Raimo Ahosola

Modelling LTE BTS Transport Parameter Interrelations for Improving Roll-out Efficiency

Helsinki Metropolia University of Applied Sciences

Master’s Degree

Information Technology

Master’s Thesis

22 Apr 2016

Abstract

Author(s)	Raimo Ahosola
Title	Modelling LTE BTS Transport Parameter Interrelations for Improving Roll-out Efficiency
Number of Pages	105 pages + 26 appendices
Date	22 Apr 2016
Degree	Master of Engineering
Degree Programme	Information Technology
Instructor(s)	Jarkko Itkonen, Snr Network Planning and Optimisation Expert Jouko Kurki, Principal Lecturer

The traffic volume in mobile networks is estimated to grow more than 100 times in the next 10 years. Mobile network operators are expanding their networks to respond to the demand and network vendors constantly improve their processes to address the growth. Long Term Evolution (LTE) technology is the leading technology to build the fourth generation (4G) mobile networks. The LTE base station is referred as evolved NodeB (eNB). The number of eNBs as compared to other network elements is large. The large number of eNBs together with the large number of parameters per eNB increase the requirement for efficient parameter planning process in LTE network roll-out projects. The goal of this study was to improve the eNB transport parameter planning process efficiency by developing a parameter model with defined parameter interrelations.

First the current practises in selected roll-out projects were analysed. The project data were collected applying a questionnaire sent to the network planners. The data were analysed to have an understanding of the current practices.

The study identifies two main parameter areas which benefit most of the parameter model and the defined interrelations. The first area is the eNB capacity related parameters including traffic engineering parameters and the second area is the Internet Protocol (IP) addressing related parameters. This study introduces a set of typical network scenarios and defines the interrelations between the eNB transport parameters in these scenarios.

The developed model and the defined parameter interrelations reduce the number of manual entries in the planning phase. In the introduced scenarios one manual entry defines five to eleven case specific parameters in eNB configuration. This introduces 80% to 90% direct work effort savings and reduces the human errors and thus the non-quality cost as well.

Keywords	4G, Backhaul, Base Station, BTS, Design, Efficiency, eNB, eNodeB, Interrelation Rule, Long Term Evolution, LTE, Network, Parameter, Planning, Roll-out, Transport

Contents

Appendices

List of Figures

List of Tables

List of Listings

Abbreviations/Acronyms

3G	Third generation (mobile network)
3GPP	3rd Generation Partnership Program
4G	Fourth generation (mobile network)
Abis, ABIS	Abis interface in GSM network between the BTS and the BSC
AF	Assured forwarding
BCF	Base control function
BCFSIG	BCF signalling (link)
BCSU	Base station controller signalling unit
BE	Best effort
BFD	Bidirectional forwarding detection
BSC	Base station controller
BTS	Base transceiver station
CBS	Committed burst size
CIQ	Customer information query
CIR	Committed information rate
cx	Complexity (metric)
DL	Down link
DSCP	Differentiated services code point
E-UTRAN	Evolved universal terrestrial radio access network
EBS	Excess burst size
EF	Expedited forwarding
EIR	Excess information rate
eNB	Evolved nodeB
EPC	Evolved packet core
ETSI	European telecommunications standards institute
EVC	Ethernet virtual connection
GBR	Guaranteed bit rate
GERAN	GSM EDGE Radio access network
GPRS	General packet radio service
GSM	Global system for mobile communications
GTP-U	GPRS tunnelling protocol
GW	Gateway
HSS	Home location server
HW	Hardware

ID	Identifier
IEEE	Institute of electrical and electronics engineers
IETF	Internet engineering task force
IP	Internet protocol
IPsec	Internet protocol security
ISDN	Integrated services digital network
IT	Information technology
IUA	ISDN user adaptation
L2	Data link layer, layer 2 in OSI model
L3	Network layer, layer 3 in OSI model
LAM	Latin America and Mexico (region)
LAN	Local area network
LAPD	Link access procedure for the D-Channel
LTE	Long term evolution
MAC	Media access control
MBH	Mobile backhaul (network)
MEA	Middle east and Africa (region)
MEC	Mobile-edge computing
MIMO	Multiple in multiple out
MME	Mobility management entity
MML	Man-machine language
MTU	Maximum transmission unit
NGMN	Next generation mobile networks
NTP	Network time protocol
O&M	Operation and maintenance
OAM	Operation administration and maintenance
OMUSIG	Operation and maintenance unit signalling
OMS	Operation and maintenance subsystem
OSI	Open system interconnection
PCRF	Policy and charging rules function
PDCP	Packet data convergence protocol
PE	Provider edge
pe	Process efficiency (metric)
PHY	Physical (layer protocol)
PIR	Peak information rate
QCI	QoS class identifier

QoS	Quality of service
RAN	Radio access network
RLC	Radio link control
PLMN	Public land mobile network
RRC	Radio resource control
S-GW, SGW	Serving gateway
S1	Logical interface between the eNB and the EPC
S1-AP, S1AP	S1 interface application protocol
S1-U	S1 interface user plane
SCTP	Stream control transmission protocol
SIR	Shaping information sate
SON	Self-organising network
SPR	Subscription profile repository
SW	Software
TAC	Transport admission control
TCP	Transmission control protocol
ToP	Timing over packet
TRX	Transceiver
TWAMP	Two way active measurement protocol
UDP	User datagram protocol
UE	User equipment
UL	Uplink
Um	Air interface, interface between the eNB and the UE
UNI	User network interface
UTRAN	Universal terrestrial radio access network
VLAN	Virtual LAN
WFQ	Weighted fair queueing
X2	X2 interface, logical interface between adjacent eNBs
X2-AP	X2 interface application protocol
XML	Extensible mark-up language

1 Introduction

The traffic in mobile networks in terms of bytes per day is estimated to grow more than a hundred times in the time period from 2015 to 2025. Even the conservative estimate predicts 61 time higher traffic volumes in 2025 compared to 2015. [1.] Mobile network operators need to expand their networks to respond to the demand. Also mobile network vendors need constantly to improve the processes in their delivery chain to address the new challenges in a cost efficient way. The traffic growth forecast prepared by Bell Labs is shown in Figure 1.

Mobile broadband networks are expanding and new technologies are taken in use to fulfil the capacity and throughput needs. Long Term Evolution (LTE) technology is one of the leading technologies to build fourth generation (4G) mobile networks. These high speed LTE networks are becoming available for even larger populations and are solving the capacity and speed bottlenecks that users are currently experiencing. The LTE network base station is referred as evolved NodeB, eNodeB, shortly eNB. [2.]

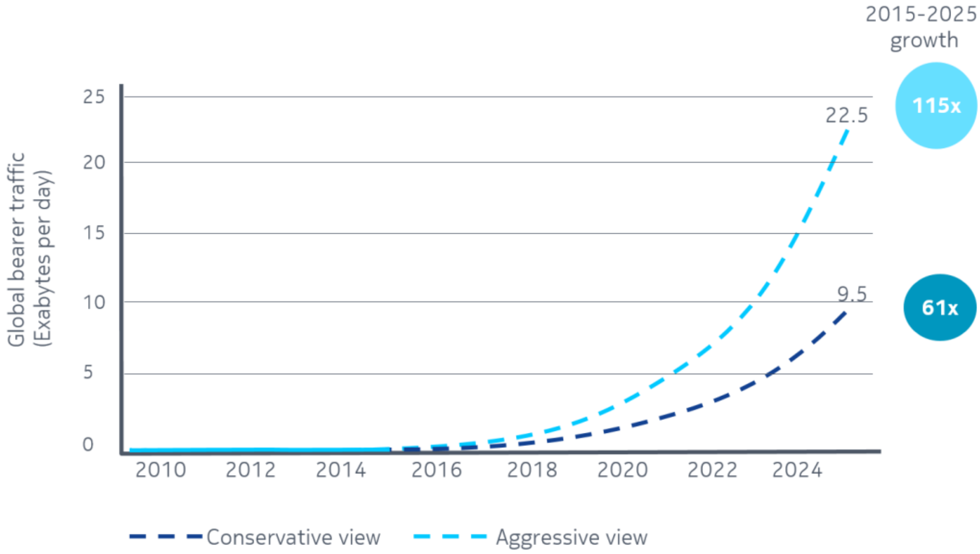


Figure 1. Bell Labs estimated traffic growth from 2015 to 2025. Even the conservative view shows growth of 61 time and aggressive view 115 times in ten years. Copied from [1].

The number of eNBs compared to other network elements is LTE network is large and the new capacity solutions are even increasing the eNB density in hot spot areas in near future [3 chapter 4]. The large number of eNBs together with the large number of parameters per eNB increases the requirement for efficient parameter planning for LTE network. Managing high number of parameters in network roll-out project is time consuming and error prone task. Network operators are looking for easier ways to manage complex networks.

One concept to minimize human effort is a frame work called Self Organized Networks (SON) [4 chapter 25.1]. The concept was introduced by the Next Generation Mobile Networks (NGMN) alliance in 2007 and it aims to minimize the operational effort and cost. This is achieved by applying automated mechanisms such as self-configuration, self-optimization and self-healing. The aim of these functions is to simplify the network operation [3 preface]. Even the self-configuration and self-optimizing functions minimizes the required human effort to configure network nodes they do not remove totally the need to plan the eNB parameters. Self-configuration of parameters such as neighbour relations is defined in 3rd Generation Partnership Program (3GPP) technical specifications, but vast number of parameters still requires manual planning.

The aim of this study was to develop an eNB parameter model for network planning purposes. The eNB parameter model was to streamline the eNB parameter planning task and thus not only to minimize the direct effort required to produce the eNB parameter plan but also to improve the quality of the plan. Improved quality has a positive impact on the non-quality cost burn for error fixing and delays on eNB roll out schedule. The goal is to minimize the required human entries required to define the values for the eNB parameters during the roll-out planning phase. This is essential to minimize the network roll-out and in particular the network planning cost.

This study focuses on the eNB transport parameters. The aim is to identify the most typical scenarios and for those scenarios to define interrelation rules between the parameters in different managed objects in the eNB configuration file. The identified interrelation rules can further be implemented in the planning tools to speed up the planning phase.

The eNB radio parameters are not within the scope of this study. Also this study focuses on one selected eNB software release (RL70). The goal of the eNB parameter model for network planning is to enhance the automation in early steps in eNB planning and integration process. The study is part of the larger program aiming to automate the eNB integration and operation steps.

This paper starts by introducing the mobile broadband network architecture and goes on by explaining the network functionalities, which are relevant from the eNB transport parameter planning point of view. Then, the current transport parameter planning practises are discussed and results of the studied cases are summarised. Next, the developed eNB transport parameter model and the eNB transport parameter interrelation rules are introduced in chapter 4 and further analysed in chapter 5 after which the critical discussion is held in chapter 6. And finally the last chapter summarises the findings and conclusions on the present study.

2 Mobile Broadband Network Planning

The objective of mobile broadband network planning is to dimension the network resources and to provide a cost efficient network design which scales well when the network capacity needs to be upgraded or new functionalities are taken in use. The design is a compromise between coverage, quality and cost. [5 section 6.2.]

Furthermore, the detailed design defines the parameters for network elements so that they can be integrated to each other. This study focuses on the eNB parameters for interfaces and processes towards adjacent eNBs and Evolved Packet Core (EPC) network. The network architecture and protocol stacks are summarized first after which the planning aspects are discussed more deeply.

2.1 Mobile Broadband Network Architecture

Mobile broadband network consists of radio network and core network. In LTE the radio network specified by 3rd Generation Partnership Project (3GPP) is referred as an Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and 3GPP core network is called Evolved Packet Core (EPC). [6.]

In addition to 3GPP defined elements a real mobile broadband network consists of transport and IP backbone elements which are mainly based on the Internet Engineering Task Force (IETF) definitions. These transport and Internet Protocol (IP) backbone networks used to connect E-UTRAN and EPC are called Mobile Backhaul Networks (MBH). [7.] The E-UTRAN architecture is discussed briefly in subsection 2.1.1 then mobile backhaul architecture is summarised in 2.1.2 and the interface concept between the eNB and the mobile backhaul is elaborated in 2.1.3 after which the protocol stacks are introduced in section 2.1.4.

2.1.1 Evolved Universal Terrestrial Radio Access Network Architecture

An Evolved Universal Terrestrial Radio Access Network (E-UTRAN) consists of several radio base stations called evolved NodeB (eNB). An eNBs provides air interface (Um) for the user equipment and terminates user plane and control plane protocols towards the User Equipment (UE). The eNB has logical interfaces towards core network and adjacent eNBs. The logical interface towards core elements is called S1 interface. Each eNB is interfacing to two types of core network elements, the signalling function interfaces to a Mobility Management Entity (MME) and user the plane traffic to a Serving Gateway (S-GW). The interface towards the MME is called S1-MME and the interface towards the S-GW is S1-U interface respectively. The logical interface towards adjacent eNBs is called X2 interface. The E-UTRAN architecture is illustrated in Figure 2. [6.]

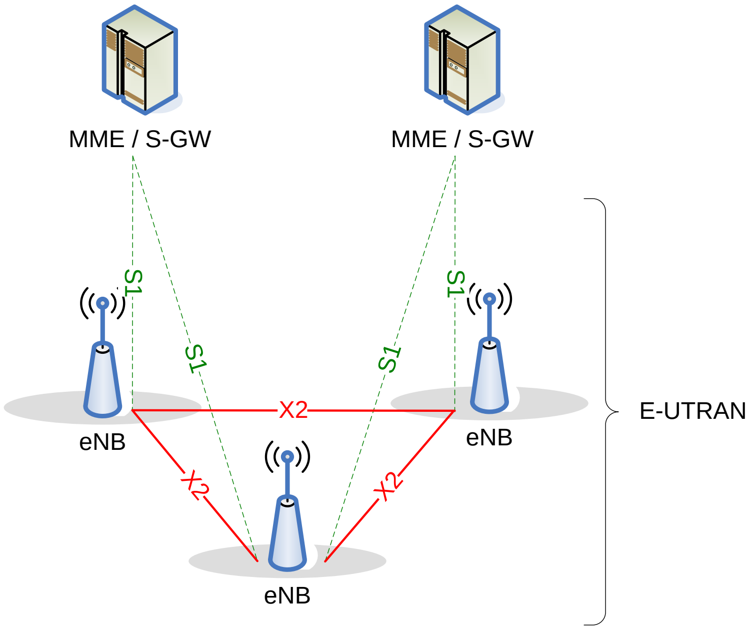


Figure 2. The E-UTRAN Architecture, LTE radio base stations (eNB) and core network elements; Mobility Management Entity (MME) and Serving Gateway (S-GW). Copied from [6].

Like the S1 interface also the X2 interface consists of user plane and control plane functionalities. The control plane of X2 interface is used for procedures between adjacent eNBs required to hand a UE over from one eNB to another eNB. The X2 user plane is required to forward the user IP packets already received by the old eNB but not yet transmitted successfully over the air interface before the UE was handed over the new eNB. In case the X2 interface is not defined between the adjacent eNBs the handover takes place in S1 interface instead. [8,170-173.]

2.1.2 Mobile Backhaul Network Architecture

The transport and packet networks providing connectivity between the eNB and the Mobility Management Entity (MME) and the Serving Gateway (S-GW) in S1 interface and between adjacent eNBs in X2 interface are called Mobile Backhaul Networks (MBH) or shortly mobile backhaul. Mobile backhaul networks connect large number of eNBs to relatively small number of core network elements. The structure of mobile backhaul network is shown in Figure 3. [7;8 subsection 12.5.1.] In addition to the tree topology shown in Figure 3 also the point to point and the ring topologies are seen at access layer section of the mobile backhaul networks [9;2,138].

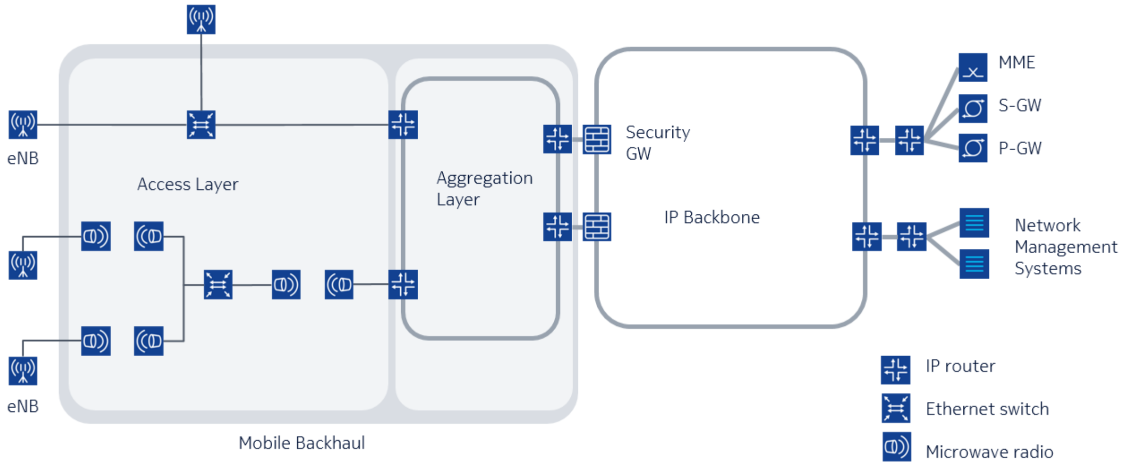


Figure 3. Access layer and aggregation layer of the mobile backhaul network. Access layer relays typically on fibre and microwave radio based physical media while aggregation layer is fibre based network. Adapted from [9;2].

Mobile backhaul network connects the eNBs to the IP backbone network, which in turn provides connectivity to the core network elements. Mobile backhaul network can be divided into two sections; access layer and aggregation layer. The access layer is also called a last mile or a first mile depending on the perspective. The access layer may be pure layer 2 network or pure layer 3 network or mix of them. Layer 2 network is typically Ethernet switching network and layer 3 is IP based network. [7 section 1.2.]

The media used in access network includes wireline copper cable-based and fibre based technologies and wireless microwave radio based technologies [10,22]. Due to high data rate targets the fibre-based and microware are the most common access media used in mobile backhaul while the copper based connection may be seen on limited capacity sites.

The interface between an eNB and the mobile backhaul network can be considered to be a User Network Interface (UNI) in the Metro Ethernet Forum terminology [11]. The concept of UNI is discussed in the next section.

2.1.3 User Network Interface

Metro Ethernet Forum defines specifications for carrier class Ethernet services. Metro Ethernet Forum focuses on four key specification work areas which are: services, architecture, management and test & measurement. The aim is to improve interoperability and accelerate deployment of Carrier Ethernet worldwide. An Ethernet service is defined as a connection between two or more User Network Interfaces (UNI). Service attributes are used to define the properties of the User Network Interfaces.

The interface between a user equipment, referred to as Customer Edge (CE) (in this case eNB) and the provider's network (in this case mobile backhaul network) is referred to as a User Network Interface (UNI). Connection between User Network Interfaces cross the providers network is defined by the Ethernet Virtual Connection (EVC). An EVC is an association of two or more UNIs. The concept of the Ethernet service model is shown in Figure 4. [12.]

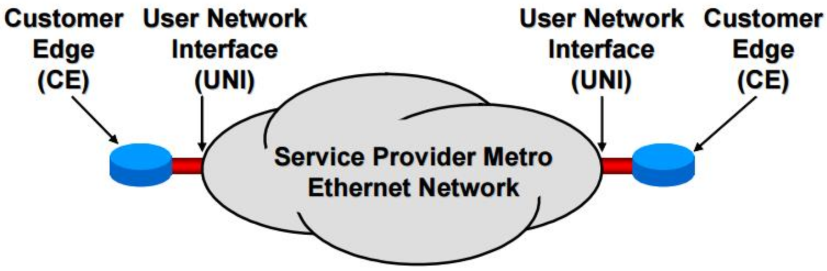

Customer Edge (CE)
User Network Interface (UNI)
User Network Interface (UNI)
Customer Edge (CE)
Service Provider Metro Ethernet Network

Figure 4. Ethernet service model according to Metro Ethernet Forum. Customer Edge is an equipment interfacing to the provider's network. User Network Interface (UNI) is a physical demarcation point between the responsivities of the subscriber and the service responsibilities of the provider. Copied from [12].

Each User Network Interface has a set of attributes which describe the characteristics of the given UNI. The most relevant attributes for this study are the bandwidth profile related attributes. The bandwidth profile may be defined per User Network Interface (UNI), per Ethernet Virtual Connection (EVC) or per Class of Service (CoS). The standard bandwidth profile attributes are listed in Table 1. [13.]

Table 1. User network interface (UNI) bandwidth profile attributes. Data gathered from [13].

Attribute name	Unit	Purpose
Committed information rate (CIR)	bit/s	The average bitrate at the ingress UNI the provider's network commits to transfer the data to egress UNI fulfilling the agreed quality targets.
Committed burst size (CBS)	bytes	Amount of data arriving in the network in one go as a single burst at the ingress interface the provider's network commits to transfer according the agreed quality targets.
Excess information rate (EIR)	bit/s	The average bitrate exceeding the committed bitrate at the ingress UNI the provider's network transfer the data to egress UNI if network capacity is available, no quality targets are committed for the excess amount of data
Excess burst size (EBS)	bytes	Amount of data arriving in the network in one go in addition to the committed burst size at the ingress interface the provider's network transfers if network capacity is available, no quality targets are committed for the excess amount of data
Coupling flag (CF)		The coupling flag controls the choice how the bandwidth profile algorithm threats the service frames declared yellow.
Colour mode (CM)		Colour mode parameter defines whether the bandwidth profile algorithm operates in colour-aware or colour-blind mode. Colour-aware mode considers colour marking on service frames at ingress interface.

The colour mode parameter defines if the Ethernet virtual connection (EVC) service is colour aware or colour blind. Colour aware mode takes the traffic marking into account in bandwidth profile algorithm thus is able to selectively drop packets in case of congestion in the network. In colour aware mode traffic is classified in three classes identify be colours. Traffic not exceeding the Committed Information Rate (CIR) is considered to be green, traffic exceeding the CIR but not exceeding the sum of CIR and EIR is considered to be yellow and traffic exceeding the sum of CIR and EIR is considered to be red. The green traffic is not dropped, the yellow traffic may be dropped in an event of network congestion and the red traffic is dropped at the ingress UNI to protect the provider's network. The colour blind profile does not consider traffic marking and thus it may end up dropping also the high priority packets in case of network congestion. [13.]

2.1.4 S1 and X2 Interface Protocol Stacks

The applications for signalling, S1-AP for S1 interface and X2-AP for X2 interface, are defined by the 3GPP. The S1 application protocol terminates the control plane between the eNB and the Mobility Management Entity (MME) and the X2 application protocol terminates the control plane between adjacent eNBs. Note that signalling message flows between the User Equipment (UE) and the Mobility Management Entity are considered to be user plane traffic in an eNB point of view. The application protocols S1-AP and X2-AP are running on top of well-known Stream Control Transmission Protocol (SCTP) and Internet Protocol (IP) defined by the Internet Engineering Task Force (IETF). The S1-AP protocol stack is shown in Figure 5. [14.]

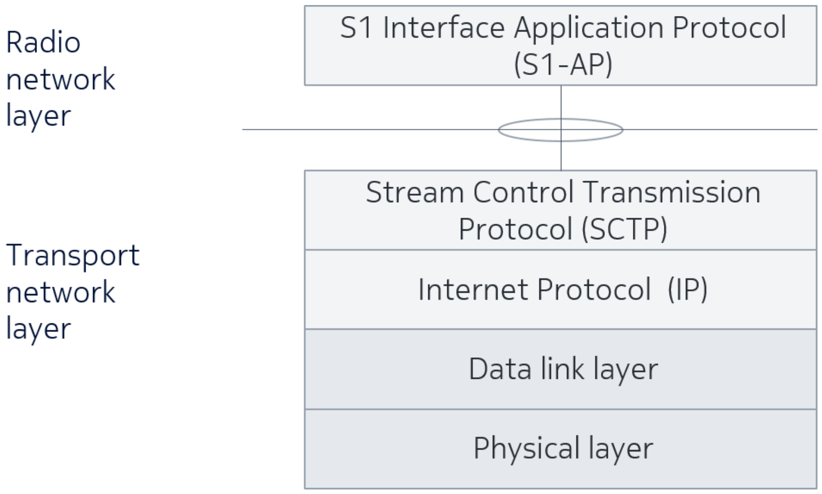


Figure 5. The protocol stack used for S1 interface application protocol (S1-AP) signalling. Stream Control Transmission Protocol (SCTP) provides reliable transport for signalling messages. Adapted from [14].

The X2 interface application protocol has an important role in a hand over process where a User Equipment is handed over to new serving cell. The X2 interface enables eNBs to perform the hand over without core network involvement. This reduces the signalling load at the Mobility Management Entity (MME). The X2-AP protocol stack is very similar as the only difference is the application layer where instead of S1-AP the X2-AP is used. S1-AP protocol stack is shown in Figure 6. [15.]

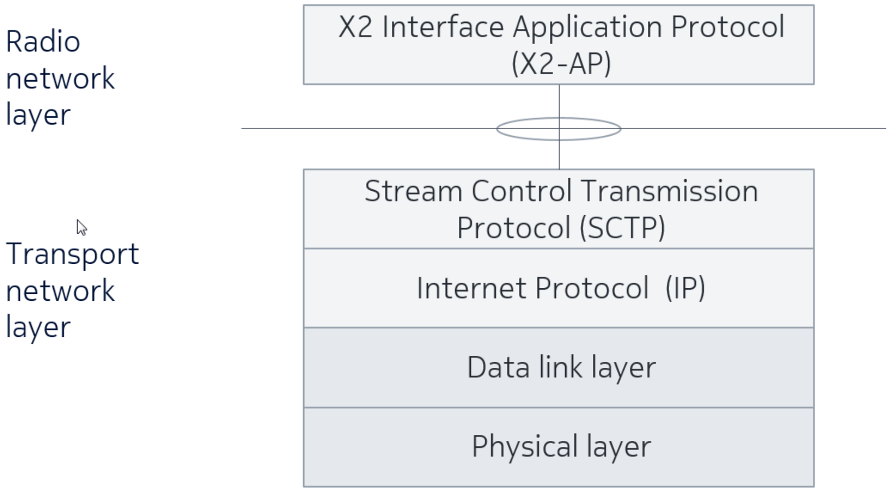


Figure 6. The protocol stack used for X2 interface application protocol (X2-AP) signalling. Adapted from [15].

The 3GPP does not limit the protocols used in data link and physical layer but in practical implementations the most common technology used for these layers is Ethernet. Ethernet scales well for bursty data traffic. [16 section 15.7.] The corresponding protocol stack to carry user data is illustrated in Figure 7. The same stack is applied both for S1 and X2 interface. [17;18.]

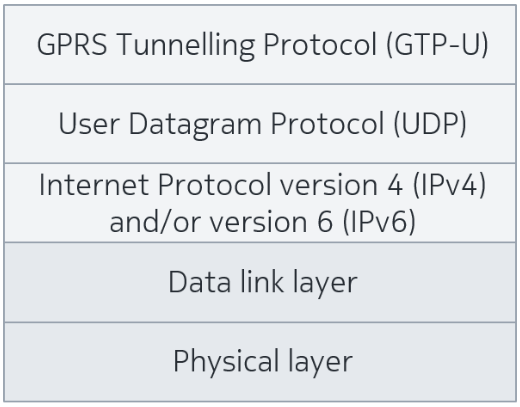

GPRS Tunnelling Protocol (GTP-U)
User Datagram Protocol (UDP)
Internet Protocol version 4 (IPv4) and/or version 6 (IPv6)
Data link layer
Physical layer

Figure 7. U-plane protocol stack used for S1 and X2 interfaces. The GTP-U is used to encapsulate the user IP packets. Adapted from [17;18]

The GPRS tunnelling protocol for user plane (GTPv1-U) is used to encapsulate the user plane data in E-UTRAN. The GTP-U is running on top of user datagram protocol (UDP) which in turn running of top of IPv4 or IPv6 network layer protocol. The GPRS Tunnelling Protocol (GTP-U) and User Datagram Protocol (UDP) relies on upper layer protocols for example User TCP for possible retransmission.

The use of particular data link layer and physical layer protocols is not specified by the 3GPP [14;15;18]. Ethernet is typically used as data link and physical layer protocol as it is widely adopted by mobile backhaul networks especially for high capacity links [7].

The eNB transport parameters discussed in this study are related to transport network layer shown in Figure 5 and Figure 6 and to parameters required for processes which are used to monitor the user plane path availability and quality. The parameters related to application layers S1-AP and X2-AP are not in the scope of this study.

2.2 Planning Problems

The problem to solve in IP network planning is to provide a network that scales well and is easy to maintain. The IP backbone is designed to be robust and fault tolerant and able to forward huge amount of data. [19.]

The problem to solve in access layer planning is to provide a cost efficient access connection to large number of sites which do not necessary have fibre connections available. The access network technology and access network planning has not been discussed much in literature as a technology providing connections for mobile broadband network elements. [7.]

Further, discussion about 3GPP radio technologies and eNB especially in literature, are mainly focused on the air interface problems but the transport interfaces S1 and X2 has been included as low focus areas. The S1 and X2 interfaces are typically discussed in the 3GPP scope point of view leaving the IETF based protocols and processes in lower attention or totally out of discussion. [7.]

2.3 High Level Design

A high level design defines the overall technical solution, design rules, technologies and concepts to be used in the given network. The high level design does not touch network element parameters in detail since that is addressed in detailed design phase. [2,131;20.]

The high level design consists of for example connectivity diagram showing the main network elements and the interfaces between them, synchronization and resilience principles, the use of virtual local area networks (VLAN) and Internet protocol (IP) subnets. High level design also addresses the quality of service (QoS) strategy to be applied. [2,131;20.]

2.4 eNB Transport Interface Dimensioning

There are two main approaches to perform the eNB transport interface capacity dimensioning. The first approach is to use the accurate traffic figures and calculate the transport overhead on top of those [2]. The second approach is to use the air interface capacity as a reference for the transport capacity calculations [21]. This approach can also be followed in case the accurate traffic estimations are not available.

For each cell a peak rate and an average data rate can be defined. Peak rate is achieved when all radio resources are used for transmission or reception with the highest modulation and coding scheme. Adding the transport protocol header over head the transport capacity to support the given cell configuration peak rate can be defined. The cell average throughput in this context refers to the situation where all the eNB radio resources are used but the user equipment (UE) are distributed evenly over the cell coverage area and thus only small share of user equipment have a possibility to benefit the highest modulation and coding schemes.

The air interface capacity based approach can be further divided into variants based on the weight of the peak and average cell throughputs. The typical approach is to assume single peak and sum of cell averages and pick the one which requires the highest transport capacity. Other options includes sum of all averages, single peak and all but one average and sum of peaks. [8 subsection12.4.1.] The air interface capacity based approach is further discussed in the *Guidelines for LTE Backhaul Traffic Estimation* and the *Backhaul Provisioning for LTE-Advanced & Small Cells*. [21;22.]

2.5 Detailed Planning

In the detailed planning phase the eNB parameters are defined. An eNB configuration may have more than 1600 parameters, most of them related to air interface processes [23]. In eNB transport area, covering interfaces S1 and X2, there are several hundred parameters. Due to high number of eNBs compared to other network elements in the mobile broadband network the efficient parameter planning and handling in general is essential for cost efficient roll-out.

The eNB transport parameters can be categorized in many ways. In this chapter the eNB transport parameters are divided into categories based on the location of the process, the parameters are controlling. First the processes close to eNB are discussed. This covers functionalities typically limited to access layer of the mobile backhaul network structure shown in Figure 3. In this study these processes are referred as *near reaching processes*.

As a second step the focus is in functionalities having eNB counterpart further in the backhaul network either in aggregation layer or in IP backbone. In this study these processes are called *far reaching processes*. As a third step the processes having the eNB peer at core or network management site are covered. In this study these processes are referred as *end-to-end processes*.

2.5.1 Near Reaching Processes

In this document the access process refers a process which has limited geographical significance and can be located close to eNB and typically is limited to the access section of the mobile backhaul as shown in Figure 3. This section discusses the access processes which parameters need to be planned case by case. The processes discussed in this section include IP addressing, traffic separation, traffic path supervision and fast traffic rerouting, Quality of Service (QoS) aware Ethernet switching and Transport Admission Control (TAC).

2.5.1.1 IP Addressing

The eNB IP addressing options in release RL70 are illustrated in Figure 8. The scenario a) shows a case where user plane (U), control plane (C), synchronization plane (S) and management plane (M) applications share the same IP address as the VLAN interface. In the scenario b) each application plane has an IP address of its own and the address is shared with the VLAN interface the application plane is associated with. The scenario c) assumes unique loopback IP address for each application plane and separate IP address for the VLAN interface (T).

These are the basic IP addressing scenarios and the actual configurations may have combinations of these. One typical practical case is to assign S-plane IP address to transport interface and the others to have loopback address as application IP address. Some features such as symmetric Stream Control Transmission Protocol (SCTP) multi-homing and transport separation for Radio Access Network (RAN) sharing introduce additional IP addresses to be considered. [8 subsection 12.2.6.]

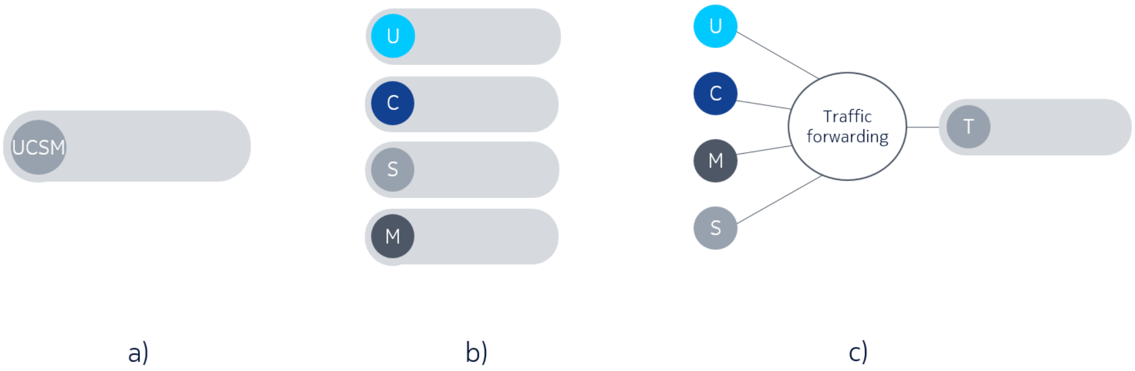


Figure 8. The basic eNB IP addressing options: a) single VLAN and single IP address shared for all applications, b) dedicated VLAN for each application, c) Single VLAN and dedicated application IP address defined as loopback address for each application. Adapted from [8].

This subsection concludes the discussion of the eNB IP addressing modes. The next subsection discussed the traffic separation.

2.5.1.2 Traffic Separation

This subsection discusses the traffic separation functionality. The traffic separation on an eNB transport interface is based on the Virtual Local Area Networks (VLAN). The VLAN tagging is based on the IEEE 802.1Q standard. The drivers for the traffic separation includes the operator's security policies, the backhaul node traffic treatment capabilities and the network monitoring requirements. The operator may want to separate the management plane from the other traffic planes. Having dedicated management network domain reduces the risk of impacting the remote management connection when modifying the parameters related to the other traffic planes.

Traffic classification in a backhaul node operating at layer 2 may be based on the source Media Access Control (MAC) address, the destination MAC address, the Virtual Local Area Network Identifier (VLAN ID) or the VLAN priority [24]. Modern layer 2 nodes are also able to use the layer 3 differentiated services code point (DSCP) marking as a base for traffic classification. In earlier eNB releases traffic monitoring was possible on VLAN level and thus in order to monitor traffic volumes per traffic plane a dedicated VLAN was defined for each traffic plane. The eNB traffic monitoring capabilities have evolved since and thus traffic monitoring is less likely the driver for traffic separation any longer.

The VLAN ID is the most relevant eNB parameter for traffic separation. The related parameters include the IP subnet assigned for the VLAN and the IP address to be applied as VLAN interface IP address in the given eNB. The VLAN ID and subnet may be common for a few to dozens of eNBs while the VLAN interface IP address must be unique for each eNB within a mobility management entity (MME) area. An example of eNB VLAN termination is illustrated in Figure 9. In this example three VLANs are defined for the eNB. The green, red and blue dotted lines in the figure illustrate the configured VLANs; VLAN 100, VLAN 200 and VLAN300 respectively. The VLANs are terminated at the first router the eNB is connected to.

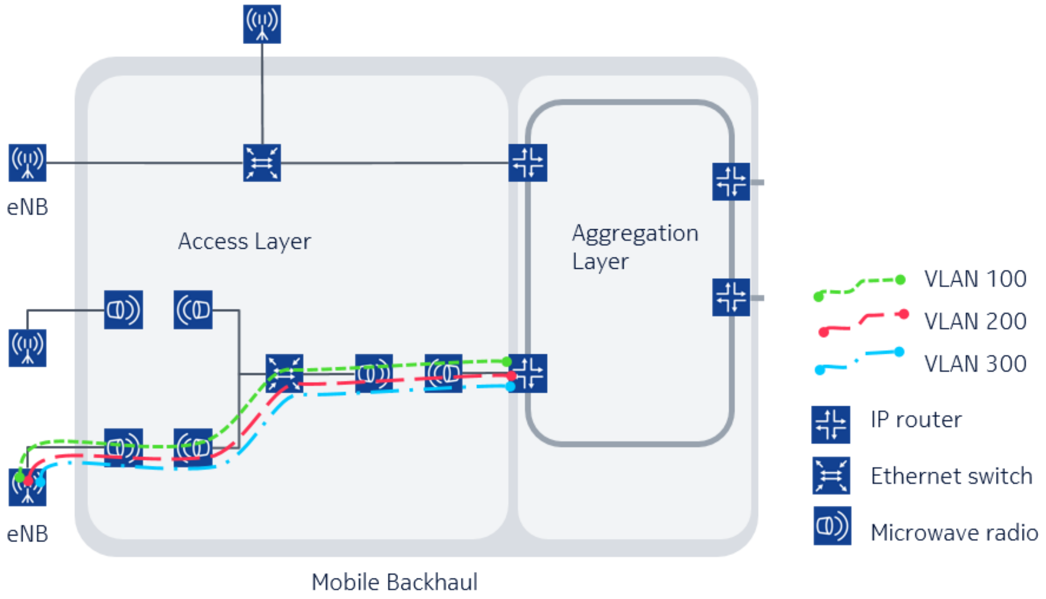


Figure 9. An example of traffic separation based on VLAN configuration. Each VLAN carries specific type of traffic for example the VLAN 100 synchronisation plane traffic, VLAN 200 management plane and VLAN 300 control plane and user plane traffic. The VLANs are terminated at the eNB and at the first hop router.

The parameters defined for VLAN managed object in the eNB configuration file are shown in Listing 1. In addition to VLAN ID and the IP address also the traffic shaping limits relevant to the given VLAN are defined. Shaping information rate (*sir*) and shaping burst size (*sbs*) are used to control average data rate and the maximum number of octets which can be sent as a one burst. Shaping is used to avoid violating the capabilities limits of the mobile backhaul nodes and agreed capacity usage.

```
managedObject class="IVIF" distName="MRBTS-xxx666/LNBTS-
xxx666/FTM-1/IPNO-1/IEIF-1/IVIF-2" operation="create"
version="LN5.0">
<p name="vlanId">3300</p>
<p name="localIpAddr">10.225.10.33</p>
<p name="netmask">255.255.255.248</p>
<p name="sir">150000</p>
<p name="sbs">4000</p>
<p name="qosEnabled">false</p>
<p name="wfqSchedQueueWeight">1000</p>
</managedObject>
```

Listing 1. An example of VLAN managed object and related parameters in an eNB XML configuration file. In addition to VLAN interface IP address the VLAN ID (*vlanId*), shaping information rate (*sir*) and shaping burst size are to be considered case by case.

The traffic separation using VLANs can be used to direct the traffic to desired interface or towards the desired node. One use case is to connect eNB to Mobile-Edge Computing (MEC) system. Mobile-edge computing refers the case where Information Technology (IT) and cloud computing capabilities are located close to mobile subscribes and thus close to the eNBs. Figure 10 shows an example network with Mobile-Edge Computing (MEC) server. In this example eNBs in the grey area are served by the applications running on the mobile-edge computing server. [25.]

The introduction of the mobile-edge computing server to existing network is transparent to 3GPP network architecture and existing interfaces. The mobile-edge computing server as well the applications running on it do not require any changes in the user equipment (UE) or mobile core network elements.

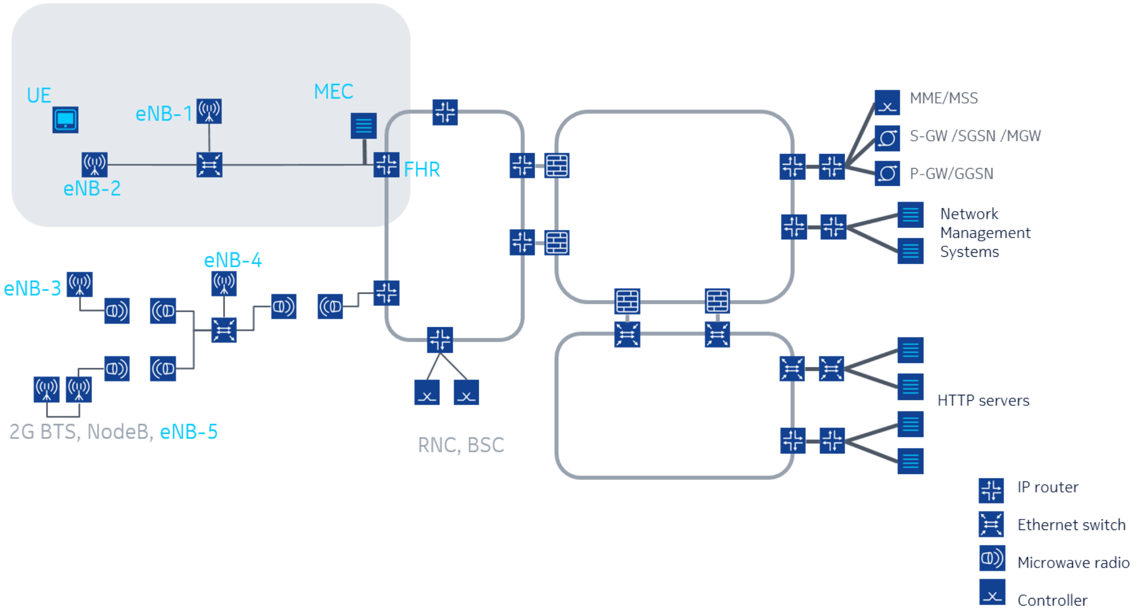


Figure 10. An example deployment scenario of the Mobile-Edge Computing (MEC) server. The user equipment (UE) under eNB-1 and eNB-2 coverage area may access the local content in Mobile-Edge Computing (MEC) server next to the First Hop Router (FHR).

The mobile-edge computing platform must not affect the availability of the network even it is out of service and thus resilience features are applied in the eNB to fulfil this requirement. In normal condition the S1 traffic is traversing the mobile-edge computing server. In case the server becomes unavailable the S1 traffic is redirected to a secondary path which bypasses the server. [25.] The resilience features are discussed next.

2.5.1.3 Traffic Path Supervision and Fast Traffic Rerouting

The way people communicate has changed a lot in past decades. Today people are expecting seamless service, always being connected to network. On the other hand businesses have been moved to network or at least heavily depend on the network connectivity. The traditional customer interaction changes to online interaction. This phenomena is called Hyper-connectivity. Hyper-connectivity has revolutionised the way the business is conducted.

As businesses relay more and more on the network connectivity the service and network availability is a key target for many network operators. For these reasons a good network design considers various resilience methods. Relying routing protocol updates in many cases is no longer fast enough and thus alternative options are made available to reduce the network outage times from a few second ranges to less than 100 millisecond ranges. To design a resilient networks several aspects needs to be considered. Common resiliency methods include the ones listed in Table 2. [26.]

Table 2. Common resilience methods. Data gathered from [26].

Common resilience methods
Multiple connections between the critical network nodes
Redundant critical network nodes and devices
Quality of service monitoring to react to service shutdowns
Redirection to avoid congestion
Analysis of the most efficient use of active connections

To increase the resiliency in the mobile network the connection between the eNB and the core network can be implemented using redundant links on chain or ring topology. The ring topology provides additional geographical redundancy and is helpful in case of for example in natural disasters causing damages on the whole site the node is installed. These provides additional traffic path in case one path has a link or node failure.

One approach to monitor the availability of a traffic path between two systems communicating with IPv4 or IPv6 is to apply the Bidirectional Forwarding Detection (BFD) process. In this contexts the link between the eNB and the gateway router can be supervised using eNB feature *link supervision with BFD* [27].

The availability information may further be used as an alarm status or to control routing in case of path failure. The eNB feature *fast IP rerouting based on BFD* enables conditional routing based on the BFD status [27]. To improve resilience two independent or partially independent paths can be implemented between the eNB and the IP gateway (GW). The path which is considered to be the primary path is supervised by the BFD process. Whenever the BFD reports path availability the primary path is used for traffic forwarding. As soon the primary path is declared to be unavailable the traffic is forwarded to the secondary path.

A single hop BFD is defined in RFC5880 and it is further clarified in RFC7419 which specifies common interval support in bidirectional forwarding detection to improve interoperability between different vendor systems [28;29]. Single hop BFD is used to monitor a connectivity cross a link and thus this is limited to peers sharing the subnet. The BFD specification was further extended to support monitoring of paths consisting several links. This extension is referred as *bidirectional forwarding detection (BFD) for multihop paths* [30]. The BFD is configured between two peers. Each peer is configured to send small “hello” messages to its peer. As far the node receives these “hello” messages from its peer the path is declared to be available but when no “hello” message is received within a specific time frame the path is declared to be unavailable.

From the planning point of view there are a few aspects to be considered. First one is the mode of operation. The BFD process may operate in single hop or multi hop mode. Single hop refers to the situation where the peer is within the same subnet and thus only one layer 3 (L3) hop exists on the path. Multi hop mode refers cases where the peer node is located in the other subnet and one or more routers are located in between the peer nodes. The selection of the mode is controlled by node interoperability and the network design targets. The second aspect which is visible in the planning point of view is the peer IP address. Each peer is identified by an IP address and these addresses need to be configured in the nodes running the BFD processes. Typically the BFD supervision is defined between the eNB and the IP GW assigned for the eNB as shown in Figure 11.

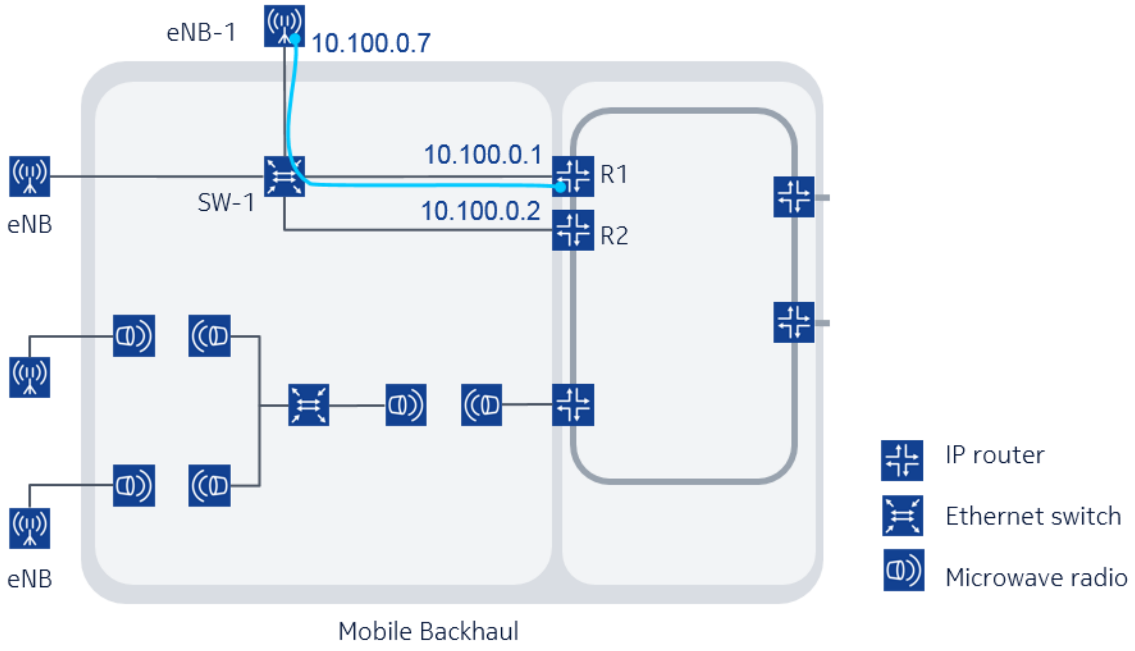


Figure 11. An example of Bidirectional Forwarding Detection (BFD) process between the eNB-1 and the router R1. In case the path from eNB-1 o R1 becomes unavailable the bath to R2 is taken in use.

Next the details of an example configuration are discussed. This example shows a case where eNB connection towards the core network is partially protected. The section between the eNB-1 and the Ethernet switch (SW-1) is unprotected; however, the connection from SW-1 onwards is protected. The blue line in Figure 11 illustrates a BFD process in the example mobile backhaul network. The BFD process supervises the path in between the eNB-1 and the router R1.

The traffic forwarding in the eNB assumes R1 as a GW to access the core network as far the path is claimed to be available by the BFD process. As soon the BFD process detects the path being unavailable the traffic forwarding in the eNB assumes R2 as a GW to access the core network. Listing 2 shows parameters applied in the eNB-1 for the BFD process in this example.

```
<managedObject class="BFD" distName="MRBTS-15/LNBTS-15/FTM-
1/IPNO-1/BFD-1" operation="create" version="TL15A">
<p name="bfdActivation">true</p>
<p name="bfdAdminUp">true</p>
<p name="bfdDestAddress">10.100.0.1</p>
<p name="bfdDetectMult">3</p>
<p name="bfdGrp"/>
```

```
<p name="bfdSourceIpAddr">10.100.0.7</p>
<p name="bfdSourceUdpPort">3784</p>
<p name="bfdType">singleHopBFD</p>
<p name="desMinTxInt">500</p>
<p name="reqMinRxInt">500</p>
</managedObject>
```

Listing 2. The BFD managed object parameters for eNB-1 shown in Figure 11. The process is defined between two IP endpoints and thus the IP addresses for this managed object needs to be defined case by case**.**

The traffic forwarding parameters for this example are shown in Listing 3. In the first item the traffic forwarding is based on the status of the BFD process (bfdid=1). When the BFD-1 indicates the path being available the gateway (GW) assuming IP address 10.100.0.1 is used for the destination 10.10.20.0/24 a as the preference is set highest (preference=1). The second item shows unconditional forwarding definition that is the traffic forwarding is not based on any BFD process. This is indicated by a special value bfdId=0. The preference of the second forwarding item is set lower than is used for the primary path (preference=3) and thus this forwarding definition takes action only if no valid forwarding options with higher preference is available. The forwarding process assumes 10.100.0.2 as GW when the first path becomes unavailable.

```
<managedObject class="IPRT" distName="MRBTS-15/LNBTS-15/FTM-
1/IPNO-1/IPRT-1" operation="create" version="TL15A">
<list name="staticRoutes">
<item>
<p name="bfdId">1</p>
<p name="destIpAddr">10.10.20.0</p>
<p name="gateway">10.100.0.1</p>
<p name="netmask">255.255.255.0</p>
<p name="preSrcIpv4Addr">0.0.0.0</p>
<p name="preference">1</p>
</item>
<item>
<p name="bfdId">0</p>
<p name="destIpAddr">10.10.20.0</p>
<p name="gateway">10.100.0.2</p>
<p name="netmask">255.255.255.0</p>
<p name="preSrcIpv4Addr">0.0.0.0</p>
```

```
<p name="preference">3</p>
</item>
</managedObject>
```

Listing 3. An example of routing manged object (IPRT-1) in the eNB XML file, traffic forwarding based on the BFD-1 process. To a destination 10.10.20.0/24 GW 10.100.0.1 is preferred. If that path becomes unavailable the less preferred path via GW 10.100.0.2 is used.

This subsection concludes the discussion of the traffic path supervision and path protection. Next the quality of service aware Ethernet switching feature is discussed

2.5.1.4 Quality of Service (QoS) Aware Ethernet Switching

The next functionality to discuss here is the Quality of Service (QoS) aware Ethernet switching. Quality awareness enhances the basic Ethernet switching capabilities. This functionality introduces a list of small processes running at Ethernet switch in the eNB. These include traffic policing, traffic classification, queuing, scheduling and traffic shaping. The QoS aware Ethernet switching enables desired treatment of aggregated traffic at the eNB Ethernet switch egress interface in case of network congestion. The traffic is delay and/or dropped in controlled manner based on how it was marked. This ensures that the aggregated traffic does not violate the bandwidth attributes of the User Network Interface (UNI). This is important especially in a case the eNB UL traffic is aggregated to other traffic at eNB Ethernet switch.

The traffic shaping in egress interface ensures that UNI capacity attributes are not violated either by too large aggregated burst or too high aggregated average data rate. The queuing system in each interface of the QoS aware Ethernet switch consists of one strict priority queue and five weighted fair queues. Traffic is classified to proper queue based on the Differentiated Services Code Point (DSCP) value on IP header or by VLAN priority bits in VLAN tag. The scheduling weights can be controlled to ensure proper traffic treatment in case on congestion at UNI.

2.5.1.5 Transport Admission Control (TAC)

In addition to control total traffic volumes by the shaping process also the Guaranteed Bit Rate (GBR) traffic can be limited in a controlled manner. Transport admission control (TAC) feature allows the operator to set a limit for the GBR traffic. The transport admission control (TAC) will check the available transport capacity before it accepts the new Guaranteed Bit Rate (GBR) bearer setup. If not sufficient capacity is available the new bearer setup is rejected. By Transport Admission Control the operator can protect the services of GBR bearers which are already served by the system in case of congestion. Separate limits can be defined for normal traffic, incoming handover traffic and emergency traffic. Listing 4 shows an example of transport admission control parameters.

```
<managedObject class="TAC" distName="MRBTS-xxx666/LNBTS-
xxx666/FTM-1/TAC-1" operation="update" version="LN5.0"/>
<managedObject class="LTAC" distName="MRBTS-xxx666/LNBTS-
xxx666/FTM-1/TAC-1/LTAC-1" operation="update" version=
"LN5.0">
<p name="tacExludeL2Overhead">false</p>
<p name="tacActivityFactor">100</p>
<p name="tacLimitGbrNormal">105000</p>
<p name="tacLimitGbrHandover">120000</p>
<p name="tacLimitGbrEmergency">150000</p>
<p name="transportNwId">0</p>
<p name="qci2AvPacketSize">200</p>
<p name="qci3AvPacketSize">80</p>
<p name="qci4AvPacketSize">300</p>
</managedObject>
```

Listing 4. An example listing of the eNB transport admission control parameters in eNB XML file. The admission limits can be defined separately for normal traffic, traffic entering the cell by hand over procedures and for emergency traffic.

This concludes the discussion of the transport admission control and also discussion about processes which are relevant close to the eNB. The next subsection elaborates processes which reach further towards the core network.

2.5.2 Far Reaching Processes

In this document the far reaching process refers a process which has wide geographical significance having one end at the eNB and the peer far away from the eNB close to or at the core network as illustrated in Figure 3. The far reaching processes includes path availability monitoring from the eNB to the Serving Gateway (S-GW), IP connectivity quality monitoring and IP security processes.

Two processes monitoring the IP path are discussed in this section. First the GPRS Tunnelling Protocol for User plane (GTP-U) path supervision is discussed after which the Two Way Active Measurement Protocol (TWAMP) is covered and finally in this section the secure connection is briefly discussed. After that the IP security is covered.

2.5.2.1 GPRS Tunnelling Protocol for User Plane (GTP-U) Path Supervision

The GPRS tunnelling protocol for user plane (GTP-U) path supervision is defined in 3GPP TS 29.281 [31]. When GTP-U path supervision is activated in the eNB the bearer establishments are accepted only to such serving gateway (SGW) which are reachable from the eNB. This reach ability is checked by continuous process of sending and receiving control messages between the selected SGWs and the eNB as illustrated in Figure 12.

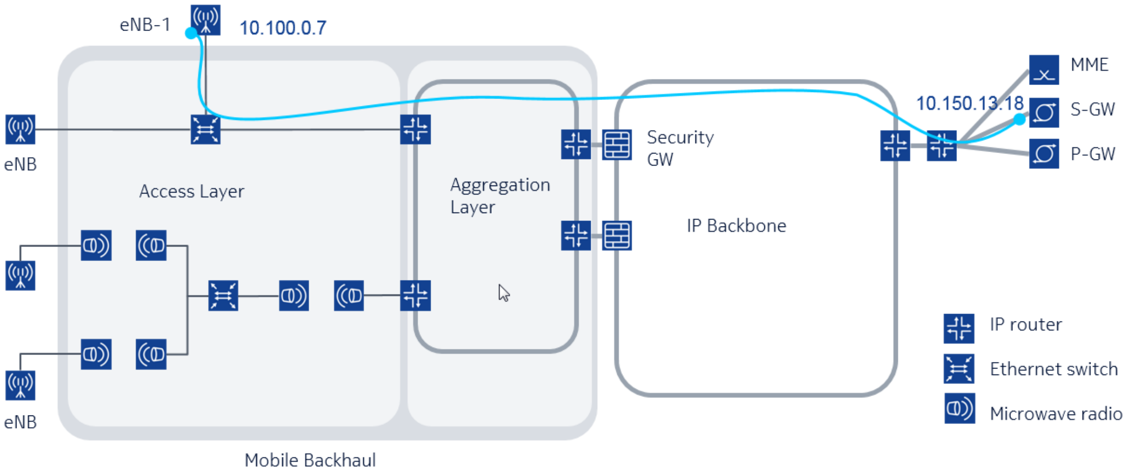


Figure 12. An example of GTP-U path supervision flow between the eNB-1 and the Serving Gateway (S-GW). Bearer establishments are accepted to the S-GW only if the path is available.

From the parameter planning point of view this means that the Serving Gateway (SGW) IP addresses are configured to eNB. These IP addresses are required only for the supervision purposes as the one to be used for the S1-bearer is signalled by the MME during the bearer setup phase. The parameters for GTP U-plane path supervision are shown in Listing 5. The list of S-GWs is reduced in this figure for clarity.

```
<managedObject class="GTPU" distName="MRBTS-xxx684/LNBTS-
xxx684/GTPU-1" operation="create" version="LN5.0">
<p name="gtpuPathSupint">60</p>
<p name="gtpuN3Reqs">5</p>
<p name="gtpuT3Resp">2</p>
<list name="sgwIpAddressList">
<item>
<p name="sgwIpAddress">10.150.13.18</p>
<p name="transportNwId">0</p>
</item>
<item>
<p name="sgwIpAddress">10.150.13.19</p>
<p name="transportNwId">0</p>
</item>
...
<item>
<p name="sgwIpAddress">189.40.170.1</p>
<p name="transportNwId">1</p>
</item>
</list>
</managedObject>
```

Listing 5. An example of a managed object (GTPU-1) and its parameters for GTP-U path supervision in the eNB XML file. Path supervision interval *gtpuPathSupint* is set to 60 seconds and a list of SGW IP addresses *sgwIpAddress* are defined.

This discussion covered path availability monitoring. Path availability status is important information in the bearer set-up phase as the bearers are set up only to those S-GWs which are reachable. This minimizes the “silence call” phenomena sometimes seen in networks. In addition to availability the connection quality can be monitored as well. The next subsection discusses the process which is specifically designed to help monitoring IP connectivity quality.

2.5.2.2 Two Way Active Measurement Protocol (TWAMP)

The Two Way Active Measurement Protocol (TWAMP) enables continuous monitoring of the IP connectivity quality. It gives the operator means to detect congestion or faults in the network. The main function is to measure the delay and packet loss between two interfaces. Increased delay is an indication of a network congestion. By using TWAMP an operator can ensure that the mobile backhaul and IP backbone networks fulfil the set design targets in terms of delay, delay variation and packet loss.

The Two Way Active Measurement Protocol (TWAMP) is defined in the RCF5357 [32]. The Two Way Active Measurement Protocol consists of control part to establish the monitoring process and the actual monitoring part. This study focuses only on the monitoring part of the TWAMP RFC. In case the monitoring is set up by the administrative means the process is referred as TWAMP light in the RFC5357. The TWAMP light is described in the appendix I of the RFC5357.

The monitoring is based on continuous flow of measurement messages sent by one peer (sender) to another peer referred as reflector. The test message contains up to four time stamps and two sequence numbers. The first time stamp is updated by the sender when the test message is sent out form its interface. The second time stamp is updated by the reflector on arrival. The third time stamp is updated when the reflector sends the message out from its interface and the fourth and the last time stamp is updated when the sender receives the reflected test message. The fourth time stamp is not visible on the link but only at the process at the sender. Based on these four time stamps the delay can be calculated to each direction separately. The sequence numbers are used to detect packet loss. If a particular sequence number is missing on reception it is a sign of a lost packet.

From the planning point of view the first tasks is to define the locations of the nodes acting as a sender and a reflector to ensure sufficient coverage for the monitoring with reasonable amount of overhear introduced by the TWAMP messages. The second task is to define the end point IP addresses to the relevant nodes. In the eNB this means one local IP address and one peer IP address for each TWAMP process. The TWAMP measurement path is illustrated in Figure 13.

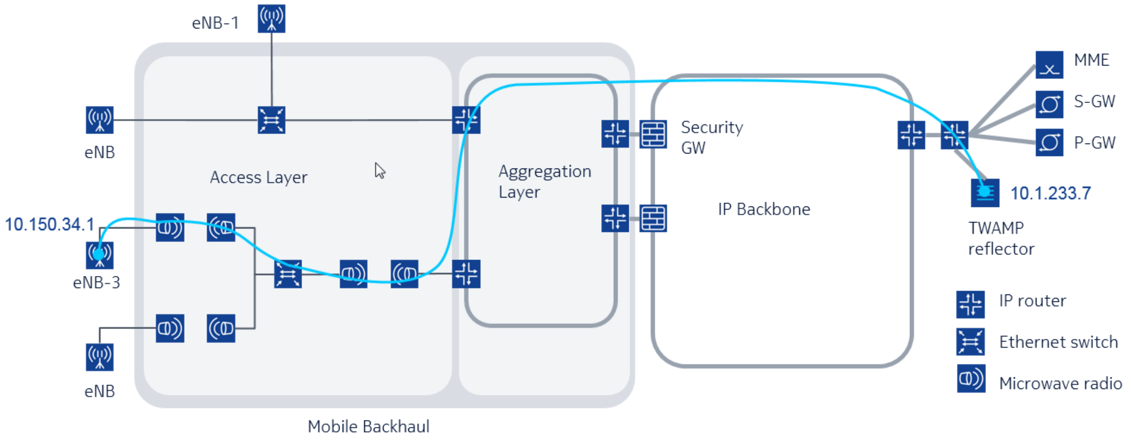


Figure 13. An example of the Two Way Active Measurement Protocol (TWAMP) flow between the eNB-3 and the TWAMP reflector. The path delay, delay variation and packet loss reports can be generated based on the measurement results.

A simplified method, UDP echo, is also available for the delay monitoring. This is useful if the peer node does not support the TWAMP. In the UDP echo process there are only two time stamps instead of four. The sender updates the first time stamp when the test message is sent out. The reflector node in case of UDP echo just sends back the test message without manipulating any time stamps. And finally the original sender updates the second time stamps on arrival of the echoed test message. Based on the time stamps the round trip delay can be calculated. The TWAMP and UDP echo are meant to be used continuously to monitor IP connection quality.

Several two way active measurement protocol (TWAMP) processes can be configured to the eNB. Also the DSCP marking can be defined for each process separately. This enables delay and packet loss reporting on traffic class basis. The parameters controlling the TWAMP sender are illustrated in example listing in Listing 6.

```
<managedObject class="TWAMP" distName="MRBTS-xxx536/LNBTS-
xxx536/FTM-1/IPNO-1/TWAMP-1" operation="create" version="LN7.0">
<p name="administrativeState">unlocked</p>
<p name="destIpAddress">10.1.233.7</p>
<p name="destPort">5000</p>
<p name="dscp">34</p>
<p name="messageSize">100</p>
<p name="plrAlarmThreshold">10000</p>
<p name="rttAlarmThreshold">1000000</p>
```

```
<p name="sourceIpAddress">10.150.34.1</p>
</managedObject>
```

Listing 6. An example of a TWAMP managed object and TWAMP parameters in the eNB XML file. The process is defined between two IP endpoints (*destIpAddress* and *sourceIpAddress*) and the traffic marking (*dscp*) is set to desired value.

This ends the discussion of the Two Way Active Measurement Protocol. The next item to discuss here is the security particularly security on transport interfaces.

2.5.2.3 Transport Security (IPsec)

The most important features in communication security consists of authenticity, confidentiality, integrity, nonrepudiation and availability. Authentication is a process of verifying the identities of the communication parties. Confidentiality ensure that the information is not obtainable by unauthorised parties. Integrity means that messages have not been altered on the communication channel. Nonrepudiation of a message means that the original sender cannot later deny having sent the message. Availability is an underlying assumption that the communication can be successful. The most relevant features in the LTE network point of view are: authenticity, confidentiality and integrity. Introduction of LTE is a step to improve the availability of the mobile access channel. The last feature, nonrepudiation, is more relevant for the application layer. [33.]

There is a need to address the authenticity, confidentiality and integrity measures not only in the air interface but also on transport interfaces. The eNB density grows all the time as the network coverage and capacity is expanded and more and more small cell eNBs are in public places such as lamp posts, bus stops and advertisement signs making the transport interfaces vulnerable. [2,190.]

According to the 3GPP technical specifications the air interface security covers the path from the User Equipment (UE) to the eNB and it is terminated at the eNB and thus does not cover the transport interfaces [34]. The security infrastructure in mobile backhaul is well established IPsec defined by the IETF. IPsec is a protocol suite rather than one protocol. These protocols may operate in transport mode or in tunnel mode. In transport mode the security association is define between two hosts while in tunnel mode the security association is define between the tunnel endpoints. In tunnel mode for confidential protection an IP packet is first encrypted and then encapsulated into the tunnel IP packet. In this way in addition to original IP packet payload also the original IP addresses are encrypted.

The authentication in the LTE backhaul is based on public key cryptography and X.509 certificates. Public key infrastructure (PKI) is used to issue and maintain the required certificates. [2,191.] The public key infrastructure planning is outside of the scope of this study and thus is not discussed further.

Network is divided into security domains and security GW (SEG) is to protect the border of such domain. One security GW is in the eNB and the other typically at the operators IP backbone or core network. IP security provides data integrity, data origin authentication, anti-replay protection, confidentiality (optional) and limited protection against traffic flow analysis when confidentially is applied. [34 chapter 5.]

An example of an IPsec scenario operating in tunnel mode is shown in Figure 14. This example assumes that the mobile backhaul network is untrusted while the IP backbone is trusted domain as it is administrated by the mobile network operator by himself and the nodes and fibre terminations are located in controlled environment. The tunnel mode isolates the IP addresses used in LTE applications and IP backbone from those used in mobile backhaul. This simplifies planning as subnets can be planned independently in these two domains.

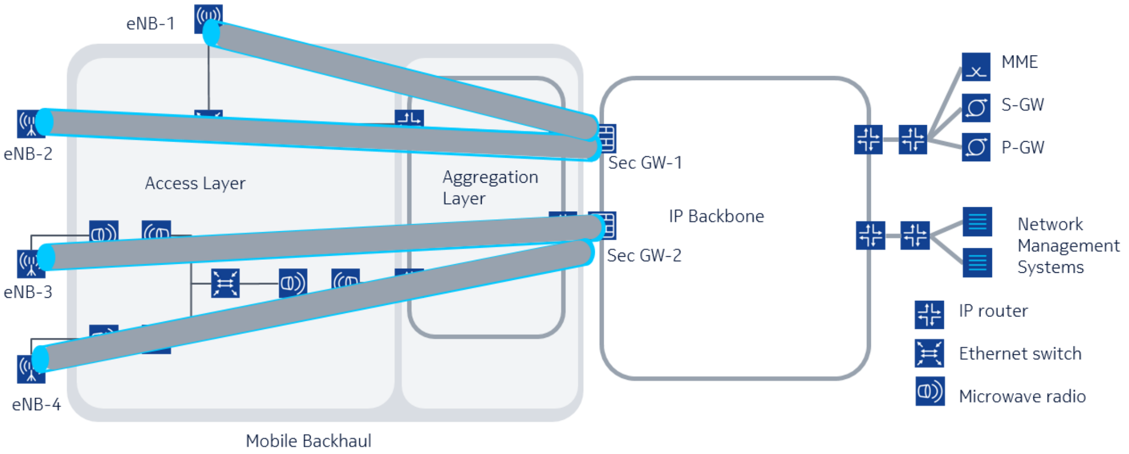


Figure 14. An example of IPsec tunnels defined between the eNB internal security GW and the security GW at the operator’s backbone network. Traffic forwarding in the mobile backhaul is based on the tunnel end point IP addresses, the outer IP addresses. The inner IP addresses are not visible to the backhaul network.

The traffic is encapsulated with IPsec headers and passed to the tunnel based on the configured policies. The peer security gateway in turn decrypts the packet and forwards the original packet further towards the final destination. In the S1 interface one security GW is located in the eNB and the peer is located in secure section of the network closer to core network.

For X2 traffic there are a few options to consider. IPsec tunnel may be configured directly between adjacent eNBs or the X2 traffic can be passed via the same security GW as the S1 traffic. In the example above the X2 traffic from eNB-2 to eNB-3 is first encrypted by eNB-2 and then placed to IPsec tunnel towards security GW-1. Security SW-1 decrypts the traffic and forwards it towards the security GW-2 which in turn encrypts the traffic again and forwards it towards the eNB-3 which finally decrypts the X2 traffic received from eNB-2.

The direct IPsec tunnel between eNBs provides low latency connections but needs lots of configuration work when new adjacent eNB is introduced to the network. The second option, sharing the IPsec tunnels configured for S1 traffic, provides simple solution at the cost of additional delay caused by longer distance and additional decryption and encryption processes.

The position of IPsec in the S1-interface protocol stack is shown in Figure 15. The traffic forwarding between the security GW and the eNB is based on the outer IP addresses and the transport IP is transparently passed cross the backhaul. The transport IP in Figure 15 is one of the application IP addresses illustrated in Figure 8 and the IPsec tunnel IP address is one of the transport interface IP address for example VLAN interface IP address. [8 subsection 12.2.2.]

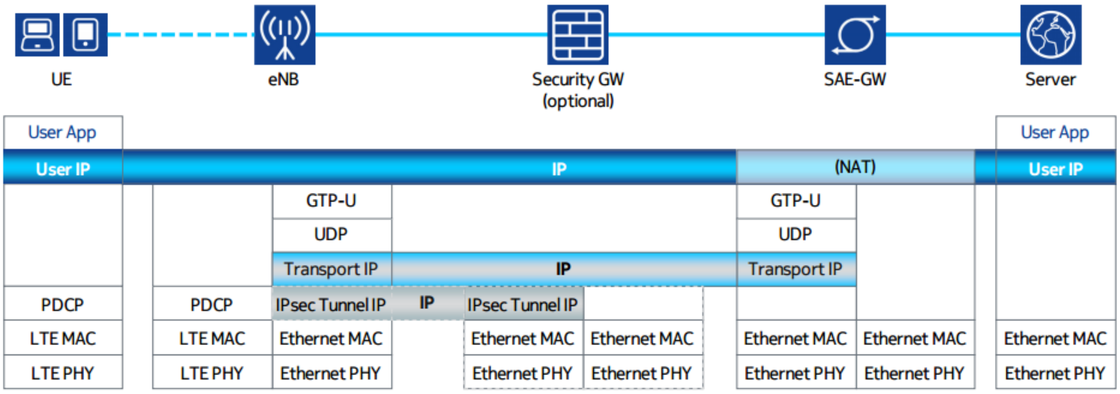


Figure 15. U-plane protocol stack with IPsec tunnel. The user IP traffic is encapsulated in GTP-U packets. Security GW further encapsulates the packet into IPsec tunnel. In the backhaul network the encapsulated packets are forwarded based on the IPsec tunnel end point IP addresses. Adapted from [8].

Most if not all access processed discussed in 2.5.1 are relaying on the outer IP addresses while the processes covered in 2.5.2 uses inner IP address ranges for peer communication.

2.5.3 End-to-End Processes

In this document the end-to-end function refers to a process which has a peer entity either in the core network element (MME or S-GW) or at management system servers. The position of these elements in the network is shown in Figure 3.

The functionalities discussed in this section include S1-flex, Stream Control Transmission Protocol (SCTP) multi-homing and a few network management related connections. From the eNB planning point of view the focus is in IP connectivity and thus no other process details are discussed here. And finally as a last end-to-end topic the Quality of Service (QoS) related functions are discussed.

2.5.3.1 Resilience and Load Balancing with S1-Flex

To improve the network level resilience the S1-flex functionality has been defined. The S1-Flex provides network resiliency by means of allowing eNB to be connected to more than one MME. S1-Flex also helps balancing the load between the MMEs the eNB is connected to. The third benefit of the S1-Flex functionality is the reduced MME load as within a MME pool area tracking area change does not imply change of serving MME and thus reduces the amount of required signalling. [35.]

In this study the only relevant part is the IP connectivity to more than one MME and thus the S1-flex functionality is not discussed further here. The eNB is provided with MME IP addresses so that it can start communication with the desired MMEs. Also the IP route to these destinations needs to be defined.

2.5.3.2 Resilience with Multi-Home Stream Control Transmission Protocol

The Stream Control Transmission Protocol (SCTP) is a transport layer protocol like Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). SCTP was originally developed by the Internet Engineering Task Force (IETF) as a transport layer protocol for the SS7 signalling networks. It has enhanced, more secure connection set-up, it can handle data in multiple logical streams both in fully or partial reliable delivery. SCTP support multi-homing for host with multiple network interfaces. [36;37.]

In LTE backhaul the SCTP multi-homing improves availability of signalling connection on S1 interface. The multi-homed SCTP association has multiple IP endpoints in each peer, eNB and the Mobility Management Entity (MME). The SCTP multi-homing relies on multiple independent paths between the peers. The primary path is used for signalling messages and the secondary paths are continuously supervised using short hello packets. In case of packet loss in delivery the retransmission takes place and this time on the secondary path ensuring fast recovery against single faults.

From the network planning point of view the SCTP multi-homing introduces one additional control plane IP address in the eNB and in the MME which need to be considered. Also the IP routes to these peer destinations have to be defined carefully to avoid routing the paths via single point of failure.

2.5.3.3 Miscellaneous Peers

The next topic in the end-to-end process category covers the connection to various management servers. In this study connections to network management systems, Network Time Protocol (NTP) servers, Domain Name Servers (DNS) and security servers such as Public Key Infrastructure (PKI) servers belong to this category are considered.

The eNB needs to know the management system IP address it is supposed to be connected to. These peer IP addresses are configured in the eNB. These IP addresses are typically common for large number of eNBs and can be define once for the whole roll-out project and thus this topic has low focus in this study.

2.5.3.4 Quality of Service (QoS) Functionalities

The Quality of Service (QoS) functionalities includes classifiers and class of services, metering and colouring functions, policer and shapers, queues and schedulers. A classifier inspects the incoming packets and decides to which class of service they belong to. A metering function measures the traffic arrival rate and assigns colours to the packet according to the measured rate. The colour indicates the desired treatment in case of congestion: green not to be dropped, yellow may be dropped and red to be dropped.

A policer is a traffic limiter which ensures that the traffic confirms with the defined bandwidth limit. The excess traffic which does not confirm the set limit is dropped. A shaper is another limiter function. The shaper limits the average output rate to set limit by delaying the excess traffic. A queue consists of fist-in-first-out (FIFO) buffer and a dropper function. The buffer holds the traffic which is waiting to be transmitted. Traffic in a queue is server in the order and no overtake is allowed.

A scheduler multiplexes traffic from two or more queues to a single output. The algorithms used to serve the queue includes for example strict priority and weighted fair queue. In the strict priory process each queue has different priority and the scheduler serves the first priority queue first. Only if the first priority queue is empty the strict priority scheduler serves the next queue.

The weighted fair queue scheduler serves the queues based on the predefined weights. Each queue is assigned a weight, a share of bandwidth, the queue is to be served. This scheduler can be configured to ensure desired share of the available link capacity. [38.]

Quality of Service (QoS) functionalities discussed further in this document includes traffic marking, traffic shaping and queuing control processes. Traffic shaping is more relevant at access section while traffic marking is more general topic.

In the LTE network the QoS attributes stored in the Home Subscriber Server (HSS) for subscribers are grouped in classes and these classes are identified by a QoS Class Indicator (QCI). The QCI value indicates how the traffic must be treated in other words how much delay or packet loss the traffic in the given class may tolerate. The eNB receives the QCI value from the MME in bearer setup signalling message. The QoS Class Indicator (QCI) value controls the air interface scheduler to ensure the desired traffic treatment.

The QoS Class Indicator is also used as an input for U-plane traffic marking in uplink (UL) direction at transport interface. As the Differentiated Services Code Point (DSCP) is used as a traffic marking method at transport interface a conversion from the QCI to DSCP is required. A configurable mapping table, to associate a Differentiated Services Code Point (DSCP) value with each QoS Class Indicator (QCI), is configured in the eNB. Preparing this mapping data is one part of the eNB parameter planning activities. The QoS marking must be applied consistently both on radio and the transport interfaces in all eNBs and thus the same mapping data is applied for all eNBs. [8 subsection 12.6.2.]

The QoS Class Indicator (QCI) to Differentiated Services Code Point (DSCP) mapping is the same in network level. However, the traffic shaping is typically case specific as eNB configurations, traffic amounts and backhaul capacities may vary from an eNB to another. Traffic shaping rate is aligned with the backhaul interface capacity for each eNB. The second parameter applied for traffic shaping is the burst size. The eNB is not supposed to exceed the burst size defined for the user network interface (UNI) and thus the traffic has to be shaped to avoid possible buffer overflows at some backhaul or backbone nodes. The maximum burst the eNB is allowed to transmit can be harmonized cross the network to simplify the eNB parameter planning.

Traffic policing may be applied to protect the system from excess traffic from being entering to the system. Policing is typically applied when untrusted network or node is connected to trusted network at the network edge. [38.]

2.6 Description of Earlier Parameter Interrelation Rule Optimisation Case

Parameter interrelation rule optimisation for network planning aims to minimize the manual entries required to complete a parameter set for a given node in a mass roll-out phase. It shall not be confused with the network optimisation where the aim is to improve the network performance by modifying the parameter values.

This study aims to define eNB parameter model so that the required entries for eNB transport parameters defined during the eNB rollout project for the given network cluster can be minimized. Similar parameter interrelation optimisation for network planning has been conducted before. The improvement was achieved by the planning sheet modifications. Summary of the previous findings are discussed shortly in this section. The parameter planning sheet optimisation in GERAN is elaborated in Appendix 1.

The results of these cases are summarised in Table 3. The first development step resulted 7% reduction in the number of required entries and 21% reduction in characters in these entries. The second development round further improved the situation and introduced 64% reduction in the number of active parameter entries and more than 90% reduction in the number of characters required for the entries compared to the case 1.

Table 3. Case comparison. Especially the case 3 has a huge decrease in required manual entries compared to the initial case, case 1.

Case	Number of entries (4200 TRX, 420 BCF)	Relative to case 1	Number of characters in entries	Relative to case 1
1 (Table 27)	64680	100%	317520	100%
2 (Table 28)	60060	93%	249900	79%
3 (Table 30)	21858	34%	30438	9.6%

The findings from this GERAN case are considered in eNB parameter model development. Key findings are listed in the Table 4.

Table 4. Key findings in GERAN planning sheet optimisation

Item	The key reasons for achieved improvement
1	Naming convention is automated
2	Double entry is eliminated. Any parameter is entered only once in the planning sheet even it is needed by several system objects.

This concludes the discussion of the earlier parameter study conducted earlier on GERAN Abis interface parameters. Next the applied study approach and material used in this this study is discussed.

3 Experiments and Results

This chapter discusses the method applied to collect the data from the selected roll-out projects, it summaries the parameter interrelation rules which were identified in the studied cases. This chapter also discusses the most relevant material used in this study.

The material is divided into three categories; product data, public data and finally the project data. First the main eNB product data are discussed. The eNB product data consist of a list of features the given HW and SW release supports and the parameters to control these features. Since this study focuses on eNB transport features (in other words those parameters which are related to S1 and X2 interfaces of the eNB), the air interface features and parameters lie outside the scope of this study.

The second important type of material is the public data. This includes standards, recommendations and white papers related to the S1 and X2 interfaces and related transport features. The S1 and X2 are open interfaces, and the functionalities used in these interfaces are based on public standards and recommendation. This part is discussed in the standards, recommendations and white paper section.

Finally the project data are discussed. This discussion starts with a definition what and how to collect and continues with the actual collected data.

3.1 Product Data

Feature and parameter descriptions represent a relevant part of the product documentation. Basic descriptions are available in customer documentation and further details can be found in the company internal documentations and databases. The main internal documentations used in this study are feature descriptions and specifications and eNB parameter database descriptions. The main product documentation used for parameter analysis in this study is listed in Table 5.

Table 5. Key product documentation used in this study.

Documentation	Title, document ID, number of pages	Date when accessed
Operating Documentation, Functional area descriptions	LTE Transport, DN0943983, 61 pages	
Operating Documentation, Features	Feature List, DN0944258 35 pages	
Operating Documentation, Features	LTE RL70, Feature Descriptions and Instructions, DN09185982, 449 pages	
Operating Documentation, Features	LTE RL60, Feature Descriptions and Instructions, DN09185955, 325 pages	
Operating Documentation, Features	LTE RL50, Feature Descriptions and Instructions, DN09185967, 304 pages	
Operating Documentation, Features	LTE RL40, Feature Descriptions and Instructions, DN09185979, 279 pages	
Operating Documentation, Features	Feature Descriptions RL30, DN0986461, 334 pages	
Operating Documentation, Features	Feature Descriptions RL20, DN0978033, 254 pages	
Operating Documentation, Features	Feature Descriptions RL10 DN0978045,250 pages	
On-line (Internal)	Parameter Knowledge Database	2 FEB 2014
On-line (internal)	Parameter Dictionary Database	2 FEB 2014

These feature descriptions are used to form a feature map. This map visualizes the feature relations. The use of a feature may depend on the other features activated in eNB. Some features are exclusive options while others complement each other. An example of the feature map is presented in Appendix 3.

The feature map is further analysed to form an eNB transport parameter map. The logic is the same as in feature map but the analysis is done in more detailed level. An example of the eNB transport parameter map is presented in Figure 24.

3.2 Standards, Recommendations and White Papers

The standards recommendations and white papers also play an important role in this analyse. The eNB transport interfaces X2 and S1 are open standard interfaces. The application layer of protocol stack is defined by 3rd Generation Partnership Program (3GPP) while the transport layer relays on well-known IP technology. These standards are mainly defined by Internet Engineering Task Force (IETF). The link layer is following the Institute of Electrical and Electronics Engineers (IEEE) and Metro Ethernet Forum (MEF) standards and recommendations. The white papers give hints and guides how to deploy the network and apply certain features. The most relevant white papers are published by Next Generation Mobile Networks (NGMN) and European Telecommunications Standards Institute (ETSI).

The standards and recommendations cover the details which are important for interoperability. These standards and recommendations are also used as a link to other application areas, where the same functionality is applied in the different technology environment. The list of standards, recommendations and white papers used in this study is given in References, at the end on the thesis.

3.3 Project Data

Project data represent a unique set of material collected from the selected projects within a certain time frame. The data are focused on eNB transport parameters and the possible rules, if any, used to resolve a parameter value based on a value already defined for another parameter in the given eNB or the eNB cluster. To collect the project data a round of questionnaire is conducted in the case companies. The received replies are analysed and unclear details are clarified by email conversations.

The current working approach in studying the eNB transport parameter interrelations is to analyse a few cases to see how the interrelation rules are applied in a planning process in roll-out projects. This study focuses on the identification of the current eNB parameter interrelation rules and how they are applied. Another interesting area is to analyse if any of the current eNB parameter plans could be considered as a model template for future projects.

The study starts with preparing the questionnaire to collect the practises used and features activated in the given roll-out projects. The questionnaire is sent to planning engineers who have shown interest to participate this eNB transport parameter study. The questionnaire is show in the appendix 1.

The study continues with analysing the replies to the questionnaire and clarifying the unclear topics. The replies consists of written free-form notes and comments to the items in the questionnaire and also one or a few eNB configuration files in Extensible Mark-up Language (XML) format. This project data are discussed in detail in subsection 3.3.2 and onwards.

The project data are analysed and eNB transport parameter interrelations are identified. Based on the findings more generic rules are introduced. This analysis considers the features of the given SW release and identifying the most complex ones. In this study a feature is consider to be a complex one if it has many parameters to be planned site by site and/or these parameters have impact on or relation to other eNB feature.

Another study branch is to identify the need to modify a parameter in roll-out phase and classify the parameters to two or a few categories based on the likelihood to a need to be modified. Based on the findings the actual number of parameter classes is defined. The findings are discussed in subsection 3.3.2 and onwards. Theoretical analysis is carried out later in this section.

Further on, the interrelations of the eNB transport features and their parameters are studied in chapter 4. The interrelations are studied within an eNB and also within a planning cluster of several eNBs. The configurations are then analysed and the common factors are identified. The target is to find an optimal set of predefined configurations which provides the required flexibility and which are simple enough to be managed in rapid network roll-outs in efficient manner.

In section 3.4, current best practices of the eNB access parameter planning are collected in network roll-out projects conducted by the case company. Five projects from two different market areas are studied. The used eNB transport features have an impact on the required parameters and thus the eNB transport features are analysed for each project. In this part, the study finds out the rules used to relate the eNB parameters in the projects. These rules are used to minimize the user entries in the eNB parameter database and thus minimize work effort and potential human errors.

Examples of simple rules as listed in Table 6.

Table 6. Example rules for parameter interrelations

Rules for parameter interrelations
The value of parameter y(i) is a copy of the value of parameter x(i).
The value of parameter y(i) is a copy of the value of parameter x(i) if condition c(i) is true.
The value of parameter y(i) is calculated based on parameter value x(i).
The value of parameter y(i) is calculated based on parameter value x(i) if condition c(i) is true.
The value of parameter y(i) is calculated based on parameter values x(i) and z(i).
The value of parameter y(i) is calculated based on parameter values x(i) and z(i) if condition c(i) is true.

An interrelation rule can be written in a form:

$$y(i) = f(x1(i), x2(i),\ldots,xn(i)). \tag{1}$$

Where

x1(i), x2(i), …, xn(i) are already defined parameters for eNB(i) and
y(i) is a resolved parameter for eNB(i).

And further more than one parameter can be resolved from the list of input parameters and thus the y(i) can be written to represent multiple resolved parameters y1(i), y2(i), …, ym(i). A group of these parameters can be marked shortly y(p,i). So far this inter-relation is limited for parameters of one single eNB. The expression can be further generalized when the common parameters for a given eNB cluster are considered. The generalised formulae can be written as:

$$y(p,i) = f(x1(i), x2(i), \ldots, xn(i), r1(j), r2(j), \ldots, rk(j)). \tag{2}$$

Where

x1(i), x2(i), …, xn(i) are already defined parameters for eNB(i),
r1(j), r2(j), …, rk(j) are already defined parameters for a cluster of eNBs the eNB(i) belongs to and
y(p,i) is a resolved parameter y(p) for eNB(i).

The interrelations applied in the studied cases are summarised in 3.4. Finally, the outcome of this study is presented in chapter 4

3.3.1 Questionnaire

The data collection form, the questionnaire, was implemented as a set of questions sent to selected project contact persons. Firsts a request to participate to this study was sent to group of potential contact persons, mainly planning engineers in various regions. Then the questionnaire was sent to the contact persons who showed interest and possibility to join the study in the given time frame.

The items in received responses were clarified if needed by means of using e-mail exchange with the project contact persons. The study analyses if any of the relevant rules to interrelate the different eNB transport parameters have been considered or used in a particular project.

The material was also collected through interviews and email exchange aimed at clarifying the on-line meetings and e-mails if needed. The material consists of the eNB transport parameters of one or a few eNBs and the list of rules and tools, if any, used to predefine some of the parameters. The rules were analysed and further development areas were studied.

In both the questionnaire and interviews, the following list of key experts were approached. The key data collection events are shown in Table 7.

Table 7. Key data collection events in this study.

Position in the company, region	Type of contact	Date
contact persons	Enquiry of possibilities to participate the study sent out to group of project contact persons.	29 June 2015
mobile access planners	Enquiry of possibilities to participate the study sent out to group of mobile access planners.	6 July 2015
mobile access planners	Questionnaire sent out.	9 July 2015
Planning engineer, MEA region	Email exchange, questionnaire return.	15 July 2015
mobile access planners	Gently reminder of the Questionnaire set out.	17 July 2015
Planning engineer 1. LAM region	Email exchange, questionnaire return.	18 July 2015
Planning engineer 2. LAM region	Email exchange, questionnaire return.	22 July 2015
Planning engineer 3. LAM region	Email exchange, questionnaire return.	22 July 2015
Planning engineer 4. LAM region	Email exchange, questionnaire return.	13 Aug 2015
Planning engineer 1. LAM region	Email exchange, clarifications.	21 Sep 2015
Planning engineer, MEA region	Email exchange, clarifications.	21 Sep 2015
Planning engineer, MEA region	Email exchange, clarifications.	22 Sep 2015
Planning engineer 4. LAM region	Email exchange, clarifications.	22 Sep 2015
Planning engineer 1. LAM region	Email exchange, clarifications.	22 Sep 2015
Planning engineer 3. LAM region	Email exchange, clarifications.	24 Sep 2015
Planning engineer 4. LAM region	Email exchange, clarifications.	30 Sep 2015
Planning engineer 3. LAM region	Email exchange, clarifications.	7 Oct 2015

For each rule, the responses to the following questions were collected: Can this rule be generalized? What could limit the generalization? Could it be valid for wide range of cases? How shall the rule be modified to make it more generic? Should the rule be limited to certain configurations only? Also the information that a rule was not used is interesting and further the reasons for not to apply a rule are very valuable for this study.

3.3.2 Experiment from Operator A

The first network to analyse is located in the Middle East and Africa region and the roll out speed at the time of study was approximately 100 integrated eNBs per month. The Nokia scope of network planning activities in this project included eNB radio planning, eNB access planning, EPC planning and mobile backhaul planning.

The first planning rule applied for eNB transport parameters in this project is the way how the IP addresses are allocated to the eNB applications: *“Subnets for application IP addresses are allocated in chunks of /20 subnets, and /22 subnet per application type. The rule within eNB is apparent from the following example. /20 subnet in below example = 10.150.34.0/20. Each application has a /22 subnet.”* The related XML configuration is shown in Listing 7.

```
<p name="uPlaneIpAddress">10.150.34.1</p>
<p name="cPlaneIpAddress">10.150.38.1</p>
<p name="sPlaneIpAddress">10.150.46.1</p>
<p name="mPlaneIpAddress">10.150.42.1</p>
```

Listing 7. The IP address block allocation rule applied in project A, a block of /22 network was assigned for each traffic plane.

No particular rule was identified for VLAN transport IP address allocation. These VLAN transport IP addresses are allocated independently from the application IP addresses. It was also noted in the answers that the LTE VLAN subnets are different from the 3G BTS VLAN subnet even the LTE BTS and the 3G BTS are located to the same site. The reason for different subnets in this project is that the IP allocation and planning for 3G was done by the other planner than the one who prepared the plans for LTE. Dedicated IP address ranges reduce the need to co-ordinate the allocation on daily basis and thus it is easier for the admin point of view.

In the answer there was a note about VLAN ID reuse: *“The same eNB VLAN IDs is often reused in different transport hubs, but seems that there is no rule for this.”* The related XML configuration is shown in Listing 8.

```
managedObject class="IVIF" distName="MRBTS-xxx536/LNBTS-
xxx536/FTM-1/IPNO-1/IEIF-1/IVIF-1" operation="create"
version= "LN7.0">
<p name="vlanId">3910</p>
<p name="localIpAddr">172.30.79.171</p>
<p name="netmask">255.255.255.224</p>
<p name="localIpv6Addr">0:0:0:0:0:0:0:0</p>
<p name="localIpv6PrefixLength">0</p>
<p name="sir">1000000</p>
<p name="sbs">4000</p>
<p name="qosEnabled">true</p>
<p name="wfqSchedQueueWeight">1000</p>
</managedObject>
```

Listing 8. The VLAN ID in IVIF-1 managed object in eNB XML file. VLAN IDs were reused but no particular rule to create the value was used.

In this network only one VLAN is used per eNB. In this case one default route per eNB is enough and thus no additional rules for routing definition was required.

The second identified planning rule in this project is that the network time protocol (NTP) server IP address is the same as the default gateway IP address. The provider edge (PE) router (eNB default gateway) to which the eNB is connected to supports NTP. It was noted in the answer that this approach leaves NTP traffic unencrypted and may be considered as a risk by some security enthusiast. The snapshot of the eNB configuration file below shows the same IP address value applied in two managed objects; in IPRT object where the static routes are defined and in the INTP object which contains address of the NTP server. The related XML configuration is shown in Listing 9.

```
<managedObject class="IPRT" distName="MRBTS-xxx536/LNBTS-
xxx536/FTM-1/IPNO-1/IPRT-1" operation="update" version=
"LN7.0">
<list name="staticRoutes">
<item>
```

```
<p name="destIpAddr">0.0.0.0</p>
<p name="netmask">0.0.0.0</p>
<p name="gateway">172.30.79.161</p>
…
</managedObject>
<managedObject class="INTP" distName="MRBTS-xxx536/LNBTS-
xxx536/FTM-1/IPNO-1/INTP-1" operation="update" ver-
sion="LN7.0">
<list name="ntpServers">
<p>172.30.79.161</p>
</list>
</managedObject>
```

Listing 9. The GW was also used as an NTP server for the given eNB. The same IP address value was reused in routing object (IPRT-1) and the Network Time Protocol object (INTP-1).

One potential planning rule came up in the clarification discussions. The QoS aware Ethernet switching feature was discussed. This feature is not needed on tail site but only in the chain sites or co-located sites where traffic for other BTS is connected to backhaul via the eNB integrated quality of service (QoS) aware Ethernet switch. Currently the QoS aware Ethernet switch feature is activated only for chain site but not for tail sites. It was discussed that even the QoS aware Ethernet switch is not required for tail site the feature activation would do no harm and thus this could be one potential action to harmonize the eNB setting cross the network. The required Ethernet ports need to be activated case by case on need basis applying the port specific settings in the eNB XML file. Listing 10 shows the QoS aware switching feature activation.

```
<managedObject class="L2SWI" distName="MRBTS-801536/LNBTS-
801536/FTM-1/L2SWI-1" operation="update" version="LN7.0">
...
<p name="enableLayer2Switching">true</p>
...
```

Listing 10. The QoS aware switching feature activation. To harmonize the setting cross different site type this feature could be activated not on in chain sites but also in the tail site.

This concludes the discussion about the case A and the discussion focuses now to the second case, case B.

3.3.3 Experiment from Operator B

This network is in the Latin America region. The average eNB integration rate is approximately 40 eNB per month. The Nokia scope in network planning activities in this project included eNB radio planning, eNB access planning and EPC planning.

The first rule mentioned in the response is the way the VLAN ID is defined. The VLAN ID definition in the eNB XML file is shown in Listing 11.

```
<managedObject class="IVIF" distName="MRBTS-xxx684/LNBTS-
xxx684/FTM-1/IPNO-1/IEIF-1/IVIF-1" operation="create"
version="LN5.0">
<p name="vlanId">80</p>  … text omitted …
<managedObject class="IVIF" distName="MRBTS-xxx684/LNBTS-
xxx684/FTM-1/IPNO-1/IEIF-1/IVIF-2" operation="create"
version="LN5.0">
<p name="vlanId">1580</p> …
<managedObject class="IVIF" distName="MRBTS-xxx684/LNBTS-
xxx684/FTM-1/IPNO-1/IEIF-1/IVIF-3" operation="create"
version="LN5.0">
<p name="vlanId">2080</p> …
<managedObject class="IVIF" distName="MRBTS-xxx684/LNBTS-
xxx684/FTM-1/IPNO-1/IEIF-1/IVIF-4" operation="create"
version="LN5.0">
<p name="vlanId">3080</p> …
<managedObject class="IVIF" distName="MRBTS-xxx684/LNBTS-
xxx684/FTM-1/IPNO-1/IEIF-1/IVIF-5" operation="create"
version="LN5.0">
<p name="vlanId">3580</p>
…
```

Listing 11. An XML file snapshot showing the VLAN ID setting applied in case B. The VLAN IDs are allocated in step of 500 for each traffic type.

The group of eNBs connected to the same aggregation point (GW) ware sharing the same VLAN and thus the same VLAN ID was assigned to them. The subnet size used in this project is /27. If the number of eNBs exceeded the available number of IP addresses in the /27 subnet the other /27 subnet was assigned for the same aggregation point.

Based on the eNB configuration XML file the eNB application addresses follows a similar rule as in case A. A snapshot of the parameter definition is shown in Listing 12.

```
<managedObject class="IPNO" distName="MRBTS-xxx684/LNBTS-
xxx684/FTM-1/IPNO-1" operation="update" version="LN5.0">
<p name="mPlaneIpAddress">10.243.13.164</p>
<p name="uPlaneIpAddress">10.243.77.164</p>
<p name="cPlaneIpAddress">10.243.141.164</p>
<p name="sPlaneIpAddress">10.243.205.164</p>
```

Listing 12. IP address block are allocated in step of /18 for different traffic types each step contains 16384 addresses to be divided further to subnets to be used for several eNB clusters.

No other obvious planning rule is identified in this case. The analysis continues with the third case, case C.

3.3.4 Experiment from Operator C

The third analysed network is also located in the Latin America region. The eNB integration rate at the time of study was approximately 160 eNBs per month. The Nokia scope of the network planning activities in this project included eNB radio planning, eNB access planning, IP backbone planning and mobile backhaul planning.

The first rule mentioned in the reply is the VLAN ID related rule. The eNB configuration contains four VLAN interfaces. The VLAN IDs are assigned for the eNB in steps of 100. The smallest VLAN ID in the example eNB is 3300 and the next 3400 and so on as. The eNB XML file snapshot showing the VLAN configurations are seen in Listing 13.

```
<managedObject class="IVIF" distName="MRBTS-xxx666/LNBTS-
xxx666/FTM-1/IPNO-1/IEIF-1/IVIF-2" operation="create"
version="LN5.0">
<p name="vlanId">3300</p>
<p name="localIpAddr">10.225.10.33</p>
…
<managedObject class="IVIF" distName="MRBTS-xxx666/LNBTS-
xxx666/FTM-1/IPNO-1/IEIF-1/IVIF-1" operation="create"
version="LN5.0">
<p name="vlanId">3400</p>
```

```
<p name="localIpAddr">10.224.234.33</p>
…
<managedObject class="IVIF" distName="MRBTS-xxx666/LNBTS-
xxx666/FTM-1/IPNO-1/IEIF-1/IVIF-4" operation="create"
version="LN5.0">
<p name="vlanId">3500</p>
<p name="localIpAddr">10.224.193.222</p>
…
<managedObject class="IVIF" distName="MRBTS-xxx666/LNBTS-
xxx666/FTM-1/IPNO-1/IEIF-1/IVIF-3" operation="create"
version="LN5.0">
<p name="vlanId">3600</p>
<p name="localIpAddr">10.224.170.33</p>
…
```

Listing 13. A snapshot of eNB XML file showing the VLAN ID assignment in case C. The VLAN IDs are assigned in steps of 100 for different traffic types.

The other planning rule mentioned in the reply is related to OMS IP address and NTP server IP address. For a regional cluster all eNBs assumes the same management system and the NTP server and thus the same IP address value is applied for all eNBs within the cluster.

In this project the eNB application addresses assumes the same IP address as the VLAN interface assigned for the given purpose. This rule can be identified based on the eNB configuration file. Listing 14 shows the eNB application IP address definition.

```
<managedObject class="IPNO" distName="MRBTS-xxx666/LNBTS-
xxx666/FTM-1/IPNO-1" operation="update" version="LN5.0">
<p name="mPlaneIpAddress">10.224.170.33</p>
<p name="uPlaneIpAddress">10.224.234.33</p>
<p name="cPlaneIpAddress">10.225.10.33</p>
<p name="sPlaneIpAddress">10.224.193.222</p>
```

Listing 14. A snapshot of eNB application IP address definition in the eNB XML file. The addresses are equal to the VLAN interface IP addresses shown in Listing 13.

No other obvious planning rule is identified in this case. The next studied case, case D, is also from the Latin America region.

3.3.5 Experiment from Operator D

The next analysed case is also from the Latin America region. The average roll-out speed in this project was 80 eNBs per month at the time of the study. The Nokia scope of the network planning activities in this project included eNB radio planning, eNB access planning and Mobility Management Entity (MME) part of the Evolved Packet Core (EPC) planning.

The first planning rule mentioned in the response in this case is the assignment of eNB application IP addresses. The applications assume VLAN interface IP address:

> *"- IVIF-1 'localIpAddr' = IPNO 'cPlaneIpAddress'*
> *- IVIF-2 'localIpAddr' = IPNO 'uPlaneIpAddress'*
> *- IVIF-3 'localIpAddr' = IPNO 'mPlaneIpAddress'*
> *- IVIF-4 'localIpAddr' = IPNO 'sPlaneIpAddress'"*

The second rule mentioned in the reply is the ID assignment: *"- MRBTS_ID = LNBTS_ID"* It was also noted that the LNBTS IDs within a planning cluster are assigned in sequence: *"- New eNB´s LNBTS ID = LNBTS ID + 1 of the last eNB planned inside same eNB´s area."*

Other common parameters within planning cluster were Timing over Packet (ToP) master IP address and Primary OMS IP address. The XML snapshot is shown in Listing 15.

```
<managedObject class="IPNO" distName="MRBTS-xxxx12/LNBTS-
xxxx12/FTM-1/IPNO-1" operation="update" version="LN5.0">
...
<p name="oamIpAddr">10.231.1.4</p>
...
<managedObject class="TOPF" distName="MRBTS-xxxx12/LNBTS-
xxxx12/FTM-1/TOPB-1/TOPF-1" operation="create" ver-
sion="LN5.0">
<p name="actTopFreqSynch">true</p>
<p name="logMeanSyncValue">-4</p>
<p name="masterIpAddr">10.105.115.148</p>
</managedObject>
```

Listing 15. Common parameters used for the whole planning cluster in this project are the operating and management system (*oamIpAddr*) and ToP master IP address (*masterIpAddr*).

No other planning rules were identified in this case. The discussion continues with the next case, case E.

3.3.6 Experiment from Operator E

This network is also in the Latin America region. The average roll-out speed in this project was 50 eNBs per month at the time of the study. The Nokia scope of network planning activities in this project included eNB radio planning and eNB access planning.

In this project templates were used to manage parameters which are common for group of sites. One of these templates contains parameters for egress shaper. The parameter values depend on the available backhaul capacity. An item in a template, containing all relevant parameter for the egress shaper, was referred using a value which was directly derived from the available backhaul capacity. For example for backhaul capacity of 50000 kbps the template ID of 50 was used.

A formula was used to calculate the scheduling weights based on the available backhaul capacity. The amount of ToP synchronisation traffic does not depend on the user plan traffic volumes and thus the share of ToP synchronisation traffic decreases when the user plane traffic volume increases. The scheduling weight parameters are illustrated in Listing 16.

```
<managedObject class="IVIF" operation="create" version=
"LN6.0" distName="MRBTS-xxx755/LNBTS-xxx755/FTM-1/IPNO-
1/IEIF-1/IVIF-1">
…
<p name="wfqSchedQueueWeight">70</p>
<p name="vlanId">1592</p></managedObject>
<managedObject class="IVIF" operation="create" version=
"LN6.0" distName="MRBTS-xxx755/LNBTS-xxx755/FTM-1/IPNO-
1/IEIF-1/IVIF-2">
<…
<p name="wfqSchedQueueWeight">830</p>
<p name="vlanId">1532</p></managedObject>
<managedObject class="IVIF" operation="create" version=
"LN6.0" distName="MRBTS-xxx755/LNBTS-xxx755/FTM-1/IPNO-
1/IEIF-1/IVIF-3">
…
<p name="wfqSchedQueueWeight">50</p>
```

```
<p name="vlanId">1502</p></managedObject>
<managedObject class="IVIF" operation="create" version=
"LN6.0" distName="MRBTS-xxx755/LNBTS-xxx755/FTM-1/IPNO-
1/IEIF-1/IVIF-4">
…
<p name="wfqSchedQueueWeight">15</p>
<p name="vlanId">1562</p></managedObject>
```

Listing 16. A snapshot of the eNB XML file showing the Weighted Fair Queue (WFQ) weights. The weights defines the share of link capacity to be scheduled for the given queue.

Also the limits used for Transport Admission Control (TAC) were calculated as a percentile of the egress Shaping Information Rate (SIR). The TAC and SIR settings are shown in Listing 17.

```
<managedObject class="LTAC" operation="create" version=
"LN6.0" distName="MRBTS-xxx755/LNBTS-xxx755/FTM-1/TAC-
1/LTAC-1">
<p name="tacLimitGbrEmergency">25000</p>
<p name="tacLimitGbrHandover">22500</p>
<p name="tacLimitGbrNormal">20000</p>
…
<managedObject class="IEIF" operation="create" version=
"LN6.0" distName="MRBTS-xxx755/LNBTS-xxx755/FTM-1/IPNO-
1/IEIF-1">
…
<p name="sirTotal">20000</p>
…
```

Listing 17. A snapshot of the eNB XML file showing the Transmission Admission Control limits and the shaping rate.

It was pointed out in the reply that many parameters (the far end IP addresses for SCTP, GTP supervision, ToP server and O&M) are the same for the cluster of the eNBs. These parameter values can be copied in all eNB files within the planning cluster. Also VLAN IDs are in some cases the same for all eNBs within the planning cluster. The HW templates are in most case the same for all eNBs.

3.4 Summary of Studied Cases

The analysed networks contain different features and follow different approaches in planning. The eNB HW product in all studied cases is *Nokia Flexi Multiradio 10 BTS*. Most of the analysed cases are running in RL50 release level. One case is in RL60 and one in RL70 release level. The applied planning rules depend on the used features and planning strategies. Among these studied case one feature was identified to have big impact on the selected rules and this in the IP Security feature. The IP security is operating in tunnel mode and thus it hides the application IP addresses from the transport IP network.

When the applied planning rules are generalised the following rule types can be identified. The generalised rule types are listed in Table 8.

Table 8. Identified rule types.

Rule type
The same eNB specific value is applied for several parameters within an eNB
The value is derived from the other parameter value by adding a constant offset value
The value is derived from the other parameter value by multiplying with a constant factor
Pseudo parameter is used as a root to generate value or values for eNB parameters
Common cluster specific values are used for several eNBs
Common network level values applied for all eNBs

The following section lists a few examples of each rule type. The most common case of applying the same value to more than one eNB transport parameter can be found in IP addressing. Four out of five examined cases applied the rule having application IP address equal to VLAN interface IP address. A snapshot of the eNB XML file highlighting the use of rule type 1 is shown in Listing 18.

```
<managedObject class="IVIF" distName="MRBTS-xxx684/LNBTS-
xxx684/FTM-1/IPNO-1/IEIF-1/IVIF-1" operation="create"
version="LN5.0">
<p name="vlanId">80</p>
<p name="localIpAddr">10.243.13.164</p>
...
<p name="vlanId">1580</p>
```

```
<p name="localIpAddr">10.243.141.164</p>
...
<p name="vlanId">2080</p>
<p name="localIpAddr">10.243.205.164</p>
...
<p name="vlanId">3080</p>
<p name="localIpAddr">10.243.77.164</p>
...
<p name="vlanId">3580</p>
<p name="localIpAddr">10.36.44.68</p>
...
<managedObject class="IPNO" distName="MRBTS-xxx684/LNBTS-
xxx684/FTM-1/IPNO-1" operation="update" version="LN5.0">
<p name="mPlaneIpAddress">10.243.13.164</p>
<p name="uPlaneIpAddress">10.243.77.164</p>
<p name="cPlaneIpAddress">10.243.141.164</p>
<p name="sPlaneIpAddress">10.243.205.164</p>
...
<p name="addCPlaneIpv4Address">10.36.44.68</p>
<p name="addUPlaneIpv4Address">10.36.44.68</p>
```

Listing 18. An example of rule type 1. Common rule applied in four out of the five studied case. Application IP addresses assumes the same values as the associated VLAN interface.

The rule is also summarised in the form of a table. This can be seen in Table 9. The additional C-plane and U-plane VLAN and addresses are used for the second operator in case of network sharing.

Table 9. An example of rule type 1. Application IP address assumes VLAN interface IP address (case B).

VLAN ID	VLAN interface IP address	Application	Application IP address
80	10.243.13.164	M-plane	10.243.13.164
1580	10.243.141.164	U-plane	10.243.141.164
2080	10.243.205.164	C-plane	10.243.205.164
3080	10.243.77.164	S-plane	10.243.77.164
3580	10.36.44.68	Additional C-plane	10.36.44.68
3580	10.36.44.68	Additional U-plane	10.36.44.68

Within these studied cases the most common parameter which value is derived from another eNB transport parameter by adding a constant offset VLAN id. Applying the rule type 2 in studied cases is summarised in Table 10.

Table 10. An example of rule type 2. Rule to define the value for VLAN ID by adding a constant.

VLAN	#1	#2	#3	#4	#5	Step[1]
Case A	3910					
Case B	80	1580	2080	3080	3580	500
Case C	3300	3400	3500	3600		100
Case D	500	501	502	503		1
Case E	1502	1532	1562	1592		30

Note 1. Not all possible step values applied for eNB in case B.

An example of applying the third identified rule is taken from transport admission control (TAC). There are three different limits to be set for the TAC; one for normal traffic the second limit is applied for incoming hand over traffic and the third limit is applied for emergency traffic. An example XML snapshot where the rule type 3 is applied is shown in Listing 19.

```
<managedObject class="LTAC" distName="MRBTS-xxx666/LNBTS-
xxx666/FTM-1/TAC-1/LTAC-1" operation="update" version=
"LN5.0">
<p name="tacExludeL2Overhead">false</p>
<p name="tacActivityFactor">100</p>
<p name="tacLimitGbrNormal">105000</p>
<p name="tacLimitGbrHandover">120000</p>
<p name="tacLimitGbrEmergency">150000</p>
…
```

Listing 19. A snapshot of the eNB XML file showing the Transmission Admission Control limits. The limits are derived from a base value by multiplying with the constant. This is an example of rule type 3.

The multiplying is not visible in the final outcome, the XML file, as it contains individual values for the parameters. The multiplication is illustrated in Table 11.

Table 11. An example of rule type 3. A rule to define limits for Transport Admission Control (TAC) (Case C).

Parameter name	Reference value	Multiplier	Applied value
tacLimitGbrNormal	150000	0.7	105000
tacLimitGbrHandover	150000	0.8	120000
tacLimitGbrEmergency	150000	1.0	150000

The method of using network parameter which is not visible directly in an eNB was mentioned in case E discussions. This kind of parameter can be called pseudo parameter in the eNB point of view. The User Network Interface (UNI), the eNB is interfacing to, has two capacity attributes; Committed Information Rate (CIR) and Excess Information Rate (EIR). Either of these is directly applied as eNB transport parameter, however, these may be used as a reference value to calculate some of the actual parameter values for the eNB.

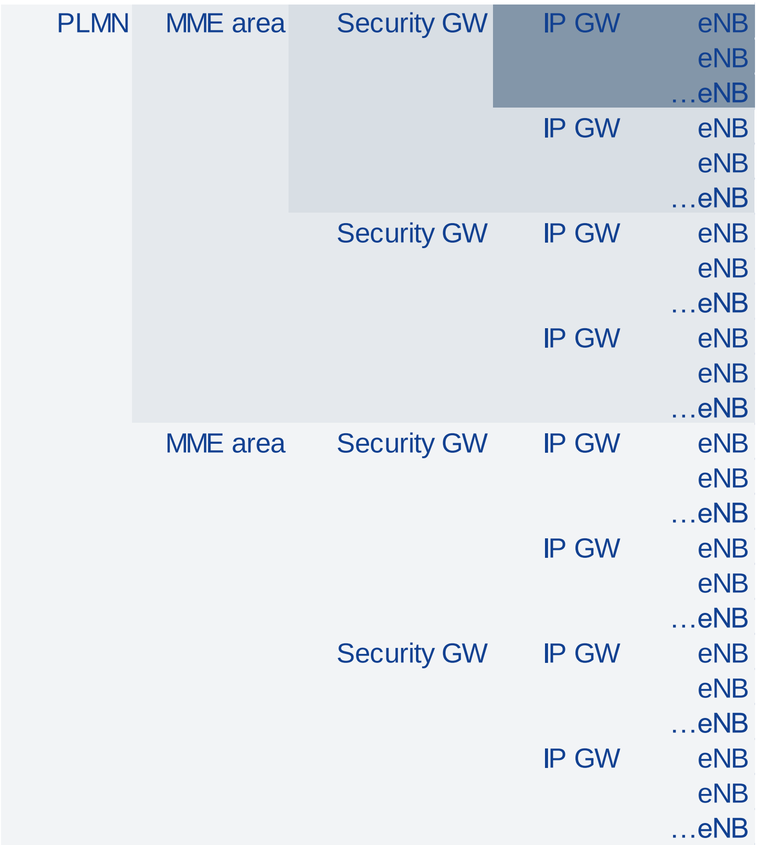
The CIR at UNI must be equal or greater than the Guaranteed Bit Rate (GBR) traffic in the eNB. The shaping rate applied in uplink (UL) at UNI shall not exceed the sum of CIR and EIR. On the other hand there is no point to apply shaping lower rate than the sum of CIR and EIR as in that case some transport capacity would remain unused. Thus the shaping rate shall be equal to the sum of CIR and EIR. Table 12 shown an example of applying pseudo parameter to define the values for the actual eNB parameters.

Table 12. An example of rule type 4. A pseudo parameter (UNI CIR) used as a reference to determine a value for actual eNB parameter (Case E).

Parameter name	UNI CIR as a reference value (from the eNB point of view this is pseudo parameter as it is not defined in eNB configuration file)	Multiplier	Applied value
tacLimitGbrNormal	30000	0.67	20000
tacLimitGbrHandover	30000	0.75	22500
tacLimitGbrEmergency	30000	0.83	25000

A planning cluster is a set of eNBs which are planned together in a limited time span. All eNBs within a planning cluster share the cluster specific parameters. The cluster can be small containing a few eNBs within the same IP subnets. These eNBs share the same IP gateway (GW). The cluster may be as large as a Mobility Management Entity (MME) area. In this case all eNBs share the same MME IP address as a first contact point for S1 interface Application (S1AP) signalling. Typically the cluster is something in between the abovementioned ones.

Figure 16 shows an example of typical planning clusters. The smallest cluster is a group of eNBs within the same subnet and these eNBs share the same IP GW. The next cluster in the given example is the security GW area. In this case all eNBs share the same security GWs. However, the IP GW is not necessary the same for all eNBs. The next level of cluster is the Mobility Management Entity (MME) area and the last mentioned in Figure 16 is the whole network (PLMN).



PLMN	MME area	Security GW	IP GW	eNB
				eNB
				…eNB
			IP GW	eNB
				eNB
				…eNB
		Security GW	IP GW	eNB
				eNB
				…eNB
			IP GW	eNB
				eNB
				…eNB
	MME area	Security GW	IP GW	eNB
				eNB
				…eNB
			IP GW	eNB
				eNB
				…eNB
		Security GW	IP GW	eNB
				eNB
				…eNB
			IP GW	eNB
				eNB
				…eNB

Figure 16. An example of planning clusters. IP GW cluster (also called VLAN cluster) is the smallest planning cluster. The security GW cluster is the second level cluster (applicable when IPsec is applied). The Mobility Management Entity (MME) area is the third cluster and finally the whole Public Land Mobile Network (PLMN) is the last cluster.

The last identified rule considers parameters which have the same value for all eNBs. These are planned once and are applied for all eNBs typically applying planning templates. Great deal of the eNB transport parameters falls in to this category. These include for example most of the Ethernet interface and QoS related parameters. Traffic marking and classification needs to be consistent within a network and thus parameters controlling marking and classification are typically the same for all eNBs.

4 Development of Parameter Models

The aim of the eNB transport parameter model is to define parameter interrelations in a way that only a few manual entries are needed to generate the values for vast number of actual parameters in eNB managed objects. The focus in this study is the eNB transport parameters which need to have a case specific value within a planning cluster. The parameters, having common value within a planning cluster, can be managed by applying predefined values in planning templates.

Based on the studied cases two main categories of case specific parameters were identified. The first category contains capacity related parameters such as queue weights, shaping rate and transport admission control limits and the second category includes addresses and identifiers mainly IP addresses and VLAN IDs. These two categories do not seem to have direct interrelations and thus the models related to these are discussed separately. The model for capacity related parameters is discussed first as it has a limited set of parameters and their combinations to consider.

4.1 Interrelation Rule Metrics

To be able to compare different scenarios the metrics for the interrelations rules are defined. One metric is a complexity. In this study the complexity is defined as a number of input entries required to create case specific transport parameters for the eNB managed objects for one eNB assuming a base configuration as a reference. In other words the number of eNB parameters which needs to be modified from the base configuration. Figure 17 illustrates complexity metric. In this example one parameter needs to be modified from base values in order to create the parameter set for eNB-1.

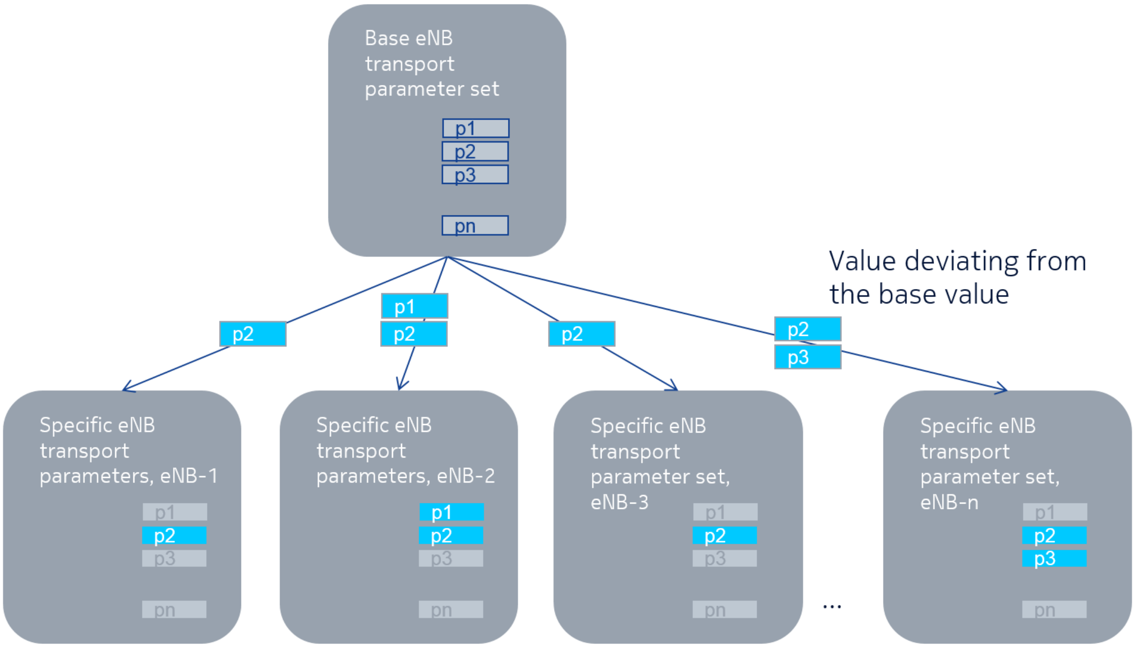

Base eNB transport parameter set
p1
p2
p3
pn
Value deviating from the base value
p2
p1
p2
p2
p2
p3
Specific eNB transport parameters, eNB-1
p1
p2
p3
pn
Specific eNB transport parameters, eNB-2
p1
p2
p3
pn
Specific eNB transport parameter set, eNB-3
p1
p2
p3
pn
...
Specific eNB transport parameter set, eNB-n
p1
p2
p3
pn

Figure 17. An illustration of the complexity metric. The complexity index indicates the average number of parameters which deviates from the base configuration value. The complexity index is a decimal number as some of the deviated parameters are applied for a cluster of eNBs and thus the impact on one eNB is a small fraction only.

Some of the modified parameters are unique for each eNB while other may be common for all the eNB in a cluster. To take this into an account the complexity metric can be written in to the following form:

$$cx(i) = n1(i) + n2(i)/k1 + n3(i)/k2 + n4(i)/k3 + \ldots . \qquad (3)$$

Where

cx(i) is the number of parameters which needs to be resolved for eNB-i,
n1(i) is the number of parameters which are unique for the eNB-i,
n2(i) is the number of parameter which are unique for the cluster k1,
n3(i) is the number of parameter which are unique for the cluster k2,
n4(i) is the number of parameter which are unique for the cluster k3,
k1 is the number of eNBs in the cluster k1,
k2 is the number of eNBs in the cluster k2 and
k3 is the number of eNBs in the cluster k3.

The parameters n() are considered to be input for the interrelation rules. The parameters k() indicates the number of eNBs in the given cluster. The ratio n()/k() is a share of parameters per one eNB in this complexity calculation. The *cluster k1* is typically VLAN cluster, VLAN ID and the IP GW are a common for all eNBs within the VLAN cluster. The subnet size limits the number of eNBs in the VLAN cluster. The k1 values in studies cases fall in a range from 1 to 29 based on the used subnet sizes. The *cluster k2* could be a security GW cluster, the *cluster k3* the Mobility Management Entity (MME) cluster. Other clusters may also exist in the network for example timing over packet (ToP) server cluster, two way active measurement protocol (TWAMP) reflector cluster etc.

The smaller the complexity, cx(i), the better, as fewer input entries are required to define the parameters. However, to compare just the complexity is not enough as the required functionality may introduce other parameters and the complexity metric does not consider the benefit of these additional parameters.

The second metric is a process efficiency index. The process efficiency metric is defined by dividing the number of calculated parameters (m) by the required input parameters (complexity). The higher the process efficiency metric the more output parameters are determined per input parameter count. The process efficiency metric indicates how efficient the eNB parameter interrelation rule is. This process efficiency metric shall not be confused with the eNB operational efficiency. In other words the high process efficiency metric does not guarantee high operational efficiency. The actual parameter values defines the eNB operational efficiency. The process efficiency metric formula is writes as:

$$pe(i) = m/cx(i). \tag{4}$$

Where

pe(i) is the calculated process efficiency metric,

m is the number of eNB parameters which deviates from the base line set (output of the interrelation rules) and

cx(i) is the calculated complexity metric for eNB(i) (number of inputs required for the interrelation rules).

The process efficiency pe(i) metric is used to compare different scenarios to each other and the higher the metric the higher is the process efficiency. The n(3) and n(4) are assumed to be small and the k(2) and k(3) large and thus these terms are not included in the further calculations used in this study. The complexity is calculated according to the following formulae:

$$cx(i) = n1(i) + n2(i)/k1. \tag{5}$$

In this study the comparison calculations are done for three different cluster sizes. The most common subnet size among the studied cases is /27 (netmask 255.255.255.224). This subnet has 30 usable IP addresses out of which one is assumed for the GW router. Roughly 30% of the address space is assumed to be reserved for future use and thus out of 29 potential eNB IP addresses 20 is assumed to be taken in use in day one.

In a similar manner for subnet /29 (netmask 255.255.255.248) out of 5 potential eNB IP addresses 3 are assumed for eNBs. One more subnet size used for comparison is /25 (netmask 255.255.255.128). This gives 125 free addresses for eNBs out of which 80 is assumed to be available for allocation on day one while the rest are reserved for future usage. The interrelation rules in different scenarios are compared and the results are represented in a table. A table format is shown in Table 13.

Table 13. A template used for scenario metrics comparison. The metrics are calculated for three different VLAN cluster sizes.

Scenario	Metric	Cluster size		
		3 eNBs	20 eNBs	80 eNBs

1	cx(i)
	pe(i)			

2	cx(i)
	pe(i)			

3	cx(i)
	pe(i)			

This concludes the theoretical discussion about the metrics used to compare the scenarios. The next sections introduce the eNB parameter model and calculate the metrics for the introduced scenarios.

4.2 Generic eNB Transport Parameter Model

The generic eNB transport parameter model defines the required input entries, required parameters in eNB managed objects and optional functions used to calculate the parameter values for a given network scenario. Network scenarios are selected so that a roll-out project applies typically only one scenario within a planning cluster. The aim is to minimise the number of required input entries for the each network scenario by applying the same input entry to many eNB managed object parameters. The input entry can be applied directly or it can be used as an input for an optional calculation used to form one or many eNB managed object parameters. A generic model of parameter interrelations is shown in Figure 18.

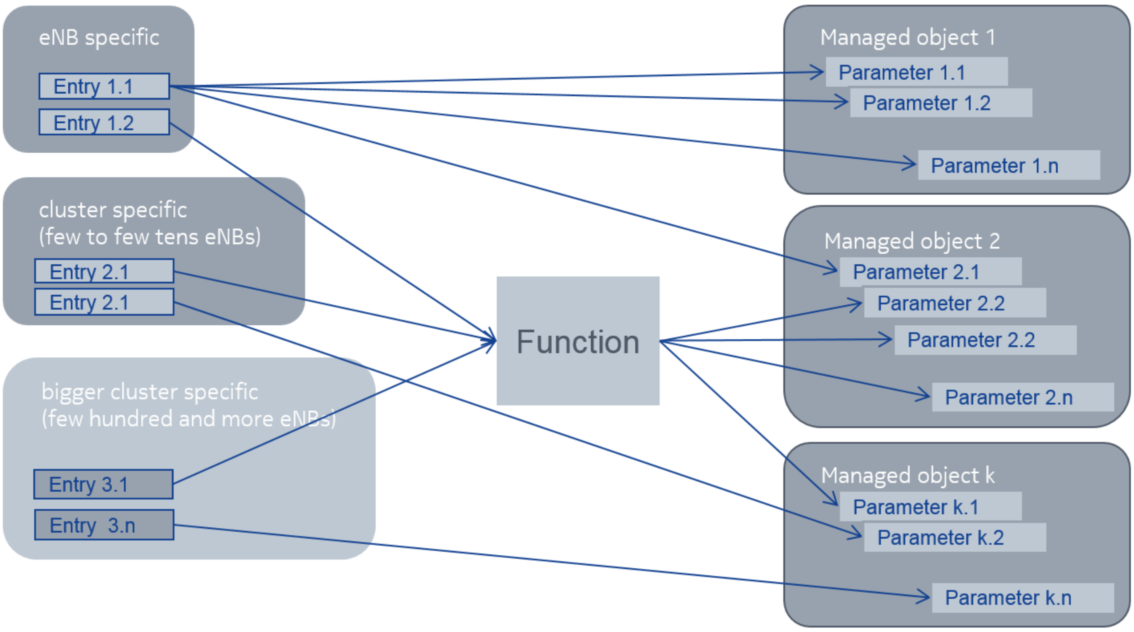


Figure 18. A generic eNB transport parameter model with interrelation rules. The eNB specific, cluster specific and bigger cluster specific input entries are used to determine the parameters in the eNB managed objects. A managed object parameter assumes a value of an input entry or a result of a function.

In this study the eNB transport parameters and thus the input entries are divided into four main categories based on how specific the parameter value is in the eNB within a planning cluster. The parameter categories are; global and network level, cluster level, capacity step or type specific and eNB specific.

The main focus is to minimise the eNB specific and the first cluster specific entries as these have the biggest impact on the complexity (cx(i)) and the process efficiency (pe(i)) as indicated by the equations (3) and (4).

A parameter belongs to the global parameter category if the same value is assumed globally for all eNBs. Global parameter value assumes a factory default value or a value generally recommended by the system vendor. By definition a global parameter is not modified. However, if a parameter which typically belongs to global category needs to be modified it can be done but after modification the parameter is no longer considered to belong to that category anymore.

A parameter belongs to network level category if it is not a global one and the same value is assumed for all eNBs within a network. A value for network level parameter is defined once for the whole network. All eNBs within the network assumes identical value. From the parameter planning point of view both global and network level parameters are straightforward to manage in the planning phase as the same copy is applied for all eNBs. This can be done for example by creating a baseline parameter template which is used as a basis for individual parameter files.

A parameter belongs to cluster level parameter category when its value has an equal value in all eNB within a cluster but it may be different in other cluster. For example VLAN cluster level parameter includes VLAN ID, subnet size and IP gateway address or addresses. From the parameter interrelation rules point of view the smallest of the nested clusters is the dominant one while the impact of larger clusters on the process efficiency and the complexity metrics is negligible.

A parameter belongs to capacity step or type specific parameter category when its value is typical for the given capacity step or site type. This category contains parameters which are related to eNB capacity or site type; for example tail site versus chain site. The tail sites have only one Ethernet port activated while the chain sites have two active ports to allow connectivity to the next site in the chain. The capacity step has an impact on the admission control thresholds and shaping rates. These are specific for the given capacity step rather than individual eNB.

The last parameter category to discuss is the eNB specific parameter category. This category includes the eNB specific IP addresses and other identifiers. Parameters which are unique per eNB consist mainly of IP addresses.

4.3 Modelling Capacity Related eNB Transport Parameters

The User Network Interface (UNI) bandwidth attributes; Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIR) and Excess Burst Size (EBS) needs to be aligned with traffic requirement of the given eNB. The eNB Peak Information Rate (PIR) at the transport interface is limited by the given eNB radio interface configuration for example available bandwidth (for example 5, 10, 20 MHz), transmission mode (for example TM1, TM4, TM9), multiple-in-multiple-out (MIMO) configuration (for example 2*2, 4*4) and number of radio cells in the given eNB.

The eNB egress rate may also be limited to configurable limit at the shaper function shown in Figure 19. The policing function at mobile backhaul network side of the UNI may discard the traffic which violates the bandwidth profiles. To avoid violating the bandwidth profiles at UNI the egress shaper shall be used to limit the transmit rate in controlled manner already in the eNB.

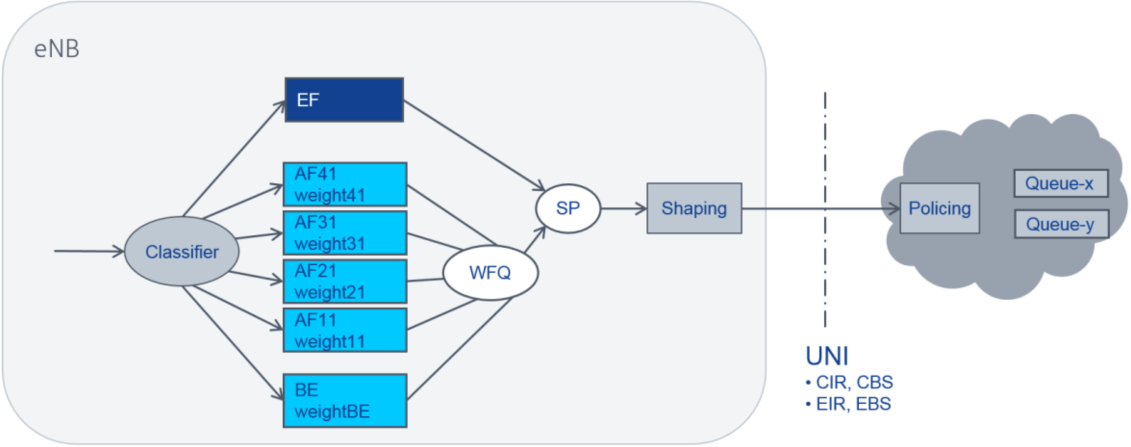


Figure 19. The traffic engineering functions; queuing and shaping in the eNB and policing in the backhaul side of the UNI. The eNB shall shape the egress traffic in order to avoid violating the UNI bandwidth profile. Violation may cause traffic loss at policer. Adopted from [20].

The first rule defines interrelation between the shaping rate and the peak information rate. The shaping information rate (sir) shall be equal to Peak Information Rate (PIR). This rule can be written in the following mathematical form:

$$\text{sir} = \text{PIR}. \tag{6}$$

Where

$$\text{PIR} = \text{CIR} + \text{EIR}, \tag{7}$$

$$\text{EIR} >= 0. \tag{8}$$

In case the bandwidth profiles are defined in the UNI level the shaping is done at UNI level as well and if the bandwidth profiles are defined in Ethernet virtual connection (EVC) level the shaping is applied in VLAN level in the eNB as an eNB VLAN is associated with an EVC at the UNI.

The acceptable burst size depends on the queuing capabilities of the backhaul nodes. A safe value can be agreed to be used cross the whole planning cluster. Only if User Network Interface (UNI) Committed Burst Size (CBS) or Excess Burst Size (EBS) is exceptional small the shaper burst size needs to be specifically optimised for the given UNI. A safe value is small but large enough to carry the largest possible IP packet. The small Committed Burst Size (CBS) value is also seen to improve efficient Transmission Control Protocol (TCP) throughput (TCP goodput) [39]. The second rule defines the relation between the Maximum Transmission Unit (MTU), the shaping burst size and the Committed Burst Size (CBS). This rule can be written as:

$$\text{MTU} < \text{shaping burst size} < k^*(\text{MTU}) < \text{CBS}. \tag{9}$$

Where k is typically a small value for example 1.5 to 5.

The burst size must be larger than the MTU to avoid the shaper being blocked in case a packet larger than the burst size is to be scheduled. The terms in the rule are given in network level (L3) including IP header and payload. The Committed Burst Size (CBS) in Metro Ethernet Forum (MEF) documentation is given as bytes in a service frame thus including Ethernet header as well and thus the CSB in L3 level (CBS_L3) needs to be adjusted to the corresponding CSB at L2 level (CSB_L2) by adding the number of bytes in Ethernet header and possible VLAN tag.

To analyse the queuing system shown in Figure 19 first the Guaranteed Bit Rate (GBR) traffic is considered. The GBR traffic is typically real time traffic which is sensitive to delays and thus the classifier typically allocates the Expedited Forwarding (EF) queue for the GBR traffic.

The User Network Interface (UNI) Committed Information Rate (CIR) parameter value can also be linked to limits used for the Transmission Admission Control (TAC) applied for Guaranteed Bit Rate (GBR) traffic. The minimum theoretical value for UNI CIR would be equal to the highest TAC limit which is the limit for emergency traffic. In practice some capacity for non-GBR traffic needs also be assumed when CIR value is defined. In general terms the rule can be written as:

$$\text{CIR} > \text{TAC emergency limit} > \text{TAC hand over limit} > \text{TAC normal limit}. \qquad (10)$$

All these four values are typically configuration dependent thus in order to maintain different configurations all these four items needs to be updated. To minimize the number of case specific items a factor (k) is introduced. Applying this factor the formula can be written in the following form where one parameter is used as a master and the other ones are calculated based on that. Anyone out of these four parameters could be a valid master parameter and in this example *TAC normal limit* was chosen to act as master parameters. Applying factor k for terms in formulae (9) the following interrelations can be written:

$$\text{TAC hand over limit} = k1 * \text{TAC normal limit} \qquad (11)$$

$$\text{TAC emergency limit} = k2 * \text{TAC normal limit} \qquad (12)$$

$$\text{CIR} >= k3 * \text{TAC normal limit}. \qquad (13)$$

Where

$$1 < k1 < k2 < k3. \qquad (14)$$

In this approach the k1, k2 and k3 are constants which are selected on network level rather than site level. This leaves only one parameter to be defined on configuration or site level.

The potential range of the Committed Information Rate (CIR) can be written the following form:

$$k3 * \text{TAC normal limit} <= \text{CIR} <= \text{PIR}. \quad (15)$$

So far only the Guaranteed Bit Rate (GRB) traffic was considered. Next the Assured Forwarding (AF) and Best Effort (BE) traffic classes are also considered and the impact of AF and BE traffic on CIR is elaborated. The use of AF traffic classes depends on the applications and services operator want to offer to the subscribers. In this model the required bandwidth of each AF class is assumed to be given as an input. Also the minimum bandwidth of the best effort (BE) is considered to be an input. The formula for the Committed Information Rate (CIR) can be written as:

$$\text{CIR} >= \text{BWGBR} + \text{BWAF} + \text{BWBE}_{min}. \quad (16)$$

Where

BWGBR is the bandwidth for GBR traffic (k3 * TAC normal limit),
BWAF is the bandwidth requirement for all AF classes and
BWBE_{min} is the minimum requirement of bandwidth for BE traffic class.

The bandwidth requirement for AF traffic classes can be further divided to the requirements for each AF class and AF queue shown in Figure 19:

$$\text{BWAF} = \text{BWAF41} + \text{BWAF31} + \text{BWAF21} + \text{BWAF11}. \quad (17)$$

Where

BWAF41 is the bandwidth requirement for AF41 traffic class,
BWAF31 is the bandwidth requirement for AF31 traffic class,
BWAF21 is the bandwidth requirement for AF21 traffic class and
BWAF11 is the bandwidth requirement for AF11 traffic class.

The next step is to define the weights for the queueing system. In the weighted fair queueing (WFQ) the weight is used to control the relative share of resources the given queue is about to get. The share the queue *i* is served is a ratio of the weight of the queue *i* to the sum of weights of the all queues in the queueing system. To make the weight values easier to interpret the sum can be selected to be a round figure for example 100,

$$100 = weight41 + weight31 + weight21 + weight11 + weightBE. \qquad (18)$$

In this case the weight value of 20 indicates the 20% share for the given queue. Applying formulae (18) the available bandwidth for the AF41 queue can be written as:

$$BWAF41 = BWWFQ * weight41/100. \qquad (20)$$

Where

BWWFQ is the total available bandwidth for the WFQ scheduler.

The BWWFQ can be written based on the Guaranteed Bit Rate (GBR) traffic and User Network Interface (UNI) Committed Information Rate (CIR) values in the following form:

$$BWWFQ = CIR – BWGBR. \qquad (21)$$

And the bandwidth for AF41 queue can further be expressed as:

$$BWAF41 = (CIR – BWGBR) * Weight41/100. \qquad (22)$$

In the similar manner a bandwidth for any queue in the WFQ system can be defined.

The interdependencies of the eNB transport capacity control parameter are visualised in Figure 20. The input parameters can be seen in the left hand side. The peak rate can be based on the eNB air interface configuration or optionally on the limit given manually. The limiting factor may be the available backhaul link capacity rather than the air interface capability and thus this manual limit is required in some cases.

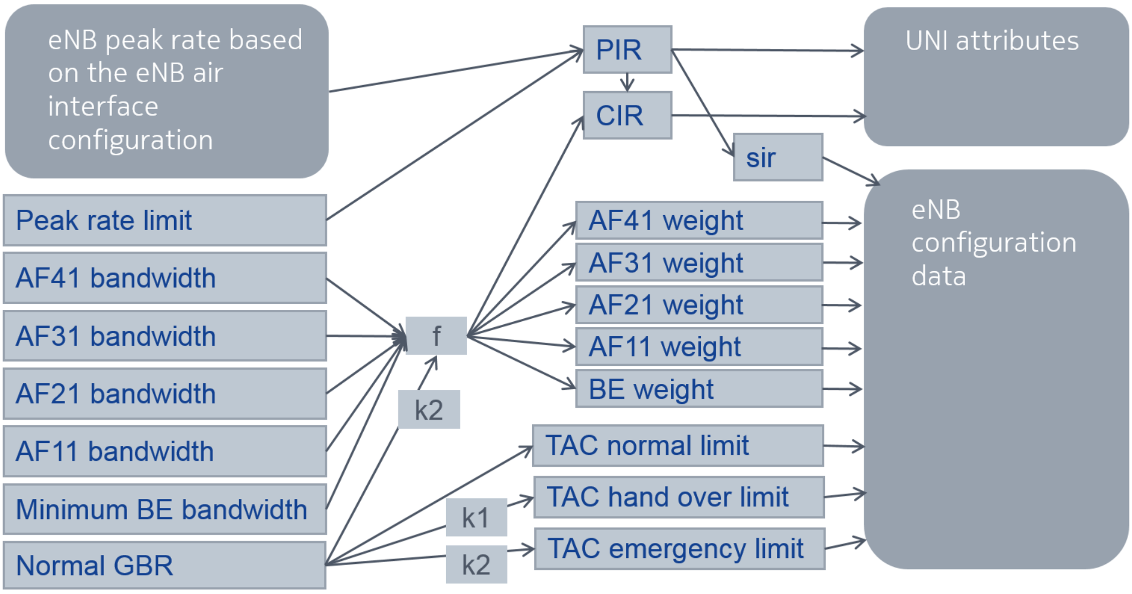


Figure 20. A model of the capacity related parameters interdependencies, model 1. The target amount of traffic in each traffic class is used as an input to generate the required WFQ weights, Transport Admission Control (TAC) limits and the shaping information rate (*sir*).

Figure 20 shows an approach where the bandwidth requirements are given separately for each traffic class that is for each Assured Forwarding (AF) queue. In cases where the share of bandwidth requirements between the traffic classes is constant from an eNB to another the approach can be modified so that the bandwidth requirement of one traffic class and the relative shares are given as input instead of the absolute values. That approach scales well for different total traffic volumes.

The last input parameter in Figure 20 is *the normal GBR*. The normal Guaranteed Bit Rate (GBR) is used to define the Transport Admission Control (TAC) limits and it is also essential input for the Committed Information Rate (CIR) calculation. In this model the normal GBR parameter is left to be given as a manual entry. In further studies inter-dependencies between the radio parameters and the optimal GBR value may be defined. The k1, k2 and k3 represent constants at least in the cluster level maybe on the network level as well. Finally in the right hand side the solved parameters are shown. The most of them are used in the eNB configuration data and two as the UNI attributes and thus affects the configuration of the network side node. The metrics for the interrelation rule is shown in Table 14.

Table 14. A scenario metrics comparison for capacity parameters. The impact of the number of unique input entry sets on metrics with three different cluster size. The process efficiency is very high in large cluster if the number of different sets is small.

Scenario: The number of different input entry sets in a cluster	Metric	Cluster size		
		3 eNBs	20 eNBs	80 eNBs

1	cx(i)
	pe(i)
		3.3
		3.3
			0.5
			22
				0.13
				88

2	cx(i)
	pe(i)
		5.7
		1.9
			0.9
			13
				0.21
				52

3	cx(i)
	pe(i)
		8
		1.4
			1.2
			9.2
				0.30
				37

4	cx(i)
	pe(i)
		N/A	1.6
			7.1
				0.39
				28

5	cx(i)
	pe(i)
		N/A	1.9
			5.8
				0.48
				23

each eNB has unique set of input parameters	cx(i)
	pe(i)
		8
		1.4
			7.2
			1.5
				7.0
				1.6

The following assumptions applies to the calculations: The seven inputs in the left hand side in Figure 20 is one entry set. The three constants k1, k2 and k3 are calculated once per cluster and as the output both eNB and UNI parameters are considered that is 11 outputs per eNB. For small cluster (3 eNBs) the scenario 4 and 5 are not applicable (N/A) as the number of input entry sets is exceeding the number of eNBs.

This concludes the discussion of capacity related parameters and their interrelations. The next section discusses the interdependencies of the identification and IP address parameters.

4.4 Modelling Identification and IP Address Parameters

This section discussed the identifier and address parameters related to eNB transport interfaces and features. These parameters includes VLAN IDs and IP addresses. The eNB parameters which contain an IP address as a value can be divided into several groups. One possible grouping could be based on the use of the parameter as listed in Table 15.

Table 15. A list of possible use cases for an IP address value. An IP address value has many other roles than just an interface or application address.

IP address parameter use case
An identifier of own application and/or interface
An identifier of peer node and/or interface
An identifier of an endpoint for a process
A criteria in filter or policing rule
A destination or a gateway for a route

The own application and interface address parameter values are unique in each eNB. The peer node and endpoint identifiers are typically common for a group or the eNBs. The policy rules may apply both the own and the peer IP address. The discussed IP addressing scenarios are divided into three main groups. The first IP addressing scenario represents simple cases where VLAN interface IP address is assumed for eNB application IP address as well. The second scenario represents cases assuming loopback address as eNB application IP address and the third scenario discusses IP addressing with IPsec feature. Each of these scenarios variates in terms of number of VLANs, number of different application addresses and the redundancy approach to be used. The IP addressing scenarios are listed in Table 16.

Table 16. The main eNB IP addressing scenarios

#	Scenario	Applied in the studied case(s) / typical use case	Typical sub-scenarios
1	Application IP assumes the VLAN interface IP address	B, C, D and E	Single VLAN Dedicated VLAN for M-plane VLAN per application
2	Application IP assumes loopback address, no IPsec	Path protection	Single VLAN pair Dedicated VLAN pair for M-plane VLAN pair per application
3	IPsec scenario	A	Single IPsec tunnel Dedicated IPsec tunnel for M-plane

VLAN ID interdependencies are discussed next after which the IP address parameter interdependencies are looked at in more detail.

4.4.1 VLAN ID Interdependencies

One of the identification parameter in eNB transport domain is the VLAN ID. The VLAN ID ranges used in the eNB are aligned with the VLAN ID ranges used in the GW router or with the service VLAN used in the user network interface (UNI) Ethernet virtual connection (EVC). The VLAN is terminated at the GW router; however, the VLAN ID used at EVC at the UNI may be mapped to another VLAN ID at the peer [12]. The possibility to remap the VLAN IDs gives flexibility in cases where customer end VLAN ID conflicts with the ones already used at the peer for other purposes. However, unnecessary remapping shall be avoided as it is known to complicate the network configuration and thus introduces additional risks to misinterpret or miss configure the network nodes. This model assumes that the VLAN ID applied in the eNB is equal to the one applied in the GW router for the given purposes.

Rule1: The GW router may be connected to several independent link layer (L2) domains which are identified unambiguously by a unique VLAN ID.

Rule2: Several eNBs may share the same L2 domain and thus assumes the equal VLAN ID value.

Rule3: each eNB may assume several VLANs (to separate different traffic types or for the primary and secondary paths).

An example scenario of two independent VLANs each serving a few eNBs is shown in Figure 21. In this figure the eNB-1 and the eNB-2 assumes the same green VLAN while the eNB-3, the eNB-4 and the eNB-5 assumes another, the blue VLAN.

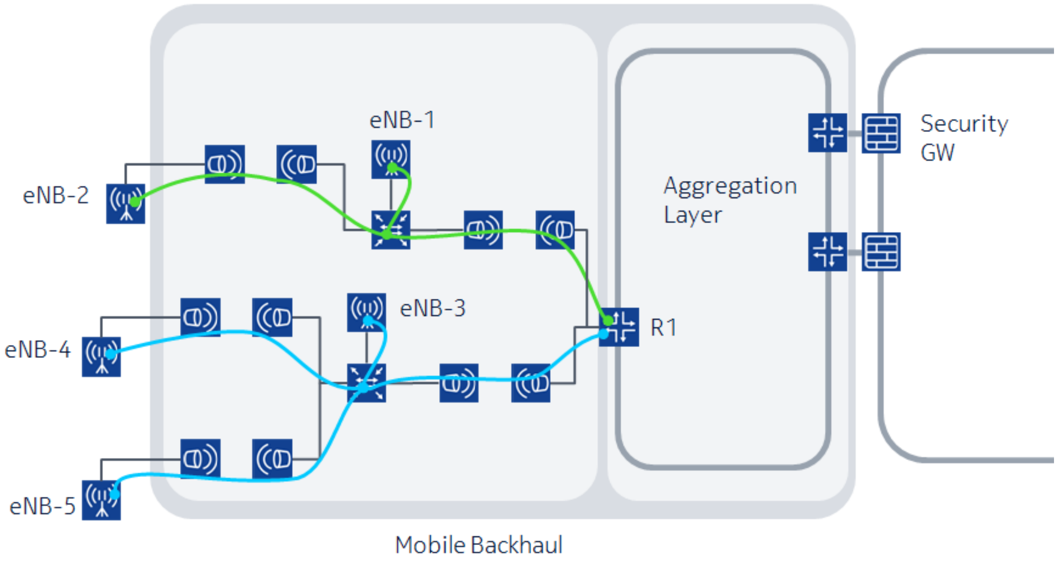


Figure 21. An example of two VLANs each shared with a few eNBs. The green line in the top illustrates VLAN which interconnects eNB-1, eNB-2 and router R1. The blue line below that illustrates a VLAN which is used to interconnect eNB-3, eNB-4, eNB-5 and router R1.

All eNB traffic is forwarded within a single VLAN in this example. In case traffic separation within an eNB is required then several VLANs are used per eNB. Within the cases studied only one case has single VLAN, one has five VLANs and the rest three have four VLANs per eNB each. Based on the subnet size assigned for the VLAN it can be assumed that most of the cases share the VLAN between several eNBs or other radio technology BTS.

The VLAN ID range can be divided into blocks per function and per geographical location of the L2 domains and thus the VLAN ID can be calculated based on the following formula.

$$\text{VLAN ID} = f(x,y). \tag{23}$$

Where x defines the traffic plane and
y defines physical location of the L2 domain.

In the example shown in Figure 22 three VLANs are assumed for traffic separation for each eNB. Each VLAN group is shared among several eNBs within the same IP GW cluster. The first two most significant digits defines the traffic plane and the last two digits the L2 domain in question. In that case the formula can be written as

$$\text{VLAN ID} = 100 * x + y \qquad (24)$$

Where x = 33 for M-plane

X = 34 for S-plane

X = 35 for C/U-plane and

y identifies 100 possible L2 domains.

The main idea is to apply simple rule which can be followed cross the network.

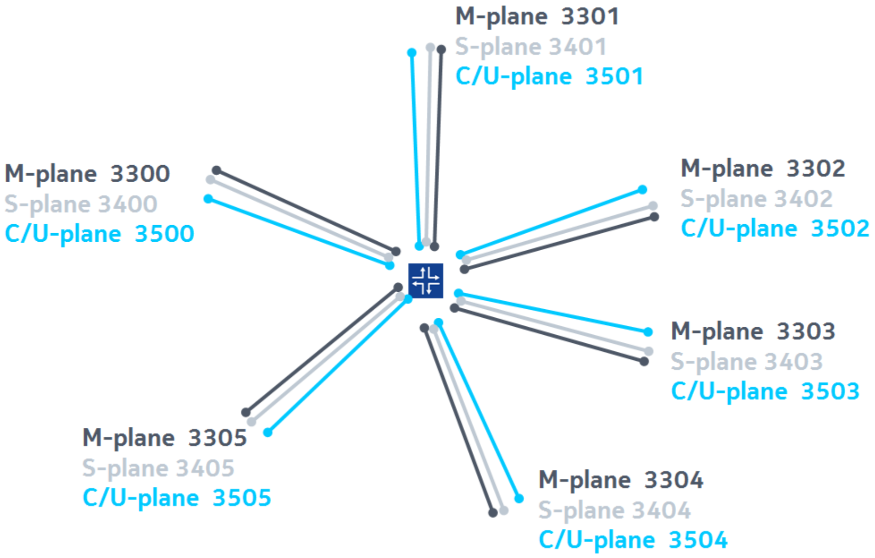


Figure 22. A principle of VLAN ID range distribution by function and by geographical area. The function is a traffic plane; management plane (33 M-plane), synchronisation plane (34 S-plane) and combined control and user plane (35 C/U-plane). Each physical L2 domain reach to particular geographical area. A VLAN ID value is a combination of a function and a geographical area number (00, 01, 02,…).

This concludes the discussion of the VLAN ID interdependencies and next topic to discuss is the IP address parameters and their interdependencies.

4.4.2 IP Addressing Scenario 1

The first IP addressing scenario assumes VLAN interface IP address as an application IP address. This scenario like all addressing scenarios variates in terms of number of VLANs, number of different application addresses and the redundancy approach to be used.

In scenario 1 with single VLAN all application IP addresses have the same value as the VLAN interface IP address and thus five different parameters assumes the same value. A configuration file snapshot is shown in Listing 20.

```
<managedObject class="IPNO" distName="MRBTS-107303/LNBTS-
107303/FTM-1/IPNO-1" operation="update" version="LN7.0">
<p name="mPlaneIpAddress">10.1.100.11</p>
<p name="uPlaneIpAddress">10.1.100.11</p>
<p name="cPlaneIpAddress">10.1.100.11</p>
<p name="sPlaneIpAddress">10.1.100.11</p>
…
<managedObject class="IVIF" distName="MRBTS-107303/LNBTS-
107303/FTM-1/IPNO-1/IEIF-1/IVIF-1" operation="create"
version="LN7.0">
<p name="vlanId">100</p>
<p name="localIpAddr">10.1.100.11</p>
<p name="netmask">255.255.255.224</p>
…
</managedObject>
```

Listing 20. An example of scenario 1. Single IP address value is assumed for VLAN interface (*localIpAddr*) and for all eNB applications (*mPlaneIpAddress, uPlaneIpAddress, cPlaneIpAddress* and *sPlaneIpAddress*).

One variation is to add a secondary GW and apply Bidirectional Forwarding Detection (BFD) process to monitor the availability of the path to the primary GW. This would add a new managed object where the same IP address is applied as a local IP address. A snapshot of BFD parameters are shown in Listing 21.

```
<managedObject class="BFD" distName="MRBTS-xxx303/LNBTS-
xxx303/FTM-1/IPNO-1/BFD-1" operation="create" version=
"LN7.0">
…
<p name="bfdSourceIpAddr">10.1.100.11</p>
…
</managedObject>
```

Listing 21. An example of Bidirectional Forwarding Detection (BFD) process also assuming the same IP address value as a source address as is used for VLAN interface IP address above.

The second possible variation is to add the Two Way Active Measurement Protocol (TWAMP) process. This will introduce one more managed object with the same IP address as a local end identifier as shown in Listing 22.

```
<managedObject class="TWAMP" distName="MRBTS-xxx303/LNBTS-
xxx303/FTM-1/IPNO-1/TWAMP-1" operation="create" version=
"LN7.0">
…
<p name="sourceIpAddress">10.1.100.11</p>
</managedObject>
```

Listing 22. An example of parameters required for the Two Way Active Measurement Protocol (TWAMP) process. The IP address used as a local end point (*sourceIpAddress*) assumes the same value as the VLAN interface shown in Listing 20.

In this scenario one of the IP address parameters is taken as a master parameter and the others just assumes a copy of the value. The question is: Which of the parameters shall be selected as a master? Based on the scenario1 with single VLAN only the two last IP address parameters (BFD and TWAMP managed objects) can be excluded from the list of candidates as there do not exists in all configurations.

Next the second sub-scenario of the scenario1 is analysed. In the second sub-scenario a dedicated VLAN is assumed for M-plane traffic. This scenario is illustrated in Listing 23.

```
<managedObject class="IPNO" distName="MRBTS-xxx303/LNBTS-
xxx303/FTM-1/IPNO-1" operation="update" version="LN7.0">
<p name="mPlaneIpAddress">10.1.200.11</p>
<p name="uPlaneIpAddress">10.1.100.11</p>
<p name="cPlaneIpAddress">10.1.100.11</p>
<p name="sPlaneIpAddress">10.1.100.11</p>
…
</managedObject>
<managedObject class="IVIF" distName="MRBTS-xxx303/LNBTS-
xxx303/FTM-1/IPNO-1/IEIF-1/IVIF-1" operation="create"
version="LN7.0">
<p name="vlanId">100</p>
<p name="localIpAddr">10.1.100.11</p>
…
```

```
</managedObject>
<managedObject class="IVIF" distName="MRBTS-xxx303/LNBTS-
xxx303/FTM-1/IPNO-1/IEIF-1/IVIF-2" operation="create"
version="LN7.0">
<p name="vlanId">200</p>
<p name="localIpAddr">10.1.200.11</p>
…
</managedObject>
```

Listing 23. IP addressing scenario assuming dedicated VLAN and thus dedicated IP address for the NB M-plane. In this example M-plane application address (`mPlaneIpAddress`) has the same value as the interface of the VLAN 200 (`localIpAddr`).

In general terms the sub-scenarios of the scenario1 can be expressed as a function of the number of the VLANs to be used. Table 17 shows the few valid combinations with typical use cases.

Table 17. A few valid IP addressing sub-scenarios of the scenario 1.

Number of VLANs (applications)	Scenario ID	Typical use case
1 (CUSM)	1.1	No traffic separation required between traffic planes. Simple configuration.
2 (CUSM,C2)	1.2	No traffic separation required between the traffic planes. The secondary C-plane VLAN is due to the SCTP multi-homing.
2 (CUS, M)	1.3	M-plane traffic needs to be separated from the other traffic to fulfil the operator’s security policies.
3 (CUS,C2,M)	1.4	M-plane traffic needs to be separated from the other traffic to fulfil the operator’s security policies. The secondary C-plane VLAN due to SCTP multi-homing.
3 (CU,S,M)	1.5	Traffic separation is driven by the backhaul capabilities in cases where the backhaul is able to classify traffic only based on the VLAN ID but not based on VLAN priority or DSCP. C-plane and U-plane are kept together to simplify X2 routing.
3 (CU,SC2,M)	1.6	Traffic separation is driven by the backhaul capabilities in cases where backhaul is able to classify traffic only based on the VLAN ID but not based on VLAN priority or DSCP. C-plane and U-plane are kept together to simplify X2 routing.

		S-plane and C2 assumes the same VLAN as the similar traffic treatment is required.
4 (C,U,S,M)	1.7	Traffic separation is driven by the backhaul capabilities in cases where backhaul is able to classify traffic only based on the VLAN ID but not based on VLAN priority or DSCP.
5 (C,C2,U,S,M)	1.8	Traffic separation is driven by the backhaul capabilities in cases where backhaul is able to classify traffic only based on the VLAN ID but not based on VLAN priority or DSCP. The secondary C-plane VLAN due to SCTP multi-homing.

The first sub-scenario, scenario 1.1, is the simples in terms of configuration complexity. It has single VLAN and single IP address used for the VLAN interface and for the applications as well. Figure 23 illustrates scenario 1.1 on the left hand side and the scenario 1.1 with BFD based traffic protection on the right hand side.

UCSM
GW
BFD
GW1
UCSM
GW2

Figure 23. eNB IP addressing scenario 1.1 on left and scenario 1.1 with Bidirectional Forwarding Detection (BFD) on right. One IP address is shared by all eNB applications and the VLAN interface. On the left hand side single IP Gateway (GW) is used while with path protection with BFD process the secondary GW is also defined.

Figure 24 visualises the eNB IP addressing parameter interrelations in the basic scenario 1.1. In the left hand side the minimum set of input parameters; eNB specific IP address, VLAN cluster specific VLAN ID and GW IP address, and parameters which are common for several VLAN clusters. These are used to generate the required eNB transport parameters shown in the right hand side. In this scenario single input entry, IP address, is used to solve all required four application IP address parameter values in IPNO-1 object and the VLAN interface IP address in IVIF-1 object. The larger cluster contains parameters which values are applicable for several VLAN clusters. Typically all the VLANs used for the same purpose, for example for M-plane, assumes the same subnet size and thus the VLAN subnet netmask is considered to be bigger cluster specific rather than VLAN specific in this model.

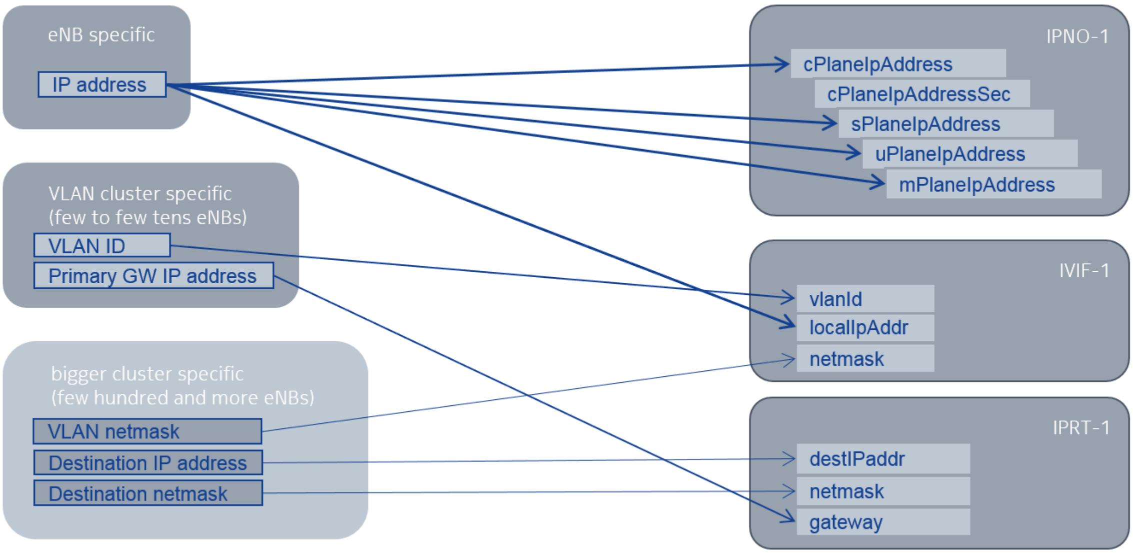


Figure 24. eNB IP addressing parameter interrelations in the scenario 1.1. One eNB specific entry is used as a value for five different parameters in the eNB XML configuration file. Each of the two VLAN cluster level entries and three bigger cluster (for example Mobility Management Entity (MME) cluster) level are used once in the XML file.

Each additional VLAN introduces one eNB level input entry (IP address) and two VLAN cluster level input entries; VLAN ID, Primary GW IP address. These additional VLANs require six parameters in the eNB configuration file; *vlanId*, *localIpAddr*, *netmask* in IVIF-object *and destIPaddr, netmask* and the *gateway* in the IPRT-object. In case the VLAN is to be used for multi-home stream control transmission protocol (SCTP) one more out-put parameter is counted (*cPlaneIpAddressSec*).

The complexity and the process efficiency metrics are defined for scenarios shown in Table 17. The calculated metrics are listed in Table 18.

Table 18. Metrics for eNB IP addressing scenario 1

Scenario	Metric	Cluster size		
		3 eNBs	20 eNBs	80 eNBs

1.1	cx(i)
	pe(i)
		1.7
		4.2
			1.1
			6.4
				1.0
				6.8

1.2	cx(i)
	pe(i)
		3.3
		4.2
			2.2
			6.4
				2.1
				6.8

1.3	cx(i)
	pe(i)
		3.3
		3.9
			2.2
			5.9
				2.1
				6.3

1.4	cx(i)
	pe(i)
		5.0
		3.8
			3.3
			5.8
				3.1
				6.2

1.5	cx(i)
	pe(i)
		5.0
		3.6
			3.3
			5.5
				3.1
				5.9

1.6	cx(i)
	pe(i)
		5.0
		3.8
			3.3
			5.8
				3.1
				6.2

1.7	cx(i)
	pe(i)
		6.7
		3.5
			4.4
			5.2
				4.1
				5.6

1.8	cx(i)
	pe(i)
		8.3
		3.5
			5.5
			5.3
				5.1
				5.7

It can be seen that increasing the cluster size from 3 eNBs to 20 eNBs both metrics shows notable improvement; complexity (cx) decreases and process efficiency (pe) increases. Further cluster size increase from 20 eNBs to 80 eNBs shows still some improvement, however, the small one.

The eNBs may require additional features such as redundant GW and backhaul quality monitoring based on two way active measurement protocol (TWAMP). In case those additional features are not applied to all site in the cluster they can be added as a conditional item in the parameter model. Figure 25 illustrated scenario 1.1 with additional inputs to create the conditional items. The dotted lines represents the conditional items. By giving a value for *the secondary GW IP address* input entry the required additional object, in this case the BFD-1 object, is created and the object parameter values are filled in based on the inputs given. In the similar manner the conditional TWAMP objects and related parameters are defined on need basis.

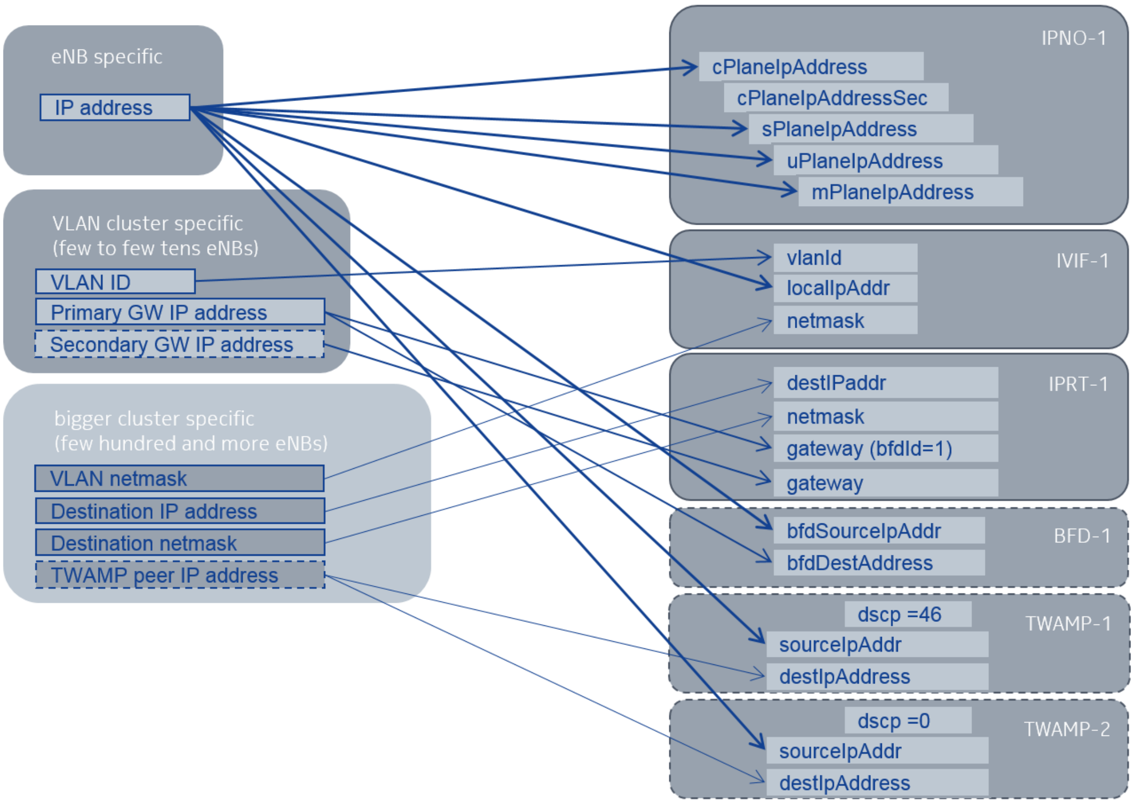


Figure 25. eNB IP addressing parameter interrelations in the scenario 1.1 with Bidirectional Forwarding Detection (BFD) and Two Way Active Measurement Protocol (TWAMP). Compared to the basic scenario 1.1 the BFD and TWAMP introduces additional elements in the eNB XML file. Many newly introduced parameter assumes a value of already defined input entry.

The metrics are also compared taken the Bidirectional Forwarding Detection (BFD) and the Two Way Active Measurement Protocol (TWAMP) features in to an account. Table 19 shows the calculated metrics values for the same scenarios assuming both BFD with additional route and TWAMP processes. Comparing Table 18 and Table 19, it can be seen that the additional features, BFD and TWAMP, increases the complexity as additional input parameters are required. However, the process efficiency increases much more. This is because the input parameters are used to define a much larger number of the output parameters in the latter case.

Table 19. Metrics for eNB IP addressing scenario 1 with Bidirectional Forwarding Detection (BFD) and Two Way Active Measurement Protocol (TWAMP).

Scenario	Metric	Cluster size		
		3 eNBs	20 eNBs	80 eNBs

1.1	cx(i)
	pe(i)
		2.0
		8.5
			1.2
			14.8
				1.0
				16.4

1.2	cx(i)
	pe(i)
		4.0
		6.2
			2.3
			10.9
				2.1
				12.0

1.3	cx(i)
	pe(i)
		4.0
		6.0
			2.3
			10.4
				2.1
				11.6

1.4	cx(i)
	pe(i)
		6.0
		5.3
			3.5
			9.3
				3.1
				10.3

1.5	cx(i)
	pe(i)
		6.0
		5.2
			3.5
			9.0
				3.1
				10.0

1.6	cx(i)
	pe(i)
		6.0
		5.3
			3.5
			9.3
				3.1
				10.3

1.7	cx(i)
	pe(i)
		8.0
		4.7
			4.6
			8.3
				4.2
				9.2

1.8	cx(i)
	pe(i)
		10.0
		4.6
			5.8
			8.0
				5.2
				8.9

Typically the same scenario is applied for all eNBs within the planning cluster and thus it is practical to fine tune the parameter model to the given scenario rather than trying to solve all scenarios with a single model applying complex logic. The rest of the sub scenarios are not discussed in detail. The second scenario listed in Table 16 is discussed next.

4.4.3 IP Addressing Scenario 2

In the second IP addressing scenario all or most of the applications assume a loopback address as an application IP address. This adds flexibility and enables additional means to provide transport redundancy. More than one VLAN can be defined to be used for an application and based on the availability of the path on given VLAN it is either used for traffic forwarding or ignored as a valid option. Quite like the scenario1 also the scenario2 variates in terms of number or VLANs for traffic separation, the redundancy path and backhaul quality monitoring requirements. Table 20 lists the typical sub-scenarios for scenario 2.

Table 20. A few sub-scenarios of the scenario 2.

Number of VLANs	Scenario ID	Typical use case
1 (CUSM)	2.1	No traffic separation required between traffic planes. Simple configuration. Applications may assume the same IP address or they may have dedicated IP address. It can also be a combination of these.
2 (primary/ secondary)	2.2	The second VLAN is defined to provide an alternative traffic path in case the primary path is not operational.
2 (CUSM,C2)	2.3	No traffic separation required between the traffic planes. Secondary C-plane VLAN is used in case the SCTP multi-homing is to be configured. C2 must not be equal to C.
2 (CUS, M)	2.4	M-plane traffic needs to be separated from the other traffic to fulfil the operator’s security policies.
3 (CUS,C2,M)	2.5	M-plane traffic needs to be separated from the other traffic to fulfil the operator’s security policies. A secondary C-plane VLAN due to SCTP multi-homing.
3 (CU,S,M)	2.6	Traffic separation is driven by the backhaul capabilities in cases where the backhaul is able to classify traffic only based on the VLAN ID but not based on VLAN priority or DSCP. C-plane and U-plane are kept together to simplify X2 routing.
3 (CU,SC2,M)	2.7	Traffic separation is driven by the backhaul capabilities in cases where backhaul is able to classify traffic only based on the VLAN ID but not based on VLAN priority or DSCP. C-plane and U-plane are kept together to simplify X2 routing. S-plane and C2 assumes the same VLAN as the similar traffic treatment is required.
4 (C,U,S,M)	2.8	Traffic separation is driven by the backhaul capabilities in cases where backhaul is able to classify traffic only based on the VLAN ID but not based on VLAN priority or DSCP.
5 (C,C2,U,S,M)	2.9	Traffic separation is driven by the backhaul capabilities in cases where backhaul is able to classify traffic only based on the VLAN ID but not based on VLAN priority or DSCP. A secondary C-plane VLAN due to SCTP multi-homing.
n2m (Primary/ Secondary)	2.10	A generic case for *n* different application IP addresses and *m* VLANs to be used for primary and secondary paths.

Next the n2m sub-scenario is discussed in detail. Figure 26 illustrates the principle of the n2m scenario. One example use case for this scenario is the mobile-edge computing (MEC) connectivity case. In that case VLAN having interface IP address T1 is used as a primary path for U- and C-plane traffic towards the MEC node, VLAN T2 is used for S-plane traffic and also as a secondary path for U- and C-plane traffic in case the path via the MEC or the MEC itself becomes unavailable. The last VLAN (T3) is used for M-plane traffic.

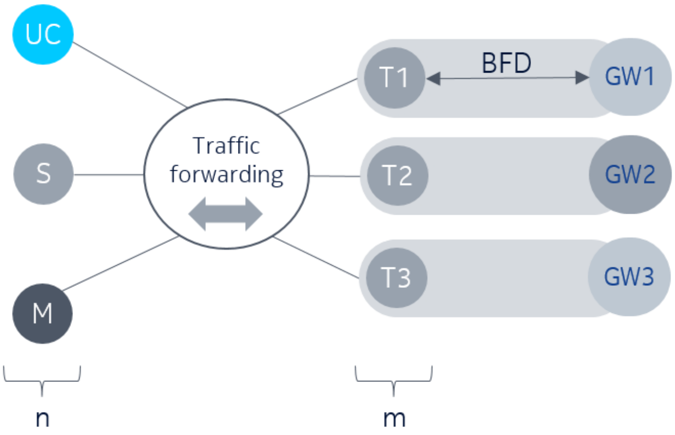


Figure 26. An IP addressing n2m scenario (n=3, m=3). In this generic scenario the *n* represents the number of the unique IP addresses assigned for the application as a loopback address and *m* is the number of IP addresses assigned for the VLAN interfaces.

The eNB IP parameter interdependencies are illustrated in Figure 27. In this scenario only a few interdependencies can be identified. First the U-plane and C-plane application IP address parameter values in IPNO object are equal. The second object which can reuse other parameters is the BFD object. In this example the BFD object assumes VLAN IP address (T1) as the *bfdSourceAdd*r and the GW1 as the *bfdDestAddress* parameters. Other potential choices for the *bfdSourceAddress* parameter value is the one used as the U-plane application address (*uPlaneIpAddress*). Also in the BFD process may monitor connection further in the network on multi-hop basis other value for *bfdDestAddress* is to be applied. Such address may not be used for any other purposes in the eNB and needs to be introduced as an additional input in the model.

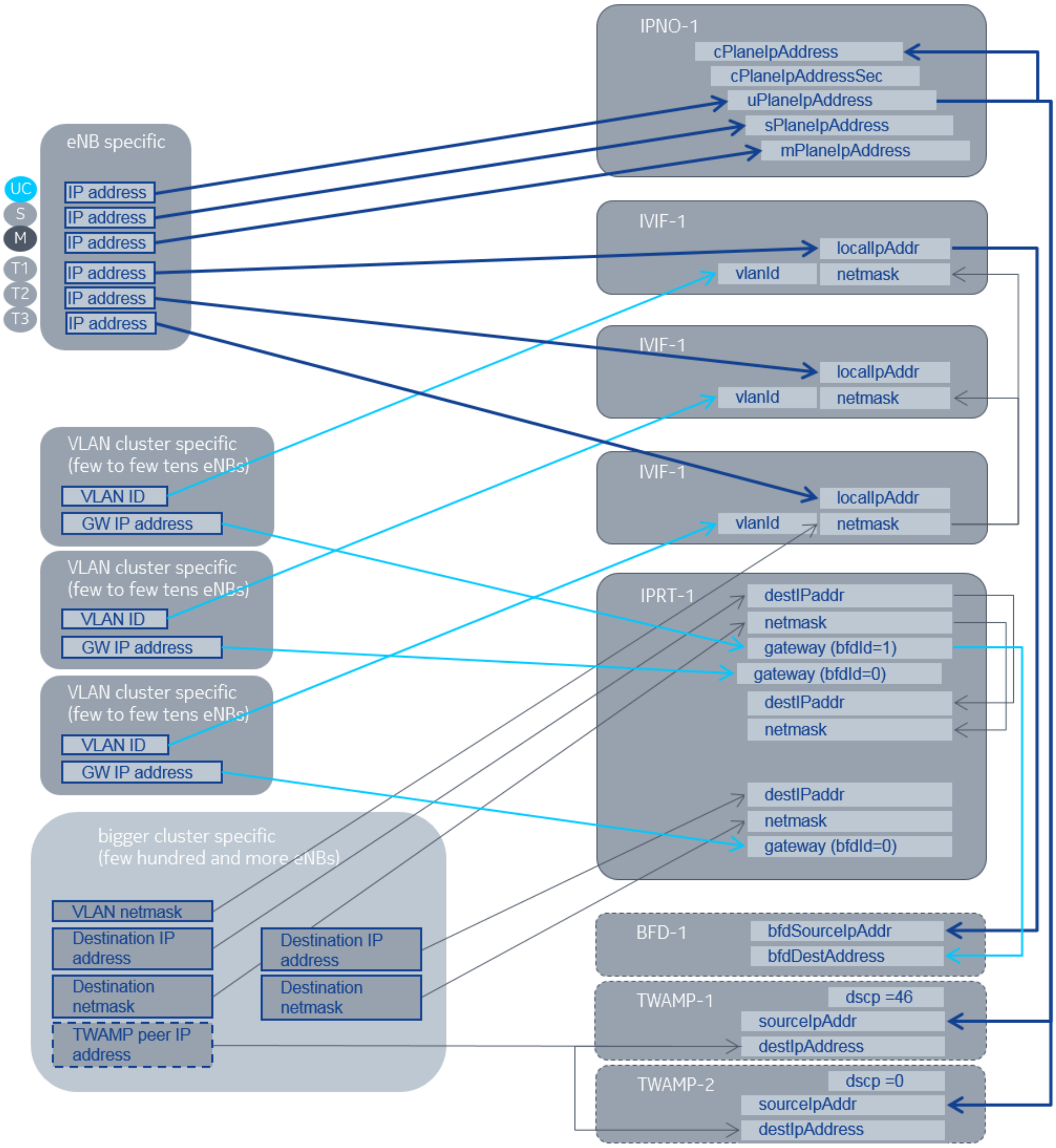


Figure 27. eNB IP addressing parameter interrelations in the n2m example scenario. The combined C/U-plane IP address entry value is copied into five different eNB XML file parameters. The first GW is used twice, the VLAN mask is used three times, destination IP address and mask twice each and the Two Way Active Measurement Protocol (TWAMP) peer IP address is used twice in this example.

The scenario metric are calculated for scenarios shown in Table 20. These calculated metrics are shown in Table 21. Scenarios up to 2.9 are predefined and scenario 2.10 is generic and variates in terms of number of different application IP addresses (n) and the number of VLANs (m). Scenario 2.10 assumes protected path for each application.

Table 21. Metrics for eNB IP addressing scenario 2 with Bidirectional Forwarding Detection (BFD) and Two Way Active Measurement Protocol (TWAMP).

Scenario	Metric	Cluster size		
		3 eNBs	20 eNBs	80 eNBs

2.1	cx(i)
	pe(i)
		4.7
		3.4
			4.1
			3.9
				4.0
				4.0

2.2	cx(i)
	pe(i)
		7.3
		3.1
			6.2
			3.7
				6.1
				3.8

2.3	cx(i)
	pe(i)
		6.3
		3.5
			5.2
			4.2
				5.1
				4.4

2.4	cx(i)
	pe(i)
		7.3
		3.1
			6.2
			3.7
				6.1
				3.8

2.5	cx(i)
	pe(i)
		8.0
		3.5
			6.3
			4.4
				6.1
				4.6

2.6	cx(i)
	pe(i)
		9.0
		3.2
			7.3
			4.0
				7.1
				4.1

2.7	cx(i)
	pe(i)
		8.0
		3.5
			6.3
			4.4
				6.1
				4.6

2.8	cx(i)
	pe(i)
		10.7
		3.3
			8.4
			4.2
				8.1
				4.3

2.9	cx(i)
	pe(i)
		11.3
		3.5
			8.5
			4.7
				8.1
				4.9

2.10
n2m=122
	cx(i)
	pe(i)
		4.3
		5.1
			3.2
			6.9
				3.1
				7.2

2.10
n2m=224
	cx(i)
	pe(i)
		8.7
		3.9
			6.4
			5.3
				6.1
				5.6

2.10
n2m=326
	cx(i)
	pe(i)
		13.0
		3.5
			9.6
			4.8
				9.2
				5.0

2.10
n2m=428
	cx(i)
	pe(i)
		17.3
		3.3
			12.8
			4.5
				12.2
				4.8

This concludes the discussion about the IP addressing scenario 2. In the following section the IP addressing scenario with IP security is discussed.

4.4.4 IP Addressing Scenario 3

The last eNB IP addressing scenario to discuss is scenario 3. This scenario covers IP addressing cases when IPsec is to be used. Two independent IP address domains needs to be considered when IP address interrelations are studied. The outer domain is applicable between the eNB and the security GW. The forwarding of the IP packets in outer domain is based on the IPsec tunnel IP endpoint addresses and these IP addresses are relevant only in the transport network between the eNB and the security GW. At the eNB the outer domain IP address that is the IPsec tunnel end point IP address is the VLAN interface IP address. The inner domain IP addresses, transport IP in Figure 28, have relevancy only in between the security GW and the core elements like MME and SAE-GW and inside the eNB. The inner domain IP addresses in the eNB includes the application IP addresses (U-plane, C-plane, M-plane and S-plane).

It was identified that some of the processes, for example the Bidirectional Forwarding Detection (BFD), operates between the eNB and the GW router within the unsecure IP domain operating with the outer IP addresses while the Two Way Active Measurement Protocol (TWAMP) endpoint is typically in the core site thus in a secure area and the relevant IP address to look at is the inner domain IP address.

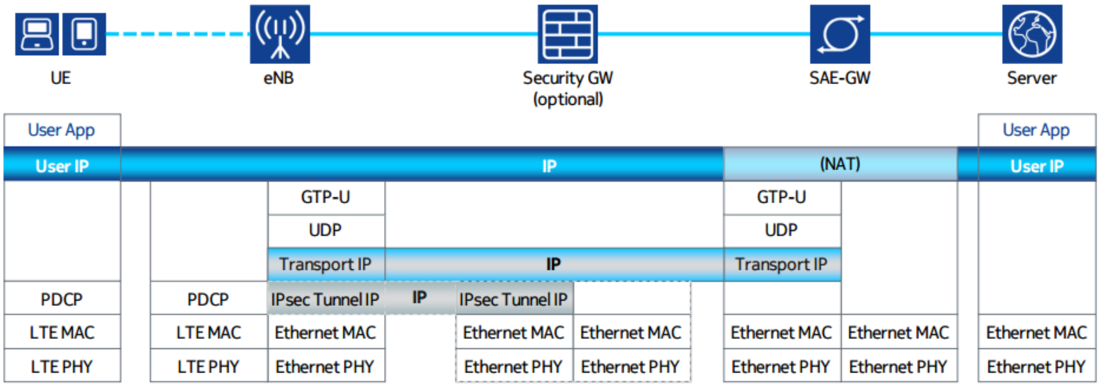


Figure 28. U-plane protocol stack with IPsec tunnel [8]. The near-by processes for example the Bidirectional Forwarding Detection (BFD) operates in the same domain the IPsec Tunnel IP addresses while the far-reaching processes for example the Two Way Active Measurement Protocol (TWAMP) operates in the inner domain and thus assumes Transport IP address as a local end IP point address. Adapted from [8].

The example snapshot of an eNB XML file below in Listing 24 shows three different managed objects which all contain the same IP address value equal to 10.200.0.7 and two managed objects which contain IP address value equal to 10.200.0.1. The first managed object (IVIF-2) defines a VLAN interface and assigns IP address (10.200.0.7) to this VLAN interface. The second managed object (BFD-2) defines a BFD process to supervise the path availability from the VLAN interface (10.200.0.7) to the primary GW (10.200.0.1) and finally the third object (IPNO-1) defines the IP addresses for applications. In this example the S-plane IP address assumes the VLAN (IVIF-2) IP address (10.200.0.7). The primary GW IP address defined in the routing object (IPRT-1) contains the value (10.200.0.1) which can be found also in the bidirectional forwarding detection (BFD-1) managed object.

```
<managedObject class="IVIF" distName="MRBTS-15/LNBTS-
15/FTM-1/IPNO-1/IEIF-1/IVIF-2" operation="create" version=
"TL15A">
<p name="vlanId">200</p>
<p name="localIpAddr">10.200.0.7</p>
...
<managedObject class="BFD" distName="MRBTS-15/LNBTS-15/FTM-
1/IPNO-1/BFD-2" operation="create" version="TL15A">
…
<p name="bfdDestAddress">10.200.0.1</p>
…
<p name="bfdSourceIpAddr">10.200.0.7</p>
..
<managedObject class="IPNO" distName="MRBTS-15/LNBTS-
15/FTM-1/IPNO-1" operation="update" version="TL15A">
...
<p name="sPlaneIpAddress">10.200.0.7</p>
...
<managedObject class="IPRT" distName="MRBTS-15/LNBTS-
15/FTM-1/IPNO-1/IPRT-1" operation="create" version="TL15A">
<list name="staticRoutes">
...
<item>
<p name="bfdId">2</p>
<p name="destIpAddr">0.0.0.0</p>
<p name="gateway">10.200.0.1</p>
…
<item>
<p name="bfdId">0</p>
<p name="destIpAddr">0.0.0.0</p>
<p name="gateway">10.200.0.2</p>
…
</item>
```

Listing 24. An example of IP addressing scenario where the same IP address value (10.200.0.7) is used for three different managed objects (*IVIF*, *BFD*, and *IPNO*). And the other value (10.200.0.1) is applied in two different managed objects (*BFD* and *IPRT*).

These eNB IP address parameter interrelations are visualized in Figure 29. The IPsec introduces new object (IPSECC) in the eNB configuration file. The traffic treatment in IPsec process is controlled by means of security policy rules. These policy rules contain criteria some of which are eNB specific and others are common for the whole security GW cluster. The eNB specific criteria contains the already introduced eNB IP addresses and thus no new eNB specific input entries are necessary for IPsec.

Some traffic types may assume several security policies. In this example case U-plane and M-plane assumes two different security policies. For U-plane the aim is to define each destination (SGW) separately and for M-plane the motivation for multiple policies is to encrypt certain M-plane traffic on transport and bypass the other type of M-plane traffic as it has already been encrypted on application layer.

The quantity of required security policies needs to be defined case by case as the policies applied in eNB shall be in line with the operator’s overall security policies. Some of the policies may be aggregated to single policy to simplify the configuration. This can be done by relaxing the accuracy applied in the security policies in other words instead of applying two policies, one for each destination SGW, one common policy with wider IP address block to cover IP address of both SGW may be consider.

For clarity only the parameters which are relevant to understanding the IPsec scenario are shown and thus bidirectional forwarding detection (BFD) and two way active measurement protocol (TWAMP) related objects are not shown in Figure 29.

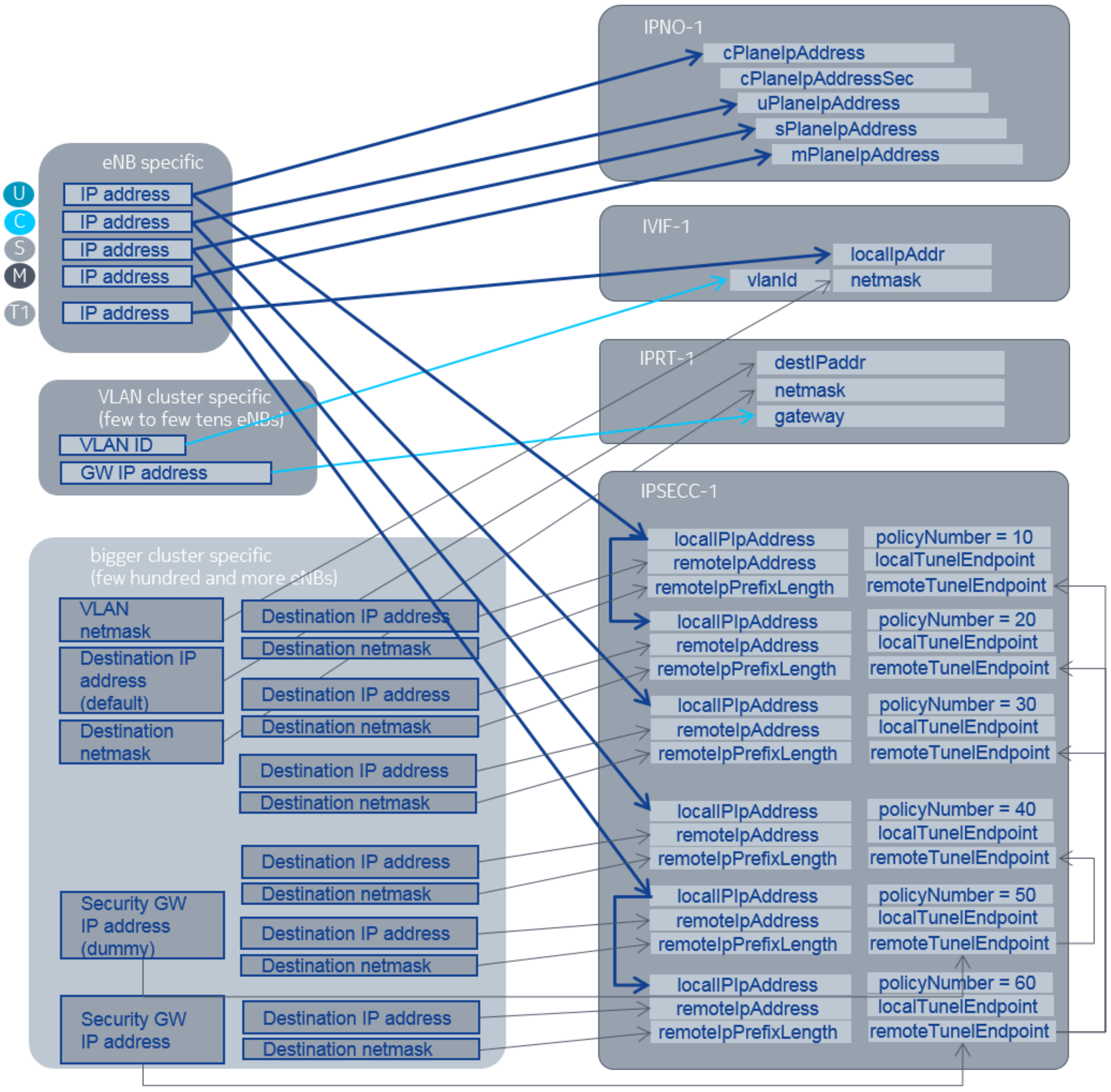


Figure 29. eNB IP addressing with IPsec, scenario 3.1. IPsec introduces policies which are used to control the traffic treatment in the eNB security gateway. This example shows policies 10 to 60. Most of the policies uses IP addresses as policing criteria and thus a few additional IP address entries are introduced.

In this study one IPsec case is studied. For reference the metrics is calculated to one IPsec case, referred as 3.1. This scenario 3.1 assumes single VLAN and four different eNB application IP addresses and thus it is like scenario 2.10 (n2m=421) with IPsec. The IPsec adds many parameters on top of those required in scenario 2.10. These need to be defined for the eNB configuration file. However, most of them can be derived from the other parameters already defined for scenario 2.10. The calculated metrics are shown in

Table 22. This calculation assumes six security polices each requiring two security GW cluster level input entries.

Table 22. Metrics for eNB IP addressing scenario 3.

Scenario	Metric	Cluster size		
		3 eNBs	20 eNBs	80 eNBs

3.1	cx(i)
	pe(i)
		5.7
		8.1
			5.1
			9.0
				5.1
				9.1

3.1 with
TWAMP
	cx(i)
	pe(i)
		5.7
		8.8
			5.1
			9.7
				5.1
				9.9

It should be noted that the calculated metrics for scenario 3 shall not be compared directly to metrics calculate for scenario 2 as the scenarios have different assumptions. Unlike the scenario 2 the scenario 3 assumes no bidirectional forwarding detection (BFD) object and related parameters.

5 Analysis and Conclusions

The aim of this study was to develop an eNB transport parameter model to simplify the eNB transport parameter planning in network roll-out phase. The parameter model defines parameter interrelation rules and it suggests a small set of input entries which are to be used to solve a large number of transport parameters in eNB managed objects. This study identifies that most of the eNB transport parameters assume the same values within a planning cluster or even within the whole network.

In this study the eNB transport parameters are divided into four main categories based on how specific the parameter value is in the eNB within a planning cluster. The parameter categories are; global and network level, cluster level, capacity step or type specific and eNB specific. The input entries in the parameters model follows the same categories. The generic model is illustrated in Figure 30. The global and network level parameters are not visible in this model as those are prepared in the base configuration already before the eNB specific planning starts.

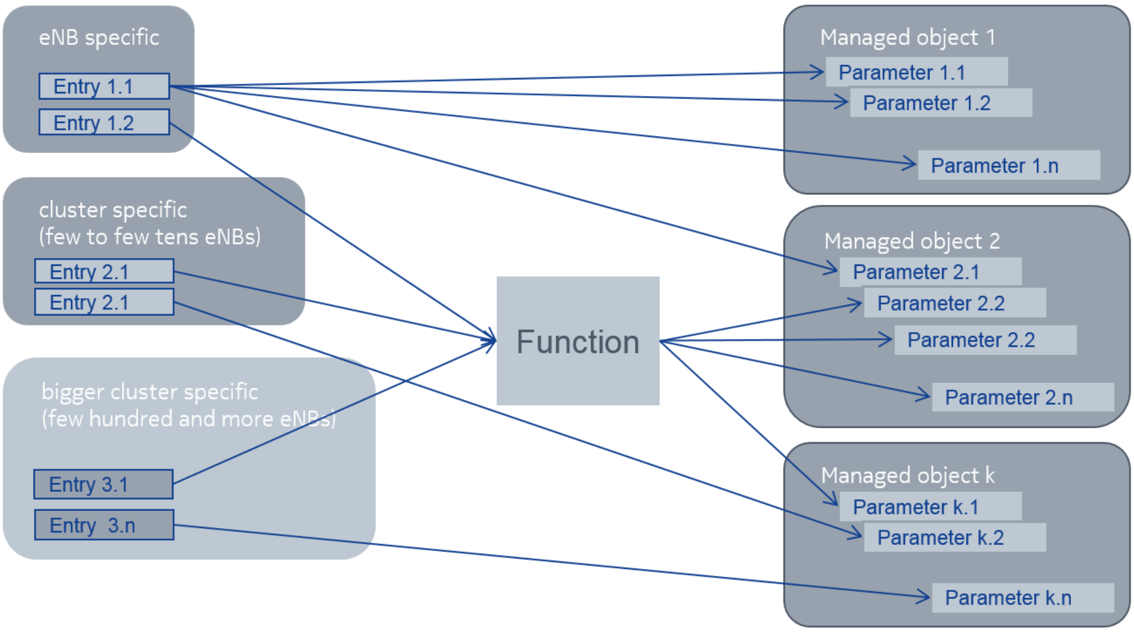


Figure 30. A generic eNB transport parameter model with interrelation rules. The eNB specific, cluster specific and bigger cluster specific input entries are used to determine the parameters in the eNB managed objects. A managed object parameter assumes a value of an input entry or a result of a function.

This study identifies two different areas where the parameter interrelation rules benefit most the planning process. Fist the interrelation rules between the different traffic engineering parameters are introduced. The traffic engineering parameters include shaping, transport admission control and scheduling parameters. The characteristic of these parameters is that these parameters do not need to be defined for each eNB separately but rather for each eNB target capacity step for example if the given planning cluster contains only two different capacity steps then only two different sets of traffic engineering parameters needs to be defined.

The second parameter area which benefits from the parameter interrelation rules in planning process is the VLAN and IP addressing parameters. To manage the VLAN and IP addressing parameters this study suggests to divide all possible configurations into more manageable scenarios and sub-scenarios. This narrows down the parameter management process in a roll-out project as a project typically assumes a limited number of scenarios in a given time frame. The main IP addressing scenarios suggested by this study are listed in Table 23.

Table 23. The main IP addressing scenarios suggested by this study.

#	Scenario	Typical sub-scenarios
1	Application IP assumes the VLAN interface IP address	Single VLAN Dedicated VLAN for M-plane VLAN per application
2	Application IP assumes loopback address, no IPsec	Single VLAN pair (primary, secondary) Dedicated VLAN pair for M-plane VLAN pair per application
3	IPsec scenario	Single IPsec tunnel Dedicated IPsec tunnel for M-plane

Further this study suggest to define the eNB transport parameter interrelation rules in sub-scenario level. This reduces the number of required input entries as a sub-scenario is optimised for the specific network configuration and thus unnecessary selections can be avoided. The actual benefit of the suggested scenarios and rules depends on the feature set used in the given network.

This study analyses the basic scenarios also with Bidirectional Forwarding Detection (BFD), Fast IP Rerouting and Two Way Active Measurement Protocol (TWAMP) processes. These processes are seen more and more often in the advanced networks as the first two are meant to improve the network resilience and the last one gives the operator visibility to the mobile backhaul network load and quality. All of these processes benefit from the interrelation rules as the related managed objects require parameters which are already defined in the basic scenario.

The benefits of the suggested scenarios are evaluated using the process efficiency metric defined in equation (4). The average process efficiency in introduced IP addressing scenarios is in range of 4.7 to 11.1 assuming cluster size 80 eNBs. In practical terms this means that every introduced input entry defines a value for five to eleven eNB specific parameters in average.

The planning cluster size has an impact on the benefit of the parameter interrelation rules. In every introduced scenario the calculated metrics shows the highest benefit at the largest planning cluster. Complexity metrics (cx(i)) shows 11% to 48% improvement and the process efficiency metrics (pe(i)) improves 13% to 93% when the cluster size is increased from 3 eNBs 80 eNBs in calculated scenarios (Table 14, Table 18, Table 19, Table 21 and Table 22). This study considers relatively small cluster sizes (3, 20 and 80 eNBs). From the parameter interrelation rules point of view the higher the cluster size is the more efficient the process becomes. It is left for further studies to determine the most optimal cluster size. The large VLAN cluster implies a large layer two domain and thus large broadcast domain which is known to have negative impact on network stability and performance.

As it can be seen from the metrics the actual benefit depends strongly on the scenario in question. In addition to direct time savings due to less required effort spend in the input entries the introduced parameter interrelation rules when applied minimise human errors and thus the non-quality cost as well. In roll-out projects the non-quality cost may even exceed the actual effective work effort spent on parameter planning due to process delays and potentially additional site visits required to rectify the errors. The accurate non-quality cost analysis is left for future studies.

6 Discussion

The developed parameter model and the introduced eNB transport parameter interrelation rules simplify the planning tasks, reduce the work effort and minimise the risk of human errors. The suggested scenarios simplify the planning tasks as the most optimal network scenario can easily be identified and selected among the introduced scenarios and sub-scenarios.

The discussion and descriptions of the interrelation rules help operators to adjust the given scenario for the current case. The discussion and descriptions of the introduced eNB transport parameter interrelation rules enable the flexibility and adaptability to fulfil the local requirements that the operator may have. The work effort is reduced as the number of decisions to be made is reduced due to the parameter interrelation rules. The number of human errors is reduced also as the number of manually entered entries are reduced notable. Assuming that each manual entry has a relation to every other manual entry and the probability for human error is constant for each manual entry pair, the reduction of the number of input entries reduces the number of such entry pair approximately exponentially. This explains the exponential impact on non-quality cost as shown in Figure 31.

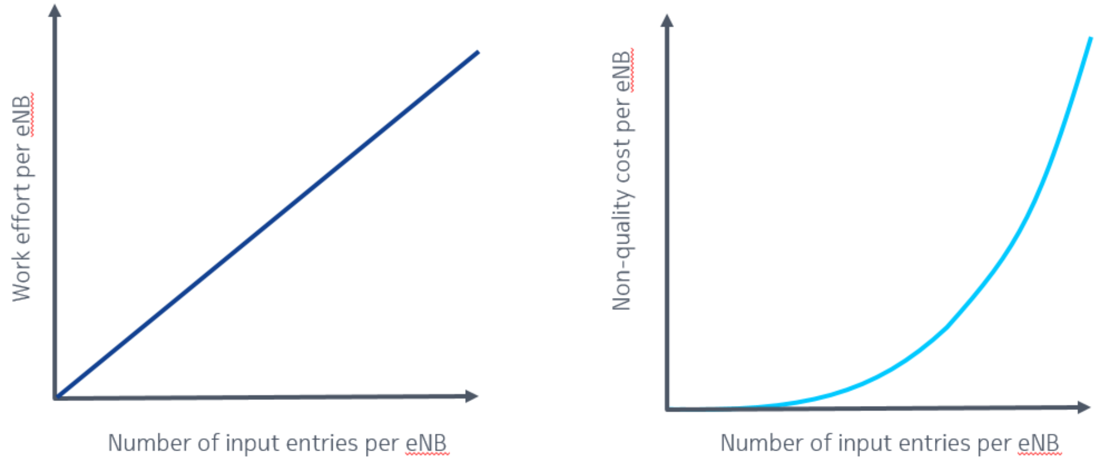


Figure 31 Impact of the number of entries on the work effort and the non-quality cost. Reducing the number of input entries decrease the direct work effort approximately linearly while the non-quality cost reduction is estimated to follow exponential curve.

The eNB transport parameter model and the introduced interrelation rules help operators to introduce more advanced transport features in a cost effective manner as the model and the theory behind guide the operator in parameter definition process. Examples of Bidirectional Forwarding Detection (BFD) based path monitoring and Fast IP rerouting protection as well as examples of Two Way Active Measurement Protocol (TWAMP) guide the operator when deploying a highly resilient and high quality aware network.

By applying the introduced eNB transport parameter interrelation rules the operator can eliminate the logical errors for example in traffic engineering parameters and minimise human errors in general as the number of considered entries is reduced. Logical errors are avoided as the interrelation logic is predefined and well explained and thus the operator does not need spend time to create such logic for the case.

The findings in this study are mainly based on the five studied cases. In addition to that a few other eNB configurations were also considered. The five studied cases represent only a small share of all ongoing projects. Out of these five studied cases four are following the same basic IP addressing scenario while one is having clearly different IP addressing scenario. All the four similar cases are from the same Latin America region. The bigger number of analysed cases would have given wider view to current practises. Also it would have been better if the cases would have been evenly distributed over the globe. Now the Latin America region is over weighted and project practises in other regions such as China, Europe, North America and Far East are not analysed thoroughly.

It became evident that the networks are constantly evolving and the additional transport features are foreseen in the future in many studied cases. Similar messages are also seen from other projects. Typical additions to current configurations are the transport quality monitoring based on the Two Way Active Measurement Protocol (TWAMP) process and the features to connect eNBs to several operators’ core networks. Also the Mobile-Edge Computing (MEC) is mentioned in many occasion when future evolution is discussed.

Taking this into an account the introduced scenarios are believed to cover most of the typical design cases. The scenarios are created based on the RL70 release feature set and are valid for that release. Most of the parameters discussed in this study are available on earlier releases as well and thus these scenarios can be considered also in networks running on earlier releases. However, some fine-tuning may be required before the model for the given scenario is taken into use.

On the other hand since RL70 release, new releases are made available for operators. These new releases contain also new eNB transport features and possible modified parameters for the current functionalities. This may mean that if the model introduced in this paper is taken in use it may not be the most efficient for the newest releases. Further work is required to update the introduced scenarios to support the latest eNB transport features and related parameters.

Based on the earlier similar parameter process optimisation cases and comments in the questionnaire replies it is seen that there is a room to define parameter interrelation rules for various identifiers (IDs) like *MRBTS_ID* and *LNBTS_ID*. The *MRBTS ID* identifies a Multiradio Base station site object and the *LNBTS ID* identifies the LTE base station radio network parameter object in an eNB configuration file. Both of these IDs are unique within the entire network and in Flexi Multiradio 10 BTS the *MRBTS_ID* and the *LNBTS_ID* may assume the same value. In this study, however, the detailed discussion about the IDs is limited to the VLAN ID as the *MRBTS_ID* and the *LNBTS_ID* are considered to belong to eNB radio parameters rather than eNB transport parameters and thus are outside of the defined scope of this study.

The traffic engineering parameters are looked at only from the transport parameter perspective. It shall not be forgotten that also the eNB radio parameters contains various parameters which can be seen as traffic engineering parameters. The parameter interrelation rules may further be enhanced by considering both the eNB radio and the eNB transport parameters at the same time in the same rule set. The traffic engineering parameters have a highly important role in network design. Suboptimal traffic engineering parameters are seen to have a negative impact on the achievable user throughput and in worse case may block the traffic totally in a given interface.

As a future study it is suggested to look at the eNB radio configuration parameters to determine the cell and the eNB peak data rates. These peak data rates could be determined based on the already available information such as available radio bandwidth, applied MIMO configuration, Transmission Mode (TM) and number of cells just to mention a few. This enhancement would potentially further reduce the number of required manual entries in capacity related eNB parameter scenario discussed in this study.

The suggested scenarios and the introduced parameter interrelation rules could be implemented in a planning tool. The eNB transport parameter interrelation rules can also be applied in Excel work sheets. In this manner the scenarios and the rules can be taken in use without massive tool development effort. The planning tool and planning sheet development aspects are not discussed in this study as these lie outside of the scope of this study.

7 Summary

The aim of this study was to introduce an eNB transport parameter model to improve planning process efficiency and thus reduce planning cost in roll-out projects. This study introduces an eNB transport parameter model and defines the parameter inter-relations. This model is estimated not only to reduce the work effort 80% to 90% but also reduce the risk for human errors. This study has reached the set objectives.

The eNB transport parameter model is presented in a form of network scenarios and the eNB transport parameter interrelation rules in these network scenarios. The complexity and process efficiency metrics are defined to make it possible to evaluate the impact of the given model on the work effort. These metrics show process efficiency between five and eleven indicating that for each manually given entry five to eleven eNB specific configuration parameters are resolved.

This study identifies two main types of parameters which benefit the most of the defined eNB transport parameter interrelation rules. The first to discuss is the eNB capacity related parameters including the traffic engineering parameters such as shaping rate and admission control limits. This study defines a logic between the various traffic engineering parameters and it leaves the numeric details for example the actual shaping rate, for the case specific projects to solve.

The second parameter area which is identified to benefit from the eNB transport parameter interrelation rules are the eNB VLAN IDs and IP addressing parameters. In addition to the role of interface or application address an IP address is seen in a role of an identifier of a process peer. In such a case the IP address, local end identifier, must be selected from the list of already defined interface or application IP addresses. This implies that the same IP address value must be configured in many eNB managed object parameters. These interrelations are defined in this study.

This study identifies three main IP addressing scenarios and additionally sub-scenarios for the most typical variations. As a working approach this study suggests to select one or a few introduced scenarios and adapt the interrelations for the given case. This study does not give any recommendation for certain scenarios but tries to discuss the relevant aspects to make it easier for an operator to select the best fit scenario for their network.

The study suggest further studies to enhance the introduced eNB transport parameter interrelation rules. Especially some of the input entries in the capacity parameter model can potentially be replaced by a rule applying to radio configuration parameters.

8 References

1 Weldon M. K., The future X network a Bell Labs perspective. CRC press. 2015.

2 Metsälä E. ed, Salmelin J. ed LTE backhaul planning and optimization. John Wiley & Sons. 2016

3 Hämäläinen S., Sanneck H., Sartori C. (eds) LTE Self-Organising Networks (SON): Network Management Automation for Operational Efficiency. John Wiley & Sons. 2012

4 Sesia S., Toufik I., Baker M. LTE: The UMTS Long Term Evolution: From Theory to Practice, Second Edition. John Wiley & Sons. 2009

5 Elnashar A., El-saidny M., Sherif M. Deployment Strategy of LTE Network Design, Deployment and Performance of 4G-LTE Networks: A Practical Approach. John Wiley & Sons. 2014.

6 3Gpp TS 36.300. V8.12.0. Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2. 2010.

7 Metsälä E., Salmelin J. Mobile Backhaul. John Wiley & Sons. 2012.

8 Holma H., Toskala A. LTE for UMTS: Evolution to LTE-Advanced, Second Edition. John Wiley & Sons. 2011

9 ngmn. LTE Backhauling Deployment Scenarios. White paper. Ngmn. 2011. https://www.ngmn.org/uploads/media/NGMN_Whitepaper_LTE_Backhauling_Deployment_Scenarios_01.pdf Accessed 17 Dec 2015.

10 Anttalainen T., Jääskeläinen V., Introduction to communication networks. Artech House 2015

11 MEF, Technical Specification MEF6.2 EVC Ethernet Services Definitions Phase 3, 2014 http://www.mef.net/Assets/Technical_Specifications/PDF/MEF_6.2.pdf Read 6 Feb 2016

12 MEF, Technical Specification MEF10.2 Ethernet Services Attributes Phase 2, 2009 http://www.mef.net/PDF_Documents/technical-specifications/MEF10.2.pdf Read 7 Oct 2015

13 MEF, Bandwidth Profiles for Ethernet Services MEF (Metro Ethernet Forum) http://www.metroethernetforum.org/Assets/White_Papers/Bandwidth-Profiles-for-Ethernet-Services.pdf Read 7 Oct 2015

14 3Gpp TS 36.412. V8.6.0. Evolved Universal Terrestrial Access Network (E-UTRAN); S1 signaling transport. 2009.

15 3Gpp TS 36.422. V8.6.0. Evolved Universal Terrestrial Access Network (E-UTRAN); X2 signaling transport. 2009.

16 Penttinen J. (ed). The LTE/SAE Deployment Handbook. John Wiley & Sons. 2012

17 3Gpp TS 36.414. V8.4.0. Evolved Universal Terrestrial Access Network (E-UTRAN); S1 data transport. 2009.

18 3Gpp TS 36.424. V8.4.0. Evolved Universal Terrestrial Access Network (E-UTRAN); X2 data transport. 2009.

19 Grayson M, Shatzkamer K, Wainner S. Design, Measurement and Management of Large-Scale IP Networks—Bridging the Gap between Theory and Practice. Cambridge University Press; 2009. URL: http://mmlviewer.books24x7.com/book/id_30921/viewer.asp?bookid=30921&chunkid=1&endofproduct=1. Accessed 2 Feb 2014.

20 NSN. LTE Access Transport Planning Guideline. RL40 and earlier releases. [online] company internal document. 2013. URL: https://sharenet-ims.inside.nokiasiemensnetworks.com/Overview/D496799637. Accessed 2 Feb 2014.

21 ngmn. Guidelines for LTE Backhaul Traffic Estimation. White paper. Ngmn. 2011. https://www.ngmn.org/uploads/media/NGMN_Whitepaper_Guideline_for_LTE_Backhaul_Traffic_Estimation.pdf Accessed 17 Dec 2015.

22 ngmn. Backhaul Provisioning for LTE-Advanced & Small Cells. White paper. Ngmn. 2014. https://www.ngmn.org/uploads/media/150929_NGMN_P-Small-Cells_Backhaul_for_LTE-Advanced_and_Small_Cells.pdf Accessed 17 Dec 2015

23 NSN. LTE Domain of Parameter Dictionary Database (PDDB) [online] company internal database. URL http://pddb.inside.nokiasiemensnetworks.com/pddb/parameters/index.jsp Accessed 2 Feb 2014.

24 IEEE std 802.1Q-2011. Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks. IEEE. 2011

25 ETSI. Mobile-edge Computing, White paper. 2014 https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf Accessed 17 Dec 2015.

26 Solomon M. G., Kim D., Carrell J. L. Fundamentals of Communications and Networking, Second Edition. Jones and Bartlett Learning. 2015.

27 LTE Radio Access, Rel. RL70, Operating Documentation, Issue 02, Feature List, DN0944258

28 Katz D., Ward D. RFC5880. Bidirectional Forwarding Detection (BFD). IETF. 2010

29 Akiya N., Binderberger M., Mirsky G. RFC7419. Common Interval Support in Bidirectional Forwarding Detection. IETF. 2014.

30 Katz D., Ward D. RFC5883. Bidirectional Forwarding Detection (BFD) for Multihop Paths. IETF 2010.

31 3GPP TS 29.281. V10.0.0. General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U). 2010

32 Hedayat K, Krzanowiski R, Morton A, Yum K, Babiarz J. RFC5357. A Two-Way Active Measurement Protocol (TWAMP). IETF. 2008 [online] URL http://www.rfc-base.org/txt/rfc-5357.txt. Accessed 2 Feb 2014.

33 Forsberg D., Horn G., Moeller W-D., Niemi V. LTE security. John Wiley & Sons. 2013

34 3GPP TS 33.210. V10.0.0. Network Domain Security (NDS); IP network layer security. 2010

35 Kunimoto K., Morita T., Suzuki K., Uchiyama T. Technology Supporting Core Network (EPC) Accommodating LTE. NTT Dokomo Technical journal Vol. 13 No 1.

36 Leung V C.M, Ribeiro E. P., Wagner A., Iyenyar J. (eds), Multihomed Communication with SCTP (Stream Control Transmission Protocol). Auerbach Publications. 2013

37 Steward R. RFC 4960. Stream Control Transmission Protocol. IETF 2007

38 Barreios M., Lundqvist P. QoS-Enabled Networks: Tools and Foundations. John Wiley & Sons. 2011.

39 Bonaventure O., De Cnodder S., RFC2963 A Rate Adaptive Shaper for Differentiated Services. IETF 2000

40 Nokia, Signaling Transport over IP (M3UA and IUA), DN01141526, GSM/EDGE BSS, Rel. RG30(BSS), Operating Documentation, Issue 04

41 ITU-T I.412. ISDN user-network interfaces interface structure and access capabilities. 1993

42 ITU-T Q.920. ISDN user-network interface data link layer – General aspects. 1993

43 ITU-T Q.921. ISDN user-network interface – Data link layer specification. 1997

44 ITU-T Q.931. ISDN user-network interface layer 3 specification for basic call control. 1998

45 Morneault K.,Rengasami S., Kalla M., Sidebottom G. RFC4233, Integrated Services Digital Network (ISDN) Q.921-User Adaptation Layer. IETF 2006

46 GSM/EDGE BSS, Rel. RG40 (GSM 15), Operating Documentation, Issue 03 Product description of Flexi BSC DN70577137

47 Nokia. DN70646579. OY - SCTP Configuration Handling. GSM/EDGE BSS, Rel. RG30(BSS), Operating Documentation, Issue 04

48 Nokia. DN063312. DW – Primary Rate Access D-Channel for IUA Data Handling. GSM/EDGE BSS, Rel. RG30(BSS), Operating Documentation, Issue 04

49 Nokia, DN9813866, BSS Radio Network Parameter Dictionary, Reference, GSM/EDGE BSS, Rel. RG30(BSS), Operating Documentation, Issue 04

Parameter Planning Sheet Optimisation in GERAN

1 Description of the Parameter Planning Sheet Optimisation

This appendix discusses shortly about the parameter interrelation optimisation in planning sheets used for GSM EDGE Radio Access Network (GERAN). The planning sheets discussed are used to manage the Base Station Controller (BSC) and Base Transceiver Station (BTS) parameters during the planning phase in roll-out projects. These planning sheets are called BSC datafill and BTS integration sheet. Parameter interrelation optimisation aims to reduce the number of human entries to generate a given number of required parameters. Parameter interrelation optimization shall not be confused with the network optimisation where the aim is to improve the network operational performance by tuning the network parameters.

In the GERAN parameter interrelation optimization case the signalling connection parameters in Abis interface is studied. In GERAN architecture the Abis interface is located in between the Base Transceiver Station (BTS) to Base Station Controller (BSC). The number of entries a planner have to fill in or at least have to consider for a full Base Station Controller (BSC) configuration, containing 4620 signalling links, is reduced from 134000 down to 115500. This is achieved by the planning sheet modification.

In the first improvement step two group of parameters are merging to single group. Originally a group is defined as a set of parameters required for a single command line command. By merging two groups to a single group is feasible as many of the parameters required in these two groups are the same and must be aligned manually anyhow. By this merge a design for services principle that one parameter is entered only once in the system is fulfilled.

The planning sheets under discussion are listed in Table 24.

Table 24. Company internal data used in GERAN parameter analysis.

file	File name and version	Link
BSC datafill template version 69	V69-RG20EP1_data-fill_template.xls.	https://sharenet-ims.inside.nokiasiemensnet-works.com/Overview/D433288722 Accessed 9 Mar 2014 using version control to get earlier version.
BSC datafill template version 74	V74-RG20EP1EP2_data-fill_template.xls.	https://sharenet-ims.inside.nokiasiemensnet-works.com/Overview/D433288722 Accessed 9 Mar 2014.
BTS Integration sheet.	V46-BTS IP@ template - RG30.xlsx	https://sharenet-ims.inside.nokiasiemensnet-works.com/Overview/D486848059. Accessed 9 Mar 2014.

The use of the planning sheets is discussed in in the company internal planning guidelines. The achieved improvement is clearly notable in the planning sheets themselves and in the planning guidelines. These company internal documents are listed in Table 25.

Table 25. Company internal planning documents discussing the planning sheets (GERAN).

Company internal planning documents discussing the planning sheets (GERAN)	Document number
RG 20 Packet Abis and AoIP Dimensioning and Planning Guidelines	D424443119
RG 20(EP1) Packet Abis and AoIP Dimensioning and Planning Guidelines	D437437766
RG 30 Packet Abis and AoIP Planning Guidelines	D486927060

Next the Abis signalling links are discussed shortly and the discussion continues with the improvement iterations.

2 Description of the Abis Signalling Links and Parameters

The signalling protocol stack of the packet Abis is shown in Figure 32 [40]. In legacy Abis the control plane messages are transferred according to Link Access Procedure on the D-channel (LAPD) at Integrated Services Digital Network (ISDN) user-network interface. Originally the D-channel used in Abis was defined as a 64 kbit/s channel in E1/T1 frame [41]. Later on also 16 kbit/s and 32 kbit/s channel were adopted to optimise the E1/T1 capacity usage. The link layer aspects related to the D-channel are defined in ITU-T Q.920 and Q921 specifications [42;43]. The specifications are defined for TDM based D-channels. The corresponding network layer aspects are covered in ITU-T Q.931 specification [44].

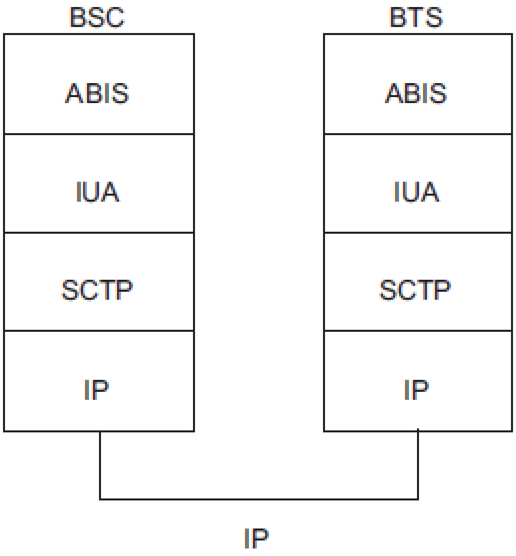


Figure 32. A protocol stack for Packet Abis C-plane and M-plane in GERAN. The Abis application part is interfacing IUA adaptation layer and not the SCTP directly as in the LTE. Copied from [40].

The original link protocol recommendations Q.920 and Q.921 are not optimal for IP/Ethernet based packet networks. Instead the Stream Control Transport Protocol (SCTP) defined by the Internet Engineering Task Force (IETF) is used to carry signalling messages in GERAN. To maintain the compatibility to the Q.921 / Q.931 boundary primitives for example addressing scheme an adaptation between the Q.931 and the SCTP is required. The ISDN Q.921-User Adaptation (IUA) layer provides the necessary adaptation [45].

The Stream Control Transport Protocol (SCTP) provides reliable in-sequence transport of signalling messages between the BSC and the BTS [36;37]. The IUA and SCTP together provide the similar functionality as the Q.921 does in TDM based transport connections. The parameters related to Q.931/Q.921 boundary and the SCTP protocol are in focus in the parameter interrelation optimisation. The BSC model used in this analysis is Nokia FlexiBSC.

The full FlexiBSC configuration in RG20 release supports up to 4200 Transceivers (TRXs) [46]. In this implementation each TRX requires a TRX signalling link (TRXSIG) of its own. Furthermore, a management function for the Base Transceiver Station (BTS) equipment, *Base Control Function* (BCF), requires similar BCF Signalling link (BCFSIG) also called as Operation and Maintenance Signalling link (OMUSIG). Four Man Machine Language (MML) commands are required to configure and activate each TRX signalling (TRXSIG) operation and maintenance signalling (OMUSIG) link. An example of the syntax of the MML commands required to create and activate an OMUSIG link is shown in Table 26. The ZOPX command is used to create a SCTP association and the ZOYP is used to manage association IP addresses [47]. The ZDWP command creates an Abis D-channel and finally the ZOYS is used to modify the state of the association [47;48].

Table 26. MML command for OMUSIG SCTP association creation.

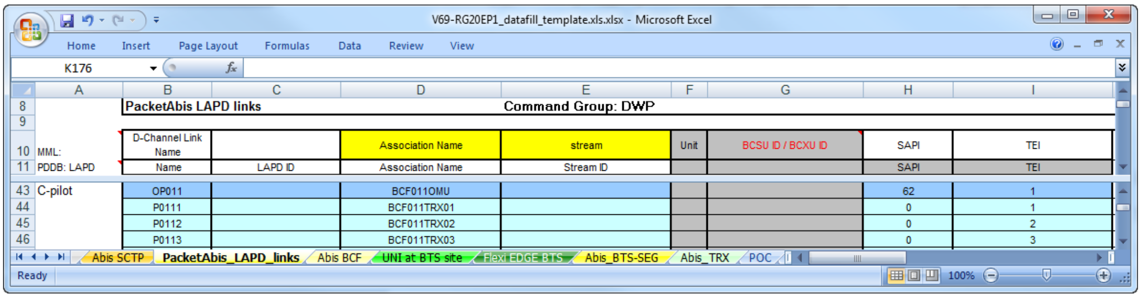
MML command for OMUSIG SCTP association creation
ZOYX:BCF313OMU:IUA:S:BCXU,0:AFASTNEW;
ZOYP:IUA:BCF313OMU:"10.11.22.20",,49152:"10.66.0.3",27,,,49152;
ZDWP:OP313:BCXU,0:62,1:BCF313OMU,;
ZOYS:IUA:BCF313OMU:ACT:;

These parameters are visible in a planning sheet and thus needs to be defined during the access planning phase. Three different approaches how the parameters are organised in the planning sheets are discussed in the following subsections. The following presentation is based on the planning sheets listed in Table 24.

Next the different planning sheet versions are discusses. First the version 69 of the BSC datafill is discussed. This is the last release before applying the improvements discussed later in this document.

2.1 Case 1 – BSC Datafill Version V69

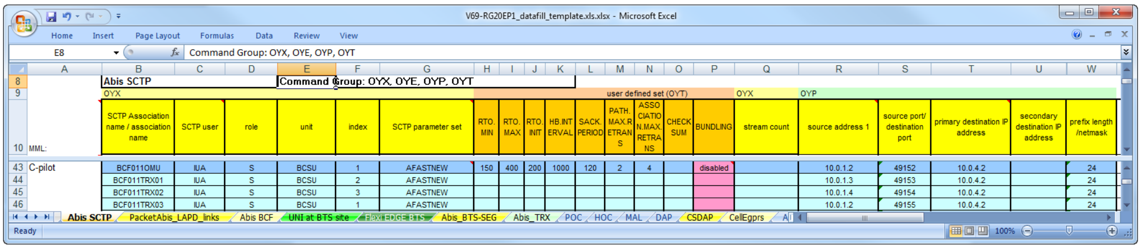
The parameters for the four MML commands were presented individually in the BSC datafill (version V69). BSC datafill is a planning Excel (XLS) sheet for BSC parameters. The BSC datafill snapshot containing the Link Access Procedure on the D-channel (LAPD) parameters for Packet Abis is shown in Figure 33. In this structure of the planning sheet eight entries was required to include all possible parameters for the given MML command. In this example four out of the eight fields (D-Channel Link Name, Association Name, SAPI and TEI) were updated for each signalling link.



	A	B	C	D	E	F	G	H	I
8		PacketAbis LAPD links			Command Group: DWP				
9									
10	MML:	D-Channel Link Name		Association Name	stream	Unit	BCSU ID / BCXU ID	SAPI	TEI
11	PDDB: LAPD	Name	LAPD ID	Association Name	Stream ID			SAPI	TEI
43	C-pilot	OP011		BCF011OMU				62	1
44		P0111		BCF011TRX01				0	1
45		P0112		BCF011TRX02				0	2
46		P0113		BCF011TRX03				0	3

Figure 33. A snapshot of the LAPD link parameters for packet Abis in the BSC Datafill Version V69. For each parameter in MML command to create the LAPD link an entry is introduced in the planning sheet (GERAN).

In addition to Packet Abis Link Access Procedure on the D-channel (LAPD) parameters the Stream Control Transmission Protocol (SCTP) parameters are needed for each signalling link. The parameters required for SCTP association creation are shown in Figure 34. This table contains of parameters for several MML commands; OYX, OYT, OYX and OYP. The total number of parameter entries is 21 for each SCTP association. Some of the entries contain the same values always for example *the SCTP user* for Abis interface is always 'IUA' and *the unit* is always 'BCSU' for FlexiBSC. Further, some of the parameters may assume the system default value and thus be left empty in the planning sheet.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W
8		Abis SCTP			Command Group: OYX, OYE, OYP, OYT																	
9		OYX						user defined set (OYT)									OYX	OYP				
10	MML:	SCTP Association name / association name	SCTP user	role	unit	index	SCTP parameter set	RTO. MIN	RTO. MAX	RTO. INIT	HB.INTERVAL	SACK. PERIOD	PATH. MAX.RETRANS	ASSOCIATION.MAX. RETRANS	CHECK SUM	BUNDLING	stream count	source address 1	source port/ destination port	primary destination IP address	secondary destination IP address	prefix length /netmask
43	C-pilot	BCF011OMU	IUA	S	BCSU	1	AFASTNEW	150	400	200	1000	120	2	4		disabled		10.0.1.2	49152	10.0.4.2		24
44		BCF011TRX01	IUA	S	BCSU	2	AFASTNEW											10.0.1.3	49153	10.0.4.2		24
45		BCF011TRX02	IUA	S	BCSU	3	AFASTNEW											10.0.1.4	49154	10.0.4.2		24
46		BCF011TRX03	IUA	S	BCSU	1	AFASTNEW											10.0.1.2	49155	10.0.4.2		24

Figure 34. SCTP parameters for Packet Abis in the BSC Datafill Version V69 (GERAN)

The SCTP timer values (columns H to P) are managed as *SCTP parameter set* which then can be applied for several associations. Timer values needs to be tuned if the characteristic of the transport path deviates from the reference one. One use case is the satellite connection. The SCTP timer parameter values are entered in SCTP parameter set level and thus not needed for each signalling link.

The total number of entries in BSC datafill V69 for each OMUSIG and TRXSIG link and for the reference BSC configuration is summarized in Table 27. These values are used as a base line reference values for further cases.

Table 27. Case 1 - Entries for SCTP association and D-channel in the BSC Datafill Version V69 (GERAN).

Object level	Parameter entries note1	Number of entries note2	Number of characters in entries note2
BCF	D-channel (Figure 33 SCTP associations (Figure 34)	4 + 10 = 14	17+49 = 66
TRX	D-channel , SCTP associations	4 + 10 = 14	18+51=69
Total for total 4620 signalling links 4200 TRX (420 BCFs)		420 *14 + 4200*14 = 64680	420*66 + 4200*69= 27720 + 289800 = 317520

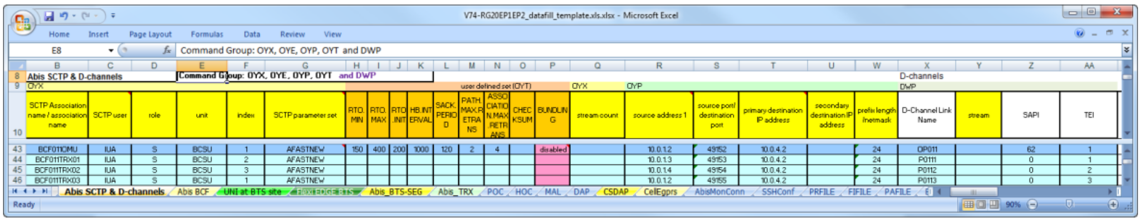
Note 1. Only actively used entries counted.

Note 2. SCTP timer parameters (OYT command group) not counted.

The next case represents minor improvement for BSC datafill structure. This was introduced in BSC datafill version 74.

2.2 Case 2 – BSC Datafill Version V74

In the BSC datafill version V74 the LAPD and SCTP planning sheets are merged. This is possible as the MML commands are sharing the same parameters. The merged planning sheet is shown in Figure 35.



Command Group: OYX, OYE, OYP, OYT and DWP

Abis SCTP & D-channels

D-channels

	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	W	X	Y	Z	AA
9	OYX						user defined set (OYT)									OYX	OYP					DWP			
10	SCTP Association name / association name	SCTP user	role	unit	index	SCTP parameter set	RTO.MIN	RTO.MAX	RTO.INIT	HB.INTERVAL	SACK.PERIOD	PATH.MAX.RETRANS	ASSOCIATION.MAX.RETRANS	CHECKSUM	BUNDLING	stream count	source address 1	source port/ destination port	primary destination IP address	secondary destination IP address	prefix length /netmask	D-Channel Link Name	stream	SAPI	TEI
43	BCF011OMU	IUA	S	BCSU	1	AFASTNEW	150	400	200	1000	120	2	4		disabled		10.0.1.2	49152	10.0.4.2		24	OP011		62	1
44	BCF011TRX01	IUA	S	BCSU	2	AFASTNEW											10.0.1.3	49153	10.0.4.2		24	P0111		0	1
45	BCF011TRX02	IUA	S	BCSU	3	AFASTNEW											10.0.1.4	49154	10.0.4.2		24	P0112		0	2
46	BCF011TRX03	IUA	S	BCSU	1	AFASTNEW											10.0.1.2	49155	10.0.4.2		24	P0113		0	3

Abis SCTP & D-channels / Abis BCF / UNI at BTS site / FlexiEDGE BTS / Abis_BTS-SEG / Abis_TRX / POC / HOC / MAL / DAP / CSDAP / CellEgprs / AbisMonConn / SSHConf / PRFILE / FIFILE / PAFILE

Figure 35. Abis SCTP & D-channel planning sheet in the BSC Datafill Version V74. The D-channel and SCTP association tabs are merged as they contain may same parameters. This reduces the number of required entries.

The total number of entries in *the Abis SCTP & D-channel* sheet is 25 per OMUSIG and TRXSIG link. The number of entries in BSC datafill v69 was 29 thus almost 14% reduction was achieved by the sheet merge. The reduction in actively used entries from case one is from 64680 to 55440 and the number of characters to be typed from 317520 down to 249900. The number of entries for case 2 is summarised in Table 28.

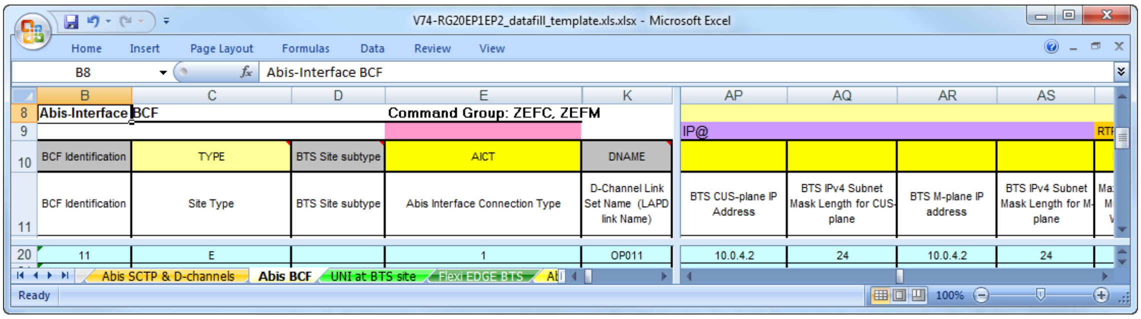
Table 28. Case 2 – The number of entries required for the SCTP associations and the D-channel in the BSC Datafill Version V74 (GERAN).

Object level	Parameter entries note1	Number of entries note2	Number of characters in entries note2
BCF	D-channel , SCTP associations	13	55
TRX	D-channel , SCTP associations	13	54
Total for total 4620 signalling links 4200 TRX (420 BCFs)		420 *13 + 4200*13 = 60060	420*55 + 4200*54 = 23100 + 226800 = 249900

Note 1. Only actively used entries counted.

Note 2. SCTP timer parameters (OYT command group) not counted.

This solution still had couple of problems which could be solved by further optimizing the parameter interrelations. The SCTP association is created between two computer units one in the BTS and another in the BSC. In this implementation two parameters are used to identify a computer unit thus introducing a redundant step. The BTS computer unit is identified directly by *the primary destination IP address* (10.0.4.2) and also indirectly at BCF creation step. In other word the BTS IP address is entered twice, once in SCTP association creation phase and again in the BCF object creation phase. *The BTS M-plane IP address* (10.0.4.2) and the D-channel name, *DNAME*, are given to BCF object as a parameter when the BCF is created. This process introduces redundant entry which a planner must consider. A snapshot of parameters needed for BCF object is given in Figure 36.

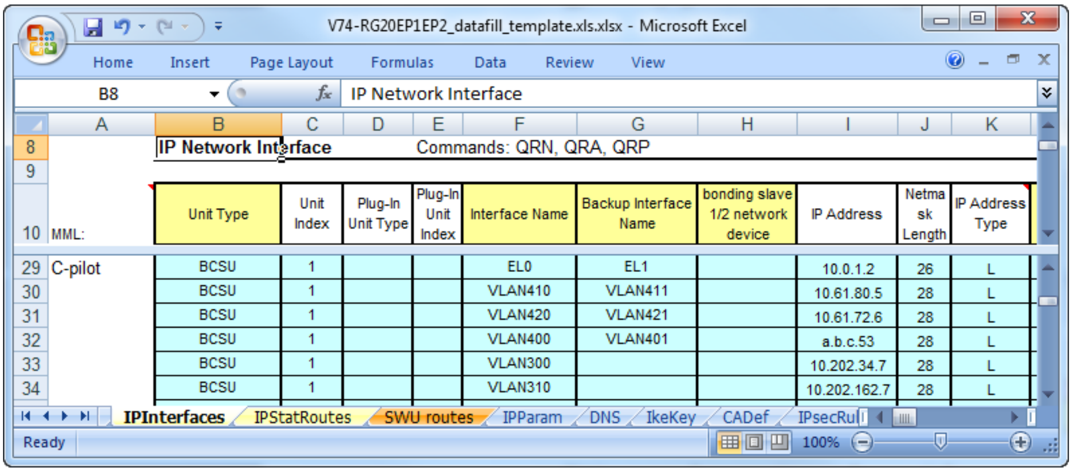


	B	C	D	E	K	AP	AQ	AR	AS
8	Abis-Interface BCF			Command Group: ZEFC, ZEFM					
9						IP@			
10	BCF Identification	TYPE	BTS Site subtype	AICT	DNAME				
11	BCF Identification	Site Type	BTS Site subtype	Abis Interface Connection Type	D-Channel Link Set Name (LAPD link Name)	BTS CUS-plane IP Address	BTS IPv4 Subnet Mask Length for CUS-plane	BTS M-plane IP address	BTS IPv4 Subnet Mask Length for M-plane
20	11	E		1	OP011	10.0.4.2	24	10.0.4.2	24

Figure 36. A snapshot of parameters for BCF creation in the BSC Datafill Version V74. The D-channel which was defined earlier is now associated with the BFC.

Similarly the reference to BSC computer unit is redundant. The computer unit is identified not only by the signalling unit and index, *BCSU 1*, but also by the signalling unit IP address given as *source address 1* (10.0.1.2) in Figure 35. This double reference to the same unit cause additional typing and it is also a source for potential human errors as the IP address given in *the Abis SCTP & D-channel* sheet must match the one given for the BSCU in *the IP Interfaces* section shown in Figure 37.

In this snapshot several VLAN interface IP addresses and one interface IP address can be seen. The interface address is the same what was used in this example for SCTP association.



IP Network Interface Commands: QRN, QRA, QRP

MML:	Unit Type	Unit Index	Plug-In Unit Type	Plug-In Unit Index	Interface Name	Backup Interface Name	bonding slave 1/2 network device	IP Address	Netmask Length	IP Address Type
C-pilot	BCSU	1			EL0	EL1		10.0.1.2	26	L
	BCSU	1			VLAN410	VLAN411		10.61.80.5	28	L
	BCSU	1			VLAN420	VLAN421		10.61.72.6	28	L
	BCSU	1			VLAN400	VLAN401		a.b.c.53	28	L
	BCSU	1			VLAN300			10.202.34.7	28	L
	BCSU	1			VLAN310			10.202.162.7	28	L

Figure 37. A snapshot of the IP interface section in the BSC Datafill Version V74. The IP addresses used in the SCTP association must match the ones defined for the computer units.

The double reference situation across these four BSC objects is shown in Figure 38. The actual parameter naming syntax depends on the MML command in question. In this figure the parameter names are harmonized for clarify in the illustration. In the left hand side the SCTP association object has two references to a BCSU, one to BCSU index and other to BCSU IP address. The same BCSU is referred third time in D-channel object. Also the reference to BTS (BCF managed object) is redundant. The SCTP association has Destination IP address parameters to refer a BTS M-plane or C-plane IP address. This relation could be solved also via D-channel object.

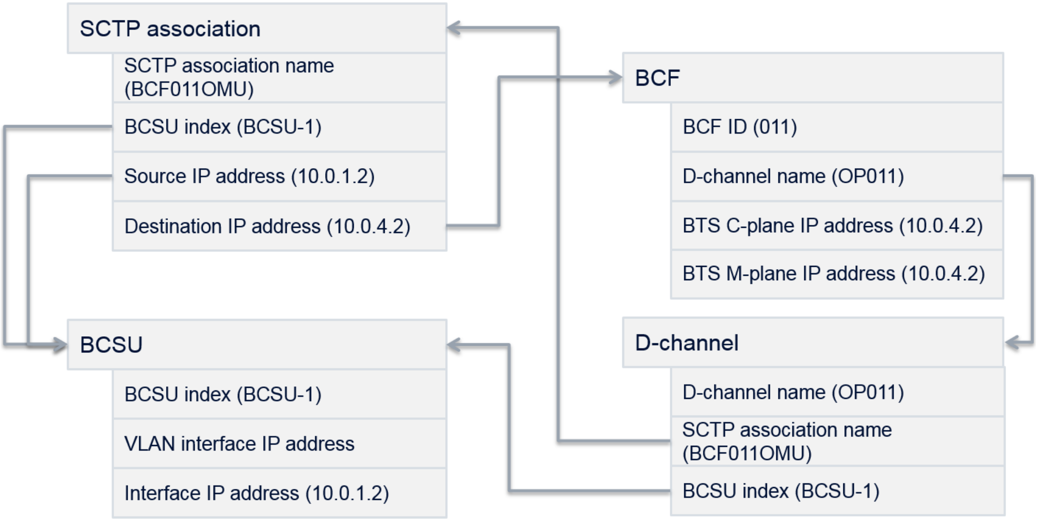

SCTP association
SCTP association name (BCF011OMU)
BCSU index (BCSU-1)
Source IP address (10.0.1.2)
Destination IP address (10.0.4.2)
BCF
BCF ID (011)
D-channel name (OP011)
BTS C-plane IP address (10.0.4.2)
BTS M-plane IP address (10.0.4.2)
BCSU
BCSU index (BCSU-1)
VLAN interface IP address
Interface IP address (10.0.1.2)
D-channel
D-channel name (OP011)
SCTP association name (BCF011OMU)
BCSU index (BCSU-1)

Figure 38. An example of BSC parameter double reference. The SCTP association refers to the signalling unit by the unit index and by the unit interface IP address. The same unit index is also used in D-channel definition. The IP address given for the BCF must match the value used in the SCTP association definition.

The second problem is that the relatively long strings are required repetitively for frequent parameters. The two IP addresses and two name parameters in this example generated the need to type 32 characters for each signalling link. The IP addresses used in this example represents a simple one containing less characters to type than in average. The next step is to addresses these two problems. The improvements which are considered to solve the problems are listed in Table 29.

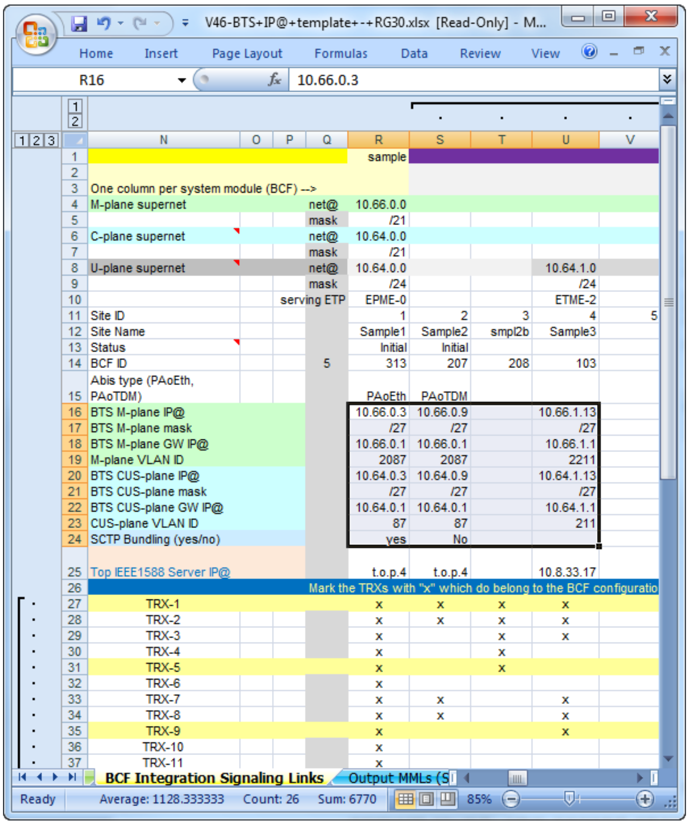
Table 29. Improvements which are considered to address the problems listed in Table 28.

Considered improvements
The BTS M-plane and C-plane IP addresses shall be given only once per BCF and not for each TRX separately. Entry per TRX leads to 10 and more entries per BCF in average.
The double reference to BCSU in the SCTP association shall be replaced by single reference, BCSU index only. The IP address shall be solved from the data defined for the BCSU before.
The name parameters shall be generated automatically based on the other parameters for example BCF and TRX ID.

The solution required another structure and was implemented in a separate planning sheet. The solution is discussed in next subsection.

2.3 Case 3 – BTS IP Address Template

BTS IP address template was developed. The parameters are organised in this planning sheet by base station equipment (BCF managed object), one column per each BCF. The entries required to solve the MML command required for SCTP association and D-channel creation are divided into two sections. Firstly the BTS M-plane and C-plane IP address data and BTS TRX configuration is given as input. Snapshot of this is shown in Figure 39.


V46-BTS+IP@+template+-+RG30.xlsx [Read-Only] - M...

R16 10.66.0.3

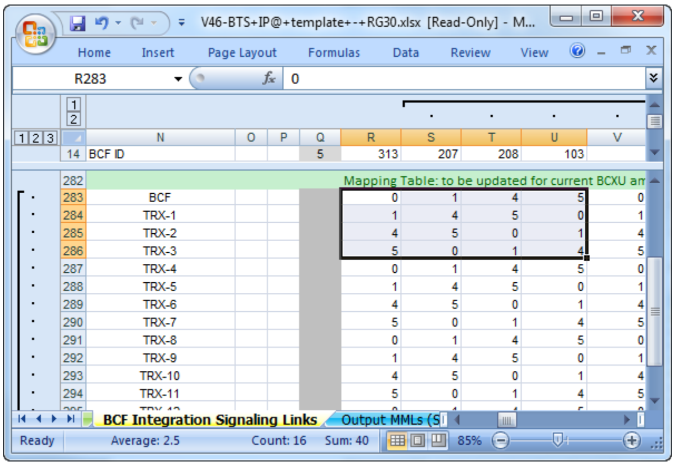
	N	O	P	Q	R	S	T	U	V
1					sample				
2									
3	One column per system module (BCF) -->								
4	M-plane supernet			net@	10.66.0.0				
5				mask	/21				
6	C-plane supernet			net@	10.64.0.0				
7				mask	/21				
8	U-plane supernet			net@	10.64.0.0			10.64.1.0	
9				mask	/24			/24	
10				serving ETP	EPME-0			ETME-2	
11	Site ID				1	2	3	4	5
12	Site Name				Sample1	Sample2	smpl2b	Sample3	
13	Status				Initial	Initial			
14	BCF ID			5	313	207	208	103	
15	Abis type (PAoEth, PAoTDM)				PAoEth	PAoTDM			
16	BTS M-plane IP@				10.66.0.3	10.66.0.9		10.66.1.13	
17	BTS M-plane mask				/27	/27		/27	
18	BTS M-plane GW IP@				10.66.0.1	10.66.0.1		10.66.1.1	
19	M-plane VLAN ID				2087	2087		2211	
20	BTS CUS-plane IP@				10.64.0.3	10.64.0.9		10.64.1.13	
21	BTS CUS-plane mask				/27	/27		/27	
22	BTS CUS-plane GW IP@				10.64.0.1	10.64.0.1		10.64.1.1	
23	CUS-plane VLAN ID				87	87		211	
24	SCTP Bundling (yes/no)				yes	No			
25	Top IEEE1588 Server IP@				t.o.p.4	t.o.p.4		10.8.33.17	
26					Mark the TRXs with "x" which do belong to the BCF configuratio				
27	TRX-1				x	x	x	x	
28	TRX-2				x	x	x	x	
29	TRX-3				x		x	x	
30	TRX-4				x		x		
31	TRX-5				x		x		
32	TRX-6				x				
33	TRX-7				x	x		x	
34	TRX-8				x	x		x	
35	TRX-9				x			x	
36	TRX-10				x				
37	TRX-11				x				

BCF Integration Signaling Links | Output MMLs (S

Ready Average: 1128.333333 Count: 26 Sum: 6770 85%

Figure 39. BTS IP address section and TRX configuration section in the BTS IP address template. These addresses were introduced once and look-up function was used to pick up the relevant IP address to the given association. The traffic plane was used as a key for the look up.

Secondly the TRX to BCSU mapping logic is defined. This represents control data rather than site specific planning data and thus can be prepared well in advanced for future BCFs. This is done once as a preparation step for the planning sheet. Figure 40 shows an example of TRX to BCSU mapping control.


V46-BTS+IP@+template+-+RG30.xlsx [Read-Only] - M...

R283 0

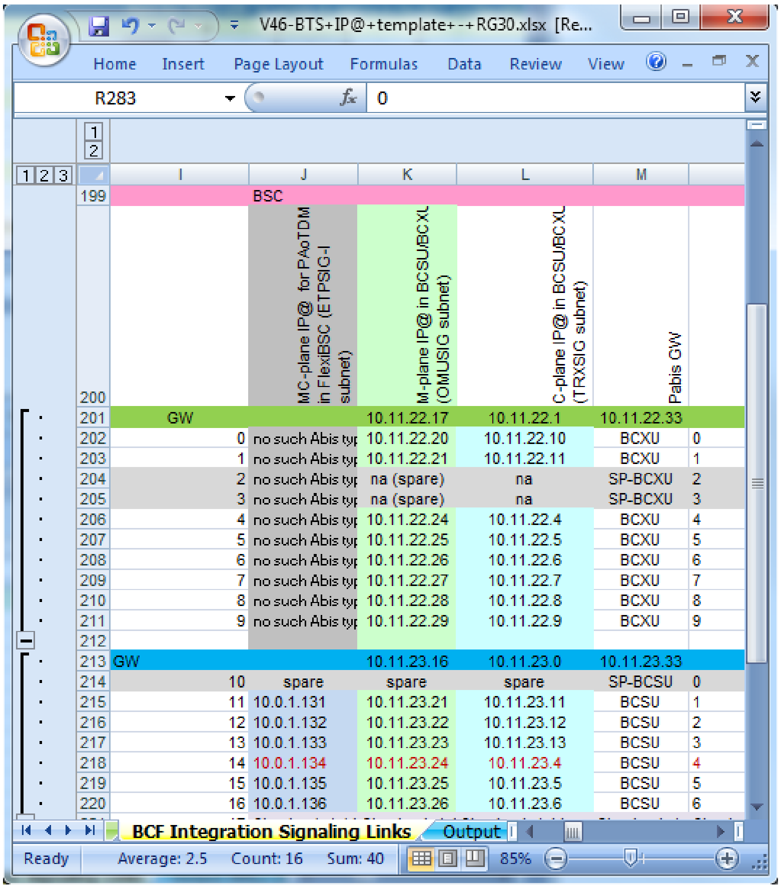
	N	O	P	Q	R	S	T	U	V
14	BCF ID			5	313	207	208	103	
282					Mapping Table: to be updated for current BCXU am				
283	BCF				0	1	4	5	0
284	TRX-1				1	4	5	0	1
285	TRX-2				4	5	0	1	4
286	TRX-3				5	0	1	4	5
287	TRX-4				0	1	4	5	0
288	TRX-5				1	4	5	0	1
289	TRX-6				4	5	0	1	4
290	TRX-7				5	0	1	4	5
291	TRX-8				0	1	4	5	0
292	TRX-9				1	4	5	0	1
293	TRX-10				4	5	0	1	4
294	TRX-11				5	0	1	4	5

BCF Integration Signaling Links | Output MMLs (S

Ready Average: 2.5 Count: 16 Sum: 40 85%

Figure 40. TRX to BCSU mapping section in the BTS IP address template. This approach distributed the SCTP associations and also the load evenly to the signalling units.

Round robin method is used to distribute the TRXs to active signalling units (vertical). The number in the table identifies the signalling unit which processes the SCTP association and D-channel for the given TRX and BCF. In this example the signalling units 0, 1, 4 and 5 belong to the BSC configuration. Round robin is also applied cross the BCFs (horizontal). Another control data are the BCSU IP addresses. In this planning sheet these are defined once for the BSC and not for each SCTP association separately. Snapshot is shown in Figure 41.



R283 | 0

	I	J	K	L	M	
199		BSC				
200		MC-plane IP@ for PAoTDM in FlexiBSC (ETPSIG-I subnet)	M-plane IP@ in BCSU/BCXL (OMUSIG subnet)	C-plane IP@ in BCSU/BCXL (TRXSIG subnet)	Pabis GW	
201	GW		10.11.22.17	10.11.22.1	10.11.22.33	
202	0	no such Abis typ	10.11.22.20	10.11.22.10	BCXU	0
203	1	no such Abis typ	10.11.22.21	10.11.22.11	BCXU	1
204	2	no such Abis typ	na (spare)	na	SP-BCXU	2
205	3	no such Abis typ	na (spare)	na	SP-BCXU	3
206	4	no such Abis typ	10.11.22.24	10.11.22.4	BCXU	4
207	5	no such Abis typ	10.11.22.25	10.11.22.5	BCXU	5
208	6	no such Abis typ	10.11.22.26	10.11.22.6	BCXU	6
209	7	no such Abis typ	10.11.22.27	10.11.22.7	BCXU	7
210	8	no such Abis typ	10.11.22.28	10.11.22.8	BCXU	8
211	9	no such Abis typ	10.11.22.29	10.11.22.9	BCXU	9
212						
213	GW		10.11.23.16	10.11.23.0	10.11.23.33	
214	10	spare	spare	spare	SP-BCSU	0
215	11	10.0.1.131	10.11.23.21	10.11.23.11	BCSU	1
216	12	10.0.1.132	10.11.23.22	10.11.23.12	BCSU	2
217	13	10.0.1.133	10.11.23.23	10.11.23.13	BCSU	3
218	14	10.0.1.134	10.11.23.24	10.11.23.4	BCSU	4
219	15	10.0.1.135	10.11.23.25	10.11.23.5	BCSU	5
220	16	10.0.1.136	10.11.23.26	10.11.23.6	BCSU	6

Figure 41. BSC M-plane and C-plane IP addresses for Abis interface in the BTS IP address template. These addresses were introduced once and look-up function was used to pick up the relevant IP address to the given association. The signalling unit index was used as a key for the look up.

The number of entries in this planning sheet can be divided into two groups: entries per BCF and entries per BSC. In the original approach the entries are per signalling link. Using the same assumptions; FlexiBSC with 4200 TRX, in average 10 TRX per BCF, the number of entries required for the SCTP associations and D-channels is calculated. Table 30 shown the number of required entries for case 3.

Table 30. Case 3 – The number of entries required for the SCTP associations and the D-channels in the BTS IP address template (GERAN).

Object level	Parameter entries	Number of entries	Number of characters in entries [note1]
BCF (case specific inputs)	BFC-ID (313), BTS M-plane IP address (10.66.0.1), BTS M-plane IP mask (/27), BTS C-plane IP address(10.64.0.1), BTS C-plane IP mask(/27), TRX configuration (10*"x")[note2]	15	35
BCF (controls)	TRX to BCSU mapping table	37	37
BSC	BCSU IP addresses[note3]	18	18*11 = 198
Total for 4200 TRX (420 BCFs)		420*(15+37) + 18 = 21858	420*(35+37) + 198 = 30438

Note 1 to be compatible with previous calculations 8 characters per IP address is assumed.

Note 2 to be compatible with previous calculations 10 TRX per BCF assumed

Note 3 worst case figures. The planning sheet supports single IP address entry per BSC. That approach can be used when predefined BSC subnet structure can be used in the given project.

The outcome of the BTS IP@ planning sheet is the list of required command line commands, Man Machine Language (MML) commands, shown in Table 31. For each signalling link four MML command is generated and thus for full BSC configuration more than 18000 MML commands are generated.

Table 31. The MML commands required for a signalling link of TRX 3 in BCF 208.

Man Machine Language (MML) commands for signalling link creation
ZOYX:BCF208TRX03:IUA:S:BCXU,1:AFASTNOB;
ZOYP:IUA:BCF208TRX03:"10.11.22.11",,49155:"0",,,,49155;
ZDWP:P2083:BCXU,1:0,3:BCF208TRX03,;
ZOYS:IUA:BCF208TRX03:ACT:;

In this approach the level of automation is extend to the MML command creation. The likelihood for mistyping MML commands is nil.

2.4 Naming Convention

The naming convention is automated in case 3 and this is reducing the required typing considerable. The SCTP association name parameter is an ASCII string having 1 to 16 characters. This name string is composed by fixed and variable fields. The syntax of the composed string is the following:

BCF<BCF ID><object>(<TRX ID>)

Where,

BCF

BCF is a constant string. “BCF” is used to distinguish the signalling association used at Abis interface (towards the BCF) from those used towards core elements.

<BCF ID>

BCF ID is a unique identifier of the BCF within a BSC. The range is from 1 to 4400, however, in practice the average number of TRX per BCF is more than 5 and thus less than 1000 BCF is created within a BSC having capacity of 4400 TRX [49, 200]. In this process three digit number is used to identify a BCF.

<object>

object is a string “OMU” or “TRX” to distinguish the operation and maintenance signalling links (OMUSIG) from telecom signalling links (TRXSIG)

<TRX ID>

Optional. *TRX ID* is used when <object> equals to “TRX”. It identifies the TRX within a BCF, range from 1 to 36.

SCTP association name for TRX 3 within BCF 208 is constructed as *BCF208TRX03*.
The second name parameter in this example is the D-channel name. Due to historical reasons this parameter is an ASCII string of up to 5 characters. Allowed characters are limited to “A” to “Z” and “0” to “9”. Traditionally the D-channel name indicates the TRX and the BCF the TRX belongs to. This approach is also used in this automated name construction.

The syntax for D-channel name is the following

<type><BCF ID><TRX ID>

Where,

type identifies the type of the D-channel. Typically used values

O	indicates an OMUSIG for legacy Abis interface
OP	indicates an OMUSIG for packet Abis interface
T	indicates a TRXSIG for legacy Abis interface
P	indicates a TRXSIG for packet Abis interface

BCF ID three digit number

TRX ID single digit coded number

1 to 9	TRX ID 1 to 9
A to Z	TRX ID 10 to 35
0 TRX	ID 36 (TRX IDs greater than 18 are seldom used)

D-channel name used at packet Abis interface for TRX 3 within BCF 208 is constructed as *P2083*.

2.5 Double Entries

To avoid double entry for frequently used parameters look-up method is used. In the original approach the computer unit identifier and the interface IP address were parameters which were required for each signalling link separately. In the case 3 the double entry is avoided by applying a lookup method. Based on the computer unit identifier the relevant IP addresses is fetched from the predefined table. This method introduced a need for some preparation works including the computer unit identifier – computer unit interface IP address –table preparations. This preparation work, however, is small when large number of SCTP associations is to be prepared. For small number of associations the tradition method may be found more practical due to the less amount of required preparation work.

2.6 Summary of the Previous Findings

The results of these cases are summarised in Table 32. The first development step resulted 7% reduction in the number of required entries and 21% reduction in characters in these entries. The second development round further improved the situation and introduced 64% reduction in the number of active parameter entries and more than 90% reduction in the number of characters required for the entries compared to the case 1.

Table 32. Case comparison. Especially the case 3 has a huge decrease in required manual entries compared to the initial case, case 1.

Case	Number of entries (4200 TRX, 420 BCF)	Relative to case 1	Number of characters in entries	Relative to case 1
1 (Table 27)	64680	100%	317520	100%
2 (Table 28)	60060	93%	249900	79%
3 (Table 30)	21858	34%	30438	9.6%

The findings from this GERAN case are considered in eNB parameter model development. Key findings are listed in the Table 33.

Table 33. Key findings in GERAN planning sheet optimisation

Item	Findings
1	Naming convention was automated
2	Double entry was eliminated. Any parameter was entered only once in the planning sheet even it was needed by several system objects.

This concludes the discussion of the parameter interrelation study conducted earlier on GERAN Abis interface parameters.

Questionnaire for the eNB Transport Parameter Planning Practices

I am studying the practices used in eNB transport parameter planning. The target group for this study is the mobile access planners who have been doing the eNB transport high level design and defining the eNB transport parameter rules to be applied in a project.

I appreciate if you can invest few minutes of your time to help me in this study. This questionnaire has few questions I hope you can answer based on your best understanding.

If you have being doing eNB parameter planning you belong the main target group of this study.

I thank you for your time and effort. If you have any questions or comments please do not hesitate to contact me.

Best regards,
Raimo Ahosola
raimo.ahosola (at) nokia.com
<phone number>

Return address: raimo.ahosola (at) nokia.com

1 Motivation

The parameter planning is time consuming and error prone task. In many cases the very same value needs to be entered to many different parameters. Errors are hard to detect until the plan file is downloaded to the target eNB. And even the download is successful and the eNB seems to work properly still some parameter errors may remain undetected.

The aim is to simplify the required manual steps in planning phase and thus save time and cost and minimize the human errors and thus reduce the non-quality cost in the roll-out project.

The purpose of this questionnaire is to collect current practices from eNB roll-out projects.

Contents

2 eNB Transport Parameter Planning Practices

The purpose of this study is to gather the current practices used in LTE Access panning. The LTE access planning in this context refers the eNB transport interface and parameter planning.

This questionnaire is divided into three sections. The first section contains contact information and the characteristics of the project for example the roll-out speed and project scope and size. The second section is the free form area to collect practices how the parameter values have been chosen and what logic and rules have been used to generate values for parameters based on the values of the other parameters.

The third section summarizes the main eNB transport features. This is included here for your reference.

2.1 Scope

The scope of this study is the steps before the parameter formatting phase in the planning process. The simplified planning process is shown in Figure 1.

The interest area in this questionnaire is the rules and decisions used to define the eNB transport parameter interdependencies in the given project. The parameter formatting or organizing in tools such as Daisy or BTS Site Manger is not in the focus of this study.

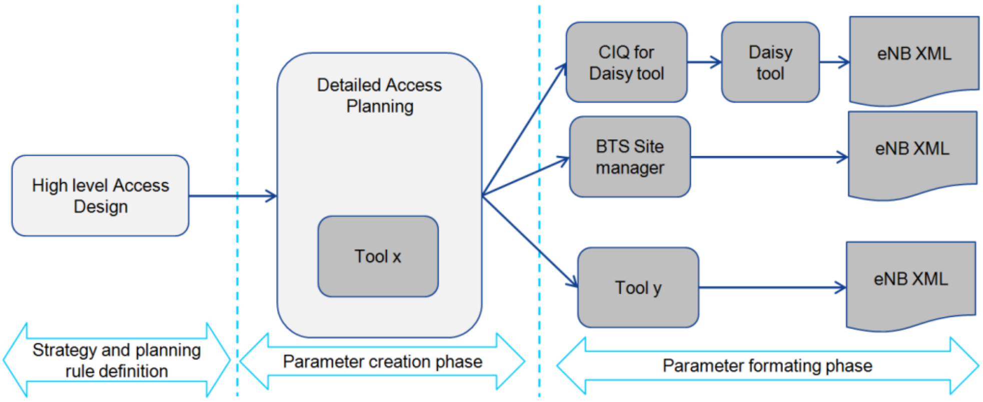


Figure 1. Access planning process

3 Contact Information Section

The study will handle the project anonymously. No contact person names or references to country or operator are shown in the final study report. The contact person information in this query is important on data collection phase. Further clarifications may be required after the first analysis.

Please fill in the following tables. Table 1 is filled with name and e-mail address of the technical expert who is able to further clarify the planning rules developed for and applied in the given project.

Table 1 Contact information

Contact item	Fill-in area
Operator/region	
Nokia Contact person name e.g. the eNB access planner	
Nokia Contact person e-mail address	
Nokia Contact person phone number	

Table 2 is filled in with project scope related data. This information may be used to categorize the similar projects to common category.

Table 2 Background information

Background item	Fill-in area
Average roll-out speed [eNB per month]	
Average roll-out speed per eNB access planner [eNB per month]	
Nokia planning scope in the given project.	[ ] eNB radio planning [ ] eNB access planning [ ] EPC planning [ ] IP backbone planning [ ] mobile backhaul planning
Nokia implementation scope	[ ] site acquisition [ ] civil works [ ] eNB installation, commissioning and integration

The example eNB XML file is useful to check what features are use in the given network. This may also be used to categorize the projects by used feature sets. Pls. if possible include an example XML to the return e-mail if possible or a link where I can access the file.

Table 3 Example eNB XML

eNB data item	Fill-in area
Current SW release	
[ ] link to the sample XML file(s)	<add link here>
attached eNB XML file [ ] TRS section only [ ] complete BTS and TRS	<attach file here>

4 Practice Section

This section collects the practices not only applied but also considered to streamline the eNB transport parameter planning. Explain shortly what kind of rules or mathematical formulas were used/considered for the parameter interdependencies. Examples:

1. Parameters: mPlaneIpAddress, uPlaneIpAddress, cPlaneIpAddress and sPlaneIpAddress shall all assume the VLAN interface IP address
2. Parameter: C-plane VLAN ID shall assume value M-plane VLAN ID +100

In this questionnaire the rules have been divided into the following categories depending on which information the given parameter value is based on.

An eNB transport parameter value is based on

1. the other transport parameter value of the same eNB
2. the other non-transport parameter value of the same eNB
3. the transport parameter value of the other eNB
4. the common, possible pseudo parameter, used for the cluster of the eNBs
5. the other means

Think of any rule even not written down which was found useful or was considered for defining the eNB transport parameters. It may be as simple as parameter x shall have the same value as parameter y, once y is defined x will be known based on y.

Also think of the planning cluster of eNBs. What parameters were common for the eNBs within the cluster? Was any systematic method used to manage these parameters?

Fill in the relevant categories.

eNB transport parameter definition based on the other transport parameter of the same eNB

/* add a free form explanation here. Possible mathematical formulas are well come as well */

eNB transport parameter definition based on the other BTS parameter of the same eNB
/* add a free form explanation here. Possible mathematical formulas are well come as well */

eNB transport parameter definition based on the transport parameter of the other eNB
/* add a free form explanation here. Possible mathematical formulas are well come as well */

eNB transport parameter definition based on the common, possible pseudo parameter, used for the cluster of the eNBs
/* add a free form explanation here. Possible mathematical formulas are well come as well */

eNB transport parameter definition based on the common possible pseudo parameter used for the cluster of the eNBs
/* add a free form explanation here. Possible mathematical formulas are well come as well */

5 Feature Section

In this section the radio, transport and operability features which presence is assumed to have an impact on the planning rules are listed. Please indicate if the given feature is used in the network. A feature in the list may have a clarification question which I hope is answered. In case different feature sets are used in different planning clusters one questionnaire per such cluster shall be filled in.

Table 4 eNB transport features

Feature ID	Feature name
LTE713 [1]	Synchronous Ethernet
LTE132 [1]	VLAN based traffic differentiation
LTE134 [1]	Timing over packet
LTE2 [2]	S1 Flex
LTE4 [2]	RAN Sharing
LTE140 [2]	Ethernet OAM
LTE491 [2]	FlexiPacket Radio Connectivity
LTE564 [2]	IPsec on FTIB
LTE592 [2]	Link Supervision with BFD
LTE649 [2]	QoS Aware Ethernet Switching
LTE775 [2]	SCTP Multi-homing (MME)
LTE475 [2]	Automatic iOMS Resiliency - introduction
LTE521 [2]	Security on Ethernet ports on FCM/FSM2
LTE144 [3]	Transport admission control
LTE574 [3]	IP Transport Network Measurements
LTE866 [3]	Fast IP Rerouting
LTE931 [3]	Ethernet Jumbo Frames
LTE612 [4]	Synchronization Hub
LTE628 [4]	FTIF Transport PDH / Ethernet
LTE593 [4]	Security for Ethernet Ports on FCT/FSM3
LTE947 [4]	FSMF Flexi Multiradio 10 System Module
LTE505 [5]	Transport Separation for RAN Sharing
LTE125 [6]	IPv6 for U/C-Plane
LTE1390 [6]	IPsec Emergency Bypass
LTE1401 [6]	Measurement based TAC
LTE610 [7]	Timing over Packet Resilience
LTE648 [7]	SCTP Multi-homing
LTE891 [7]	Timing over Packet with Phase Synch
LTE1240 [7]	User Layer TCP MSS clamping
LTE1753 [7]	Backup IPsec Tunnel

6 References

1 Feature Descriptions RL10, DN0978045

2 Feature Descriptions RL20, DN0978033

3 Feature Descriptions RL30, DN0986461

4 LTE RL40, Feature Descriptions and Instructions, DN09185979

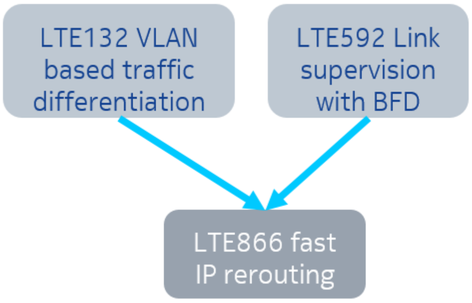
5 LTE RL50, Feature Descriptions and Instructions, DN09185967

6 LTE RL60, Feature Descriptions and Instructions, DN09185955

7 LTE RL70, Feature Descriptions and Instructions, DN09185982

An Example of a Feature Interrelations Map

Many eNB transport feature has relation to other transport feature. In the example shown in Figure 1 three features together forms a desired function, in this example traffic protection against the link failure. VLAN based traffic differentiation feature (LTE132) allows to define independent traffic paths for primary and secondary usage. Link supervision with BFD (LTE592) provides capability to detect failures on a link and finally the fast IP rerouting feature (LTE866) provides eNB with the capabilities to switch over to the secondary path when the primary path becomes unavailable.


LTE132 VLAN based traffic differentiation
LTE592 Link supervision with BFD
LTE866 fast IP rerouting

Fast IP rerouting relays on the link supervision feature in fault detection and it relays on VLAN based traffic differentiation feature for primary and secondary paths

Figure 1. An example feature interrelation map.

The IP addressing for this scenario is illustrated in Figure 2. In this example all eNB applications assume the same IP address (UCSM). The primary path is defined to us eNB VLAN interface T1 and the traffic will forwarded towards the next hop gateway GW1. This path is supervised with the bidirectional forwarding detection (BFD) process and the fast IP rerouting is defined to use this path as primary path for all traffic based on the BFD condition. The secondary path is given lower priority in the routing table and thus it will only be used when the primary, higher, priority path is declared to be unavailable by the BFD process.

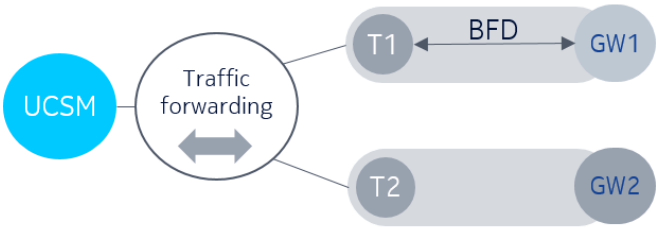


Figure 2. An IP addressing with traffic protection using VLAN based traffic differentiation, link supervision with BFD and fast IP rerouting features