ICT-318784 STP TROPIC

Distributed computing, storage and radio resource allocation over cooperative femtocells

D22

Design of network architecture for femto-cloud computing

Contractual Date of Delivery to the CEC:	**28th Feb 2013**
Actual Date of Delivery to the CEC:	**29th Mar 2013**
Author(s):	**Felicia Lobillo Vilela, Ana Juan Ferrer, Miguel Ángel Puente (ATOS), Zdenek Becvar, Matej Rohlik, Tomas Vanek and Pavel Mach (CTU), Olga Muñoz, Josep Vidal (UPC), Hadi Hariyanto, F.X. Ari Wibowo (TELK), Mariana Goldhamer (4GC), Enrico De Marinis, Fabrizio Gambetti (DUNE), Francesco Lo Presti (CINI)**
Participant(s):	**ATOS (Editor), CTU, UPC, SAP, DUNE, TELK, 4GC, CINI**
Workpackage:	**2**
Est. person months:	**8**
Security:	**R**
Dissemination Level:	**PU**
Version:	**a**
Total number of pages:	**96**

Abstract:

This deliverable intends to provide an analysis of the network architecture required for small-cell-cloud computing. The architectural framework considered in this document refers to LTE small cell architecture options outlined in the 3GPP standard.The individual elements for radio, cloud and backhaul are described and various possibilities are considered and compared in order to bring them all together for the operation of a small cell cluster to take place in an LTE environment, taking into account the differences between residential and corporate environments. The inter-cluster scenario, for greater computing capabilities, is also analysed. Finally, several solutions are provided for different problems encountered during the analysis, such as Over the Air Communication and distributed cluster management, among others. This document can be used as a recommendation for operators adopting the small-cell-cloud paradigm. The architectural choices are recommendations that telecom operators may study and evaluate according to their requirements and preferences.

Keyword list: Architecture,femto-cloud, Small Cell cloud computing, SCM, LTE.

Document Revision History

DATE	ISSUE	AUTHOR	SUMMARY OF MAIN CHANGES
29 Mar 2013	a	All	First version of D22
28 Jun 2013	b	All	• Distributed SCM included after patent registration (section 9.2.1). • Extended conclusions (section 10 and Annex 1) and IP addressing (Annex 2) • Review of sections 9.2 and 10

Executive Summary

The main challengefor running a cloud of small cells is to support both the radio and application levels. For this, several new features need to be introduced at the UE (offloading module, section 4.1.1) and at the SCeNBces (cloud-enabled HeNBs, section 4.2.2). The introduction of the SCM (Small Cell Cloud Manager) or FCM (Femto-cloud Manager) –section 4.2.4– completes the integration of radio and cloud. This new element needs to be introduced in the framework of LTE and a new protocol named Z-protocol –section 7– defines the operation of the cluster and ensures the service delivery.

The architectural framework considered in this document refers to LTE small cell architecture options outlined in the 3GPP standard [SCF01]. Since the definite architecture of LTE has several variants and is constantly evolving, various possibilities are considered in order to bring together SCeNBce, the SCM, the HeNB-GW (if it exists) so that the operation of a small cell cluster can take place in an LTE environment. For this, the TROPIC approach follows a simplified framework making general assumptions –section 2– such as considering that all SCeNBces belong to the same operator or that no handover to macro base stations will be done for the cloud application as the end-user goes away from the cluster radio domain.

The analysis of different architectural possibilities –section 5– leads to the conclusion that a telecom operator adopting small-cell-clouding has to consider different aspects before choosing an approach. The criteria for analysis include, among others, the current deployment of the own architecture on which the small-cell-cloud will be based, the approach as far as the applications it is willing to offer, energy-efficiency, the cost, the target users (residential, corporate), etc.A single deployment model will not suit all operators. Moreover, additional architectural possibilities can be introduced in case the operator intends to do small-cell-clouding among different clusters –section 6–.

The study carried out in this document leads to the following recommendations:

- In a residential scenario, the best approach is to place the SCM as an extension of the HeNB-GW.
- In corporate scenarios: the best possible approaches are 1) to place the SCM as an extension of the HeNB-GW or 2) to deploy an In-cloud standalone SCM (provided that the latency between SCM-SCeNBs is acceptable).
- In a public indoor scenario: the best possible approaches are 1) to place the SCM as an extension of the HeNB-GW, 2) to deploy an In-cloud standalone SCM (provided that the coordination latency between SCM-SCeNBs are concerned) or 3) SCM as an extension of MME (if microcells are considered).

Another important aspect TROPIC has covered is the analysis of the SCeNBce-SCM communication in case the latter is placed over the backhaul in a standalone mode, which requires additional security –section 8.1– and probably additional traffic offload using the Local IP Address feature –section 8.2–.

As for the concrete approach to follow in TROPIC, there are several implementation possibilities that need to be evaluated as work in technical workpackages (WP3, WP4, WP5)goes on. Basically, the possibilities include:

- A centralised approach in which the SCM is a new network element that manages the cluster. This is simpler to implement and it allows the operator a greater control of the applications that run over the cluster, however it implies higher delays and scalability problems.
- A distributed approach in which the SCM's features are carried out by the SCeNBces themselves. This seems challenging and its efficiency needs further study, since the dynamic scenario of small-cell-clouding requires the duplication of information across all SCeNBces within the cluster and increased signalling within the cluster.

Finally, as for the SCeNBce-SCeNBce communication, the use of the backhaul seems to be the simplest choice provided it can cope with the traffic requirements –section 9.1–. Alternatively, Over the Air communication can be used when SCeNBces belong to a small cluster and have visibility of one another.

Additional further studies have also arisen during the study of the architecture. Some of these are alternative solutions to cope with the traffic (alternative backhauls –section 9.1.1–) or to minimise delays in case the SCM needs to be placed on the core network (Hierarchical SCM and Virtual hierarchical SCM –sections 9.2.2 and 9.2.3–). TROPIC has also studied a totally distributed approach including both HeNB and low power eNBs with communication over the backhaul or over the air –section 9.2.1–.

DISCLAIMER

The work associated with this report has been carried out in accordance with the highest technical standards and the TROPIC partners have endeavoured to achieve the degree of accuracy and reliability appropriate to the work in question. However since the partners have no control over the use to which the information contained within the report is to be put by any other party, any other such party shall be deemed to have satisfied itself as to the suitability and reliability of the information in relation to any particular use, purpose or application.

Under no circumstances will any of the partners, their servants, employees or agents accept any liability whatsoever arising out of any error or inaccuracy contained in this report (or any further consolidation, summary, publication or dissemination of the information contained within this report) and/or the connected work and disclaim all liability for any loss, damage, expenses, claims or infringement of third party rights.

Table of Contents

References

[3GPP TR23.829] 3GPP TR 23.829 V10.0.1 (2011-10); Technical Specification Group Services and System Aspects; Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO) (Release 10)

[3GPP TR23.830] 3GPP TR 23.830 V9.0.0(2011-10); Technical Specification Group Services and System Aspects; Architecture aspects of Home NodeB and Home eNodeB (Release 9)

[3GPP TR36.932] 3GPP TR 36.932 V12.0.0 (2012-11); Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Scenarios and Requirements for Small Cell Enhancements for E-UTRA and E-UTRAN; (Release 12)

[3GPP TS22.220] 3GPP TS 22.220 V11.6.0 (2012-09); Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB) and Home eNode B (HeNB) (Release 11)

[3GPP TS23.002] 3GPP TS 23.002 V11.5.0 (Dec.2012) 3GPP; Technical Specification Group Services and System Aspects; Network architecture (Release 11)

[3GPP TS23.401] 3GPP TS 23.401 V11.4.0 (2012-12), "Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network - (E-UTRAN) access (Release 11)

[3GPP TS36.413] 3GPP TS 36.413 V11.2.1(20013-2); Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)

[3GPP TS36.420] 3GPP TS 36.420 V11.0.0 (2012-09); Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 general aspects and principles (Release 11)

[3GPP TS36.422] 3GPP TS 36.422 V11.0.0 (2012-09); Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); X2 signalling transport (Release 11)

[3GPP-TS36.300] 3GPP TS 36.300 V11.3.0 (2012-09); 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 11)

[adsl-rates] http://en.wikipedia.org/wiki/Asymmetric_digital_subscriber_line

[cisco-femto] http://www.techrepublic.com/blog/networking/solutionbase-does-the-cisco-self-defending-network-really-work/602

[Cisco-IPsec delay] Cisco, "Enterprise QoS Solution Reference Network Design Guide", Chapter 6, Version 3.3

[Cloud12] "Advances in Clouds. Research in Future Cloud Computing". European Commission. Lutz Schubert and Keith Jeffery.

[DMVPN4] http://www.cisco.com/en/US/docs/ios/security/configuration/guide/dmvpn_dt_spokes_b_nat.html

[DMVPN6] http://www.cisco.com/en/US/docs/ios-xml/ios/ipv6/configuration/15-2s/ip6-dmvpn.html

[Femtocells] Jie Zhang, Guillaume de la Roche, "Femtocells Technologies and Deployment", Wiley, 2010

[Fujitsu-LTE] http://www.fujitsu.com/global/services/telecom/product/femto.html#id2

[IETF01] http://tools.ietf.org/html/rfc5996

[Jeff09] "Server Virtualization Architecture and Implementation". Jeff Daniels. 2009.

[Kitz01] http://www.kitz.co.uk/adsl/interleaving.htm

[LTE Protocols] Mohammad T. Kawser, "LTE Air Interface Protocols", Artech House, 2011

[LTE Signaling] Ralf Kreher, Karsten Gaenger, "LTE signalling; Troubleshooting & Optimisation", Wiley,2011

[Nist01] The NIST definition of cloud computing (http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf)

[OF-stats] http://www.integer-research.com/2011/wire-cable/news/fiber-optic-cable-growth-continues-2012/

[Oguchi08] "Sever virtualization Technology and its Latest Trends", Y. Oguchi et al. (http://www.fujitsu.com/downloads/MAG/vol44-1/paper06.pdf)

[OpenNebula] http://opennebula.org/documentation:features

[Q-Femtos] Gavin Horn, "3GPP Femtocells: Architecture and Protocols", Qualcomm Inc., Sept. 2010

[RFC3947] http://tools.ietf.org/html/rfc3947

[RFC4187] http://tools.ietf.org/html/rfc4187

[RFC6296] http://tools.ietf.org/html/rfc6296

[RFC5448] http://tools.ietf.org/html/rfc5448

[SCF01] HeNB (LTE Femto) Network Architecture (http://smallcellforum.org/smallcellforum/resources-white-papers#HeNB)

[Sotomayor09] B. Sotomayor et al.,"Virtual Infrastructure Management in Private and Hybrid clouds"

[Spidercloud] http://www.spidercloud.com/service-node

[TROPICD21] Deliverable D21, "Scenarios and requirements", TROPIC project, www.ict-tropic.eu

[TS32593] http://www.3gpp.org/ftp/Specs/html-info/32593.htm

[TS33320] http://www.3gpp.org/ftp/Specs/html-info/33320.htm

[Wiki1] http://en.wikipedia.org/wiki/Asymmetric_digital_subscriber_line

[Wiki2] http://en.wikipedia.org/wiki/Very-high-bit-rate_digital_subscriber_line

[Xen] http://wiki.xen.org/wiki/Xen_Overview

List of abbreviations & symbols

AS	Access Stratum
BSC	Base Station Controller
CDMA	Code Division Multiple Access
CN	Core Network
CSG	Closed Subscriber Groups
DL	Down Link
E-UTRAN	Evolved Ultra Terrestrial Radio Access Network
ECM	EPS Connection Management
eNB	Evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
FAP	Femto Access Point
FCM	Femto-cloud Manager
GTP	GPRS Tunnelling Protocol
GUMMEI	Globally Unique Mobility Management Entity Identifier
HeMS	Home eNode B Management System
HeNB	Home enhanced Node B (Femtocell)
HeNBce	Home enhanced Node B cloud enabled
HSS	Home Subscriber Server
ICIC	Inter-cell Interference Coordination
IMS	IP Multimedia Subsystem
IP	Internet Protocol
L-GW	LIPA Gateway
LIPA	Local IP Access
LIPA	Local IP access
LTE	Long Term Evolution
MME	Mobility Management Entity
NAS	Non Access Stratum
NAT	Network Address Translation
PCRF	Policy and Charging Rules Function
PGW	PDN (Packet Data Network) Gateway
PLMN	Public Land Mobile Network
QCI	QoS Class Identifier
RNC	Radio Network Controller
S-GW	Serving Gateway
S1AP	S1 Application Part
SCeNB	Small Cell enhanced Node B
SCeNBce	Small Cell enhanced Node B cloud enabled
SCM	Small Cell Cloud Manager
SCM-BS	Small Cell Cloud Manager Base Station component
SCM-UE	Small Cell Cloud Manager User Equipment component
SCTP	Stream Control Transmission Protocol
SIPTO	Selected IP Traffic Offload
TA	Tracking Area

TAC	Tracking Area Code
TAI	Tracking Area Identifier
UE	User Equipment
UL	Up Link
UMTS	Universal Mobile Telecommunications System

1 INTRODUCTION

1.1 Introductory explanation of the deliverable

This deliverable intends to provide the description of the network architecture for small-cell-cloud computing. Although the name of this deliverable refers to a femto-cloud scenario, we mostly use the term small-cell-cloud for the sake of generality.

The architectural framework considered in this document refers to LTE small cell architecture options outlined in the 3GPP standard[SCF01]. Since the definite architecture of LTE has several variants and is constantly evolving, various possibilities are considered in order to bring together SCeNBce, the SCM, the HeNB-GW (if it exists) so that the operation of a small cell cluster can take place in an LTE environment.

In order to analyse architectural possibilities, we consider that the small-cell-cloud architecture has three main segments that can be studied in parallel and then assembled in a final architecture. These three elements are:

- Radio plane: This segment includes modifications in the small cells architecture (regardless of the cloud) derived from the enhancements that are going to be introduced in the scope of WP3 and WP5.
- Cloud plane: The introduction of new elements and components for storage and computing capabilities in the nodes and the SCM[1] that orchestrates the deployment and delivery of applications running in the small-cell-cloud.
- Backhaul:This segment also takes part in the overall functioning of the small-cell-cloud network, and although no modifications of this segment are introduced in the scope of TROPIC, it is important to consider how it can affect the overall operation.

These essential components need to be combined in a global architecture where the interaction between them is defined according to what information is available and from where it needs to be retrieved.

Several possibilities are studied and evaluated according to several criteria:

- Maximum coverage of requirements gathered in D21 [TROPICD21].
- Optimisation criteria such as, for example:
    - Signalling overhead introduced
    - Overall latency
    - Computation/storage potential performance
    - Computational capacity required in the SCM
    - Cost of deployment and maintenance
    - Implementation complexity
    - Minimal impact on legacy systems
    - Energy consumption

They also need to be compared taking into account different perspectives since the criteria listed above are not equally important to several stakeholders: end-users, manufacturers and operators.

The approach followed by TROPIC is to establish a simplified framework making general assumptions that allow analyse different architectural options, going from the situation in which only one cluster is considered to an environment in which several clusters can be combined.

[1]We use SCM (Small Cell Coud Manager) and FCM (Femto-cloud Manager) indistinctively along the document.

1.2 Structure of the document

Therest of this document is structured as follows:

- Section 2 establishes the general assumptions that allow a simplification of the framework in which the SCM is placed.
- Section 3 describes the 3GPP standard (release 11) in which the SCM operates.
- Section 4 lists and describes the specific components for each of the segments (radio, cloud, backhaul) that need tointeroperate.
- Section 5 presents some architectural options for the single-cluster scenario, including anevaluation and a comparison of all alternatives.
- Section 6 describes and evaluates options for the architecture in a multi-cluster scenario.
- Section 7 presents the Z-protocol from a high-level perspective, including the functional elements of the architecture and the information that needs to be exchanged between them.
- Section 8 analyses how the communication can be achieved between SCeNBces (cloud-enabled HeNB) and SCM when the SCM is a standalone component (not in the core network).
- Section 9further considerations and it includes possible solutions for problems encountered during the analysis.
- Section 10gathers conclusions and final recommendations as far as architecture is concerned.

2 GENERAL ASSUMPTIONS

The architecture options explained in this document have been studied under several assumptions that help establish a simplified framework that reduces the number of alternatives:

- The framework is 3GPP architecture, according to release 11.
- All SCeNBces in the architecture belong to the same operator.
- A user is only served by one SCeNBce at a time.
- Not all small cells are cloud-enabled, SCeNBces coexist with current small cell devices.
- The femto-cloud mobility from a small cell cluster to macro base stations is out of the scope of TROPIC. When a user leaves a small cell clusterneighbourhood while an application is running, there will be no means to provide the result back while he is away of the cloud coverage zone.
- Differences of deployment in the residential and corporates use case are not taken into account for the comparison of alternatives, although they are examined in section 3.1.2.

The architectural options always take into account these two main approaches:

  - Avoid functional duplicity by taking as much advantage as possible from LTE features (for example, for user authentication the HSS should be used by contacting the MME).
  - Avoid as much as possible the modification of existing interfaces. The SCM is a new component in the network and will interface with LTE legacy nodes through dedicated interfaces when required.

There are several aspects such as the service delivery model or the application and improvement to the radio architecture that have not been defined at the time the architecture is being approached. This is why the options presented in this document could evolve as project outcomes do. The architecture strongly depends on the SCM's functionality,which, in turn, is related to the application scope(since this determines, for example, what information is provided to the SCM at request time or, as another example, what source of data should be used for recovery in case of node failure[2]) and to the service model.For example, if the SCM follows a best effort approach there is no need to do resource reservation but, in case some SLA is guaranteed, the interaction with resources may change for reservation purposes prior to provision.

Finally, the architectural choices are recommendations that telecom operators may study and evaluate according to their own requirements and preferences.

[2] In case the cluster is used as a near storage system for internet content cache, the source for the original information will be the internet.

3 LTE ARCHITECTURE

The SCM must be placed in the framework of LTE architecture. The aim of this section is to provide an overview of LTE nodes, features and interfaces, including all variants. This will later be used to analyse the interactions between the SCMand the LTE network entities.

3.1 General LTE architecture

The general LTE architecture, based on [3GPP TS 36.300] and [Q-Femtos], is provided inFigure 1. The following entities and logical interfaces are included:

- **eNBs**, the LTE base stations, serving either macro cells or small cells; the eNBs are connected to the core network entities S-GW and MME through the S1 interface The eNBs are interconnected with each other by means of the X2 interface. The eNBs are also connected by means of the S1 interface to the EPC (Evolved Packet Core), more specifically to the MME by means of the S1-MME interface, carrying control messages, and to the S-GW by means of the S1-U interface, transporting the user data. The S1 interface supports a many-to-many relation between MMEs / Serving Gateways and eNBs. Based on LTE Release11, there is no connection via X2 between an eNB and a HeNB.
- **HeNBs**, LTE femto base stations, in the immediate user proximity; they can be installed by residential or business users on their premises; they are interconnected by the X2 interface but they cannot reach through this interface the eNBs connected through the operator backhaul. The HeNBs are similar with the eNBs but, in general, the HeNBs are deployed by the users and have an xDSL backhaul.
- **S-GW** (Serving Gateway), the Serving GW, part of the operator core network, serving as mobility anchor; the S-GW is controlled by the MME.
- **MME**(Mobility Management Entity), Mobility Management Entity, with main functionality related to the control of the transport and handover process over the S1 interface;
- **P-GW**, connecting the user traffic from the S-GW to the general packet data network (Internet) and IMS;
- **HeNB-GW**,deployed to allow the S1 interface between the HeNB and the EPC to support a large number of HeNBs in a scalable manner. The HeNB-GW serves as a concentrator for the C-Plane, specifically the S1-MME interface. The S1-U interface from the HeNB may be terminated at the HeNB-GW, or a direct logical U-Plane connection between HeNB and S-GW may be used.
- **HSS** (Home Subscriber Server) is the master database for a given user. It is the entity containing the subscription-related information to support the network entities actually handling calls/sessions [3GPP TS23.002].
- **CSG List Server** provisions the allowed CSG list and the Operator CSG list on the UE.

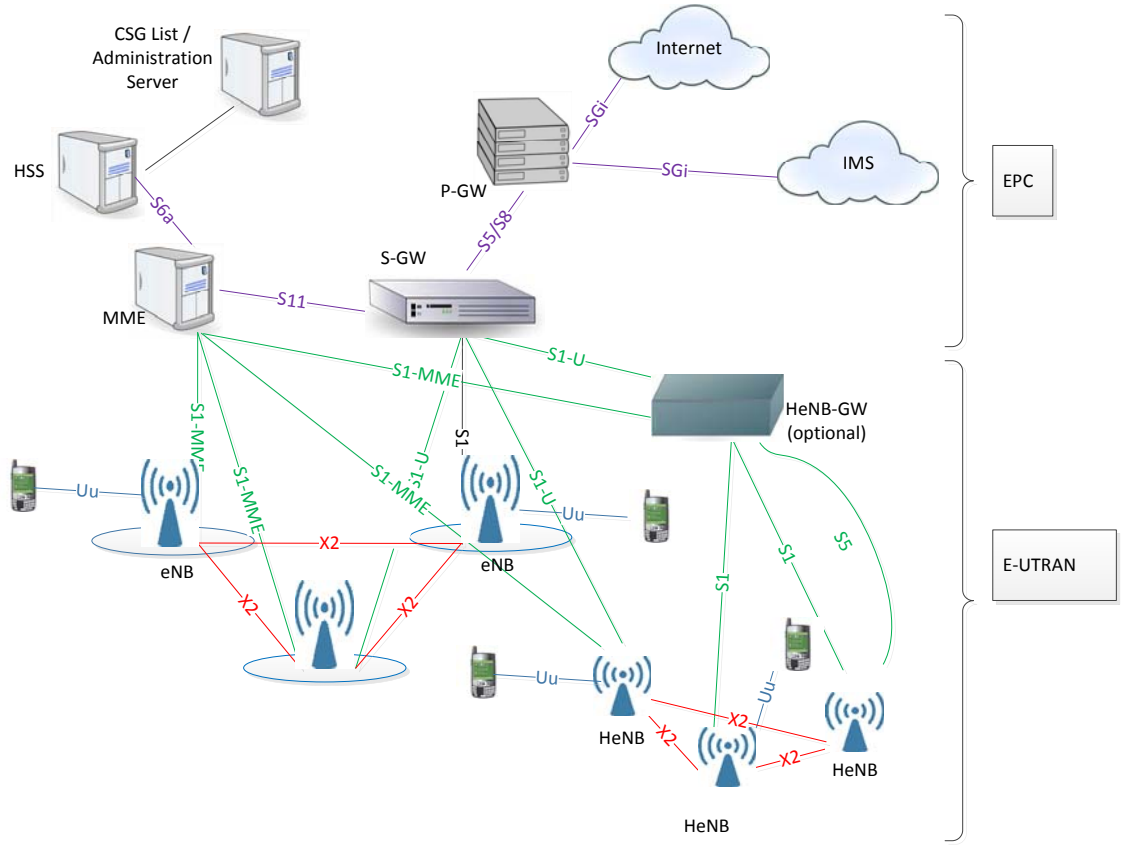


Figure 1. LTE overall architecture

3.1.1 Functionalities

A summary of the functionality of different network entities, based on [3GPP TS36.300] is provided below:

eNB

- Functions for Radio Resource Management: Radio Bearer Control, Radio Admission Control, Connection Mobility Control, Dynamic allocation of resources to UEs in both uplink and downlink (scheduling);
- IP header compression and encryption of user data stream;
- Selection of an MME at UE attachment when no routing to an MME can be determined from the information provided by the UE;
- Routing of User Plane data towards Serving Gateway;
- Scheduling and transmission of paging messages (originated from the MME) and of broadcast information (originated from the MME or O&M);
- Measurement and measurement reporting configuration for mobility and scheduling;
- CSG handling;
- Transport level packet marking in the uplink.

HeNB

A HeNB hosts the same functions as an eNB, with the following additional specifics in case of connection to the HeNB-GW:

- Discovery of a suitable Serving HeNB-GW;
- The HeNB will not simultaneously connect to another HeNB-GW or another MME.

- The TAC and PLMN ID used by the HeNB shall also be supported by the HeNB-GW;
- Selection of an MME at UE attachment is hosted by the HeNB-GW instead of the HeNB. Upon reception of the GUMMEI from a UE, the HeNB shall include it in the INITIAL UE MESSAGE; upon reception of the GUMMEI Type from the UE, the HeNB shall also include it in the message.
- HeNBs may be deployed without network planning. A HeNB may be moved from one geographical area to another and therefore it may need to connect to different HeNB-GWs depending on its location;
- Signalling the GUMMEI of the Source MME to the HeNB-GW in the S1 PATH SWITCH REQUEST message.
- Regardless of HeNB-GW connection:
- The HeNB may support the LIPA function.

HeNB-GW

The HeNB-GW hosts the following functions:

- Relaying UE-associated S1 application part messages between the MME serving the UE and the HeNB serving the UE.
- Terminating non-UE associated S1 application part procedures towards the HeNB and towards the MME. In case of S1 SETUP REQUEST message, verifying, as defined in TS33.320, that the identity used by the HeNB is valid.
- If a HeNB-GW is deployed, non-UE associated procedures shall be run between HeNBs and the HeNB-GW and between the HeNB-GW and the MME.
- Optionally terminating S1-U interface with the HeNB and with the S-GW.
- Supporting TAC and PLMN ID used by the HeNB.
- A list of CSG IDs may be included in the PAGING message. If included, the HeNB-GW may use the list of CSG IDs for paging optimization.

HeNBSubSystem

A HeNBSubSystem consists of the HeNB and, optionally, the HeNB Gateway belonging to it.

MME

- NAS signalling;
- NAS signalling security;
- AS Security control;
- Inter CN node signalling for mobility between 3GPP access networks;
- Idle mode UE Reachability (including control and execution of paging retransmission);
- Tracking Area list management (for UE in idle and active mode);
- PDN GW and Serving GW selection;
- Authentication;
- Bearer management functions including dedicated bearer establishment.
- Access control for UEs that are members of Closed Subscriber Groups (CSG):
- Membership Verification for UEs handing over to hybrid cells:
- CSG membership status signalling to the E-UTRAN in case of attachment/handover to hybrid cells and in case of the change of membership status when a UE is served by a CSG cell or a hybrid cell.
- In case of a HeNB directly connected, verifying that the identity used by the HeNB is valid,as defined in TS33.320.
- Routing of handover messages, MME configuration transfer messages and MME Direct Information Transfer messages towards HeNB-GWs based on the TAI contained in these messages.

- The MME may support the LIPA function with HeNB.

Serving Gateway (S-GW):

- The local Mobility Anchor point for inter-eNB handover;
- Lawful Interception;
- Packet routeing and forwarding;
- Transport level packet marking in the uplink and the downlink;
- Accounting on user and QCI granularity for inter-operator charging;
- UL and DL charging per UE, PDN, and QCI.

PDN Gateway (P-GW)

- Per-user based packet filtering (by e.g. deep packet inspection);
- Lawful Interception;
- UE IP address allocation;
- Transport level packet marking in the uplink and the downlink;
- UL and DL service level charging, gating and rate enforcement;
    - DL rate enforcement based on APN-AMBR.

Home Subscriber Server (HSS)

- Central database that contains user-related and subscription-related information
- Mobility management
- Session establishment support
- User authentication
- Access authorization
- Holds information about the PDNs to which the user can connect
- EPS-subscribed QoS profile
- Identity of the MME to which the user is currently attached or registered

The network architecture with HeNB-GW is presented inFigure 2. Some new elements can be observed:

- A Local GW inside the HeNB, connected to the MME via the S5 interface
- An optional security GW, for both user and control traffic;
- An optional HeNB-GW, intended for the S1-MME control traffic.

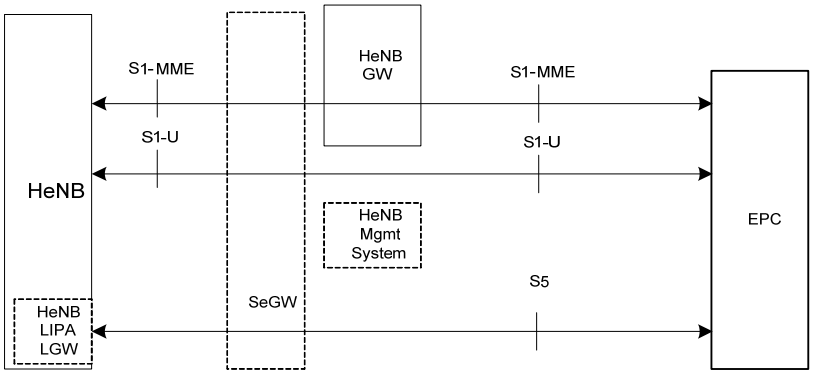


Figure 2. LTE network architecture with HeNB-GW

3.1.2 Residential / enterprise / public scenarios

We can differentiate three main deployment scenarios for LTE HeNBs with important differences between them: residential, public and corporate [TROPICD21]. These differences have to be taken into account in the definition of the reference architecture for TROPIC.

The big differences between the three are transmission power, user numbers, type of backhaul connectivity, and access mode (open, closed, or hybrid). Also, business small cells may have to serve as “de facto” private networks for the company and its customers.

The following picture and table [Fujitsu-LTE] depict an overview of the different areas considering the amount of users they have to deal with, and the openness or closeness of the accessing. The following table analyses the specifications for each area regarding indoor/outdoor coverage, close/open mode and coverage radius.

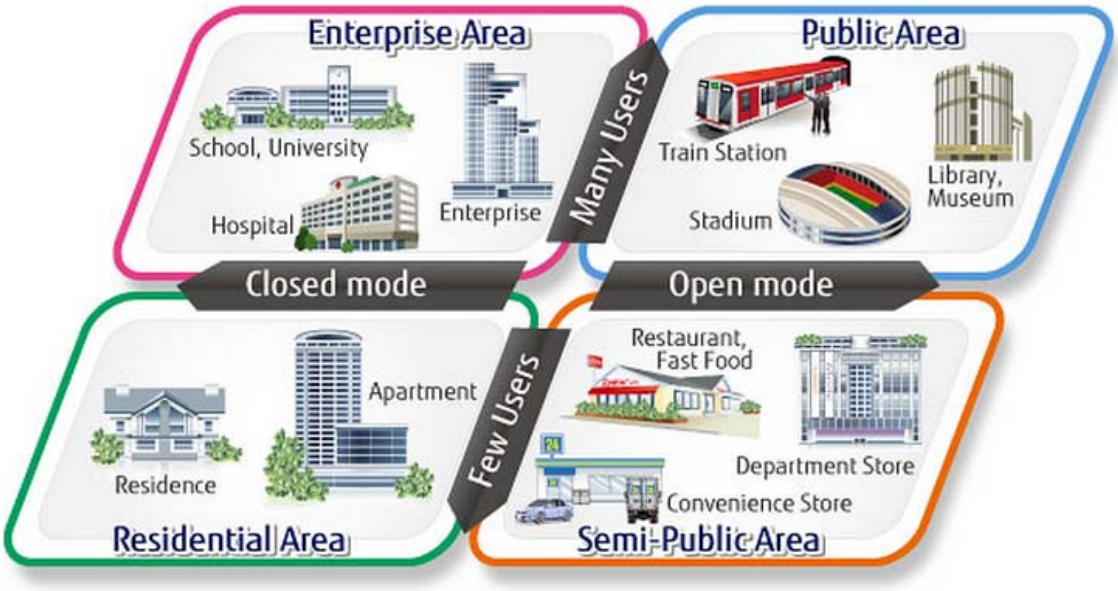


Figure 3. LTE HeNB target areas

Residential	Enterprise	Public	Semi-public
Indoor Close/open mode < 20 m	Indoor Close/open mode < 100 m	Indoor/Outdoor Open mode < 100 m	Indoor/Outdoor Open mode < 100 m

Table 1. LTE HeNB target specifications

In the following we present a brief description of the small cells’ characteristics for each scenario:

- **Residential**small cells generally cover one household with a radius of about 25 meters. Service providers or subscribers can furnish these plug-and-play devices. Digital subscriber line (xDSL) cable and a passive optical network (xPON) already installed in the house connect the devices to the core network. Operating mainly in closed and hybrid access modes, they support seamless mobility with the surrounding macro layer. Only user equipment (UE) within the closed subscriber group can camp on a small cell in closed access mode. Accommodating between 4 and 8 concurrent users, and perhaps up to 20 in connected mode, these small cells are managed by a system based on TR069 protocols, connected to the radio access network’s management system.

- **Enterprise** small cells must interwork to ensure service continuity and seamless handover, which may call for the X2 interface. It will probably take 'light' network planning to deploy these plug-and-play devices. The data transmission link currently in place connects these devices to the core network, but it may have to evolve for a better LTE user experience.
  Companies want simple, secure local services. Service providers want to keep huge loads of enterprise packet traffic off their core network. A local breakout for data traffic satisfies both demands. Accommodating between 32 and 64 concurrent users, enterprise small cells are managed by the service provider's enterprise management system, possibly with a TR069 system serving as the front end to small cells.
- **Public** small cells cover buildings such as airports, railway stations, shopping malls, and large plants, or outdoor hotspots. They need dedicated backhaul links, probably deployed by the service provider, and may accommodate hundreds of concurrent users, if necessary. The macro network's management system will most likely also manage the public small cell, often called a picocell.

3.1.2.1 Residential scenario

In the residential scenario, HeNBs are deployed at private homes, i.e. individual homes or different flats within the same building. This deployment is made under customer premises, so no one apart from the customers has the capability of influence in the deployment architecture. Costumers deploy HeNBs at their homes following a random pattern, which leads to random architecture and coverage areas. Besides, customers have the ability to switch on and off the HeNBs, choose different operators, allow the connection of just certain devices under their control, etc. All this increases the randomness of the scenario.

Regarding the architecture, we can assume that the deployment within each individual home is going to be the same. Typically each customer has an ADSL router at his home, to which all the customer's devices are attached via Wi-Fi or Ethernet (laptop, tablet, etc.). In this case the HeNB would be attached to the router, through its Ethernet interface, as just another device. Once the HeNB is deployed, it can provide LTE coverage to mobile devices. The following image, taken from the SmallCell Forum, illustrates the scenario in case of individual homes.

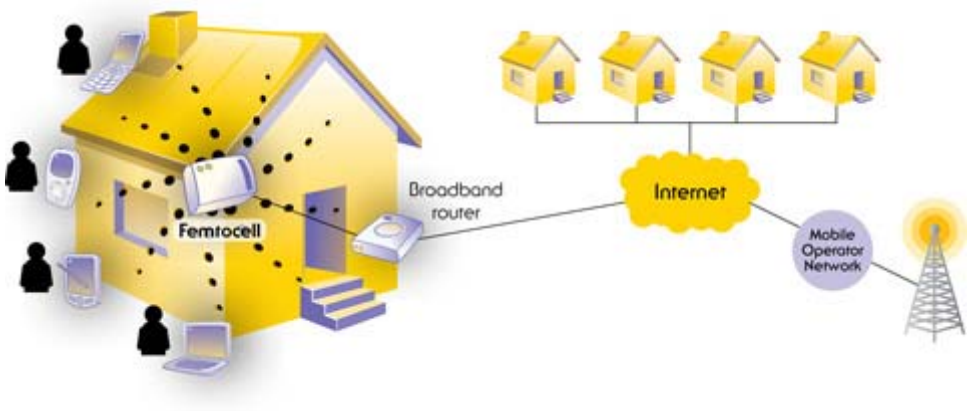


Figure 4. Residential HeNB scenario

In case the customers live in flats within the same building, the scenario is the same. Customers would have their own Internet connection (typically ADSL) with their own router. The main difference between both cases – individual homes and flats in the same building – is basically the distance among HeNBs. In individual homes deployment, the distance among HeNBs is greater than in the building case. That has several implications for TROPIC, as it is explained in the following subsection.

In the residential scenario, when working with IPv4, the home router performs Network Address Translation (NAT) functions. All domestic devices attached to the router share an internal IP address,

while externally they all are represented by the same external address, known as the public address of the router. This public address is assigned by the operator, and in most cases it's dynamic. That is, it changesover time. That implies that, unless the router has address mapping, an internal device cannot be contacted from outside the cluster. That involves several implications for TROPIC, as described in section3.1.2.5.

3.1.2.2 Corporate scenario

In a corporate scenario, HeNBs are deployed in an enterprise environment. We can understand this enterprise environment as the physical location of a certain business organization, such as an office building, industrial bay, or any other large facility used for the company's purposes. In this environment, all the HeNBs are deployed following a certain deployment plan and they are located in a restricted and well-identified location. As mentioned before, the main objective is to ensure service continuity and seamless handover, which implies a controlled HeNB deployment, facilitating HeNB interwork making use of the X2 interface.

Unlike the residential scenario, in the corporate case HeNBs cannot be switched on and off randomly. That would be up to the system manager, who is the one that has control of all the deployment. Moreover, in the corporate scenario it is not likely that HeNB belong to different operators.

Regarding the architecture, the HeNB deployment in a corporate scenario would make the most of the existing company's network architecture. The network architecture within a company's buildings is highly variable from one company to another, as each organization deploys networked resources based on its own needs, but we can make some assumptions that we can consider common architectural aspects in a company's network. The following picture, adapted from one from Cisco [cisco-femto], depicts a possible HeNB deployment scenario in a corporate environment.

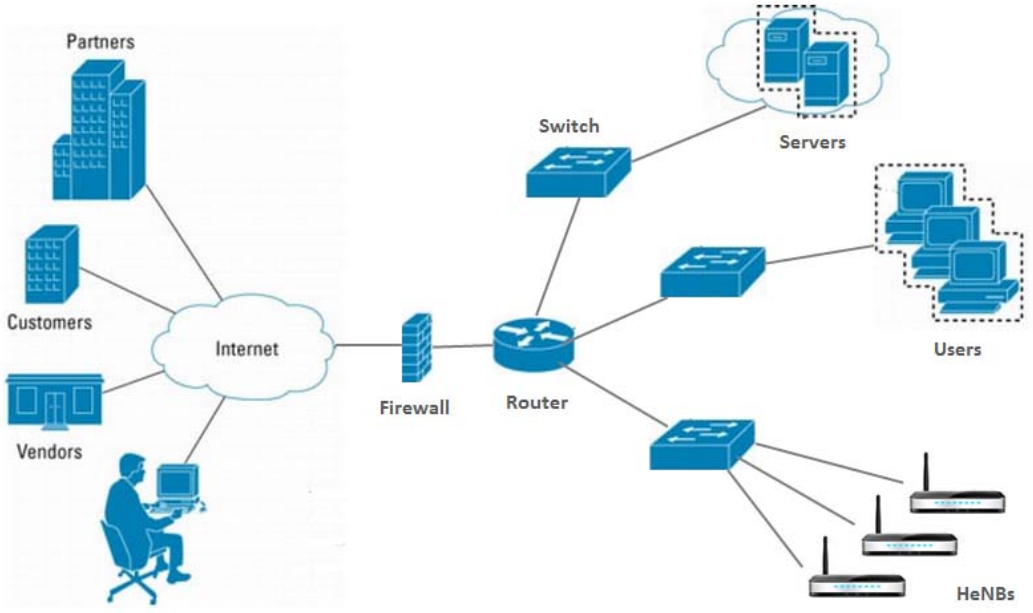


Figure 5. Corporate HeNB scenario.

We can assume that the network architecture has the following characteristics:

- Single access point from and to the Internet – that can be considered accurate for each building block or isolate location, as it is the easiest way to connect and aggregate traffic from the outside, and most of the network architectures are implemented in that way. In the

previous picture, the aggregating device is a router, but it could also be a gateway or any other routing device.

- Firewall at the entrance of the network – this is a security issue that is implemented in almost every enterprise network architecture.
- Hierarchical architecture – In a large network, devices are grouped by means of an aggregation layer (switches). Routers could be used instead of switches, but it is not the usual option to form a LAN network. A hub is another possible device to use in the aggregation layer.
- Devices grouped by functionality (or location) – In large companies, it is common to group similar devices under dedicated LANs. For example, dedicated switches aggregate employee's devices while other switches aggregate the servers. Devices can be aggregated depending on their location. For instance, we can have one aggregating switch per floor, set of rooms, etc.

Taking all this into account, companies can deploy HeNBs using their existing network infrastructure. The HeNB deployment depicted in the picture represents an aggregation layer, which groups devices of the same kind, so one switch aggregates the network infrastructure dedicated for the HeNBs. However, HeNBs could also be grouped by location.

Regarding the IP address allocation for HeNBs, telecom operators most commonly offer a dedicated public IP address for premium customer/enterprise whereas they allocate a dynamic public IP address for normal residential customers. Besides, NAT functions may be present at the entrance of the network, which implies some issues when connecting devices from outside the network to the inside. Those NAT problems can be avoided as long as address mapping exists, otherwise, the servers cannot be contacted from the outside.

In case we do not have NAT, for example, companies which use IPv6 and manage without NAT, we wouldnot have this kind of problems and inner devices could be contacted without problems.

All that has several implications for TROPIC, as explained in subsection 3.1.2.5.

Enterprise small cells have certain characteristics that make them significantly different from residential small cells. More specifically, inter-small-cell interactions play an important role in enterprise small cell deployment and pose new challenges compared to the residential case. The coverage area of an enterprise small cell is typically larger than that of a residential deployment. Moreover, in a large enterprise, RF variations can be much greater than those observed in a residential scenario. These large RF variations need to be taken into account in the deployment of enterprise small cells to ensure that the small cell provide sufficient coverage in the entire enterprise while limiting the interference to non-enterprise users. Further, the larger area per small cell coverage leads to lower path-loss differentials relative to the surrounding macrocells. This results in higher uplink interference to macrocell from an enterprise femto UE compared to that from a typical residential femto UE. In addition, the number of users served by an enterprise small cell can be large. As a consequence of these issues, femto-macro interference needs to be well managed for enterprise deployment, both on the downlink (DL) and on the uplink (UL).

From the point of view of mobile network operators, one the most lucrative markets is the business segment where call volumes and ARPU (Average Revenue per User) are considerably higher (many users may make international calls and/or travel abroad). They derive more than 30% of their revenue from business customers, and competition is fierce to sign up this attractive market segment.

There are a number of factors that need to be designed into a small cell enterprise solution targeted at the larger corporate premises.

- Seamless Mobility. A residential or small office small cell user may leave the building only two or three times a day, and is unlikely to be mid-call. Large offices, equipped with many

small cells, frequently have people walking around mid-call or mid-session. There are several issues with this:
    - Calls/Sessions need to be seamlessly transferred between the small cells and by default would be handled by the core network. This places a heavy load that could better be handled locally.
    - Frequent hard handovers require additional processing and transmissions with the mobile device, increasing battery consumption and reducing battery life.
    - There may also be a greater risk of call drops.
- Consistently high throughput. One issue with DAS systems is that they distributed a fixed amount of capacity around the building – improving coverage but not necessarily capacity. Each extra small cell provides substantial extra throughput, essential to meet the growing demand and avoid wide variations in data rates.
- Enterprise-Centred Management. An operator should be able to manage each enterprise small cell system as a single entity, rather than having to manage individual small cells. This reduces operational costs and allows the operator to offer and report on SLAs (Service Level Agreements) to its enterprise customers.
- Rapid deployment. The cost of an enterprise installation impact both parties – businesses can't afford periods of long or disruptive downtime, while the operator needs the cost to be low to remain viable and competitive. The system should be smart enough not to require specialist technical planning or deployment staff, use commonly available wiring/cabling, and be self-organising and self-optimising to adapt to each individual corporate environment.
- Efficient use of Backhaul. Dedicated transmission between the customer site and the operator's core network can be costly, but is likely to be justified to ensure good QoS. Optimising the traffic on this link by reducing unnecessary signalling overhead, routing calls and intranet traffic locally within the building improves system efficiency, security and reduces cost. A by-product is the reduced transaction load on the core network.
- Scalability. A solution needs to be able to cope with the largest enterprise buildings and campuses of anything up to 500,000 square feet. It also needs to handle the forecast growth in higher traffic demand either by subsequent addition of extra small cells and/or use of Wi-Fi and/or LTE within the same radio heads.

3.1.2.3 Public scenario

In a public deployment, HeNBs are deployed in a public area and users have open access, unlike the residential/corporate scenario, where only the allowed users can connect to a certain HeNB. An airport, a sport stadium, a train station, a library or any other public space where public access is to be facilitated to the users are examples of public deployments.

In this case, as the corporate scenario and unlike the residential scenario, a deployment plan is followed to design and deploy the network architecture. Infrastructure aspects must be controlled by the deployment administrator, for example: HeNB locations and coverage ranges are completely identified, HeNBs cannot be switched on and off randomly, and a single operator is chosen for the deployment.

The resulting network architecturedepends entirely on the designer of the deployment. We can assume that most of these public spaces do not have any existing network infrastructure, so all the network devices needed for the HeNB deployment must be installed from scratch. Dedicated backhaul links are needed, and those most likely are to be installed by the service provider. In general, we can imagine a hierarchical architecture with an aggregation layer which groups HeNB stations by location. The network topology, security mechanisms, etc. are up to the designer, who must fulfil the required needs.

3.1.2.4 Summary

The following table summarises LTE deployment characteristicsfor the residential, enterprise and public cases from the architectural point of view.

	Residential	Enterprise	Public
Access mode	Operating mainly in closed and hybrid access modes	Operating mainly in open and hybrid access modes	Operating in open mode
Users	Between 4 and 8 concurrent users	Between 8 and 32 concurrent users	Between 16 and 64 users
X2 interface	The LTE architecture in TS36300 indicates X2 connectivity between HeNBs, however it will work only through an X2 proxy	Small cells must interwork to ensure service continuity, interference coordination and fast handover, which require the X2 interface	Small cells must interwork to ensure service continuity, interference coordination and fast handover, which require the X2 interface
Small cells handover	Handover between small cells is not significant or absent	Yes	Yes
Local breakout for data traffic	Optional	Necessary to keep huge loads of enterprise packet traffic off the core network	Optional
Interference	Low	Medium to high	Medium to high
Broadband connection	Often less than 10 Mbit/s downlink, 512kb/s uplink	Higher speed connection	Higher speed connection
Delays of user and application data	High for cases when the uplink traffic is large; at 512kb/s will take 4sec. to transmit 1MByte	Lower than in the residential case, depending of the enterprise connection to Internet	High for cases when the uplink traffic is large; at 512kb/s will take 4sec. to transmit 1MByte
Delays of X2 interface used for ICIC	High when the users transmit uplink video and data	Lower than in the residential case, depending of the enterprise connection to Internet	High when the users transmit uplink video and data

Table 2: LTE deployment characteristicsfor the residential, enterprise and public cases

3.1.2.5 Implications for TROPIC

In the above subsections, we have exposed the different HeNB deployment scenarios with their characteristics and specific layouts. Note that these HeNBs are the current devices, without the enhanced computational and storage capabilities we include in TROPIC. In TROPIC, we have the small-cell-cloud concept, which is the aggregation of a certain number of cloud enabled HeNBs (SCeNBces) under the domain of an entity which manages them (SCM). In this new scenario, with cloud-enabled HeNBs, several new implications arise, which are explained in this subsection.

The main aspects to take into account in TROPIC, that is, for the different SCeNBces' deployment scenarios, are the following:

- **Location** – the location of the SCeNBces depends on the scenario. The SCeNBce location is going to affect the small-cell-cluster area, the small-cell-cluster dispersion, the network architecture topology, etc. SCeNBce location also affects SCeNBce handover. As they may call for the X2 interface, SCeNBces must be located within the coverage range from one another.

- **Operator** – SCeNBces within a small-cell-cluster can belong to the same operator or to different operators.

- **Hardware characteristics** – different scenarios may imply different SCeNBce hardware characteristics, which may have implications on the small-cell-cluster performance.

- **IP address allocation** – SCeNBces need to be contacted from outside their local network. This has some implications when they are behind a NAT function or the public IP address is dynamic. Theoretically, that should not represent a problem as long as SCeNBces can reach Se-GW and can establish an IPSec tunnel. As soon as the SCeNBce is activated, it will establish a tunnel towards the Se-GW/HeNB-GW and within the tunnel, the HeNB will have internal IP address. With this internal IP address, now the SCeNBce is in the same network with Se-GW, HeNB-GW, HeMS, etc.

The following table shows the implications for the different SCeNBce deployment scenarios for TROPIC.

	Residential	Enterprise	Public
Location	The SCeNBces within a cluster are located over a larger area. SCeNBces may not be within coverage and that poses a constraint for the usage of the X2 interface.	The SCeNBces within a cluster are located over a restricted area. Their location is planned and known. They must provide seamless handover through X2 interface.	The SCeNBces within a cluster are located over a restricted area. Their location is planned and known. They must provide seamless handover through X2 interface.
Operator	In general the SCeNBces within the cluster belong to different operators.	SCeNBces within the cluster belong to the same operator.	SCeNBces within the cluster belong to the same operator.
Hardware characteristics	SCeNBces may have very different hardware characteristics	All the SCeNBces have the same hardware characteristics	All the SCeNBces have the same hardware characteristics
IP address allocation	Most likely SCeNBces are behind a NAT function	SCeNBces may be behind a NAT function	SCeNBces may be behind a NAT function

Table 3: TROPIC implications summary

Even if in TROPIC we have considered some initial assumptions in order to simplify the architectural analysis (section2), these aspects should be taken into account by small-cell-cloud operators when deploying the SCM for different scenarios.

3.2 Support of LIPA (Local IP Access) with HeNB

Local IP Access provides access for IP capable UEsconnected via a HeNBto other IP capable entities in the same residential/enterprise IP network [3GPP TS22.220]. Data traffic for Local IP Access is not expected to traverse the mobile operator's network except mobile operator network components in the residential/enterprise premises. Signalling traffic will continue to traverse the mobile operator network. The residential/enterprise IP network itself and the entities within that network are not within the scope of 3GPP standardisation.

The local traffic offloading through the L-GW is very important for the small-cell-cloud approach, which is why we will dedicate a more detailed architecture description.

The general architecture scheme is provided inFigure 6:

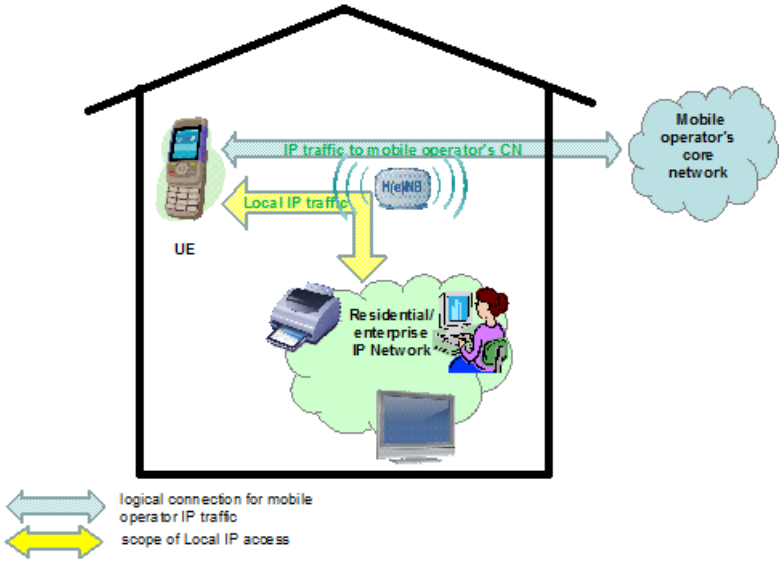


Figure 6. IP traffic split between local and core networks

The description of the logical architecture for the HeNB when it supports the LIPA function through the internal L-GW below is based on [3GPP TS23.401], while the deployment scenario in the figure below is taken from [3GPP TR23.829].

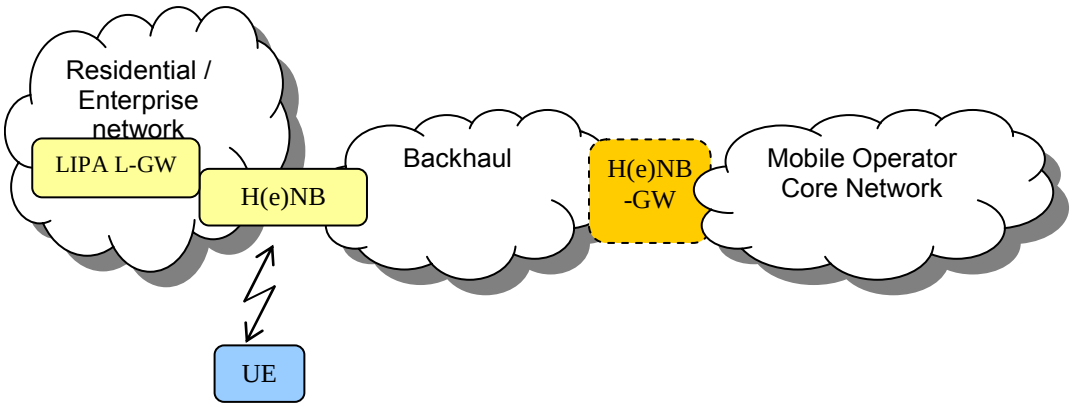


Figure 7. LIPA deployment scenario

The LIPA function enables an IP capable UE connected via a HeNB to access other IP capable entities in the same residential/enterprise IP network without the user plane traversing the mobile operator's network except HeNB subsystem.

LIPA is established by the UE requesting a new PDN connection to an APN for which LIPA is permitted, and the network selecting the Local GW associated with the HeNB and enabling a direct user plane path between the Local GW and the HeNB. The HeNB supporting the LIPA function includes the Local GW address to the MME in every INITIAL UE MESSAGE and every UPLINK NAS TRANSPORT control message as specified in [3GPP TS36.413].

For this release of the specification, no interface between the L-GW and the PCRF (Policy Charging and Rules Function) is specified and there is no support for dedicated bearers on the PDN connection used for Local IP Access. The Local GW (L-GW) shall reject any UE requested bearer resource modification.

The direct user plane path between the HeNB and the collocated L-GW is enabled with a Correlation ID parameter that is associated with the default EPS bearer on a PDN connection used for Local IP Access. The Correlation ID is used in the HeNB for matching the radio bearers with the direct user plane path connections from the collocated L-GW.

LIPA is supported for APNs that are valid only when the UE is connected to a specific CSG. LIPA is also supported for "conditional" APNs that can be authorized to LIPA service when the UE is using specific CSG. APNs marked as "LIPA prohibited" or without a LIPA permission indication cannot be used for LIPA.

MME shall release a LIPA PDN connection to an APN if it detects that the UE's LIPA CSG authorization data for this APN has changed and the LIPA PDN connection is no longer allowed in the current cell.

As mobility of the LIPA PDN connection is not supported in Release 11, the LIPA PDN connection shall be released when the UE moves away from HeNB.

The following additional information is based on [3GPP TS36.300]:

- For a LIPA PDN connection, the HeNB sets up and maintains an S5 connection to the EPC. The S5 interface does not go via the HeNB-GW, even when present.

- The HeNB may reuse the IP address used for S1 interface for this S5 interface in order to reuse the S1 secure interface or it may also use another IP address which would result in the establishment of another secure interface.

- The LIPA connection is always released at outgoing handover as described in [3GPP TS23.401]. The L-GW function in the HeNB triggers this release over the S5 interface.

In case of LIPA support, the HeNB supports the following additional functions, regardless of the presence of a HeNB-GW:

- Transfer of the collocated L-GW IP address of the HeNB over S1-MME to the EPC at every idle-active transition,
- Transfer of the collocated L-GW IP address of the HeNB over S1-MME to the EPC within every Uplink NAS Transport procedure,
- Support of basic P-GW functions in the collocated L-GW function such as support of the SGi interface corresponding to LIPA,
- Additional support of first packet sending, buffering of subsequent packets, internal direct L-GW - HeNB user path management and in sequence packet delivery to the UE,
- Support of the necessary restricted set of S5 procedures corresponding to the strict support of LIPA function as specified in TS 23.401,
- Notification to the EPC of the collocated L-GW function uplink TEIDs for the LIPA bearers over S5 interface within the restricted set of procedures to be forwarded over S1-MME and further used by the HeNB as "correlation id" for correlation purposes between the collocated L-GW function and the HeNB,
- In case of outgoing handover triggering the L-GW function to release the LIPA PDN connection and only handing over the non-LIPA E-RABs.

3.3 LTE HeNB architecture

The architecture of LTE HeNB introduces a new device with regard to the macro LTE architecture explained above. This device is the Femto Gateway (HeNB-GW). As already stated, the presence of

the HeNB-GW is not mandatory. It is also required the presence of a Security Gateway (Se-GW) as a function or logical entity, located as a separate physical entity or co-located with an existing architectural entity.

The HeNB-GW provides an aggregation or concentration functionality for a large group of HeNBs (from tens to hundreds of thousands). This preserves the hierarchical architecture of the current generation of the Core Network as it does not expose a large number of HeNB base stations to the Core Network elements.

Different solutions are provided by different operators. For example, Polaris Networks [polarisNetworks] offers a HeNB-GW with an integrated Se-GW and both user plane and control plane aggregation. Their HeNB-GW also provides traffic offload, helping to reduce traffic in the CN by offloading users from the cellular network, by implementing S-GW and PGW functionality within the HeNB-GW.

According to the small cell forum proposal [CSF01] and [TR23.830], we discuss three possible variants for LTE HeNB architecture in TROPIC. Advantages and disadvantages of each variant are relevant to the operator and can be found in the referenced documentation.

3.3.1 Variant 1

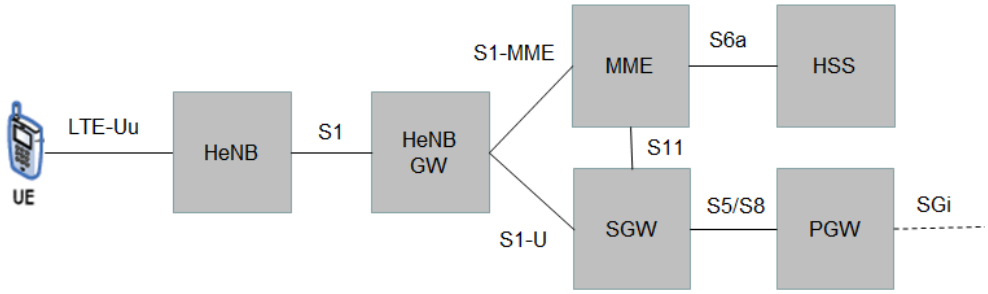


Figure 8. LTE variant 1

For variant 1, HeNB-GW serves as a concentrator for the C-Plane and also terminates the user plane towards the HeNB and towards the Serving Gateway[3].

[3] Existing commercial FGW devices are racks supporting the management of very large amounts of HeNBs (from tens to hundreds of thousands per rack). For instance, the NEC's solution (http://www.nec.com/en/global/solutions/nsp/3g/products_and_solutions/prod_femtocell/products_solutions/products_ran-gateway.html) refers to millions of femtocells managed by one FGW. The Polaris FGW (http://www.polarisnetworks.net/henb-gw.html) claims to manage up to 20.000 femtocells per single FGW rack. The Newgrid solution (http://www.newgrid.com/solutions/small_cell_lte_henb_gateway/index.jsp) also specifies that their SMEC LTE Small Cell Gateway (HeNB-GW) manages up to 120.000 HeNBs. All this indicates that the operator's policy seems steered toward the deployment of just a few FGWs to manage all their HeNB subscribers. For instance, assuming that one operator has 300.000 HeNBs, just 3 or 4 FGWs installed in the operator's infrastructure would suffice. This makes sense, as the opposite would entail major difficulties by the operator's perspective: in a hypothetical scenario in which each FGW would manage the HeNBs of a block (in urban scenario), say 30 HeNBs per FGW, the operators should insure the deployment of several tens of thousands FGW, each managing the interfacing with the CN. The considerations about costs deployment, complexity and maintenance seems to push the operators toward architectures in which the HeNB Gateway concentrates a large number of HeNBs and appears as an MME to the HeNB and the EPC.

3.3.2 Variant 2

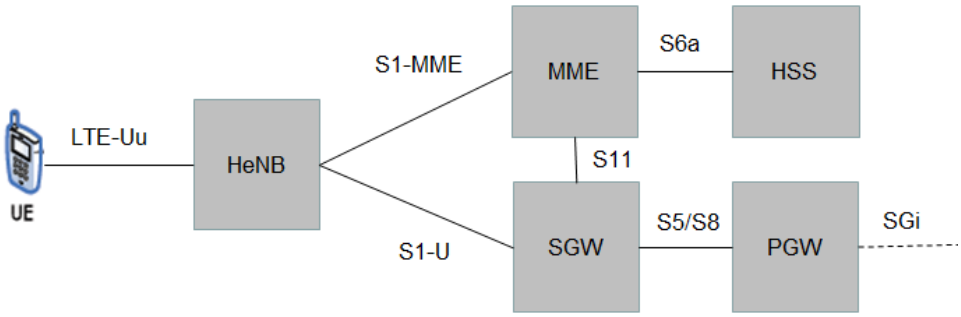


Figure 9. LTE variant 2

For variant 2, the S1-U interface of HeNB is terminated in S-GW and S1-C interface in MME, as per eNB. The HeNB may have connection to multiple MME/S-GW, i.e., may support S1-flex.

3.3.3 Variant 3

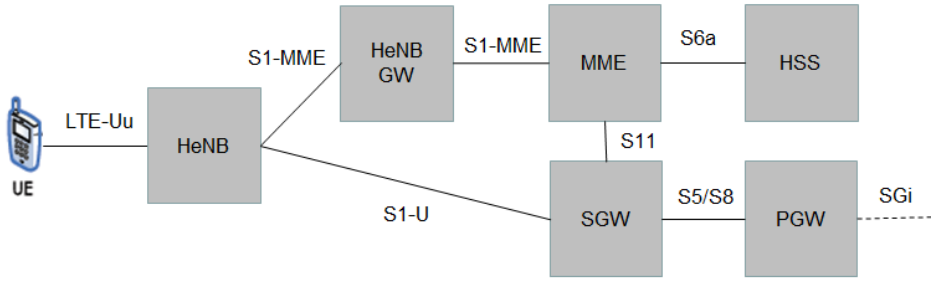


Figure 10. LTE variant 3

For variant 3, HeNB-GW is deployed and serves as a concentrator for the C-Plane. The S1-Uinterface of HeNB is terminated in S-GW, as per eNB.

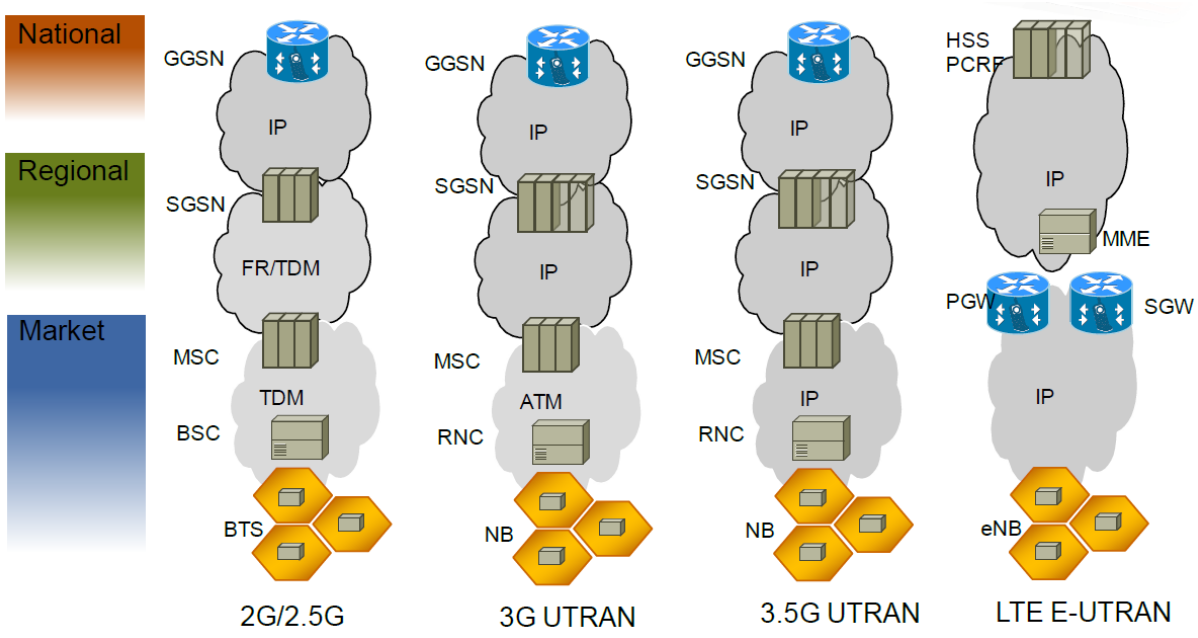
3.4 LTE network deployment

LTE is a relatively young technology that has not yet replaced the previous; therefore the new LTE networks must coexist with 2G/3G still operational equipment. One of the main deployment considerations is the location of each of the EPC functions, both initially and over time. Each operator has unique requirements; therefore, no single deployment model will suit all operators and there will be a clear dependency on what equipment has already been deployed.

In existing mobile networks, the base station controllers or BSCs (for 2G) and radio network controllers or RNCs (for 3G) perform radio resource management and mobility management functions. Typically, these controllers reside at the local Mobile Telephone Switching Office (MTSO)[4] and the connection between the base station and the controllers is enabled via the backhaul network. The backbone network is not involved and can be functionally separate, being utilized primarily for the interconnection of MTSOs.

[4] The MTSO contains the switching equipment or Mobile Switching Centre (MSC) for routing mobile phone calls. It also contains the equipment for controlling the cell sites that are connected to the MSC.

With LTE, the mobility management functions are performed by the mobility management entity (MME). The MMEs, serving gateways (S-GWs) and PDN gateways (PGWs) can be distributed across local, regional or national (data centre) sites with each eNodeB connecting to MMEs at any of these levels. The mobile transport network must enable connectivity between the eNodeBs and the MMEs and S/PGWs at the lowest cost per bit. For service providers who own the transport network, it is advantageous to utilize the same transport technology end-to-end to gain synergy and cost reductions from common operations, administration and maintenance.



MME – Mobility Management Entity, SGW – Serving Gateway, PGW – PDN Gateway

Figure 11.Hierarchical Architecture

3.4.1 Integration of Functions

A key optimization and deployment consideration is integration (or colocation) of multiple core functions on a single platform. Options to consider are the integration of discrete 4G functions, and integration of 2G/3G, 4G, and/or non-3GPP core network functions to achieve capital and operational efficiencies along the upgrade path. For example, a single node acting as a co-located SGSN+MME and a node acting as a co-located GGSN+S-GW+PGW can serve both the 2G/3G and the 4G networks.

The integration of functions simplifies the network topology, makes it easier to manage, and provides service uniformity. The reduction in "box" count could lower capital and operational expenses (CapEx and OpEx) and also eliminates external servers, load balancers, interfaces and related management equipment.

The following are some of the more common integration options:

- Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN): When EPC is deployed for 4G and requires mobility with an existing 2G/3G network, the EPC MME will interact with the SGSNs to perform mobility management. The signalling load between the MME and SGSN can be significant as the network grows. As separate nodes, both generate signalling traffic toward external nodes such as the Home Subscriber Server (HSS) and Mobile Switching Centre (MSC). In an integrated SGSN/MME, signalling functions can be internalized, eliminating heavy signalling traffic between the two functions and external

nodes. Additionally, performance and capacity utilization are substantially improved reducing costs up to 30 % over separate elements.

- MME, SGSN, and Serving Gateway (S-GW): Additional performance and cost improvements are possible if the S-GW is combined with the MME and SGSN. This could improve transaction performance by up to 80 % over separate elements.
- S-GW and Packet Data Network Gateway (PGW): The flexibility to split PGW functionality and co-locate S-GW and PGW functionalities allows traffic to be offloaded from the network closer to the customer, eliminating backhaul costs for a large portion of traffic. In addition, this integration could lower CapEx and OpEx as it takes fewer physical nodes to deploy and maintain, and the software and hardware utilization of the physical node will be better in many cases compared to separate nodes. Typical cost savings with this option range between 25 and 35 % for a distributed deployment model, primarily from core network backhaul savings. In the separate model, there is always some redundancy and leftover capacity in each node, not to mention the duplication of common functions.

3.4.2 Deployment Architecture

One of the key EPC considerations is the deployment architecture. The majority of 3G core deployments use a centralized architecture where a centralized GGSN serves multiple SGSNs at distributed locations. EPC, with many of the considerations already described, opens the door to revisit deployment architectures, including:

- *Centralized bearer/distributed control*: The traditional 3G architecture expanded to 4G where the PGW is located at a centralized location and the MME and S-GW is distributed.
- *Centralized control/distributed bearer*: A scenario where the PGW/S-GW is distributed and the MME is located at a centralized location.
- *Completely centralized*: An architecture where all the EPC functions are centralized.
- *Completely distributed*: An architecture where all the EPC functions are distributed and generally deployed together.

Deployment Architectures	Centralized Functions	Distributed Functions
Completely centralized	SGSN+GGSN MME+S-GW+PGW	-
Completely distributed	-	MME+SGSN+GGSN S-GW+PGW
Centralized bearer/distributed control (traditional 3G)	S-GW+PGW+GGSN	MME+SGSN
Centralized control/distributed bearer	MME	PGW+S-GW

Table 4: Potential Deployment Architectures (Cisco)

One of the main considerations is the variation of the deployment architecture over time. The first steps toward evolving the existing 2G/3G mobile packet core will be to provide initial EPC functional capabilities. Scaling and densification of the EPC will be required at a later stage (generally 3–4 years after initial deployment), as the rollout of LTE coverage progresses and subscriber numbers increase. Depending on the operator requirements, the architecture may vary between initial deployment and densification.

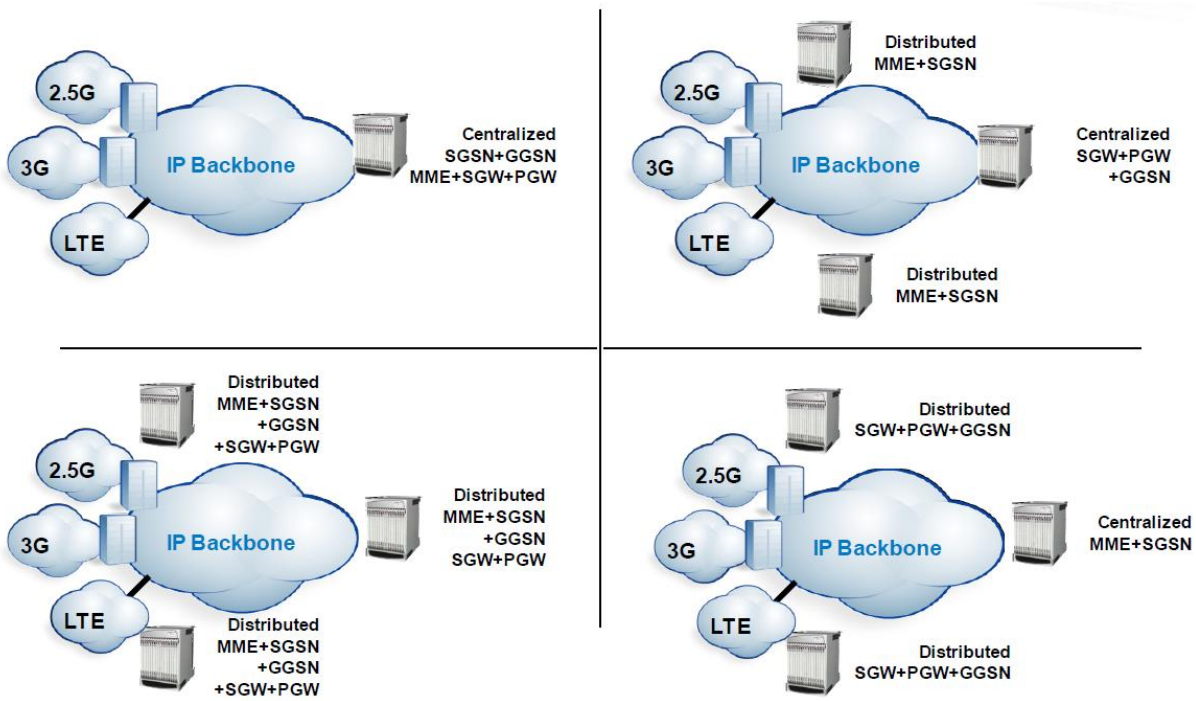


Figure 12.Potential Deployment Architectures (Cisco)

The following table shows the best choice for the placement of the main EPC elements:

Entity	Placement Considerations
MME	**Moderate distribution** Latency <50ms from eNB to MME (S1-MME), Faster signalling/call setup Use MME pooling -scaling & geographical redundancy
S-GW/PGW	**Distributed, close to edge** Ability to serve video locally Latency <50 ms from eNB (S1-U), better user experience Co-locate/Co-host S-GW/PGW if design permit Mobile Service Edge gateway (MSEG) might be an option to offload usertraffic, closer to edge
HSS	**Centralized/Moderate distribution** Latency <100 ms. Latency impact default bearer set-up Partition HSS as front end and backend if design permit Front-endco-locate with MME if possible
PCRF, Balance Manager, OnlineCharging System	**Centralized** Latency <100 ms. Latency impact policy download, updates Can share database with HSS Balance Manager, Online Charging co-located with PCRF

Table 5: Recommendation LTE/EPC Gateways Location

To meet the different requirements of the operators, the mainstream network equipment vendors support three basic models for providing mobile service elements in Evolved Packet Core:

1. Elements can be discrete nodes, with each logical EPC component representing a unique device.
2. Elements can be fixed cards or interfaces on a router/switch device, so that logical EPC components are mapped not to their own devices but to specific packet metro/core elements.
3. Elements can be "logical" and hosted by one of many switch/router or other service components in the network.

For any of these models, 3G and 4G functionality can be provided either independently or hosted in a single device. The latter solution is optimal where there will be considerable 4G deployments, where 3G elements are older (and thus represent less asset displacement cost) and where service evolution to 4G is expected to be fast.

Where it's not feasible to replace SGSN/GGSN functionality with a dual 3G/4G/EPC node set (MME/S-GW/PGW), the only option is to link the 3G elements with the 4G network in order to combine the traffic. Where integrated fibre backhaul connects tower sites with both 3G and 4G radio access networks (RANs), the use of integrated functionality for 3G/4G elements is much preferred because all traffic will emerge from the backhaul at the same point.

4 SPECIFIC ELEMENTS OF THE GENERAL ARCHITECTURE

This section intends to describe the different components that have to be integrated for being able to deliver the kind of service TROPIC is proposing.

The main components belong to the radio and cloud plane and derive from use cases and requirements described in [TROPICD21].

4.1 Radio plane

The radio architecture should support the connectivity requirements for developing the cooperative TROPIC approaches at both radio and user data (application) levels. We take as a requirement to develop this architecture based on these basic requirements:

- Provide solutions built on top of the LTE Release 11 architecture specifications;
- Strive for low cost solutions, while using the existing HeNB internal blocks;
- Strive for low cost operator solutions.

In the next subsections we present the building blocks of the radio plane for the TROPIC architecture (section 4.1.1) and we discuss the suitability of the LTE architecturein the framework of TROPICas well as open issues relative to this context (section 4.1.2.)

4.1.1 User equipment

A regular UE comprises blocks such as radio, modem, processor, memory and communication interfaces, such as USB, Ethernet, Wi-Fi, Bluetooth, etc. There is a processor and the associated memory (may be different memory types). The applications run over the resources of the processor and memory. In TROPIC, the UE will (automatically or manually by the end user) launch a request to use the cluster either for storing data or for running applications.

In the next subsections, we describe the mechanisms that will trigger the SCM actions.

4.1.1.1 Application, computing capabilities and physical layer

The application layer is the layer that initiates the process and requests to launch a concrete application.

The cluster of SCeNBces is suitable for running different types of applications:

- **Storage**:
  - Upload data (images, files, etc.) to be stored locally and could be shared or not.
  - Cache data from the internet (Youtube, images) to be accessed more quickly by any user

  This storage can be done in virtualised shared disk (allowing privacy options).
- **Processing:**
  - Applications residing in the cluster (for example, facial recognition application installed at an airport).

  This requires virtual machines in order provide an enhanced service to the end user and to be able to migrate these processes to another SCeNBce in case of disconnection.

The execution of applications in the cluster can be the result of a direct request by the end user but it can also be determined by the user equipment thanks to the offloading module, whichwill evaluate, for an application, if it is more suitable to run it over a cluster according to a certain number of criteria.

This application has several characteristics that are determined by the application layer:

- Maximum allowed latency in the delivery of the data resulting from the execution of the application (QoS parameter).
- The suitability of the application to be split and run in parallel processes.
- For each parallel run possibility, there is some data load that must be sent to the cloud and an expected result to retrieve from it.
- Each application requires a certain number of computation cycles to be run.

Besides, the computation at the UE is characterized by the following terms:

- Processor speed: number of execution cycles per second.
- Energy efficiency: Joules per execution cycle.

Based on the previous parameters, for each possible configuration for the execution of the application, the UE can calculate which would be the latency and the energy cost associated to the execution of the corresponding local subprocesses at the UE:

- Energy spent by the UE associated to the execution of the local subprocesses corresponding to this configuration.
- Latency associated to the execution of the local subprocesses at the UE corresponding to this configuration.

Finally, for each possible configuration, the UE will have to send and receive a different amount of data to and from the cluster. Since the UE knows the channel state, the maximum power transmission, the possible cooperative transmission strategies for both the uplink and downlink, the quantity of data to be transferred for such configuration, etc., the UE can calculate locally for each possible configuration, the optimum trade-off curve between communication energy and communication latency.

These optimum trade-offs are obtained as described in the work performed in WP5.

4.1.1.2 Offloading decision module

With all the previous information, the offloading module at the UE can build the offloading trade-off curves. These curves are based on the previous optimum communication trade-off curves and are shifted according to:

- The energy spent by the UE associated to the execution of the local subprocesses corresponding to a certain configuration.
- The latency associated to the execution in the cluster of the offloaded subprocesses associated to each configuration. These parameters are to be provided by the SCM.

Using these curves, the offloading module at the UE will decide which is the best configuration in the sense of minimizing the energy spent by the UE, while fulfilling the maximum latency constraint.

4.1.2 Suitability of the LTE architectures for the TROPIC cooperative concepts

4.1.2.1 LTE architecture and cooperative RRM

The X2 interface, allowing the implementation of the CoMP approach, including the distributed RRM, is of paramount importance for TROPIC collaborative concepts. In the following we are going to analyse the involved latency, which is critical for the implementation of the TROPIC concepts.

Based on [3GPP TR36.932] the small cells can use a variety of backhauls, the most used being DSL and fibre. The macro BSs and the EPC use in general a fibre backhaul. So it would be of interest to

show a real deployment case, using xDSL/FTTx for SC backhauling and fibre/wireless for Macro cell and EPC backhauling.

We will take as basis for delay computations the typical case of a LIPA architecture using tunnelling.These situations, together with the delays mentioned for the different backhaul options, are shown in Figure 13.

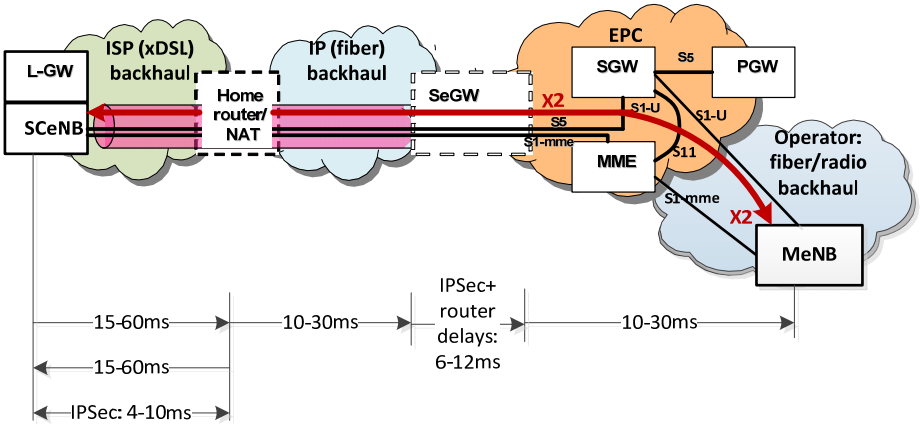


Figure 13. Network delays of X2 connection over different backhaul types

There are two cases to be analysed:

- Case 1 : the SCeNB connection is over the P-GW, when one SCeNB is deployed using the local ISP (Internet Service Provider) facilities and the other SCeNB or the MeNB are deployed using the mobile operator backhaul ;
- Case 2 : the SCeNB connection is done at the ISP premises.

It should be mentioned that both the ISP and EPC use aggregation routers implementing a number of services, such as QoS enforcement and traffic shaping, in addition to the routing itself. Cisco, a very popular aggregation router provider, has measured and presented the latency results in [Cisco-delay]. The delays are under 1ms in these routers. However, the tunnelling using IPsec involves higher additional delays, in the order of 4-10ms, as shown in [Cisco-IPsec delay].

Based on the delays mentioned in [Cisco-IPSec delay] and [3GPP TR36.932], both shown in Figure 13, the approximated end-to-end delays are:

- Case 1: 39-162ms;
- Case 2: 36-132ms.

The internal SCeNBce delays should be addedto the above delays. As these depend of implementation, we are not in the position to provide numerical values.

The computed accumulated delays are too high for the TROPIC cooperative RRM, such that we consider the usage of alternative solutions (section 9).

4.1.3 General TROPIC radio-level architecture

In the typical backhaul cases (DSL for SCeNBce and fibre/wireless for MeNB) the delay is too high (see Figure 13) for supporting efficient ICIC, either based on X2 or on the new cooperative MIMO functions.

In the collaborative MIMO processing, the channel variations, especially at the 3.5GHz target LTE frequency, are too fast for being supported with such delays.

Based on this analysis, we propose another architecture concept, where the SCeNB-MeNB communication is done over the air (OTA), as shown inFigure 14.

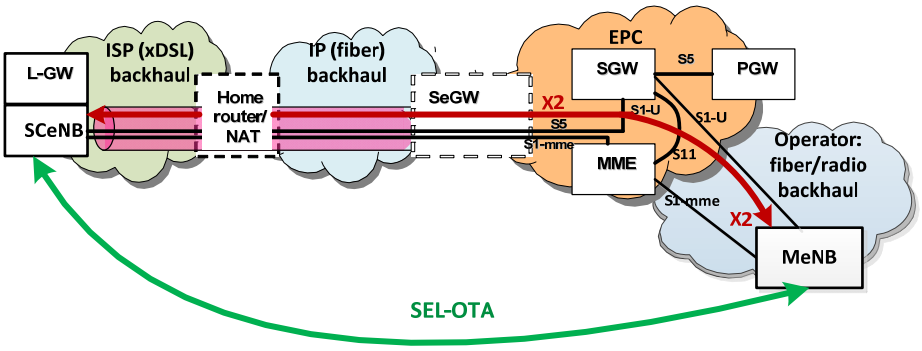


Figure 14. SCeNB-MeNB communication is Over the Air

4.1.4 Architecture for X2 MP-MP communication over the air

Given a number of factors related to the uplink backhaul characteristics and often changing traffic distribution between SCeNBces in some deployment cases it could make sense to use the OTA (Over The Air) communication.

While OTA was developed in LTE for relay support, conducting to a P-MP architecture, the TROPIC Cloud requires rather a MP-MP X2 connectivity. This is further described in section 9.2.1.

4.2 Cloud plane

4.2.1 Introduction

Multiple definitions of Cloud exist today, that leave users, providers and developers equally confused about what can actually be expected from a Cloud. [Cloud12] exposes different definitions from different points of view. Among all these definitions, the most popular is probably the one provided by the National Institute of Standards and Technology (NIST). According to this definition:

"CLOUD computing is a model for enabling ubiquitous, convenient, ondemand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This CLOUD model is composed of five essential characteristics, three service models (Software / Platform / Infrastructure as a Service), and four deployment models, whereas the five characteristics are: on-demand self-service, broad network access, resourcepooling, rapid elasticity, and measured service. The deployment models include private, community, public and hybrid CLOUD."

According to NIST [Nist01], the essential characteristics of a Cloud would be:

- **On-demand self-service**. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad network access**. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource pooling**. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the

exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacentre). Examples of resources include storage, processing, memory, and network bandwidth.

- **Rapid elasticity**. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service**. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

In TROPIC, the so-called small-cell-cloud should comply with these characteristics, as the main functionality of the Small Cell Cloud Manager (SCM) is based on these premises.

NIST also provides the service models definitions [Nist01]:

- **Software as a Service (SaaS).** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings
- **Platform as a Service (PaaS).** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **Infrastructure as a Service (IaaS).** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

In TROPIC, the small cell cloud would not fall into the Software as a Service model, since the user is not supposed to interact with the cloud resources (processing, storage, etc.) directly or deploy his/her own applications over the cloud infrastructure.

NIST also provides the deployment models definitions [Nist01]:

- **Private cloud**.The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud**.The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

- **Public cloud.**The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. Itexistsonthepremises of thecloudprovider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

In this case, the small cell cloud in TROPIC would fall into the private cloud, since all the clusters will be managed by a single operator and no possible interactions with other operators or individuals are considered.

4.2.2 Computing and storage resourcesof SCeNBces

In any cloud infrastructure, the back-end devices must have certain computation and storage capabilities. For instance, in current data centres, servers run over computers with their own CPU and storage capacity. This storage capacity could be allocated in the computers' hard disks drives or in an independent storage network, which servers can access in order to save or retrieve data.

Thus, in TROPIC scenario, SCeNBces(the new generation of small cells) musthave certain computation and storage capabilities to perform as back-end cloud devices. SCeNBs are supplied with CPU and storage devices,i.e. a RAM memory and a Hard Disk Drive (HDD). In our case the storage devices would be allocated within the SCeNBce itself.

We consider this SCeNBce with computational capabilities an extension or enhancement of acurrent HeNB, which do not offer this kind of computation capabilities but whose features are rather those of an antenna with limited intelligence. However, in our scenario, small cells act as the computing back-end nodes, making use of these computation and storage capabilities for running the applications and serving the user requests. Expected capabilities of SCeNBces are defined in [TROPICD21].

4.2.3 Cloud scenario

One approach we could make is to understand small cells as typical servers. A typical server would take the client request, perform the appropriate actions to serve that request, and send the response to the client. If necessary during the process, the server could request other servers in order to form the final response, so a server would also serve requests coming from other servers and not directly from the client. This is the basic server functionality, as it is performed in current data centres and server farms.

The figure below shows the basic request-response flow in a typical data centre or server farm. A server receives the request coming from the client and optionally requests other servers in order to form the response properly. Then it forwards the response back to the client through the same interface by which it received the request.

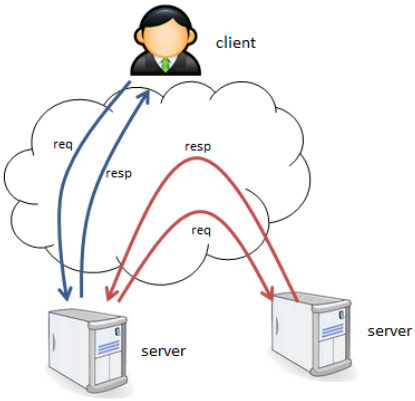


Figure 15. Request-response flow in a typical data centre / server farm.

In this way, SCeNBces would have the same behaviour. First, they would handle requests coming from the clients attached to that SCeNBce (as described in section 4.1.1). In the other hand, they would also serve requests coming from the cluster and deliver the responseback to the cluster, which will be then delivered to the corresponding client. This behaviour would be managed by the Small Cell Cloud Manager, as we will see later in this section.

The main difference from the server scenario is that while servers serve and responds requests through the same interface, SCeNBcesserve requests coming from two different interfaces. One is the air interface which connects the user with the SCeNBce, and the other one is be the interface with the backhaul which connects the SCeNBceto the cloud.

The following picture shows the request-response flow in the small cell cluster scenario. First, the client requests the corresponding SCeNBce. Then, the SCeNBce forwards the request to the cluster in order to be processed. The SCM handles the request accordingly, querying the SCeNBces under its domain to form the response, which is sent back to the client through the air interface of the SCeNBce the user is attached to.

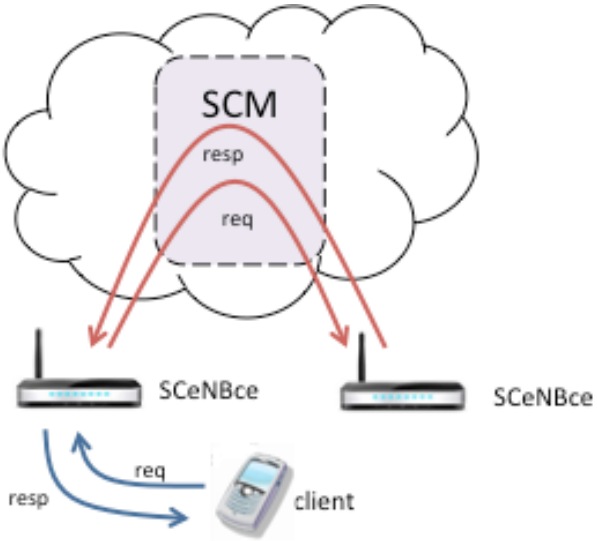


Figure 16. Request-response flow on the small cell cluster scenario.

From this point of view, SCeNBces have a similar role asa server but with the differences implied by the small cell clusterscenario.

4.2.4 Cloud and Virtualization management

Virtualization is a trending technology currently more and more used in cloud applications. A Virtual Machine (VM) is an abstraction of a real machine. Virtual Machines are isolated from the hardware of the host machine, and run operative systems as the real machines do. Applications can be deployed over these operative systems, which will run within the VM context.

Server virtualization is a common example. In server virtualization, a physical machine hosts several virtual servers, which have the same characteristics as the real ones. By means of server virtualization costs can be reduced and resources can be better utilized.

In current data centres, the control of the VMs requires a Virtual Infrastructure Manager (VIM), which is the entity in charge of the VM lifecycle and implementing functionalities like elasticity. Some well-known solutions are Open Nebula, Eucaliptus, VMWare, etc.

Listed below are the main features and functionalities of Open Nebula [OpenNebula]. We can assume that the functionalities of the other VIMs are similar, so it is interesting to have them in mind, as we are going to use a VIM or an enhanced VIM entity (Small Cell Cloud Manager) in our small cell cluster scenario. Those VIM features and functionalities are:

- Powerful User Security Management
- Advanced Multi-tenancy with Group Management
- On-demand Provision of Virtual Data Centres
- Advanced Control and Monitoring of Virtual Infrastructure
- Complete Virtual Machine Configuration
- Advanced Control and Monitoring of Physical Infrastructure
- Broad Commodity and Enterprise Platform Support
- Distributed Resource Optimization
- Centralized Management of Multiple Zones
- High Availability
- Virtual Appliance Marketplace
- Hybrid Cloud Computing and Cloudbursting
- Standard Cloud Interfaces and Simple Self-Service Portal for Cloud Consumers
- Rich Command Line and Web Interfaces for Cloud Administrators
- Multiple Deployment Options
- Easy Extension and Integration
- Reliability, Efficiency and Massive Scalability

As part of the cloud management, TROPIC envisages the addition of a new functional entity, theSCM, within the fixed operator network. The SCM is seen by TROPIC as an extended VM Manager, so the previous features exposed should be supported and extended.

The location of the SCM is a key point of the cluster architecture, and it is an issue that is addressed in the architecture section of this document. Here, we are going to discuss the main functionalities of this entity without taking into account its location within the architecture.

The main functionalities (but not the only ones) of the SCM are:

- Virtual Machine placement / deployment.
- Virtual Machine monitoring.
- Virtual Machine migration.
- Virtual Machine resource modification.
- User management.
- Back-up and recovery operations.

- Self-environment performance (self-service, self-managing, …)
- Selection of the location where the application is processed (which SCeNBces within the cloud, UE, …)
- Decision making about distributed application processing (in case the application computation must be distributed among several SCeNBces).
- Bursting.

A first approach we can make to define the definite SCM functionalities is to separate them into control plane and user plane. Control plane functionalities comprise those related to control and management policies such as VM and user management, monitoring, resource control and modification, etc. User plane functionalities would comprise those related to the user service delivering such as application running and scheduling, bursting and other functionalities related to the request and delivering of services.

The SCM is intended to receive messages from UEsthrough SCeNBcesand from SCeNBces themselvesand perform the control and managing operations that apply in each case. For example, when a new SCeNBce is connected, it would notify the SCM of its presence. Another example would be the messages sent from the SCeNBces to allow the SCM to monitor their VMs status. The SCM would send some kind of control message and control datato the SCeNBces. For example, when a VM is deployed, the control plane sends a message to the destination SCeNBce, along with all the necessary data.

The SCM would also include the polling operations for monitoring purposes. In that case, the SCM would send polling messages to the SCeNBces, waiting for a response. An example of this would be the case in which the SCM wants to know if a certain SCeNBce is still active, so it would send a polling message to that SCeNBce, waiting for its response.

The SCMalsohandles the application requests coming from the users through the serving SCeNBce. It would take the request and perform the necessary operations in order to manage it properly and so that the response is delivered within the established policies.

4.3 Backhaul

The different backhaul types used in [3GPP TR36.932]areinsufficiently characterised for understanding the complex problems introduced by the xDSL backhaul.

Below is a more detailed characterisation, addressing the different key characteristics of this type of backhaul.

Backhaul Technology	Latency SCeNB to SCeNB on DSL only	Latency SCeNB to ISP	UL Throughput	DL Throughput	Jitter (UL) (IPV6 fragment + H.264/MPEG4 I-frame)	Packet loss
ADSL	**23-80ms**	**15-60ms**	**0.25-3.5Mb/s**	**1-24Mbps**	**0 - 570ms**	**0-40%**
VDSL			**0.5-15Mb/s**	**10-100Mb/s**	**0 - 549ms**	

Table 6: ADSL/VDSL backhaul characterisation

While the delay is the most relevant parameter for the characterisation of fibre/wireless backhauls, this is not the case for DSL links. Additional throughput and QoS parameters are needed for understanding the full DSL behaviour. As can be seen below, the jitter may be more important than the delay.

The references for the values in the previous table are [Wiki1] and [Wiki2].

QoS metrics: Latency, jitter and packet loss are generally are used

ADSL Latency: The IPSec delay of 4-10ms per SCeNB have to be both considered.

ADSL Jitter: This parameteris affected by the variations of the UE's traffic and the modem interleaving. As the modem interleaving was already considered, we will calculate the jitter as additional delay for the following scenario: 2 UEs, one sending data and the other one having a video call MPEG4-AVC and sending a I frame. The first UE has just sent the IPv6 fragment, which is already in queue and the second UE sends the main video frame I, marked with high priority in the IP header. The uplink speed is very important for determining the jitter.

ADSL Packet loss: the search results show frequently 30% or 40%.
The uplink low throughput and the problematic QoS will have a big impact on the operation at both radio and cloud levels.

4.4 Security

Considering the network is composed of mixed legacy small cells (SCeNB) and cloud enabled SCeNB, (SCeNBce), to connect to the Se-GW, both types of devices use the same security mechanism, which is the IPsec tunnel. Since the SCeNBce is assumed to be only a feature added to the legacy SCeNB, both functions use the same IPsec tunnel because the SCeNB is verified and, after the successful verification procedure, the SCeNBce is enabled to authenticate. This approach provides a backward compatibility feature if the legacy Se-GW and SCM is the same device (two SW functions on the same physical appliance), which seems as the most likely implementation from the cost-efficiency perspective. Therefore, the SCeNBces feature is assumed to be only another (third) function enabled on the same device.

In terms of authentication, the case with HeNB and pico/microcell are different. Once a common HeNB is powered up, it authorizes itself via the IPsec tunnel to the Se-GW. Considering, the "cloud capability feature" implemented in HeNB beside the legacy functions, the authorization traffic will be routed via the existing IPsec tunnel to the SCM. As the "cloud capability feature" is an optional function of the legacy HeNB, it is also assumed that the SCeNBce will never be run without the legacy HeNB function. Therefore, the IPsec tunnel is always available to encrypt the mutual communication. The previously described approach is not required for picocells and microcells because they are connected to the core network (EPC) via private telecommunication circuits which are considered to be trusted environments.

Users of a SCeNB log into the cloud services via the SCM which forwards the credentials to the appropriate EPC entities (HLR/HSS, MME, etc.) Once the user is authenticated to use the cloud services, he/she is charged appropriately and the charging data is sent to the respective infrastructure entities. The SCM provides the key-management for user-to-SCeNBs communication and cloud services security.

Detailed analysis of security issues and design of necessary measures to avoid any increase in security risks will be targeted in frame of WP5 (5A3).

5 ARCHITECTURE

The elements within the LTE architecture that need to interact with the SCM have been identified according to the information they will provide to the SCM and the information they will be provided by it. The following diagram represents what elements in the LTE architecture need to interact with the SCM, indicating the nature of the information required:

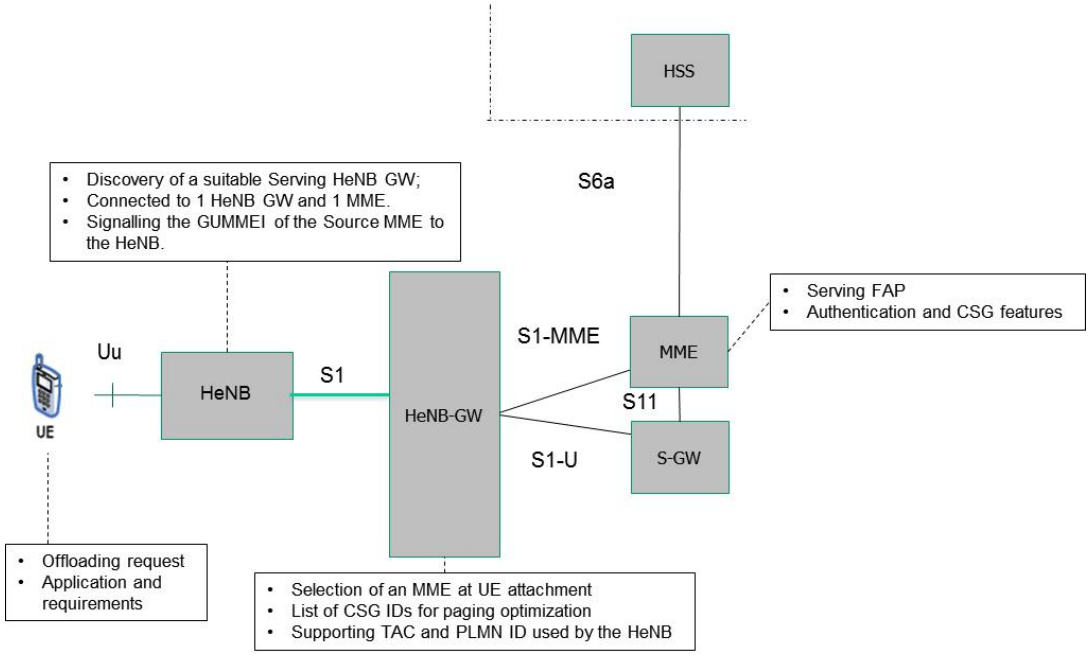


Figure 17. SCM LTE interacting nodes

In the previous picture the HeNB-GW has been depicted in order to achieve the broadest case. In case the HeNB-GW does not exist, the functionality of the remaining nodes does not change dramatically, it is only the information concerning the serving HeNB-GW, which would not be necessary.

The UE provides:

- The offloading module
- The client application data and requirements

The SCeNBce provides:

- The HeNB-GW to be addressed
- The serving MME

The HeNB-GW provides:

- The serving MME
- The list of Closed Subscriber Groups
- Tracking area code (TAC)
- The operator, although in our approach all SCeNBces belong to the same telecom provider.

The MME provides:

- Access to authentication information in the HSS.
- The serving access point.

As for the S-GW, our first conclusion is that there is no need for a SCM managing one cluster to interact with it. The S-GW will only be informed of monitoring information for charging purposes.

The S-GW could also be interfaced with the SCM in case several clusters are connected through this node (for inter-SCM communication as explained in section6).

Another example in which the SCM should be interfaced with the S-GW is the case in which we consider applications whose backup source is also in the internet. If this sort of applications is considered, the SCM should retrieve information from external clouds (e.g., Youtube or other cloud service providers). As stated in the General Assumptions (Section2), by the time this document was being written, no considerations concerning the sort of applications to be supported had been made yet.

Besides, according to section 3.1.2, there are differences between the residential and enterprise deployments. These use cases also differ as far as IP addresses management is concerned, which also requires some study, since the SCM will access the HeNB using its IP address and viceversa.

In the scope of TROPIC, when the SCeNBce is located within a private network masqueraded behind a NAT mechanism, which is common in the residential use case, the situation can be critical because home router typically has dynamic IPs provided by their associated ISP. The communications initiated in the private network (the cluster) to the outside world would reach their destination and the response would reach the source within the private network without problems, since the translation tables are set when the internal request reaches the NAT.

A typical problem present in NAT masqueraded networks occurs when an external entity wants to connect an internal destination. NAT translation tables are not uploaded in this case, and when an IP within the private network changes, the external entity cannot reach the internal destination.

In our case, the SCeNBce would establish an IPSec tunnel with the Se-GWat startup. The SCeNBce would have its own internal IP address within the IPSec tunnel, which means that the SceNBce and Se-GW are in the same network, and the connection from the Se-GW to SCeNBce could be established at any moment, although the external SCeNBce IP address has changed.

The same argument could be applied in the connection case between SCeNBce and SCM when the latter is not behind the HeNB-GW, and as long an IPSec tunnel is established between them.

Different alternatives for SCeNB-SCM communication are described in section 7 in case the SCM is a standalone module not placed in the LTE core network.

The protocol managing the small cell cloud, including the operation of the virtual machines, is named Z-interface, and may have different parts as Z-U (user data part) and Z-C (control part) and is described in section 7.

The architectural options described hereafter propose different placements of the SCM within the LTE architecture. Following the operator's approaches as shown in section 3.4, different synergies are searched.

5.1 Evaluation criteria

The criteria used to evaluate all architectural options are described below. At evaluation time, a comparative approach has been followed in order to analyse all options:

- Requirements coverage: This relates to what extent the architecture covers the TROPICrequirements provided [TROPICD21].
- Signalling overhead: The signalling overhead is the extra signalling load due to the architecture modifications. It is obvious that the introduction of a new component brings along moresignalling but some of them introduce greater overhead than others.
- Latency: It is the delay the user will perceive when requesting computing and storage to be done over the cluster. Latency depends on the kind of backhaul, as explained in section 9.1.1.

- Computation/storage performance: it refers to the number of resources the SCM will be able to manage, which will be available to the end user as computing and storage nodes.
- SCMcomputational capacity requirements: Required computational load of the SCM in order to carry out its operations.
- Cost of deployment and maintenance: Overall cost due to current LTE architecture modifications and maintenance derived costs.
- Implementation complexity: Overall complexity regarding the modifications of the current LTE architectures.
- Impact on existing LTE deployments:Overall changes to be performed in order to implement the solution. The changes have been analysed taking into account the LTE variant the architecture is based on.
- Energy consumption: overall energy consumption. This will be closely related to the number of nodes involved.

5.2 Architecture description

5.2.1 Option 1: Variant 1 - SCM as an extension of the HeNB-GW

5.2.1.1 Description

In this option the SCM is placed at the HeNB-GW, either as an additional component or as a new element in the gateway itself.

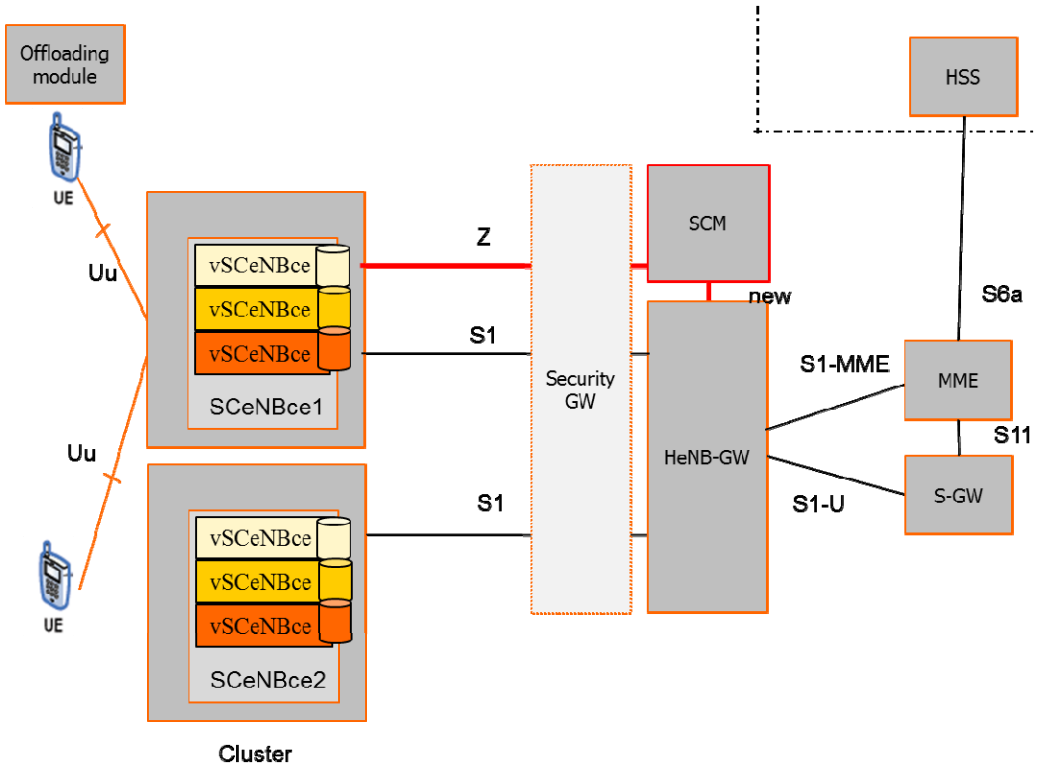


Figure 18. Option 1: SCM as an extension of the HeNB-GW

5.2.1.2 Evaluation

	SCM as an extension of the HeNB-GW
Requirements coverage	Yes, with the limitations explained in this table
Signalling overhead	Low – If the SCM is integrated in HeNB-GW, it could utilize some of the signalling sent from and to the gateway.
Latency	Medium- the SCM is close to the UEs
Computation/storage performance	Medium- only nodes under a single HeNB-GW are available to pool their resources
SCM computational capacity requirements	Medium- management of nodes over a small cluster
Cost of deployment and maintenance	Medium- a medium amount of SCMs have to be deployed (one per HeNB-GW)
Implementation complexity	Low- if the SCM is part of the HeNB-GW, less interfaces required and even less/none if the SCM is an integrated part of the HeNB-GW. In the latter case, the Security-GW also requires modifications
Impact on current LTE deployments	Low - one interface is needed between the SCM and the HeNB-GW. In case they merge, an internal interface would be enough.
Energy consumption	Medium- less SCMs entities are required

Table 7: Option 1 evaluation

5.2.2 Option 2: Variant 1 - In-cloud Standalone SCM

5.2.2.1 Description

In this case the SCM is a new component closer to the computing nodes. In corporate environments, the SCM could be placed at the enterprise's premises. In the residential case, and according to what is explained in section 3.1.2.1, the SCM would be located at the ISP's premises as closest possible location. The placement of SCM in ISP means less control by MNO, thus this situation would require some additional business agreement between both for operational support. This scheme requires the SCeNBces to differentiate the traffic that needs to be directed to the Security GW from the internal traffic of the cloud. Different alternatives for this are described in section 8.

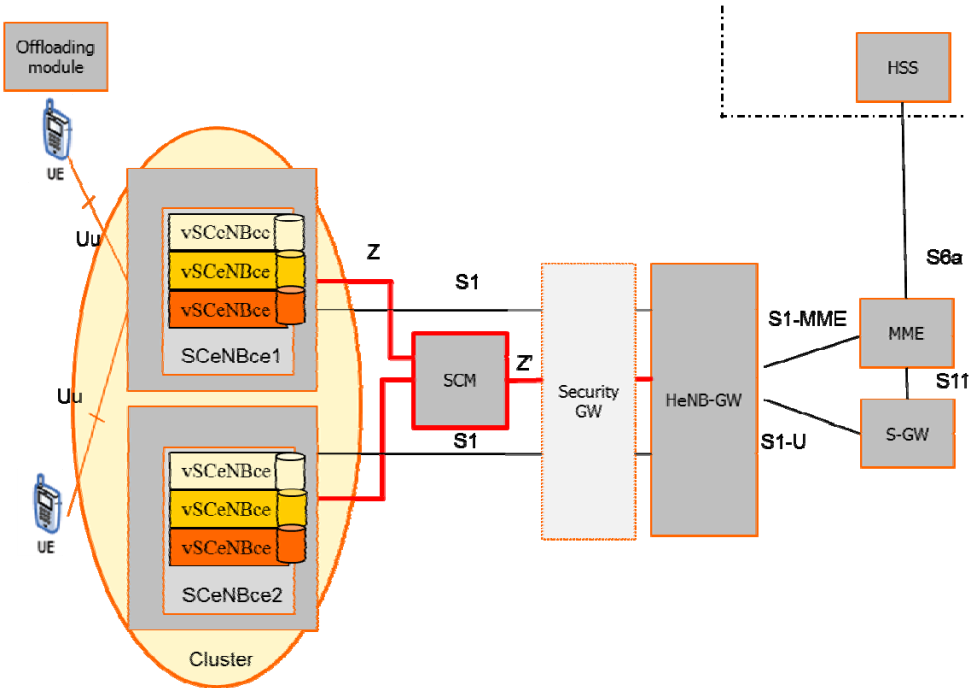


Figure 19. Option 2: In-cloud Standalone SCM

5.2.2.2 Evaluation

	In-cloud Standalone SCM
Requirements coverage	Yes, with the limitations explained in this table
Signalling overhead	Medium – the SCM is closest to the UEs and less hops are required, but as standalone, the SCM would need dedicated signalling.
Latency	Low- the SCM is closest to the UEs
Computation/storage performance	Low- only nodes under a single HeNB-GW are available to pool their resources
SCM computational capacity requirements	Low- management of nodes over a small cluster
Cost of deployment and maintenance	High- high amount of standalone SCMs have to be deployed (one per cluster)
Implementation complexity	High- New interfaces required
Impact on current LTE deployments	Medium – new interface betweenSCM and HeNB-GW
Energy consumption	High – a greater number of consuming nodes must be deployed

Table 8: Option 2 evaluation

5.2.3 Option 3:Variant 1 - Standalone SCM

5.2.3.1 Description

The SCM in this case is a standalone element not necessarily close to the cluster. In this case, the SCM is connected to several HeNB-GW in order to achieve larger clusters for greater computation capabilities.

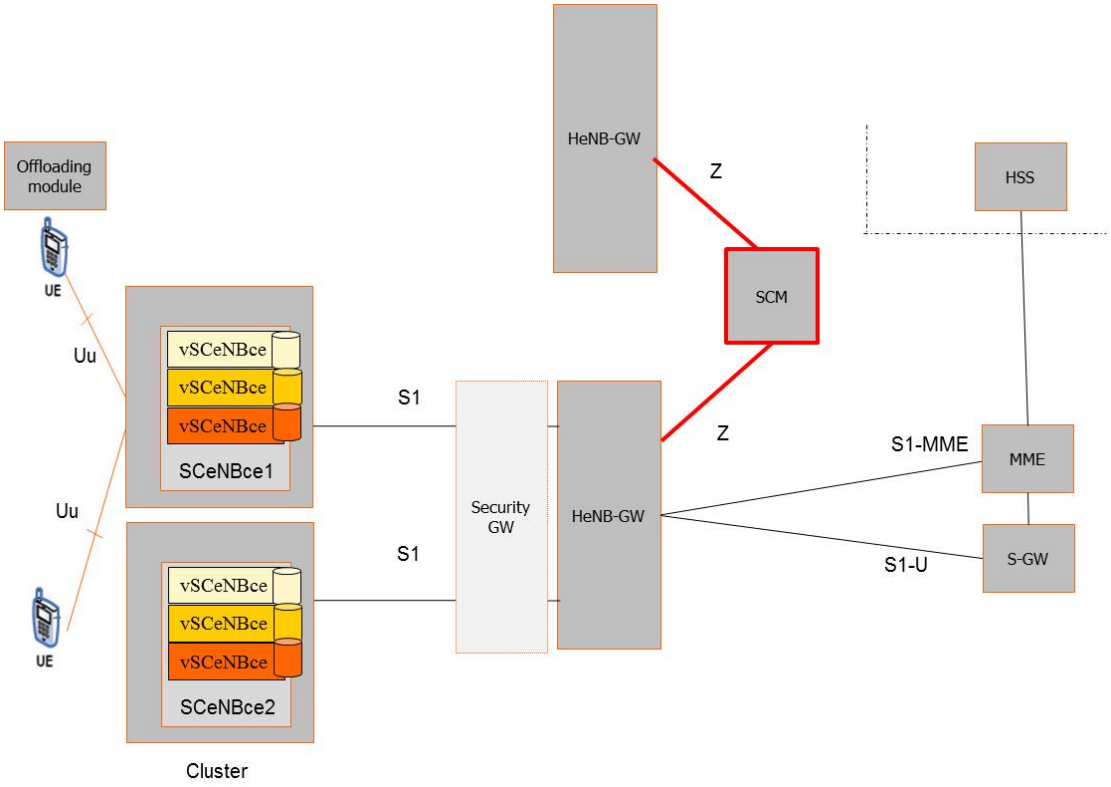


Figure 20. Option 3: Standalone SCM

5.2.3.2 Evaluation

	Standalone SCM
Requirements coverage	Yes, with the limitations explained in this table
Signalling overhead	High – Signalling requires a greater number of hops as more entities are involved. Also, as standalone, SCM would need dedicated signalling.
Latency	High– Greater SCM computational load and number of resources under its domain.
Computation/storage performance	High- Greater number of resources under SCM domain.
SCM computational capacity requirements	High- Greater number of resources under the SCM domain.
Cost of deployment and maintenance	Medium- less amount of SCMs have to be deployed (one per cluster assembly)
Implementation complexity	Medium – the SCMis more complex than in other cases
Impact on current LTE deployments	Medium – a new interface between the SCM and the HeNB-GW is required
Energy consumption	Low – less SCM are required

Table 9: Option 3 evaluation

5.2.4 Option 4:Variant 2 - In-cloudStandalone SCM without HENB-GW

5.2.4.1 Description

As in the In-cloud Standalone SCM (Option 2), in this case the SCM is a new component closer to the computing nodes. In corporate environments, the SCM could be placed at the enterprise's premises. In

the residential case, and according to what is explained in section 3.1.2.1, the SCM would be located at the ISP's premises as closest possible location. The placement of SCM in ISP means less control by MNO, thus this situation would require some additional business agreement between both for operational support. This scheme requires the SCeNBces to differentiate the traffic that needs to be directed to the Security GW from the internal traffic of the cloud. Different alternatives for this are described in Section 8.The only difference between this option and the Option 2 is the existence –or not- of the HeNB-GW, which is beyond the control of the SCM and this study. This is something the operator must decide according to the LTE deployment envisaged.

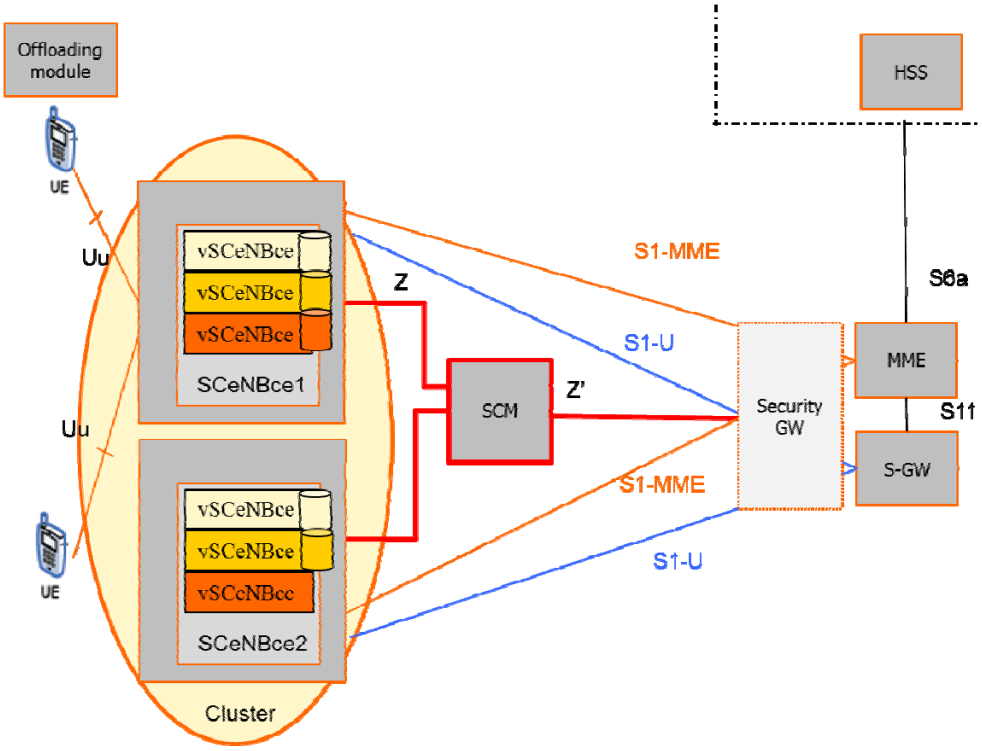


Figure 21. Option 4: In-cloud Standalone SCM without HENB-GW

5.2.4.2 Evaluation

The evaluation of this option would be the same as the In-cloud Standalone SCM option with HeNB-GW. The SCM domain would be exactly the same, and the only difference would be that in this case the SCM would be connected directly to the MME instead of be connected to the HeNB-GW. The choice is then up to the operator, depending on his LTE strategy.

	In-cloud Standalone SCM without HeNB-GW
Requirements coverage	Yes, with the limitations explained in this table
Signalling overhead	Medium – the SCM is closest to the UEs and less hops are required, but as standalone, the SCM would need dedicated signalling.
Latency	Low- the SCM is closest to the UEs
Computation/storage performance	Medium–less nodes are available to pool their resources
SCM computational capacity requirements	Low- management of nodes over a small cluster
Cost of deployment and maintenance	High- high amount of standalone SCMs have to be deployed (one per cluster)
Implementation complexity	High- new interfaces required
Impact on current LTE deployments	Low – a new interface between the SCM and the SCeNBce is required
Energy consumption	High – a greater number of consuming nodes are to be deployed

Table 10: Option 4 evaluation

5.2.5 Option 5: Variant 2 - SCM as an extension of the MME

5.2.5.1 Description

The SCM is placed as an additional component at the MME node. The SCM, however, communicates with the SCeNBce through a dedicated interface and not through the S1-MME interface. Since the number of MMEs is smaller than the number of HeNB-GWs for an operator, the number of required SCM is smaller than in Option 1 and the number of SCeNBcemanaged by one SCM is greater, which increases computing and storage capabilities.

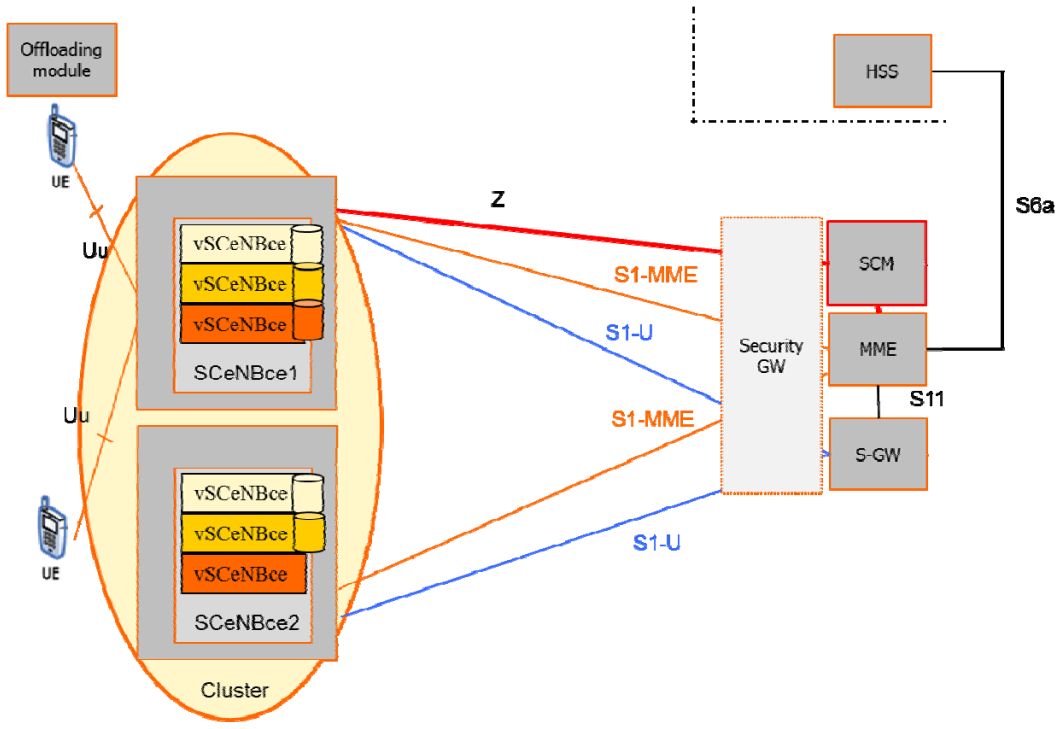


Figure 22. Option 5: SCM as an extension of the MME

5.2.5.2 Evaluation

	In-cloud Standalone SCM without HeNB-GW
Requirements coverage	Yes, with the limitations explained in this table
Signalling overhead	Low – If the SCM is integrated in the MME, some signalling may be reused
Latency	High – the SCM is far away from the SCeNBces
Computation/storage performance	High – an MME is related to a high number of SCeNBces
SCM computational capacity requirements	High - an MME is related to a high number of SCeNBces
Cost of deployment and maintenance	Low – less SCM are required (as many as MMEs)
Implementation complexity	Low - one interface between the SCM and the MMEis required unless they are merged(in this case only and internal interface would be needed)
Impact on current LTE deployments	Low – in internal interface with the MME is required
Energy consumption	Low – very few SCMs are required

Table 11: Option 5 evaluation

5.2.6 Option 6: Variant 3 - SCM as an extension of the HeNB-GW

5.2.6.1 Description

In this option the SCM is placed at the HeNB-GW, either as an additional component or as a new element in the gateway itself. The only difference between this option and option 1 is the fact that the HeNB-GW is only used for signalling.

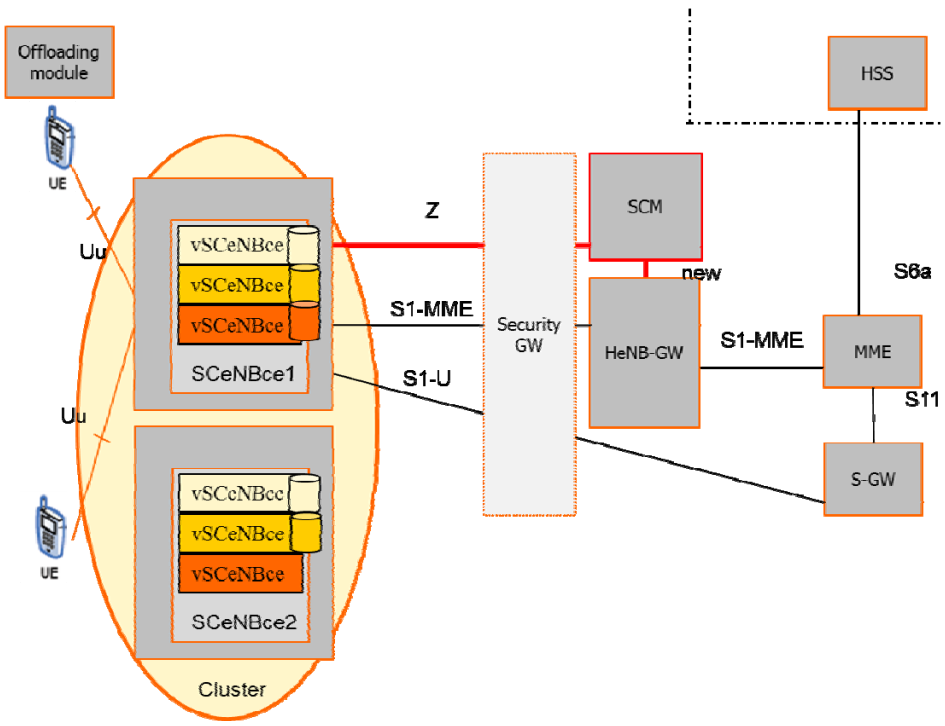


Figure 23. Option 6: SCM as an extension of the HeNB-GW

5.2.6.2 Evaluation

This option is very similar to Option 1. The differences between them are those explained in section 3.3 and do not differ as far as the introduction of the SCM is concerned.

	SCM as an extension of the HeNB-GW
Requirements coverage	Yes, with the limitations explained in this table
Signalling overhead	Low – If the SCM integrated in HeNB-GW, it could utilize some of the signalling sent from and to the gateway.
Latency	Medium- the SCM is closest to the UEs
Computation/storage performance	Medium- only nodes under a single HeNB-GW are available to pool their resources
SCM computational capacity requirements	Medium- management of nodes over a small cluster
Cost of deployment and maintenance	High- a high amount of SCMs have to be deployed (one per HeNB-GW)
Implementation complexity	Low- if the SCM is part of the HeNB-GW, less interfaces required and even less/none if the SCM is an integrated part of the HeNB-GW. In the latter case, the Security-GW also requires modifications
Impact on current LTE deployments	Low - one interface is needed between the SCM and the HeNB-GW. In case they merge, an internal interface would be enough
Energy consumption	Medium- less SCMs entities are required

Table 12: Option 6 evaluation

5.2.7 Option 7: Variant 3 - Standalone SCM

5.2.7.1 Description

In this case the SCM is a new component closer to the computing nodes. The only difference between this option and option 2 is the fact that the HeNB-GW is only used for signalling here. Otherwise, they are identical as far as the introduction of the SCM is concerned.

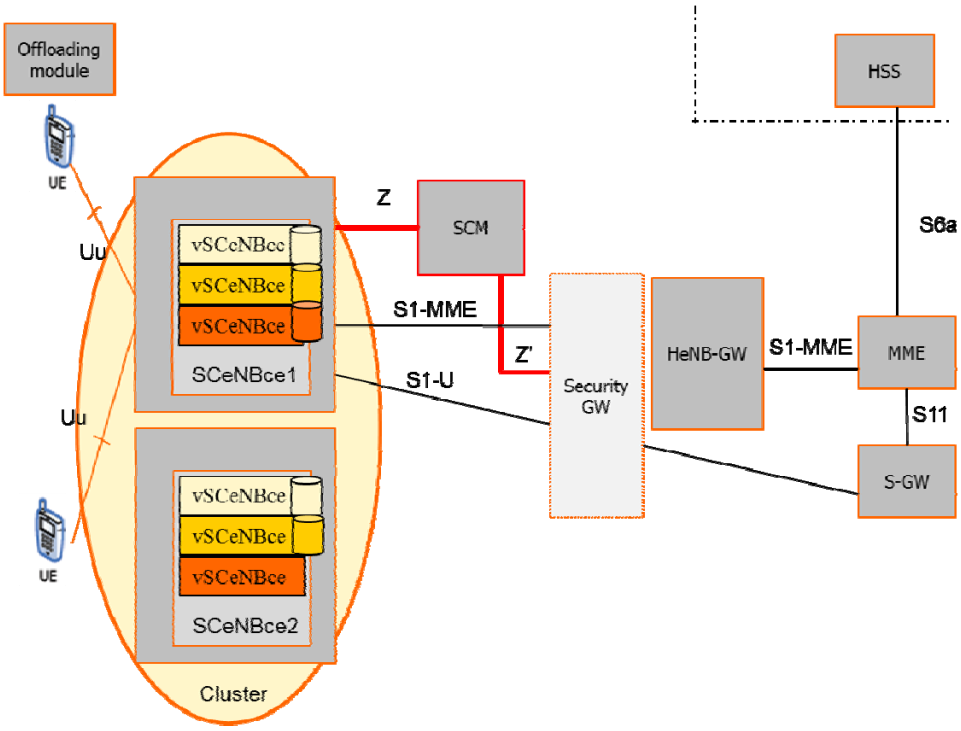


Figure 24. Standalone SCM for variant 3

5.2.7.2 Evaluation

This option identical to Option 2. The differences between them are those explained in section 3.3 and do not differ as far as the introduction of the SCM is concerned.

	Standalone SCM
Requirements coverage	Yes, with the limitations explained in this table
Signalling overhead	Medium – the SCM is closest to the UEs and less hops are required, but as standalone, the SCM would need dedicated signalling.
Latency	Low- the SCM is closest to the UEs
Computation/storage performance	Medium- only nodes under a single HeNB-GW are available to pool their resources
SCM computational capacity requirements	Low- management of nodes over a small cluster
Cost of deployment and maintenance	High- high amount of standalone SCMs have to be deployed (one per cluster)
Implementation complexity	High- New interfaces required
Impact on current LTE deployments	Medium – new interface between SCM and HeNB-GW
Energy consumption	High – a greater number of consuming nodes must be deployed

Table 13: Option 7 evaluation

5.2.8 Comparison of architectures

The architectural options analysed in the previous section need to be compared in order to select the best one for each variant.

However, the comparison needs to take into account that the different criteria cannot be all equally considered. Different stakeholders can consider one of these aspects as critical or not that relevant. For instance, latency is more critical for the end user than for a device manufacturer whereas energy consumption in the network is more important for an operator than for an end-user.

This is why these different criteria have been weighted according to what should be more important for each of these stakeholders and this has been included in the evaluation as a dimension to consider. The following table contains the relevance of each criterion for each stakeholder (♣not relevant,♣♣relevant,♣♣♣very relevant).

	End user	Manufacturer	Operator
Requirements coverage	♣♣♣	♣♣♣	♣♣♣
Signalling overhead	♣	♣♣	♣♣♣
Latency	♣♣♣	♣	♣♣
Computation/storage performance	♣♣♣	♣♣	♣♣
SCM computational capacity requirements	♣	♣♣♣	♣♣
Cost of deployment and maintenance	♣	♣♣♣	♣♣♣
Implementation complexity	♣	♣♣	♣♣♣
Impact on current LTE deployments	♣	♣♣	♣♣♣
Energy consumption	♣	♣♣	♣♣♣

Table 14: Weighted evaluation criteria for different stakeholders

Moreover, for all of the options and variants, the most critical issue would be the bandwidth required in order to reach high performance. It is obvious that the greater the bandwidth, the greater the performance. The greatest constraint is the uplink direction in the case of a DSL backhaul since, in this case, user data should travel from SCeNBces to the SCM. This might increase latency, which is critical for end users according to Table 14. In order to ease this problem, which is explained in section 7, direct Over the Air (OTA) communication among SCeNBces might be considered, as explained in section 9.2.1.

5.2.8.1 Variant 1

The three options analysed for LTE variant 1 have been compared in the following table.

	Option 1	Option 2	Option 3
Requirements coverage	☺	☺	☺
Signalling overhead	☺	😐	☹
Latency	😐	☺	☹
Computation/storage performance	😐	☹	☺
SCM computational capacity requirements	😐	☺	☹
Cost of deployment and maintenance	😐	☹	😐
Implementation complexity	☺	☹	😐
Impact on current LTE	☺	😐	😐

	Option 1	Option 2	Option 3
deployments			
Energy consumption	😐	☹	☺

Table 15: Comparison of architectures for LTE variant 1

Option 1 seems to be the best one when we take all criteria into consideration. However, this solution could have scalability problems, since one HeNB-GW can assemble a great number of SCeNBces. For further considerations please refer to section9.

5.2.8.2 Variant 2

The three options analysed for LTE variant 2 have been compared in the following table.

	Option 4	Option 5
Requirements coverage	☺	☺
Signalling overhead	😐	☺
Latency	☺	☹
Computation/storage performance	☹	☺
SCM computational capacity requirements	☺	☹
Cost of deployment and maintenance	☹	☺
Implementation complexity	☹	☺
Impact on current LTE deployments	😐	☺
Energy consumption	☹	☺

Table 16: Comparison of architectures for LTE variant 2

The analysis points that Option 5 is the most suitable according to the chosen evaluation criteria. However, according to Table 14, this option seems to be very convenient for operators and not so much for end users, since latency is the most critical of the criteria. For further consideration, please refer to section9.

5.2.8.3 Variant 3

The three options analysed for LTE variant 3 have been compared in the following table.

	Option 6	Option 7
Requirements coverage	☺	☺
Signalling overhead	☺	😐
Latency	😐	☺
Computation/storage performance	😐	😐
SCM computational capacity requirements	😐	☺
Cost of deployment and maintenance	☹	☹
Implementation complexity	☺	☹

	Option 6	Option 7
Impact on current LTE deployments	☺	😐
Energy consumption	😐	☹

Table 17: Comparison of architectures for LTE variant 3

The evaluation leads to conclude that Option 6 brings more benefits than Option 7. Again, it depends on the weighted evaluation criteria for different stakeholders whether to choose one or the other. Option 7 offers a better situation in terms of latency in exchange of greater cost for deployment and maintenance, impact on legacy nodes, implementation complexity, etc.

For further consideration, please refer to section9.

5.2.8.4 Conclusions

- One of the objectives of having femto-cloud/smallcell-cloud is to monetize the small cell infrastructure not only as coverage/capacity improvement, but also as revenue generator. SCM module integrated with mobile operator network (Option 1, option 5 and option 7) meet the objective, allowing the operator to control/manage the performance and the business (compared to third party entity like OTT todays).
- In general, the use of a gateway (variant 1 and 3) is mandatory to deal with customer-controlled access points such as femtocells (HeNB). The use of gateway must be considered for residential and SME deployment.
- Option 1 is reasonable to be adopted. In general SCM can be treated as the extension of small cell management system that usually interacts with HeNBs intensively over TR.069. Option 1 has been adopted widely in 3G/LTE femto/pico products. And surely it is applicable for residential, enterprise deployment, assuming femtocell and picocell are referred as small cells.
- In case of residential scenario (femto over xDSL network) placing standalone SCMs (option 2, option 4 and option 7) option in ISP networks are not preferable for MNO, since it is beyond control of MNO, furthermore, since the problem of delay performance exists within last mile access, it won't completely overcome the challenge in xDSL network.
- In case of enterprise, high rise building, public mall, apartment, placing standalone SCM (option 2, option 4 and option 7) in customer building may potentially improve the latency (SCM communication), reduce the signalling overhead coming to the MNO core network. Given that, the SCM is still under control of MNO. The standalone SCM for enterprise customer has a potential implementation, as proposed in section 8.1.
- The use of variant 2 (option 5) can be considered for metrocell and microcell deployments. If we are referring to femtocell and picocell, most vendors adopt the use of a gateway (Smallcell Gateway).
- The mapping between scenarios and architecture options could be like this:

  - Residential scenario: Option 1.
  - Entreprise scenarios: Option 1, Option 2 (provided that the latency between SCM-SCeNBs is acceptable).
  - Public indoor scenario: Option 1, Option 2, Option 5 (if microcells are considered).

6 ARCHITECTURAL ASPECTS FOR SEVERAL CLUSTERS

So far we just have considered the case in which only one cluster of SCeNBces is present. However, we alsostudy the case with two or more clusters are interconnected because this scenario could be used to combine resources of different clusters for greater computation and storage capabilities or even for bursting and offloading. For example, when cluster resources are overloaded, the SCM could burst the application or offload some tasks to interconnected clusters. That would be performed according to established policies and it would be controlled by the SCM of each cluster.Each cluster is managed by a different SCM, which must inter-communicate in order to distribute and run applications across different clusters and provide greater cloud capabilities to end users.

In inter-cluster communications, SCMs must communicate in order to elastically extend the offloaded tasks from one cluster to another. The SCM of the source cluster must take the decision of offloading a certain task. Then, some discovery procedure must be performed in order to find a destination cluster. Finally, the SCM of the destination cluster must deploy the task among the SCeNBces under its domain.

SCM-to-SCM communication depends on the architecture of the small-cell-cloud and the clusters themselves. There are several cases which are described in the following sections. Before going deeper into this analysis, two scenarios must be described for clusters to interoperate.

The first one is the case in which clusters are already interconnected through the operator's core network:

- This sort of clusters would be interconnected by an intermediate point within the EPC. Analysing the EPC components and the LTE standards it is foreseen that the elements that could act as connection points are S-GWs (for supporting handover in the region margin) and MMEs (in this case, only for signalling traffic). That leads to different possibilities, which are explained in the following subsections. It's important to note that current EPCs do not support cloud functionalities and the interconnection of some of the nodes considered in the reminder of this section are not currently supported by LTE standards, which means that new interfaces and functionalities must be defined in order to perform inter-cluster functionalities in those cases.

The second oneis the case of external clusters, which can be interconnected only through the Internet (thus not interconnected by any component of the operator's core network).

- That implies that they are distant clusters that do not share EPC's components. One of the questions that arise when considering this option is what benefits are obtained from the interconnection of those distant clusters. We must wonder whether this possibility is worth or not since there seems to be no difference between an external small cell cloud and an external typical cloud (servers in a server farm or data centre). The latter seems to be more efficient since there is no need to go through the operator's core network for cloud traffic, whereas this is required in case we use an external small cell cluster.

The architectural possibilities are studied for some of the options described in section 5. However, not all options are analysed but only those that leverage from the fact that analogous nodes are interconnected. Besides, for instance, for LTE variant 1 (full HeNB-GW), all possibilities are analysed, since HeNB-GWs are not foreseen to be interconnected according to LTE standards. But in the case of standalone SCM, the case of interconnected S-GWs or MMEs would be preferred over inter-connected HeNB-GWs since they are already foreseen.

6.1 Option 1: Variant 1 - SCM as an extension of the HeNB-GW

6.1.1 Clusters interconnected through operator's core network

6.1.1.1 Interconnected HeNB-GWs

This option is not currently covered by LTE standard (HeNB-GWs are not supposed to intercommunicate). Here, inter-cluster communications could be performed through this HeNB-GW to HeNB-GW interconnection.The following figure depicts the case in which the SCM is in the HeNB-GW (Option 1).

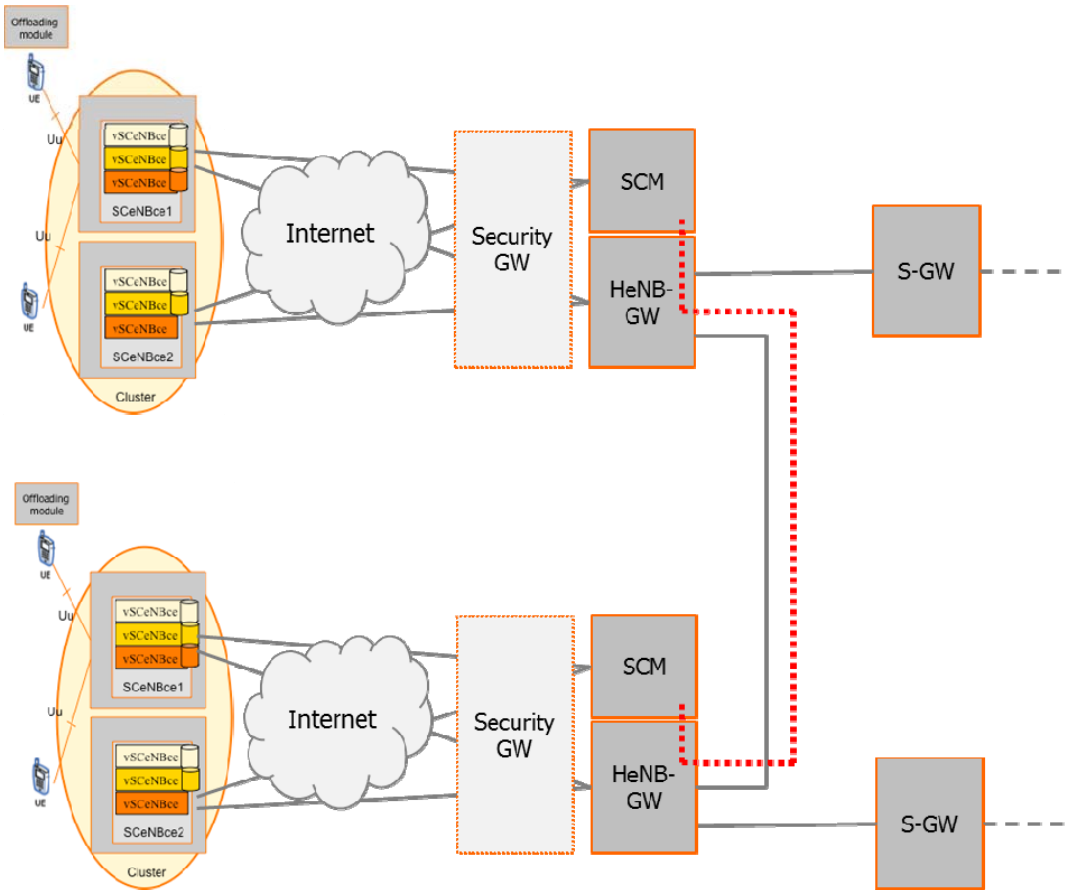


Figure 25.SCM communication for Option 1for interconnected clusters viaHeNB-GW

It is important to note that current HeNB-GWs are not intended for that feature. As they do not support any kind of cloud concept or similar, they are not required to intercommunicate among one another. This option would require modifications in this node and a new interface between HeNB-GWs.

This new interface is intended specifically for SCM to SCM communication. Some protocol must be established so that inter-cluster operations can be carried out. That implies handling signalling and data (control and user plane), since both kinds of messages must be exchanged. For instance, signalling messages among SCMs would prepare the scenario, set the required resources, locations, etc… Data messages would exchange application data, including the offloading tasks, the necessary data, requests, responses, etc.

With interconnected HeNB-GWs, the SCMs can exchange all necessary data as they can interconnect directly by means of the HeNB-GW to HeNB-GW interconnection. They can exchange signalling and user data as long as they are aware of the IP address (or network location) of the other SCM. The

HeNB-GWs would forward messages through the new interface, which will reach the destination SCM.

In this case and, in general, the SCMs must relay signalling data. That means that they are in charge of setting the background of the inter-cluster operation. On the contrary, user data would be relayed through the HeNB-GW and not through the SCM. That means that the user operations, such as task offloading, user data forwarding, etc., can be carried out without going through the SCM. For example, there could be policies to enforce the HeNB-GWs to relay user data among them directly, of course, under the SCM command.

6.1.1.2 Clusters sharing S-GW

Another possible scenario would be that clusters share the same S-GW. In this case, the connections would be carried out through the S-GW, as depicted in the following figure.

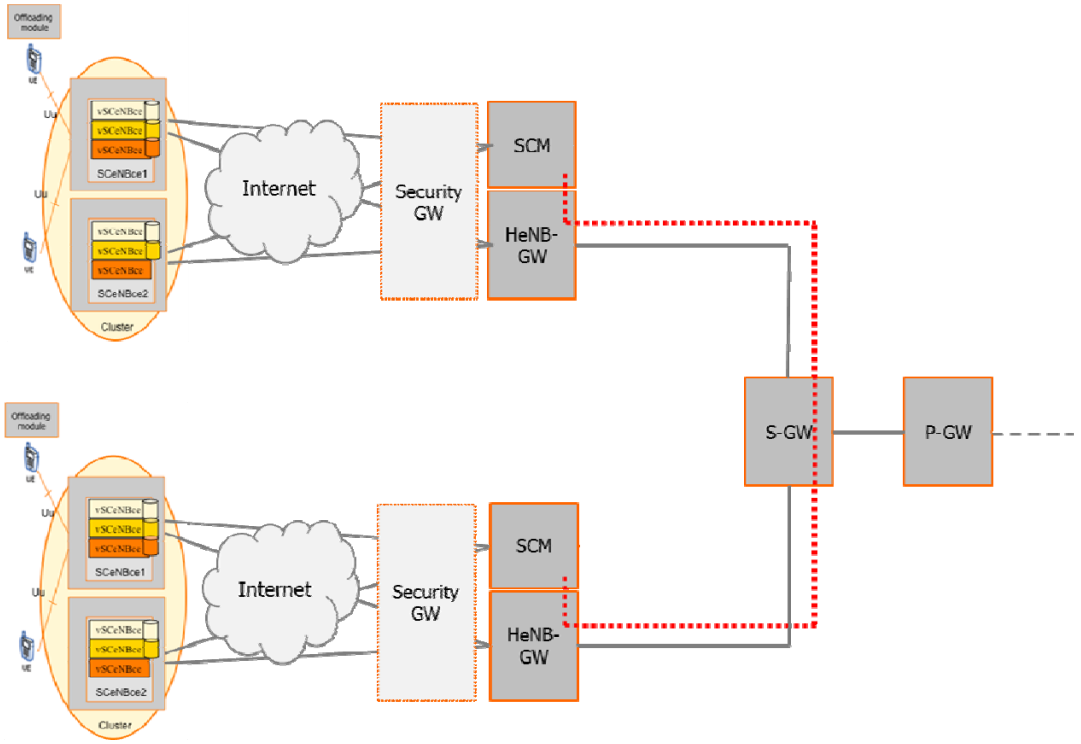


Figure 26.Inter-cluster communication for Option 1for interconnected clusters sharing S-GW

In this option, no new interfaces are needed, since that configuration already exists in the operator's network. Multiple HeNB-GWs can be connected to the same S-GW, as the S-GW is the aggregating node in case several HeNB-GW are present. The needed interfaces are HeNB-GW to S-GW and viceversa, which are already supported by the LTE standard.

In the LTE standard, the HeNB-GW toS-GW interface is the S1-U (S1 for the user plane). That interface passes user plane data while the control plane data is forwarded to the MME through the S1-MME interface. It is important to note that this does not affect the inter-cluster operation. Signalling among SCMs can be delivered through S1-U interface by means of GTP-U tunnelling. On the other hand, user data exchange does not represent a major problem, since it can be delivered through GTP-U tunnelling as foreseen in LTE.

As in the previous case, the SCMs must relay signalling data among them but they may not relay user data as user data can be delivered directly by means of the HeNB-GW and the S-GW without passing through the SCM.

6.1.1.3 Interconnected S-GWs

Wecan also consider the case in which different S-GWs are interconnected, and the inter-cluster communications can be carried out through them. This case is depicted in the figure below.

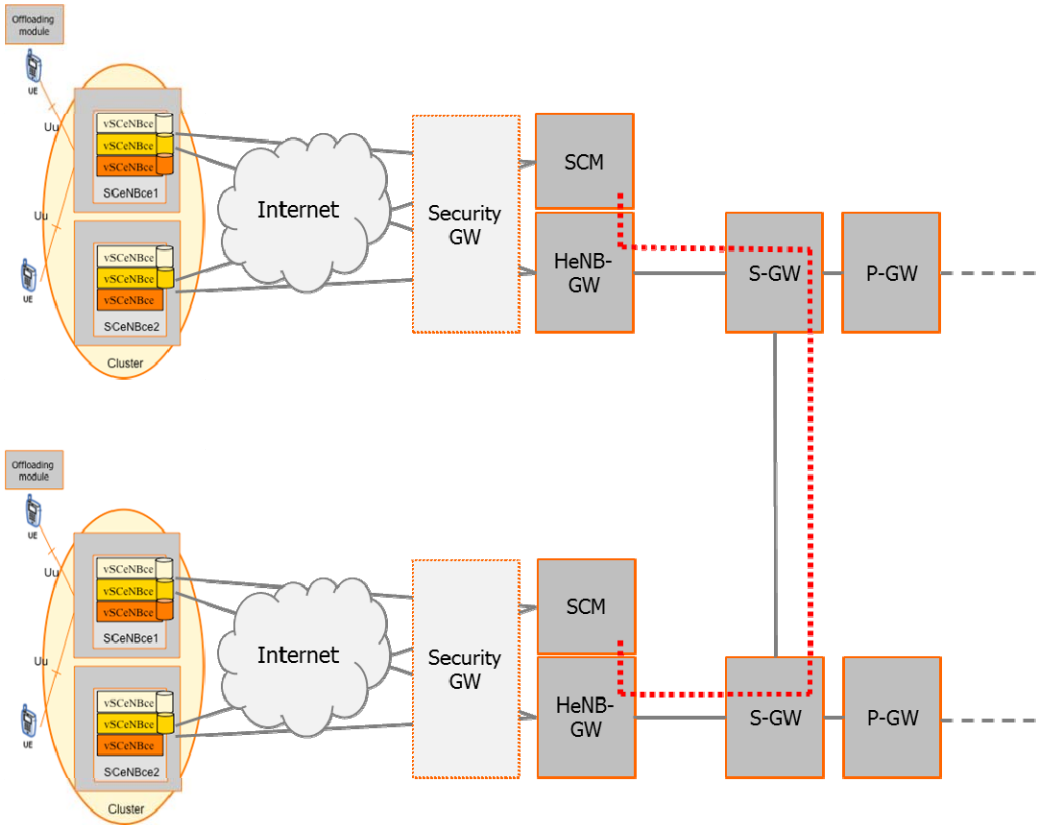


Figure 27. Inter-cluster communication for Option 1for interconnected clusters via S-GW

This possibility is an extension of the previous one.The only difference is that now the interconnection path includes more than one S-GW. The interconnection of several S-GW is already included in current LTE standards since this is required in order to support handovers between different regions. Besides, operators have different nodes for different countries. Therefore, this option is not as costly to deploy as others because no new interfaces between components are required. As inthe previous case, the interfaces of the interconnection path belong to the user plane and forward user data. As signalling among the SCMs is necessary for inter-cluster operations, it can be tunnelled through those interfaces.

6.1.1.4 Interconnected MMEs

In the next case, different MMEs are interconnected and the inter-cluster communications is carried out through them.This case is depicted in the figure below.

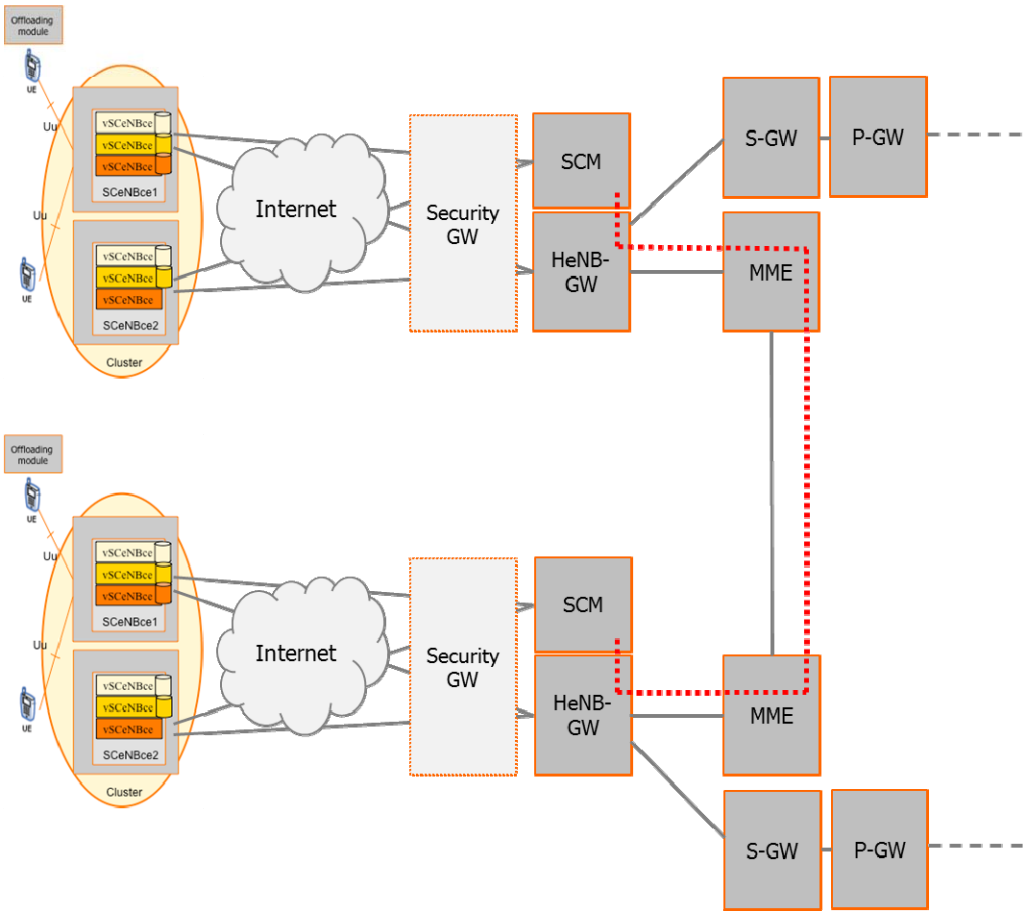


Figure 28. Inter-cluster communication for Option 1for interconnected clusters via MME

In this case some problems arise. Since the MME is the termination of the S1-MME interface for the control plane and no user data reaches this node, the MME would only be capable of dealing with signalling data. That means that the MME -MME interface would be a control plane interface. That represents a problem for the inter-cluster scenario, where both control and user data must be forwarded to the destination cluster. Anyway, we could use that MME-MME interface for signalling among the SCMs, as long as another channel to forward the user data is available, for example, an additional S-GW to S-GW interconnection. But that would be inefficient, sincethe S-GWs interconnection showed in the previous case copes with it all.

The MME is a node the SCM needs direct communication with (and not the S-GW, as explained in section 5). Anyway, the interconnection of MMEs is more suitable for the case presented in Option 5(Section 6.5)than for this one, since in that scenario the SCM is located at the MME itself.

6.1.2 External clusters

At first sight, it seems pointless the interconnection of external small-cell-clusters, but being cautious, we should at least consider and study that option. It could be the operator'schoice, for instance, whether to implement that solution or not.For example, in case the operator prefers to deploy an application (e.g. an online game) in his own premises (clusters) instead of using a hired external cloud.

6.1.2.1 *SCM Interconnection through operator's core network*

In this case, both SCMs are connected through the internet making use of the EPC.

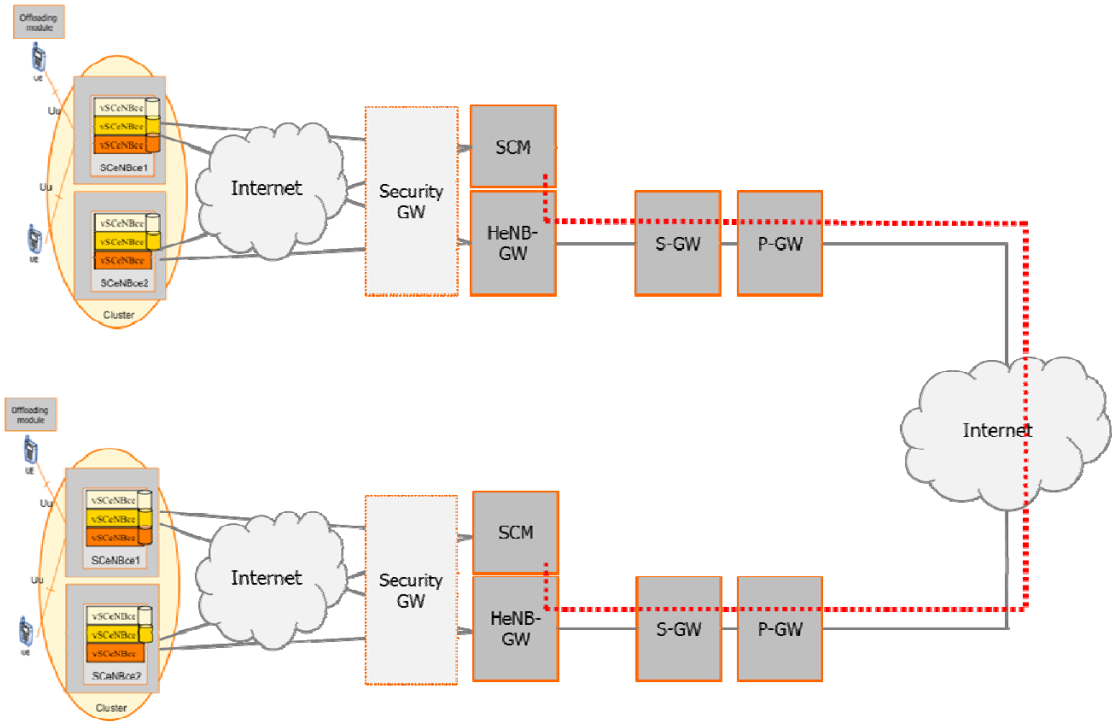


Figure 29.Inter-cluster communication for Option 1 for external clusters with SCM interconnected through the core network

The fact that the SCM interconnection is done via the EPC could be interesting in case the operator requires registering some of this information for accounting or billing purposes. Besides that, this option is not really interesting from a practical point of view unless the operator needs to intercommunicate several clusters for avoiding the use of an external cloud.

6.1.2.2 Direct SCM interconnection through the Internet

In this case, both SCMs are connected through the internet directly.

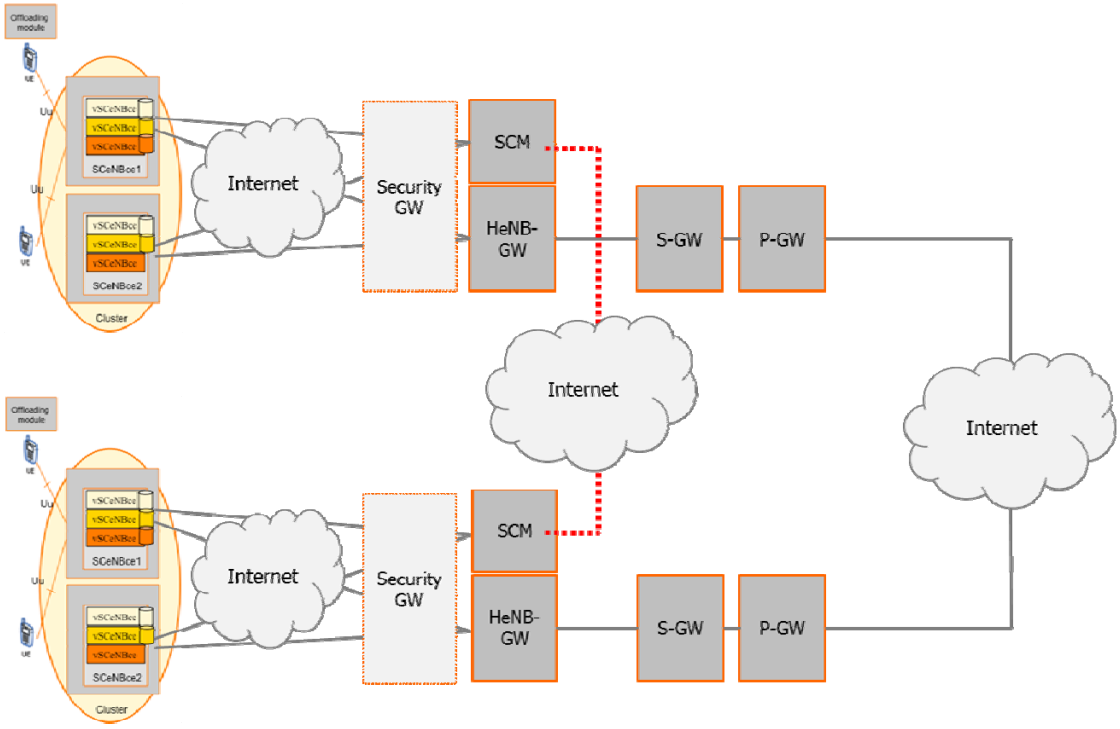


Figure 30.Inter-cluster communication for Option 1 for external clusters with direct SCM interconnection through the internet

This option is not really interesting from a practical point of view unless the operator needs to inter-communicate several clusters for avoiding the use of an external cloud. Following the same argument we used in the precious option, please note that the operator would not be able to control de inter-cluster traffic for accounting or billing purposes.

6.2 Option 2: Variant 1 - In-cloud Standalone SCM

In this case, all possibilities are grouped in the same picture (interconnected and external clusters). Figure 31illustrates this scenario with different possibilities interconnecting analogous nodes. It seems that the best solution is the direct interconnection between the SCMs. Otherwise, additional mechanisms would be required at different LTE nodes in order to route requests from one SCM to another, which would have an impact on legacy systems and would also require a greater number of hops in order to get information from one cluster to another. Besides, direct SCM communication provides the possibility for the operator to easily decide which SCMs can operate with others. This, for instance, canbe useful in the corporate use case in order to combine small cells within the same company but located at different sites.

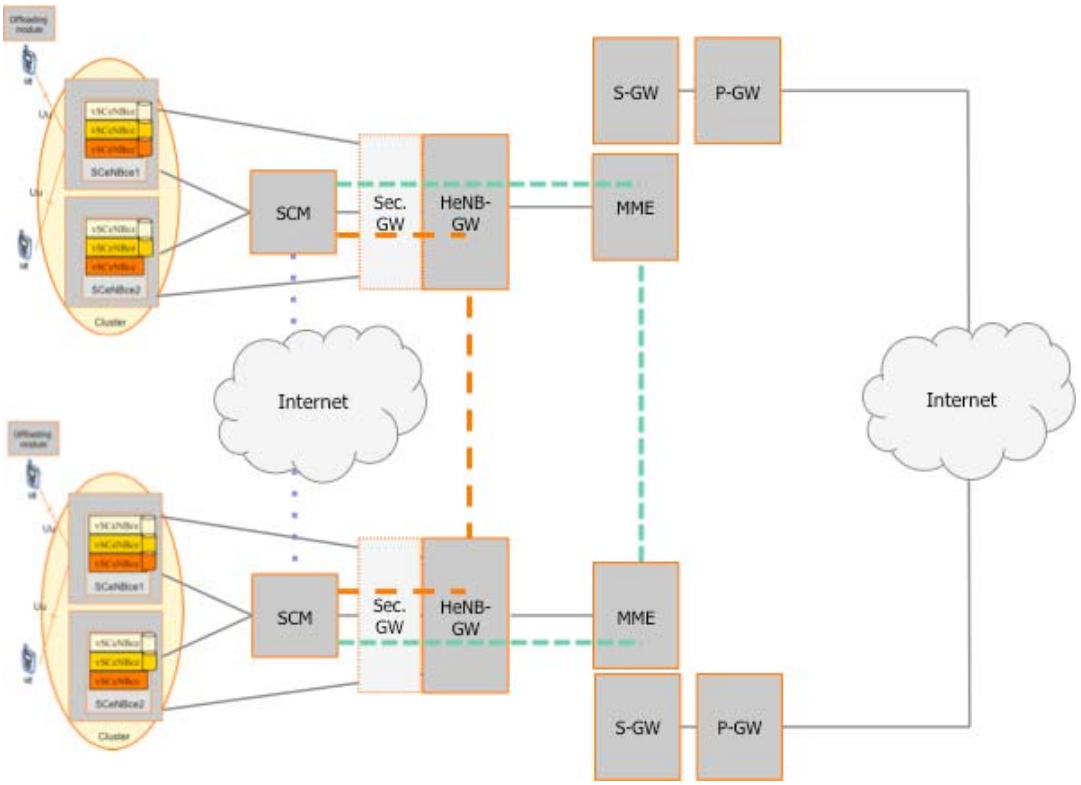


Figure 31.Inter-cluster communication for Option 2 possibilities

Please note that in the previous picture, the case of interconnected S-GW is discarded. The MME-MME communication is more efficient since it leverages from the SCM-MME interface, which is required anyway.

However, as stated before, direct SCM communication does not allow to control theinter-cluster traffic for accounting or billing purposes.

6.3 Option 3:Variant 1 - Standalone SCM

This case, depicted in Figure 32, is identical to the previous one as far as signalling and intercommunicating nodes are concerned. The advantage of this architecture is the fact that one SCM has visibility of a greater number of SCeNBces, which increases computing and storage capabilities to the end-user. In this picture, both interconnected clusters scenario and externals cluster scenarios are depicted together.

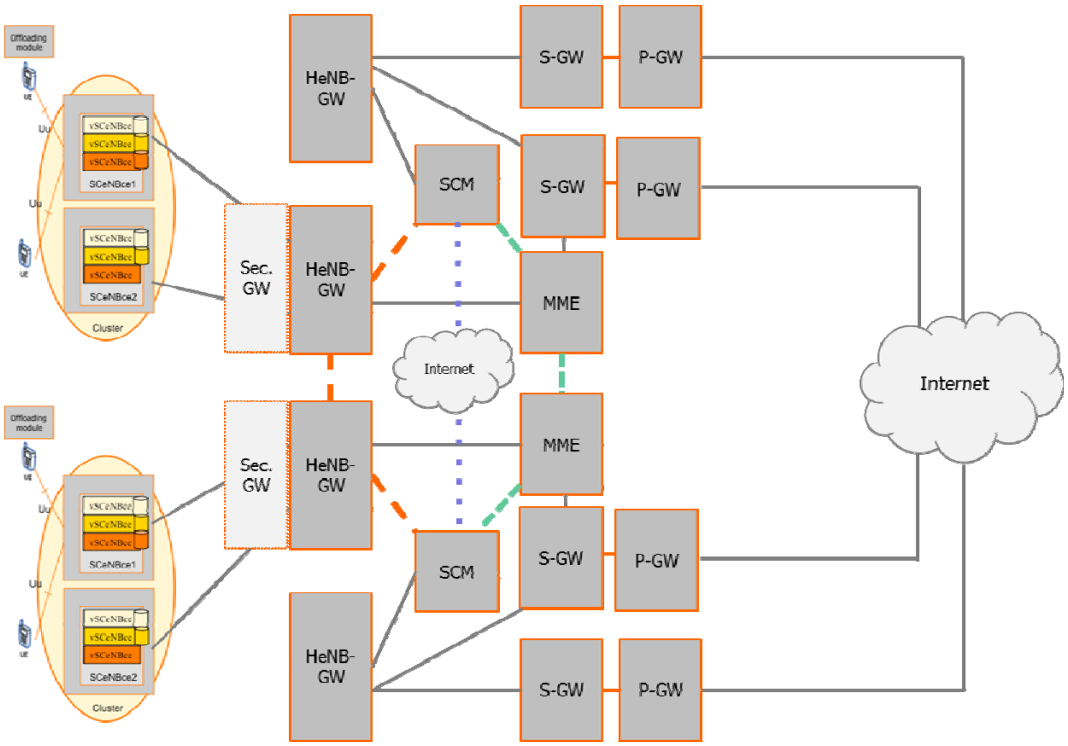


Figure 32. Inter-cluster communication for Option 3 possibilities

6.4 Option 4: Variant 2 - In-cloudStandalone SCM without HENB-GW

If the HeNB-GW is not present, the best possibilities for the SCM to intercommunicate several clusters are to do it through the direct SCM communication or via the MME.

Please note that in Figure 33, the case of interconnected S-GW is discarded because the MME-MME communication is more efficient asit allows leveraging from the SCM-MME interface, which is required anyway. In this picture, both interconnected clusters scenario and externals cluster scenarios are depicted together.

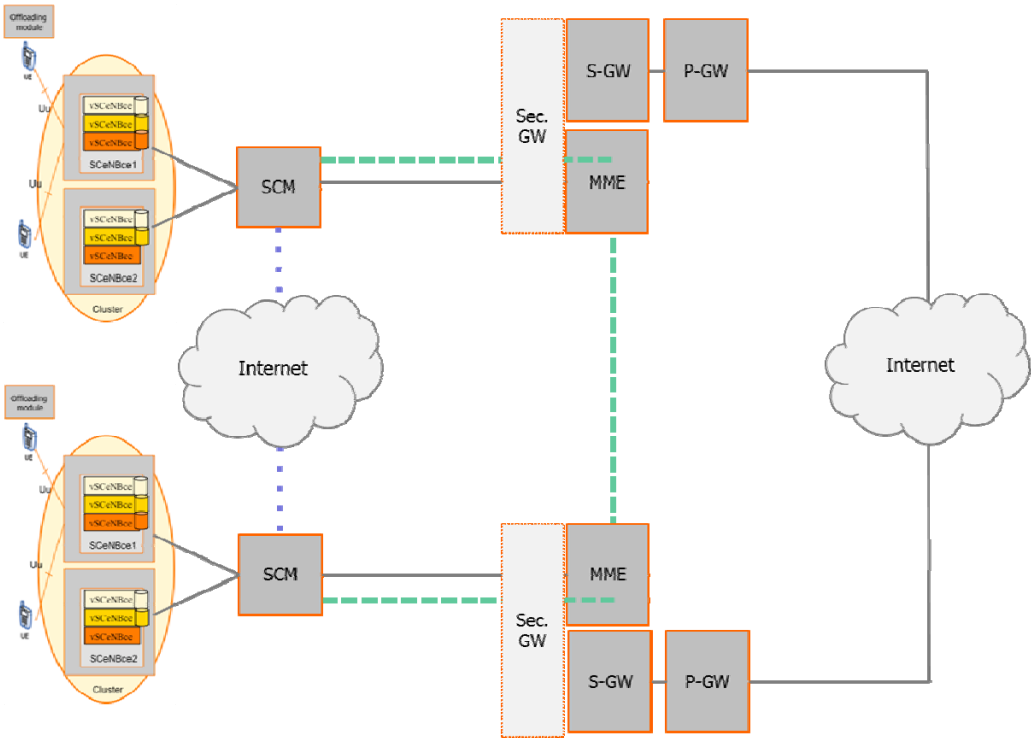


Figure 33. Inter-cluster communication for Option 4 possibilities

6.5 Option 5: Variant 2 - SCM as an extension of the MME

In this case it is obvious that the most interesting option is to have direct inter-communication between the SCMs or leveraging from the MME existing interface considered in the LTE standard.

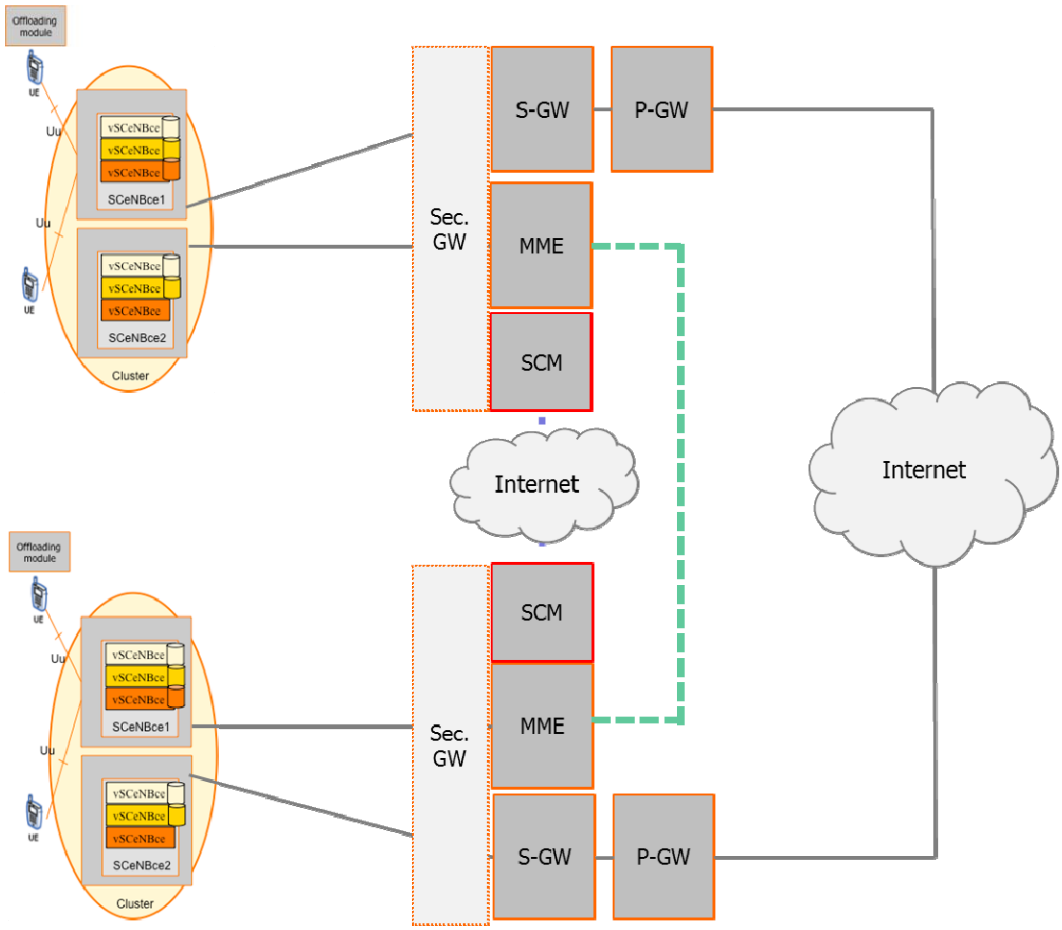


Figure 34. Inter-cluster communication for Option 5 possibilities

6.6 Option 6: Variant 3 - SCM as an extension of the HeNB-GW

This option is identical to the one described in section 6.1. and the same possibilities may be considered with identical conclusion. The only differences relate to the LTE variant.

6.7 Option 7: Variant 3 - Standalone SCM

This option is identical to the one described in section 6.3. and the same possibilities may be considered with identical conclusion. The only differences relate to the LTE variant.

6.8 Conclusions

- SCM intercommunication (inter-cluster) is required if the number of SCM is greater than HeNB-GW or MME. (option 2, option 4 and option 7).If the SCM is placed at the HeNB-GW/MME (in option 1, option 3, option 5 and option 6) the number of SCeNBces managed by the SCM could be high enough so that no inter-clustering would be required (the inter-cluster scenario is aimed to increase computing and storage capabilities).
- If inter-cluster SCM communication is really required, using inter-connected HeNB-GW or through S-GW can be used.

7 SMALL-CELL-CLOUD PROTOCOL (Z-PROTOCOL)

In this section we describe the new small-cell-cloud protocol, named "Z-protocol", which is intended to manage the small cells cloud. This protocol interacts with the new elements introduced by TROPIC, namely the offloading module in the UE, the virtualized HeNBs and the SCM. We provide here a high-level description of the Z-protocol, which will be further developed later on during the project.

This protocol has two main scopes or segments: the UE to SCeNBce communications through the existingUu interface, and the SCeNBce to SCM communications through the new Z-interface.

Z-protocol may be composed of Z-U (user data plane) and Z-C (control plane). The control plane of the Z-protocol is intended to handle signalling messages and carry outcontrol and management operations. For example, when a new SCeNBce is connected, it would notify the SCM of its presence. Another example would be the messages sent from the SCeNBces to allow the SCM to monitor their VMs status. The control plane would also be used to send some kind of control message and control datato the SCeNBces. For example, when a VM is deployed, the control plane sends a message to the destination SCeNBce along with all the necessary data. The control plane would also include the polling operations carried out by the SCM among the SCeNBces. In that case, the SCM would send polling messages to the SCeNBces, waiting for a response in order to find out if it is still active, for example. The control plane would also include all the signalling operations between the offloading module in the UE and the SCeNBces.The user plane of the Z-protocol is intended to handle the application data coming from the UE. The UE sends the request to the SCeNBce, which dispatches the request to the SCM. Upon request, the SCM performs the necessary operations in order to manage it properly and deliver the response within the established policies.

7.1 Uu interface

The new elements introduced in TROPIC that communicate through the Uu interface are the offloading module and the virtualized SCeNBce. Besides, all the applications in the UE use this interface to communicate with the serving SCeNBce.

The new cloud capabilities introduced by TROPIC are not addressed by the current protocols used in LTE over the Uu interface, so this new functionalities must be covered by Z-protocol. In the following we explain the main functionalities covered by Z-protocol regarding the Uu interface.

- The UE (all components including the offloading module) communicates with the SCeNBce and it may:
    - Create communication channels, for the new Z-Interface, with neighbour SCeNBce over the Uu air interface.
    - Gather the internal UE resources, including the battery status.
    - Decide if it is beneficial to off-load an application; the application offload decision should take into account that at relatively short intervals the intermediate results should be made available to UE, for avoiding information loss. The offloading decision depends on several criteria described in section 4.1.1.2. This creates additional traffic which will be a burden for the UE energy consumption.
    - Communicate this decision to the serving SCeNBce.
    - During application execution time, check the quality of the results from the point of view of user satisfaction.
    - If the application is offloaded, re-assess from time to time if it is preferred to continue the off-load as initially defined, to change the offload parameters or to resume the local execution

- As for the SCeNBce, communicating with the UE it may:

    - Dispatch each request coming from the UE and forward it to the SCM for processing.
    - Once the application has finished, send the result back to the SCM. This depends on the application design and where it is finally assembled.

7.2 Z-interface

The Z-interface is a new interface introduced in TROPIC between the SCeNBce and the SCM in the case of standalone-SCM. When the SCM is not stand-alone, the communications will be performed through the existing S1 interface but the Z-protocol would be present anyway.

As the SCM is a new component that is not present in current LTE deployments, all the functionalities covered by Z-protocol are completely new. In the following we explain the main functionalities covered by Z-protocol regarding the Z-interface.

- As for the SCeNBce, communicating with the SCM, it may:

    - Create a secure communication channel for the Z-Interface with the SCM.
    - Wait for further commands from the SCM.
    - Once the SCM has chosen this SCeNBce for application execution, receive the corresponding VM creation request and/or application execution request. This depends on the VM management policy (one VM per user, one VM per application, shared VM, etc.)
    - Communicate periodically to the SCM the status of the VMs and resources status.
    - During execution, wait for commands coming from the SCM (in case the application needs to be taken to another SCeNBce (in case another application is requested, etc.)

- The SCM, in communication with all SCeNBces in the cluster, may:

    - Receive the request coming from the serving SCeNBce.
    - Identify the application deployment strategy and resources required. This depends on the application design. The SCM could have an application repository or catalogue indicating the deployment possibilities for each application so that it can learn the required VM and memory resources for offloading a new application.
    - Select the SCeNBces that will execute the application. The decision should take into account that at relatively short intervals the intermediate results should be made available to UE, for avoiding information loss. This creates additional traffic, which will be a burden for the cooperating SCeNBces and will also increase the network interference levels. One of the criteria for selecting a cooperating SCeNBce should be the availability of a good backhaul connection between the serving SCeNBce and the collaborating SCeNBce. The achievable backhaul throughput should be enough for satisfying the Z-U and Z-C data rates.
    - Check from time to time that the executing SCeNBces work normally.
    - Reassess from time to time the offload status and the load of the cooperating SCeNBces.
    - Receive the results as the application ends or exits, releasing the VM and memory resources if required.
    - In case it is required (e.g. one SCeNBce fails or is turned off unexpectedly), perform the necessary actions to move the application running in this SCeNBce to another one, or assess a redeployment strategy. This hand-over can occur due to the radio conditions caused by the UE movement or load balancing or just because a better cell pops-up. Another reason for hand-over is that the available VM and memory

resources are in a different SCeNBce.The application shall be designed such that it can be exited or stopped upon request and the execution context can be saved.

- In case that the collaborating SCeNBces send back a response indicating plain refusal or some degree of refusal, the SCM may try to contact another collaborating SCeNBce. The collaborating SCeNBCes may share the status of availability of their VMs each time that a change is done.
- In situations that an UE has multiple applications running on multiple VMs and the VMs are not located in the same SCeNBce, it is needed to send the application data from the serving SCeNBce to the cooperating SCeNBce and retrieve the results provided by the application from this SCeNBce. In such a case the data in both directions will be sent in a container over the Z interface.

8 COMMUNICATION BETWEEN THE SCENBCE AND THE SCM

In the different architectural options presented in Section 6, the SCM module is placed either in the mobile operator core network or, in most of the stand-alone options, e.g., options 2, 4 and 7, in the IP backhaul. In the first case, the SCM is placed with the other EPC elements behind the Se-GW, which provides authentication of the SCeNBce and secure communication between the SCeNBce and the core network devices such the MME. In the second case, the SCM is located in the IP backhaul, out of the mobile operator core network, and possibly close to the SceNBce it manages for the cloud services. Communications between the SCeNBces and the SCM, and also between the SCM and the network core elements can be accomplished in different ways. We describe different alternatives below. In case the standalone SCM is still under MNO (mobile network operator) domain, it is MNO interest to make sure the security and the backhaul efficiency can be achieved.

8.1 Additional Se-GW

The LTE architecture usesIP backhaul for the secure communications between the SCeNBce and the different network elements. This is accomplished using an IPsec tunnel between the SCeNBce and the Se-GW, which is established during the SCeNBce setup phase [3GPP-TS 32.593]. The placement of the SCM as a standalone component in the IP backhaul, with the main goal to decrease the SCeNBce-SCM network delay, should thus preserve communication authentication and confidentiality among the different devices.

A simple solution would lie in establishing IPSec tunnels between SceNBce and the SCM and between the SCM and the Se-GW. Nevertheless, for the sake of generality, we consider the adoption of an additional security gateway Se-GW2, to be placed in front of the SCM as shown in Figure 35. After successful mutual authentication between the SceNBce and the Se-GW2, the Se-GW2 connects the SCeNBce to SCM. Any connection between the SCeNBce and the SCM is tunneled through Se-GW2. In addition, the Se-GW2 authenticates itself with the Se-GW, after which it connects the SCM to the operator core network. Connections between the SCM and the core network are tunneled through Se-GW2. The IPSec tunnel between Se-GW2 and Se-GW thus extends the private mobile core network to include the SCM (which thus must be initialized with a core network IP address). We believe that this approach is quite general and can easily accommodate a more general solution whereby several different mobile core network elements are distributed among different physical locations which require the IP backhaul for connectivity.

The solution described is based on theInternet Key Exchange protocol v2 (IKEv2) [IETF01], which is used to dynamically establish a shared state between the source and the sink of IP datagrams in IPsec.

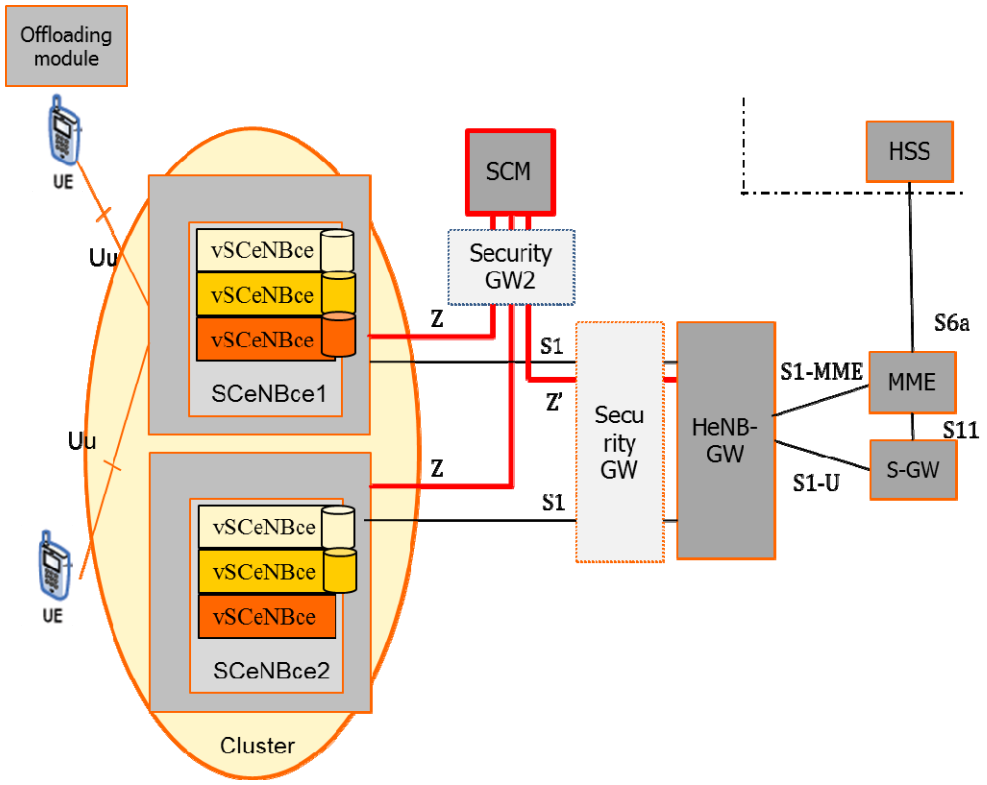


Figure 35. Standalone SCM connected via a Se-GW2.

The protocol stack of Se-GW2 and its interaction with the SCeNBce and the Se-GW2 follows directly from those of Se-GW, see, e.g., [3GPP-TS29.139, 3GPP-TS33.320]. Secure communications is ensured by IPSec over UDP, which allows IPSec to traverse the home router NAT (NAT-T) [RFC3947, RFC3948, RFC5996]. The protocol stack, which is identical to the one of Se-GW, is depicted from 36 to 39 (taken from [3GPP-TS29.139]). Similar protocol stack for the Se-GW2-Se-GW interactions is gathered. In this case, though, there is no intermediate NAT router.

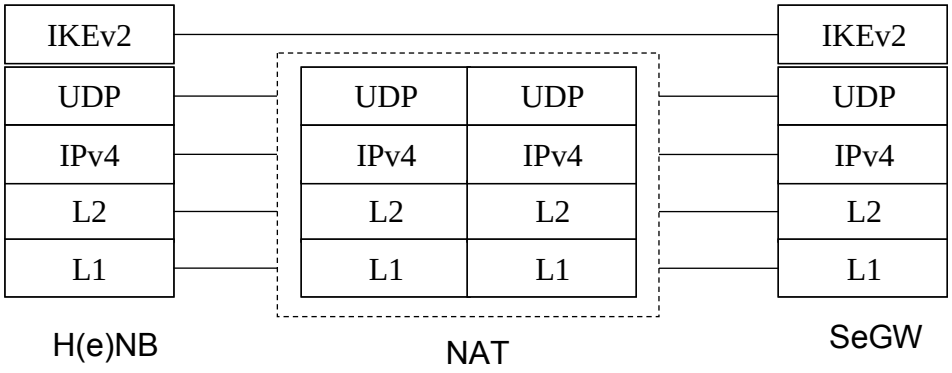


Figure 36. Control Plane for SCeNBce- Se-GW2 Interface over IPv4.

Figure 37. Control Plane for SCeNBce- Se-GW2 Interface over IPv6

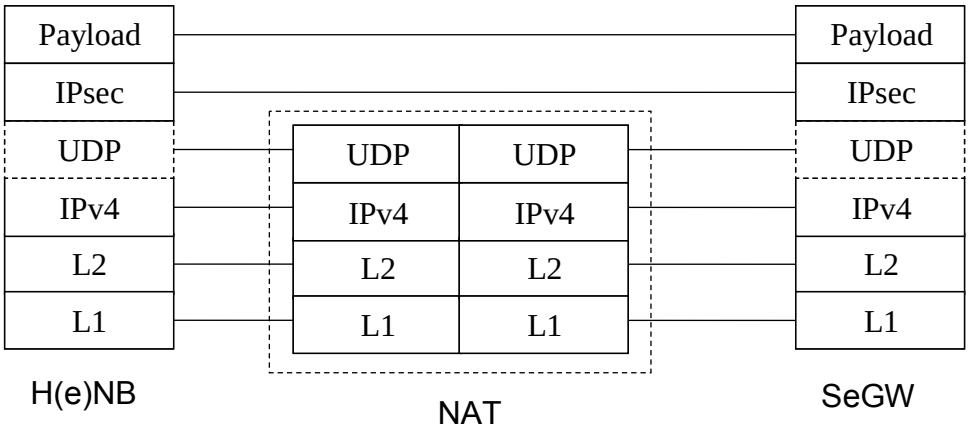


Figure 38. User Plane for SCeNBce- Se-GW2 Interface over IPv4

Figure 39. User Plane for SCeNBce- Se-GW2 Interface over IPv6.

If we turn our attention to the SCeNBce, it is worth observing that the SCeNBce needs to establish two IPSec tunnels (Figure 35), one with the Se-GW and one with Se-GW2 following similar procedures. The S1 and S5 interface (the latter not in the figure) will be tunneled in the IPSec tunnel with the Se-GW, while the new Z-interface will be tunneled in the SCeNBce-Se-GW2 tunnel. This poses no problem under IPv6. For IPv4, this can be handled by IPSec over UDP which allows the secure tunnel to traverse the NAT by having the SCeNBce encapsulating IPSec traffic in UDP datagrams (port 4500).

Moreover, given the additional computational and bandwidth overhead associated with the use of the additional IPSec tunnels, we will need to investigate the performance degradation to ensure it does not offset the benefits associated to the presence of a close by SCM.

Finally, as described in section 6, the standalone SCM deployment is only interesting in the case of corporate scenarios. Spider Cloud [Spidercloud] proposes the implementation shown in the picture below:

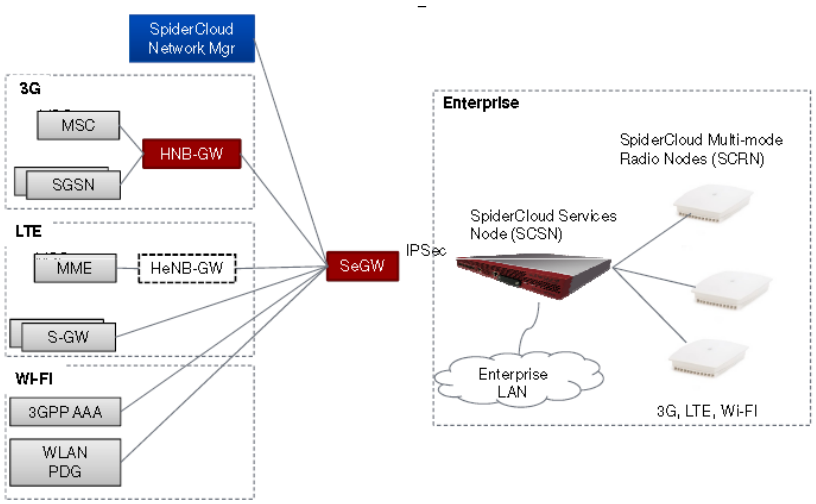


Figure 40. Spider Cloud implementation for the corporate use case with standalone SCM

In this case, Spider Cloud introduces the SCSN (Spider Cloud Services Node), which allows to massively decrease the amount of backhaul bandwidth and offload the signalling overhead from the mobile core network. Furthermore, this solutions involves a single IPSec connection into MNO core (compared to multiple IPSec from individual small cells, which consume backhaul bandwidth). By placing the SCSN (as an intermediate gateway for enterprise customer, with 50-5000 employees), the access to enterprise data is still controlled by multifactor authentication and also use simplified robust self-organised network.

It can be seen that placing the SCM in the enterprise allows the control of the MNO, provide tight security control with minimum signalling overhead, hence backhaul efficiency can be achieved.

8.2 Local IPAccess (LIPA)

The LIPA function (please refer to section 3.2) enables IP capable devices connected via a HeNB to access other IP capable entities in the same residential/enterprise IP network without the user plane traversing the mobile operator's network except HeNB subsystem. In addition, Section 4.3 in [3GPP-TR23.829] states that if the home based network provides a route to other private networks or to the public internet, then these networks may be accessible via LIPA. The required functionalities are provided by the Local GW (L-GW) that in release 10 is located in the SCeNBce subsystem [3GPP-TR23.829].

In TROPIC, we assume that LIPA does provide access to the public Internet. This allows the UE and the SCeNBce to access the Internet directly without traversing the operator network. Hence, in addition to the solution described in the previous subsection, the SCeNBce can also communicate with the SCM when it is placed in the backhaul using LIPA. This solution works in case described above where the SCM is behind Se-GW2 (which has a public IP address), or if the SCM is directly accessible without a Se-GW2. The main difference from the solution described in section 8.1, is that SceNBce-SCM traffic needs to traverse the L-GW (at least logically since in release 10 it is co-located

with the SCeNBce). Secure communication is again ensured by IPSec over UDP since the L_GW traffic still need to traverse the home network NAT which require encapsulation of IPSec over UDP.

9 FURTHER CONSIDERATIONS AND STUDIES

This section gathers possible further studies that could be beneficial for the overall operation of the SCM. These ideas have arisen during the study of architectural options of the SCM in the framework of LTE. We discuss uplink performance limitations and advanced SCM placement and operation.

9.1 Considerations for the uplink performance in TROPIC

TROPIC has mostly considered a DSL backhaul in this document. That makes sense, since long as the small-cell-cloud is deployed in residential or corporate scenarios where a DSL infrastructure already exists and thus it is a very likely case.

ADSL is intended to provide high downstream rate, while the upstream rate is kept low. The ADSL uplink represents a limitation in several cases. For example, we can observe this when attaching a heavy photo to an email, or uploading a video to the Internet. In these cases we can observe a huge delay, which is caused by the low upstream rate. The following table [adsl-rates] shows the downstream and upstream rates for the different versions of ADSL in the market.

	Downstream rate	Upstream rate
ADSL	12 Mbit/s	1.3 Mbit/s
ADSL2	12 Mbit/s	1.3 – 3.5 Mbit/s
ADSL2+	24 Mbit/s	1.1 Mbit/s
ADSL2+M	24 Mbit/s	3.3 Mbit/s

Table 18. Downstream and upstream ADSL rates

As we can see, the upstream rate never goes higher than 3.5 Mbit/s. However, this is a very optimistic rate, since the ADSL rate depends very much on the distance of the link (attenuation issues), and the upstream rate seldom goes higher than 512 Kbit/s.

Indeed, ADSL/ADSL2/ADSL2+ (ITU-T G.992.1, G.992.2, G.992.3, G.992.4, G.992.5) operate with theoretical uplink speed less than 2Mbit/s on physical layer. Standards ITU-T G922.5 Annex M or G992.3 Annex J specifies upload speed can reach up to 3,5Mbit/s but most of the countries donot use them. Annex M is being used in Australia; Annex J is used in Germany by Deustche Telecom. Moreover, these theoretical maximum speeds decrease as distance of the ADSL modem from DSLAM increases. This means that most of the DSL lines will not reach these theoretical limits because of the attenuation or noise level on the phone line.

In TROPIC, the SCeNBces are supposed to use the uplink since not only they download traffic from the Internet but they also send traffic to it in case of application offloading. As far as we are concerned by the time this is written, there are no studies which analyse the upstream vs. downstream traffic in small cell deployments. We can assume that is more or less accurate to consider that SCeNBces deal with approximately the same amount of traffic regarding upstream and downstream, since SCeNBces handle voice calls and the applications that are intended to run in the small-cell-cloud involve a similar traffic regarding upstream and downstream. Note that this is an approximation to show that there is no big difference between upstream and downstream traffic and we need a similar capacity for the uplink than the downlink. Obviously, the more the user surfs the Web, download data, consume multimedia, etc., the more downstream traffic the SCeNBce handles, but anyway, a wide uplink is needed.

This uplink overutilization can represent a huge limitation in small-cel-cloud deployment. Uploads from SCeNBces to the small-cell-cloud could be seriously delayed, causing serious trouble to application performance and user experience. This is beyond the scope of TROPIC, since it is an issue intrinsically related to ADSL technology.

We propose two different alternatives for avoiding this problem, explained in the following subsections.

9.1.1 Alternative backhaul technologies

The first alternative is to use additional backhaul infrastructures to solve this problem. xDSL backhaul has high penetration rate in Europe. The problem is not only the uplink but also the line speed subscribed by most of customers, which is still below or equal to 10 Mbps. The following table shows the downstream and upstream rates for different non-ADSL backhaul technologies.

	Downstream rate	Upstream rate
SDSL	14 Mbit/s	14 Mbit/s
VDSL	52 Mbit/s	16 Mbit/s
Optic fibre	Up to several tens/hundreds of GBits/s	
LTE (radio)	300 Mbit/s	75 Mbit/s
HSPA+ (radio)	168 Mbit/s	22 Mbit/s

Table 19. Downstream and Upstream rates for Non-ADSL backhaul

Using any of these technologies as backhaul would diminish the ADSL uplink problem, as they have higher upstream rate, even if they are not very extended today. Optical fibre has been increasingly growing in the past years [OF-stats] and provides very high traffic rates, so it wouldn't entail any uplink limitation. Symmetric Digital Subscriber Line (SDSL) and Very high bit-rate Digital Subscriber Line (VDSL) are an alternative to ADSL which use the subscriber line, but also not very extended. LTE and HSPA+ radio channels provide higher upstream rate that could also be utilized.

Among all the proposed technologies, optical fibre seems to be the most suitable as backhaul technology. If optic fibre is not available and we can only make use of the subscriber line, VDSL or even SDSL backhauls would be appropriate. LTE and HSPA+ do not seem to be suitable if a wired backhaul is feasible. Perhaps in some cases a radio backhaul would seem interesting, but for most residential, enterprise or public deployments, an optic fibre backhaul would fulfil all the small-cell-cloud requirements without introducing any link rate limitations.

9.2 Advanced options for SCM placement

We have analysed different options for placing the SCM in the framework of an LTE network. Besides these alternatives, there are also different ways to implement this new component. The SCM can operate as a centralised element or it can be implemented in a decentralized manner. In the latter case, the SCM functionality would be carried out by distributed SCMs or by the SCeNBces themselves. This section presents several options for decentralised solutions.

9.2.1 Distributed SCM carried out by SCeNBces themselves (D-SCM)

This solution is based on the radio neighbourhood. It can use wired or combined wired and Over the Air communication in order to avoid the use of the limiting DSL uplink. The distributed approach for the SCM allows for greater scalability and lesser cost. In this subsection, SCeNBce includes both HeNB and low power SCeNBs (both can be connected to DSL backhaul).

There are few basic concepts which constitute the basics of this solution:

- UE-centric radio neighbourhood;
- UE-centric applications;
- UE-centric mobility;
- UE-centric energy availability;

- Embedded security of the radio communication.

9.2.1.1 Solution Description

The distributed SCM approach is based on small clusters, each cluster containing a number of cooperating SCeNBce. Macro eNBs can be optionally included for radio, especially when the small cluster is formed based on the neighbourhood cells, as seen by the UE.

Each SCeNB includes a SCM-BS, which communicates with its pair part in the UE (SCM-UE) and also with the other SCM-BSs in the cooperative cluster. The control of the femtocloud serving a given UE can reside either in SCeNB or in UE; in the last case the UE can delegate some of its functions to the SCM-BS in the serving eNB.

One SCeNBce may belong to several clusters, based on the UE neighbour list. Figure 41 illustrates this approach. UE1 is served by SCeNB2, but its coverage area allows also the connection with SCeNB1, SCeNB3, SCeNB4 and MeNB8 which are part of its femtocloud. On other side, the same SCeNB1, SCeNB3, SCeNB4 and MeNB8 are part of the UE3 femtocloud, UE3 being served by SCeNB1.

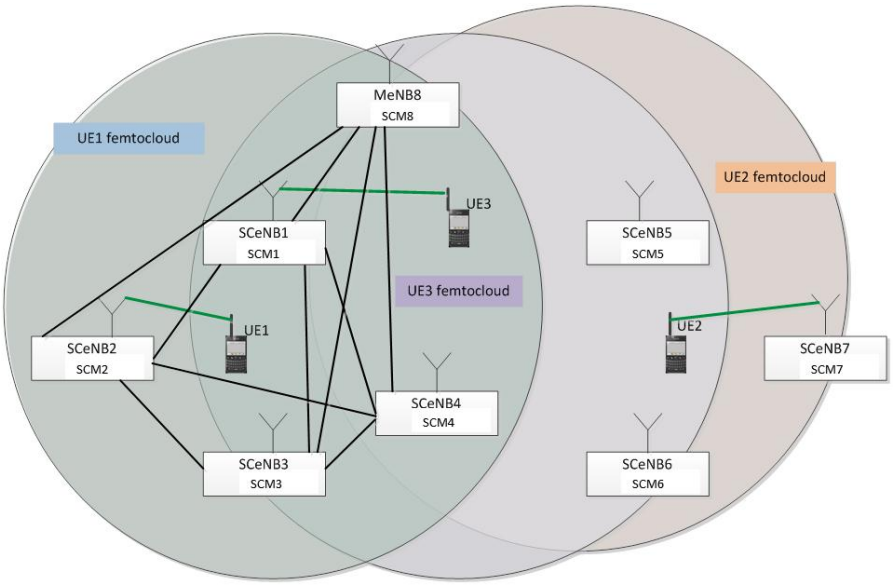


Figure 41. Clusters of collaborating eNBs

In case of mobility support, the list of neighbour eNBs as seen by UE or provisioned by the management system may dynamically change.

The protocol managing the small cell cloud, including the operation of the virtual machines, is named Z-interface, and may have different parts as Z-U (user data part) and Z-C (control part). While the Z-C interface runs between the FCMs, the Z-U interface is transporting regular user data.

The possibility of the UE handover eliminates the need for a SCM playing the role of a dedicated GW in order to switch at least a part of the application traffic to the selected VM, resolving the problems related to the secure communication and placement of the SCM and the additional generated traffic.

9.2.1.2 Intra-system communication

The communication between SCM-UE and SCM-BS is based on the new Z-protocol and takes place over the radio Uu interface. The protocol number of the Z-interface should be different from the assigned numbers of the already existing radio protocols.

The communication between SCM-BSs should also carry a specific protocol number.

The communication between different SCM-BSs takes place either over the backhaul or over the air.

The criteria for selecting the over the air communication is related to the capacity of the uplink eNB backhaul and QoS parameters, such as latency, packet loss and jitter. For example, the DSL backhaul has uplink capacities between 0.25-2Mb/s, which may create traffic congestion and high latency.

In case that the backhaul connection is over a public network, like DSL, it may be needed a secure connection between eNBs. However in practice the eNB address may be local (under NAT) and multiple tunnelled secure connections to a single eNB IP address may not be feasible. Even in case of a single connection a home user is not qualified for adequately programming the home router. In such a case the inter-eNB connection should be over the air (OTA) only. Figure 42 shows full MP-MP inter eNB connections, but eNB3 is connected to eNB4 over a secure wired backhaul, while all the other eNB-eNB connections are over the air. The picture shows only Uu (eBN to UE), X2 (eNB to eNB) and Z protocols communicating over the air, however due to security concerns may be also appropriate the forwarding of those S1 packets not encapsulated over IPSec to an eNB connected by an IPSec tunnel to the Se-GW. In such a case the packets forwarded over the air may carry special identification.

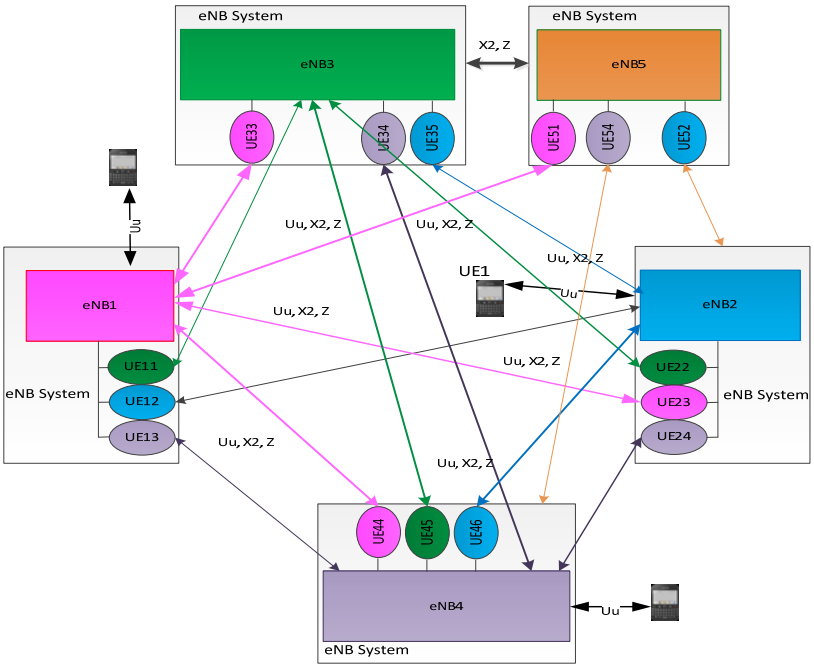


Figure 42. Combined wired and OTA MP-MP eNB communication

9.2.1.3 UE in the D-SCM approach

The minimum functionality of the UE in the D-SCM approach is:

- Create over the Uu air interface communication channels, for the new Z-Interface, with neighbour BSs;
- Gather the internal UE resources, including the battery status;
- Decide if it is beneficial to offload an application; the application offload decision should take into account that at relatively short intervals the intermediate results should be made available to UE, for avoiding information loss. This creates additional traffic which will be a burden for the UE energy consumption.
- Communicate to the serving SCM-BS (SCeNBEce) this decision;

- During offloading, check the quality of the results from the point of view of user satisfaction;
- If the application is offloaded, re-assess from time to time if it is preferred to continue the offload as initially defined, to change the offload parameters or to resume the local execution;
- Check from time to time that the executing SCeNBces work normally

In a more extended functionality, the UE can undertake part of the tasks executed by SCM-BS.

9.2.1.4 SCeNBce in the D-SCM approach

The SCM-BS serving a specific UE is located in the serving eNB. Its main responsibilities are:

- Create secure communication channels for the Z-Interface with the neighbour eNBs, either over the wired medium or alternatively over the air;
- Get from the eNB machine the neighbour eNB list for each UE;
- At VM-UE request learn the required VM and memory resources for offloading a new application;
- Communicate, at VM-UE request, with the collocated eNB machine and the UE-specific neighbour eNBs and get the available VM and memory resources;
- Get over the X2 interface the load indication, including the radio resource reservation, of the candidate SCeNBces.
- Establish if the application is already available on these SCeNBces;
- Decide on which machine should be executed the application offload; the decision should take into account that at relatively short intervals the intermediate results should be made available to UE, for avoiding information loss. This creates additional traffic which will be a burden for the cooperating eNBs and also will increase the network interference levels. One of the criteria for selecting a cooperating SCeNBce which is NOT a candidate for the UE handover to should be the availability of a good backhaul connection between the serving eNB and the collaborating eNB or, alternatively, the availability of the OTA communication between the the serving eNB and the collaborating eNBs. The achievable throughput when using OTA or the wired connection should be enough for satisfying the Z-U and Z-C data rates.
- Seize the VM and the memory resources;
- Check from time to time that the executing SCeNBces work normally;
- Reassess from time to time the offload status and the load of the cooperating eNBs;
- When the application ended or was exited, release the VM and memory resources;
- In case of handover, apply the handover policy rules and store the VM and memory context;
- After the handover is ended and the new VM has been identified, transfer the old VM and memory contexts (over the Z-C interface) to the new SCM which in turn will update the new VM and memory resources.

9.2.2 Hierarchical SCM (H-SCM)

In this section we present asolutionfor backhaul shorter delay. The solution consists on splitting the SCM in a hierarchical manner into two levels: a local SCM (L-SCM) and a centralized SCM (C-SCM). The L-SCM is deployed as close to the users as possible (see Figure 43). Therefore, it manages only a low number of SCeNBces. The provided computation capacity is relatively low (only couple of SCeNBces). However, communication delay between SCeNBces and L-SCM is minimized. If a user requires more computation power than which is offered by SCeNBces controlled by the L-SCM, the request is forwarded to the C-SCM. The C-SCM is located farther from the end users and thus, it implies higher delay. On the other hand, very high computation power is available since a large number of SCeNBces is under control of a C-SCM.

In general, the process of handling the user's request is as follows. First, a UE decides to offload computation to the network (cloud) following the approach described in section 4.1.1. This request is received by the closest L-SCM, which evaluates the request from the delay and computation load point

of view. If the request is of a real time type and requires as low delay as possible, then the L-SCM compares the required computational complexity with resources available at local SCeNBces. If the local SCeNBces are able to satisfy the request, the computation is distributed over these local cells. If either the local SCeNBces are not able to provide sufficient computation capacity or the service does not require low delay (non-real time service), the request is forwarded to the C-SCM. The non real-time request can be computed also at the local SCeNBces when featured with enough computation power. However, the decision whether to compute locally or to forward the request to the C-SCM must be done based on the load of the local SCeNBces and the number of expected incoming requests. Such decision could follow common call admission control procedure used for admission of new users or users performing handover from other cells.

Note that the C-SCM can be deployed in any configuration mentioned in Section5 considering its respective pros and cons.

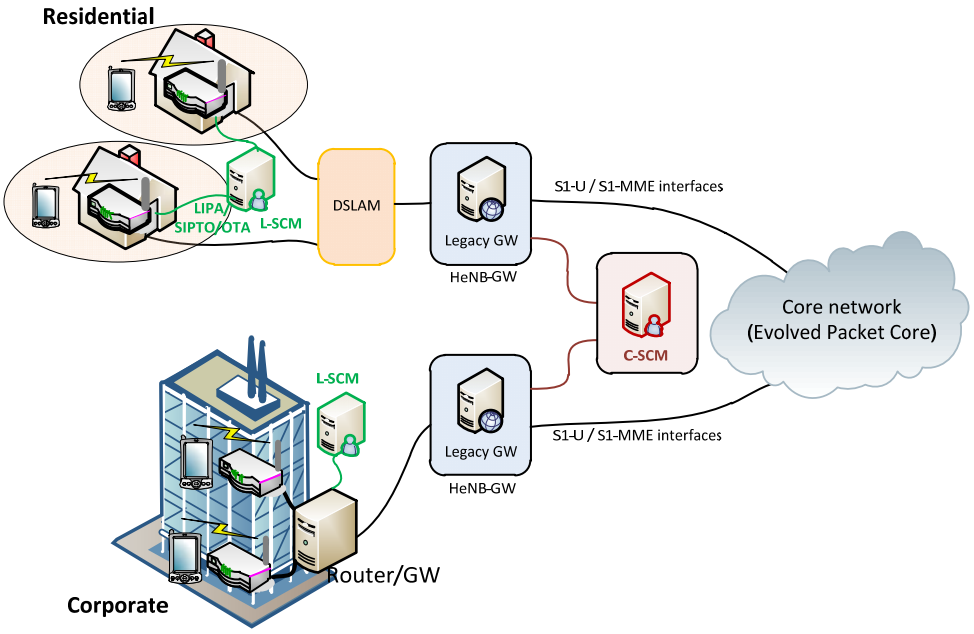


Figure 43. General scenario for H-SCM.

Next, an analysis of deployment of L-SCM is discussed. For this purpose, we distinguish two scenarios: residential and corporate as shown in Figure 43.

9.2.2.1 L-SCM in residential scenarios

In residential scenarios with users spread among houses, the L-SCM must be deployed as close to the users as possible (in terms of communication delay). The physical deployment of the L-SCM can be either at one of the SCeNBces or at a specific separated place. The management information for the L-SCM is routed through a new interface of the SCeNBces. This interface connects the SCeNBces with L-SCM.

The interface can be represented by a wired connection (e.g., an optical fiber) or by the OTA communication among SCeNBces and the L-SCM. A problem of the H-SCM in the residential scenario consists in high the cost implied by the need of communication among SCeNBces and L-SCM. For wired communication, it implies to build up a new infrastructure that connects all entities. This problem is analogical to the physical implementation of the OTA interface (previous section). In case of physical deployment of the L-SCM in an SCeNBces, the OTA interface can be used for the communication among SCeNBces and L-SCM.

9.2.2.2 L-SCM in corporate scenarios

The situation is much less complex for the corporate scenario. In this case, the deployment of L-SCM is assumed at the interference between LAN of the company and the Internet (in Figure 43 shown as a router/GW). As all equipments in the LAN are close to the L-SCM, low delay in communication with L-SCM is experienced by UEs. The L-SCM is connected to a specific port of router/GW and it is deployed in premises of the company.

9.2.3 Virtual Hierarchical SCM (VH-SCM)

An extension of H-SCM can be represented by Virtual H-SCM (VH-SCM). This approach is very similar to the H-SCM with a difference in the implementation of the L-SCM. The L-SCM is not a physical device but a logical function of the selected SCeNBce(s). It is necessary to point out that following scenario is not suitable for residential case or for small cells deployment. As mutual IP connectivity (i.e., broadcast domain) among small cells is required, this scenario cannot be generally applied in smallcells but only for mobile networks with small cells. Moreover, this approach is reasonable only for corporate scenarios with a larger number of SCeNBces deployed in a geographically limited area. Note that this solution can be implemented also locally without need for the C-SCM.

In the corporate scenario, it is not efficient to create an IPsec tunnel from each SceNBce to the SCM located in the core network or elsewhere. It is better to transferthe SCM functionality to a selected SCeNBce. In such scenario, the SCM will not be a physical device but just a logical function of an existing SCeNBce. This new logical function will be denoted as Virtual Local Small cells Cloud Manager (VL-SCM). Operation area of every VL-SCM is restricted to the broadcast domain of used IP based network (e.g., LAN).

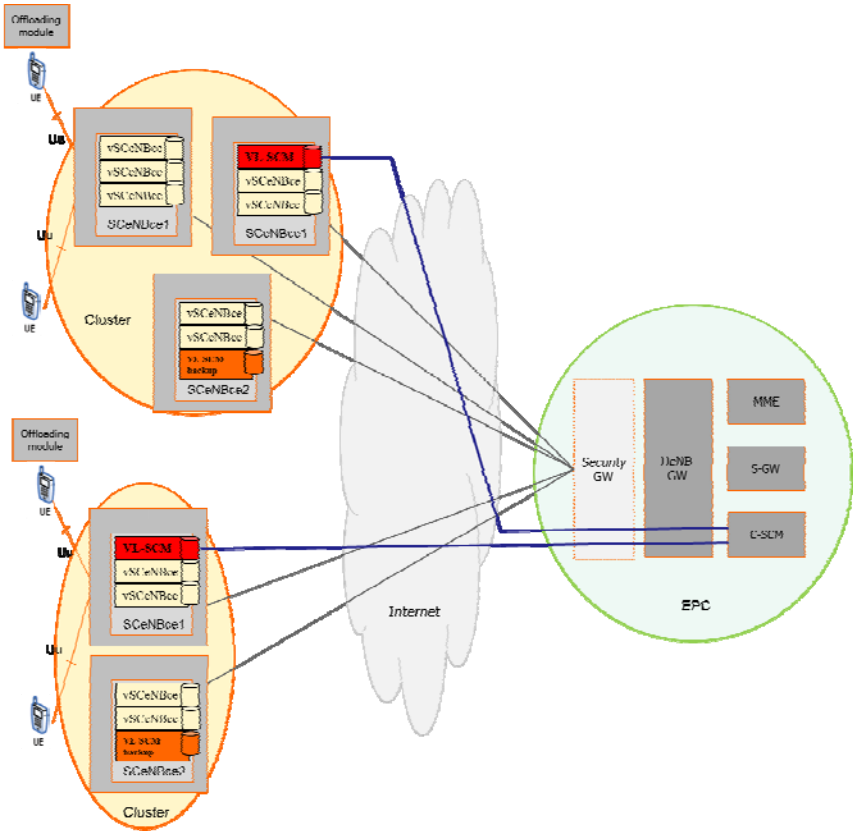


Figure 44. General idea of Virtual Hierarchical SCM.

The process of establishing a VL-SCM can be done in the following steps:

1) Discovery of cells within the same broadcast domain (e.g., LAN).
2) The process of election of the VL-SCM is initiated. The election process is based on a variable denoted as “capability”. A cell with the highest capability is elected as the VL-SCM. The capability is understood as a parameter derived from the following components: computation power, delay in communication with other SCeNBces in the same cluster, IP address, etc. Note that the election process does not make sense if only a very low number of cells in broadcast domain is discovered. In this case, the VH-SCM approach is useless and cannot be applied.
3) The election process results in a selection of one VL-SCM and also one Backup VL-SCM (not shown in Figure 44).
4) The VL-SCM establishes a secure connection to the C-SCM through a Se-GW in the operator core network (EPC). This step is optional and takes place only if C-SCM is required.

After the election process, the VL-SCM distributes work packages to the SCeNBces and it acts as a proxy in communication between the SCeNBce and the C-SCM. Any communication from the SCeNBce to the VL-SCM uses a special multicast address as a destination address. Only the VL-SCM and the Backup VL-SCM listen on this specific address. To handle potential failure of the VL-SCM, any packets from the SCeNBce to the VL-SCM has to be confirmed by the VL-SCM in a time interval T. Otherwise, a failure of the VL-SCM is indicated and the Backup VL-SCM overtakes the management role of and become a new VL-SCM. In parallel, supplementary election of the Backup VL-SCM must be processed.

The Distributed SCM, Hierachical SCM and Virtual Hierarchical SCM are very innovative and beyond state of the art solutions. Some additional study would be required in order to further analyse the feasibility of such solutions, including:

- Computation/storage potential performance
- Computational capacity required in the SCM
- Cost of deployment and maintenance
- Implementation complexity
- Minimal impact on legacy systems

10 CONCLUSIONS

The analysis of different architectural possibilities leads to the conclusion that a telecom operator adopting small-cell-clouding has to consider different aspects before choosing an approach. The criteria to analyse include, among others, the current deployment of the own architecture on which the small-cell cloud will be based (LTE), the approach as far as the applications it is willing to offer, energy-efficiency, the cost, etc.A single deployment model will not suit all operators.Additional architectural possibilities are analysed in the case the operator intends to do small-cell-clouding among different clusters.

The study carried out in this document leads to the following recommendationsconsideringa centralized solution for the architecture:

- In a residential scenario, the best approach is to place the SCM as an extension of the HeNB-GW.
- In corporate scenarios: the best possible approaches are 1) to place the SCM as an extension of the HeNB-GW or 2) to deploy an In-cloud standalone SCM (provided that the latency between SCM-SCeNBs is acceptable).
- In a public indoor scenario: the best possible approaches are 1) to place the SCM as an extension of the HeNB-GW, 2) to deploy an In-cloud standalone SCM (provided that the coordination latency between SCM-SCeNBs are concerned) or 3) SCM as an extension of MME (if microcells are considered).

It is clear, however, that the introduction of the small-cell-cloud paradigm involves a new protocol we denoted as “Z-protocol” that takes place between the UE, the SCeNBce, and the SCM in order to guarantee the operation of the cluster and the service delivery taking into account the radio and cloud situation as far as resources are concerned.

As for the concrete approach to follow in TROPIC, there are several possibilities that need to be evaluated as work in technical workpackages (WP3, WP4, WP5)goes on. Basically, the possibilities include:

- Centralised approaches in which the SCM is a new network element that manages the cluster. This is simpler to implement and it allows the operator a greater control of the applications that run over the cluster, however it implies higher delays.
- Advanced approaches in which the SCM’s features are carried out by in a decentralized way or by the SCeNBces themselves. This seems challenging and its efficiency needs further study, since the dynamic scenario of small-cell-clouding requires the duplication of information across all SCeNBces within the cluster and increased signalling within the cluster. This kind of deployment is initially out of the scope of TROPIC but those options will be also considered in WP3/4/5 in order to study the possibility of performance improvement of specific techniques.

Finally, as for the SCeNBce-SCeNBce communication, the use of the wired backhaul is the priority for the project as this is the most common solution deployed by operators. Nevertheless, as it can cope with the traffic requirements of our use cases, Over the Air communication can be consideredwhen SCeNBces belong to a small cluster and have visibility of one another. It is clear that SCeNBces will always have a backhaul connection to one another. However, TROPIC also proposes that SCeNBces have communication Over The Air. This could be an interesting solution to complement the existing backhaul communication in cases in which, for example, the backhaul condition is bad. OTA communication, obviously, is not always possible since it can only be carried out between SCeNBces that have mutual visibility.

The OTA channel can be used to exchange not only signalling data, but also user data when suitable. The convenience of OTA depends on the cluster's dispersion (e.g., how visible SCeNBces are for one another) and on the backhaul performance compared to the performance achieved by radio channel used for OTA. The SCM can decide when to use one or the other, depending on the destination's visibility, the radio and backhaul channel conditions or the energy required to send the data at a certain moment in time.

11 ANNEX 1: DECENTRALISED VS. CENRALISED APPROACH

TROPIChas analysed different options for placing the SCM in the framework of an LTE network. Besides these alternatives, there are also different ways to implement this new component. The SCM can operate as a centralised element or it can be implemented in a decentralized manner..

One important issue to consider is that the SCM has access to the context vector, which is the entity that stores the overall cluster situation. In the centralized solution, the context vector is stored centrally along with the SCM. In the decentralized solution the context vector storage is distributed among all involved SCMs.

This subsection tries to analyse implementation choice aspects, which both the operators and the manufacturers should consider..

SCM implementation	Distributed/Virtual	Hierarchical	Centralised
Scalability	**Pros**: SCM load is distributed among the SCeNBces, so the attachment of new SCeNBs to the cluster does not affect the overall SCM performance. **Cons**: The context vector should be updated and replicated in a distributed fashion.	**Pros:** SCM load is partly distributed among Central and Local SCMs. The solution is scalable according to the requred computation power. **Cons**: The context vector should be updated and replicated in a distributed fashion.	**Pros**: The context vector keeps light and easy to access/modify. **Cons**: The greater the number of SCeNBces in the cluster, the higher the SCM load. When the number of SCeNBces is too high, the SCM performance is compromised.
Implementation complexity	The SCeNBce would be a more sophisticated component to be built by vendors. The context vector is stored in a distributed fashion, which implies complex distributed storage techniques.	The context vector is stored in a distributed fashion, which implies complex distributed storage techniques.	Easier SCM implementation. Flexibility of placement according to operator's needs.
Operator's control	**Cons**: Less control by the operator. Distributed software is less controllable.	**Pros**: The central SCM can be easily accessed by the operator **Cons**: Local SCM is less controllable by operator.	**Pros**: The SCM can be more easily accessed by the operator. **Cons**: This approach seems to be against current trends (SON).
Energy consumption	Greater for the end user for disctributed SCM; for virtual SCM, the same as in case of the Hierarchical SCM	Slightly increased for the user (not at the UE, only SCeNBce); for the operator the increase is lower than in case of the centralized approach	Greater for the operator
Latency (for the same backhaul condition)	**Pros**: SCeNBces communicate with one another with no intermediate player. Latency depends on SCeNB to SCeNB distance and network conditions.	**Pros:** in case of low computation requirements, the latency is low as only local SCM is in charge. **Cons:** For high computational demanding case, latency is high since central SCM is in charge.	**Cons**: The centralised SCM may cause greater delays since it is an intermediate component. Latency depends on SCeNB to SCM distance and network conditions.
Signalling	**Cons**: Greater signalling	**Pros**: Signalling load is	**Pros**: Less overhead is

SCM implementation	Distributed/Virtual	Hierarchical	Centralised
overhead	for an n-n communication (*) Many SCM instances that must communicate with one another and the SCeNBces. Moreover, context vector replicas must be accessed in a distributed fashion.	smaller than in case of distributed/virtual SCM. **Cons**: Local SCM communicates with central SCM in case of requirement for high computation load.	required for a 1-n communication. Only one SCM instance that communicates with the SCeNBces.
Computing overhead	Computing load in the SCeNBces is increased. SCM is not intended to have great computing load, so this is not an important factor.	SCM computing is on the network. No user resources are used for management computation.	SCM computing is on the network. No user resources are used for management computation.
Storage overhead	**Cons**: Context vector must be stored and replicated in a distributed fashion. It needs more storage capacity and this capacity is provided by user's devices.	**Cons**: The Context vector must be stored and replicated in a distributed fashion; however, it influences neither user's devices nor small cells.	**Pros**: The Context vector needs less storage capacity and do not consume user's storage capacity.

(*) It is important to define the efficiency of resource utilisation in the distributed scenario. Since signalling and context-related storage will be more important in this case at the SCeNBCes, it is interesting to analyse how efficient this approach is by comparing how much resources are dedicated to useful end activity and how much are used for management purposes.

12 ANNEX 2 – IP ADDRESSING ISSUES

TROPIC contemplates a scenario in which a set of SCeNBces managed by a SCM provide computing services to end users. This implies that SCeNBces can be compared to servers. As such, they need to be able to receive requests from the SCM and/or from other SCeNBces.

The objective of this annex is to provide clarifications and possible solutions based on existing technology that TROPIC needs to rely on in order for the SC-cloud to be able to operate.

12.1 NAT Concerns

SCeNBce Behind NAT

If we consider how femtocells are currently deployed (connected to a router that provides a local IP address to these devices), we find several issues that need to be clarified. First of all, as was mentioned in section 3.1, SCeNBces need to be contacted from outside their local network. This has some implications when they are behind a NAT function or the public IP address is dynamic.

When the SCeNBce is placed behind a NAT, the SCM is only aware of the SCeNBce's public IP. In order for the SCM to be able to contact a SCeNBce, IPsec tunnelling is required. Additionally, NAT-T (traversal NAT) is also required in order for IPsec to go through a NAT without losing IP information NAT-T is a method of enabling IPsec-protected IP datagrams to pass through network address translation (NAT) [RFC 3947]. An IP packet is modified while passing through a network address translator device in a manner that is incompatible with Internet Protocol Security (IPsec). NAT-T protects the original IPsec encoded packet by encapsulating it with another layer of UDP and IP headers.

Dynamic Public Address

SCeNBce IP addresses are provided by the ISP. Whenever the public IP is changed by the ISP, the IPsec tunnel will be triggered again. Moreover, as new requests are originated in the SCeNBces or new proactive (originated in the SCeNBce) monitoring events occur, the situation will be recovered.

Note

SCeNBce real (private) IP address is never known to the SCM until the IPsec is established. Since the IPsec tunnel is established between the SeGW and the SCeNBce (which is hidden behind the NAT IP of the Internet router), the SCM is contacted by it after the IPsec tunnel is up.

12.1.1 Simple Design

This section provides detailed overview to proof that Network Address Translation (NAT) is not a problem for femto-cloud design.

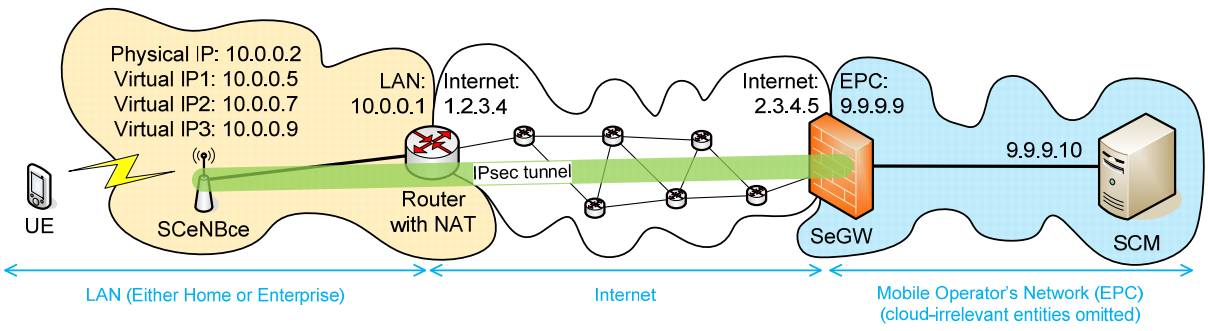


Figure 45. Design example

To make the explanation clear, hypothetical IPv4 addresses were used (see **Figure 45**). The 10.0.0.0/24 IPv4 private address space is taken as per RFC1918 range on purpose (commonly used in today's home/enterprise networks). The rest of the IPv4 addresses are public.

12.1.2 Concern #1 – NAT Is an Obstacle to Establish an IPsec Tunnel

To create an end-to-end connection between the UE and the SCM, the IPsec tunnel needs to be established because the 10.0.0.0 network cannot be routable due to ambiguity (as per RFC1918, more networks can use such IPv4 address space).

Because the SCeNBce is "hidden" behind the Router with NAT and its public IPv4 address (1.2.3.4), the SCeNBce must request the IPsec tunnel negotiation (using NAT-Traversal mechanism). Otherwise, the tunnel will not be established because the SeGW does not know the NAT-T IPv4 address (which is the public IPv4 address of the Router with NAT, i.e. 1.2.3.4).

Considering the IPsec tunnel is established, the SeGW now "knows" how to route traffic to the SCeNBce and its IPv4 address 10.0.0.2 (all traffic to it is routed via the IPsec tunnel).
From the SCM perspective, the SCeNBce private IPv4 address is now available thus both devices can communicate directly.

12.1.3 Concern #2 – Public IPv4 Address Change of the Router with NAT Is an Obstacle to establish an IPsec Tunnel

Because the public IPv4 address of the Router with NAT was not known to the SeGW before the first IPsec establishment message arrived (addressed in Concern #1), the same situation occurs in this case.
Once the public IPv4 address changes, a new request comes to the SeGW. Considering that the credentials match (as they matched in the previous attempt from a different public IPv4 address), a new IPsec tunnel (a pair of security associations (SAs) to be more precise) is successfully established.
Once the new tunnel is established, the SCeNBce is available and its IPv4 private address routable again. This rekeying process is seamless and arranged by the Internet Key Exchange (IKE) protocol. The process itself is quite complex and can be found in section "*1.3 The CREATE_CHILD_SA Exchange*". Generally, the old SA is deleted after the new one is established [RFC5996].

Note
The note tries to clarify the operation of the DHCP. *"Table 2: DHCP messages"* [RFC2131] defines messages which are used by the DHCP. None of them enables the DHCP server to enforce the client to renew its leased IP address. Therefore, there is no way from the server side to get back the leased IP address from the client before the lease expires or the client decides so (DHCPRELEASE). Even though there exist mechanisms to prevent the DHCP address pool exhaustion, also known as the DHCP starvation DoS attacks, (for more details see the section "2.2 Dynamic allocation of network addresses" [RFC2131]), it is impossible to make the client renounce its leased IP address. The RFC4361 and other updates (3396, 5494, and 6842) update the original RFC2131 in the terms of IPv6 environment. However, there is no change in the protocol behaviour.

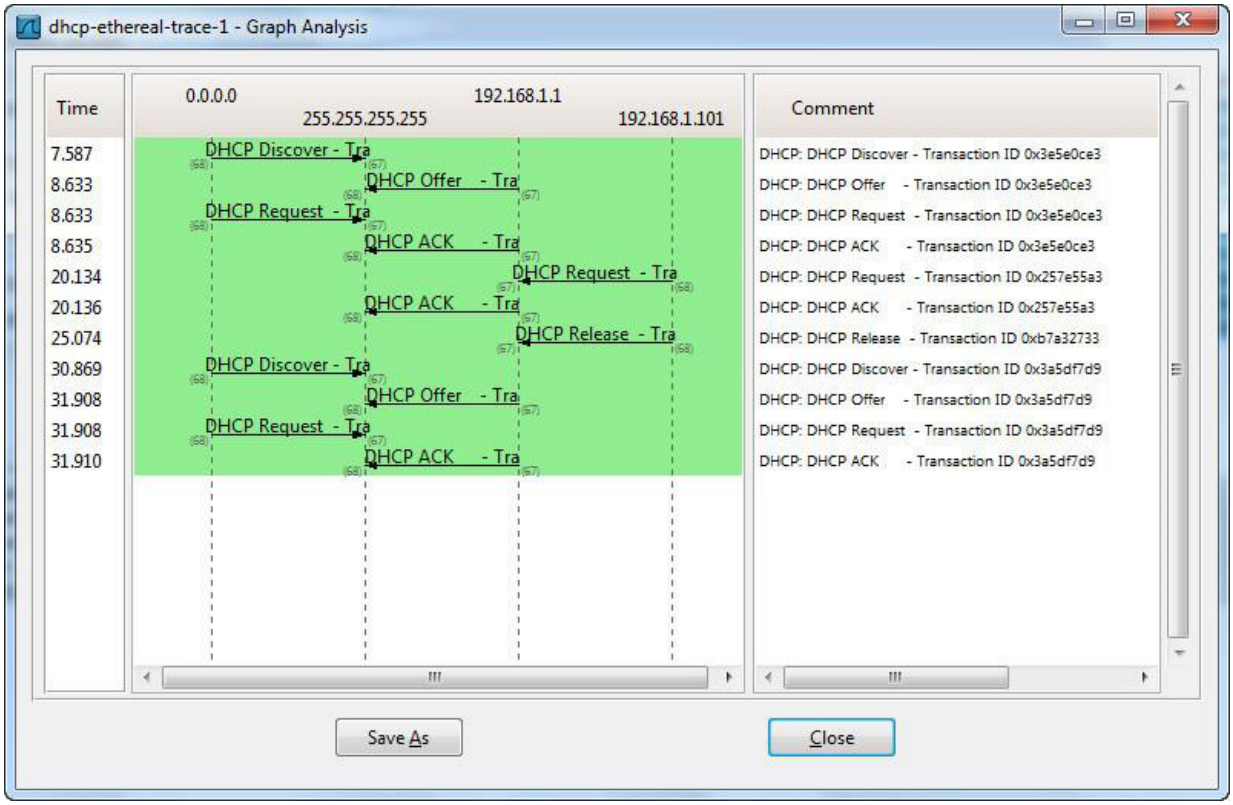


Figure 46. Timing of DHCP Messages

The DHCP client is responsible for renewing its IP address before expiration, and it must stop using the address once the interval has expired, unless it has been allowed to. The process is a little bit complex (see *"4.4.5 Reacquisition and expiration"* [RFC2131]), but generally, the client can reuse the leased IP address once allowed so.

The renegotiation of the leased IP addresses if quite a fast process (see the attached dhcp-capture.jpg file). The renegotiation of the leased address (or negotiation of a new one) takes about one second (see Figure 1). However, the device is still able to communicate as having the former or the newly assigned IP address.

Note
IPv6 introduces Neighbour Discovery Protocol (NDP) which basically enables the devices to communicate without any DHCPv6 server. On the other hand, if required by the environment, DHCPv6 can be used in the same way as the DHCPv4.

12.1.4 Concern #3 – Two SCeNBces Hidden Behind a Different NAT IPv4 Address Require a Direct Mutual Communication

Generally, the SCeNBce can be assigned with a public or private IPv4 address. Assuming the NAT and no protocol/port filtering is applied in the network environment between the SCeNBce and the SeGW, no issue occurs at all. On the other hand, where the SCeNBce is located behind a device applying NAT function, specific measures need to be applied to resolve the direct unavailability (indirect accessibility) of the SCeNBce. Currently, there exists an experimental proposal for IPv6-to-IPv6 Network Prefix Translation[RFC6296]. Therefore, the NAT issue known from IPv4 environment exists with IPv6 as well.

There exists a solution provided by Cisco, Inc. to enable multiple devices located behind NAT (spokes) to establish a secure direct connection using a publicly available device (hub). This solution is referred to as a DMVPN. The overview can be found, for instance, in [DMVPN4].

Such approach can be adopted by the Tropic design as well as the solution is generally based on the commonly available standards (technologies), which are:

- **RFC 1701/1702/2784/2890**: Generic Routing Encapsulation (GRE) and Multipoint GRE
- **RFC 2332/2333**: Next-Hop Resolution Protocol (NHRP)
- Dynamic Routing Protocols:
  - EIGRP (This only is not an IETF standard)
  - **RFC 2453/4822**: Routing Information Protocol (RIPv2)
  - **RFC 2080**: RIP next generation for IPv6 (RIPng)
  - **RFC 2328**: Open Shortest Path First version 2 (OSPFv2)
  - **RFC 5340**: Open Shortest Path First for IPv6 (OSPFv3)
  - **RFC 4271/6286** and **RFC 2545**: A Border Gateway Protocol 4 (BGPv4)
- IPsec encryption (many RFCs):
  - **RFC 4301**: Security Architecture for the Internet Protocol
  - **RFC 4302**: IP Authentication Header
  - **RFC 4303**: IP Encapsulating Security Payload (ESP)
  - **RFC 5996/5998**: Internet Key Exchange Protocol Version 2 (IKEv2)

In spite of the fact, that the DMVPN originally required an IPv4-based WAN network (Internet backbone), nowadays, it can be applied in IPv6-based environment as well [DMVPN6].

Requirements on the Devices

Requirements on the intermediate devices between the SCeNBce and the SeGW, which are switches, routers, and firewalls, are as follows.

1) **Layer two (L2) switches**: There are no requirements, as these devices process only L2 protocol data units (PDUs), i.e. the Ethernet frames.
2) **Layer three (L3) routers/switches**: These are required to have the connectivity related routing information stored in their routing tables when necessary. This means that they need to be informed of the network changes dynamically. This is generally ensured by the Internet service providers (ISPs), thus there is no requirement on them. Or, the routers need to be configured with a default IP route where each IP packet heading to IP destination which is not specified will be routed. The default gateway (an appropriate router of the ISP) is always configured on the Router with NAT, thus there is no requirement on the L3 devices, either.
3) **Firewalls (L4 and above)**: The purpose of these devices is to filter the network traffic. Therefore, our requirement is that these devices do permit communication of protocols ID 50 (ESP), ID 51 (AH), UDP on port 500 (IKE) and UDP on port 4500 (NAT-T).

IP Security

The requirements on the security of the SCeNBce can be adopted from the current 3GPP standard defined in [TS33320], where the Figure A.2 specifies the combined certificate and EAP-AKA-based authentication. The Extensible Authentication Protocol (EAP) Method for Universal Mobile Telecommunications System (UMTS) Authentication and Key Agreement (EAP-AKA) is an authentication mechanism (framework) for authentication and session key distribution using the UMTS Subscriber Identity Module (USIM). EAP-AKA is defined in [RFC4187 and RFC5448].
Unfortunately, the [TS33320] also assumes the public IP address of the HeNB. Most of the current deployments operate with private addressing schemas (as per RFC1918).

SCeNBce Management

Operations, Administration, Maintenance and Provisioning (OAM&P) procedures between the SCeNBce and the SCM can be adopted from the current 3GPP standard defined in [TS32593], where Figure 5-2 specifies the original HeNB registration to the HeNB Management System (HeMS).

12.1.5 Conclusion

From the above, we conclude that from the femto-cloud perspective, there is no problem with the NAT technology. This means there is no problem with the change of the public IPv4 address of the Router with NAT when the dynamically assigned IPv4 address expires and a new one is obtained.

On the other hand, there is indeed a "hidden" problem which is: How to route LANs (SCeNBces) addressed with the same address space? For instance, two networks which are addressed with 10.0.0.0/8 LAN IPv4 range.

The possible solution to the IPv4 overlap is addressed in the next section.

12.2 IP Overlap Challenge

A second interesting issue that must be studied for the feasibility of te TROPIC approach is indeed a "hidden" problem: How to route LANs (SCeNBces) addressed with the same address space? For instance, two networks which are addressed with 10.0.0.0/8 LAN IPv4 range.

This section provides detailed overview to provide a solution for overlapping IPv4 LAN spaces in the femto-cloud design.

12.2.1 Simple Design

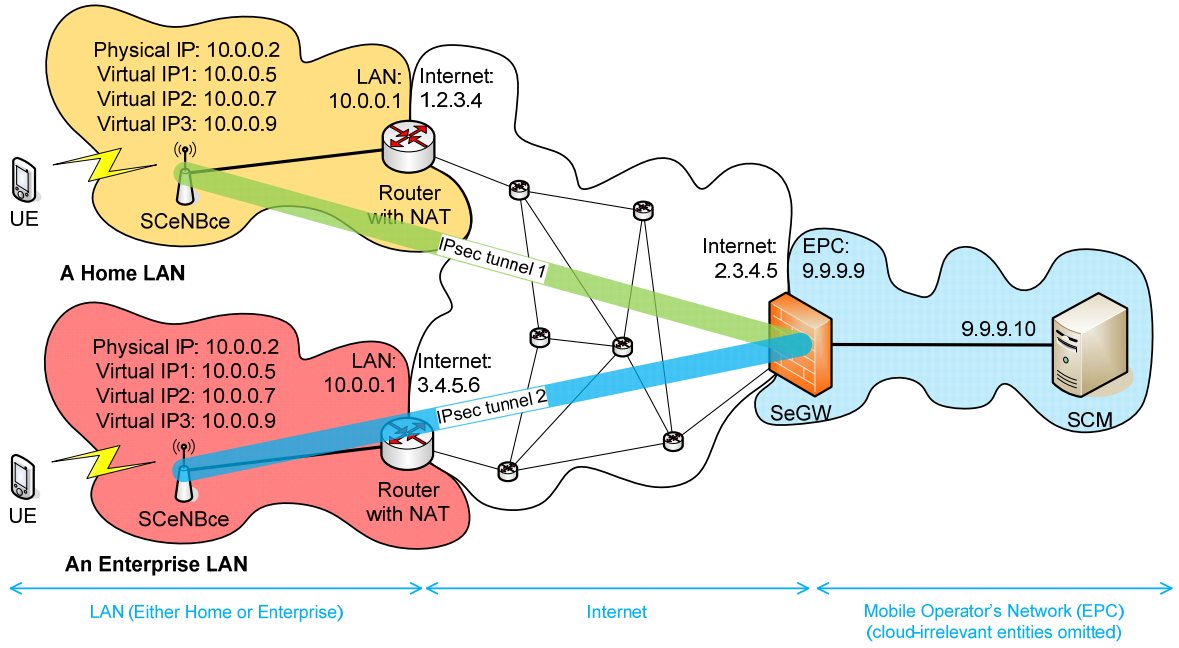


Figure 47. Design example

To make the explanation clear, hypothetical IPv4 addresses were used (see Figure 47). The 10.0.0.0/24 IPv4 private address space is taken as per RFC1918 range on purpose (commonly used in today's home/enterprise networks). The rest of the IPv4 addresses are public.

12.2.2 The Design Requirements and Properties

Routers with NAT have different public IPv4 address (to be routable/available in the public Internet). As the IPv4 address space of both LANs is determined by the LAN Administrators, the Mobile Operator cannot change it. If this IP address is 1:1 NATed to another (second) public IP address (bought by the local network administrator), then no issue occurs (such example is not depicted in). On the other hand, if both use the same private IPv4 ranges (see Figure 47), one of them will not be

available. If there are more than two, then only the first will be accessible and routable. In more detail, the routing table of SeGW may have more than one rule pointing 10.0.0.0 network in different interfaces (IPsec in our case). However, only the first (best metric) will be chosen.

Moreover, let's focus on the IPsec tunnel establishment which occurs prior to a routing rule is inserted into the routing table of the SeGW. For successful IPsec tunnel establishment, the SeGW needs to know two IPv4 things. An IPv4 address of the SCeNBce and other IPv4 addresses which should be routed into the IPsec (in our case, the Virtual IPs). Let's assume the Home LAN is the first to successfully establish the IPsec tunnel. Based on the prior explanation, the Enterprise LAN IPsec tunnel will never be established as the Virtual IPs overlap.

As per the previous clarification, a scheme, where virtual IPv4 addresses are assigned and managed by a LAN device (Home/Enterprise DHCP server), cannot be used for the Tropic design purpose.

12.2.3 Solution

For native IPv4, we could consider Multiprotocol Label Switching (MPLS) combined with Virtual Routing and Forwarding (VRF) technology. However, these bring further complexity and device requirements to the whole scenario and decrease the total efficiency of transmitted bits (further inevitable encapsulation of data units etc.)

The simplest solution for the overlapping problem seems to be the usage of IPv6 (see Figure 48). The logical design is a cloud-oriented scenario. Therefore, the IP addresses (either v4 or v6) should be assigned and managed by a dedicated device(s) located in the cloud network, which is the mobile operator's network, i.e. in the evolved packet core (EPC).

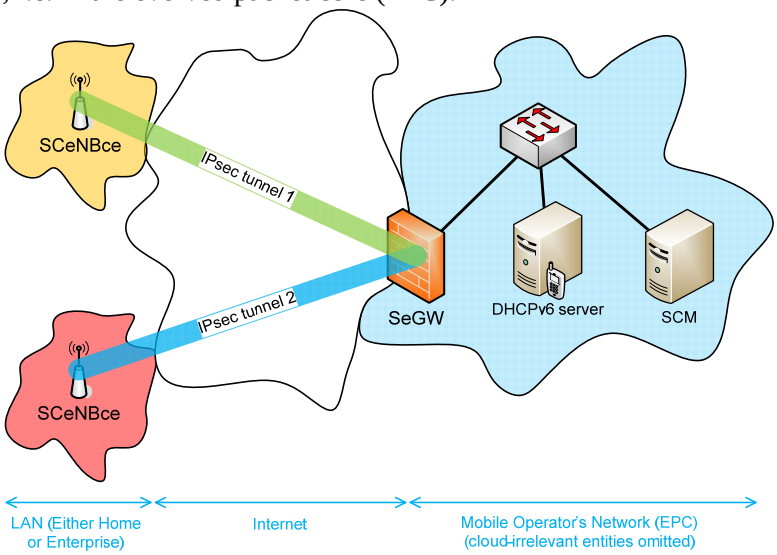


Figure 48. IPv4 address space overlap solution

Case Study

After the IPsec tunnel is established, based on the cloud task requirements, several virtual resources (machines) are assigned. These virtual devices need identification – an IP address. The virtual IPv6 addresses are assigned by the dedicated (centralized) DHCPv6 server, which is managed by the mobile operator. The mobile operator systems will also update the respective routing tables of the involved devices (SeGW, routers, etc.) and modify the IPsec setup of the SeGW accordingly.