steps outlined above to configure it to have a range of 4 MMEs and 4 eNodeBs, one range of 20K Ues. Different values for the UE identifiers must be defined, as configured in the network under test.

14. Modify parameters in the User Equipment layer > Access Points > Timeline sub-tab. Select the **Enable Lifetime** checkbox, and enter the Lifetime as 10 seconds.
15. Add an HTTP client activity to the NetTraffic. Connect it to the same server activity. Configure one command: GET 1b.html, and iterate the command list.

16. In the Timelines and Objectives section, select a throughput objective for the HTTP activity on the throughput network, and configure an objective constraint of Simultaneous Users equal to 8000. Set the throughput objective to 9 Gbps. Configure a 60-minute timeline.

17. Select a Simultaneous Users objective for the HTTP activity for high control plane traffic, and set the objective to 20K. Configure 60 minute timeline duration, with a ramp up value of 1500 users/second.

18. In the Port Assignments section, assign the throughput NetTraffic to the first 8 port CPUs of the Acceleron-NP card.

19. Assign the remaining 4 port CPUs to the control plane NetTraffic.

20. Assign the server NetTraffic to the 12 port CPUs of the second Acceleron-NP load module.

21. Enable 10G aggregation mode for both Acceleron-NP load modules.

22. In the Test Options section, select the Network Diagnostics checkbox to enable the GTP statistics.
Test Variables

Table 3. Test Variables for Throughput Test with High Control Plane (Signaling) Traffic

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE Count for throughput network</td>
<td>8000</td>
</tr>
<tr>
<td>MME count for throughput network</td>
<td>8</td>
</tr>
<tr>
<td>eNodeB count for throughput network</td>
<td>8</td>
</tr>
<tr>
<td>UE count for control plane activity network</td>
<td>20000</td>
</tr>
<tr>
<td>MME count for throughput network</td>
<td>4</td>
</tr>
<tr>
<td>eNodeB count for throughput network</td>
<td>4</td>
</tr>
<tr>
<td>Objective for throughput HTTP activity</td>
<td>Throughput = 8 Gbps</td>
</tr>
<tr>
<td>Objective for control plane HTTP activity</td>
<td>Simultaneous Users = 20K</td>
</tr>
</tbody>
</table>

Results Analysis

In addition to the normal array of statistics to monitor during this test, the most important are the statistics showing the control plane activity on GTP-C and the HTTP throughput, because they are the objectives of the test.

The session activation and deactivation statistics are seen in the EGTP Rates – All Ports view, located in the Network folder of the statistics screen. This view clearly shows both the session establishment rate and the session deactivation rate.
The normal **HTTP Throughput** view shows the user plane throughput results for the test.
EPC Test Case: Constant BHCA

Overview

This is an EPC test case where the system under test is comprised of the SGW, PGW and possibly the PCRF. The test case is performed using IxLoad by simulating the eNodeBs, MME, and internet servers on the SGi interface. The traffic activity is HTTP.

BHCA is a telephony term meaning Busy Hour Call Attempts. Typical telephony test models incorporate this concept along with a constant call hold time to have a predictable and deterministic test. The amount of active calls at a certain point in time is always constant, given a fixed call hold time, and a fixed BHCA. While this concept does not reflect a practical model when considering data sessions instead of circuit switched voice calls, the requirement to be able to execute this deterministic test still exists.

The formula to follow is as follows:

Simultaneous sessions = BHCA/3600 * SHT

Where SHT = Session Hold Time, and simultaneous sessions refer to the amount of default bearers active at one point in time.

To accomplish this type of test, the time duration of a particular session must be constant, and configurable for the user. The lifetime configuration option of IxLoad is used to accomplish this test.

Objective

The objective of the test case is to provide basic user plane load traffic while maintaining a constant control plane activity and a deterministic amount of sessions being active at a point in time.

Setup

The test case is set up as follows:

- Assign 12 ports of an Acceleron-NP load module as the MMEs/eNodeBs, and assign 12 ports of another Acceleron-NP load module as servers.
- Use 10G aggregation mode.
- Define 12 MME/eNodeB pairs, and use 120K subscribers for the test.

The L7 traffic is itself moderate http traffic, downloading a 100K web page, waiting 10 seconds, and repeating, for each subscriber. The sessions are configured to last 30 seconds, after which the session are deactivated, and a new session are created. This ensures that the constant control plane activity required by the test is achieved. Only default bearers are used for the test.
Step by Step Instructions

1. Insert a new NetTraffic on the server side. Configure it to have a range of **12 IPs**, using IP addresses that correspond to the network under test settings.

2. Add an HTTP server activity to the NetTraffic. Use the default settings.

3. Insert a new NetTraffic on the client side. Select it to configure it, and delete the existing default IP stack by clicking Delete Stack.

4. Add the MME/eNB S11/S1-u stack from the Add Stacks > Wireless menu.

![Figure 22. MME/eNB S11/S1-U Stack](image)

5. Click the User Equipment layer to configure the UEs (subscribers) for the test. This layer contains two tabs that are configured as follows:

![Figure 23. User Equipment layer](image)

**UE Tab**

This tab contains the following additional sub tabs.

**Basic sub-tab:**

Configure the Maximum Active UE Count value to match the test variables section.
**Identification sub-tab:**
Configure the appropriate values for IMEI, Software Version, IMSI and MSISDN. These values identify the subscription and equipment, and usually customers provide them. These values must match the values configured in the system under test.

**Mobility sub-tab:**
Do not enable mobility for this test.

**Access Points tab**

![Figure 24. Access Points tab](image)

The Access Points tab contains the following additional sub-tabs:

**Basic sub-tab:**
Configure the **APN Name** and corresponding **PGW IP** to match the values configured in the system under test. Leave the other values at default.

**Default bearer sub-tab**
The QoS values associated to the default bearer are configured here. Configure the QCI to a value of 8, and leave the remaining values to default.

**Timeline sub-tab:**
Select the **Enable Lifetime** check box, and set the Lifetime value to 30 seconds. This value causes the default bearer, and therefore the subscriber, to last for exactly 30 seconds, after which the bearer is deleted, and then re-established. This process happens for every iteration of the HTTP command in the list.
6. Click eNB in the stack to configure the eNodeBs for the test. The eNB layer contains the following tabs:
EPC Test Case: Constant BHCA

**Figure 26. eNodeBBasic Tab**

**E-NodeB Tab**

The E-NodeB tab contains the following additional sub-tabs:

*Basic sub-tab:*

No change.

*Location sub-tab:*

Configure values that match the values from the network under test. The MNC and MCC values are typically selected to match the network’s values exactly. The Location Area Code, Routing Area Code, Service Area Code, Tracking Area Code and EUTRAN Cell Identifier values must match values configured in the network under test for the simulated Radio Access Network (RAN).

**ENodeBs Connectivity Tab**

In this tab, the user can configure the presence/absence of X2 interfaces between eNodeBs. No change is necessary.

7. Click MME to configure the MMEs for the test. This layer contains the following additional sub-tabs as shown in the following figure.
MME Tab

The MME tab contains the following additional sub-tabs:

**Options sub-tab:**

Configure the **SGW IP** address - the main IP address to be used for all initial control plane messages destined to the SGW. The SGW may change this IP address during the course of the session signaling, but that is handled by IxLoad dynamically. Multiple IPs are supported, so if this is required by the configuration, increase the **Count** value to the appropriate value. Typically, this is left to 1. Using the Source UDP Port Column, the user can configure the UDP source port to be used by the MME for the GTP-c signalling. Configure the RAT-Type column (Radio Access Technology) to EUTRAN, because this test is an LTE test.

**Timers sub-tab:**

These timers are the GTP protocol timers and counters, which are set to the default values. There is no need to modify them.

**Network Group Settings Tab**

No changes are needed.

8. Select the IP layer in the eNB stack. This IP layer corresponds to the eNodeBs for the test. For each range defined in the eNodeB settings, there is a corresponding range automatically defined in the IP layer. Configure the appropriate IP range of eNodeBs corresponding to the configuration of the network under test. Configure the Count to a value of 12.
9. Select the IP layer in the MME stack. This IP layer corresponds to the MMEs for the test. For each range defined in the MME settings, there is a corresponding range automatically defined in the IP layer. Configure the appropriate IP range of MME corresponding to the configuration of the network under test. Configure the Count to 12.

10. Click the Settings button for the network plugin. Configure the Interface Behavior selection to Create interface at the start and teardown at the end of the command list. This enables dynamic control plane mode.

11. Add an HTTP client activity to the NetTraffic. Configure it to have the previously configured HTTP server as a target. Configure two commands in the command list: GET the 128k.html file, and Think for 30s. Make sure the iterate command list is selected.

12. Click the Commands tab of the HTTP activity, and select the APN command. Make sure to select the Use Dedicated Bearer checkbox. This selection causes the http activity to run on the default bearer for each UE.
13. In the Timelines and Objectives section, select a Simultaneous Users objective for the HTTP activity. Configure a 60 minute timeline.

14. In the Port Assignments section, assign the client NetTraffic to the 12 port CPUs of the first Acceleron-NP load module.

15. Assign the server NetTraffic to the 12 port CPUs of the second Acceleron-NP load module.

16. Enable 10G aggregation mode for both Acceleron-NP load modules.

17. In the Test Options section, enable the Network Diagnostics check box to enable the GTP statistics.

**Test Variables**

**Table 4. Test Variables for Constant BHCA Test**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE Count</td>
<td>120000</td>
<td></td>
</tr>
<tr>
<td>MME count</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>eNodeB count</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>HTTP activity -&gt; EGTP -&gt; Session Timeout</td>
<td>Enabled</td>
<td>To enable the precise time duration of the default bearer for each UE</td>
</tr>
</tbody>
</table>
EPC Test Case: Constant BHCA

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP activity -&gt; EGTP -&gt; Session Timeout -&gt; Timeout Value</td>
<td>30s</td>
<td></td>
</tr>
<tr>
<td>Objective for HTTP activity</td>
<td>SU = 120K</td>
<td></td>
</tr>
</tbody>
</table>

Results Analysis

The statistics that are important to monitor for a constant BHCA test are the rates at which the sessions are being activated and deactivated, and how many sessions are active at one point in time.

IxLoad provides the session activate and deactivation rates in the EGTP Rates – All Ports statistics view. Both the activation and deactivation rates are shown in the same view. The example below shows a reduced configuration where the session duration timeout configured for 30s. From second 6 of the test to second 36, sessions are established and maintained. Starting at second 36, the originally established sessions start terminating, because of the session duration timeout. Thus, the session deactivation rate ramps up at the same rate that the sessions were established. Afterwards, both stats maintain the same rate, which corresponds to a constant BHCA.

![Figure 31. EGTP - Rates Control](image)

To view the amount of active sessions, the EGTP General view is used. By selecting the All Bearers tab at the bottom of the view, the Active Sessions statistic is immediately available. For a constant BHCA test, it must remain at the same value during the sustain period of the test.
The *Sessions Terminated* stat starts increasing steadily after 30s, the value corresponding to the session time configuration value.

![Figure 32. EGTP General View](image-url)
EPC Test Case: Small Packets and Multiple Bearers

Overview

In an EPC test case, the system under test comprises the SGW, PGW, and possibly the PCRF. The test case is performed using IxLoad by simulating the eNodeBs, MME, and internet servers on the SGi interface. The traffic activity is HTTP.

Mobile environments sometimes result in the user plane traffic being transported using small packets, either because of the nature of the traffic or because of the radio interface itself. The average packet size can be approximately 600 octets. In addition, LTE offers the possibility to have multiple bearers per UE. Multiple bearers are meant to address QoS differences between the traffic types being run by the subscriber. Network policy determines if the subscriber will be allowed dedicated bearers or not, thus allowing a network operator to offer differentiated services.

Objective

The EPC test case has a dual objective:

- Testing the packet switching ability with small packets
- To exercise this functionality with multiple bearers per subscriber.

Setup

The test case will be set up as follows:

- Assign 12 ports of an Acceleron-NP load module as the MMEs/eNodeBs, and assign the 12 ports of another Acceleron-NP load module as servers.
- Use 10G aggregation mode.
- Define 12 MME/eNodeB pairs, and use 120K subscribers for the test.

The L7 traffic itself is the http and ftp traffic, where the http runs over the default bearer, while the ftp downloads are given a dedicated bearer.

Step by Step Instructions

1. Insert a new NetTraffic on the server side. Configure it to have a range of 24 IPs, using IP addresses that correspond to the network under test settings.
2. Add an HTTP server activity to the NetTraffic. Use the default settings except for Effective Send MSS (Tx) under the activity settings, advanced options: set this value to 600.
3. Add an FTP server activity to the NetTraffic. Use the default settings except the Effective Send MSS (Tx): set this value to 600.
4. Insert a new NetTraffic on the client side. Select it to configure it, and delete the existing default IP stack by clicking Delete Stack.

5. Add the MME/eNB S11/S1-u stack from the Add Stacks > Wireless menu.

6. Click User Equipment to configure the UEs (subscribers) for the test. The User Equipment layer contains two tabs that must be configured as follows:

**UE Tab**

The UE tab contains the following additional sub-tabs:

*Basic sub-tab:*

Configure the **Maximum Active Total UE Count** value to match the test variables section.
**Identification sub-tab:**
Configure the appropriate values for IMEI, Software Version, IMSI and MSISDN. These values identify the subscription and equipment, and usually customers provide them. These values must match the values configured in the system under test.

**Mobility sub-tab:**
Do not enable mobility for this test.

**Access Points tab**

![Access Points tab](image)

The Access Points tab contains the following additional sub-tabs:

**Basic sub-tab:**
Configure the APN Name and corresponding PGW IP to match the values configured in the system under test. Leave the other values to default.

**Default bearer sub-tab:**
The QoS values associated to the default bearer are configured here. Configure the QCI to a value of 8, and leave the remaining values to default.

**Timeline sub-tab:**
In the lifetime configuration, the user can define a precise duration for the subscriber. In this test, lifetime is not used. Leave the Enable Lifetime checkbox cleared. Also, leave the HSS Update Enable checkbox cleared as well.

7. Click eNB in the stack to configure the eNodeBs for the test. The eNB layer contains 3 tabs.
The E-NodeB tab contains the following additional sub-tabs:

**Basic sub-tab:**
No change.

**Location sub-tab:**
Configure values that match the values from the network under test. The MNC and MCC values are typically selected to match the network’s values exactly. The Location Area Code, Routing Area Code, Service Area Code, Tracking Area Code and EUTRAN Cell Identifier values must match values configured in the network under test for the simulated Radio Access Network (RAN).

**ENodeBs Connectivity Tab**
This tab allows the configuration of the presence/absence of X2 interfaces between eNodeBs. No change is necessary.

8. Click the MME layer to configure the MMEs for the test. This layer contains two tabs that must be configured as follows:
MME Tab

The MME tab contains the following additionalsub-tabs:

Options sub-tab:

Configure the SGW IP address. This is the main IP address is used for all initial control plane messages destined to the SGW. The SGW may change this IP address during the course of the session signaling, but IxLoad dynamically handles it. Multiple IPs are supported, so if this is required by the configuration, increase the Count value to the appropriate value. Typically, this is left to 1. Users can configure the UDP source port to be used by the MME for the GTP-c signaling using the Source UDP Port column. Configure the RAT Type column (Radio Access Technology) to EUTRAN, because this is an LTE test.

Timers sub-tab:

These timers are the GTP protocol timers and counters that are set to the default values. There is no need to modify them.

Network Group Settings Tab

No changes are needed.

9. Click the IP layer in the eNB stack. This IP layer corresponds to the eNodeBs for the test. For each range defined in the eNodeB settings, there is a corresponding range automatically defined in the IP layer. Configure the appropriate IP range of eNodeBs corresponding to the configuration of the network under test. Configure the Count to a value of 12.
10. Click the IP layer in the MME stack. This IP layer corresponds to the MMEs for the test. For each range defined in the MME settings, there is a corresponding range automatically defined in the IP layer. Configure the appropriate IP range of MME corresponding to the configuration of the network under test. Configure the Count to a value of 12.

11. Click the Settings button for the network plugin. In the Interface Behavior section, click Create interface with user, and select the Teardown interface with user checkbox. This enables dynamic control plane mode.

12. Add an HTTP client activity to the NetTraffic. Configure it to have the previously configured HTTP server as a target. Configure one command in the command list: GET the 1024k.html file, and make sure the iterate command list is selected.

13. Click the Commands tab of the HTTP activity, and select the APN command. Make sure that the Use Dedicated Bearer checkbox is unselected. This selection causes the http activity to run on the default bearer for each UE.
14. Add an FTP client activity to the NetTraffic. Configure it to have the previously configured FTP server as a target. Configure two commands in the command list: {get} the /#1048576 file, and Think for 30s. Make sure the iterate command list is selected.

15. Click the Commands tab of the FTP activity, and select the APN command. Select the Use Dedicated Bear check box. This selection causes the http activity to run on the default bearer for each UE. Click MS Initiated Bearer, and clear Use Default QCI. Enter the value for QCI as 9.
16. In the Timelines and Objectives section, select a Simultaneous Users objective for the HTTP client activity, and set the objective to 120K. Configure a 60 minute timeline. Configure the same values for the FTP client activity.

17. In the Port Assignments section, assign the client NetTraffic to the 12 port CPUs of the first Acceleron-NP load module.

18. Assign the server NetTraffic to the 12 port CPUs of the second Acceleron-NP load module.

19. Enable 10G aggregation mode for both Acceleron-NP load modules.

20. In the Test Options section, select the Network Diagnostics checkbox to enable the GTP statistics.
Test Variables

The test variables highlights are shown in the following table.

Table 5. Test Variables for Small Packets and Multiple Bearers Test

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE Count</td>
<td>120000</td>
<td></td>
</tr>
<tr>
<td>MME count</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>eNodeB count</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Objective for HTTP activity</td>
<td>SU = 120K</td>
<td></td>
</tr>
<tr>
<td>Objective for FTP activity</td>
<td>SU = 120K</td>
<td></td>
</tr>
<tr>
<td>FTP activity -&gt; EGTP - &gt; Use default bearer for this activity</td>
<td>Unselected</td>
<td>This is to ensure that the FTP activity obtains a dedicated bearer</td>
</tr>
<tr>
<td>Server MSS</td>
<td>600</td>
<td>This is to ensure that the downlink packets from both the HTTP and FTP servers will not exceed 600 octets.</td>
</tr>
</tbody>
</table>

Results Analysis

The main statistics that you need to track for this test are, the GTP-U packets/second and the session statistics for eGTP.

The session statistics become a highlight for the test results, because this test uses default and dedicated bearers. The view containing these stats is the EGTP General view. For each simulated UE, two bearers are established. This is indicated by the Sessions Initiated, Sessions Succeeded and Sessions Succeeded(D) statistics. Sessions Initiated corresponds to the total amount of bearers activated during the test, while Sessions Succeeded shows how many initiated sessions were successfully established. The Sessions Succeeded(D) stat shows the same result for dedicated bearers only.
Typically, when a test with small packets is run, a goal of the test is to reach a certain packet/second rate on the GTP-U protocol. It will be stressed harder than usual because of the small packet size. IxLoad provides the GTP-U packets/second stat in the **EGTP-U Rates** view, which shows the Tx and Rx GTP-U packet rates.
EPC Test Case: Small Packets and Multiple Bearers

Figure 43. EGTP - Packet Rates Statistics
Figure 44. EGTP – Data Rates Statistics
EPC Test Case: Handovers

Overview

This test case exercises handover capability while forwarding traffic at a high rate. The test simulates 120,000 subscribers browsing Web pages while performing various types of handovers. Specifically, the types of handovers that are performed are as follows:

- X2-based handovers
- S1-based handovers with MME relocation
- S1-based handovers without MME relocation

There are no handovers involving SGW relocation, because this test uses default and dedicated bearers.

Handovers are configured to happen at an interval of 65 s for each individual UE. As there are 120,000 UEs active during the test, the amount of handovers executed per second during this test are as follows:

Handover rate = 1/65s * 120K = 1846 handovers/second

Objective

The Handovers test case is a system test case that has the dual objective of simultaneously generating high throughout user plane data combined with a medium rate of constant handovers during the test.

Setup

The test case is set up as follows:

12 MME + eNodeB pairs, one per port CPU, with 10000 subscribers per pair, each generating high throughput http traffic and performing handovers.

Multiple configuration parameters depend on the network under test, such as IP addresses for the MMEs and UEs, UE identifier parameters like IMSI and MSISDN, and networking parameters. These are typically obtained by knowing the network configuration.
Step by Step Instructions

1. Insert a new NetTraffic on the server side. Configure it to have a range of 12 IPs, by using IP addresses that correspond to the network under test settings.

2. Add an HTTP server activity to the NetTraffic. The user can use the default settings.

3. Insert a new NetTraffic on the client side. Select it to configure it, and delete the existing default IP stack by clicking Delete Stack.

4. Add the MME/eNB S11/S1-u stack from the Add Stacks > Wireless menu.

5. Click the MME layer to configure the MMEs for the test. This layer contains two tabs that are configured as follows:

**MME Tab**

The MME tab contains the following additional sub-tabs:
EPC Test Case: Handovers

**Options sub-tab:**
Click the green ‘+’ icon at the bottom left of the pane to add an additional MME.

Configure the **SGW IP** address for each MME range. Assuming that there is only one SGW under test, use the same SGW IP address for both MME ranges. This is the main IP address to be used for all initial control plane messages destined to the SGW. The SGW may change this IP address during the course of the session signaling, but IxLoad dynamically handles it. Multiple IPs are supported, so if this is required by the configuration, increase the **Count** value to the appropriate value. Typically, this is left to 1. Users can configure the UDP source port to be used by the MME for the GTP-c signaling by using the **Source UDP Port** column. Configure the **RAT Type** column (Radio Access Technology) to **EUTRAN**, because this is an LTE test.

**Timers sub-tab:**
These are the GTP protocol timers and counters, which are set to the default values. We recommend you not to modify them.

6. Click the IP layer in the MME stack. This IP layer corresponds to the MMEs for the test.

![MME IP layer](image)

**Figure 47.** MME IP layer

In this layer, a user can configure the IP address range for the MME ranges. For this test, configure a **Count** of **12** for each MME range (corresponding to one MME per port CPU used for this NetTraffic, for each MME range). Configure the starting IP address, mask, and gateway according to the network under test configurations.

7. Click the eNB layer to configure the eNodeBs for the test. The e-NodeB tab contains three tabs that are configured as follows:
EPC Test Case: Handovers

The E-NodeB tab contains the following additional sub-tabs:

**Basic sub-tab:**
Click ‘+’ icon at the bottom left of the pane to add three more eNodeB ranges (for a total of four ranges). For the eNB-R2 range, select MME-R2 as the parent MME ID. eNodeBs are configured such that each range gets one parent MME.

**Location tab:**
Configure values that match the values from the network under test. The **MNC** and **MCC** values are typically selected to match the network’s values exactly. The **Location Area Code**, **Routing Area Code**, **Service Area Code**, **Tracking Area Code**, and **EUTRAN Cell Identifier** values must match values configured in the network under test for the simulated Radio Access Network (RAN).
ENodeB Connectivity Tab

The ENodeBs connectivity tab serves to configure the connections between the eNodeBs for the test. This connectivity matrix represents the presence or absence of the X2 interface between eNodeB ranges. If a check box is selected between two eNodeB ranges, it means that there is an X2 interface connecting those two eNodeB ranges. For this test, select the check boxes between eNB-R1 and eNB-R4, and eNB-R3 and eNB-R4, as indicated in the following figure.

Figure 49. ENodeBs Connectivity Sub-Tab

If the presence of an X2 interface between two eNodeBs is indicated, this means an X2 handover is possible between those eNodeBs. But if the X2 interface is not present between two eNodeBs, a handover between them is a S1-based handover.

8. Click the IP layer in the eNodeB stack. For each range defined in the eNodeB settings, there is a corresponding range automatically defined in the IP layer. Configure the appropriate IP range of eNodeBs corresponding to the configuration of the network under test. Configure the Count to a value of 12.

9. Click the User Equipment layer to configure the UEs (subscribers) for the test. The User Equipment layer contains two tabs that are configured as follows:
UE Tab

The UE tab contains the following additional sub-tabs:

**Basic sub-tab:**
Configure the Count value to match the test variables section.

**Identification sub-tab:**
Configure the appropriate values for IMEI, Software Version, IMSI and MSISDN. These values identify the subscription and equipment, and usually customers provide them. The values must match the values configured in the system under test.

**Mobility sub-tab:**
The Mobility tab is used to configure handovers for the UEs. Select the Enable Mobility check box to enable handovers for the UE range. Next, click the ellipsis in the Mobile Path column to configure the handover path that the UEs traverse. This configuration determines the exact handovers that each UE performs, moving from one eNodeB to the next.
Click the green ‘+’ icon in the bottom left-pane of the window to add three steps to the mobile path. Knowing that the UE range is configured to be on eNB-R1, to begin the test (from the UE configuration, basic tab), configure the first step to be eNB-R2, the second step to be eNB-R3, and finally the last step to be eNB-R4, as illustrated in the figure.

This activity creates the following handovers to occur, for each UE in the range:

- The UE will handover from eNB-R1 to eNB-R2
- The UE will handover from eNB-R2 to eNB-R3
EPC Test Case: Handovers

- The UE will handover from eNB-R3 to eNB-R4
- The UE will handover from eNB-R4 to eNB-R1

This mobile path is then repeated for the entire duration of the test.

Close the **Mobile Path Configuration** window, and configure the rest of the mobility tab values as follows:

- **Mobility Interval**: 65. This value represents the time (in seconds) between each step of the mobile path, independently for each UE in the range.

- **Maximum Interval Variation**: 5. This value is the variation value for the interval, such that handovers do not occur exactly every 65 s, but happen each 65 +/- 5%.

- **Start Delay**: 120. This value delays the handovers such that no handover occurs until 120 s from the start of the test have elapsed. The delay is to give time for the UEs to ramp up before the handover signaling starts.

- **Maximum delay variation**: 0.

**Timeline tab:**

Do not enable the timeline for this test. Use the default values.

**Access Points Tab**

![Access Points tab](image)

The Access Points tab contains the following additional sub-tabs:

- **Basic sub-tab:**
  Configure the **APN** and corresponding **PGW IP** to match the values configured in the system under test. Leave the other values to default.

- **Default bearer sub-tab:**
  The QoS values associated to the default bearer are configured here. Configure the QCI to a value of 8, and leave the rest of the values to their default values.
**Timeline tab:**
The lifetime configuration allows the user to define a precise duration for the subscriber. In this test, lifetime is not used. Clear both the **Enable Lifetime** and **The HSS Update Enable** checkboxes.

10. Click Settings for the network plugin. In the Interface Behavior section click Create interface with user, and select the Teardown interface with user check box. This enables dynamic control plane mode.

![Image of Settings Button](image1)

**Figure 54. Settings Button**

![Image of Interface Behavior](image2)

**Figure 55. Interface Behavior**

11. Add an HTTP client activity to the NetTraffic. Configure it to have the previously configured HTTP server as a target. Configure one command in the command list: GET the 1024k.html file, and make sure the iterate command list is selected.

12. Click the Commands tab of the HTTP activity, and select the APN command. Make sure that the Use Dedicated Bearer checkbox is cleared. This action causes the http activity to run on the default bearer for each UE.
13. In the Timelines and Objectives section, select a Simulated Users objective for the HTTP activity on the client network, and configure an objective value of 120000. Configure a 60-minute timeline duration, with a ramp up value of 1000 users/second.

14. In the Port Assignments section, assign the client NetTraffic to the 12 port CPUs of the first Acceleron-NP card.

15. Assign the server NetTraffic to the 12 port CPUs of the second Acceleron-NP load module.

16. Enable 10G aggregation mode for both Acceleron-NP load modules.

17. In the Test Options section, select the Network Diagnostics check box to enable the GTP statistics.
Test Variables

Table 6. Test Variables for Throughput Test with High Control Plane (Signaling) Traffic

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE Count</td>
<td>120K</td>
<td></td>
</tr>
<tr>
<td>MME count for client network (eNodeB and MME)</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>eNodeB count for client network (eNodeB and MME)</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Objective for HTTP activity</td>
<td>SU = 120K</td>
<td></td>
</tr>
<tr>
<td>Mobility interval</td>
<td>65s</td>
<td></td>
</tr>
<tr>
<td>Maximum interval variation</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td>Start delay</td>
<td>120s</td>
<td></td>
</tr>
<tr>
<td>Start delay variation</td>
<td>0s</td>
<td></td>
</tr>
</tbody>
</table>

Results Analysis

The statistics here to watch are the handovers, because this is a handover focused test. All handover related statistics are available in the same view called eGTP – Handover.

The view contains five tabs:

- **All**: Contains all the statistics related to all the different types of handovers.
- **Total**: Contains totals initiated and failed for all handover types.
- **X2 Based Handovers**: Contains statistics that only relate to X2-based handovers.
- **S1 Based Handovers**: Direct Forwarding: Contains the statistics related to S1-based handovers by using direct forwarding.
- **S1 Based Handovers**: Indirect Forwarding: Contains the statistics related to S1-based handovers that do not make use of direct forwarding.

All the tabs will be interesting to monitor during the test, because this test contains handovers of all types as outlined earlier.
### Figure 57. The Handover Statistics View, All tab

The preceding figure shows the **Total** tab. It summarizes the various handovers types that were attempted, and shows how many succeeded, and also if any have failed to complete.
The above figure shows more details related to the X2 based handovers executed during the test.
EPC Test Case: eNodeB Plugin IDLE/Paging Procedure Using Subscriber Model

Overview

In an EPC test case, the system under test comprises of the MME, SGW, PGW, and possibly the PCRF. The test case is performed using IxLoad by simulating the eNodeBs and internet servers on the SGi interface. The traffic activity is StatelessPeer (UDP).

Objective

This is a system test case that has the objective of simulating UEs going into IDLE mode and receiving Downlink traffic which triggers Paging procedure.

Setup

1 eNodeB, one port CPU, with 1 subscriber, using Subscriber mode on eNodeB side and 1 host (IP) on SGi side (internet), using NetTraffic mode, one port CPU.

Multiple configuration parameters depend on the network under test, such as IP addresses for the MMEs and eNodeB, UE identifier parameters like IMSI and MSISDN, and networking parameters. These are typically obtained by knowing the network configuration.

Step by Step Instructions

1. Insert a new NetTraffic on the Terminate side. Configure it to have a range of 1 IP, by using IP address that corresponds to the network under test settings (PGW SGi interface).
2. Add a StatelessPeer activity to the NetTraffic. Refer to below section detailing activity settings.
3. Insert a new Subscriber on the Originate side.
4. Select it to configure, and delete the existing default IP stack (Delete Stack).
5. Add the eNodeB S1-MME/S1-U stack.
UE Tab

The UE tab contains the following additional sub-tabs:

**Basic sub-tab:**
Configure the **Count** value to match the test variables section.

**Details sub-tab:**
Configure the appropriate values for **MCC**, **MNC**, **IMEI**, **Software Version**, **Auth K Value** and **Auth OP Value**. These values, usually provided by the customers, identify the subscription and equipment and must match the values configured in the system under test (MME).

**Mobility sub-tab:**
Do not enable mobility for this test.

**Access Points Tab**

The Access Points tab contains the following additional sub-tabs:
**Basic sub-tab:**
Configure the **APN Name** and **IP Type** to match the values configured in the system under test. Leave the other values at default.

**Timeline sub-tab:**
Timeline configuration is disabled when running in Subscriber mode.

**eNodeB Tab**
The eNodeB tab contains the following additional sub-tabs:

**Options sub-tab:**
eNodeBs are configured such that each range gets one parent MME.

Configure the **Macro eNodeB Start ID** and **Source SCTP Port** to match the value configured in the system under test. Leave the other values to default.

Select **Use “User Plane” IP for “Control Plane” IP** if your configuration uses a single IP address for both Control and User Planes. Active IP address is the one configured under **UP-IP** range.
Location tab:
Configure values that match the values from the network under test. The **Home MCC**, **Home MNC**, and **TAC** values must match the system under test values exactly. Leave the other values to default.

**MME Pools Tab**
Configure the values that match the values from the network under test: **MME IP Address** and **IP Type**.

**eNodeB Connectivity Tab**
No change needed.

**Network Group Settings Tab**
No change needed.

**eNB S1-MME CP Tab**
Select Control Plane section (**eNB S1-MME CP**) to add network commands.

6. Add the following: Think, Enter Idle State, Wait For Paging, Think. Each UE executes this command list after Initial Attach until Sustain Time lapses.

   Leave default value for both Think commands (1000 ms). The main purpose of Think is to synchronize Control Plane with L7 commands.
StatelessPeer activity

Click the green + button on the Subscriber ribbon to add StatelessPeer activity to the Subscriber.

StatelessPeer command list

Add StatelessPeer commands by selecting Subscriber layer and using green + button available in StatelessPeer Command Editor window.
Configure the following commands: **Generate Trigger** (needed for Terminating side to learn UE’s IP address dynamically allocated during Attach procedure), **Generate UDP Stream**, **Think**, and **Generate UDP Stream**. First the system runs **Generate UDP Stream** immediately after attach, before UE going into IDLE state. Enter Idle State is triggered by the subsequent Think command from the StatelessPeer activity through Sync Event.
7. Configure the following parameters for Generate Trigger command:

<table>
<thead>
<tr>
<th>Initiator and Responder Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port (s)</td>
</tr>
<tr>
<td>Destination</td>
</tr>
<tr>
<td>Responder Peer</td>
</tr>
<tr>
<td>Responder Port(s)</td>
</tr>
<tr>
<td>Enable Random Source Ports</td>
</tr>
<tr>
<td>Enable Random Responder Ports</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trigger Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Size</td>
</tr>
</tbody>
</table>

Figure 67. Sync Event used for Control – User Plane synchronization

Figure 68. Generate Trigger parameters
8. Configure the following parameters for Generate UDP Stream commands; by setting different values for port and payload size the user can easily identify packets in the flow and capture:

<table>
<thead>
<tr>
<th>Command Properties for 'Generate UDP Stream'</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiator and Responder Settings</td>
</tr>
<tr>
<td>Destination: Traffic1_StatelessPeer2</td>
</tr>
<tr>
<td>Source Port (s): 5000</td>
</tr>
<tr>
<td>Responder Peer: Traffic1_StatelessPeer2</td>
</tr>
<tr>
<td>Responder Port(s): 5000</td>
</tr>
<tr>
<td>Enable Random Source Ports:</td>
</tr>
<tr>
<td>Enable Random Responder Ports:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stream Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Frequency:</td>
</tr>
<tr>
<td>Minimum Value: 1 packets/sec</td>
</tr>
<tr>
<td>Maximum Value: 1 packets/sec</td>
</tr>
<tr>
<td>Duration: 10 second(s)</td>
</tr>
</tbody>
</table>

**1st Generate UDP Stream command**

**Terminating side StatelessPeer**

Add the following commands to SGi StatelessPeer activity: **Wait for Trigger** and **Generate UDP Stream**.
9. Configure the Delay Next Command parameter with a value of 25 seconds. This configuration allows enough time for other commands to run and for Paging to occur while UE is in IDLE state.

![Figure 70. Terminating side StatelessPeer](image1)

**Command Properties for 'Wait For Trigger'**

<table>
<thead>
<tr>
<th>Trigger Options</th>
<th>Delay Next Command</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>25 seconds</td>
</tr>
</tbody>
</table>

![Figure 71. Wait For Trigger settings](image2)

10. Configure the following parameters for Generate UDP Stream command. The Source and Responder Port(s) must match with the values configured for Generate Trigger on eNodeB side.

![Figure 72. Generate UDP Stream settings](image3)

11. Configure Parallel Stream Count (Settings – Advanced Options) with a value of 10. This parameter must match the number of active UEs, because the number of IP hosts on Terminate (SGi) side must be kept to a minimum (that is, value of 1) to generate symmetrical traffic.

![Figure 73. Parallel Command Count](image4)

**General Settings**

Click the **Settings** button for the network plugin. In the **Interface Behavior** section, click **Create interface at the start and teardown at the end of the command list**. This selection enables dynamic control plane mode.
12. In the Timelines and Objectives section, select Subscribers objective for the StatelessPeer activity on the client network, and configure an objective value of 10. Configure a 3-minute timeline duration, with a ramp up value of 1 users/second.

13. In the Port Assignments section, assign 1 port CPUs of the first Xcellon-NP card to the Subscriber on Originate side.


15. In the Test Options section, select the Network Diagnostics check box to enable the GTP statistics.
EPC Test Case: eNodeB Plugin IDLE/Paging Procedure Using Subscriber Model

Test Variables

Table 7. Test Variables for eNodeB IDLE/Paging test

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE Count</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>eNodeB count for client network</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>IP count on SGi (Terminate) side</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Objective for Subscriber Stateless Peer activity (eNodeB)</td>
<td>Subscriber = 10</td>
<td></td>
</tr>
<tr>
<td>Objective for NetTraffic Stateless Peer activity (SGi)</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Parallel Stream Count</td>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>

Results Analysis

As this is a Control Plane procedure test, the statistics to watch are the Sessions and Messages.

In the eNodeB S1-MME/S1-U Sessions view user needs to validate that all sessions were successful and active:

Same view displays counter for Paging events followed by an equal number of Service Requests (counter should be a multiple of active UEs):
In the **eNodeB S1-MME/S1-U Messages** view, user should validate number of transmitted UE Context Release Request (sent when entering IDLE state) to match the Service Request (sent when exiting IDLE as a consequence of Paging):

Next figure shows typical call flow for this procedure (S1AP messages captured on S1-MME interface, including S1-Setup which establishes link between eNB and MME):
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

Overview

With the migration of mobile networks to all IP networks defined by the LTE specification, there is a need to migrate the voice and sms services as well. Today, there are several options for carrying voice over LTE, using different technologies:

- **CSFB, Circuit Switched Fall Back**: The circuit switched fallback, CSFB option for providing voice over LTE has been standardized under 3GPP specification 23.272. Essentially LTE CSFB uses a variety of processes and network elements to enable the circuit to fall back to the 2G or 3G connection (GSM, UMTS, CDMA2000 1x) before a circuit switched call is initiated.

- The specification also allows for SMS to be carried as this is essential for very many set-up procedures for cellular telecommunications. To achieve this, the handset uses an interface known as SGs which allows messages to be sent over an LTE channel.

- **SV-LTE - simultaneous voice LTE**: SV-LTE allows running packet switched LTE services simultaneously with a circuit switched voice service. SV-LTE facility provides the facilities of CSFB at the same time as running a packet switched data service. This is an option that many operators will opt for. However, it has the disadvantage that it requires two radios to run at the same time within the handset. This has a serious impact on battery life.

- **VoLGA, Voice over LTE via GAN**: The VoLGA standard was based on the existing 3GPP Generic Access Network (GAN) standard, and the goal was to enable LTE users to receive a consistent set of voice, SMS (and other circuit-switched) services as they transition between GSM, UMTS and LTE access networks.

- **Voice over LTE, VoLTE (initially called One Voice)**: The Voice over LTE, VoLTE aims for providing voice over an LTE system utilizes IMS enabling it to become part of a rich media solution.

One additional approach which is not initiated by operators is the usage of Over-the-top (OTT) content services, using applications like Skype and Google Talk to provide LTE voice service. However, handing the LTE voice service over completely to the OTT actors is expected to not receive too much support in the telecom industry, while the voice call service is, and will still be, the main revenue source for the mobile operators.
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

The typical topology for VoLTE is shown below. The SIP registration and call control messages are sent from the User Endpoint (UE) over the default bearer in EPC to the Proxy Call Session Control Function (P-CSCF), the entry point in the IMS domain. In some networks a Session Border Controller (SBC) is used for this function. The Serving Call Session Control Function (S-CSCF) is the central node of the signaling plane. It is a SIP server that communicates to the Home Subscriber Server to download the users' profiles. S-CSCF controls over the Mr or Mg interfaces the Media Server and Media Gateway for voice routing.

![VoLTE Topology](image)

To assure a good quality of voice, a dedicated bearer with high QoS is used for conversational speech in the EPC domain. The allocation of the dedicated bearer is requested by the P-CSCF to the Policy and Charging Rules Function (PCRF) over the Rx interface (this is a Diameter interface).

SMS-over-IP is also a functionality specified by VoLTE. The UE submits a short message via a SIP MESSAGE request that follows the same path to the S-CSCF. From this point, depending on the user profile (obtained by S-CSCF from HSS) the SIP request is sent to the IP-SM-GW (IP Short Message Gateway); for simplicity this server is not represented in the topology shown in the figure above. The submission report is sent by the IP-SM-GW to the UE as a SIP MESSAGE Request. The SMS submit and submission report requests use the same SIP Method, but with different content-body.

**Objective**

The goal of this test methodology is to determine the capacity of the EPC to handle a specific volume of calls without degradation of voice quality.
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

Setup

The EPC isolation test configuration is used for this test, where IxLoad will emulate:

- the User Endpoints over eNodeBs and MME (the left side of the topology diagram in the diagram below)
- the IMS network; that is the P-CSCF and all the devices behind it

Voice calls originate from the UEs (eNodeB /MME) and are terminated by user agents behind in the IMS network.

![EPC Isolation Test Configuration](image)

**Figure 77. EPC Isolation Test Configuration**

Step by Step Instructions

The step-by-step instructions highlight how to set the essential parameters of this configuration and explain additional options, which may be used to change the behavior of the test.

The final IxLoad configuration as a result of these steps is provided in the blackbook.ixiacom.com Web site - see `VoIP-VoLTE-IxLoad6.0.crf`. The configuration consists in two files: the test repository, a file with .rxf extension, and the test scenario for the SIP call flow, a file with the .tst extension. These two files are archived in a single .crf file. To import a Compressed Repository File (.crf) in IxLoad, use the command **Import** under the **File** menu.
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

Create the Network Traffic for UEs

1. Open the IxLoad GUI
2. Add the Originate Net Traffic

The menu is context sensitive; to have access to Add Net Traffic button first select the Networks and Traffic in the navigation pane.
3. Add the MME/eNB S11/S1-U Stack Manager interface to the Originate Net Traffic.

By default, the Net Traffic added in step 2 contains a range of IPv4 addresses. The intention in this configuration is to emulate User Endpoints over MME and eNodeB that are connected through S11 and S1-U interfaces to the S-Gateway. These interfaces are provided by the MME/eNB S11/S1-U stack manager component. Select the Network1, right click on the IP-1, select Add above, and then MME/eNB S11/S1-u

![Figure 80. Add MME/eNB S11/S1-U Stack](image)

4. Configure the IP addresses for the emulated eNodeB and emulated MME:
   a. One eNodeB with the IP address 30.0.0.1 is emulated by this configuration. Select the **IP-ENB** element and set the **Address** and the **Count**

![Figure 81. Setting the eNodeB IP address](image)
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

b. One MME with the IP address 30.0.1.1 is emulated by this configuration. Select the IP-MME element and set the Address and the Count

![Figure 82. Setting the MME IP address](image)

5. Configure the emulated User Equipment parameters:

a. the APN (Access Point Name) must match the name configured on the system under test; for this example the APN is set to apn-1.test.com

b. The IP address of the PGW to which the APN refers must be set in the PGW IP; for this case the real PGW has the IP address 22.0.0.1.

Select the User Equipment element and, in the Access Points tab, set the APN name and the PGW IP.

Note: The PGW IP address can be resolved by DNS query if the option Resolve DNS is enabled in the MME DNS tab; in that case there is no need to fill the PGW IP field.

![Figure 83. User Equipment Settings](image)
Create the Network Traffic for emulated P-CSCF

6. Add a Net Traffic on the Terminate side

Click Terminate in the Navigation Pane or in the Terminate column in the Networks and Traffic pane; then click the Add Net Traffic button in the Toolbar, or right click and select Add Net Traffic

Figure 84. Add Net Traffic by right click on the Network and Traffic pane

7. Set the IP address of the emulated P-CSCF

One P-CSCF server is emulated in this configuration. Set its IP Address to 22.22.22.1 and the Count to 1

Figure 85. Table 8. IP Address of the emualted P-CSCF
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

**Add the emulated P-CSCF**

8. Add the SIP Cloud activity

Move the mouse pointer over the Traffic element. A plus sign appears. Click on it and select the VoIPsIPCloud activity

![Figure 86. Add a SIP Cloud activity - this is the emulated P-CSCF](image)

9. Set the Distribution Group of the IP address range to IP Round Robin

The SIP Cloud requires that the distribution of the network ranges by port to be set to IP Round Robin.

Select the Traffic element in the Net Traffic, select the IP Mappings tab, double click the Distribution Group and select the IP Round Robin distribution type.

![Figure 87. Distribution Type of Network Ranges](image)

**Add and configure the SIP Peer activities**

In this moment, the configuration contains all the network elements. The next steps are to add the definition of the application traffic. The intention of this configuration is to emulate SIP UEs
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

on the eNodeB/MME side that originate calls routed by the emulated P-CSCF to emulated SIP endpoints placed behind the P-CSCF. This is emulated by adding a SIP activity to originate calls on the **MME/eNB S11/S1-u** network and a SIP activity to receive calls under the **SIP Cloud**.

10. Add a SIP peer activity on the Originate side

Move the mouse pointer over the Traffic element of the Originate network; a plus sign will be shown; click on it and select the VoIP/SIP Peer activity.

11. Add a SIP peer activity on the Terminate side.

Repeat the operation of adding a SIP peer activity on the terminate Net Traffic.
12. Use one of SIP Sample message flows as the call flows for VoIP SIP Peer1 and 2 activities. Drag and drop the lollipop of the VoIP SIP Peer1 over VoIP SIP Peer2. Select the SIP EP – Registration and Call with Voice message flow from the drop down list.

13. Set the parameters of VoIP SIP Peer1 activity.

   Select the VolPSIPPeer1 activity

   a. Set the Dial Plan

   In this example, we emulate 10 UEs with Phone Numbers 1001 to 1010. Click the Dial Plan tab and edit the sequence [1001-1010] in the Source / Phone Numbers field of the Dial Plan. Leave the Destination as the Symbolic Link to the Terminate VoIP activity; the phone numbers defined there are used in building the SIP Invite requests.
b. Set the SIP Server Address

The UE must know the IP address of the P-CSCF; it can be configured as an IP address or as a domain name in the SIP Tab. In this case, while the P-CSCF is the entry point to the IMS network, the IP address of the registrar server is the same. The P-CSCF knows how to route the registration and call setup requests. But for the UEs this is transparent; it sends all the SIP requests to the same P-CSCF.

Click the SIP Tab, and select Use External Server checkbox. Set the Server address and Domain name or local IP to the IP address of the P-CSCF (22.22.22.1 in this example) and select the Registrar server checkbox.

Figure 92. Set the SIP Server IP address
c. Set the Authentication credentials

In the practical deployments, the SIP requests for registration or call setup are authenticated by the server. The UE must use the proper credentials to have access to the service. Several authentication methods are defined for SIP, IxLoad supporting all of them. In this example, we use digest MD5, that requests each user to have a username and a password. We use the sequence user0001 to user0010 for the username and the same password 12345 for all users; it is possible also to use a sequence for the password also. In cases where the phone numbers, usernames or passwords of the emulated UEs are not in sequence, a phonebook can be used.

In the **SIP** tab edit the Username and Password fields.

![Figure 93. Authentication Credentials](image-url)
d. Set the Audio Codec to AMR-WB

VoLTE requires AMR codec for the speech communication. This is a multi-rate codec optimized for speech with capability to adapt to variations of network conditions. IxLoad supports both AMR-NB and WB versions.

Click the **Codecs** tab; in the table of audio codecs, select the first one, and choose AMR-WB codec from the drop down list. The user can change the order of preferred codecs. The SDP is automatically built with the parameters configured in this window.

![Figure 94. Set the AMR-WB as preferred codec](image-url)
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

e. Set the Audio parameters

To have media during an established SIP call, the call flow must contain a media function and that type of media to be enabled on the activity. The call flow contains the function Voice Session that plays and listen audio clips in the same type; it implements the full duplex audio functionality. In the Audio tab, enable the Audio Activity. In the same window, specify the duration of the voice session and implicit the duration of the call (assuming only voice session function is executed during the call).

Click the Audio tab, Select the Enable audio on this activity check box. Set the Play for to 30 seconds, and enable the Perform MOS checkbox.

![Figure 95. Audio Settings](image-url)
14. Set the parameters of VoIPSipCloud1 activity

Select the VoIPSipCloud1 activity

a. Map the SIP cloud activity to the IP address defined for the Terminate Network

In the **Settings** tab, select the IP address from the list. Only the Network Ranges with the Distribution Group Round Robin are shown.

![Map the SIP cloud to an IP address](image-url)

**Figure 96.** Map the SIP cloud to an IP address
b. Enable the Rx interface on the emulated P-CSCF

The P-CSCF and the PCRF are connected through the Rx interface – see image below. The interface confirms that call media requests conform to the appropriate policy, open gates and pinholes in the media route and specifies the appropriate QoS, requests per-flow charging information when needed, inform the P-CSCF of media-plane events. The Rx interface uses the Diameter protocol and can be emulated by the SIP Cloud module in IxLoad.

In the VoIPSIPCloud1 activity click the Diameter tab, and check the Enable Rx Interface check box.

![Diagram](image-url)

**Figure 97.** Enable the Rx interface for the emulated P-CSCF
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

c. Set the PCRF parameters

The P-CSCF must communicate with the PCRF. The IP address of the Hostname and the realm of the PCRF are parameters of the Diameter configuration window. In this example, the PCRF hostname is pcrf.test.com, and the realm is test.com (these are configuration parameters of the system under test).

![PCRF parameters](image)

Figure 98. PCRF parameters

Note: the PCRF implementations have variations in supported AVPs (Attribute Value Pair). To interoperate with a specific PCRF, use custom AVPs in the Diameter messages on Rx interface. This is possible in IxLoad by loading a file with the description of custom AVPs (the field User defined AVPs allows this).
d. Set the SIP Security parameters on the Server

The SIP Cloud acts as the P-CSCF; a real P-CSCF does the authentication of the SIP requests. The emulated P-CSCF can do the same functionality. In the **Security** tab, the user can define the type of requests for authentication, as well as the Authentication algorithm and the credentials for each UE.

Click the Security tab, select MD5 Authentication Algorithm and clear the AKA Authentication check boxes.

Click on **Security Profiles Pool** button. Create a new profile; and make sure you set the same values for the Phone Number, Username, and Password as for the emulated UEs (on the originate side).

![Figure 99. Security profile on the SIP Server](image-url)
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

15. Set the parameters of VoIPSipPeer2 activity

Select the VoIPSipPeer2 activity

a. Set the Dial Plan

In this example, we emulate 10 User Agents with Phone Numbers 2001 to 2010. Click the Dial Plan tab and edit the sequence [2001-2010] in the Source / Phone Numbers field of the Dial Plan. Leave the Destination as none; this activity is only receiving calls, so it does not need destination phone numbers.

![Figure 100. Dial Plan](image)

b. Enable this activity with the SIP Cloud

The VoIPSipPeer2 activity emulates SIP User Agents in the IMS core, behind the P-CSCF that is emulated by the SIP Cloud activity. It means that all the traffic between EPC and the IMS core goes through the P-CSCF (VoIPSipCloud1 activity) that receives the SIP Requests, and forwards them to the User Agents behind it.

Click the Cloud tab. Select the SIP Cloud simulation and Virtual IPs checkboxes, and a range of 10 Virtual IPs with the staring IP Address 23.23.23.1.
Figure 101. Associate a SIP Peer Activity with a SIP Cloud activity to emulate SIP User Agents behind a SIP Proxy

There is no need to set the SIP Server IP address or the Credentials for Authentication for this activity as it communicates internally to the emulated P-CSCF.
c. Set the Audio Codec to AMR-WB

Click the Codecs tab in the audio codecs table, select the first one, and choose AMR-WB codec from the drop-down list. The user can change the order of preferred codecs. The SDP is automatically built with the parameters configured in this window.

![Figure 102: Set the AMR-WB as preferred codec](image-url)
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

d. Set the Audio parameters

As on the originating side, the terminating side must have the Audio settings on to play and receive audio.

Click the Audio tab. Select the Enable audio on this activity checkbox. Set the Play for to 30 seconds, and select the Perform MOS checkbox.

Figure 103. Audio Settings

16. Set the Timeline and Objective

For the capacity test, a test objective type is set to Channels. The specified number of channels is concurrently active executing the call flow defined in the activities. Set the Objective Value to 10. If you want to increase the test objective, then:

- Increase the number of Maximum Active UE Count in the User Equipment plugin under Network1
- Extend the sequence of Phone Numbers in the VoIP SIP Peer1 dial plan
- Extend the sequence of User names for the VoIP SIP Peer1 Authentication
- Extend the sequence of Phone Numbers in the VoIP SIP Peer2 dial plan
- Increase the number of virtual IP Addresses for VoIP SIP Peer2 activity (under Cloud tab).
- Set the Sustain Time to 5 min.

17. Ports mapping

Map ports to the Traffic Networks. You need a pair of ports, connected to the EPC system (the DUT)
Running the test

18. Save the configuration

   Click Save in the Quick Access Tool Bar to save the configuration. Users can also save using the keyboard shortcut CTRL+s or through the menu, File > Save. To save for the first time, the system prompts you to enter a name for the rxf configuration and a name for the tst file. The .tst file contains the SIP call flow.

19. Run the test.

Result Analysis

The EPC, SIP, and RTP stats must be analyzed in this configuration.

![Figure 104. EPC Packet Rates](image)

The Packet Rate increases when new calls are established, but majorities of packets are RTP.
The number of Attempted / Connected calls (on the Originating side) and the number of Received / Answered calls (on the Terminating side) must be equal in a successful test. Any difference means the calls fail; and the reasons for failure are available in the Event Viewer.

Quality of voice is the final goal of this test. Even the calls can be established, it is important to measure quality of experience for the voice service. In this case, the measure MOS is as expected (for AMR-WB codec mode 0, the expected MOS is 3.82).

Troubleshooting and Diagnostics

When issues are present, a deep down analysis can be done using various features provided by IxLoad:
VoLTE Test Case: Measuring Quality of Experience for Voice Calls in LTE

- Stats drilldown per activity / port
- Event viewer for SIP, SDP, and RTP related issues. When an error occurs on VoIP, an error is logged in the Even Viewer window indicating the endpoint ID. The error type and description, and hints to resolve the error.
- Analyzer and Traffic Packet Viewer: User can enable traffic capture per port. To save memory, the RTP outbound packets are not captured. To minimize the size of the capture, apply filters using the tcpdump syntax.

**Test Variables**

**Table 9. Voice QoE Test Variables**

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Current Value</th>
<th>Additional Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Version</td>
<td>IPv4</td>
<td>IPv6</td>
</tr>
<tr>
<td>Concurrent Calls</td>
<td>10</td>
<td>Users can emulate up to 8,000 concurrent active endpoints in calls with audio streams by a single 1G port of an Xcellon-Ultra-NP card. To increase the number of channels, you have to allocate enough resources in terms of IP Addresses and Phone Numbers/User Names (see section 16 Set the Timeline and Objective)</td>
</tr>
</tbody>
</table>
| Test Objective | Channels      | The configuration is created for capacity testing. Other test objectives are available: for testing the rate of call setup supported by the access network, the CPS test objective can be used. Besides the value of Call Per Second Rate, you have to specify the number of emulated endpoints or the call duration (the talk time). These three parameters are correlated: 

\[
CPS = \frac{\text{Number of Endpoints}}{\text{Call Duration}}
\]

where

\[
\text{Call Duration} = \text{Talk Time} + \text{Call Setup Time} + \text{Overhead Time}
\]

To increase the CPS, use more endpoints or reduce the Talk Time. |
Wi-Fi Offload Test Case: Testing WAG/Wi-Fi Gateway in Isolation

Overview

The need to offload the data traffic for the mobile phones through the Wi-Fi network is the main drive for the Internet Service Providers who want to send as little traffic as possible through the 3G/4G devices.

This test case describes the methodology of testing in isolation a Trusted Wi-Fi Access Gateway (also known as WAG or TWAG), being surrounded by Ixia equipment which emulates access and core sides.

<table>
<thead>
<tr>
<th>DXIA</th>
<th>SUT</th>
<th>DXIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE</td>
<td>WiFi AP</td>
<td>CAPWAP</td>
</tr>
<tr>
<td>AP Controller</td>
<td>EAP-SIM</td>
<td>EAP-AKA</td>
</tr>
<tr>
<td>WiFi Offload Gateway (WAG)</td>
<td>AAA</td>
<td>S2a PGW (GTPv2 based)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Radius</td>
<td>GTPv2</td>
<td>GTPv2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GGSN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Services</td>
</tr>
</tbody>
</table>

Objective

This is a system test case that has a dual objective of simultaneously generating high throughput user plane data combined with a medium rate of constant handovers. The test simulates 120,000 active UEs on the access side authenticating with RADIUS EAP-SIM, using DHCP to obtain the IP addressess and running L4/7 traffic once user plane is established. S2a PGW (GTPv2 based) is being simulated on the core side. The WAG also acts as a RADIUS proxy, so the test setup needs an AAA Server – this one is a FreeRadius server configured on a Linux computer.

The rates performed by the test are as follows:

- 1200 RADIUS authentications per second
• 1200 DHCP transactions per second
• 1200 GTPv2 session establishments per second on the PGW

Setup
The test case is setup with 12 Access Points, each having associated 10,000 subscribers (UEs), each UE generating high throughput HTTP traffic.

Multiple configuration parameters depend on the network under test, such as IP addresses for the WiFi Access Gateway and RADIUS proxy, UE identifier parameters like Calling Station Id (MAC address). These are typically obtained by knowing the network configuration.

Step by Step Instructions
1. Insert a new NetTraffic on the server side. Select it to configure it, and delete the existing default IP stack by clicking Delete Stack.
2. Add the PGW S5/S8/S2a stack from the Add Stacks > Wireless menu.

![Figure 107. PGW S5/S8/S2a Stack](image)

3. Click the PGW layer to configure the PGW details. This layer contains two tabs that are configured as follows:
The PGW tab contains the following additional sub-tabs:

**Basic sub-tab:**
Click the green + icon at the bottom left of the pane to add an additional PGW range. This tab can be used to enable PGW load balancing on control plane and/or user plane.

**Timers sub-tab:**
These are the GTP protocol timers and counters set to the default values. No need to modify them.

4. Click the left IP layer in the PGW stack. This IP layer corresponds to the PGWs for the test. If load balancing is needed for the PGW, it can be configured using options in the CP-IP and UP-IP layers.
This layer is used to configure the IP address range for the PGWs. Configure a **Count of 12**. Configure the starting IP address, mask, and default gateway according to the system under test configurations.

5. Click the **PCRF** layer to configure the UE ranges. The **PCRF** layer contains four tabs configured as follows:

**Basic Tab**

The **Basic** tab contains the information that identifies the UE range: **Access Point Name**, **PDN Type**, **IMSI**, **UE Start IP**, **MSS**.
Configure a count of 120000 for the PCRF range in this test.
Click + icon at the bottom left of the pane if more PCRF ranges are needed.

**Dedicated Bearers Tab**

The **Dedicated Bearers** tab is used for configuring network initiated dedicated bearers for the S2a stack.

By clicking **Dedicated Bearers** field, a pop-up window appears for configuring the dedicated bearer parameters. Not used in this test.
Wi-Fi Offload Test Case: Testing WAG (Wi-Fi Access Gateway) in Isolation

**Default Bearer QoS/APN AMBR and Timeline tabs:**
Leave default values for these tabs.

6. Add a HTTP server activity to the NetTraffic. Leave the default settings.

7. Insert a new NetTraffic on the client side. Select it to configure it, and delete the existing default IP stack by clicking Delete Stack.

8. Add the Trusted WiFi Client stack from the Add Stacks > Wireless menu.

9. Click the **WiFi Access Point** layer to configure the APs.
Wi-Fi Offload Test Case: Testing WAG (Wi-Fi Access Gateway) in Isolation

Figure 114. WiFi Access Point Layer

Test scenario uses an EoGRE encapsulation without a GRE key between the Access Point and the WiFi Gateway for DHCP and traffic.

Set the TWAN IP to the IP address of the Wi-Fi Access Gateway.

10. Click the IP layer in the Trusted WiFi stack. This IP layer corresponds to the APs to be used in the test.

Figure 115. Access Point IP Layer

In this layer, the user can configure the IP address range for the Access Point ranges. For this test, configure a Count of 12 for the Access Point range. Configure the starting IP address, mask, and gateway according to the network under test configuration.
11. Click the **User Equipment** layer to configure the UEs (subscribers) for the test. The User Equipment layer contains two tabs that are configured as follows:

**Mobile Subscribers Tab**

The Mobile subscribers tab contains the following additional sub-tabs:

- **Basic sub-tab:**
  
  Configure the **Subscriber Count** value to match the test variables section. Here you must also configure the **Calling Station Id (MAC)** for the UE range.

- **Authentication sub-tab:**

  ```plaintext
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  9012cf08f43f11060100000099b6c408,e4737ab7ca000000f43f1106b1120f08
  ```

**Figure 117. EAP File**

Configure the **Authentication Mode** to **EAP-SIM**. You must also load the file containing the OPc and K values for the subscribers, one line per subscriber, separated by a comma.
**DHCP sub-tab:**

Users can configure to accept DHCP offers only from a specific DHCP server. Keep the default settings for these tabs.

**Network Group Settings Tab**

![Network Group Settings tab](image)

**Network Group Settings**

- **Setup and Teardown Rate**
  - Override Global Rate Settings
  - Setup Rate
  - Teardown Rate
  - Max Outstanding

- **Protocol Settings**
  - Global Timeout
  - 3GPP-GGSN-MCC-MNC
  - Use software version in IMEISV
  - Software Version
  - Use separate control plane address
  - Accept Duplicate IPs

**Figure 118. Network Group Settings tab**

The **Network Group Settings** tab contains global options for this specific network group. Leave these options set to their default values.

12. Click the **Radius** extension to configure the Radius options for the test.
For the Radius extension, you must configure the IP addresses for the **Authentication Server** and **Accounting Server**. Also, configure the **Authentication Port** and **Accounting Port** for the servers.

**Shared Secret** must match the value configured in Device Under Test.

13. Click **Settings** for the network plugin. In the **Interface Behavior** section click **Create interface with user**, and select the **Teardown interface with user** check box. This enables dynamic control plane mode.

14. Add an **HTTP client** activity to the NetTraffic. Configure it to have the previously configured **HTTP server** as a target. Configure one command in the command list: **GET** the **1024k.html** file.
15. Click the **Commands** tab of the **HTTP activity**, and select the **APN** command. Make sure that the **Use Dedicated Bearer** checkbox is cleared. This action causes the http activity to run on the default bearer for each UE.

![APN command](image)

**Figure 122.** APN command

16. In the **Timelines and Objectives** section, select a **Simulated Users** objective for the HTTP activity on the client network, and configure an objective value of **120000**. Configure a **60-minute timeline** duration, with a ramp up value of **1200 users/second**.

17. In the **Port Assignments** section, assign the client NetTraffic to the 12 port CPUs of the first Acceleron-NP card.

18. Assign the server NetTraffic to the 12 port CPUs of the second Acceleron-NP load module.

19. Enable 10G aggregation mode for both Acceleron-NP load modules.

20. In the **Test Options** section, select the Network Diagnostics check box to enable the Radius and DHCP statistics.
Test Variables

Table 10. Test Variables for WiFi Test

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE Count</td>
<td>120K</td>
<td></td>
</tr>
<tr>
<td>AP count for client network</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>Objective for HTTP activity</td>
<td>SU = 120K</td>
<td></td>
</tr>
<tr>
<td>TPS for Radius EAP/SIM Authentications</td>
<td>1200</td>
<td></td>
</tr>
<tr>
<td>TPS for DHCP Transactions</td>
<td>1200</td>
<td></td>
</tr>
<tr>
<td>TPS for S2a PGW</td>
<td>1200</td>
<td></td>
</tr>
</tbody>
</table>

Results Analysis

Validate the results from DHCPv4 and RADIUS views. Following messages must match: the DHCP Discovers/Offers/Requests/Acks/Nacks and the Radius Access Request/Challenge/Accept/Reject messages.
EPC Test Case: Single Radio Voice Call Continuity (SRVCC) with IR94

Overview

This use case simulates the Single Radio Voice Call Continuity (SRVCC) procedure while in a call with both audio and video sessions active. The test has 100 subscribers attaching in 4G and initiating a VoLTE call with audio and video (IR94). After a configured amount of time, the subscribers will initiate a SRVCC procedure to handoff the session from 4G to 3G, while maintaining the active sessions. The SRVCC handover is anchored in the IMS core network, and the circuit-packet function in the IMS core performs the necessary inter-working functions. The CS part is not visible in this scenario. Figure 124 below shows a high level overview of the SRVCC procedure.

Objective

The IR94 SRVCC test case has the objective of generating audio and video RTP traffic while testing the conformance of the Single Radio Voice Call Continuity procedure for both IR92 and IR94 scenarios in the SGW and the IMS Core.

Setup

The test is set up as follows:

One eNB, one MME, one SGSN, and one RNC with 100 subscribers, attaching in 4G to the eNB and initiating a VoLTE Call that also has video enabled. After a preconfigured time interval, the UEs will initiate a SRVCC procedure to continue the calls in 3G.

Figure 123. Overall high level concepts for vSRVCC from E-UTRAN to UTRAN
After a SRVCC procedure, if the UE is performing handover back from 3G to 4G, the audio and video dedicated bearers will be re-created at the start of a new voice loop while the RTP traffic is sent on the default bearer until then.

Multiple configuration parameters depend on the network under test, such as IP addresses for the MMEs and UEs, UE identifier parameters like IMSI and MSISDN, and networking parameters. These are typically obtained by knowing the network configuration.

**Step by Step instructions**

1. Insert a **new NetTraffic** on the **Terminate side**. Configure it to have a range of **1 IP** by using an IP addresses that correspond to the network under test settings. This NetTraffic will be used to simulate the SGi interface and the Landline users.

2. Add a VoIPSiP activity to the NetTraffic. Use the default settings.

3. Insert a new **Subscriber** on the **Originate side**. While having the Originate side selected, click on **Add NetTraffic** and select **Subscriber**.
Figure 125. Adding a Subscriber

Select to configure it, and delete the existing default IP stack by clicking Delete Stack.

4. Add a VolPSip activity to this NetTraffic. Drag from the activity blue lollipop and drop it on the Server side VoIP activity. A window with sample message flows should appear.

Select the Basic Call with Multimedia sample.

Figure 126. Sample message Flows

This adds a scenario to the Voice activity that contains both audio and video calls setup and RTP functions. Click on the VolPSipPeer activity to see or modify the scenario in Scenario Editor.
5. Select the Subscriber on the Originate side and add the SGSN/RNC S4/S12 + eNB/MME S11/S1-u stack from the Add Stacks > Wireless menu.

6. Click the SGSN layer to configure the SGSNs for the test.
7. Click the **IP layer** in the SGSN stack. This IP layer corresponds to the simulated SGSNs for the test. Use an IP address that corresponds to the network under test settings.

### SGSN IP Configuration

In this layer, user can configure the IP address range for the SGSN ranges. Configure the IP for the SGSN and configure the count to at least 1 (SGSNs).

8. Click the MME layer to configure the MMEs for the test.
Configure the SGW IP of the SGW that will be connected to the simulated MMEs (using the S11 interface).

9. Click the IP layer in the MME stack. This IP layer corresponds to the MMEs for the test.

In this layer, the user can configure the IP address range for the MME ranges. Configure the IP for the MME and configure the count to at least 1 (MMEs).

10. Click the User Equipment layer. This layer has two tabs.
Set the Maximum Active UE Count to 100. Select eNB-R1 as the Parent Range for this UE. By doing this, the UE will attach in 4G.

**Mobility tab:**

The user can configure the mobility path that will be followed by the UEs when doing Handover events. Enable the Mobility Path by clicking on **Enable Mobility**. Do not configure the Mobility Interval as this parameter will be ignored in subscriber tests with active commands. The time between mobilities will be adjusted by controlling the Think intervals between eGTP Commands in the eGTP Control Plane Command List.

Click on **Mobility Path** to make the (...) button visible. Click to configure the mobility path.
Click on the + sign to add a new node in the path and from the drop down menu select the BSC/RNC-R1 node. By doing this you will configure a handover from the source node of the UE (that is ENB-R1), to the BSC/RNC-R1 node.

11. Click the **Access Points** tab in the User Equipment layer to configure the IMS APN.

Configure the APN name that will be used by the VoIP activity, IP type for this APN and PGW IP.
The **IMS APN** checkbox needs to be checked to mark the APN as an IMS APN and to enable the SRVCC behavior in case of handover from 4G to 3G.

12. Click on **Subscriber1** and configure the **Egtp Control Plane Network Commands** as seen below. Configure all the **Think** command to 2000ms. By varying the Think commands duration user can control the time between procedures.

![Egtp Control Plane command list](image)

**Figure 137.** Egtp Control Plane command list

13. Synchronize the VoIPSipPeer activity with the egtp Control Plane as follows:

   Drag and drop from the OK event in the SIP MakeCall procedure to the **Think** located after the Create Session command and from the OK and Error events in the SIP EndCall Initiate procedure to the last **Think** in the egtp Control Plane command list.

   This is needed to ensure that SIP MakeCall command is not executed until the session has been created, and that Delete Session command is not executed until the SIP EndCall Initiate command has completed the execution.
This configuration will simulate Subscribers attaching to the network, then executing a handover procedure and after some more time disconnecting from the network.

14. Click on Subscriber1 and then on the APN command.
Since this is a VoLTE test, the voice and video traffic needs to have dedicated resources allocated. For this we need to configure the voice and video traffic to use dedicated bearers.

Configure the VoIP traffic item to use the dedicated bearer by clicking on **Use Dedicated Bearers**.

Set the **Bearer Special Function** for the dedicated bearer to **Audio**.

Click on the + sign to add another bearer to the VoIPSip Activity. This will be the dedicated bearer used for video. Configure the **Bearer Special Function** for the second bearer to **Video**. Users can navigate between bearers using the drop down menu.

Use the default value for QCI and MBRU/MBRD/GBRU/GBRD and ensure that the Ignore TFT option is enabled. These default values are the recommended values specified by the technical specifications.

15. From the Scenario Editor, click on both multimedia blocks and disable **Overwrite playback activity settings**. By doing this, the multimedia block will receive the audio and video configurations from the configuration in the rxf.
16. Select the VoIP Activity on the Originate side. Go on the Audio tab and click on **Enable audio on this activity**. Select the **US_042_WB16.wav** clip from the list of predefined clips. Use default value for the rest of the parameters in this tab.

Repeat the same steps on the VoIP activity on the Terminate side.
17. Select the VoIP activity on the Originate side. Click on the **Codecs** tab. In the Audio Codecs sections, delete the default values by using the X button and add another new value using the + sign. From the dropdown menu select **AMR-WB** codec. Keep the default configuration for this codec. 

Repeat the same steps on the VoIP activity on the Terminate side.

18. Select the VoIP Activity on the Originate side. Go on the Audio tab and click on **Enable video on this activity**. Select the **Wireless_CBase_384_SingleNalUnit.mp4** clip from the list of predefined clips. Use default value for the rest of the parameters in this tab. 

Repeat the same steps on the VoIP activity on the Terminate side.
19. From **Timeline and Objectives**, set the Objective Type for the VoIPPeer activity to Subscribers and the Objective Value to 100. Set the **Ramp Up Value** and **Ramp Down Value** to 100, and **Sustain time** to at least 20 sec.

20. Click on **Analyzer** and enable the packet capture on both ports by enabling the **Control-Enable** corresponding to each port.
21. Click Settings for the network plugin. In the Interface Behavior section click Create interface with user and select the Teardown interface with user check box. This enables dynamic control plane mode.

![Analyzer configuration](image1)

![Settings Button](image2)

![Interface Behavior](image3)

**Test Variables**

<table>
<thead>
<tr>
<th>Variables</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>UE Count</td>
<td>100</td>
</tr>
<tr>
<td>Mobility interval</td>
<td>2 sec</td>
</tr>
<tr>
<td>Objective for VoIPSip Activity</td>
<td>Subscriber</td>
</tr>
</tbody>
</table>
Results Analysis

The statistics to watch are the handovers, because this is a handover focused test. The statistics are divided in two sections: **SGSN +MME S11** statistics that count events triggered while the UE is attached in 4G and **SGSN S4** statistics that count events triggered while in 3G.

The handover statistics are counted at the destination of the handover, so, for a Handover from 4G to 3G, the handover will be counted in the **SGSN S4 – Handover** view.

1. First we need to verify that the eGTP session has been successfully created. To do this, check the **SGSN+MME S11 – General** statistics view and check if all the users are successfully attached.

![Figure 1. SGSN + MME S11 – General view](image)

2. After 2 seconds from the start of the test, when the Handover command is executed, check the **SGSN S4 – Handover** view, in the Handover from E-UTRAN tab to see if the handover has been executed successfully.

![Figure 148. 3G to 4G statistics view](image)

3. Check the **Calls (VoIP/Sip)** statistic to verify that all the calls have been set up correctly.
4. Check the Event Viewer log to see that there were no errors reported during the test run.

5. Check the Errors (VolPSip) statistics view to verify that there are no SIP errors.

6. Save the packet capture from Analyzer and open it in Wireshark. Apply the following filter to the packet capture to filter out the GTPv2 control plane packets for the first UE:

   gtpv2.f_teid_gre_key == 0x00325ac1 ||(gtpv2.teid == 1) ||( gtpv2.teid == 3300033)
The figure below shows the complete call flow of the Single Radio Voice Call Continuity (SRVCC) procedure. Please note that in our configured scenario, only the S4/S11 and S12/S1-U interfaces are exposed and only messages on these interfaces will be visible in the packet capture.
Figure 151. SRVCC call flow
The following messages are part of the GTPv2 control plane signaling related to the SRVCC procedure.

<table>
<thead>
<tr>
<th>17694</th>
<th>2.056537</th>
<th>::10.170.0.1</th>
<th>::10.10.2.89</th>
<th>GTPv2</th>
<th>88 Delete Bearer Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>17698</td>
<td>2.057315</td>
<td>::10.10.2.89</td>
<td>::10.170.0.1</td>
<td>GTPv2</td>
<td>79 Delete Bearer Request</td>
</tr>
<tr>
<td>17702</td>
<td>2.057938</td>
<td>::10.170.0.1</td>
<td>::10.10.2.89</td>
<td>GTPv2</td>
<td>95 Delete Bearer Response</td>
</tr>
<tr>
<td>17703</td>
<td>2.081231</td>
<td>::10.10.2.89</td>
<td>::10.10.2.89</td>
<td>GTPv2</td>
<td>149 Modify Bearer Request</td>
</tr>
<tr>
<td>17807</td>
<td>2.082814</td>
<td>::10.10.2.89</td>
<td>::10.10.0.2</td>
<td>GTPv2</td>
<td>83 Delete Bearer Command</td>
</tr>
<tr>
<td>18400</td>
<td>2.118791</td>
<td>::10.10.2.89</td>
<td>::10.10.0.2</td>
<td>GTPv2</td>
<td>79 Delete Bearer Request</td>
</tr>
<tr>
<td>18403</td>
<td>2.119280</td>
<td>::10.10.0.2</td>
<td>::10.10.2.89</td>
<td>GTPv2</td>
<td>95 Delete Bearer Response</td>
</tr>
</tbody>
</table>

![Figure 152. Signaling for the SRVCC IR94 procedure](image)

After moving the audio and video on CS, the voice bearer is deleted and all other bearers are moved from 3G to 4G (if PS support is available). The SIP part of the voice activity is continued until the end of the activity command list. This is done to ensure proper closing of the current call.

Single Radio Voice Call Continuity (SRVCC) provides continuity for a VoIP/IMS call when that call moves from the LTE packet domain to a legacy circuit domain (GSM/UMTS or CDMA 1x).

The Delete Bearer Command for the voice bearer is marked with Bearer Flag - VB (Voice Bearer).
Figure 153. The Voice Bearer is deleted before moving the session

After the session is moved from the eNB to the SGSN the video bearer is also deactivated.
EPC Diameter Test Case: S6a Procedures for Attach and AVP Modification

Overview

The S6a interface enables the transfer of subscriber related data (subscription and authentication) between the MME and the HSS as described in the 3GPP TS 23.401 for authenticating/authorizing user access to the evolved system.

The S6 application implements the following 3GPP procedures:

- Update Location
- Cancel Location
- Purge UE
- Insert Subscriber Data
- Delete Subscriber Data
- Authentication Information Retrieval
- Reset
- Notification

Figure 154. S6a interface: Server (HSS) and Client (MME)

Objective

This test case provides step-by-step instructions on how to use the S6a MME and HSS simulations.

The objectives of the lab are:

- To introduce the IxLoad Diameter configuration editor and current feature support
- To configure the test for specific scenarios and call flows: S6a MME – HSS with AIR/AIA, ULR/ULA messages
- To configure IxLoad to perform specific AVP manipulation
- To understand statistics and packet capture
EPC Diameter Test Case: S6a Procedures for Attach and AVP Modification

**Setup**

The test will be executed in back2back configuration using two separate plugins for MME and HSS S6a.

Two 10G ports from XT80 appliance will be used for the test.

![Diagram showing 2 x 10G ports connecting S6a MME and S6a HSS](image)

The test will use one subscriber and the following message flow: AIR/AIA, ULR/ULA

![Diagram showing message flow: AIR/AIA, ULR/ULA](image)

Test goal is to have one subscriber executing the above message flow. The reason the message flow is important is because it is part of Attach procedure.
Step by Step instructions

1. Start IxLoad. From the File Menu create a new Diameter scenario by using the built-in templates provided with the IxLoad installation. Load one template as shown below.

![Figure 156. Selecting S6a RXF from Templates section](image)

2. Select the S6a config shown below:

3. Go to the S6a MME simulation
4. The IP of the MME node and gateway information can be changed from the IP Layer as shown below. For our test we’ll use the default values:

![Figure 157. Configuring MME IP address](image)

5. To change the destination IP (the IP of the HSS to which the MME is connecting to) you have to select the MME S6a layer -> Diameter connection. This will open a pop-up window where the destination IP can be configured.
6. To configure the node details, go to MME Layer -> Network Group Settings and open the advanced GUI editor. Another window will pop-up.

7. Under the configuration pane, scroll down to the Subscriber database. Here, users can configure the subscriber count and define identification info relevant for their test. In our test we will use one subscriber and the default IMSI value.
8. Next step is to define the subscriber behavior. Go to the commands tab. In this template users will find some predefined commands. **Delete all** except the first one and we will edit that first one to match our intended message flow.

9. Select the first command (and the only one left) and click the “Edit” button. This will open the command editor window.
10. We will configure the test to run for one cycle, only for the one subscriber we have defined and execute “attach” procedures at a rate of 1 TPS. Important to mention here is that users can define an infinite number of cycles by setting “Cycles” value to “-1”. This will have the test running until manually stopped or until the Timeline set at step 15 ends. But we will use one cycle for our test.

11. Once done with editing the command click the **Update Command** button to complete command editing and then the **Save** button to save the advanced configuration. Now you can close the advanced GUI and return to the main IxLoad GUI.

12. At this point we can move to the HSS configuration. Users can repeat the steps similar to steps 3 thru 5 to configure IP connectivity for the HSS.

   Also, you will launch the advanced GUI editor for the HSS similar to how you did it in step 6. For this test we can use the default values from the template. Users will have to make sure subscriber information is the same on both ends.

   **Note: HSS simulation will reply by default to MME requests**, so there is no need to configure any command or state machine, we only need to start the node.

13. Next step is to configure test duration:
14. Assign ports to the MME and HSS Network (from XT80 appliance or from VirtualMachine):

![Assigning ports to Network](image)

**Figure 1. Assigning ports to Network**

15. Enable statistics in the rxf.
16. Enable capture on ports.

17. For XT80, the license server resides outside the appliance/port. So you have to configure and external license server.
18. Input here the IP of the license server (it can be localhost):

Results Analysis

Run the test and check the results:

- Rates per second for each procedure
- All procedures should be successful
- No errors should appear
- The capture should be as per the desired message flow
- Statistics should indicate the desired behavior.
Analyse the capture:

a. CER/CEA exchange for establishing the Diameter connection
b. Authentication Information Request for IMSI 10000000000001

Command Code: 318 3GPP-Authentication-Information
ApplicationId: 16777251
Hop-by-Hop Identifier: 0x24ca9bea
End-to-End Identifier: 0x0004f56b
[Answer In: 11]

- AVP: Session-Id(263) l=54 f=-M- val=test2.developingsolutions.com;324969;
- AVP: Origin-Host(264) l=37 f=-M- val=test2.developingsolutions.com
- AVP: Origin-Realm(296) l=31 f=-M- val=developingsolutions.com
- AVP: Destination-Realm(283) l=31 f=-M- val=developingsolutions.com
- AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
- AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
- AVP: User-Name(1) l=23 f=-M- val=1000000000000001
  AVP Code: 1 User-Name
- AVP Flags: 0x40
  AVP Length: 23

```
```

c. Authentication Information Answer for IMSI 10000000000001

Command Code: 318 3GPP-Authentication-Information
ApplicationId: 16777251
Hop-by-Hop Identifier: 0x24ca9bea
End-to-End Identifier: 0x0004f56b
[Response In: 101
[Response Time: 0.0001310000 seconds]

- AVP: Session-Id(263) l=54 f=-M- val=test2.developingsolutions.com;324969;702400879
- AVP: Origin-Host(264) l=37 f=-M- val=test1.developingsolutions.com
- AVP: Origin-Realm(296) l=31 f=-M- val=developingsolutions.com
- AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
- AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
- AVP: Result-Code(268) l=12 f=-M- val=DIAMETER_SUCCESS (2001)
  AVP Code: 268 Result-Code
- AVP Flags: 0x40
```
```

d. Update Location Answer
Objective: AVP Modification

Use cases:

- Positive testing:
  - Adding custom AVPs (optional, proprietary, vendor-specific signaling information, AVPs not present in the current specification version, etc.)
  - Modifying the AVP to contain a specific value or changing the position of the AVP as desired within the message
  - Removing unwanted AVPs from a specific message

- Negative testing:
  - Returning error codes in Answer messages
  - Introducing corrupt or invalid AVPs
  - Removing mandatory AVPs
  - Configuring more instances than allowed for a certain AVP
**SmartAVP™ Features:**

- AVP customization and substitution
- Create/modify/remove any AVP in any Diameter Application Message
- Configure an AVP from scratch
- Include vendor-specific or other optional AVPs in Diameter messages
- Insert multiple AVPs inside an AVP (nested AVPs)
- Define proprietary signaling or corrupt AVPs to facilitate negative testing
- Possibility of being compatible with any 3GPP spec version
- Simulate scenarios that are not as per specification to address some custom/specific scenarios (eq EUTRAN simulation with UTRAN parameters)
- Support for subscriber specific-data as AVPs data through the use of „transparent-data“ option e.g. IMSI, IMEI, MSISDN, public/private identity, IP address of the subscriber (IPv4 or IPv6).
- Inter-operability with any customer equipment
- Negative testing

**Step by Step instructions**

1. Use IxLoad configuration created above.

2. Look into capture and identify a DIAMETER_SUCCESS result code for ULA message

```
[Response Time: 0.000119000 seconds]
[Request Id: 13]
Command Code: 316 3GPP-Update-Location
ApplicationId: 16777251
Hop-by-Hop Identifier: 0x24ca9beb
End-to-End Identifier: 0x0004f56c
AVP: Session-Id(263) l=54 f=-M- val=test2.developingsolutions.com;324969;702400879
AVP: Origin-Host(264) l=37 f=-M- val=test1.developingsolutions.com
AVP: Origin-Realm(296) l=31 f=-M- val=developingsolutions.com
AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
AVP: Auth-Session-State(277) l=12 f=-M- val=NO_STATE_MAINTAINED (1)
AVP: Result-Code(268) l=12 f=-M- val=DIAMETER_SUCCESS (2001)
  AVP: 268 Result-Code
```

3. Go to the S6a HSS simulation and launch the Advanced GUI editor
4. Under the configuration pane, scroll down to the Subscriber database
5. Enable Smart Events State machine
6. Select “View/Configure” button on SmartEvents™ State Machine to open the editor and change the behavior
7. Add only one “Idle” state with one AVP configuration block inside it
8. Configure two SmartEvents™ instances that take effect on S6 interface on the Update event
9. Remove the current result code:
10. Add the new failure result code:

11. Update the Smart Events configuration

12. Save the Advanced configuration
Results Analysis

Run the test and check the following:

- ULA message should have a Result Code of 5002.
- The capture should be as per the desired message flow.

**Frame 6:** 30 bytes on wire (246 bytes), 30 bytes captured (246 bytes)
- Ethernet II, Src: 00:00:88:99:24:64, Dst: 00:00:00:00:00:24, Len: 247
- Internet Protocol Version 6, Src: 100:10:10:0.1, Dst: 00:00:00:00:00:24, Len: 247
  - Diameter Protocol
  - Version: 0x01
  - Length: 216
  - Flags: 0x80

**Frame 7:** 30 bytes on wire (246 bytes), 30 bytes captured (246 bytes)
- Ethernet II, Src: 00:00:00:00:00:24, Dst: 00:00:00:00:00:24, Len: 247
- Internet Protocol Version 6, Src: 100:10:10:0.1, Dst: 00:00:00:00:00:24, Len: 247
  - Diameter Protocol
  - Version: 0x01
  - Length: 216
  - Flags: 0x80

**Command Code:** 316 3GPP-Update-Location
- ApplicationId: 16777251
- Hop-by-Hop Identifier: 0x5e3ae055
- End-to-End Identifier: 0x0004e0c1

**[Request In: 25]**
- [Response Time: 0.000116000 seconds]
  - AVP: Session-Id(261) l=35 f=M- val=test1.developingsolutions.com;32495;1610101602
  - AVP: Origin-Host(264) l=37 f=M- val=test1.developingsolutions.com
  - AVP: Origin-Realm(296) l=31 f=M- val=developingsolutions.com
  - AVP: Vendor-Specific-Application-Id(260) l=32 f=M-
  - AVP: Auth-Session-State(277) l=12 f=M- val=NO_STATE_MAINTAINED (1)
  - AVP: UL-Flags(1406) l=16 f=VM- vnd=3GPP val=1
  - AVP: Subscription-Data(1408) l=408 f=VM- vnd=3GPP

**AVP: Result-Code(205) l=12 f=M- val=DIAMETER_UNKNOWN_SESSION_ID (5002)**
- AVP Flags: 0x00

Find us at www.keysight.com