Specific Targeted Research Project

FLAVIA
FLexible Architecture for Virtualizable wireless future Internet Access

Deliverable Report

D 3.1.2 – Revision of 802.16 architecture and interfaces specification

Deliverable title	802.16 architecture and interfaces specification
Version	1.0
Due date of deliverable (month)	M24
Actual submission date of the deliverable (dd/mm/yyyy)	16/07/2012
Start date of project (dd/mm/yyyy)	01/07/2010
Duration of the project	36 months
Work Package	WP3
Task	Task 3.1
Leader for this deliverable	ALVARION
Other contributing partners	IMDEA, BGU, NEC, SEQ, CNIT
Authors	Izhak Duanis, Jesus Alonso (ALVARION), Guillaume Vivier (SEQ)
Deliverable reviewer	Erez Biton (BGU)
Deliverable abstract	The Document is a revision of the specification of the FLAVIA architecture (modules, functionality and interfaces) for the case of 802.16 technologies. The revision is based on the 802.16 modules specification described in D3.2
Keywords	802.16, architecture, interface, services

Project co-funded by the European Commission within the Seventh Framework Programme		
DISSEMINATION LEVEL		
PU	Public	**X**
PP	Restricted to other programme participants (including the	

	Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

FLAVIA

FLexible Architecture

for Virtualizable wireless future Internet Access

Grant Agreement: FP7 - 257263

STATEMENT OF ORIGINALITY

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

Executive summary

This report describes the second specification iteration of a FLAVIA-based 802.16 architecture and interfaces. Following the work carried out in WP2 and described in D2.1.1 [1] and D2.2.1 [2], the first design was carried out by addressing the **structure** and the **behavior** of an 802.16 network framework able to support: (i) **modularity**, in terms of defining different 802.16 MAC services; (ii) **flexibility**, in terms of dynamic configurability of the 802.16 MAC; (iii) **scalability and upgradability**, in terms of multiple service instances according to scale (femto, pico, micro, macro) or standard revision. Based on such first approach, the partners designed a validation platform that was described in D3.2. Taking present the outcome of D3.2 [12] we have upgraded the definition of the MAC Services that were described in D3.1.1 [11].

After a short introduction given in Section 1, Section 2 overviews the mapping of scheduled access MAC like 802.16 and LTE over the generic FLAVIA architecture, and explains the services and interfaces needed to port the 802.16/LTE protocol architecture over FLAVIA. Section 3 introduces the specification of the service architecture for an 802.16 MAC in terms of design of the MAC service functionalities and interfaces specification. The architectural definition focuses on the core 802.16 MAC services and the interfaces that allow inter-service communication and that provide access to/from the upper layers, and to the FLAVIA Control subsystem, as defined in D2.2.1. Flow sequence diagrams are presented to illustrate interaction between MAC services. Some of the key aspects of D32 are introduced for each MAC service. Each MAC Service provides parameters that can be externally configured for a higher level of flexibility. The parameters can be configured via both the Command Line Interface and SNMP (using a SNMP browser, Alvarion's NMS or its North Bound Interface – via Web Services).

To better understand how new services can be loaded, configured and operated with the support of the FLAVIA Control subsystem, Section 4 presents a few use case examples, showing the corresponding interaction among the different modules by means of the messages and the interfaces defined in the former sections.

Section 5 summarizes the work and the results presented in the deliverable, while a short Appendix concludes the deliverable with an example describing the flow of downlink data packets during the scheduling process.

1 Introduction

FLAVIA is specifying a flexible architecture that accommodates a set of programmable and customizable MAC services.

The contribution of WP3 is to specify and prototype a flexible 802.16 MAC framework. That is, WP3 will produce two main results:

- Detailed architecture and interfaces specification of an 802.16 system in terms of modules and interfaces.
- Prototyping of basic framework modules in order to demonstrate the efficiency of the devised architecture.

In this deliverable belonging to WP3, we address the specification of the architecture of an 802.16 system extended with some exemplificative non-standard functionalities (e.g., Self Optimization Network support). We specify how the different 802.16-based MAC operations are decomposed into major services and how these services communicate.

While the present deliverable focuses on 802.16e [8], the devised design is as generic as possible to support both other existing scheduled access standards such as LTE [4] as well as future standards such as 802.16m [3] and LTE advanced [5].

More specifically, this deliverable focuses on the architectural specification of the different services, interfaces and primitives, in order to identify critical interactions between the corresponding software blocks and the required functionality to be supported in the FLAVIA architecture.

In this second iteration on this architectural specification we take into account the design of the validation platform of FLAVIA concept for scheduled system that was done in D3.2. Therefore the architecture for scheduled systems depicted in D3.1.1 is updated in this document with the particularities of D3.2.

This deliverable is structured as follows. In Section 2 we overview the high-level FLAVIA architecture for scheduled systems and describe some necessary definitions and notations used in this document. In Section 3 we provide detailed specification of the MAC services. Specifically, for each service we describe its responsibilities, primitives of the interfaces and main scenarios description (sequence diagrams). In Section 4 we provide a few examples to demonstrate how defined services are integrated within FLAVIA Control subsystem.

2 Architecture overview

2.1 FLAVIA Architecture for 802.16/LTE

The high-level FLAVIA architecture for scheduled systems is depicted in Figure 1. In particular, the figure focuses on the architecture of a base station MAC and its interfaces towards the hardware, the higher levels, and other MAC entities present in the wireless network, e.g., a mobile station, a relay station or another neighbor base station.

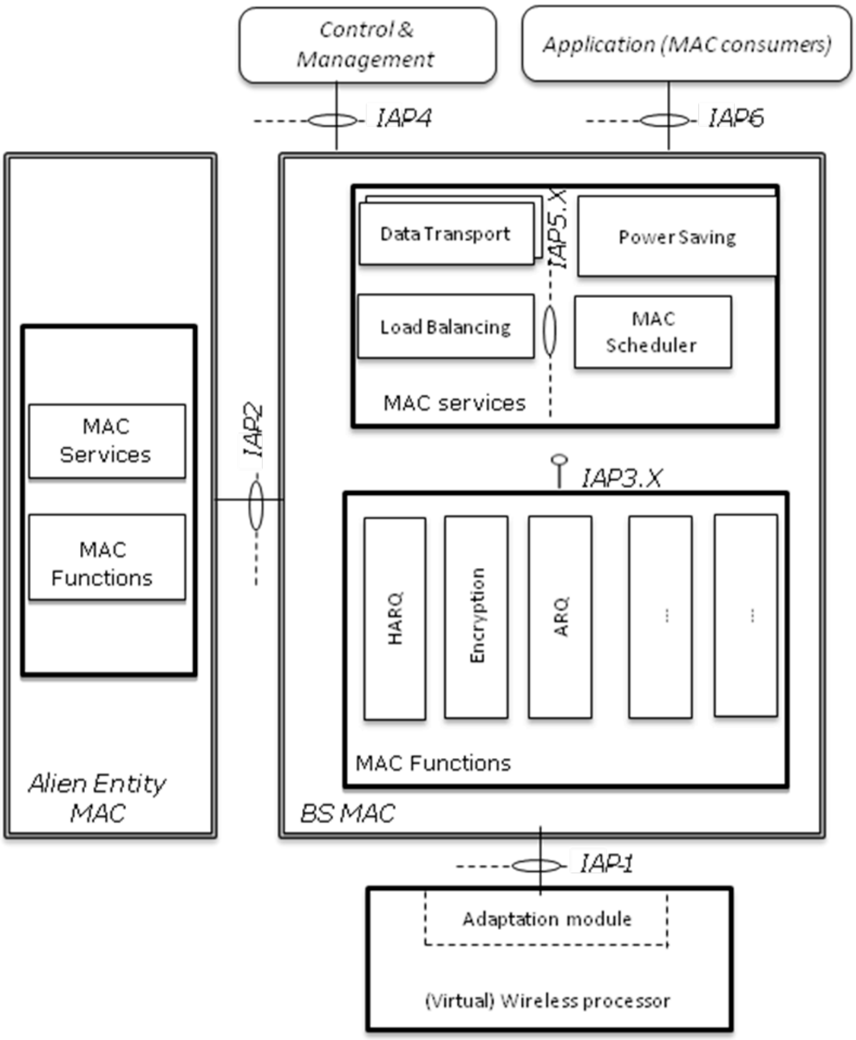


Figure 1: FLAVIA high-level view: framework architecture for scheduled MAC.

Within the base station MAC, as well as in any other MAC entity, we can identify the following main components:

- MAC services: Instantiated MAC services are located in a service container. As defined in Deliverable D2.1.1 [1] each service is a composition of functions, i.e., a service is implemented through a module containing the logic needed to access a set of MAC functions. Each service can be loaded and configured by the FLAVIA control plane. Each application (MAC consumer) is bound to one or more particular service instances through an interface.

- MAC functions: Available stateless functions are located in a function container. A function running in the function container is a logic module using the commands made available by the hardware. Functions are loaded, configured, and managed by the FLAVIA control.
- External interfaces: interface access point (IAP) 1, 2, 4, and 6, are used to interconnect the MAC to, respectively, the wireless modem (IAP1), other *alien* MACs (IAP2), FLAVIA control (IAP4), and higher levels, i.e., applications (IAP6).
- Internal interfaces: IAP 3 and 5 are used to interconnect different MAC components, either services to services or services to functions. In particular IAP3 is used by MAC services running in the service container in order to access the MAC functions needed to compose the service. IAP5 provides a set of inter-service interfaces and allows the development of modular, programmable, and flexible MAC services.

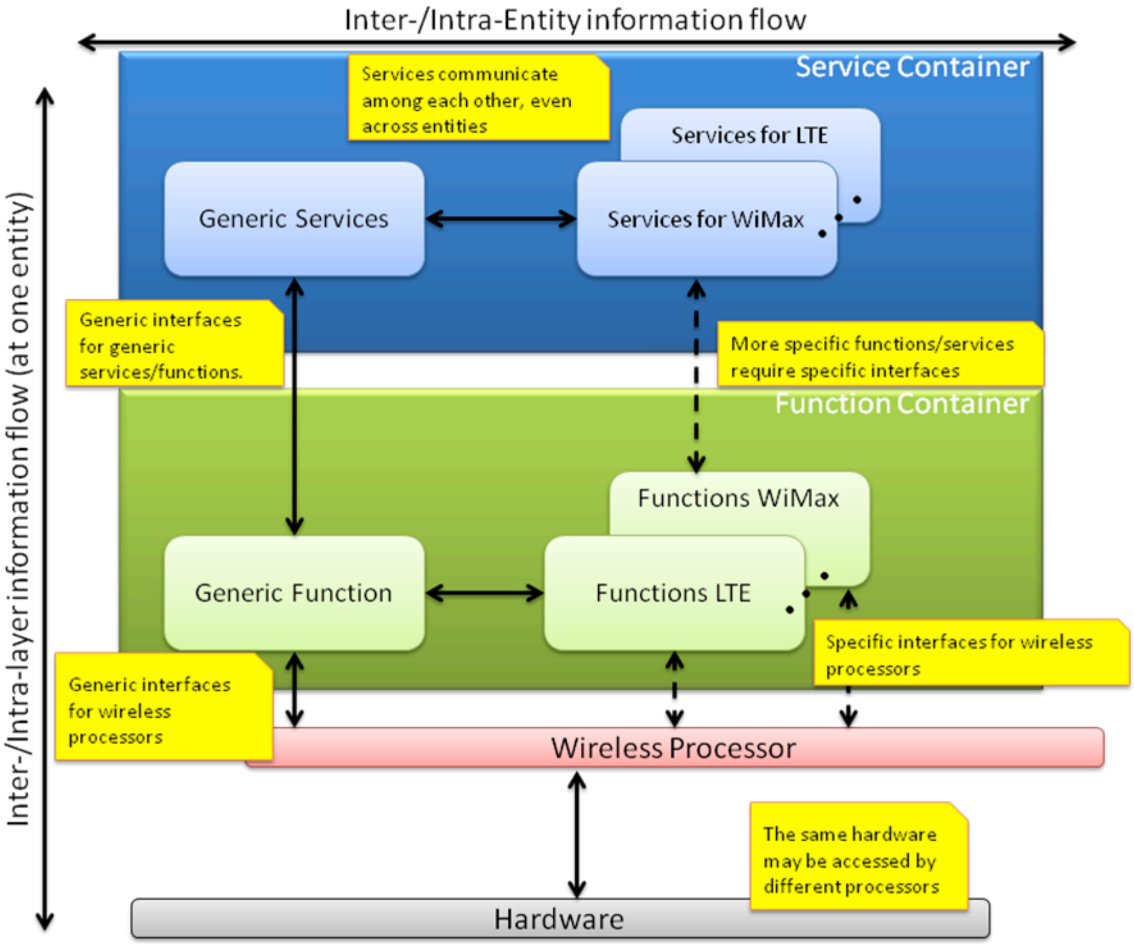


Figure 2: 802.16 MAC modular architecture and information flow description.

The modular architecture of the FLAVIA 802.16 MAC is shown in Figure 2. In the figure, we focus on the logical partition of the MAC layer into services and functions. MAC functions are closed MAC *atomic* building blocks/operations, typically stateless pieces of code, with limited interface access to services (e.g., to notify an event to a service) or to the hardware (e.g., via wireless processor). MAC services offer more complex operations with rich interfaces towards the FLAVIA control subsystem, other services (located on the same machine or on a remote device), applications (higher layers), and MAC functions.

Figure 2 shows that services can be classified into generic services and technology-specific services. Generic services are in common for all scheduled systems, while technology specific services are only needed in a subset of the possible MAC instantiations, e.g., only when a particular scheduling technology is adopted. Nonetheless, generic services have to be tailored to the technology adopted for the specific deployment, i.e., generic services can behave differently with different technologies (e.g., a scheduling service is always present in 802.16 or LTE implementations, but the scheduling logic can change from implementation to implementation and from technology to technology). Accordingly, MAC functions can be classified into generic functions and technology specific functions. Likewise, the IAP in between services and functions has to contain some standard interfaces to allow for the deployment of generic services, plus some technology specific interfaces to allow for the deployment of technology specific services through generic and technology specific functions. Note that services can communicate with other services running on alien MAC entities, i.e., on different devices, through a specific inter-MAC IAP. On the contrary, MAC functions can only communicate with services on the same MAC entity (limited access), and with the hardware processor running on top of the available hardware.

2.2 MAC services and functions

Following the generic FLAVIA architecture presented in D2.2, we divide the MAC functionality into MAC services and MAC functions.

MAC functions are "atomic" MAC operations, which are typically stateless. MAC functions can interact with:

- The FLAVIA control subsystem;
- The wireless processor(s);
- MAC services within same MAC entity (limited interface access by event notification).

MAC services are typically referred as more complex MAC operations and typically use several building blocks low level MAC functions. They have interfaces towards:

- The FLAVIA control subsystem;
- Other services (located on the same machine or on a remote device);
- Applications (higher layers);

- The wireless processor(s).

2.3 FLAVIA core MAC services

In this section we define the core services within a scheduled system. These are the services required to allow high level MAC modularity. Each service can be seen as a building block of the FLVIA architecture that can be replaced, reconfigured and updated without requiring any change in the other services. Table 1 summarizes this set of services with their corresponding acronyms and short descriptions. In Section 3.2 each of these services is specified in terms of interfaces specifications and interaction with other modules.

MAC Service	Acronym	Owner	Description
MAC Scheduler (*)	SCHE	ALVR	Managing frame construction process.
Data transport	DATA	NEC	Receiving/sending packets from/to the MAC upper layer. Packets manipulation within MAC, including multiplexing, encryption, adding necessary headers, segmentation, etc.
QoS Strategy (*)	QOSS	ALVR	Preparing a candidates list to be potentially scheduled in a specific frame, taking into account QoS requirements and time constraints.
Scheduling Strategy (*)	SCST	ALVR	Implementing a specific scheduling strategy on a set of connections on given resources.
Admission control	ADCO	BGU	Decide whether to accept or refuse a new connection in the cell.
Load balancing	LOBA	BGU	Once a new connection request arrives, the load balancing service decides on the distribution of users amongst the available cells.
Power saving	POSA	ALVR	Manage power saving intervals synchronized between BS and MS.
Inter-cell coordination & cooperation	ICIC	BGU	Inter-cell interference control and inter-cell synchronized scheduling.

Link Adaptation	LADA	ALVR	Provides functionality to adjust link parameters to target requirements.
Mobility Support	MOSU	NEC	Support for mobility-related functionalities including hand-over and location updates.
Support for SON	SSON	IMDEA	Automatic intra-cell and inter-cell network monitoring and self-optimization of MAC/PHY parameters.
Application Optimization Support	AOPS	IMDEA	Statistics collection and analysis of the run-time performance of MAC/PHY protocols. Application detection and MAC/PHY adaptation to running applications.
Measurements and Monitoring	MEAS	SEQ	Collect measurements and statistics related to low layer and MAC modules; Monitor low layer and MAC key performance indicator to trigger events when necessary.
Cell selection and tracking	CEST	SEQ	MS synchronizing, acquiring and tracking to the DL channel of BSs.

Table 1: FLAVIA core MAC Services

(*) – "QoS Scheduling" service defined in D2.1.1 was partitioned into three levels. The higher level, termed as QoS Strategy, handles the support for different QoS classes in the system and can assign different Scheduling Strategies to subsets of connections. The middle level, termed as the Scheduling Strategy, defines different scheduling schemes incorporating Link Adaptation inputs. Both QoS Strategy and Scheduling Strategy services can be designed to be technology-agnostic. The third lower level of the scheduling, termed as the MAC Scheduler, is responsible for resource allocation of a MAC frame and defines specific resources portion per connections subset and Scheduling Strategy (see Figure 3). It is tightly dependent of the technology.
The described partitioning supports different flexibility and modularity levels. For example, when a new scheduling scheme is decided to be added to the system using the FLAVIA Control, a new dedicated Scheduling Strategy service is simply added to the services container and coupled into the relevant QoS classes. Another advantage is easing the integration of innovative third-party scheduling schemes into existing commercial systems.

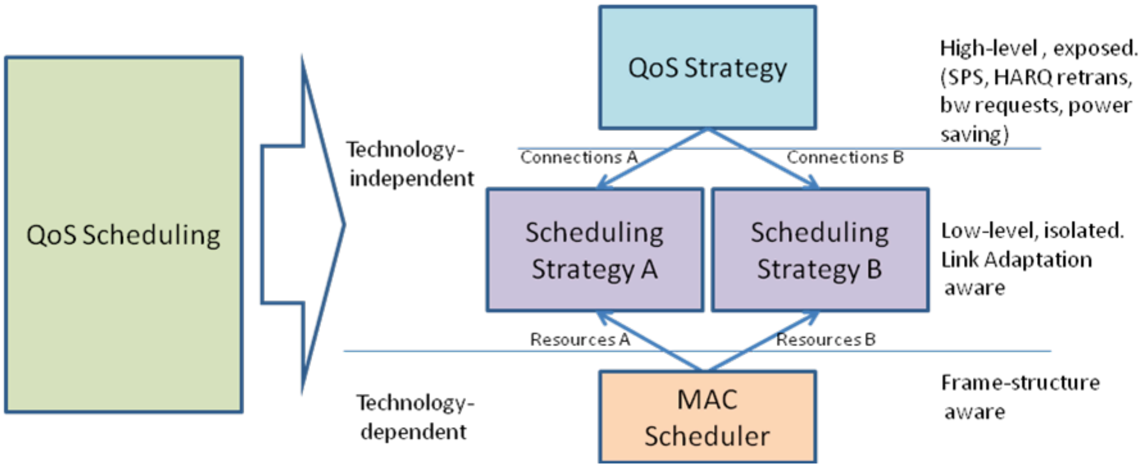


Figure 3: Scheduling services.

2.4 Virtualization

Different levels of virtualization can benefit from the specified architecture. First, the architecture allows running different MAC entities, potentially of different technologies, over shared air resources. Secondly, in the service level, different instances of services can be virtualized over shared frame resources. For example, different scheduling strategies can be performed on pre-allocated portions of a same frame. Another example is to virtualize connections of a same service flow to achieve additional level of prioritization within the same application.

2.5 Interface Access Points

This section specifies the set of interfaces that each module is exposing for a correct operation of the proposed 802.16 MAC architecture. We choose to define the following interfaces: MAC to upper layer (MAC consumer, e.g., application), MAC to lower layer (PHY), between different MAC entities (MS-BS, BS-BS, BS-relay), MAC to Control & Management (FLAVIA Control) and internal services and functions interfaces. Each of the interfaces has been defined as an Interface Access Point (IAP), which typically defines a generic access to a MAC module. The IAP definition is simply a set of primitives of different types, in which every primitive includes the set of required parameters to ensure the processing of the required operation. In the first revision we left the data structures definition required over interfaces out of the task progress. We will further discuss data structures in the next deliverables of WP3. Rather, we decided to focus on interfaces related to MAC services.

Num	MAC Service	Description
IAP1	MAC – PHY interface	Control and data signaling/transfer between MAC and PHY.
IAP2	Inter-entity interface	Interactions between services in different MAC entities (e.g., mobile station, relay station or neighbor base station).
IAP3	MAC Services-Functions interface	Functionality required by MAC services from MAC functions.
IAP4	Control & Management interface	Control & Management by FLAVIA control framework.
IAP5	Intra MAC services interface	Interactions between services within same MAC entity.
IAP6	Application (MAC consumer) interface	Communication between MAC services and upper layers.

Table 2: Interface Access Points (IAPs)

In this work we focus on specification of MAC Services interfaces. Therefore, IAP2, IAP4, IAP5 and IAP6 will be described in current document. IAP1 and IAP3 will be specified in D3.1.2.

IAP1: MAC-PHY interface

Basically it is the interface between the MAC and PHY within the same radio entity. Although a comprehensive MAC-PHY interface was defined by the FAPI LTE femto project, we may need to expand it to be fit into a Radio Access Networks (RAN) involving more capacity stations as pico and macro systems. We will elaborate on this IAP in the context of the D3.1.2 work.

IAP2: Inter-entity interface

The Inter-entity interface allows different entities to communicate (MS-BS, BS-BS, BS-relay). For example, mobile station initiated handover request would pass through this interface. The interface allows communication between both peer services (at different entities) as well as different services from different entities (e.g., MS measurement and BS mobility support). Inter-cell coordination and cooperation would also use this interface.

IAP3: MAC Services-Functions interface

This interface will gather all the functionality required by MAC services from MAC functions in order to operate. This IAP will be specified during MAC functions specification in the D3.1.2 work.

IAP 4: Control & Management interface

IAP4 is terminated at the FLAVIA control subsystem, which is responsible for system control, consistency and configuration. It is used to obtain configuration parameters and to notify the control module about significant changes in the system state. A module can change its own configuration and notify the FLAVIA Control. In case a module requires modifying other module's configurations, it should be preferably performed via FLAVIA Control, especially in case of possible consistency problems. In addition, each service/function can be loaded and configured by the FLAVIA control subsystem (Framework).

IAP 5: Intra MAC services interface

IAP5 defines interactions between services within same MAC entity. For example, the Link Adaptation service provides information on the modulation and coding scheme to other services through IAP5, which is used by, e.g., the Scheduling Strategy. The primitives offered by IAP5 are generic primitives to support all MAC functionality of various scheduled systems (WiMax, LTE).

IAP6: Application (MAC consumer) Interface

IAP6 is intended for the communication in between MAC services and upper layers. We refer to the upper layer as to the *applications* or the *MAC* *consumers*. Data messages are conveyed to and from the upper layers through IAP6. Packets exchanged by control protocols running on top of the MAC are also using IAP6. Conversely, FLAVIA control messages, which are internal to the MAC, use a different interface flow to or from the MAC services. The primitives offered by IAP6 are generic primitives for the dialogue between a generic MAC and an upper layer; IAP6 basically moves packets from and to the logical link control layer, and protocol control messages or application commands (operations to be performed, and that are requested by an application running in the user space), to and from the upper layers.

2.6 Name Conventions

2.6.1 MAC Services Interfaces

Multiple Interface Access Points (IAPs) are defined for each service:

IAP4 – primitives exposed for FLAVIA Control & Management
IAP2 – primitives exposed for alien MAC entity (e.g. other BS or MS)
IAP5 – primitives exposed for other services within same MAC entity
IAP6 – primitives exposed for MAC consumer (upper layers)

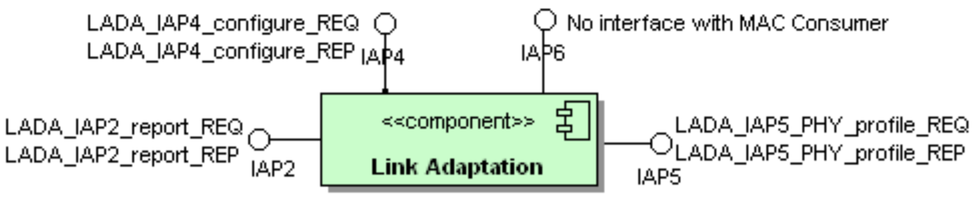


Figure 4: An example for MAC Service with IAPs

2.6.2 Name convention for interfaces primitives

In this document we use the following name convention for interface primitives:

<Acronym>_<IAPx>_< primitive name>_<primitive type>

where:

- Acronym is one of the acronyms defined for the MAC services in Table 1 or for the external entities as defined in Table 3.
- x is the IAP number defined in Table 2.
- Primitive type is REQ/REP/IND/SUB (see Primitives Types)

Entity	Acronym	Description
Control & Management	CTRL	FLAVIA Control
Application or MAC Consumers	APPL	Upper layer
Wireless Processor	PHYL	Physical Layer

Table 3: External entities acronyms.

2.6.3 Primitive Types

Here we define different types of primitives.

Request (**REQ**) – a module is requested to perform an operation.
Reply (**REP**) - a module is replying to a previously requested operation. For example, some BS service requests for specific measurements from MS. MS starts reporting these measurements via REP. Majority of the REQ primitives has a matching REP primitive. Therefore, we usually combine it in the interfaces specification, as in the given example:
MEAS_IAP2_get_meas_REQ/REP – actually represents two primitives MEAS_IAP2_get_meas_REQ and MEAS_IAP2_get_meas_REP.

Subscription (**SUB**) – subscription to the indication of an event class in a system module (service or control).
Indication (**IND**) – indication of an event from a module.
Modules can register to a specific event (usually during system initialization) by means of the SUB primitive, which will enable event notification as soon as the specific event occurs. We use the IND primitive to convey the event notification to subscribed modules. Figure 5 shows an example for an

indication primitive. In the figure, the Admission Control service notifies QoS Strategy and Data Transport services about a new connection creation. Each IND primitive has matching SUB primitive. Therefore, we usually combine it in the interfaces specification, as in the given example:
ADCO_IAP5_connection_conf_IND/SUB – actually represents two primitives ADCO_IAP5_connection_conf_IND and ADCO_IAP5_connection_conf_SUB.

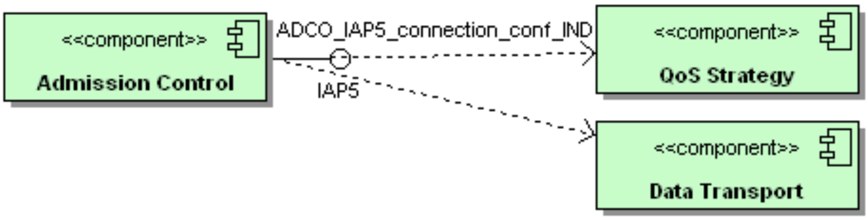


Figure 5: Example for an indication primitive.

3 MAC Service Architecture

This section introduces the specification of the service architecture for an 802.16 MAC in terms of design of the MAC service functionalities and interfaces specification. Following the MAC services defined in T2.1 we identified the core services within a scheduled system required to allow high level MAC modularity. The partitioning to the specific service list aims to converge into the MAC building blocks as the basic replaceable and configurable entities.

Starting from the Scheduler MAC functionality, three services are specified: MAC Scheduler, QoS Strategy and Scheduling Strategy. The MAC Scheduler manages the frame construction process by getting a candidates list from QoS Strategy and applying different Scheduling Strategies on candidate subsets and frame resources portions. The Link Adaptation service provides user's link quality estimations and Power and Interference Control mechanisms. The Data Transport service is an access point for receiving/sending DL/UL packets from/to the MAC upper layer. It is responsible for packets manipulation within MAC, including multiplexing, encryption, adding necessary headers, segmentation, etc. The Power Saving service manages the mobile stations power saving modes (e.g. idle/sleep modes). Load Balancing and Admission Control services are responsible to balance the load between neighboring BSs and preserve required QoS for the connected users. The Inter-cell Coordination and Cooperation service enables inter-cell interference management and inter-cell synchronized scheduling. The Measurements service collects MAC/PHY statistics/measurements and enables extendable BS-MS interface. As an example, currently there is no support in the standard for the MS to report its mobility level to the BS. However, reporting such measurement can help the BS to take decisions regarding different aspects such as hand over, most adequate scheduling strategy, etc. The SON support service is responsible for dynamic MAC/PHY operational modes in order to improve the network performance, e.g., by adopting interference mitigation techniques (e.g. FFR scheme). The Application Optimization service aims to optimize specific application protocol performance by dedicated MAC operations.

The primary focus of FLAVIA is on the base station or access point. However, the flexible architecture is generic enough to be applied both at base station and at terminal station with minor adjustments.

3.1 Services Interactions

Figure 6 illustrates main interactions between MAC services identified in this work. Each arrow corresponds to data exchange between services, i.e. one service feeds another with specific data/information (by arrow's direction). The pink-colored services are mainly involved in data path, blue-colored are optimization services and orange-colored services relate to inter-cell processes.

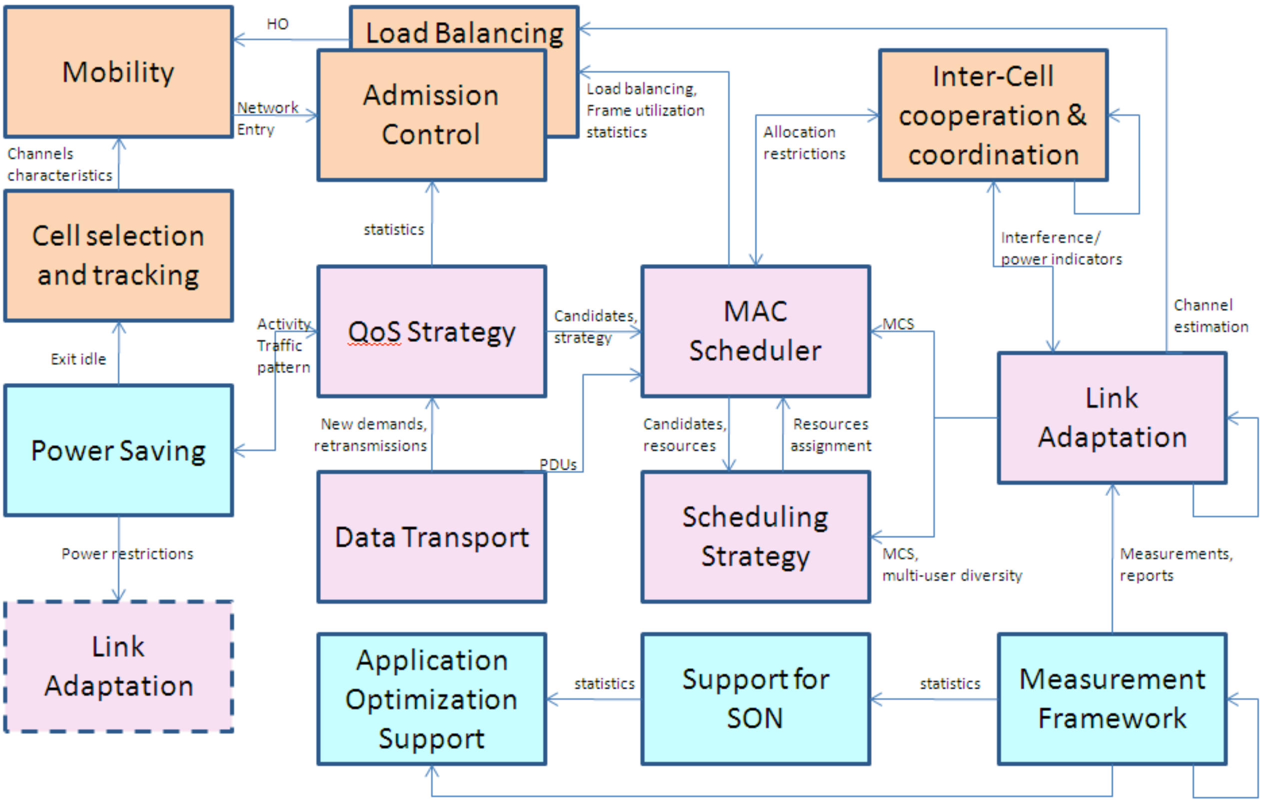


Figure 6: Main interactions between MAC Services. The pink services are mainly involved in data path, blue are optimization services and orange services relate to inter-cell processes.

Data Transport receives SDUs from upper layer and feeds QoS Strategy with new demands. QoS Strategy prepares candidates for scheduling in a specific frame. It may also assign specific scheduling strategy per group of candidates. MAC Scheduler is actually frame building manager. It receives candidates for scheduling, decides about frame resources per group of candidates and requests a Scheduling Strategy to schedule the given candidates on the given resources. Link Adaptation provides modulation and coding scheme (MCS) and multi-user diversity information for performing different scheduling metrics (for example, frequency-selective Proportional Fairness with co-MIMO). After resources assignment, Data Transport builds MAC PDUs. Power Saving service interacts with QoS Strategy. It can define sleep cycles per MS/connection and can be updated by QoS Strategy about changes in traffic pattern. MS performs Cell Selection and Tracking as a part of network entry or hand-over processes. Network entry and connections creation processes are controlled by Admission Control Service. Both Admission Control and Load Balancing use statistics about frame resources utilization, QoS requirements satisfaction and channel estimation for their decisions. Inter-cell Coordination and Cooperation service provides information about the neighbour cells and their users, which allows inter-cell interference management and inter-cell synchronized scheduling. Measurements and Monitoring service provides MAC/PHY measurements to other services (located on the same machine or on a remote device). SON and Application Optimization Support services should be able to configure MAC/PHY parameters via FLAVIA control.

3.2 MAC Services Specification

3.2.1 MAC Scheduler (SCHE)

In the validation platform the MAC scheduler will be provide by Alvarion's BS Frame builder module that is tightly dependent on WiMAX technology.

General Description:

The MAC Scheduler provides the construction of MAC frames by using the resource assignments of one or more arbitrary scheduling-strategies as well as the pre-processing of the QoS-Strategy. Using the output of these services, the MAC scheduler creates the final frame structure based on a frame template (depending on UL/DL ratio, FFR, …) including resource assignment map, broadcast and multicast regions, HARQ regions, feedback region, and preambles. Therefore, the MAC scheduler represents the "main-function" of the user-to-resource assignment process.

Responsibilities:

1. Building resource assignment map including broadcast and multicast zone, preambles, feedback zone, HARQ resources
2. Managing interaction with QoS scheduling
3. Managing interaction with Scheduling Strategy
4. Managing interaction with data-transport by filling resource assignments with actual user data
5. Management of resource assignment types, i.e. distributed and localized resource units
6. Logical and transport channel management

7. Map resources management
8. Decision in which zone/region each candidate should be scheduled (FFR)
9. Managing time transmitting interval

Service interface primitives:

IAP	Primitive name	Description
IAP4	SCHE_IAP4_configure_REQ/REP	Allows the FLAVIA control to configure the service. REP - to acknowledge FLAVIA Control configuration request.
IAP5	SCHE_IAP5_construct_frame_REQ/REP	Triggers the process of creating a frame according to the current setup. This primitive might be triggered internally by MAC Scheduler or by other MAC module which manages timing constraints of frame building.
IAP5	SCHE_IAP5_statistics_REQ/REP	Provides statistics about frame utilization per different regions (reuse1, reuse3, dl/ul map and etc.)
IAP5	SCHE_IAP5_set_sched_constraints_REQ/REP	Imposing scheduling constraints for scheduling specific users on specific frame resources (time and frequency domains). Example: inter-cell synchronised scheduling (via ICIC).
IAP5	SCHE_IAP5_set_power_interf__budget_REQ/REP	Enables setting power/interference budget per resources regions.
IAP5	SCHE_IAP5_set_neighbours_interf_REQ/REP	Enables setting regions with different levels of interference from neighbouring BSs.
IAP5	SCHE_IAP5_get_planned_power_interf_pattern_REQ/REP	Planning of different levels of power/ interference per frame resources regions. For example, can be based on quantities of cell-edge users. To be published to neighbouring BSs (by ICIC).

Service indication primitives:

IAP	Primitive name	Description
IAP4	SCHE_IAP4_update_config_IND/SUB	Suggest to the FLAVIA control a configuration modification.
IAP5	SCHE_IAP5_received_frame_IND/SUB	Notifies attached services that UL frame has been received (e.g. the Measurements service may then use the received pilots to estimate the channel).
IAP5	SCHE_IAP5_scheduled_feedback_IND/SUB	Feedback from current frame scheduling (to take into account in the next frames): 1. Allocation size per connection, including transmitted packets/allocated bytes; 2. Filters such as: a. Assignments of users to different groups (e.g. by different FFR regions); b. quantities of candidates to prepare, per group QoS Strategy and Scheduling Strategy should be notified.

Required primitives from other services:

IAP	Primitive name	Description
IAP5	QOSS_IAP5_candidates_REQ/REP	Gets candidates to be potentially scheduled in current frame
IAP5	LADA_IAP5_estimated_MCS_REQ/REP	Estimate the expected MCS for a user's connection (for FFR decision).
IAP5	SCST_IAP5_schedule_REQ/REP	For each group of candidates a scheduling strategy is assigned. This specific scheduler then receives a list of candidates, QoS constraints, and available frame resources. REP returns the users assignments to the frame resources.
IAP5	DATA_IAP5_fill_assignments_REQ/REP	Fills the final resource assignments with actual user data.

MAC Functions:

1. Logical and transport channel management

This function provides a list of transport channels available in this frame, e.g. depending on UL/DL configuration, FFR configuration, bandwidth, CP configuration and etc.

2. MAP Resource Allocator

Diagrams:

The MAC Scheduler service is involved in DL Data Path flow, which is explained and illustrated in Section 3.3.1 . In addition, Section 3.3.3 presents a detailed sequence diagram of "Scheduling frame" use case.

3.2.2 Data Transport (DATA)

In the validation platform Alvarion's available Data transport called High Level MAC will be used.

General Description:

The data transport service provides forwarding and processing of user or control data before sending to the physical layer. Data can be transport with protocols to increase transport reliability, like ARQ and/or HARQ. Data can be encrypted. The Data transport service provides an interface towards higher layers which expects SDUs from a *service flow*. Several service flows can be multiplexed. The actual functionality of this service is illustrated in Figure 7.

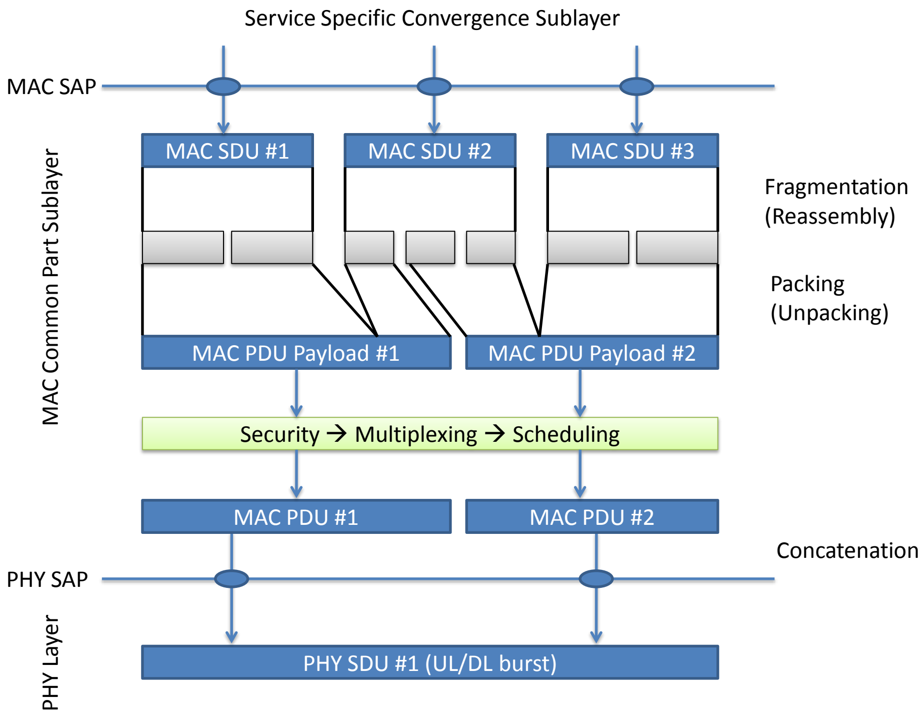


Figure 7: Illustration of Data Transport

<u>Responsibilities:</u>

1) Interface to MAC Consumer in order to receive and to deliver MAC SDUs
2) Transport of MAC messages created inside MAC
3) Encryption/Security
4) Fragmentation and packing of MAC SDUs
5) ARQ and HARQ management
6) Manipulating/Parsing and forwarding of UL received packets
7) Multiplexing/demultiplexing
8) Data queue management and congestion avoidance
    a. Traffic Policing (discard packets above max rate)
    b. Random Early Discard (RED) [9]
    c. Ageing – drop old packets
9) Assignment of traffic classes based on SON recommendations

Service interface primitives:

IAP	Primitive name	Description
IAP4	SCHE_IAP4_configure_REQ/REP	Allows the FLAVIA control to configure the service. REP - to acknowledge FLAVIA Control configuration request.
IAP6	DATA_IAP6_add_sdu_REQ/REP	Adds SDU (to be sent) to the data buffer of user's connection. Input: sdu
IAP5	DATA_IAP5_add_mac_msg_REQ/REP	Adds MAC message (to be sent) to the data buffer of user's connection. Input: MAC message, [frame num to be sent].
IAP5	DATA_IAP5_statistics_REQ/REP	Returns the current buffer statistics (fill level, delays and etc.) of a user's connection (DL specific). Statistics about traffic activity (e.g. packets time arrival, bandwidth requests time arrival).
IAP5	DATA_IAP5_fill_resource_assignments_REQ/REP	Fills the given resource assignments with data from users' connections. It also invokes internal procedures to fragment SDUs, pack payload, apply CRC/ARQ, encrypt, and multiplex PDUs. Returns the final list of PDUs.
IAP5	DATA_IAP5_register_class_REQ	Request to update the class-filtering rules (from AOPS), i.e., ask the data transport system to manage a new class or update the rules for an existing class.
IAP5	DATA_IAP5_register_class_REP	Acknowledge the class-filtering request.
IAP5	DATA_IAP5_deregister_class_REQ	Request the data transport system to dismiss an existing traffic class (from AOPS).
IAP5	DATA_IAP5_deregister_class_REP	Acknowledge the change in the class-filtering rules.
IAP5	DATA_IAP4_transport_params_REQ/REP	Fetch the currently in use parameters for the Data Transport service for a specific connection

Service indication primitives:

IAP	Primitive name	Description
IAP4	DATA_IAP4_update_config_IND /SUB	Suggest to the FLAVIA control a configuration modification.
IAP5	DATA_IAP5_received_data_IND /SUB	Notifies attached services about successfully received user data. Data Transport disassembles UL PDUs to SDUs, parse it and notify registered modules (e.g. QoS Strategy should be updated about bandwidth requests from MS).
IAP5	DATA_IAP5_harq_feedback_IND /SUB	Notify registered modules about HARQ ack/nack.

Required primitives from other services/entities:

IAP	Primitive name	Description
IAP6	APPL_IAP6_send_packet_REQ	Forwards received UL packets from MAC to the MAC Consumer.

MAC functions:

1. SDUs classifier to different connections
2. Encryption/Security
3. Fragmentation and packing of MAC SDUs
4. ARQ
5. HARQ
6. Multiplexing/demultiplexing
7. Traffic Policing (Token/Leaky buckets)
8. Random Early Discard (RED) [9]
9. Ageing – drop old packets

Primitive name	Description
FUNC_fragment_SDU / FUNC_build_SDU	Fragments buffered SDUs before they are assigned to PDUs (and its inverse function)
FUNC_pack_payload / FUNC_unpack_payload	Packs payload data for PDUs after SDUs were fragmented (and its inverse function)
FUNC_apply_CRC / FUNC_check_CRC	Applies CRC to packed payload data (and its inverse function)

FUNC_apply_ARQ / FUNC_update_ARQ	Applies ARQ header and updates ARQ status before transmitting a PDU. Its inverse function also updates the ARQ status depending on the success of decoding. Both functions together implement the ARQ process.
FUNC_encrypt_payload / FUNC_decrypt_payload	Encrypt the payload before transmission and decrypt before reception.
FUNC_multiplex / FUNC_demultiplex	Multiplex multiple streams/connections into PDUs (and its inverse function).

Diagrams:

The Data Transport service is involved in DL Data Path flow, which is explained and illustrated in Section 3.3.1 . In addition, Sections 3.3.2 and 3.3.3 present detailed sequence diagrams where Data Transport receives DL packets from MAC Consumer and manipulates packets when a frame is constructed.

3.2.3 QoS Strategy (QOSS)

QoS strategy as described in the following is part of the validation platform that will be provided.

General description:

QoS strategy mainly takes responsibility to prepare a candidates list to be potentially scheduled in a specific frame, taking into account QoS requirements and time constraints (e.g. sleep windows, semi-persistent scheduling, HARQ time constraints and etc).

The candidates are prioritized by QoS classes, defined by QoS attributes, such as QoS type, guaranteed rate, latency requirement and etc.

The idea of QoS strategy separation from the Scheduling Strategy is to allow different scheduling strategies to be used with the same QoS strategy.

The way the QoS strategy will be responsible for the following activities:

QoS strategy module sorts the incoming packets towards the DL direction (associated with CID – Connection Id) into different queues according to their

QoS attributes including the QoS type, CIR (Committed Data Rate), priorities and MIR (the uncommitted data rate up to the Maximum Information Rate).

QoS strategy module sorts the bandwidth requests belonging to outgoing packets in UL direction (associated with CID) into different queues, according to their QoS attributes, i.e., the QoS type, CIR, priorities and MIR (uncommitted data rate).

The QoS strategy is responsible for data traffic shaping when the quota exceeds the uncommitted data rate. The shaping is done by exceeding traffic delaying. The transport layer will be responsible to drop the exceeding data on time to prevent air-link occupation by old traffic. The recommended drop mechanism can work once per 1sec.

The QoS strategy mainly takes responsibility to prepare the list of candidates to be potentially scheduled in a specific frame, according to QoS requirements and time constraints (e.g., sleep windows, semi-persistent scheduling, HARQ[1] time constraints and etc.). The candidates are prioritized by QoS classes, defined by QoS attributes, such as QoS type, guaranteed rate, latency requirement and etc. An example for QoS classes and priorities is represented in Table 4. The highest priority class is "voice retransmissions" including connections from UGS/ertPS WiMax service types (see **Errore. L'origine riferimento non è stata trovata.**) with packets that need to be retransmitted by HARQ mechanism; following by "voice" connections with packets that will be transmitted first time. The next classes include real-time connections, with additional level of prioritization by checking if under/over guaranteed rate (Minimum Reserved Traffic Rate). In addition, QoS Strategy shapes the traffic based on the predefined per connection minimum and maximum rates (Minimum Reserved Traffic Rate and Maximum Sustained Traffic Rate).

Service Type	Abbrev.	Description
Unsolicited Grant Service	UGS	Real-time data streams comprising fixed-size data packets issued at periodic intervals
Extended Real-time Polling Service	ertPS	Real-time service flows that generate variable-sized data packets on a periodic basis

[1] Hybrid Automatic Repeat Request or 'Hybrid ARQ',

Real-time Polling Service	rtPS	Real-time data streams comprising variable-sized data packets that are issued at periodic intervals
Non-real-time Polling Service	nrtPS	Delay-tolerant data streams comprising variable-sized data packets for which a minimum data rate is required
Best Effort	BE	Data streams for which no minimum service level is required and therefore may be handled on a space-available basis

Table 4: IEEE 802.16e-2005 QoS classes

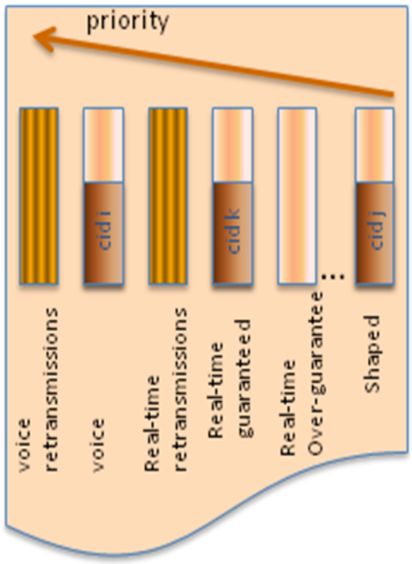


Figure 8: Example for QoS classes arrangement by QoS Strategy

For each QoS type/class different scheduling strategies can be applied (see ***Figure 10***). For example, real-time connections and packets may be scheduled by Earliest Deadline First (EDF) algorithm, which is sensitive to delay requirements. Meanwhile, non-real time connections can be scheduled by opportunistic schemes, such as Proportional Fairness.

As described above, the QoS Strategy will prepare a candidates list to be potentially scheduled in a specific frame according to pending demands (DL buffered data, UL bandwidth requests and retransmissions) and QoS rules. Such candidate list will be sent to the MAC Scheduler (see *Figure 9*). QoS

Strategy may categorize candidates to different groups, and determine a specific scheduling strategy per group. In addition, MAC Scheduler can define groups by resources constraints (e.g., users for scheduling in Reuse 1 or in Reuse 3 **Errore. L'origine riferimento non è stata trovata.**). Note that QoS Strategy is not aware of resources constraints. MAC Scheduler can provide filters about quantities of candidates per group to be prepared in the next frames.

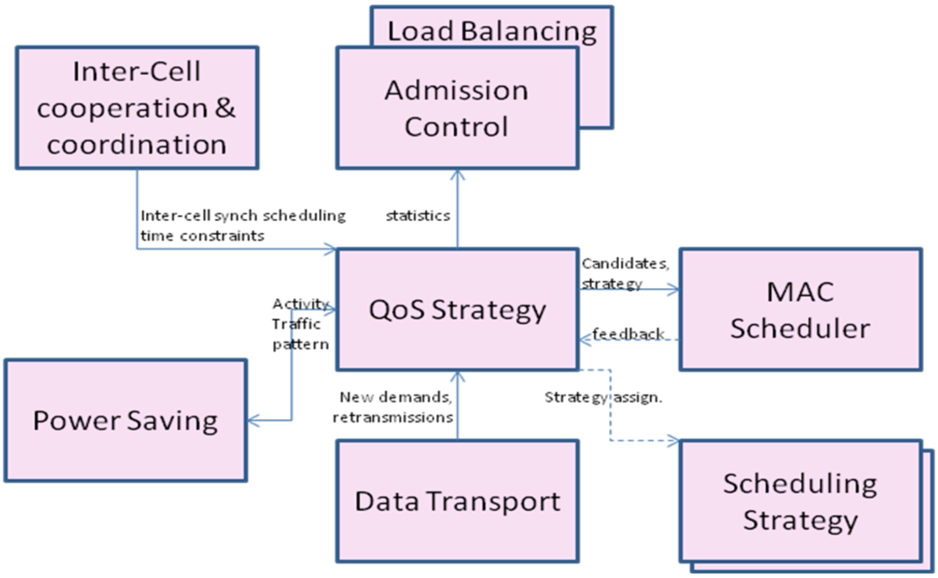


Figure 9: Main interactions between QoS Strategy and other services

The QoS Strategy might be requested to prepare candidates list on-demand (e.g., by the MAC Scheduler service); or in background (triggered internally or by external service which manages time constraints for frame construction).

Responsibilities

These are the module's responsibilities:

1. Bandwidth requests manager (DL and UL, control and data messages)
2. QoS attributes per service flow
3. Prioritization between different QoS classes (QoS type, traffic priority, Minimum Reserved Traffic Rate/Maximum Sustained Traffic Rate, HARQ retransmissions, etc)
4. Traffic shaping

5. Prioritizing HARQ retransmissions
6. Mapping of scheduling strategy to groups of users
7. Assignment QoS strategy metric (for combining in next stage)
8. Semi-persistent scheduling (time-domain)
9. Synchronization with the Power Saving service
10. Handling feedback from MAC Scheduler (scheduled connections, assignment to groups, filters about candidates list)

<u>MAC functions</u>

In order to cope with the aforementioned responsibilities, the module will provide the following MAC functions

1. Traffic shaping (token/leaky buckets)
2. Assignment of connection/packets to a specific QoS class/group
3. Assignment of a scheduling strategy to a specific QoS class/group

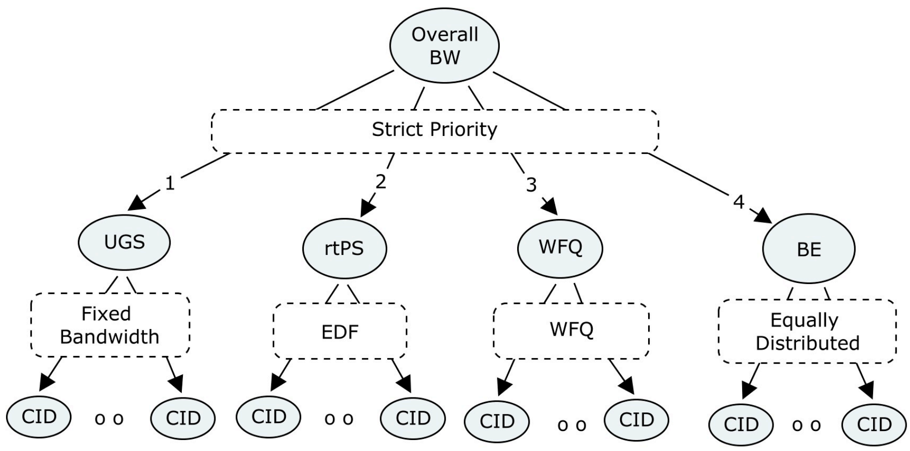


Figure 10: Strict priority queues management per QoS class/group

The QoS Strategy will be responsible for strict priority queues arrangement (*Figure 10*) considering the QoS types committed data rates, priorities and uncommitted data rates means MIR. The strict priority queues are arranged for UL and DL as describe in ***Table 5***:

Uncommitted (MIR-CIR)	Priority 0
	Priority 1
	Priority 2
	Priority 3
	Priority 4
	Priority 5
	Priority 6
	Priority 7
nRT Committed (CIR)	Priority 0
	Priority 1
	Priority 2
	Priority 3
	Priority 4
	Priority 5
	Priority 6
	Priority 7
RT Committed (CIR)	Priority 0
	Priority 1
	Priority 2
	Priority 3
	Priority 4
	Priority 5
	Priority 6
	Priority 7
eRT Committed (CIR)	Priority 0
	Priority 1
	Priority 2
	Priority 3
	Priority 4
	Priority 5
	Priority 6
	Priority 7
UGS Committed (CIR)	Priority 0
	Priority 1
	Priority 2
	Priority 3
	Priority 4
	Priority 5
	Priority 6
	Priority 7

Table 5: Queues arrangement per priorities, QoS types and services

The interface between QoS Strategy and Scheduling Strategy shall use the following TLVs (Type Length Value elements).

- For DL committed queues: CID, CIR, Priority, total arrived data length
- For DL uncommitted queues: CID, MIR-CIR, Priority, total arrived data length
- For UL committed queues: CID, CIR, Priority, total arrived BW requests
- For UL uncommitted queues: CID, MIR-CIR, Priority, total arrived BW requests

Service Interface primitives

For the communications with other modules the QoS Strategy module will offer the service interface primitives described in **Table 6**.

IAP	Primitive name	Description
IAP4	QOSS_IAP4_UL_configuration_REQ/REP	int32 uplink_sfid; int8 uplink_QoS_parameter_type; int32 uplink_maximum_sustained_traffic_rate;(MIR) int32 uplink_minimum_reserved_traffic_rate; (CIR) int8 uplink_traffic_priority; int32 uplink_maximum_latency; int32 uplink_tolerated_jitter; int16 uplink_unsolicited_grant_interval; int8 uplink_convergence_sublayer_type; int8 uplink_classifier_type; int16 uplink_classifier_value;
IAP4	QOSS_IAP4_DL_configuration_REQ/REP	int32 downlink_sfid; int16 downlink_flow_number; int8 downlink_QoS_parameter_type; int32 downlink_maximum_sustained_traffic_rate; (MIR) int32 downlink_minimum_reserved_traffic_rate; (CIR) int8 downlink_traffic_priority; int32 downlink_maximum_latency; int32 downlink_tolerated_jitter; int8 downlink_convergence_sublayer_type; int8 downlink_classifier_type; int16 downlink_classifier_value;
IAP6	QOSS_IAP6_UL_connection_creation_REQ/REP	int32 uplink_sfid; int16 uplink_cid; int8 uplink_QoS_parameter_type; int32 uplink_maximum_sustained_traffic_rate;(MIR) int32 uplink_minimum_reserved_traffic_rate; (CIR) int8 uplink_traffic_priority; int32 uplink_maximum_latency; int32 uplink_tolerated_jitter;

		int16 uplink_unsolicited_grant_interval; int8 uplink_classifier_type; int16 uplink_classifier_value;
IAP6	QOSS_IAP6_DL_connnection_creation_REQ/REP	int32 downlink_sfid; int16 downlink_cid; int8 downlink_QoS_parameter_type; int32 downlink_maximum_sustained_traffic_rate; (MIR) int32 downlink_minimum_reserved_traffic_rate; (CIR) int8 downlink_traffic_priority; int32 downlink_maximum_latency; int32 downlink_tolerated_jitter; int8 downlink_grant_scheduling_type; int8 downlink_classifier_type; int16 downlink_classifier_value;
IAP5	QOSS_IAP5_add_demand_REQ	New dl/ul bandwidth request for specific data or control connection. Input: connection process, packet size, timestamp and optionally frame number it should be transmitted/allocated. <u>Interface parameters list:</u> int cid, int xi_no_of_bytes
IAP5	QOSS_IAP5_add_retrans_REQ	Allocation demand for DL/UL retransmission for specific MS and HARQ channel. <u>Interface parameters list:</u> int msId, int acid, enum direction, int bytes, enum SLA.
IAP5	QOSS_IAP5_candidates_REQ/REP	If candidates were prepared in background and meanwhile some urgent demands were received (e.g. retransmissions), candidates list should be refreshed. Input: frame num REP: sorted candidates, scheduling strategy per group of candidates, QoS information/metric per candidate <u>Interface parameters list:</u> Returns quota_struct: Type={retransmission, new trans} quotaBytes cid actuallyAllocatedBytes, QoS_info_struct {QoS_parameter_type, maximum_sustained_traffic_rate, minimum_reserved_traffic_rate, traffic_priority, maximum_latency, tolerated_jitter }, SchedStrategy {scheduling_type, abuse_protection_level }

Table 6: Service interface primitives for QoS Strategy module

3.2.3.1 Update about the implementation of the architecture

In this reviewed version of the QoSS Service we have selected the design proposed in D32. This upgraded QoSS Service together with the Scheduling Strategy Service will provide the core functionality for the Dynamic Scheduling Strategy application scenario, one of the demonstrators that will validate FLAVIA's architecture for scheduled-based systems.

For a given Service Flow Id and a Connection Id the following parameters can be externally modified.

UL/DL	Parameter name	Type
UL	uplink_QoS_parameter_type	int8
	uplink_maximum_sustained_traffic_rate (MIR)	int32
	uplink_minimum_reserved_traffic_rate (CIR)	int32
	uplink_traffic_priority	int8
	uplink_maximum_latency	int32
	uplink_tolerated_jitter	int32
	uplink_unsolicited_grant_interval	int16
	uplink_convergence_sublayer_type;	int8
	uplink_classifier_type;	int8
	uplink_classifier_value;	int16
DL	downlink_QoS_parameter_type	int8
	downlink_maximum_sustained_traffic_rate (MIR)	int32
	downlink_minimum_reserved_traffic_rate (CIR)	int32
	downlink_traffic_priority	int8
	downlink_maximum_latency	int32
	downlink_tolerated_jitter	int32
	downlink_convergence_sublayer_type	int8
	downlink_classifier_type	int8
	downlink_classifier_value	int16

Table 7: Configurable parameters at the QoSS

3.2.4 Scheduling Strategy (SCST)

Scheduling Strategy defined in the following is part of the validation platform that will be provided

<u>General description:</u>

This module strategy implements a specific scheduling scheme on a set of connections on given resources.

A scheduling strategy may be characterized in terms of:

- Resources or Bytes Fairness allocation;
- Opportunistic;
- Delay-sensitive.

Various scheduling schemes can be applied on different groups of candidates (as described in QoS Strategy section). These schemes will be implemented as different instances of Scheduling Strategy service.

For the shake of clarity,**Table 8** describes some abbreviations and terminology used in this module's description.

Term	**Description**
BWR	Bandwidth request
QoS type	Scheduling type (UGS/eRT/RT/nRT/BE)
Traffic Priority	(0-7)
MIR (bits/sec)	Maximum Sustained Traffic Rate
CIR (bits/sec)	Minimum Reserved Traffic Rate
Jitter (ms)	Tolerated Jitter
Latency (ms)	Maximum Latency
UGI (ms)	Unsolicited Grant Interval
UPI (ms)	Unsolicited Polling Interval
CT (ms)	Time Base
GrantQuota (bytes)	UL allocation (packet size) for eRT/UGS connections

Table 8: Abbreviations & terminology in Squeduling Strategy

Figure 11 illustrates main interactions between Scheduling Strategy and other services. The QoS strategy service provides candidates for scheduling and QoS constraints information such as packets deadlines, bytes quotas till minimum/maximum rates and etc. MAC Scheduler defines resources for scheduling and receives back scheduled candidates, assigned to specific resources. Note that Scheduling Strategy is working with a logical map of resource units; therefore it is agnostic to frame structure. The Link Adaptation service calculates and provides modulation and coding scheme (MCS) per connection and frequency. In addition, it calculates and advises transmission diversity mode and users group with low channels correlation for collaborative MIMO.

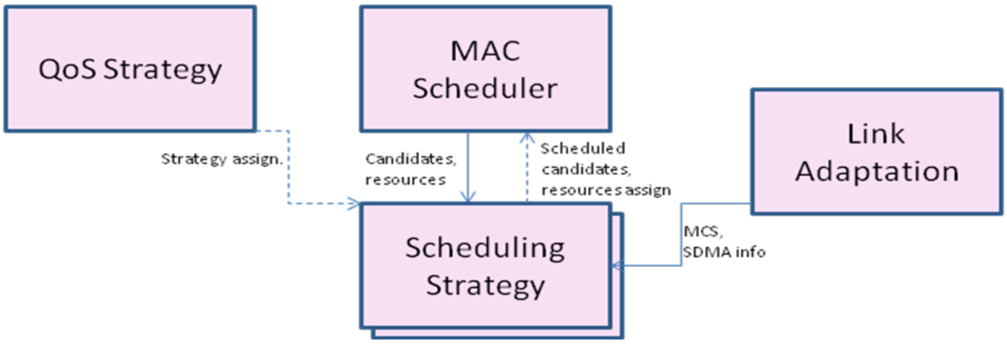


Figure 11: Main interactions between Scheduling Strategy and other services

Typically, scheduling strategy is implemented via sorting connections by metric (assigned to each connection) calculated based on already scheduled data bytes/resources, and QoS Strategy and Link Adaptation inputs.

<u>eRT/UGS Connections treatment</u>

The BS provides periodic UL allocations that may be used for requesting the bandwidth as well as for data transfer. These UL allocations should be provided each UGI (with possible jitter deviation, see *Figure 12*). The UL allocation size is GrantQuota = MIR/8/1000*UGI.

Jitter is a possible deviation from the given UGI.

Maximum Latency can be guaranteed by dropping old-age packets.

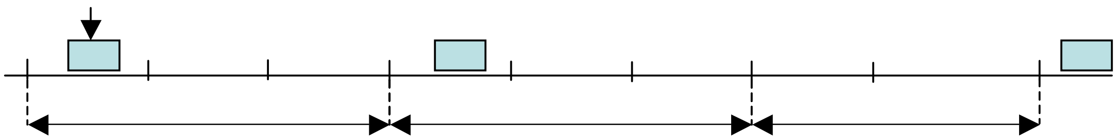


Figure 12: UL allocations

Possible Voice Codecs are introduced in Table 9

Codec UGI	Voice payload	IP Packet Grant Quota	MIR/1000
G711 20ms	160	200	80
G711 30ms	240	280	73.92
G729 20ms	20	60	24
G729 30ms	30	70	18.6

Table 9: Possible Voice Codecs

<u>RT/nRT Connections treatment</u>

Let’s denote the amount of data arrived to the transmitter’s MAC, during time interval T = Time Base. Then the BS is supposed, during each time interval of the length (Time Base), to allocate to the connection resources sufficient for transferring an amount of data according to the value of at least min {S, CIR * T}. Any SDU should be delivered within a time interval D = Maximum Latency. In the case when the amount of data submitted to the transmitter’s MAC exceeds CIR* T, delivery of each specific SDU is not guaranteed.

Time Base is a resolution of commitment for a specific traffic rate.

For example, for CIR=200,000bps.

TimeBase=1sec -> We are committed to allocate 200,000 bits somewhere in 200 frames of 1 sec.

TimeBase=5ms -> We are committed to allocate 1,000 bits in each frame.

Currently, TimeBase is constantly defined as 1 sec.

1. UGS
   - Parameters: MIR, [CIR=MIR], Traffic Priority, UGI + jitter, latency.
   - PM bit (Poll me bit) - no polling for MS unless PM bit is set.
   - SI bit (Slip Indicator) – Grant Quota is increased by 1%.
2. eRT
   - Parameters: MIR, CIR, Traffic Priority, UGI + jitter, latency.
   - Grant Quota can be changed by:
     a. BWR
     b. Extended piggyback request in Grant Management SH
     c. CQI codeword (0b111011) -> maximum Grant Quota by MIR.
3. RT
   - Parameters: MIR, CIR, Traffic Priority, UPI + jitter, latency.
4. nRT
   - Parameters: MIR, CIR, Traffic Priority.
5. BE
   - Parameters: MIR, Traffic Priority.

<u>Scheduling Strategy algorithm description</u>

While building a frame, the Scheduler iteratively returns which connection should be served in that moment and how much quota "Frame Builder" should try to allocate for this connection.

<u>Input:</u>

- Connections with their corresponding properties (QoS type, priority, CIR, MIR, BW requested).
- Traffic demands per connection.

<u>Output:</u>

- Chooses which connection to serve in that moment and advices the amount of quota to be allocated.

<u>Service Interface primitives</u>

For the communications with other modules the Scheduling Strategy module will offer the service interface primitives described in *Table 10*:

IAP	Primitive name	Description
IAP5	SCST_IAP5_schedule_REQ /REP	Input: resources, candidates REP: scheduled amount of bytes/slots per candidate, [resources assignments] quota_struct Type={retransmission, new trans} quotaBytes cid actuallyAllocatedBytes

Table 10: Service Interface Primitives Scheduling Stragegy

The current Scheduler implementation is based on a round-robin fashion of existing connections in different priority queues.

A particular connection is located in the queues according to its current status. The status is changed when demands are added/removed and when we proceed to the next frame.

There are a few levels of connections' prioritization (graphically explained in *Figure 13*):

1. Committed/Uncommitted demands: A particular connection will be inserted into committed queue if it has not been served enough to guarantee the CIR. If a connection is over CIR but is still under MIR, it will be located in uncommitted demand queue. eRT/UGS connections will be inserted into committed queue if UGI was passed, otherwise it will wait in waiting list. First, all the connections in committed demand queue will be served and then uncommitted.
2. Demands queues are actually grids with a few dimensions as depicted in the figure. A grid cell points to a heap of connections sorted by "CIR /MIR percentage". "CIR/MIR percentage" of a connection is a ratio between the amount of already allocated bytes and CIR (or MIR for uncommitted). The grid dimensions enable to retrieve connections by this order (QoS Type -> CT -> Traffic Priority -> Quota Type). Connections with the same properties are stored in the heap and connection with the minimum "CIR/MIR percentage" will be chosen.

Sorting by "CIR/MIR percentage" assists in fair distribution of the bandwidth. Note that "CIR/MIR percentage" calculation is nullified each second.

3. Committed/Uncommitted Polling: RT/nRT/BE connections are polled (6 bytes for BWR are allocated in UL). The RT connections are polled each UPI. nRT/BE are polled each 1 sec. In addition, if we are working in "automatic polling mode", connections will be polled each frame. This mode can accelerate UL traffic transfer, since BW Requests can be sent immediately.

4. Polling queues are treated in a similar fashion as demands queues, except that its cell points to a list of connections.

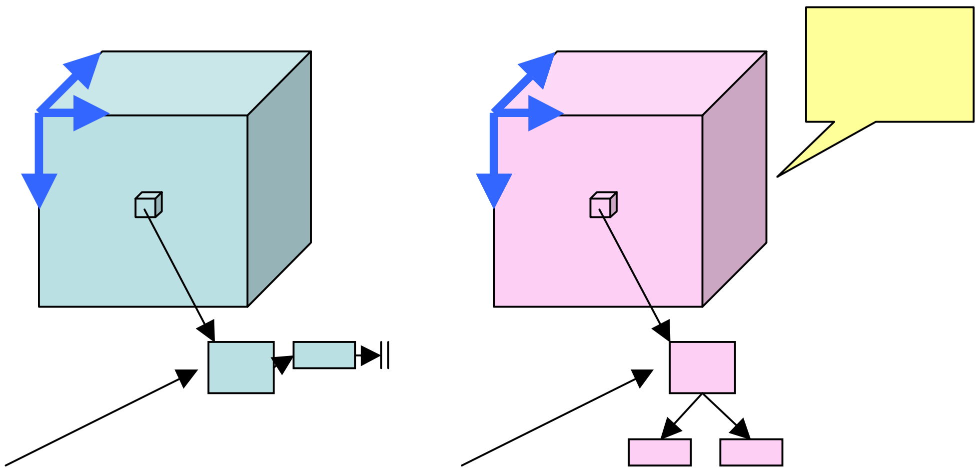


Figure 13: Scheduling strategy operation

When a specific connection is chosen by Scheduler, it also computes a quota that should be allocated for this connection. For eRT/UGS Uplink this quota is actually a GrantQuota. For polling of others connections, it is 6 bytes for BWR.

The rates (CIR/MIR) of others connections are guaranteed by the Leaky Bucket mechanism. First, we define a specific rate for a leaky bucket – its "drop" size per frame.

During traffic, tokens (demands) are added to the bucket. In each frame, one "drop" is released. If size of all the existing tokens in the bucket is less than "drop" size, all these tokens will be released.

Let’s introduce some scenarios to explain Scheduler behavior:

1. We have two MSs with one BE connection each (MIR=20,000,000bps) and we get input traffic with a rate of 2,000,000bps DL for each MS. We can see that BS inserts packets for only one MS in one frame. In the next frame the second MS is served. This happens in shortage because demands are accumulated and get_next_quota returns very high quota for currently served CID. The quota is partially satisfied till we have place in current frame. This causes that another connection can't be served at all in this frame. In the next frame the second connection will be selected and again will occupy the whole frame.
2. We have MIR=20,000,000bps which means average number of bytes per frame is 12500. We ask first demand 77 bytes, which are satisfied. In the next frame, we ask 12505 bytes and SCHD satisfies only 12500 (although previously we had extra free quota). If in the third frame we will ask again 77 bytes, it will give us 77+5.

Scheduling frame flow

The sequence diagram in *Figure 14* describes the scheduling frame flow. It shows the interaction among MAC Scheduler, QoS Strategy, Scheduling Strategy, Link Adaptaion and Data Transport modules.

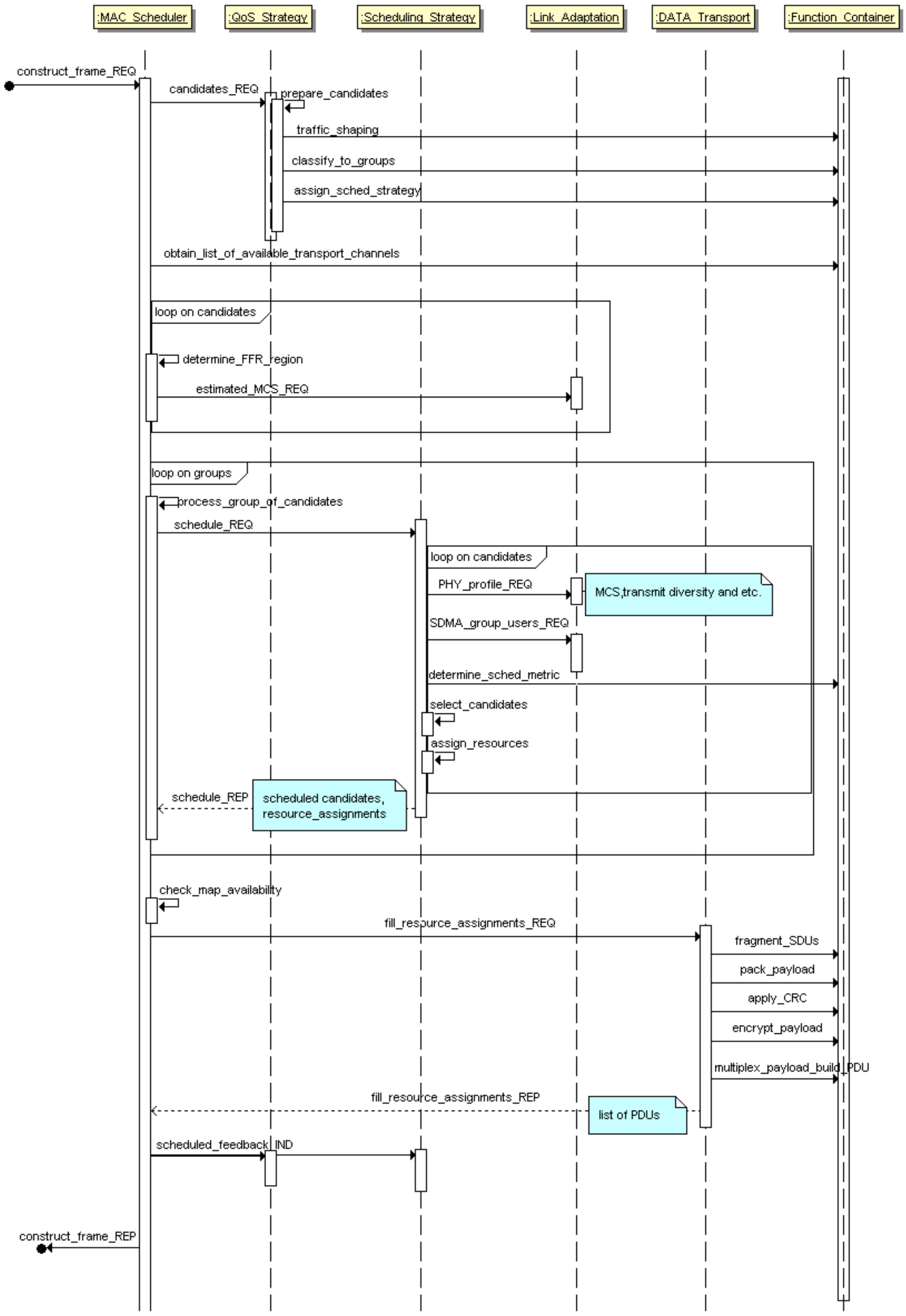


Figure 14: Scheduling frame flow

3.2.4.1 Update about the implementation of the architecture

In this reviewed version of the SCST Service we have selected the design proposed in D32. This upgraded SCST Service together with the QoS Strategy Service will provide the core functionality for the Dynamic Scheduling Strategy application scenario, one of the demonstrators that will validate FLAVIA's architecture for scheduled-based systems.

3.2.5 Link Adaptation (LADA)

Link Adaptation as defined in the following section will be part of the validation platform that will be provided.

<u>General description:</u>

The Link Adaptation service aims to maximise spectral efficiency while preserving QoS requirements and allowed interference level to neighbour BSs. Figure 15 illustrates Link Adaptation inputs/outputs:

- Measurements and reports are essential for Link Adaptation decisions since provide dynamically-changing channel quality and interference estimation;
- HARQ provides transmissions ack/nack feedbacks to learn and predict optimal MCS (modulation and coding scheme) selection;
- Maximal latency and number of HARQ retransmissions influence on MCS selection as well (e.g. delay-sensitive services will require more reliable transmissions , i.e. lower MCS);
- Transmission power should be as low as possible for minimal interference, but high enough to satisfy target packet error rate (PER);
- Capability to estimate interference created by connected users by using measurements and reports;
- Preserving interference restrictions (level) statically or dynamically defined;
- Providing/considering interference indicators to/from neighbours to enable global interference managing (via ICIC);
- Allocation size, power capabilities and link estimation define maximal transmission power and MCS.

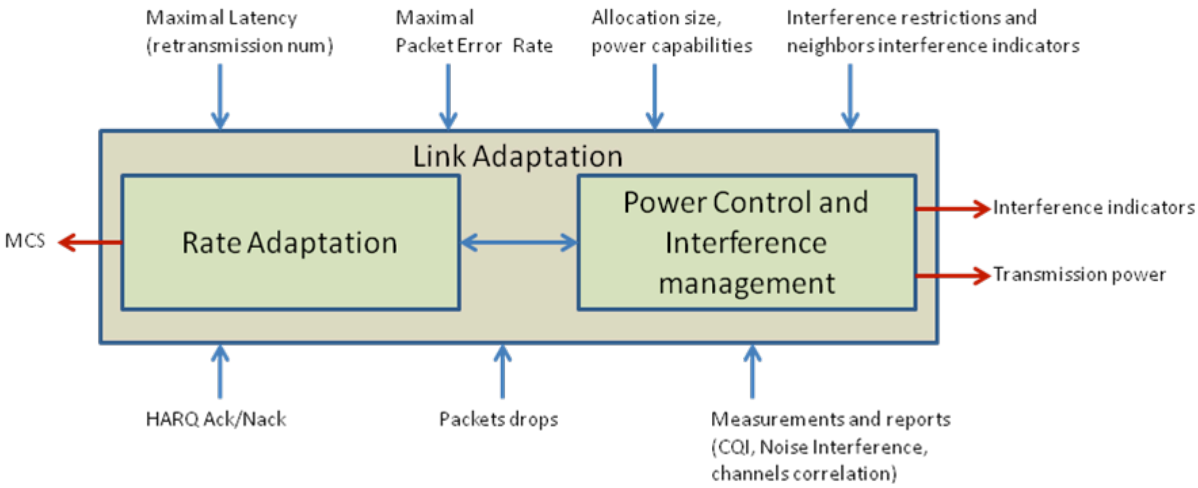


Figure 15: Link Adaptation input/outputs.

Figure 16 shows Link Adaptation main interactions with other services.

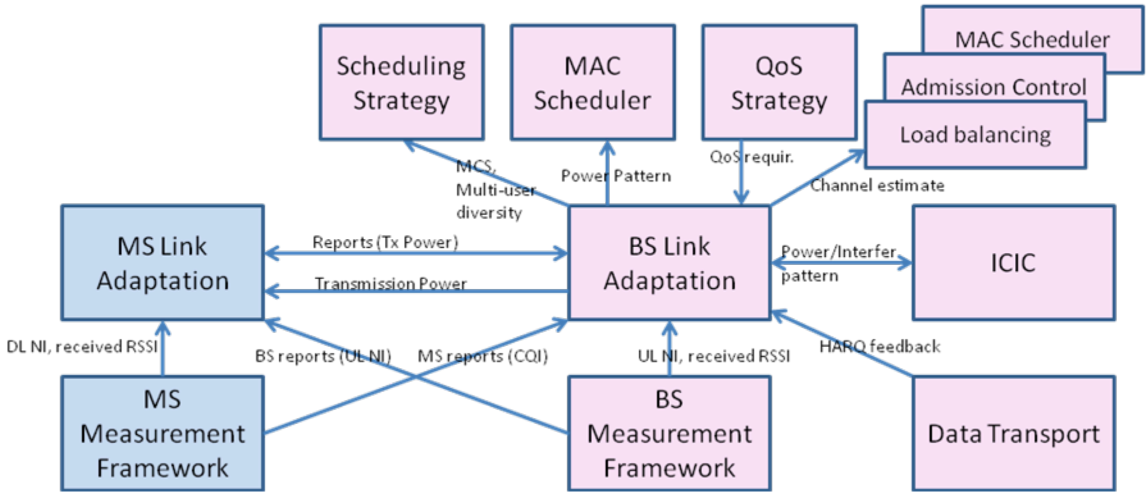


Figure 16: Main interactions between Link Adaptation and other services.

<u>Responsibilities:</u>

1. Collecting MS link quality reports
2. PER Statistics (transmissions fails, packets drops)
3. DL Rate adaptation
4. UL Rate adaptation
5. Transmission diversity decision

6. Multi-user channel correlation
7. Power control (OL/CL)
8. Interference management
9. Considering power/interference reports from neighbouring BSs

Service interface primitives:

For the communications with other modules the Link Adaptation module will offer the service interface primitives described in Table 11:

IAP	Primitive name	Description
IAP5	LADA_IAP5_PHY_profile _REQ/REP	Input: user/connection, resource unit/sub-band, power budget. Output: MCS, transmit diversity, transmission power, expected PER/number of retransmissions. <u>Interface parameters list:</u> Input: msId, direction, SLA, acid, allocRegion(Reuse1 or 1/3) Output: mcs, matrix A/B BOOL MRT_DL_Advisor(SDB_entry_ptr_t xi_sdb_entry, UINT8 xi_acid, UINT16 xi_cid, CDB_internal_sla_type_t xi_sla, /* QoS */ FCNT_frame_counter_t xi_tx_time, /* expected transmition time */ RATE_rates_t *xo_rate, PHY_e_repetition_coding_indication *xo_repetition, transaction_log_struct **pptlog, STC_Matrix_t xi_matrix_tag, // xi_matrix_tag is a request to work with specific Matrix STC_Matrix_t *xo_matrix_tag, // xo_matrix_tag == NULL means -->> DEMAND to work with xi_matrix_tag request FFR_ZONE_E_T xi_alloc_region)

Table 11: Service Interface Primitives for Link Adaptation module

3.2.5.1 MS Power Control Design

The MS power control is done in open loop by the Mobile Stations (MS).

The Base Station (BS) sends corrections if necessary during network entry process and after that sporadically in slow mode.

The corrections are done when the power calculated by the BS for the relevant MS exceeds 1dB.

Any correction will not exceed 2dB (meaning that the correction can be 1dB or 2dB). If additional corrections are required it will be done once per 20 frames (100ms).

Figure 17 describes the MS power control mechanism.

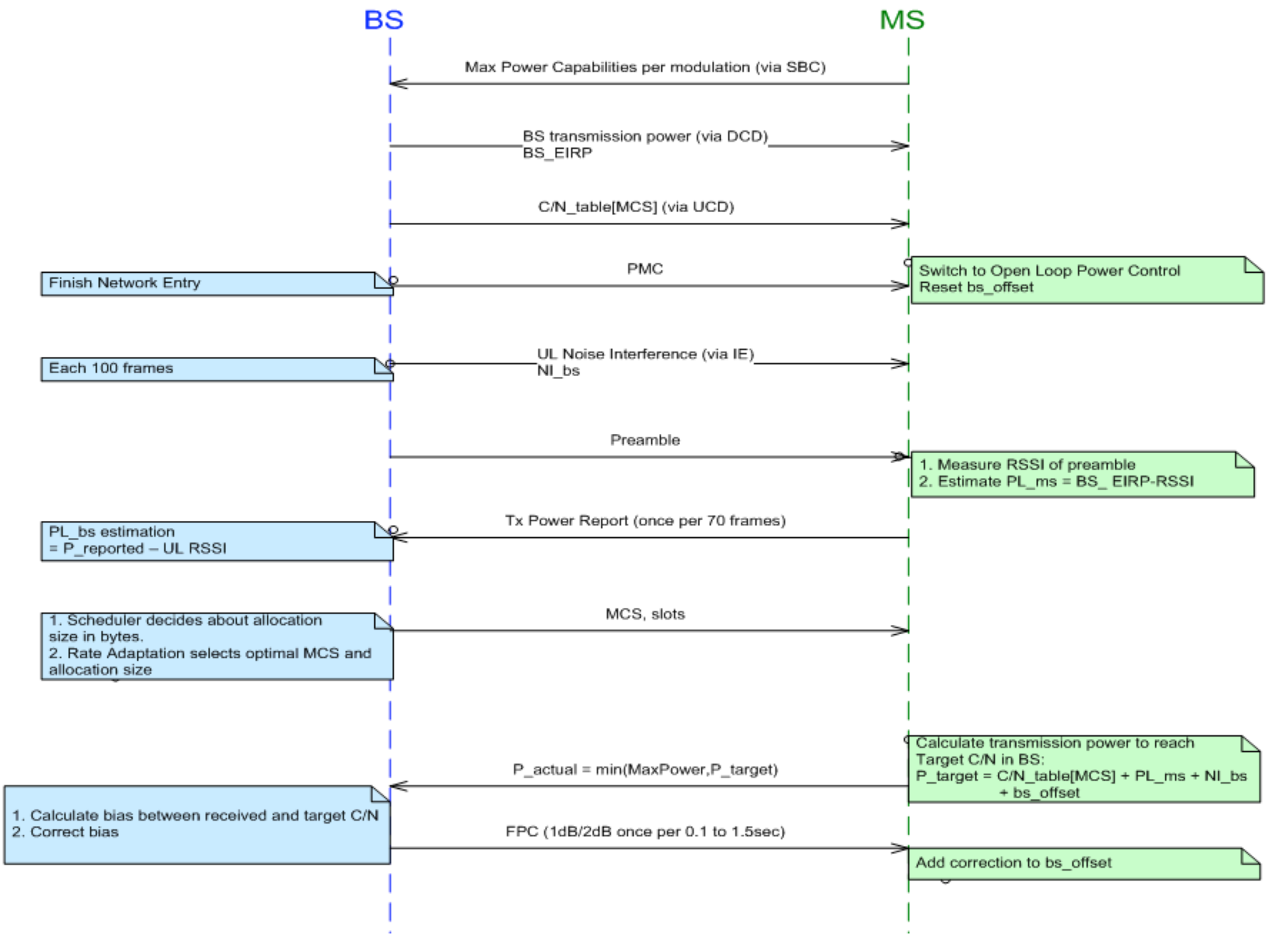


Figure 17: MS power control

Figure 18 describes the Rate adaptation and power control influencing the QoS strategy, the Scheduling strategy and MAC scheduler decisions for traffic resources allocation.

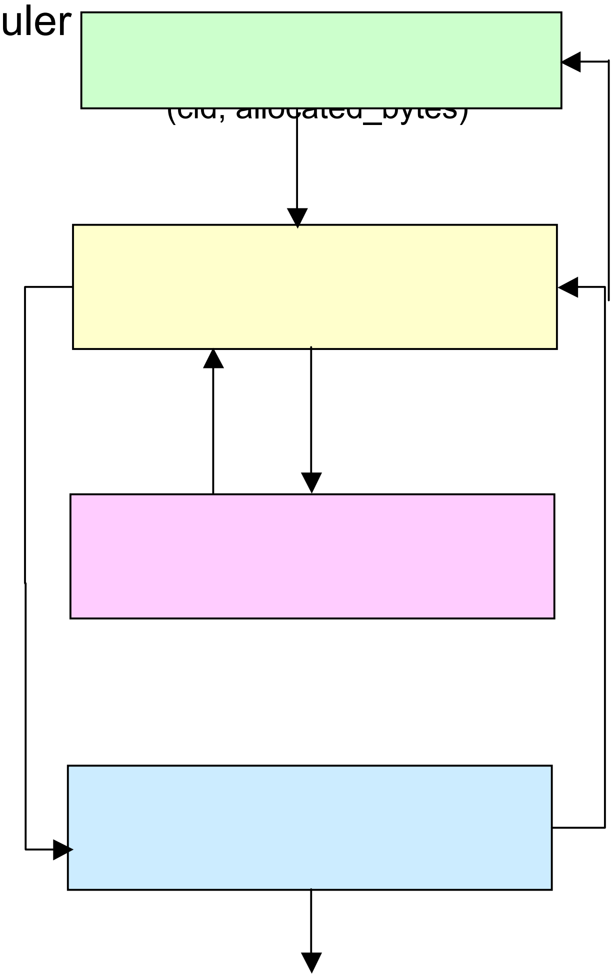


Figure 18: Link adaptation influencing traffic resources allocation

Figure 19 shows the interface of Link Adaptation (Rate Adaptation and Power Control sub-modules) with the other modules.

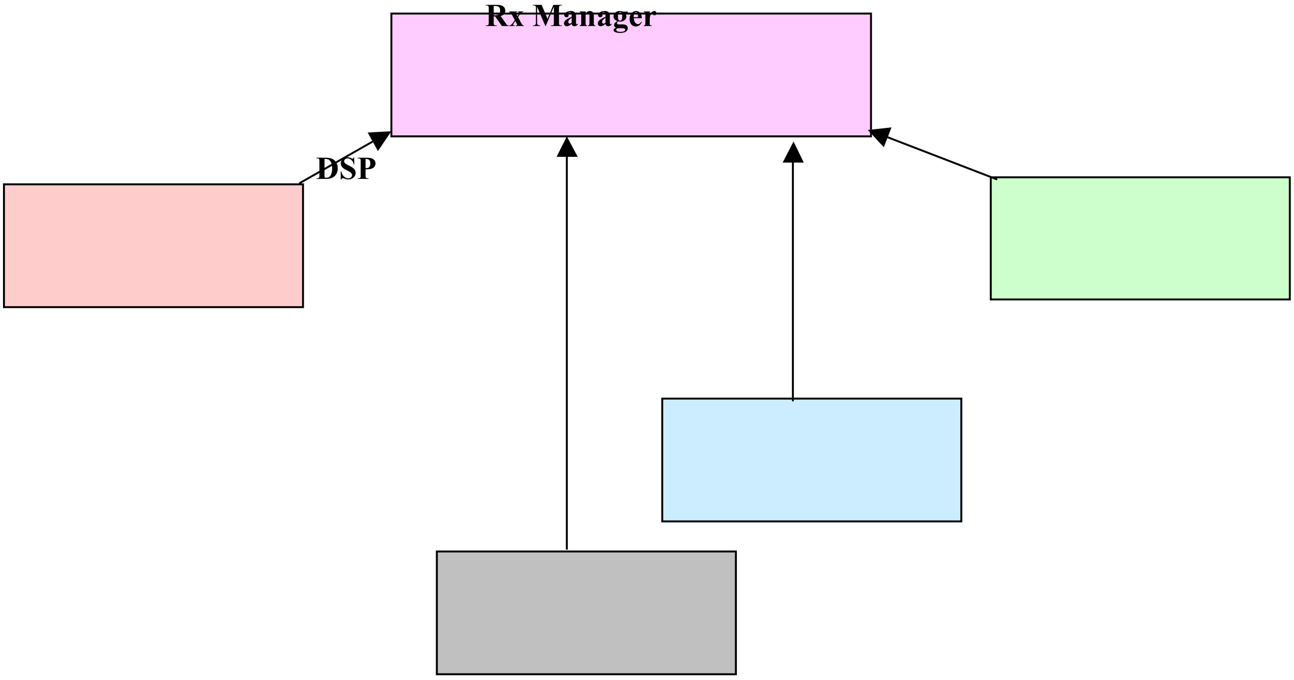


Figure 19: Link adaptation interfaces from other modules

The design of he Rate Adaptation sub-module has to achieve the following **goals**:

- **High Spectral Efficiency** (SE): MCS (Modulation and Coding Schemes) and their spectral efficiency are described in the following list:
  - QPSK ½ - SE = 2/2 = 1 bits/tone → 6 bytes/slot
  - QPSK 3/4 - SE = 2*3/4 = 1.5 bits/tone → 9 bytes/slot
  - 16QAM ½ - SE = 4/2 = 2 bits/tone → 12 bytes/slot
  - 16QAM 3/4 - SE = 4*3/4 = 3 bits/tone → 18 bytes/slot
  - 64QAM ½ - SE = 6/2 = 3 bits/tone → 18 bytes/slot
  - 64QAM 2/3 - SE = 6*2/3 = 4 bits/tone → 24 bytes/slot
  - 64QAM 3/4 - SE = 6*3/4 = 4.5 bits/tone → 27 bytes/slot
  - 64QAM 5/6 - SE = 6*5/6 = 5bits/tone → 30 bytes / slot

- **Required QoS assumptions**
  - BER - Burst error rate after HARQ (1-5%)
  - Latency shall consider the maximum transmissions number

means the allowed retransmissions are: 6 for BE/nRT and 2 for UGS/eRT/RT.

3.2.5.2 *Rate Adaptation design description*

In the **Down Link** (DL) the BS uses information coming from the Mobile Stations (MS). The MS measures DLCINR (Down Link Carrier to Interference-plus Noise Ratio, measured in dB) and reports it to the BS every 4 or 8 frames.

The BS uses DLCINR reports for selecting the most efficient DL MCS (Modulation and Coding Schema) under PER (Packet Error Rate) conditions.

Low DLCINR could be caused by high signal attenuation between the transmitter and the receiver (PL) and/or high interference from neighboring BS's (NI). DLCINR can be calculated as:

$$DLCINR = P\_bs - PL - NI\_ms$$

Where P_bs is the transmission power at the BS and NI_ms is the noise plus interference at the MS

In the **Up Link** (UL), the BS listens to the MS traffic and the MS sends periodic Tx reports in rder to calculate the ULCINR (Up Link Carrier to Interference-plus Noise Ratio)

A table with CINR Thresholds for MCS selection is built for both UL and DL directions considering Spectral Efficiency (*Figure 20*, *Figure 21*). There won't be static optimal thresholds but dynamic adaptive thresholds learning.

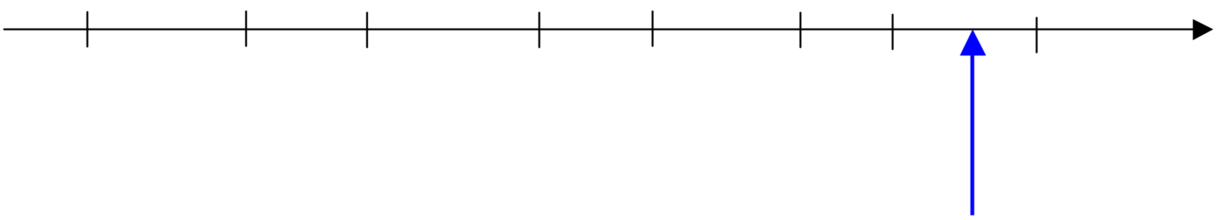


Figure 20: CINR thresholds versus different MCS values

The PER is considered. Until first_trans_PER is minor than 50% it is used retransmission instead of decrasing MCS. If it goes over 50% then the threshold will be increased and lower MCS will be selected.

For example, if we know that

$$SE(Qpsk3/4) = 1.5$$

and

$$SE(Qpsk1/2)=1$$

then

$$(1-PER)*1.5+PER*1.5/2=1$$

and so

$$PER = 66\%$$

So the system would go to Qpsk1/2 and move the threshold CINR down.

Inside certain MCS threshold physically, higher CINR causes lower PER so all samples need to be used to learn the optimal threshold value.

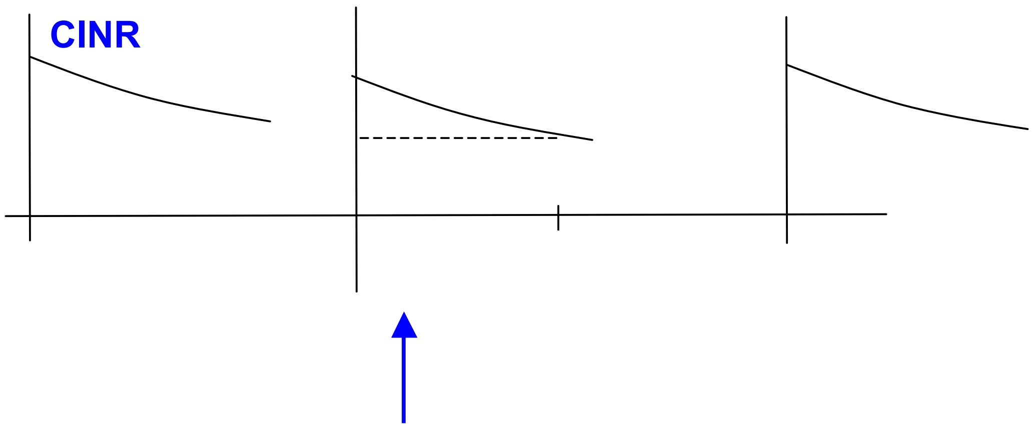


Figure 21: CINR control diagrams versus PER

In the UL direction, in addition to MCS selection, there is also sub channels selection considering the link budget and the BW required in which to optimize the best sector throughput performance. Therefore the best MCS with minimum SC shall be selected.

Using the ULCINR calculated we give MCS ranks to the sub-channels versus the MCS to be used.

Table 12 shows the CINR threshold values for each sub-channel versus the MCS to be used where as mentioned above the CINR is changed dynamically considering the BER calculated. Therefore the following table is updated from time to time.

The CINR for sub-channels used will be calculated as:

CINR (MCS, #subchan) = Max PT (MCS) – 10log (#subchan) – Ni – Path loss

MCS index	MCS / SC	35 sc	17	7sc	5sc	3sc	2sc	1sc
9	64 QAM 5/6	25	28	32	33	35	37	40
8	64 QAM 3/4	23	26	30	31	33	35	38
7	64 QAM 2/3	21	24	28	29	31	33	36
6	16 QAM 3/4	17	20	24	25	27	29	32
5	16 QAM 1/2	13	16	20	21	23	25	28

4	QPSK ¾	10	13	17	18	20	22	25
3	QPSK ½	7	10	14	15	17	19	22
2	QPSK ½ rep 2	4	7	11	12	14	16	19
1	QPSK ½ rep 4	1	4	8	9	11	13	16
0	-	N/A	1	5	6	8	10	13
-1	-	N/A	N/A	2	3	5	7	10
-2	-	N/A	N/A	N/A	N/A	2	4	7
-3	-	N/A	N/A	N/A	N/A	N/A	1	4
-4	-	N/A	N/A	N/A	N/A	N/A	N/A	1

Table 12: CINR threshold per sub-channel vs MCS

Table 13 converts the CINR values to MCS ranks.

The intention is to select the highest rank but the sub-channels allocated may prevent the required data traffic to transfer in a single frame and therefore fragmentation of the burst may be required.

We want to prevent fragmentation therefore we will select the maximal MCS rank versus the burst to be transferred. To reach this we need to go over the following 2 tables to find the optimum MCS and SC.

MCS index	MCS / SC	MCS index to be used						
		35 sc	17sc	7sc	5sc	3sc	2sc	1sc
9	64 QAM 5/6	9	9	9	9	9	9	9
8	64 QAM 3/4	8	9	9	9	9	9	9
7	64 QAM 2/3	7	8	9	9	9	9	9
6	16 QAM 3/4	6	6	7	8	9	9	9
5	16 QAM 1/2	5	5	6	7	8	9	9
4	QPSK 3/4	4	5	6	6	6	7	8
3	QPSK 1/2	3	4	5	5	6	6	7
2	QPSK 1/2 rep 2	2	3	4	4	5	5	6
1	QPSK 1/2 rep 4	1	2	3	3	4	5	5
0	-	N/A	1	2	2	3	4	5
-1	-	N/A	N/A	1	1	2	3	4
-2	-	N/A	N/A	N/A	N/A	1	2	3
-3	-	N/A	N/A	N/A	N/A	N/A	1	2
-4	-	N/A	N/A	N/A	N/A	N/A	N/A	1

Table 13: CINR values vs MCS ranks

Table 14 shows the relation between the bytes that can be transferred in each MCS versus the sub-channels used.

MCS index	MCS / SC	MCS index to be used						
		35 sc	17sc	7sc	5sc	3sc	2sc	1sc
9	64 QAM 5/6	5250	2550	1050	750	450	300	150
8	64 QAM 3/4	4725	2550	1050	750	450	300	150
7	64 QAM 2/3	4200	2295	1050	750	450	300	150
6	16 QAM 3/4	3150	1530	840	675	450	300	150
5	16 QAM 1/2	2100	1020	630	600	405	300	150
4	QPSK 3/4	1575	1020	630	450	270	240	135
3	QPSK 1/2	1050	765	420	300	270	180	120
2	QPSK 1/2 rep 2	525	510	315	225	180	120	90
1	QPSK 1/2 rep 4	262	255	210	150	135	120	60
0	-	N/A	127/134	105	75	90	90	60
-1	-	N/A	N/A	52	37	45	60	45
-2	-	N/A	N/A	N/A	N/A	22	30	30
-3	-	N/A	N/A	N/A	N/A	N/A	14	15
-4	-	N/A	N/A	N/A	N/A	N/A	N/A	7

Table 14: Bytes per MCS vs sub-channels used

3.2.6 Load Balancing (LOBA)

Load balancing is not part of the validation platform that will be provided.

General Description:

The load balancing service provides the network means to reduce connection blocking and dropping probability by controlling handover decisions. The load balancing service associates connections/users to base stations based on the load at the available base stations. The service could also balance the load between carriers, regions and zones without the need to perform handover.

Responsibilities:

1) Balance the load between cells/carriers/regions/zones
2) Initiate handovers

Service interface primitives:

IAP	Primitive name	Description
IAP4	LOBA_IAP4_configure_REQ/REP	Allows the FLAVIA control to configure the service. REP - to acknowledge FLAVIA Control configuration request.
IAP5	LOBA_IAP5_execute_REQ/REP	Triggers load balancing upon overflows initiated by Measurements and Monitoring service or periodic timer.
IAP2	LOBA_IAP2_execute_REQ/REP	Triggers load balancing upon request from peer load balancing service

Service indication primitives:

IAP	Primitive name	Description
IAP4	LOBA_IAP4_update_config_IND/SUB	Suggest to the FLAVIA control a configuration modification.

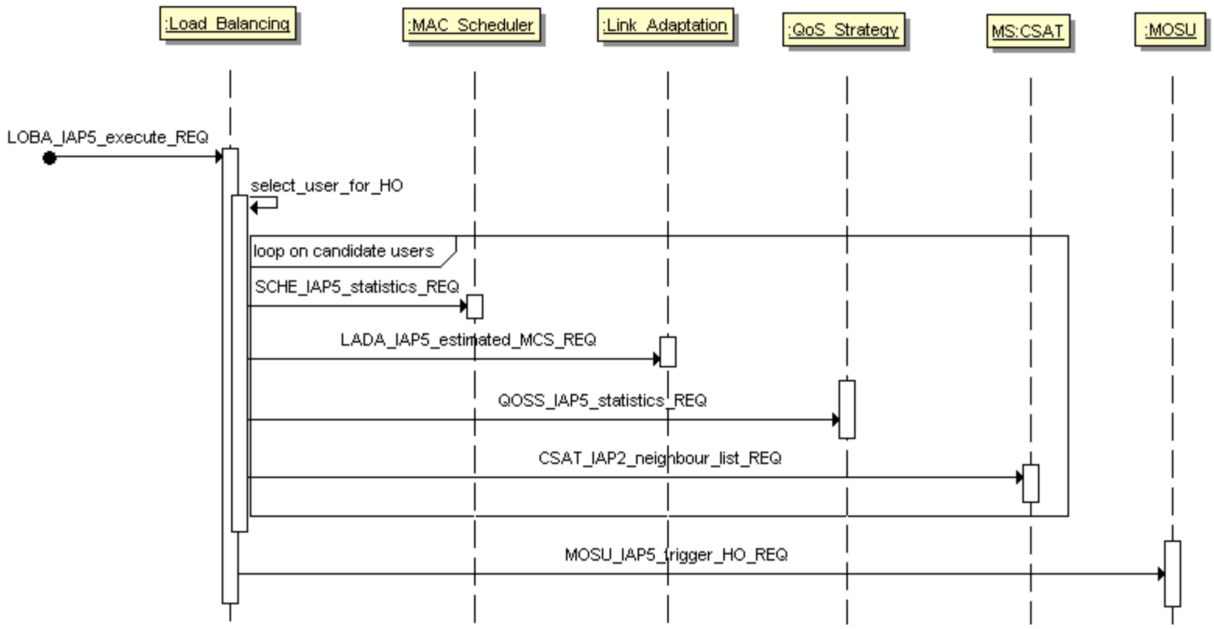
Required primitives from other services:

IAP	Primitive name	Description
IAP5	MOSU_IAP5_trigger_HO_REQ /REP	Request handover initiation from mobility support
IAP5	LADA_IAP5_estimated_MCS_REQ/REP	Obtain the channel estimation for new and existing connections/MSs
IAP5	QOSS_IAP5_statistics_REQ/REP	Obtain the QoS guarantees for existing connections
IAP2	CSAT_IAP2_neighbour_list_REQ	Obtain list of candidate target cells for handover
IAP5	SCHE_IAP5_statistics_REQ/REP	Provides statistics about frame utilization

MAC functions:

1. Load Estimation

Sequence Diagram:



3.2.7 Admission Control (ADCO)

Admission Control is not part of the validation platform that will be provided.

General Description:

The admission control service estimates the available resources and decides whether to accept a connection without jeopardizing the QoS of existing connections. Admission control may reserve resources for handover connections or/and higher priority connections. While the load balancing service has a network wide view, the admission control focus on the single cell performance.

Responsibilities:

1) Admit/block connections/MSs

2) Notify registered modules (services) about admitted new connection/MS
3) Notify registered modules (services) about blocked connection/MS

Service interface primitives:

IAP	Primitive name	Description
IAP4	ADCO_IAP4_configure_REQ/REP	Allows the FLAVIA control to configure the service. REP - to acknowledge FLAVIA Control configuration request.
IAP6	ADCO_IAP6_connection_conf_REQ/REP	Triggers the process of admission control

Service indication primitives:

IAP	Primitive name	Description
IAP4	ADCO_IAP4_update_config_IND/SUB	Suggest to the FLAVIA control a configuration modification.
IAP5	ADCO_IAP5_connection_conf_IND/SUB	Notifies registered services on admitted new connection/MS

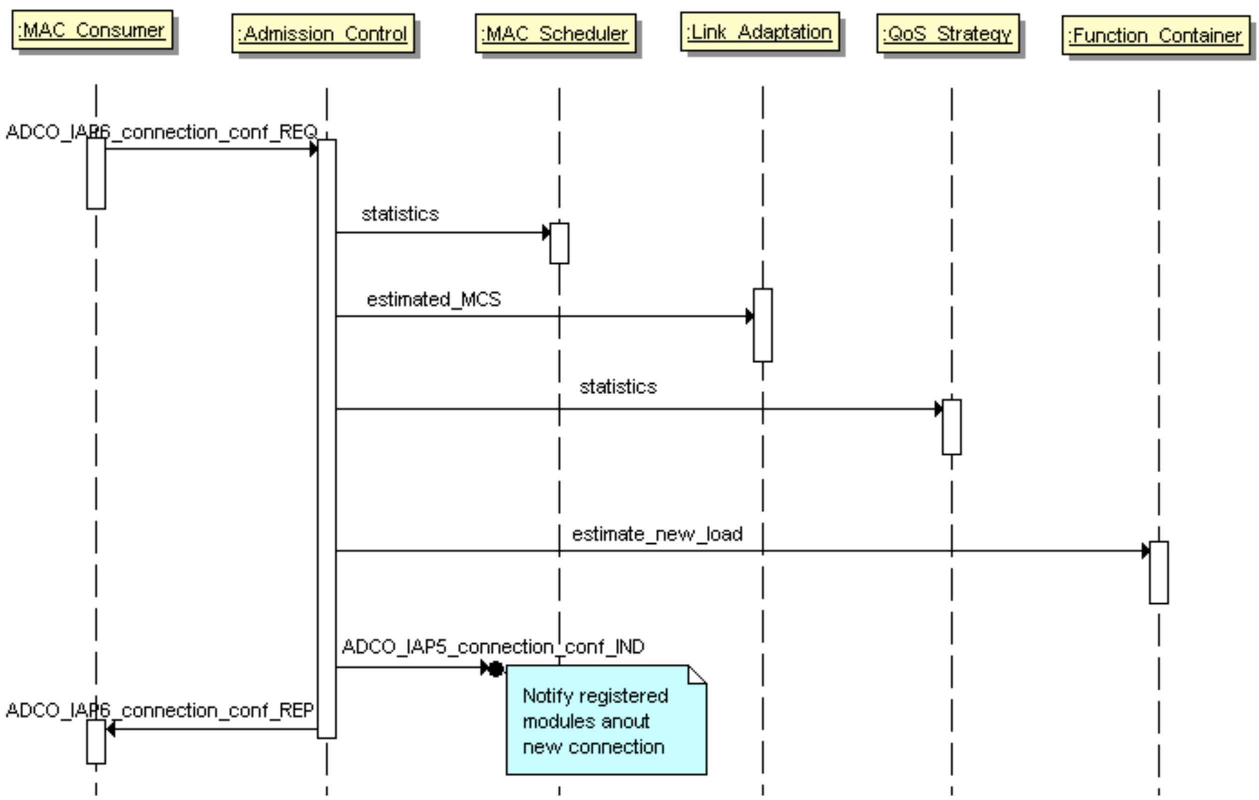
Required primitives from other services:

IAP	Primitive name	Description
IAP5	LADA_IAP5_estimated_MCS_REQ/REP	Obtain the channel estimation for new and existing connections/MSs
IAP5	QOSS_IAP5_statistics_REQ/REP	Obtain the QoS (traffic) statistics for existing connections
IAP5	QOSS_IAP5_QoS_attributes_REQ/REP	Obtain the QoS attributes for existing connections
IAP5	SCHE_IAP5_statistics_REQ/REP	Obtain frame utilization for existing connections

MAC functions:

1. Load Estimation
   Estimate the expected cell load in order to make the admission decision
2. Policy Manager (decision making)

Sequence Diagram:



3.2.8 Power Saving (POSA)

Idle mode Power Saving as described in the following section will be part of the validation platform that will be provided.

General description:

Power Saving mechanisms allow MS become unavailable on air interface for some time freeing operational resources and preserving MS power. In general, two power saving mechanisms can be outlined: sleep and idle.

In sleep mode, MS is connected to the BS. In this mode, MS does not receive/transmit any data from/to its serving BS during pre-negotiated sleep windows. Sleep window can be changed dynamically according to the traffic pattern.

In idle mode, MS is not registered to any BS. MS becomes periodically available for DL broadcast control messaging, i.e., MS paging. Using paging broadcast, BS can indicate (if necessary) the MS to exit from idle mode and return into normal operation mode. The paging message is sent over the DL of a set of BSs simultaneously. This set is called Paging group (PG). During idle mode, MS performs location updates when moving from one PG to another.

Figure 22 illustrates transition between operational and power saving modes in WiMax.

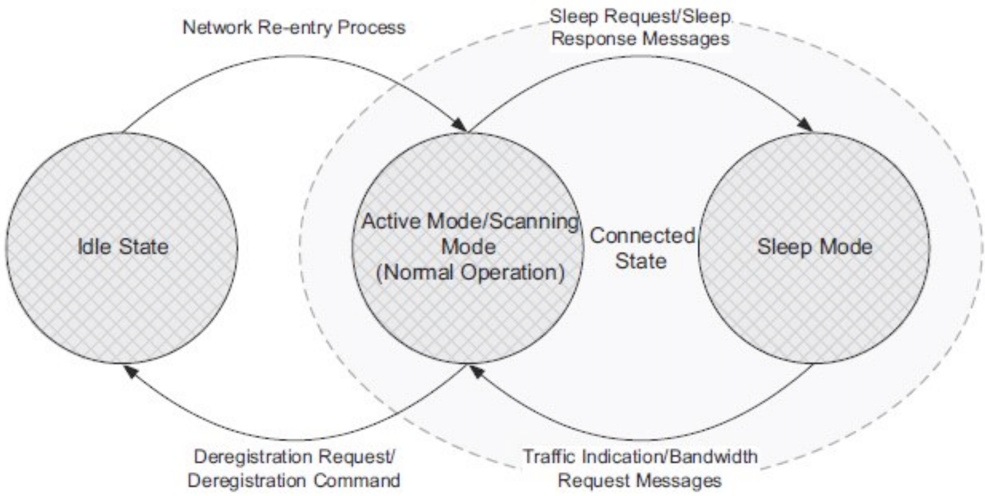


Figure 22: Transitions between Normal Operation and "Power Saving" modes in Wimax

Responsibilities:

This module's responsibilities are:

1. Implement Idle mode (only this mode will be deployed in FLAVIA application scenarios)
2. Inform other services about MS activity/inactivity

Service interface primitives:

For the communications with other modules the Power Saving module will offer the service interface primitives described in *Table 15*.

IAP	Primitive name	Description
IAP5	POSA_IAP5_enter_idle_bs_initiated_REQ/REP	Enter user to Idle mode bs-initiated. int16 msId
IAP2	POSA_IAP2_enter_idle_ms_initiated_REQ/REP	int16 msId
IAP4	POSA_IAP4_set_bs_paging_group_REQ/REP	Int16 Paging group per BS

Table 15: Service interface primitives in Power Saving module

Main Functionalities:

- Paging Controller (PC) entity is created in the Serving BS;
- IM negotiation between BS and MS during Network Registration procedure;
- IM Entry conditions;
- MS-initiated IM Entry;
- Location Update support:
  - Periodic Location Update;
  - Location Update by Paging Group update;
  - Power Down Location Update by MS;
- BS broadcast information (IM&P-related);
- MS Paging;
- MS IM Exit.

Sequence diagrams

The first sequence diagram (*Figure 23*) depits the process for a MS to enter into idle mode. The process is initiated by the BS for MS's. Previously the BS checks if the MS has initiated a handover (HO) process. If there's no HO process ongoing then based on the last traffic of traffic to/from the user the Power Saving module can ask a MS to enter into idle mode.

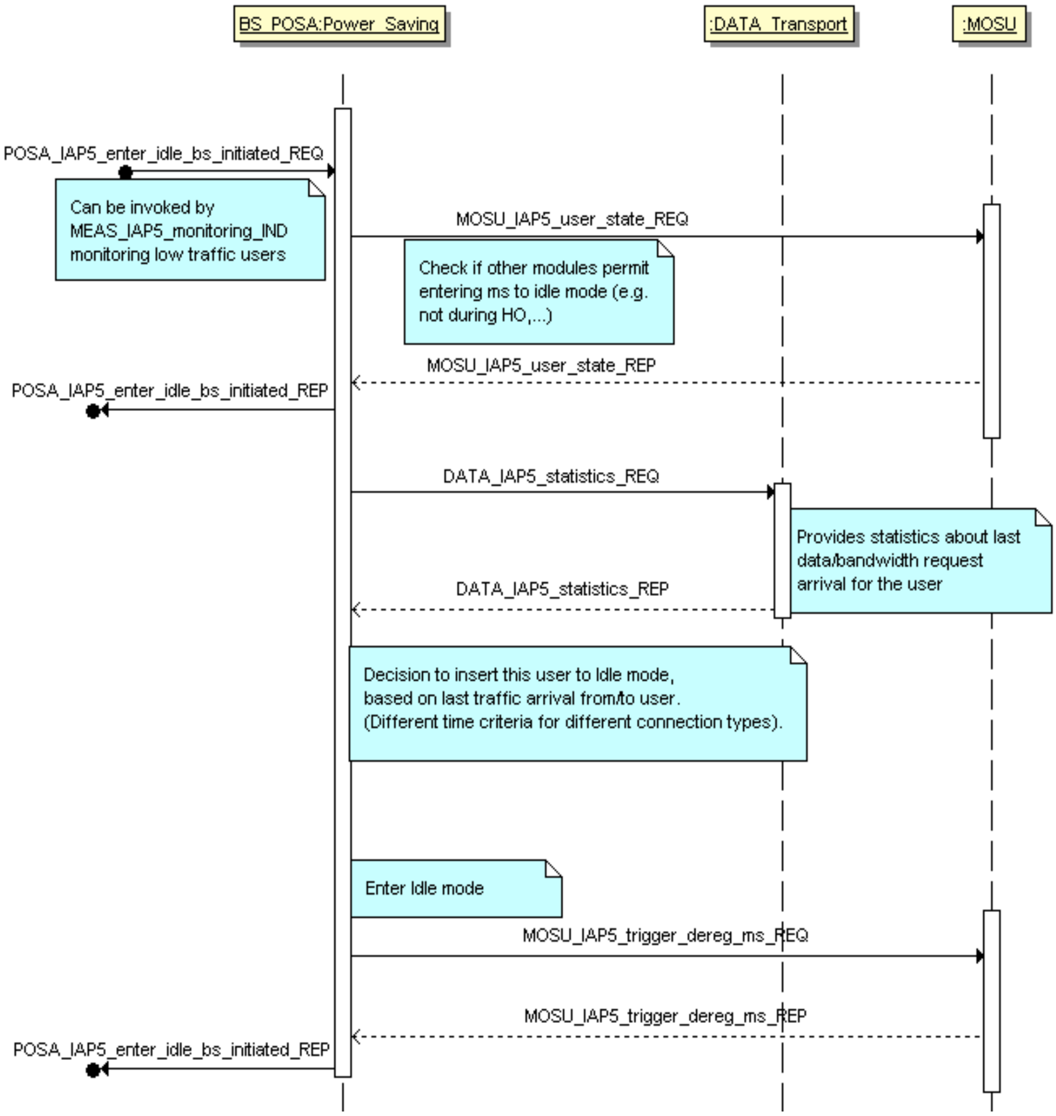


Figure 23: Enter Idle mode (BS-initiated)

As described in *Figure 24* the MAC Consumer module will detect when there is traffic for a MS which is in idle mode and will ask the Power Saving module to make it exit the idle mode via the next paging message.

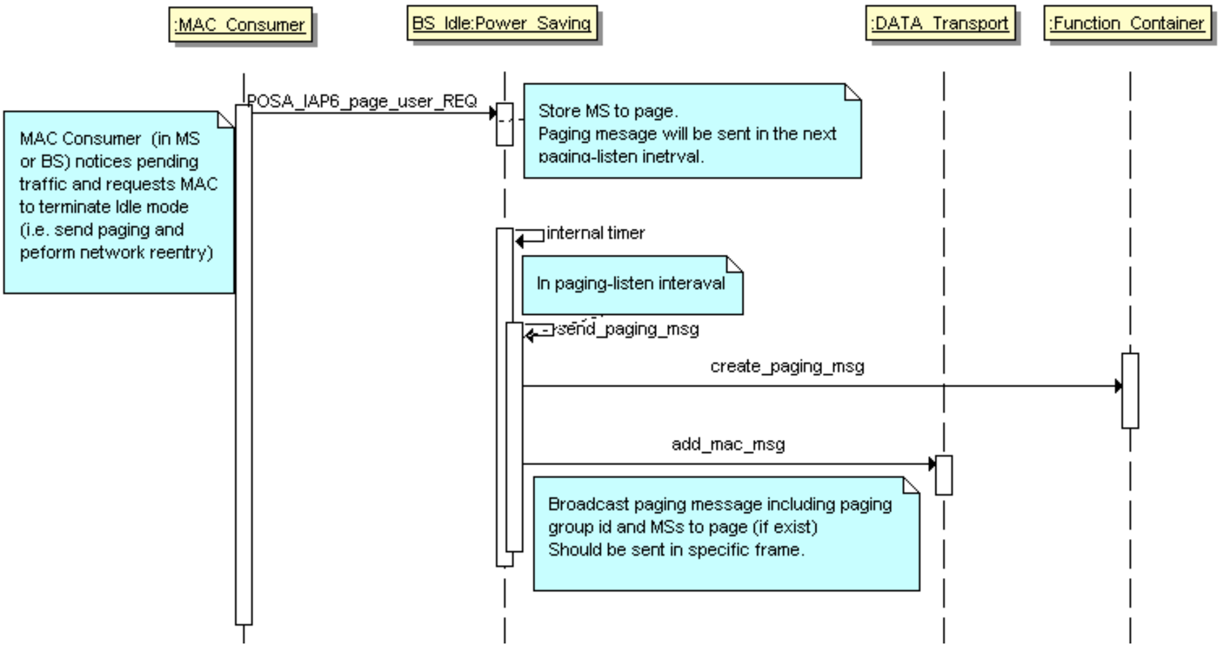


Figure 24: Page MS to exit Idle mode

Figure 25 shows the interface of the Idle Mode Manager which will be part of the Power Saving module with the other modules of the system.

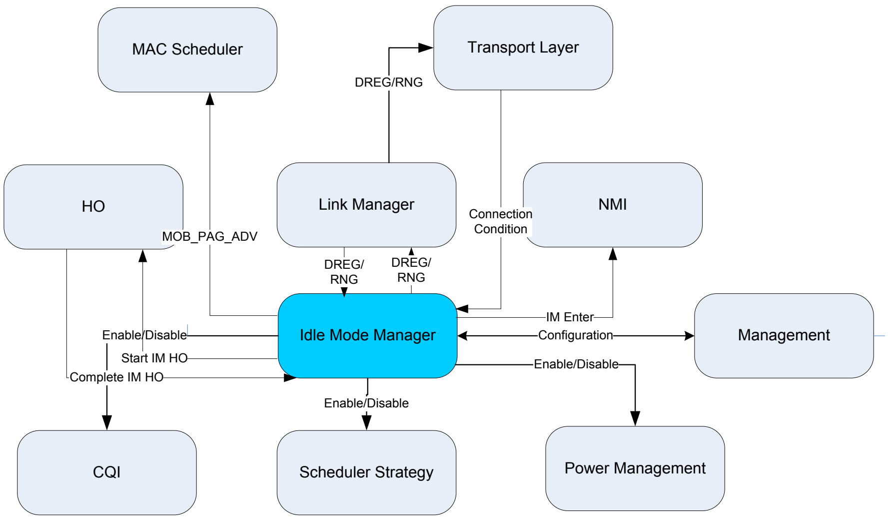


Figure 25: Idle Mode manager interfaces

<u>Paging Controller:</u>

Paging Controller (PC) entity is created in a BS (PCID = BSID) and Idle Mode/ Paging operations are not propagated to other network nodes (ASN GW). All the IM&P operations will be managed locally in the BS. *Figure 26* describes the state diagram of Paging Controller.

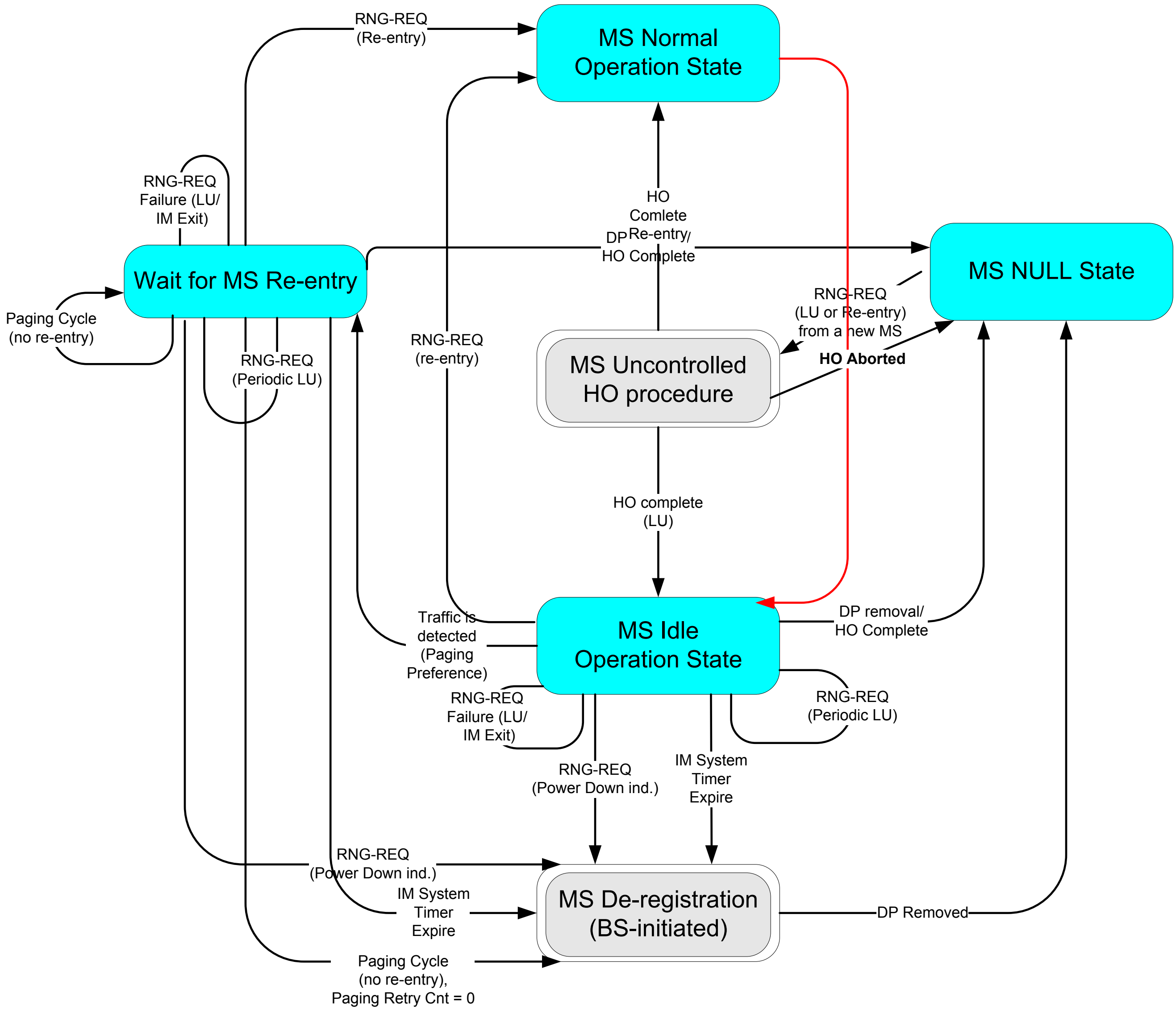


Figure 26: MS State Machine on the PC/BS

3.2.8.1 Idle Mode negotiation during Network Registration

During the Network Registration procedure, the BS & the MS negotiate the Idle Mode parameters.

Idle Mode support indication procedure

MS indicates its support of Idle Mode during Network Registration procedure using "Mobility features supported" field in REG-REQ message - bit #2 should be set to "1" indicating Idle Mode support.

If BS is provisioned to support IM&P, it shall set Idle Mode support bit in "Mobility features supported" field of REG-RSP to "1". Otherwise, it sets this bit to "0", thus prohibiting MS to request Idle Mode entry.

Idle mode System Timer

BS's Idle Mode System Timer indicates the maximum interval the PC shall maintain all MS service and operational information retained for idle mode management and indicates how frequently MS shall perform periodic Location Updates.

During network registration process, MS also provides its preferred value of Idle Mode Timeout (in the corresponding parameters of REG-REQ message). BS responds with network requested Idle Mode Timeout in REG-RSP message. Its value is pre-provisioned in BS using ***bsIdleModeSystemTimer*** parameter.

Input/ Precondition

- **bsIdleModePagMode** provisioned parameter indicates mode of IM: NONE, BASIC.
- **bsIdleModeSystemTimer** indicates the Max time interval between Location Updates.

Output (post conditions)

- Idle Mode enable/disable for current MS

3.2.8.2 IM Entry

Idle Mode may be initiated by BS command or as BS answer for MS request.

Input/ Precondition

The following conditions should be met prior to enabling MS entering IM:

- No pending downlink traffic for the MS on one of its data connection
- No pending MAC transactions with the MS on Primary connection.
- No admitted Service Flows (UGS)
- No Managed connections
- MS finished Network Entry (including any data ,DL or UL, CIDs)
- MS has IP address (according to IP address acquire timer)

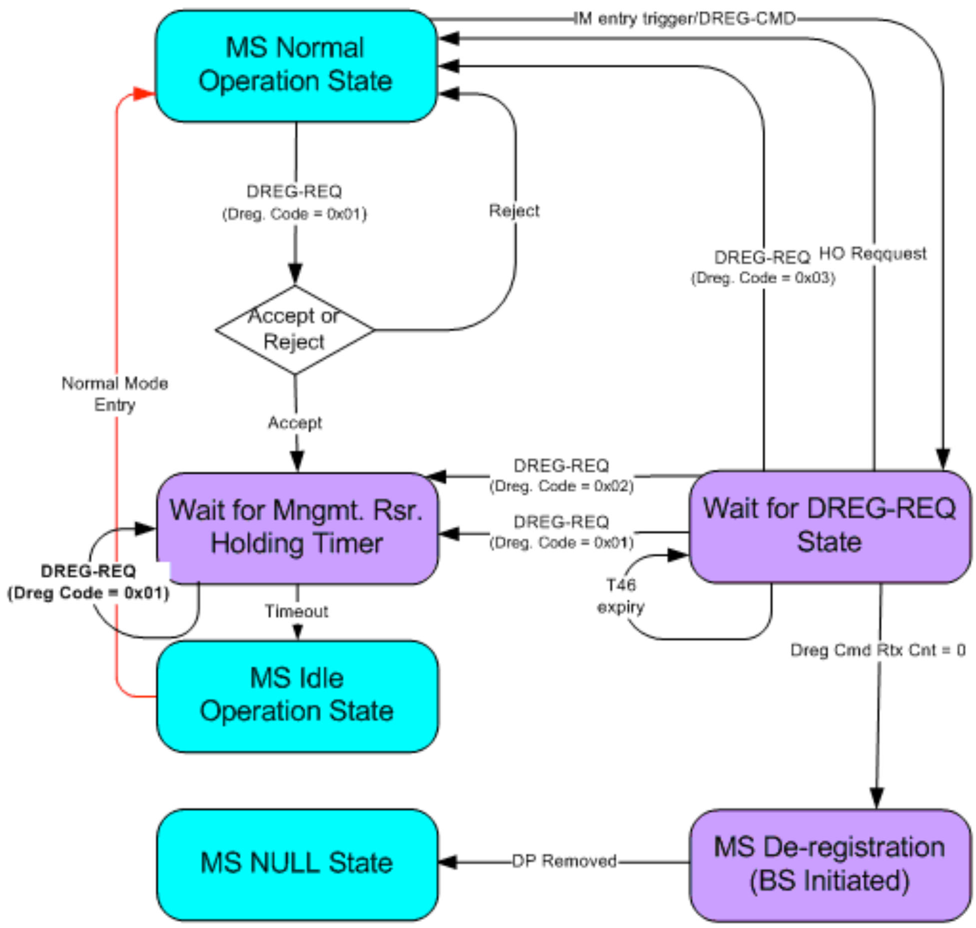


Figure 27: MS State Machine on BS for Idle mode negotiation

3.2.8.2.1 MS-initiated IM Entry Use Case

MS Normal Operational State (see *Figure 28*):

1. Bs receives MS's DREG-REQ message with action code 0x01 from MS requesting for Idle Mode initiation.
2. BS verifies whether one or more of the IM Entry conditions are violated.
3. BS replies with DREG-CMD with appropriate action code.

Rejection scenario:

One or more of the aforementioned conditions are violated event

Action:

- BS sends DREG-CMD action code 0x06 with REQ-duration TLV (rejection).

New State:

MS stays in *Normal Operational State*.

Success scenario:

BS decides to accept the MS request event

Action:

- the BS sends back DREG-CMD with action code 0x05;
- alerts Paging Controller to activate its Idle Mode System Timer;
- starts Management Resource Holding Timer.

New State:

MS moves to *Wait for Management Resource Holding Timeout state*.

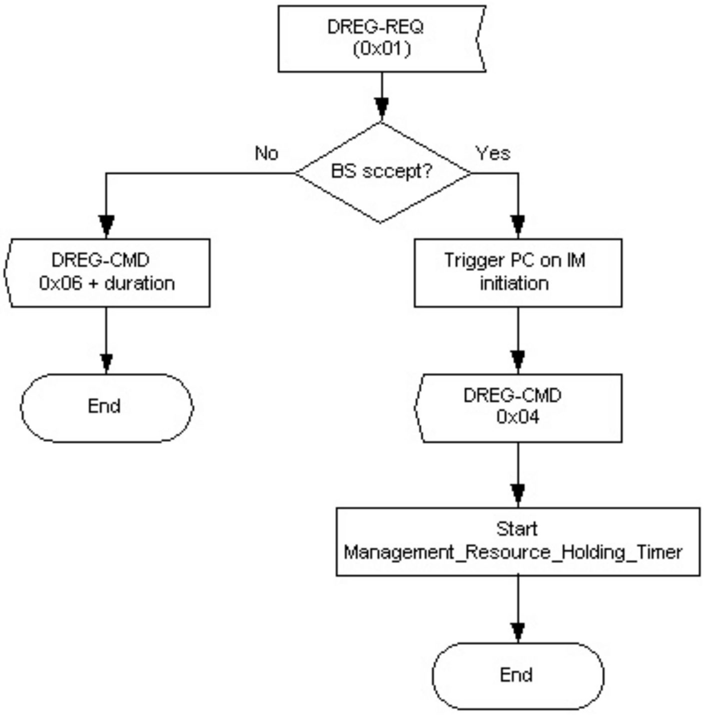


Figure 28: MS-Initiated IM.

3.2.8.3 Location Update

MS performs Location Update (LU) by sending RNG-REQ message with Ranging Purpose indicator set to indicate "Idle Mode Location Update". BS responds with corresponding RNG-RSP message indicating the results of LU in Location Update Response TLV.

LU messages (i.e. RNG-REQ/ RSP messages) are using Initial Ranging CID (MS does not have allocated CIDs in Idle mode) in Initial Ranging interval.

If an MS is in idle mode and a Target BS shares the security association (i.e. are able to sign MAC control messages with the valid CMAC tuple value), then Secure LU procedure is performed. Otherwise, Un-secure LU is conducted.

Location Update by Paging Group update

MS detects that its *new* Preferred BS does not participate in the Paging Group allocated previously for the MS;

Periodic Location Update

The MS and the PC (in the Serving BS) shall maintain an Idle Mode Timer (MS maintains Idle Mode Timer and PC maintains Idle Mode System Timer; both are started from DREG-CMD message) to prompt MS Idle Mode Location Update activity.

It is MS responsibility to avoid Idle Mode System Timer (network side) expiration by performing periodic LU operation sufficiently ahead of the expiration time (defined by Idle Mode Timer).

At the expiration of Idle Mode System Timer, BS terminates MS Idle Mode state and proceeds with MS deregistration from the network (without performing any operation on air interface).

Power Down Location Update.

MS detects power down condition and sends toward the Serving BS RNG-REQ message with Power Down indicator.

Figure 29 shows the flow for all the possible Location Update situations.

Input/ Precondition

A MS in Idle mode shall perform a Location Update procedure if any of the following conditions is met:

- MS detects that its *new* Preferred BS does not participate in the Paging Group allocated previously for the MS;
- Idle Mode Timer Update (some predefined grace time before IM timer in the MS is going to expire) - Periodic Location Update;
- Power Down Location Update (MS detects power down condition).

The MS's States on PC State Machine may be

- IM State;
- Waiting for MS Re-entry State

Processing (scenario)

Secure Location Update

1. BS receives Secure LU RNG-REQ message from MS, protected by the valid CMAC and Ranging Purpose Indication Bit #1 set to 1 indicating IM Location Update procedure.
2. Paging Controller ID TLVs.
3. BS validates CMAC tuple value.

IM State:

Received valid RNG-REQ message event

Action:

- BS responds with RNG-RSP message protected by a valid CMAC and Location Update Response value 0x00 = Success of IM Location Update.
- PC/BS shall restart Idle Mode System Timer on any successful MS network Idle Mode Location Update (starting from RNG-RSP message).

New State: Stays in Idle Mode state

Wait for MS Re-entry State (traffic detected):

Received valid RNG-REQ message event

Action

- If a BS, at the time of Secure LU, detects DL traffic for MS service flows, then the BS may set LU Response value to “0x03” indicating the MS shall terminate Idle Mode and perform network re-entry. In this case, the BS shall not include PCID and Paging Info TLVs in the RNG-RSP message. MS receiving a valid RNG-RSP with LU Response = 0x03, shall start IM Exit procedure.

New State: Stays in Wait for MS Re-entry State

IM State / Wait for MS Re-entry State (traffic detected):

Received invalid RNG-REQ message event

Action

- BS directs MS to perform Unsecured Location Update

New State: Stays in the same State

Unsecured Location Update

In this case BS instruct MS to perform full network entry procedure (initial network entry) by sending an unprotected RNG-RSP (without CMAC tuple) with Location Update Response TLV set to the value indicating "Failure of Location Update" and Location Update Response value 0x01 = Failure of IM Location Update.

Location Update by Paging Group update use case

1. The BS detecting Secure LU from the new MS (MS, it is not aware of) and provisioned to support IM&P in "Basic" mode of operation.
2. Perform Unpredictive HO procedure as described in FDR group 01-004.

   Current feature definition does not consider relocating any additional information related to MS Idle Mode state in the HO procedure. Instead, it is assumed that all the relevant parameters should be correctly provisioned in all the BSs of the same ASN.

   New MS SA IDs should be stored in the BS together with old SA IDs till MS executes IM re-entry. (During the re-entry process the SA IDs should be changed).
3. *Success Scenario:* MS in **Null State**

HO procedure for IM complete event

Action:

- When BS completes network HO procedure, it sends Success RNG-RSP message allocating the new IM-related parameters – PCID, PGID, Paging Info, etc., using old SA IDs.

- The new BS from ASN network perspective becomes the Serving BS and from MS perspective, - MS's Paging Controller and maintain the MAC context and networking contexts of the MS from the previous BS. PC/BS (acting as MS' PC) should restart IM System Timer when sending RNG-RSP **success** message (PG update).

New State:

MS moved to **Idle Mode State**

Failed scenario: MS in **Null State**

HO procedure failed event

If HO process failed then BS directs MS to perform Unsecured Location Update.

Then Target BS should follow the fail over scenario for Uncontrolled HO. In this scenario, the Target BS does not establish Data Path with Anchor ASN GW and Serving BS continues maintaining MS context as Idle.

New State:

MS in **Null State**

Power Down Location Update

IM State / Wait for MS Re-entry State (traffic detected):

Received valid RNG-REQ message with Power Down indicator event

Action

- BS responds with RNG-RSP message with Location Update Response parameter value 0x00 = Success, Power Down Response 0x01 – Success of Power Down information update.

Current implementation does not consider any logic for rejecting MS Power Down request. It means that BS normally does not respond with "Failure of Power Down Information Update".

New State:

MS moves to **Deregistration process State**

Location Update failure conditions

- MS Context in the PC (Serving BS when in "Basic" mode) or in the Authenticator is lost (e.g. as a result of idle mode timer expiry or MS Deregistration);
- BS receiving RNG-REQ (LU request) is not able to communicate MS context with MS' PC or Authenticator – for "Basic" IM&P mode it is any failure of Uncontrolled HO;
- BS is not able to validate CMAC tuple in the received RNG-REQ;

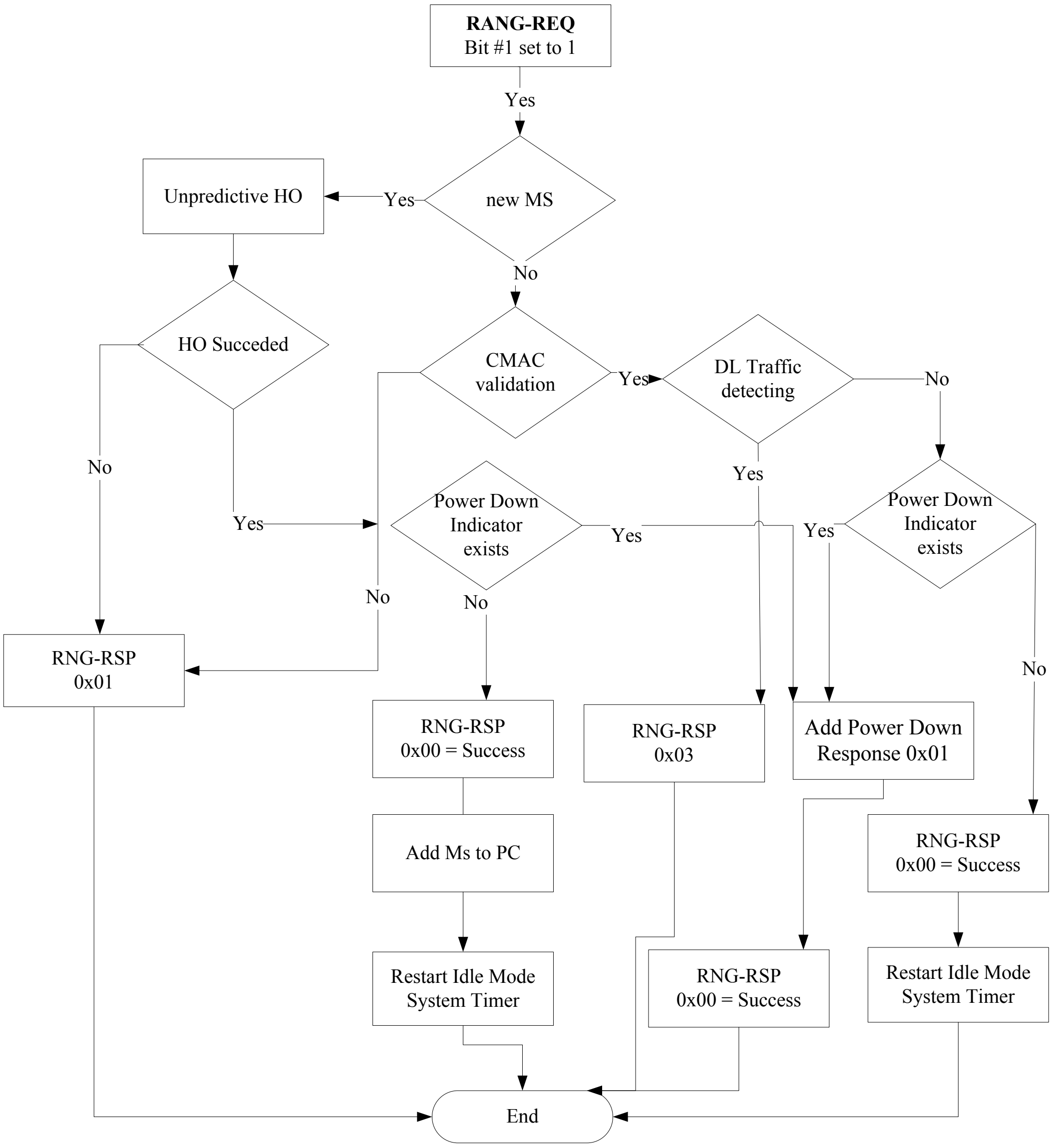


Figure 29: Location Update procedure

3.2.9 Inter-Cell Cooperation and Coordination (ICIC)

Inter-Cell Cooperation and Coordination will not be part of the validation platform that will be provided.

General description:

The scarce resource of frequency bandwidth makes inter-cell coordination and cooperation algorithms increasingly important for the mobile network operators in order to further enhance data rates and capacity. Especially the frequency re-use 1 schemes require a high degree of coordination to avoid low cell edge performance due to interference. Several static & dynamic approaches can be programmed, including interference coordination based on power and resource allocation such as FFR and soft FFR, collaborative MIMO techniques and supporting techniques for feedback. Static coordination is usually easy to achieve by pre-configuration parameters and rules between adjacent base stations and involves little or no communication between base stations. Common static coordination includes static FFR and soft FFR schemes, where physical resources are partitioned by static allocation (FFR) or power level transmission (soft FFR) between BSs, interference aware scheduling in which the total interference introduced to other base stations is limited. Dynamic coordination and cooperation schemes are more difficult to achieve and require tight and prolonged synchronization and communication between adjacent base stations. Dynamic FFR and macro-BS scheduling are examples for dynamic coordination and cooperation mechanisms. In macro-BS scheduling, same frequency/time resources are synchronically allocated from base stations to uncorrelated mobile stations and Multi-BS MIMO transmission, including single BS MIMO transmission with cooperation for interference nulling or precoding matrix indicators from other BSs and joint MIMO transmission from two or more BSs over same MS apply.
Figure 30 depicts the interaction of the inter-cell coordination and cooperation service with other services and with the peer service at neighbouring cells.

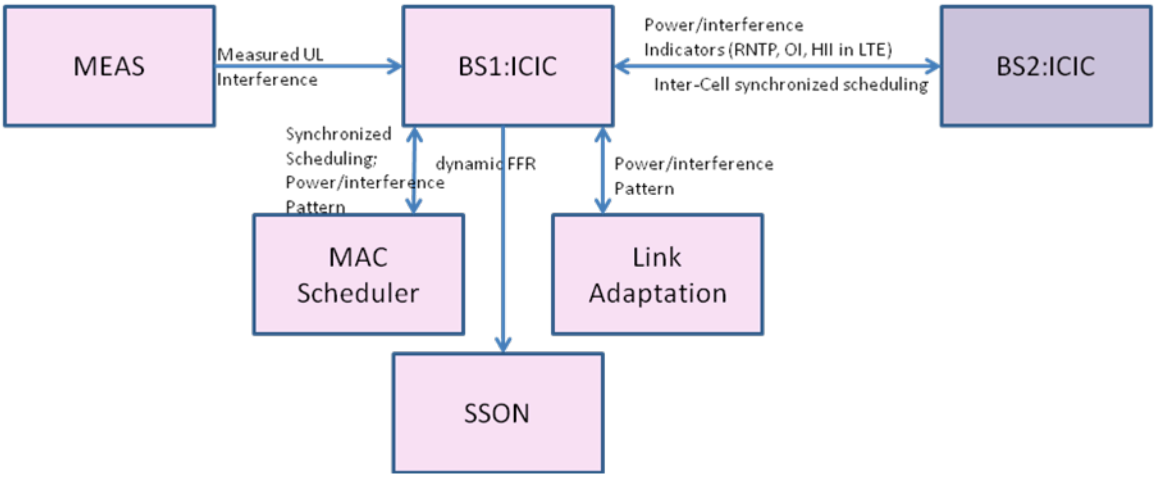


Figure 30: Main interactions between ICIC and other services.

Responsibilities:

1. Collecting neighbour power/interference reports
2. Provide inputs for SON and MAC scheduler - FFR scheme
3. Provide restrictions for:
    a. MAC scheduler (time/frequency restrictions for macro-BS scheduling);
    b. Link adaptation (power constraints).
4. Adapt to cell load
5. Adapt to user load
6. Control inter cell coordination communication
7. Synchronize inter-cell scheduling

Service interface primitives:

IAP	Primitive name	Description
IAP4	ICIC_IAP4_configure_REQ/ REP	Allows the FLAVIA control to configure the service. REP - to acknowledge FLAVIA Control configuration request.
IAP5	ICIC_IAP5_set_my_info_R EQ/REP	Set "my BS" information about: 1. Power/interference indicators; 2. Scheduling constraints for inter-cell synchronized scheduling. This information will be published to neighboring BSs. (Will be set mainly by MAC Scheduler).
IAP5	ICIC_IAP5_get_neighbours _info_REQ/REP	Request info about the neighbour cells and their users: 1. Power/interference indicators; 2. Scheduling constraints for inter-cell synchronized scheduling.
IAP2	ICIC_IAP2_get_neighbours _info_REQ/REP	Request info from the neighbour cells and their users.

Service indication primitives:

IAP	Primitive name	Description
IAP2	ICIC_IAP2_high_interferen ce_IND/SUB	Indication of expected uplink interference. Proactive ICIC mechanism, standardized by LTE as High Interference Indicator (HII). The HII includes bit per resource unit, indicating whether the serving cell intends to schedule cell-edge users causing high inter-cell interference on those resources. Can be used to avoid scheduling of cell-edge users at the same resources between two neighboring cells.
IAP2	ICIC_IAP2_overload_IND/ SUB	Indication of measured uplink interference. Reactive uplink ICIC scheme, standardized by LTE as the Overload Indicator (OI). The BS measures the uplink interference noise power, and creates OI reports based on this measurement. Low, medium, and high OI reports can be signaled. Can be used for uplink open loop power control adjustments to maintain a certain maximum desirable uplink interference noise level.
IAP2	ICIC_IAP2_tx_power_IND/ SUB	Indication of expected downlink Tx power. Proactive downlink ICIC schemes, standardized by LTE as Relative Narrowband Transmit Power (RNTP) indicator.
IAP5	ICIC_IAP5_neighbours_inf o_IND/SUB	Indication about changes in reported information from neighboring BSs.

Required primitives from other services:

IAP	Primitive name	Description
IAP5	SSON_IAP5_update_config_ REQ/REP	Request SSON to update configuration (e.g., FFR regions size)
IAP5	MEAS_IAP5_get_meas_REQ /REP	Get measured uplink interference for reactive uplink interference indicators to be sent to neighboring BSs.

Diagrams:

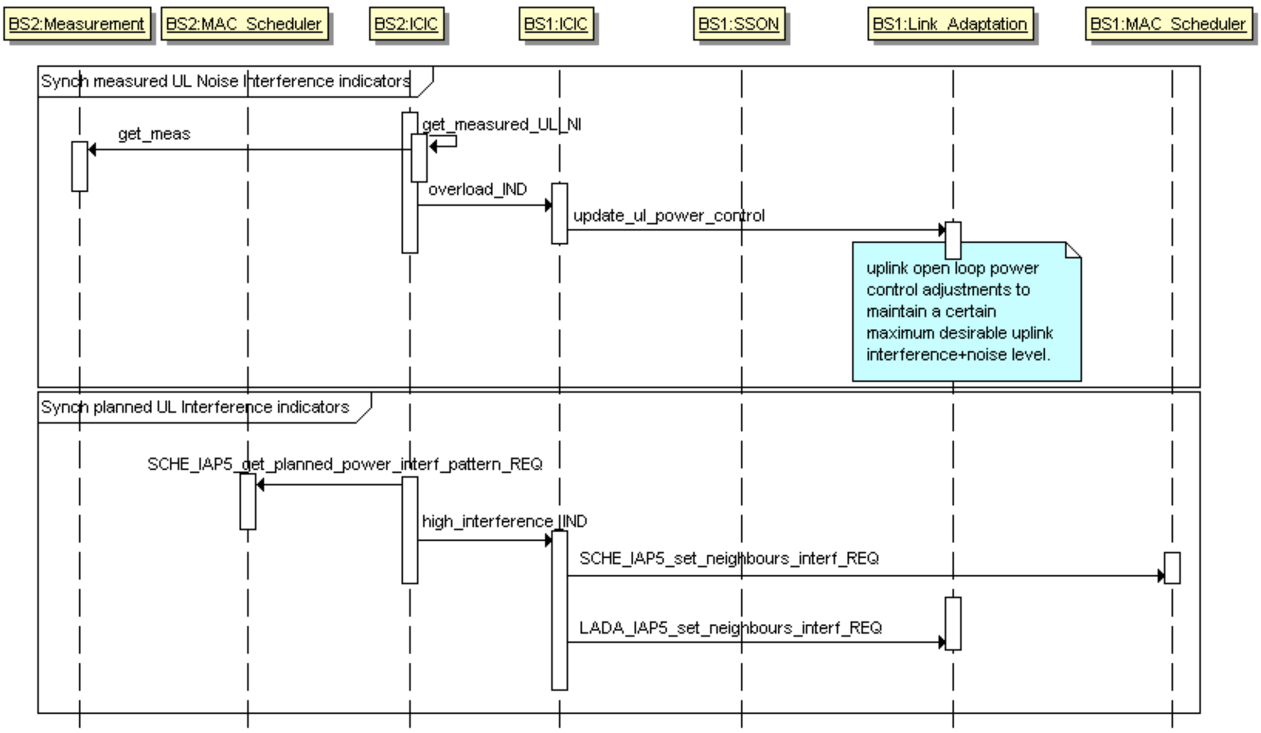


Figure 31: Inter-cell UL interference coordination.

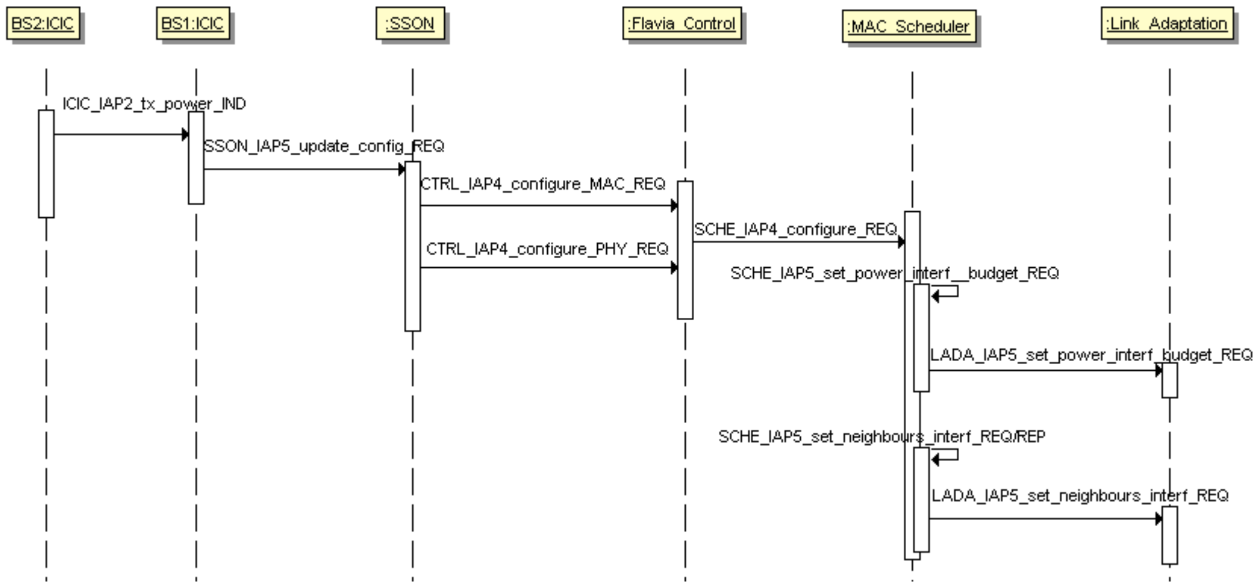


Figure 32: Dynamic DL FFR via SSON

3.2.10 Mobility Support (MOSU)

In the validation platform Alvarion's BS mobility will be provided.

General Description:

Mobility shall be supported across the wireless network. While mobility management is commonly a function in the core network, in case of WiMAX networks located in the ASN-GW, the BS and MS provide support for mobility by implementing hand-over procedures, location update procedures and related functions.

Mobility support is distinguished according to the operational state of the mobile station. We distinguish between *idle mode* and *connected mode*.

In idle mode, the MS is deregistered from the network, but performs cell scanning procedures in regular time intervals and, if required, performs location update procedures to convey the current location (i.e. the current cell) to the network. Furthermore, in idle mode the MS listens to paging message from the network in order to initiate network (re-)entry procedures if required. The MS can leave idle mode at any time if new data is pending.

In *connected mode*, the MS is registered at the network, such that it is manageable and reachable at any time. The network manages context data for different purposes like security, QoS, mobility, etc. In connected mode, seamless hand-overs of ongoing service flows to other BSs are supported.

Responsibilities:

- Performing hand-over between base stations in connected mode, including notification of other services about new serving BS and related parameters
- performing location updates in idle mode
- perform network entry and registration
- perform deregistration

Service interface primitives:

IAP	Primitive name	Description
IAP4	MOSU_IAP4_configure_REQ/REP	Allows the FLAVIA control to configure the service. REP - to acknowledge FLAVIA Control configuration request.
IAP5 IAP2	MOSU_IAP5_trigger_HO_REQ/REP MOSU_IAP2_trigger_HO_REQ/REP	Triggers HO by: 1. cell selection and tracking triggers HO according to HO hysteresis settings (triggering internally in MS - IAP5); 2. BS (IAP2) (e.g. Load Balancing decision).
IAP2	MOSU_ IAP2_HO_from_user_REQ	Hand-over request message from MS to serving BS
IAP2	MOSU_ IAP2_HO_from_user_REP	HO response message from serving BS to MS, containing information about preferred target BS from network side
IAP5	MOSU_IAP5_trigger_LU_REQ/REP	trigger conditions include paging group update, timer expiration, MS power down

IAP2	MOSU_IAP2_LU_REQ	Perform location update procedure with preferred BS
IAP2	MOSU_IAP2_LU_REP	BS indicates successful location update to MS.
IAP2	MOSU_IAP2_ranging_REQ	Perform ranging with target BS. This includes sending the ranging codes and RNG-REQ/REP messages.
IAP2	MOSU_IAP2_ranging_REP	Ranging response from the BS, including parameters for UL resources if successful, and/or indication of ranging state.
IAP2	MOSU_IAP2_register_REQ	Request registration at base station and core network
IAP2	MOSU_IAP2_register_REP	Response to registration.
IAP2	MOSU_IAP2_dereg_ms_REQ/REP	Request deregistration by MS
IAP5	MOSU_IAP5_trigger_dereg_ms_REQ/REP	Request deregistration triggered by BS (poor link detection, enter Idle mode)
IAP5	MOSU_IAP5_user_state_REQ/REP	Returns user state information (e.g. "during HO", "during DEREG").

Service indication primitives:

IAP	Primitive name	Description
IAP2	MOSU_IAP2_HO_confirm_IND	Hand-over configuration message for context transfer from serving to target BS.
IAP2	MOSU_IAP2_HO_configure_IND	Configure target BS with context data.
IAP2	MOSU_IAP2_HO_complete_IND	Target BS indicates completion of HO to serving BS.
IAP6	MOSU_IAP6_HO_complete_IND	Target or Source BS indicates completion of HO to core network/mobility controller.
IAP6	MOSU_IAP6_LU_IND	location update in the network after successful ranging procedure from the MS
IAP5 IAP6	MOSU_IAP5_finish_dereg_ms_IND MOSU_IAP6_finish_dereg_ms_IND	Remove MS context in registered modules inside BS MAC. Indicate deregistration to higher layers.
IAP5	MOSU_ IAP5_start_ms_dereg_IND	Inform registered modules about starting DREG
IAP5	MOSU_IAP5_users_distribu	Subscribe to event notification about

	tion_SUB	mobile user's location/distribution.
IAP5	MOSU_IAP5_users_distribution_IND	Let the mobility support service announce changes in the distribution of users.

Required primitives from other services:

IAP	Primitive name	Description
IAP6	ADCO_IAP6_connection_conf_REQ/REP	Request to admission control of target BS to establish a new service flow during connected mode HO REP: Indicate admission state to the requesting BS
IAP5	CSAT_IAP5_neighbour_list_REQ/REP	Request preferred target BS for HO from CSAT REP:Conveys preferred target BS to mobility support service
IAP5	DATA_IAP5_add_mac_msg_REQ	add DREG-CMD to data transport
IAP6	APPL_IAP6_HO_preparation_REQ/REP	Requests handover preparation procedure to higher layers in order to exchange status information and perform admission control with target BS. REP: Deliver result of HO procedure with possible target BSs to the source BS.
IAP6	APPL_IAP6_user_register_REQ/REP	registration request to higher layers and core network

MAC Functions:
Create deregistration message

Sequence Diagrams:

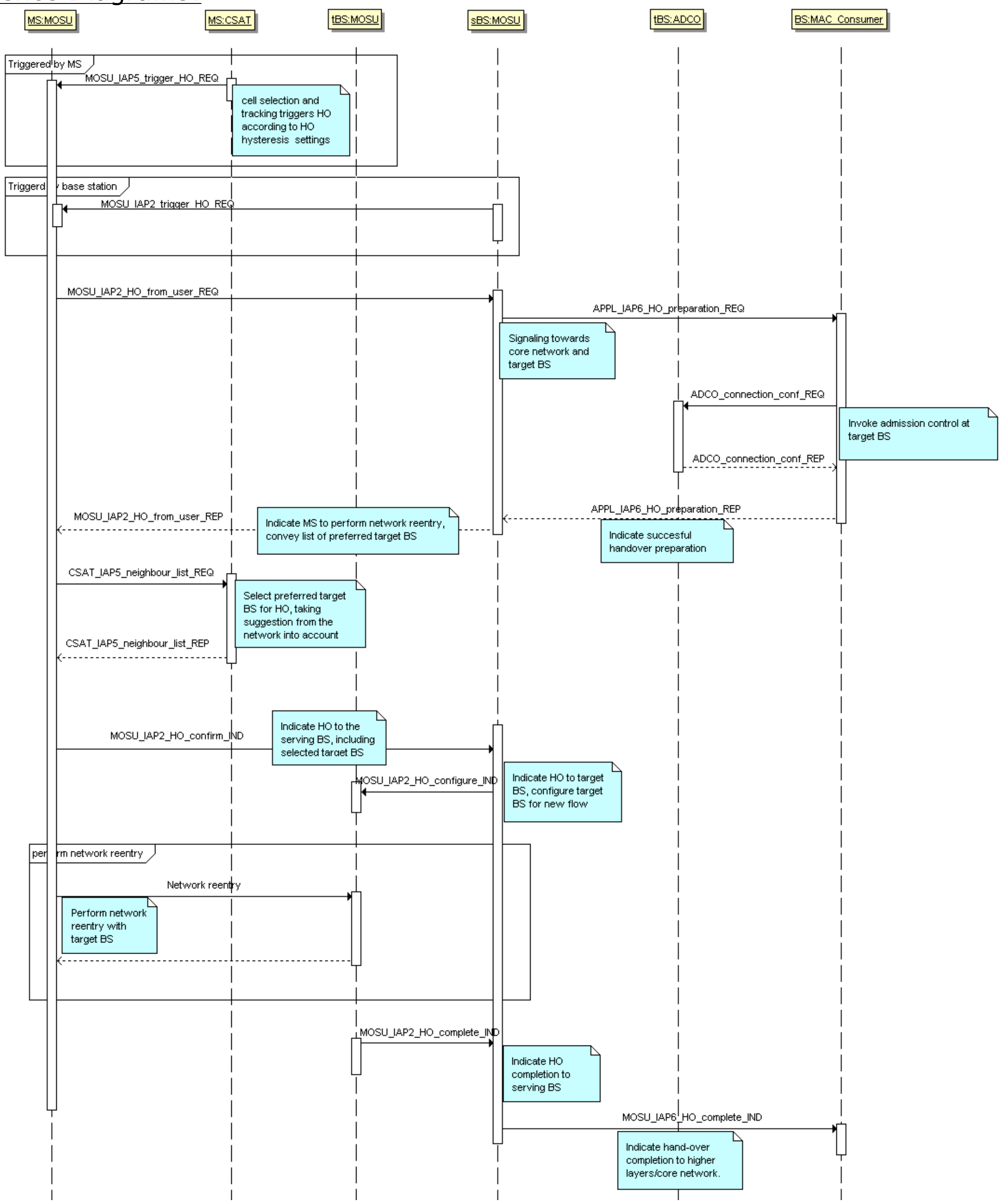


Figure 33: Connected mode mobility support

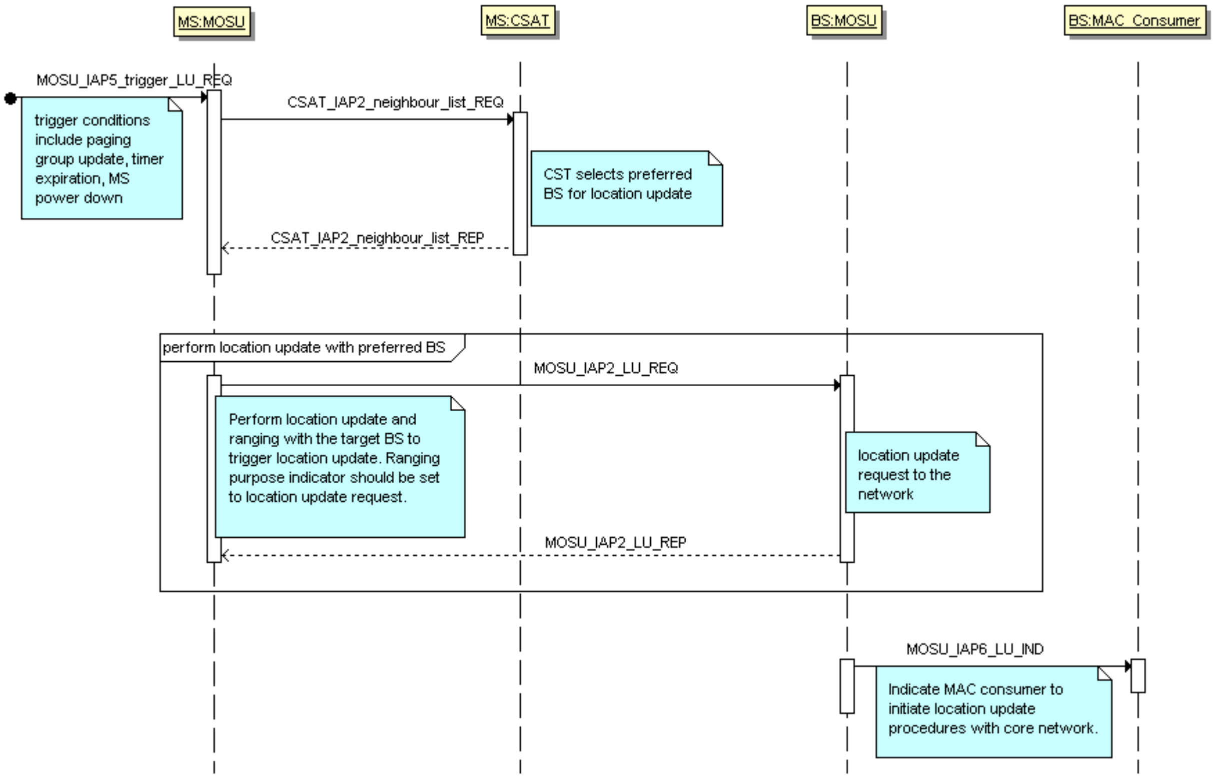


Figure 34: Idle mode location update

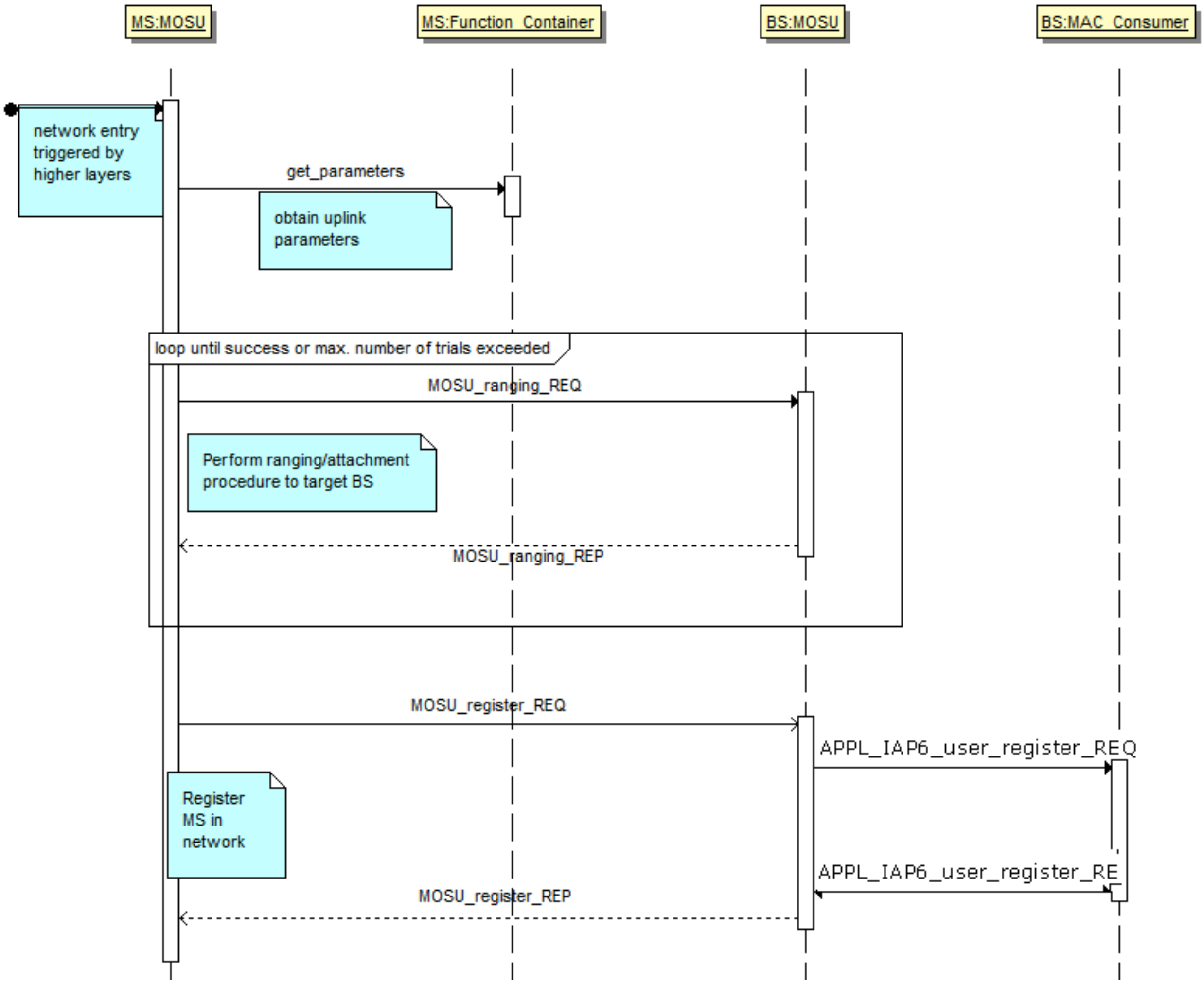


Figure 35: Network Entry

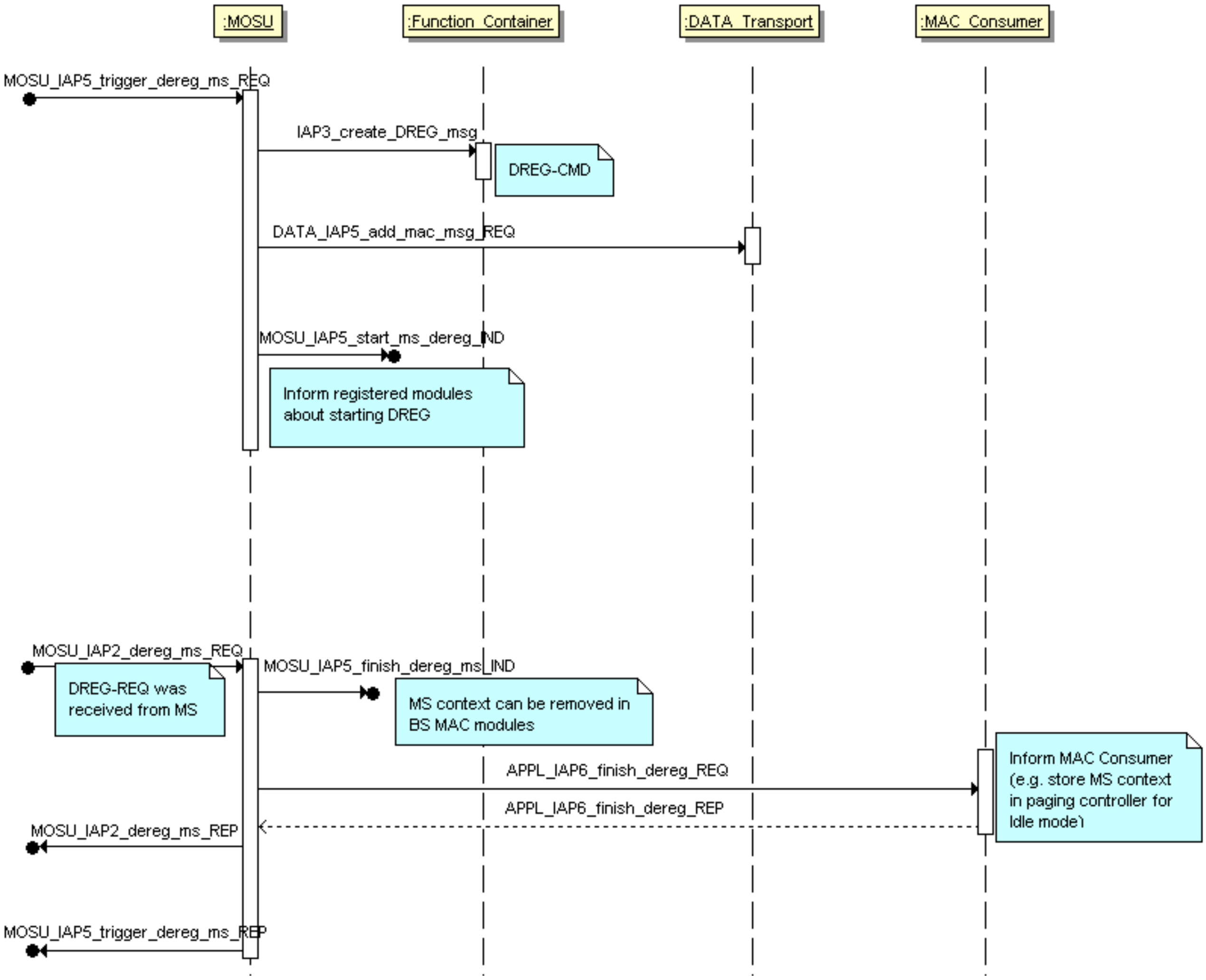


Figure 36: Deregistration

3.2.11 Support for SON (SSON)

SON will not be part of the validation platform.

General description:

This service uses per-user, per-channel, and per-base station statistics in order to self-optimize the cell configuration. Therefore, the goal of the service is to exploit a set of mechanisms for automatic intra-cell and inter-cell network monitoring, in order to enforce the self-optimization of MAC/PHY parameters.

In order to provide support to SON operations, both base station and user equipment have to be able to collect, parse, and exchange active and passive measurements on traffic and channel conditions, e.g., by tracking the quality of a channel or by actively probing the capacity of a link. Measurements are used to run self-configuration and self-optimization algorithms whose output is used to update the configuration of base stations. Measurement should be provided by the Measurement framework service to be run independently from the support for SON. Extra measurements might be required, thereby this service might request for other services to perform extra measurements, or the service itself might want to generate some ad-hoc network probing. A particular functionality to be implemented in this service consists in the surrounding cells being able to cooperate in order to adapt their coverage range and handover the traffic of other cells in case a neighbour cell fails.

Responsibilities:

1. *Fetch statistics and perform statistic analysis*
   The SSON service uses as input for its algorithms the statistics summarizing the measurements collected by the monitoring system at base station and mobile user side. Such statistics have to be fetched by using IAP5 and IAP2 primitives (to access the monitoring system locally and on the mobile stations), and IAP4 (to access statistics stored in the databases of the control and management part).

2. *Request channel probing*
   In case insufficient or out-of-date statistics were available, the SSON service might trigger the probing functions directly or ask the monitoring service to proceed with the channel probing.

3. *Detect neighbours*
   Optimization algorithms also need to figure out the network topology and discover the presence of concurrent systems.

4. *Self-configuration of PHY parameters*
   Run some proprietary algorithms to select the optimal PHY configuration, given the statistics available for channel condition, bandwidth utilization, traffic demand, currently active traffic agreements, and topological info.

5. *Self-configuration of MAC parameters*
   Run some proprietary algorithms to select the optimal MAC configuration, given the statistics available for channel condition, bandwidth utilization, traffic demand, currently active traffic agreements, and topological info.

6. *Detect failures*
   Topology changes trigger MAC/PHY reconfiguration. Therefore, the SSON service has to track the failures in the network neighbourhood to adjust cell coverage, optimize power levels and trigger load balance adjustments.

7. *BS-initiated handover*
   Force handover of terminals before reconfiguring cell coverage.

8. *Coordinate with ICIC*
   Exchange available stats and traffic demand info with neighbour cells. To this aim, the ICIC service can be exploited, since it is in charge for inter-cell coordination and communication. Additionally, the ICIC service has to be used in order to enforce the tuning of parameters that affect inter-cell interference and cell coverage, and to notify the neighbour cells about the current operational parameters used in the local cell.

The interaction between the SSON service, running both at the base station and at the mobile station, and the other MAC entities (MAC services and FLAVIA Control) is depicted in Figure 37.

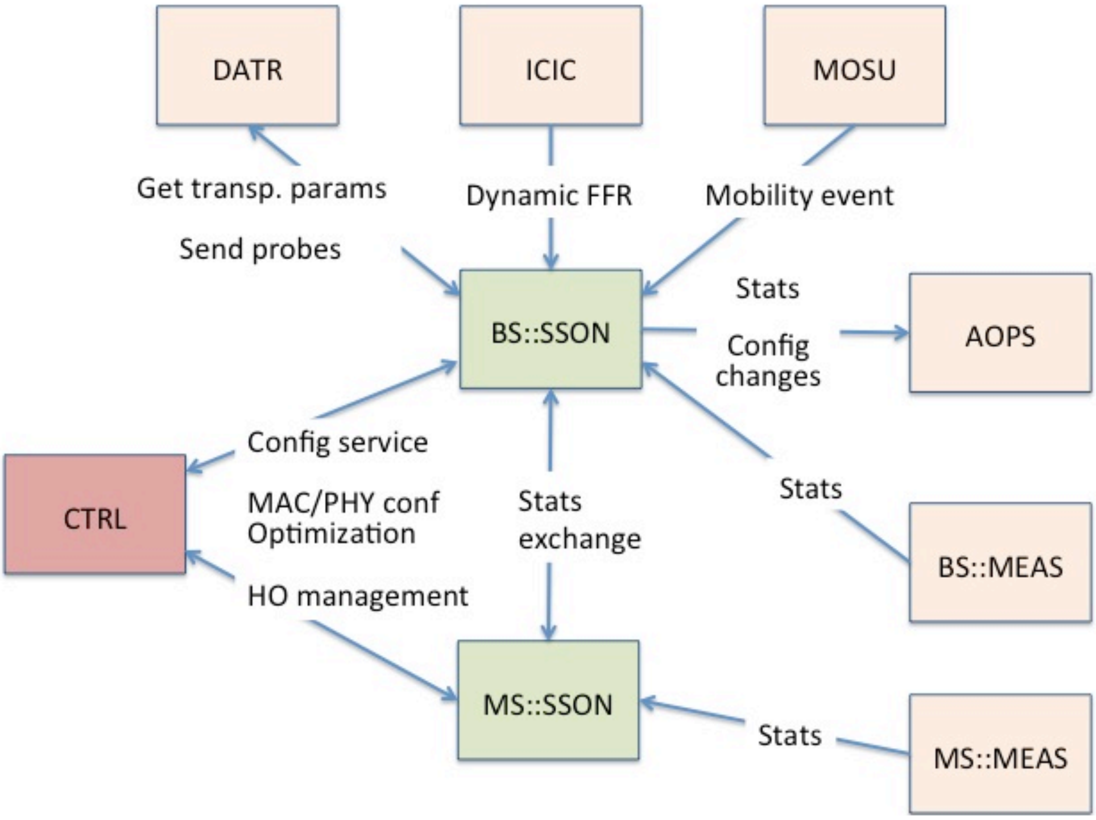


Figure 37: SSON interaction with other services.

Service interface primitives:

IAP	Primitive name	Description
IAP2	SSON_IAP2_statistics_REQ	An entity (e.g., the BS) requests stats to another entity (e.g., the MS).
IAP2	SSON_IAP2_statistics_REP	Used to convey the requested stats.
IAP4	SSON_IAP4_configure_REQ	This primitive allows the FLAVIA control to configure the SSON service.
IAP4	SSON_IAP4_configure_REP	This is to acknowledge FLAVIA Control configuration request.
IAP5	SSON_IAP5_statistics_REQ	Allow other services (e.g., MEAS, ICIC or AOPS) to fetch stats on channel quality and interference.
IAP5	SSON_IAP5_statistics_REP	Deliver locally collected stats to other services.

Service indication primitives:

IAP	Primitive name	Description
IAP4	SSON_IAP4_update_config SUB	Subscribe to configuration update notifications.
IAP4	SSON_IAP4_update_config_IND	Suggest to the FLAVIA control a configuration modification (PHY/MAC/Application).
IAP4	SSON_IAP4_new_config_SUB	Allow subscription to be notified about changes in the configuration suggested by the SSON service.
IAP4	SSON_IAP4_new_config_IND	Notify changes to the FLAVIA Control.
IAP5	SSON_IAP5_new_config_SUB	Allow subscription to be notified about changes in the configuration suggested by the SSON service.
IAP5	SSON_IAP5_new_config_IND	Notify changes to other services.

IAP	Primitive name	Description
IAP4	CTRL_IAP4_configure_MAC_REQ	Ask the FLAVIA Control system to commit some MAC configuration change,
IAP4	CTRL_IAP4_configure_MAC_REP	Allow the FLAVIA Control system to notify the result of the configuration request, i.e., return the current values of the MAC configuration parameters.
IAP4	CTRL_IAP4_configure_PHY_REQ	Ask the FLAVIA Control system to commit some PHY configuration change,
IAP4	CTRL_IAP4_configure_PHY_REP	Allow the FLAVIA Control system to notify the result of the configuration request, i.e., return the current values of the PHY configuration parameters.
IAP5	MOSU_IAP5_trigger_HO_REQ	Request to force the handover of a mobile station.
IAP5	MOSU_IAP5_trigger_HO_REP	Reports on the HO request.
IAP4	CTRL_IAP4_config_update_IND	Notify the current MAC/PHY configuration
IAP5	DATA_IAP4_transport_params_REQ	Fetch the currently in use parameters for the Data Transport service (to be used for probing)
IAP5	DATA_IAP4_transport_params_REP	Obtain the set of parameters in use in the Data Transport service.
IAP5	DATA_IAP5_add_mac_msg_REQ	Send probes and control messages using the data transport service.
IAP5	DATA_IAP5_add_mac_msg _REP	Receive a report about the probe/message that had to be sent.
IAP5	MOSU_IAP5_users_distribution_SUB	Subscribe to event notification about mobile user's location/distribution.
IAP5	MOSU_IAP5_users_distribution_IND	Let the mobility support service announce changes in the distribution of users.
IAP5	ICIC_IAP5_get_neighbours_info_REQ	Request info about the neighbour cells and their users.
IAP5	ICIC_IAP5_get_neighbours_info_REP	Deliver info about the neighbour cells and their users.
IAP5	MEAS_IAP5_get_meas_REQ	Allow other services (e.g., AOPS and SSON) to fetch stats on channel quality, interference, channel utilization, etc…

Required primitives from other services:

IAP5	MEAS_IAP5_get_meas_REP	Deliver measured stats.
IAP5	AOPS_IAP5_new_config_SUB	Allow subscription to be notified about changes in the configuration suggested by the AOPS service.
IAP5	AOPS_IAP5_new_config_IND	Notify changes to other services.

MAC functions (invoked via IAP3_invoke_REQ):

1. Collect Radio Statistics (← from MEAS)
2. Collect Neighbor Statistics (← from ICIC)
3. Collect Traffic Statistics (← from MEAS)
4. Cell Scanning (← from ICIC)
5. Channel Probing
6. LocateNeighbors (← from ICIC)
7. Optimize Antenna
8. Optimize Power
9. Optimize Coverage
10. Configure Antenna
11. Configure Power (→ through FLAVIA Control)
12. Configure Coverage (→ through FLAVIA Control)
13. Configure Bandwidth (→ through FLAVIA Control)
14. Configure Scheduler (→ through FLAVIA Control)
15. Detect Failure
16. BS Initiated HO (→ through FLAVIA Control)

3.2.12 Application Optimization Support (AOPS)

General description:

The support for application optimization consists in using local traffic statistics and channel statistics in order to improve the performance of running applications. The Application Optimization Support service is in charge of running the algorithms for such optimization. Therefore, this service has to be able to fetch the needed statistics, detect the running applications automatically, and eventually tune the MAC/PHY parameters to better suit those applications' needs.

The Application Optimization Support service is meant for cross-layer optimization. On one hand, it allows to configure the application parameters by providing the application layer with MAC/PHY real time statistics. On the other hand, the application optimization support allows to define a set of filtering rules that are used to detect which applications are currently using the data transport service and consequently trigger automatic MAC/PHY optimization and re-reconfiguration routines. Note that the optimization of applications is a local procedure, but it has to consider the constraints imposed by intra-cell optimization mechanisms as well as by the support for SON (we assume that SSON, ICIC, and AOPS coordinate through the FLAVIA control system, the latter being in charge of committing the configuration changes suggested by the services).

<u>Responsibilities:</u>

1. *Provide support for handling traffic classes*
   Define and apply filters to be used to detect running application (e.g., by using header information of TCP/IP and MAC). Suggest how to tune the queuing system on a per-class basis. Interact with the queuing system in order to manage separately the different applications detected by the AOPS service (therefore, AOPS has to configure, directly or via the Control subsystem, all traffic classes handled by DATA and QOSS).

2. *Configure PHY parameters*
   Run some proprietary algorithms to select the optimal PHY configuration, given the statistics available for the bandwidth utilization and the currently active applications.

3. *Configure MAC parameters*
   Run some proprietary algorithms to select the optimal MAC configuration, given the statistics available for the bandwidth utilization and the currently active applications.

4. *Detect running applications*
   Use traffic filtering to build a database with active application. Filtering rules should be a combination of default rules and user-defined rules.

5. *Interact with the application layer*
   Network status, and/or optimal application parameters, should be made available at the application layer.

The interaction between the AOPS service, the FLAVIA control subsystem and the other MAC services is depicted in Figure 38. Note that the AOPS is also interfaced to the MAC consumer.

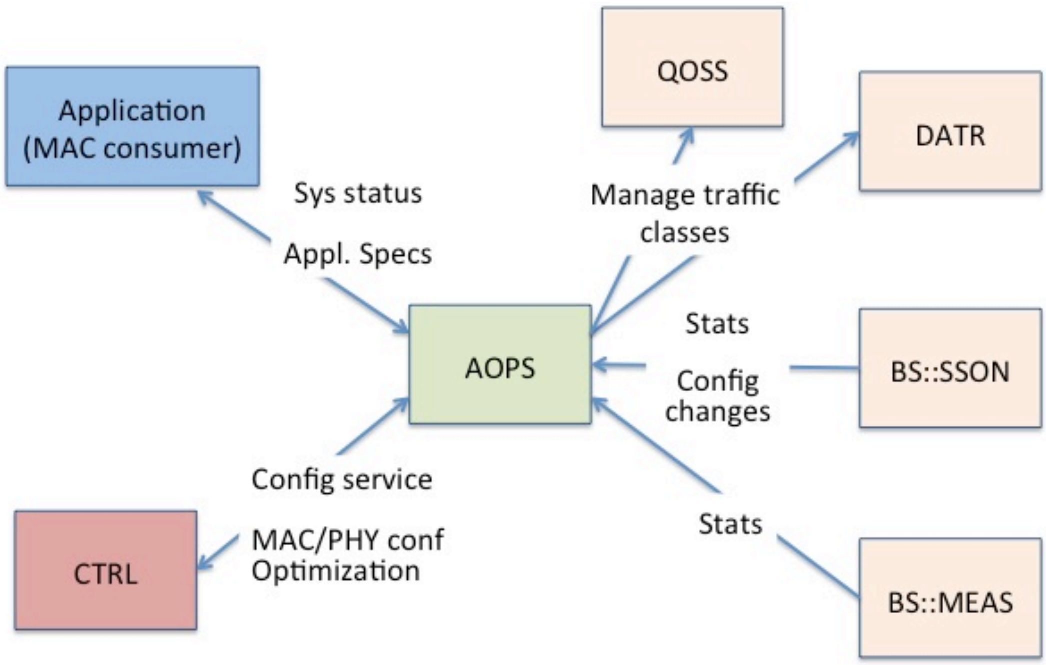


Figure 38: AOPS interaction with other services.

Service interface primitives:

IAP	Primitive name	Description
IAP4	AOPS_IAP4_configure_REQ	Allow the FLAVIA Control system to tune the AOPS service.
IAP4	AOPS_IAP4_configure_REP	This is to acknowledge FLAVIA Control configuration request.
IAP6	AOPS_IAP6_config_application_REQ	Allow the upper layers (i.e., the MAC consumer) to request a new application configuration (to be used in case the application optimization is supported and operated at MAC layer).
IAP6	AOPS_IAP6_config_application_REP	Acknowledge the new application configuration request.

IAP5	AOPS_IAP5_get_stats_REQ	Allow other services (e.g., MEAS) to fetch stats on channel quality and interference.
IAP5	AOPS_IAP5_get_stats_REP	Deliver locally collected stats to other services.

Service indication primitives:

IAP	Primitive name	Description
IAP4	AOPS_IAP4_update_config_SUB	Subscribe to configuration update notifications.
IAP4	AOPS_IAP4_update_config_IND	Suggest to the FLAVIA control a configuration modification (PHY/MAC/Application).
IAP4	AOPS_IAP4_new_config_SUB	Allow subscription to be notified about changes in the configuration suggested by the AOPS service.
IAP4	AOPS_IAP4_new_config_IND	Notify changes (to be used by the FLAVIA Control system and possibly by the ICIC service).
IAP6	AOPS_IAP6_notify_status_SUB	Subscribe to status change notifications.
IAP6	AOPS_IAP6_notify_status_IND	Deliver status info to the MAC consumer.

IAP	Primitive name	Description
IAP4	AOPS_IAP4_new_config_SUB	Allow the FLAVIA Control to subscribe for notifications about changes in the configuration suggested by the AOPS service.
IAP4	AOPS_IAP4_new_config_IND	Notify changes (to be used by the FLAVIA Control).
IAP5	AOPS_IAP5_new_config_SUB	Allow subscription of other services to be notified about changes in the configuration suggested by the AOPS service.
IAP5	AOPS_IAP5_new_config_IND	Notify changes to other services.
IAP6	AOPS_IAP6_net_info_SUB	Subscribe to receive suggestions about the current state of the PHY/MAC, so that applications can be optimized at upper layers.
IAP6	AOPS_IAP6_net_info_IND	Push towards the application layer info relevant for the optimization of running applications (to be used in case the application optimization is supported at MAC layer, but optimization is operated at allocation layer).

Required primitives from other services:

IAP	Primitive name	Description
IAP4	CTRL_IAP4_configure_MAC_REQ	Ask the FLAVIA Control system to commit some MAC configuration change,
IAP4	CTRL_IAP4_configure_MAC_REP	Allow the FLAVIA Control system to notify the result of the configuration request, i.e., return the current values of the MAC configuration parameters.
IAP4	CTRL_IAP4_configure_PHY_REQ	Ask the FLAVIA Control system to commit some PHY configuration change,
IAP4	CTRL_IAP4_configure_PHY_REP	Allow the FLAVIA Control system to notify the result of the configuration request, i.e., return the current values of the PHY configuration parameters.
IAP4	CTRL_IAP4_config_update_IND	Notify the current MAC/PHY configuration
IAP5	SSON_IAP5_get_stats_REQ	Allow other services (e.g., ICIC or AOPS) to fetch stats on channel quality and interference.
IAP5	SSON_IAP5_get_stats_REP	Deliver locally collected stats to other services.
IAP5	MEAS_IAP5_get_meas_REQ	Allow other services (e.g., AOPS and SSON) to fetch stats on channel quality, interference, channel utilization, etc…
IAP5	MEAS_IAP5_get_meas_REP	Deliver measured stats.
IAP5	DATA_IAP5_register_class_REQ	Request to update the class-filtering rules, i.e., ask the data transport system to manage a new class or update the rules for an existing class.
IAP5	DATA_IAP5_register_class_REP	Acknowledge the class-filtering request.
IAP5	DATA_IAP5_deregister_class_REQ	Request the data transport system to dismiss an existing traffic class.
IAP5	DATA_IAP5_deregister_class_REP	Acknowledge the change in the class-filtering rules.

MAC functions (invoked via IAP3_invoke_REQ):

1. Collect Radio Statistics (← from MEAS)
2. Collect Traffic Statistics (← from MEAS)
3. Define Application Filter
4. Detect Running Applications (← from DATA)
5. Optimize Antenna
6. Optimize Power
7. Configure Antenna (→ through FLAVIA Control)
8. Configure Power (→ through FLAVIA Control)
9. Configure Bandwidth (→ through FLAVIA Control)
10. Configure Scheduler (→ through FLAVIA Control)
11. Define Traffic Class (→ through FLAVIA Control)
12. Configure Traffic Class (→ through FLAVIA Control)

3.2.13 Cell Selection and Tracking (CSAT)

Cell Selection and tracking will part of the validation platform and will be provided by Alvarion 's CPEs.

The content of this chapter includes Network Detection and selection (ND&S) including preferred BS and NAP (Network Access Provider) selection algorithms.

This algorithm includes:

- Frequency Scanning per BW over all frequency band configured and by using the configured steps.
- Listing of the detecting frequencies with their CINR and BW.
- Selecting the best BS from the preferred list considering the selection priorities.

The details of this algorithm are defined in the following **subsections.**

3.2.13.1 Frequency Scanning during MS network entry

The Frequency Scanning during Network entry is done upon set of frequencies used during the scanning process. Mostly they have defaults but they can be configured by the user. The list of frequencies that participate in the scanning process can be configured both by a range of frequencies from start to stop or as a discrete frequencies (up to 10). In general the default range covers all the MS frequencies in which the discrete frequencies should not be configured. But if the operator want to jump some of the frequencies scanning to allow faster network entry he can configure discrete frequencies.

The scanning range window is defined by Start Frequency, End Frequency, Scanning Main Step and Intermediate Steps. The set of frequencies to be scanned is defined as follows:

The "Main Frequencies" are defined by the Start Frequency and the Main Step, using the following formulas:

F (N) =Start Frequency + N*Main Step;
F (1) = Start Frequency + Main Step,

F (2) = Start Frequency +2*Main Step,...
End Frequency is the upper limit of the MS frequency range.

The Intermediate Steps can be used to define additional frequencies using a finer resolution. The intermediate steps are defined as follows:

Step	Effect on scanned frequencies set when Step is Enabled
1	Start Frequency is added to the set of "Main Frequencies"
2	All intermediate frequencies defined by "Main Frequency" + 125 KHz are added to the scanning set
3	All intermediate frequencies defined by "Main Frequency" + 250 KHz are added to the scanning set
4	All intermediate frequencies defined by "Main Frequency" + 375 KHz are added to the scanning set
5	All intermediate frequencies defined by "Main Frequency" + 500 KHz are added to the scanning set
6	All intermediate frequencies defined by "Main Frequency" + 625 KHz are added to the scanning set
7	All intermediate frequencies defined by "Main Frequency" + 750 KHz are added to the scanning set
8	For a bandwidth of n*3.5 MHz: All intermediate frequencies defined by "Main Frequency" + 875 KHz are added to the scanning set For a bandwidth of n*5 MHz: All intermediate frequencies defined by "Main Frequency" + 1250 KHz are added to the scanning set

Table 16: Intermediate Steps

For example, If Steps 1,2 and 5 are enabled and all other steps are disabled, the scanned frequencies are: Start Frequency, Start Frequency + 125 KHz, Start Frequency + 500 KHz, Start Frequency +N*Main Step, Start Frequency +N*Main Step + 125 KHz, Start Frequency +N*Main Step + 500 KHz (N=1, 2,...). End Frequency is the upper limit for the scanned frequencies.
In addition, the Discrete Frequencies option enables defining up to 10 discrete frequencies to be used in the scanning process in addition to the frequencies defined by the Frequency Scanning parameters.

The following example describes how to build the scanning table upon the following configuration example:

Start freq = 3500000 KHz
End frequency = 3507000 KHz
Main step = 1250 KHz
Intermediate Steps = Start frequency + 250 KHz only

Discrete frequencies defined as follows:

3508000 KHz
3509000 KHz

The table of frequencies to be scanned upon the above configuration shall be as follows:

3500000 KHz
3500250 KHz
3501250 KHz
3501500 KHz
3502500 KHz
3502750 KHz
3503750 KHz
3504000 KHz
3505000 KHz
3505250 KHz
3506250 KHz
3506500 KHz
3508000 KHz
3509000 KHz

Any frequency in the scanning table built shall be unique and removed from the list each duplication in which only a single value of each frequency will be scanned. A separate list shall be built for each scanned BW. If any frequency's edge in the list exceeds the unit's frequency band of the MS it shall be also removed. The following formulas:

Frequency in the list – BW/2 < (frequency band lower value)
Frequency in the list + BW/2 > (frequency band higher value)

For achieving the Frequency Scanning during MS Network Entry the service interface primitives described in Table 17 are required.

IAP	Primitive name	Description
IAP4	MS_IAP4_Frequency_Set_REQ/REP	int32 Frequency_window_start; int32 Frequency_window_stop; int32 Frequency_main_step; int8 Frequency_intermediate_step_bitmap; int32 Discrete_Frequency_1; int32 Discrete_Frequency_2; int32 Discrete_Frequency_3; int32 Discrete_Frequency_4; int32 Discrete_Frequency_5; int32 Discrete_Frequency_6; int32 Discrete_Frequency_7; int32 Discrete_Frequency_8; int32 Discrete_Frequency_9; int32 Discrete_Frequency_10;

Table 17: Service Interface primitives for Freq Scan in MS NE

3.2.13.2 ND&S (Network Detection & Selection) Process

The ND&S process shall support reuse 3, reuse 1 and reuse 1/3. It can put in best BST list few BSTs with the same frequency. The process will be based on the following flow:

1. If Power up or reset start up set T/O=60sec

2. Else If link failure and Nomadicity set T/O=5min

3. Else If link failure and Mobility set T/O=500ms

4. CPE starts Scanning first for the T/O defined the above, the last used BST if available in the Data Base and only if it's a Preferred BST. If found and it is a Preferred BST and NE is succeed stop ND&S process and use the last used BST.
   If last used BST not found or it is not a Preferred BST or NE is not succeed go to the next step.

5. If not found or it is not a Preferred BST delete the last used BST and scan the Best BST short list updated from the last scan. The BW to be used is the BW found from the last scan. Select the Best BST with the better SNR from the list considering the configured NAP priorities list in case of Mobility and in case of Nomadicity from the Preferred BST list. It means

that the CPE arranges the list in accordance with the best SNR order and then selects the BST complies with the NAP ID Priority 1 or Preferred BST list that has the better SNR. If not found in the first priority NAP ID / preferred BST list then tries to find in the NAP ID Priority 2 / BST Priority 2 list with the best SNR. If not found any BST complies with the NAP priority 2 / BST Priority 2 list it will select the BST with the best SNR. Update the last used BST only after NE completion. If not succeed NE then try to select next best found in the list upon NAP ID / Preferred BST list. If not found any or not succeed any to make NE go to the next step.

6. If not found Scan the Discrete frequencies for all the BW configured, update the Best BST short list and select the best BST considering the better SNR and the NAP priorities list / Preferred BST list (depending on Mobility / Nomadicity – If Mobility from the NAP ID list, if Nomadicity from the Preferred BST list). It means that the CPE arranges the list in accordance with the best SNR order and then selects the BST complies with the NAP ID priority 1 / Preferred BST list that has the better SNR. If not found in the NAP ID Priority 1 / Preferred BST list then tries to find in the NAP ID priority 2 / BST priority 2 list the BST with the best SNR. If not found any BST complies with the NAP priority 2 / BST Priority 2 list it will select the BST with the best SNR. Update the last used BST only after NE completion. If not succeed NE then try to select next best found in the list upon NAP ID / Preferred BST list. If not found any or not succeed any to make NE go to the next step. If not found any of the best BST list delete the best BST list.

7. If not found go to Full scan.

8. If the full scan Stop frequency – Start frequency is 30MHz or less then scan all the applicable frequencies in the applicable BWs as configured (where the first scanned frequency is start freq + BW/2 and the last scanned frequency is stop frequency – BW/2), update the Best BST short list and select the best found BST considering the best SNR upon the configured NAP priorities list / Preferred BST list. It means that the CPE arranges the list in accordance with the best SNR order and then selects the BST complies with the NAP ID Priority 1 / Preferred BST list that has the better SNR. If not found in the NAP ID Priority 1 / Preferred BST then tries to find in the NAP ID priority 2 / BST Priority 2 list the BTS with the best SNR. If not found any BST complies with the NAP priority 2 / BST priority 2 list it will select the BST with the best SNR. Update the last used BST only after NE completion. If not succeed NE then try to select next

best found in the list upon NAP ID / Preferred BST list. If not found any or not succeed any to make NE go to the next step.

1. Else start scanning the full scan each frequency for each applicable BW (where the first scanned frequency is start freq + BW/2 and the last scanned frequency is stop frequency – BW/2) If first found is checked then select the first found BST conditioning the NAP ID / Preferred BS list priority. It means that NAP ID priority 2 / BST Priority 2 list can be selected just if not found BST in NAP ID priority 1/ Preferred BST list after full scan termination. Update the BST short list. Update the last used BST only after NE completion. If not succeed NE then continue to scan.

   If first found is not selected (this can be done only in nomadic mode in mobile mode it is always checked) then scan all the applicable frequencies in the applicable BWs as configured update the Best BST short list and select the best found BST considering the best SNR upon the configured NAP priorities list / Preferred BST list. It means that the CPE arranges the list in accordance with the best SNR order and then selects the BST complies with the NAP ID Priority 1 / Preferred BST list that has the better SNR. If not found in the NAP ID Priority 1 / Preferred BST then tries to find in the NAP ID priority 2 / BST Priority 2 list the BTS with the best SNR. If not found any BST complies with the NAP priority 2 / BST priority 2 list it will select the BST with the best SNR. Update the last used BST only after NE completion. If not succeed NE then try to select next best found in the list upon NAP ID / Preferred BST list. If not found any or not succeed any to make NE go to then continue to scan.

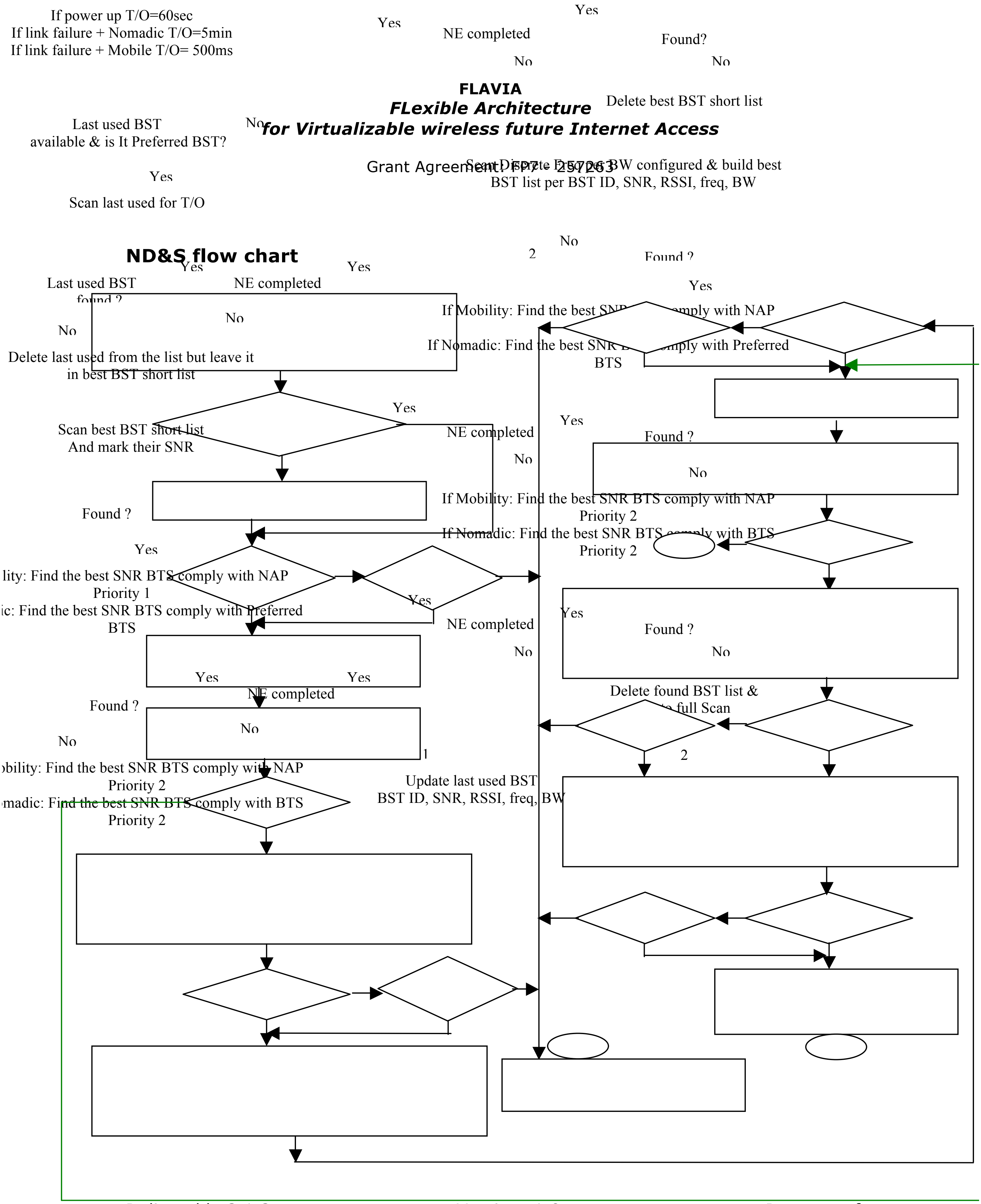
Factory Defaults Full scan means all the applicable frequencies in the band defined by the H/W (factory defaults) for all the applicable BWs in this band.

Only in case of Mobility mode is configured when the found BST does not comply with any NAP priority list the ND&S will select the best BST only by best SNR performance. This is required to allow service in any case only for Mobility mode assuming that when the serving BST will return the H/O will cause the CPE to go to the best SNR BST.If HO process changes the used BST, the last used BST shall be updated appropriately.

The Scan shall be limited by a T/O calculated by a formula:

Max (900sec, (Num_of_scanned_freq*1.5sec)

ND&S flow chart



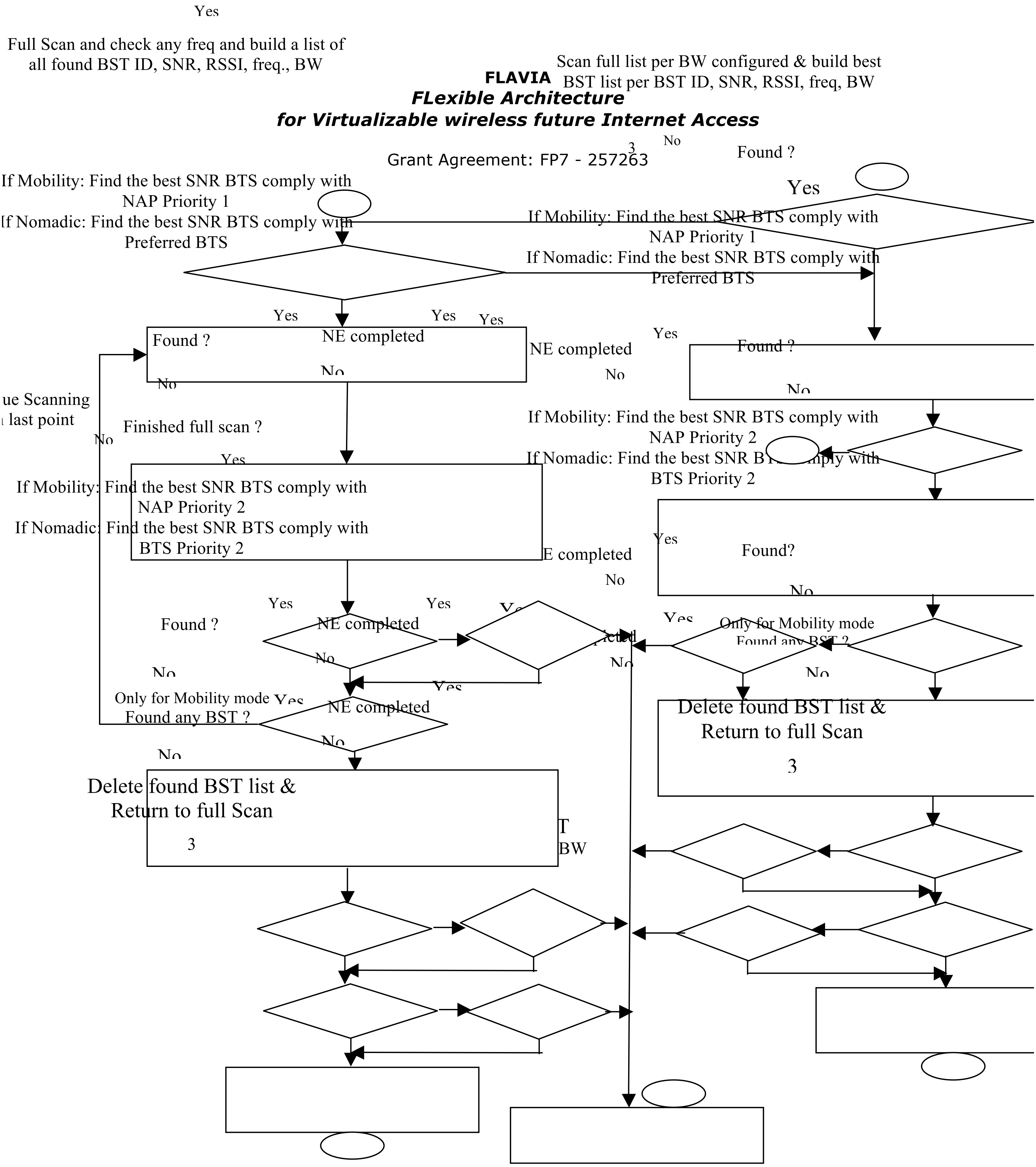


Figure 39: CPE ND&S flow chart

3.2.13.3 BST & NAP Selection control

The system will allow to Enable / Disable Preferred NAP ID / BS:

- If Enable: then Preferred NAP ID algorithm will be used.
- If Disable: NAP ID priority will not be considered in the ND&S process means only best SNR will rule in BST selection process.

Default: Enable

IAP	Primitive name	Description
IAP4	MS_IAP4_Preferred_BST_NAP _selection_REQ/RSP	int8 Preferred_NAP_BST

3.2.13.4 Preferred NAP ID Priority 1 / Preferred BST

If Mobile mode is set Preferred NAP ID Priority 1 will be configured as follows:

- Preferred NAP ID priority 1 shall be considered first for BS selection during the ND&S process.
- The configurable value is: xxx.xxx.xxx

  xxx = 0 to 255.

  The default is 0.0.0.
- Changing NAP ID priority 1 will cause the CPE to restart the ND&S process starting from short BS scan step only if the last used BS NAP ID does not comply with the new value.

If Nomadic mode is set Preferred BS will be configured as follows:

- Preferred BS ID: xxx.xxx.xxx.xxx.xxx.xxx

  xxx = 0 to 255.

  Default Preferred BS ID is 0.0.0.0.0.0
- Preferred BS Mask: xxx.xxx.xxx.xxx.xxx

  xxx = 0 to 255.

  Default Preferred BS Mask is 0.0.0.0.0.0.

- In case of Mobility Preferred BS fields shall be gray and can not be changed.
- In Case of Nomadic NAP ID shall be gray and can not be changed.

IAP	Primitive name	Description
IAP4	MS_IAP4_Preferred_BST_NAP_Priority1_REQ/RSP	int32 Preferred_NAP_BST_Priority_1_base int32 Preferred_NAP_BST_Priority_1_subnet

3.2.13.5 NAP ID Priority 2 / BST Priority 2 list

If Mobile mode is set NAP ID Priority 2 will be configured as follows:

- NAP ID priority 2 shall be considered in case the found BST list does not comply with the Preferred NAP ID Priority 1.
- If both NAP do not comply with the found BST list, to allow service the system will allow best BST selection only considering best SNR.
- The configurable value is: xxx.xxx.xxx
  xxx = 0 to 255.
  The default is 0.0.0.
- Changing NAP ID priority 2 will cause the CPE to restart the ND&S process starting from short BST scan step only if the last used is not comply with one of the NAP priorities defined.

If Nomadic mode is set Preferred BST will be configured as follows:

- BS ID Priority 2: xxx.xxx.xxx.xxx.xxx.xxx

  xxx = 0 to 255.

  Default BS ID Priority 2 is: 0.0.0.0.0.0
- BS Priority 2 Mask: xxx.xxx.xxx.xxx.xxx

  xxx = 0 to 255.

  Default BS Priority 2 Mask is 0.0.0.0.0.0.

- BS found shall be compared with the Priority 2 comparing as follows: Any BS ID AND BS Priority 2 Mask = BS ID Priority 2 AND BS Priority 2 Mask.
- In case of Mobility Preferred BS fields shall be gray and can not be changed.
- In Case of Nomadic NAP ID shall be gray and can not be changed

IAP	Primitive name	Description
IAP4	MS_IAP4_Preferred_BST_NAP_Priority2_REQ/RSP	int32 Preferred_NAP_BST_Priority_2_base int32 Preferred_NAP_BST_Priority_2_subnet

3.2.14 Measurement and Monitoring (MEAS)

General Description

The Measurement and Monitoring service is responsible to collect measurements (from PHY and MAC) and to monitor performance indicator build over these measurements that could trigger special actions. Additionally this service reports specific measurements to the alien MAC entities using IAP2 interface.

The collection of measurements from lower layers is done locally through IAP1. The collection of measurements from MAC is done through IAP5; the collection of measurements from alien entities is done using IAP2.

The measurements service provides raw information by default but compute as well statistical information, especially for the monitoring aspect. Indeed, the statistical information is used to compute key performance indicator that could trigger events when e.g. thresholds are met.

Measurements cover pure PHY related measurements (such as channel quality, power level etc.) but includes as well measurements related the MAC layer - the data flow (buffer report, traffic queue, quality levels such as latency, packet error rates etc.).

Example of usage of the Measurement and Monitoring service by other MAC modules are given below:

- By the Link Adaptation. The link adaptation uses instantaneous information related to link quality, noise level, packet error rate, etc.
- By the SON. The SON could benefit from information related to interference level, cell load information, etc.
- By the Application Optimization support. It could benefit from information related to buffer occupancy, channel quality information, etc.

Responsibilities:

- Collects MAC measurements and statistics;
- Collects PHY measurements and statistics;
- Reporting measurements and statistics to the alien MAC entity;
- Monitor key performance indicator and notify registered modules in case of some events occur. Events could be defined using the configuration primitive. Examples of events:
    - low traffic activity for a given MS;
    - Link failure;
    - High level of interference from other cells;
    - Etc.

Service interface primitives:

IAP	Primitive name	Description
IAP4	MEAS_IAP4_configure_REQ MEAS_IAP4_configure_REP	Allow the configuration of the measurement framework.
IAP5	MEAS_IAP5_get_meas_REQ MEAS_IAP5_get_meas_REP	Provide measurements and statistic to support local MAC functionalities. Can be defined as periodic reports. For example, it could provide interference levels information to ICIC module.
IAP2	MEAS_IAP2_get_meas_REQ MEAS_IAP2_get_meas_REP	Provide measurements and statistic to an alien MAC entity to support alien's MAC functionalities. Can be defined as periodic reports.

Service indication primitives:

IAP	Primitive name	Description
IAP5	MEAS_IAP5_monitoring_IND/SUB	This indication is triggered when an event occurs during the monitoring phase. As examples: • Link failure indication • Cell congestion event • No traffic event • Etc.
IAP5	MEAS_IAP5_meas_IND/SUB	Provides a mechanism to be notified about specific measurements related to pre-defined

		events/thresholds (e.g. provides NI measurement only if different from previous in certain delta).
IAP2	MEAS_IAP2_meas_IND/SUB	Provides a mechanism to be notified about specific measurements related to pre-defined events/thresholds (e.g. report tx power only if different from previous in certain delta).

<u>Required primitives from other services:</u>

IAP	Primitive name	Description
IAP5	DATA_IAP5_staticstics_REQ /REP	To provide to the MEAS module the information related to buffer and queue
IAP5	LADA_IAP5_statistics_REQ/ REP	Provides statistics about channel quality, power control and interference management.
IAP5	QOSS_IAP5_statistics_REQ/ REP	Provides statistics about users DL/UL traffic activity, throughput, guarantees satisfaction, etc.
IAP5	SCHE_IAP5_statistics_REQ/ REP	Provides statistics about frame utilization per different regions (reuse1, reuse3, dl/ul map and etc.)

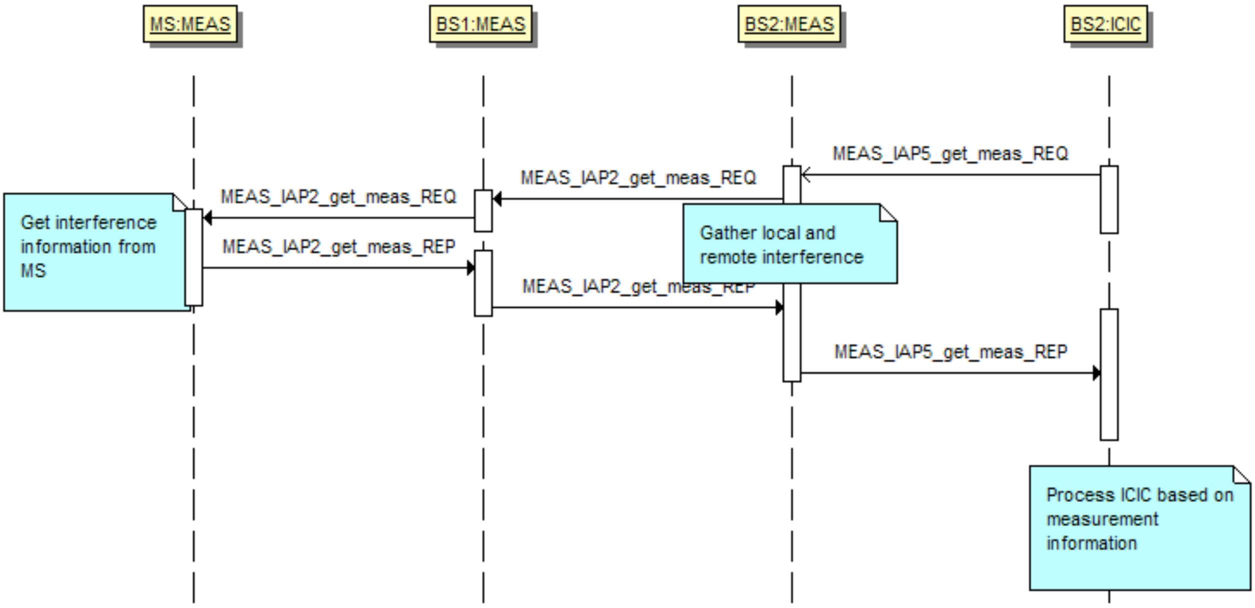


Figure 40: Basic example of usage of Measurement and Monitoring services

Figure 40 illustrates a basic usage of Measurement and Monitoring service by the ICIC module. The figure assumes that the MEAS service was configured and started before being triggered by the ICIC.
The BS#2 likes to update its ICIC policy and thus requires the knowledge of interference levels, especially seen by neighbouring cells. It thus interrogates the MEAS module of BS#2 to get access to the information, using IAP5.
The BS#2 then interrogates neighbouring cell BS#1, using IAP2.
The BS#1 then requests to the MS an update of the interference level. It uses IAP2 for that.
The MS reports the measurement information to the MEAS entity at BS#1. The MEAS at BS#1 then responds to BS#2 MEAS module which finally answers to ICIC modules.

In D3.1.1, we have defined the architecture and interface related to Flavia scheduled systems (WiMAX), inherited from the WP2 overall interface and architecture.
With respect to the measurement and monitoring framework, the architecture was extrapolated to the user terminal.

The requirements of the measurement and monitoring framework were:

- to be able to control the wireless processor (in the terminal case, it corresponds typically to the system on chip embedded in the user device such as a USB dongle connected to a host (laptop)).
- to be able to collect and report information coming from the wireless process
- to be able to interact with alien entities (alien MAC, possibly remote)

Definitely, having flexibility between WiMAX and LTE in mind, it was important that the framework would apply to both systems, even if it was primarily focused for WiMAX as stated in the definition of Flavia project.
It is the reason why the activity of interface definition and related development is shared between WP3 (WiMAX focused) and WP8 (applicability to LTE).
This constraint in mind, the architecture was designed in such a way that it could adapt to any wireless process, as long as the wireless processor includes the appropriate API. Typically, the capability in terms of available measurements and control are declared by the wireless processors through IAP 1
Then, the information is coming up to the control entity through IAP4 and measurement / control information could be accessed to alien entities using IAP2.

In order to implement this architecture on a hosted device, we decided about the partition of the interface between the device and the host (and for the host, whether it should be part of the kernel/driver space or in the user space).
The partition is depicted in the ***Figure 41***, and illustrates the architecture envisaged for the practical development towards the demonstration of WP7.

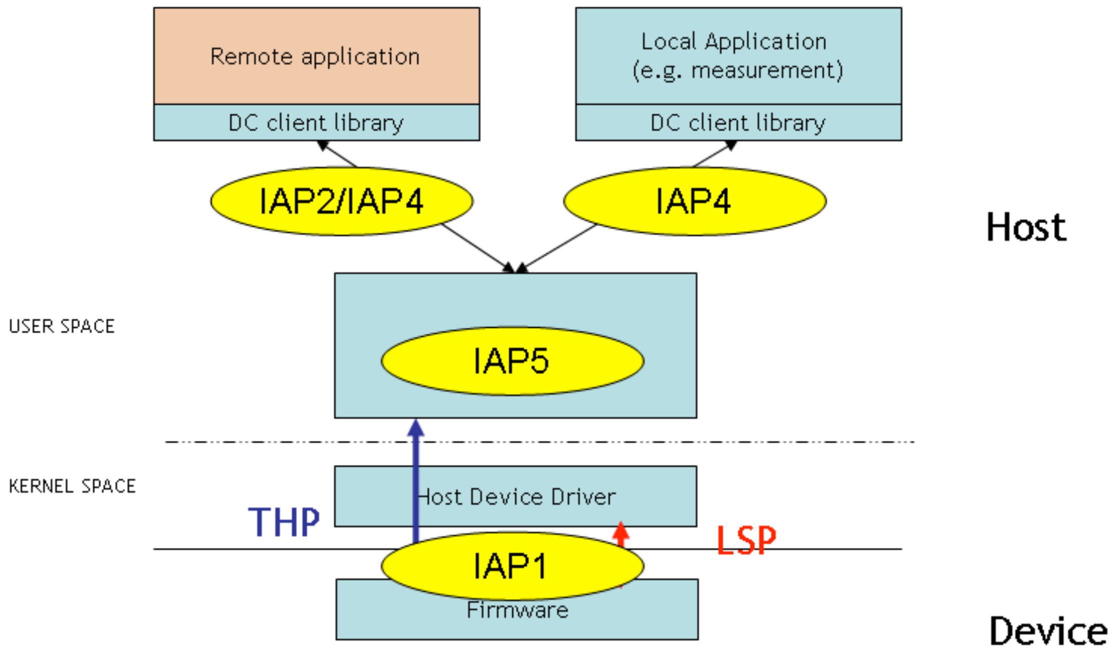


Figure 41: Implementation of the Flavia architecture on a hosted receiver device

The firmware is first updated to be able to interact with the driver in a generic manner. As a result, when an upgrade of the device capability occurs, the measurement framework could be kept.
The interaction with the wireless processor (say the system on chip) is handled at the low layer by a driver which is dependant of the host type (mostly the operating system).
Then, above the driver, we have specified a deamon (in Linux) or a service (in Windows) which hide the hardware specificities to the application running above the deamon.
This deamon manages the interactions with the device and has aggregated the offered capabilities and possible interaction provided by the device.
On top of this deamon, application could be developed in a generic way, that could control the device or gather measurements of interests.

3.2.14.1 List of available parameters (WiMAX)

In the following, list the foreseen measurements that could be aggregated through the measurement framework. This list depends on the capability of the system of chip of the device and is given below for the current family of WiMAX terminal product from SEQ. For each measurement, we indicate the possible service (as described in D3.1.1) that could use the information, bearing in mind that they are all available for the MEAS service.

Measurement	Type	Description	Possible Service
rssi-preamble-ch0&ch1	RX Stats	both antennas preamble RSSI substracting RX chain gains	LADA, MOSU, SSON, ICIC
rssi-mean		Mean via alpha filter (configurable)	LADA, MOSU, SSON, ICIC
cinr-preamble-ch0&ch1		both antennas CINR, calculating via stats (Signal power – Noise power) for all subcarriers	LADA, MOSU, SSON, ICIC
cinr-mean		Mean via alpha filter (configurable)	LADA, MOSU, SSON, ICIC
cinr-r1-mean		CINR from R1 subcarriers	LADA, MOSU, SSON, ICIC
cinr-r3-mean		CINR from R3 subcarriers	LADA, MOSU, SSON, ICIC
backoff-ch0&ch1		both antennas backoff from saturation of the RX chain	LADA, MOSU, SSON, ICIC
rx-analog-gain		analog gain of the RX chain	LADA, MOSU, SSON, ICIC
rx-doppler		weighted speeds weighted from two antennas	LADA, MOSU, SSON, ICIC
rx-doppler-mean		Mean via alpha filter (configurable)	LADA, MOSU, SSON, ICIC
rx-freq-offset		carrier frequency offset taken either from frequency offset estimation on data or from measurement on preamble	LADA, MOSU, SSON, ICIC
tx-power	UL Power Control	the current transmitted power	LADA (UL), SSON, ICIC
tx-psd		the Tx root power per subcarrier + NI(PUSC)[dBm]	LADA (UL), SSON, ICIC
tx-sat-backoff		the transmit saturation backoff	LADA (UL), SSON, ICIC
Sniff-rx-fch	Scheduler	the received FCH in case the FCH was correctly received	Link maintanace, SSON, ICIC
sniff-rx-fchbad		the received FCH in case the FCH was erronously received	Link maintanace, SSON, ICIC
traffic-burst-dl		data descriptor of a data burst (length, Cid, last FEC code, HARQ?)	
traffic-burst-dl-crc		data descriptor of a good burst	
sniff-rx-ucddcd	Message Dispatcher	UCD and DCD	SSON, ICIC
sniff-rx-mapdl		DL MAP	SSON, ICIC
sniff-rx-mapdlcmp		all compressed maps	SSON, ICIC
sniff-rx-mapul		UL MAP ARQ FBCK	SSON, ICIC
sniff-rx-		any MAC message	SSON, ICIC

macmsg			
sniff-tx-macmsg		any MAC message	SSON, ICIC
qos-pkt-pending	Map Scheduler	waiting packet qty when choosing Bwr Grant (parames: cid, pkt Per Cid, byte Per Cid)	SCHE (UL)
traffic-pkt-rf-tx		if the number of packets was changed after processing (reserving BW for BWR headers, retransmitting ARQ data), send the difference when processing the map (params: difference)	SCHE (UL)
traffic-byte-rf-tx		if the number of payload bytes was changed after processing (reserving BW for BWR headers, retransmitting ARQ data), send the difference when processing the map (params: difference)	SCHE (UL)
traffic-grant-ul		granted information for two types of grants - UMSS_GRANT_HARQ & UMSS_GRANT_UNICAST (parames: fecCode, #bytes, #stuffed Bytes)	SCHE (UL)
traffic-grant-ul-retry		on every grant which is UMSS_GRANT_HARQ sends the needed information (parames: fecCode, # grantes Bytes)	SCHE (UL)
traffic-pkt-rf-rx	RF traffic Monitoring	- retrieve the complete ARQ data packets from the ARQ module - counts current HARQ packet - counts the packets that are delayed for further transmissio	SCHE (UL)
traffic-byte-rf-rx		accumulating appropriate number of Bytes	SCHE (UL)
traffic-pkt-rf-rx-drop		accumulating appropriate number of Bytes dropped	SCHE (UL)
wimax-state	Mobility	curent state of the MS (SWM_SS_INIT, SWM_SS_ABORTED, SWM_SS_IDLE, SWM_SS_SLEEP, SWM_SS_OPERATIONAL)	MOSU
ho-actions		Ho action taken: SEND_SCN-REP, HO_ABORTED, SEND_HOIND, BS_HO_REQ, update nBS, MOBS_EVENT_SCAN_ENABLED/DISABLED, HANDOVER, TRIGGER (trigger, function, metric, action)	MOSU
neighbor-bs-stats		Statistics on neighboring BS represented by {frequency, preamble} are rssi, cinr, cinrReuse1, cinrReuse3, rtd	MOSU, SSON, ICIC
serving-bs-stats		Statistics on serving BS represented by {frequency, preamble} are rssi, cinr, cinrReuse1, cinrReuse3, rtd	LADA, MOSU, SSON, ICIC

3.3 Main Scenarios

The complete list of services primitives typically defines the inter-service communication. The validation of the primitives list is done using main inter-service MAC scenarios such as downlink packet chain and scheduling frame.

3.3.1 DL Data path

In this section we illustrate how the DL data path can be implemented using FLAVIA services and interfaces. A schematic illustration of the DL data path is shown in Figure 42. Furthermore, Section 7.1 provides more details about the data packet representation in different services.

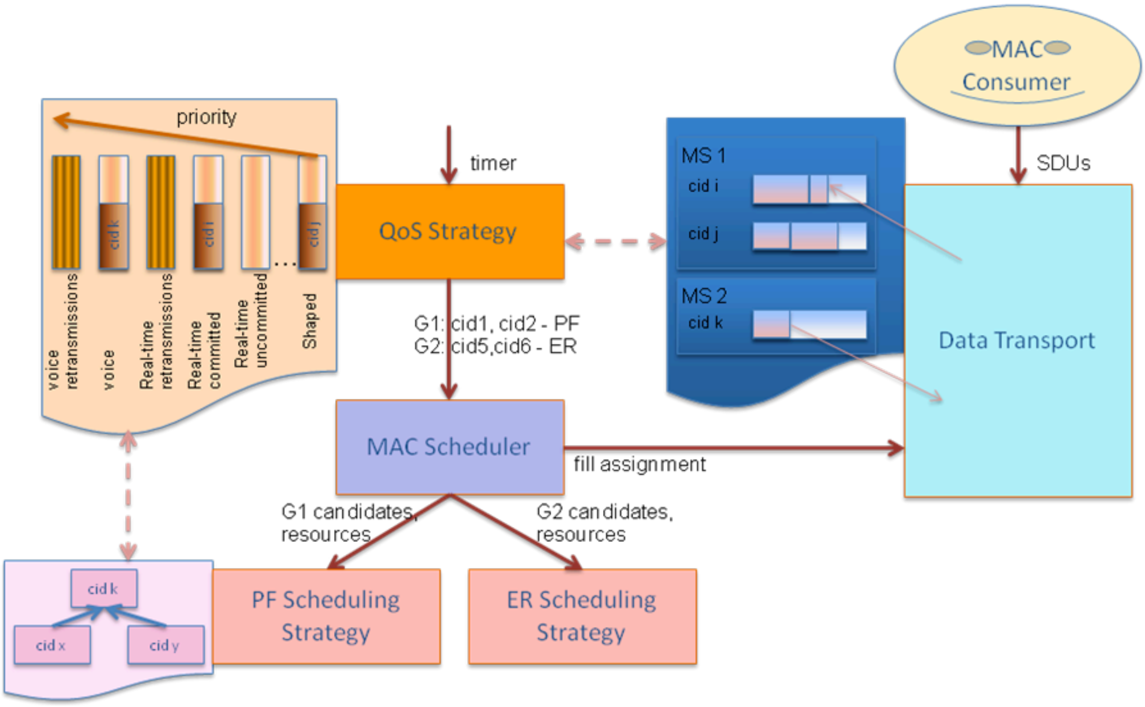


Figure 42: Schematic presentation of DL Data Path process.

The DL Data Path process can be described by the following stages:

Stage 1:

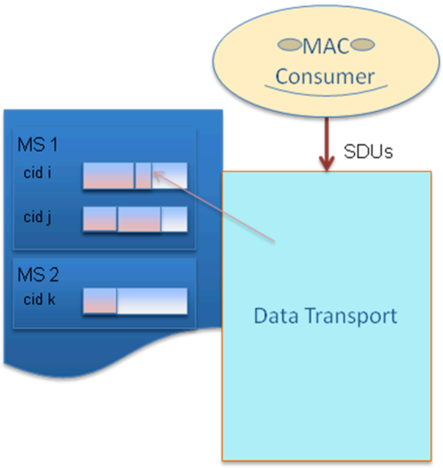


Figure 43: DL Data Path flow, Stage1.

In stage 1 the following individual steps are executed by the Data Transport service:

1. SDUs are received from the MAC consumer,
2. SDUs are classified and assigned to the appropriate connections,
3. It applies Random Early Discard (RED) [9] and rate policing to drop packets,
4. SDUs are stored in connections queues (data buffers), and finally
5. It updates QoS Strategy service about new bandwidth demands. This update may be done using two different interfaces:
    - PUSH: The Data Transport service notifies the QoS Strategy service about queue updates, and
    - PULL: The QoS Strategy service will request buffered SDUs info from the Data Transport service.

<u>Stage 2:</u>

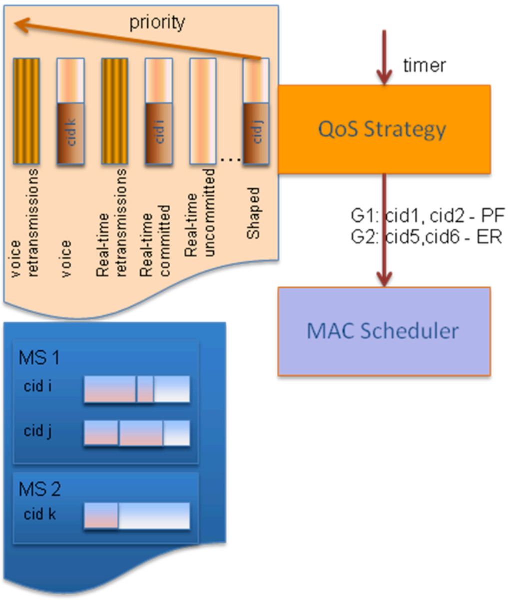
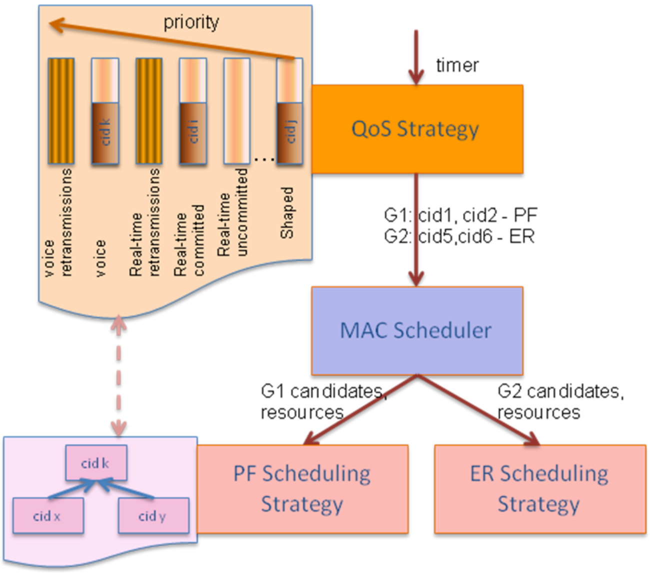


Figure 44: DL Data Path flow, Stage2.

In the second stage, the QoS strategy mainly takes responsibility to prepare a candidates list to be potentially scheduled in a specific frame. This process can be executed in background or on-demand requested by the MAC Scheduler service. QoS strategy manages all information related to bandwidth requests for DL/UL connections or HARQ processes. Bandwidth requests may be virtual packet-descriptors including QoS-relevant information such as packet/request size and timestamp. In addition, the QoS strategy service assigns a scheduling strategy per groups of candidates. In the given example (Figure 44), it assigns the Proportional Fairness strategy to group G1 of candidates, and Equal Rate strategy to group G2.
Furthermore, the QoS strategy service performs the following tasks:

- Prioritization between different QoS classes (QoS type, traffic priority, Minimum Reserved Traffic Rate/Maximum Sustained Traffic Rate, HARQ retransmissions, etc)
- Traffic shaping
- Assignment QoS strategy metric (for combining in next stage)
- Semi-persistent scheduling (time-domain)
- Synchronization with the Power Saving service

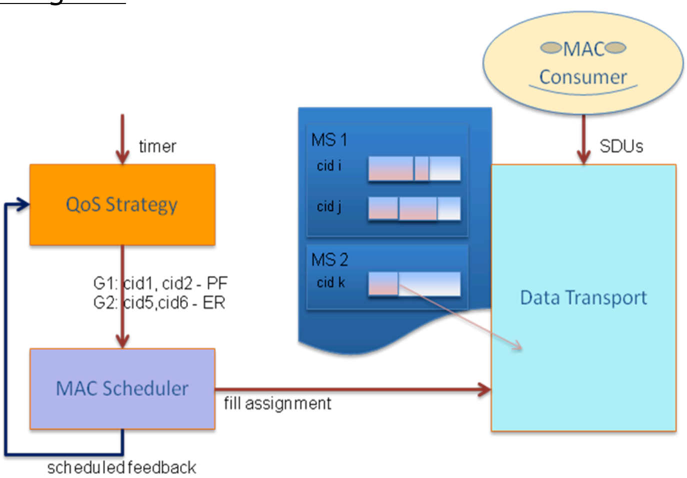
<u>Stage 3:</u>



In the third stage, the MAC scheduler service receives the candidates, decides about frame portion per group of candidates and requests Scheduling Strategy service to schedule the given candidates on the given resource units. Scheduling Strategy works on a logical map of resources (agnostic to frame structure) and applies a specific scheduling scheme to decide which candidates will be served, allocation size and resources assignments. Scheduling Strategy executes the following tasks:

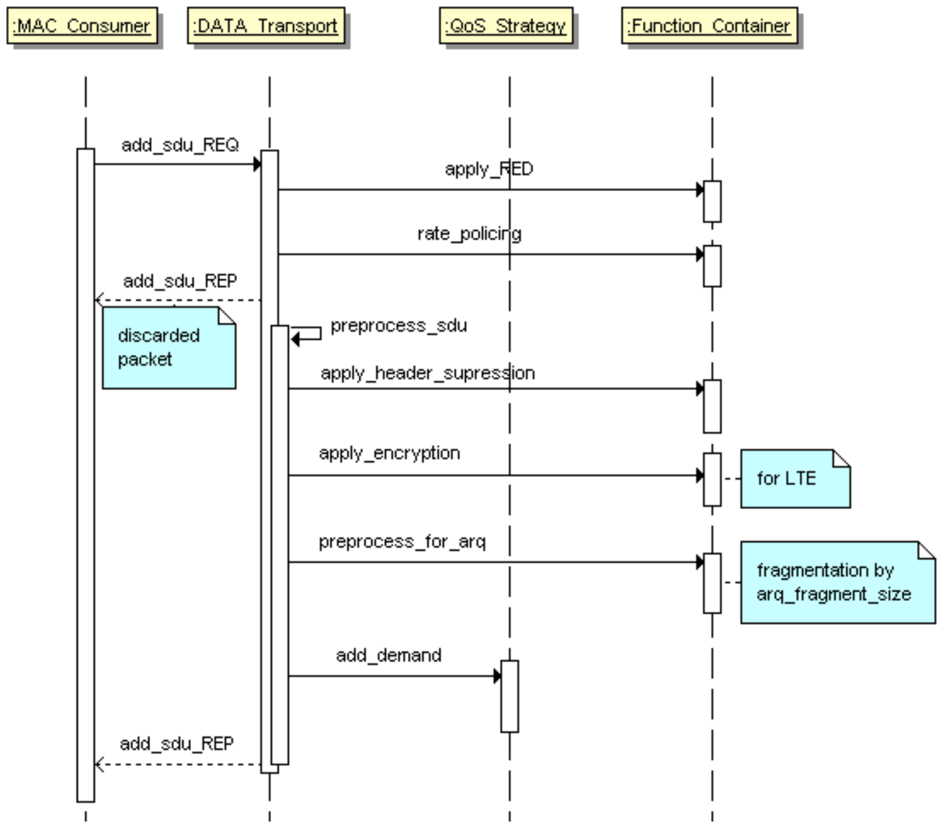
- Application of (frequency-selective) link-adaptation,
- Multi-users coupling for collaborative MIMO,
- Combination with QoS Strategy metric, and
- Creating an output record with the scheduled amount of bytes per connection and resource assignment.

<u>Stage 4:</u>

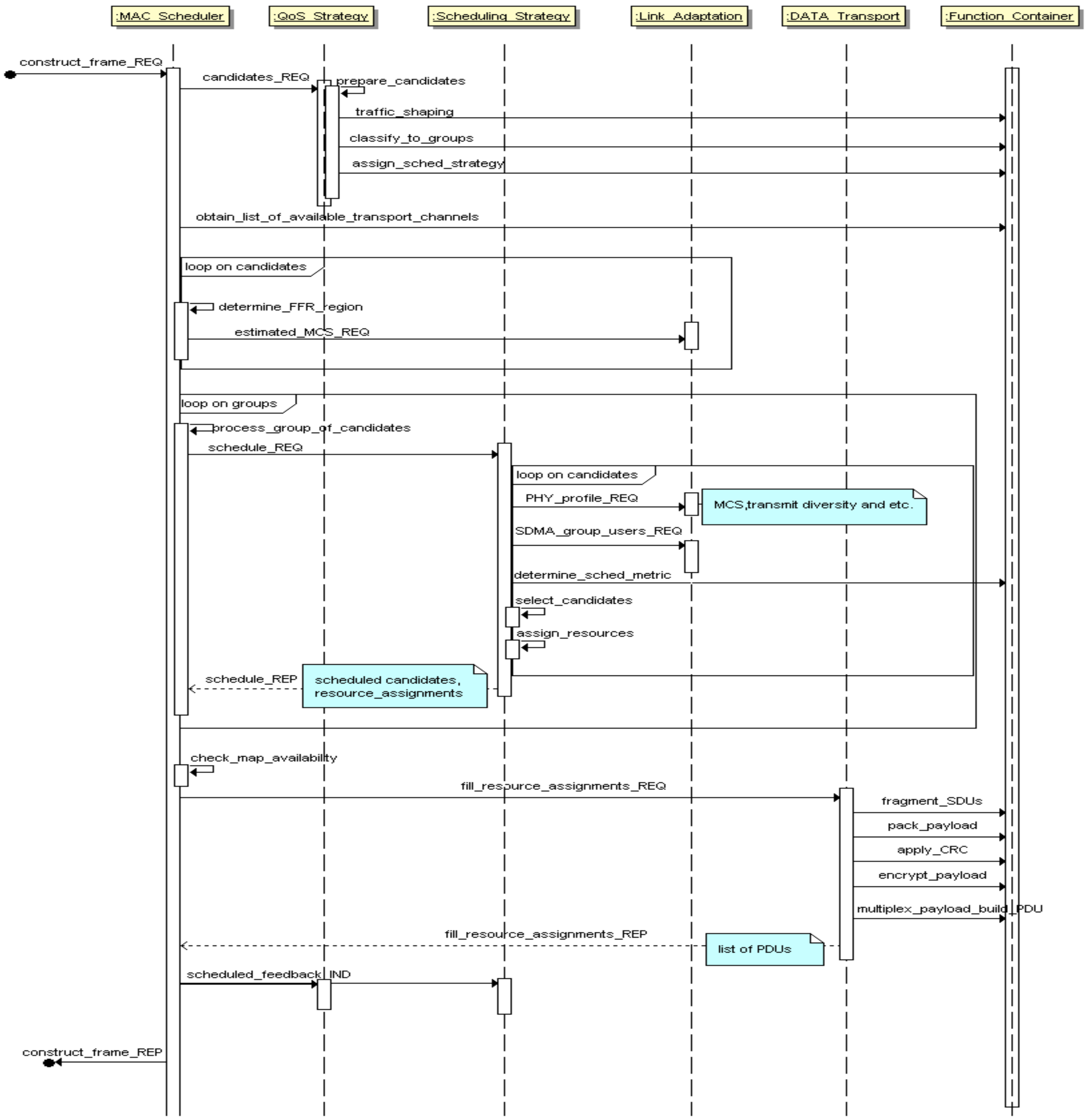


Finally, the MAC scheduler service checks the availability of control-channels and afterwards calls the Data Transport service to fill the resource assignment with data packets. The Data Transport service then manipulates the SDUs and constructs MPDUs. Finally, the QoS Strategy service and MAC Scheduler are updated on the actually scheduled candidates.

3.3.2 Receive DL packet from MAC Consumer



3.3.3 Scheduling frame



4 FLAVIA Framework Use Cases

4.1 Self Optimization – MAC Configuration Update

Figure 45 provides a schematic view about how services are loaded and configured within the FLAVIA framework. First, MAC services are loaded and started via IAP4 interface. Self Optimization Service (SSON) may dynamically change MAC/PHY configuration based on collected measurements/statistics. For example, SSON may invoke reuse-3 region upon monitoring poor cell edge users performance across multiple neighboring BSs. A service configures other services configuration through FLAVIA Control Manager, which for example verifies consistency of the updated parameters. The FLAVIA Control Manager directs configuration changes to the relevant MAC services. In Figure 45, the Control Manager reconfigures, for example, the FFR parameters of the MAC Scheduler service (e.g. a frame template).

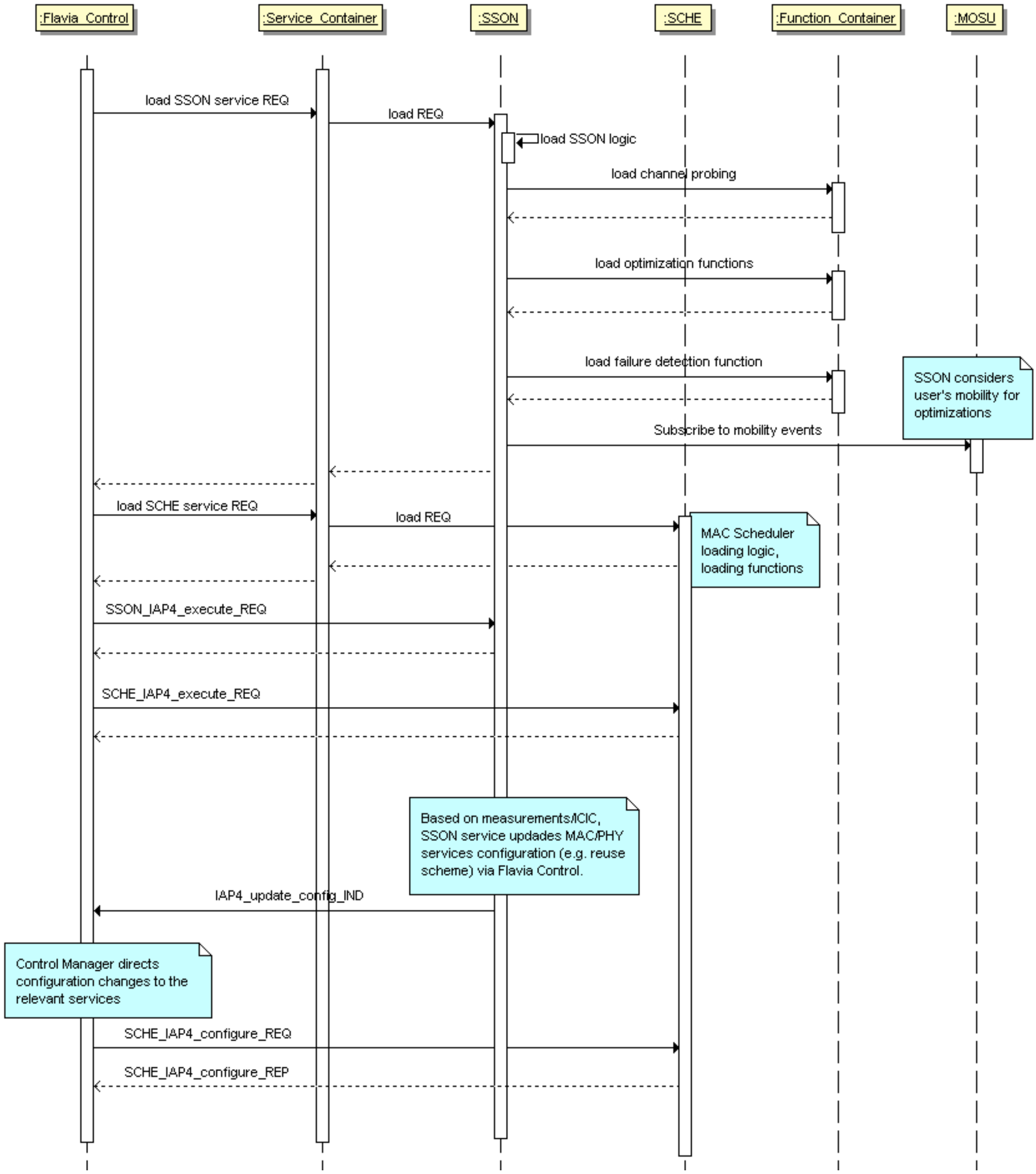


Figure 45: SON configures MAC Services via FALVIA Control.

4.2 Application optimization support – MAC optimization and Configuration Update

In this subsection we depict the loading process of the AOPS service, and give some examples of events and message exchanges that can occur during the service operation or in relation to the AOPS operation.

The AOPS service is meant to support the optimization of running applications. The intended optimization is a cross-layer optimization, thereby requiring the interaction of the MAC with the application sending data traffic over through the MAC. On one side, AOPS is responsible for a fine-tuning of MAC/PHY parameters that considers the current status of resource utilization in the system. On the other hand, AOPS is responsible for interfacing the running applications, i.e., the MAC consumers, to the MAC optimization routines. Here we want to show the basic operations that have to be performed in order to enable the AOPS service and the basic operations that involve AOPS activities and, in particular, the system configuration updates driven by AOPS.

As shown in topmost part of Figure 46, the AOPS service has to be loaded by the FLAVIA Control, and then executed upon the loading procedure is completed. In the figure, for sake of readability, we omit most of the _REP primitive names, which travel in the diagram over dashed arrows. The service loading procedure involves the FLAVIA Control, the Service container, the specific service to be loaded (AOPS), the function container, and the other services that have to be configured in order to support the operation of the AOPS service.
Specifically, the AOPS service has to access the function container in order to load all the functions that are needed for AOPS operation, e.g., the optimization functions. The, DATA and QOSS services have to be configured through IAP5 in order to support traffic differentiation. As a matter of fact, AOPS manages the traffic classes that are supported in the system, and specifies the dropping policy that has to be enforced by the DATA service, plus the QoS rules (e.g., the modulation schemes allowed, or the fragmentation options available for a flow) to be used at the QOSS. During the loading procedure, only default traffic classes are loaded. Note that, in the figure, we depicted the case that AOPS can directly request DATA and QOSS to use a set of traffic classes. However, this procedure might be implemented in a different way, by using the FLAVIA Control. In this latter case, AOPS should send an indication to the FLAVIA Control, containing the list of traffic classes to be enforced and their parameters; the FLAVIA Control should then decide whether to enforce the change and notify DATA and QOSS about the new traffic classes to be handled.

After loading the service and having started AOPS execution, the FLAVIA Control tells the MAC consumer that AOPS is running and accepting traffic classification requests.

At this point, AOPS would have started to periodically compute the optimization of MAC/PHY parameters and detect the set of running applications. If the optimization routine's output consists in the request for a new MAC/PHY configuration, then AOPS sends an indication primitive to the FLAVIA Control using IAP4, and the FLAVIA Control will therefore decide whether to enforce any change in the configuration of the other running services. The FLAVIA Control will also notify AOPS with the new, currently enforced, system configuration.

The diagram in Figure 46, also shows the interaction between the MAC consumer and AOPS. On one hand, when AOPS detect, determines, or is notified about configuration changes and system status updates, then it can notify the MAC consumer with the new network status. As a consequence, the MAC consumer can adapt its traffic behavior accordingly to the new network status.
On the other hand, when the MAC consumer decides to introduce a new traffic class, it sends a traffic class request over IAP6. Hence, AOPS will try to enforce the new traffic class (a) by directly interfacing to DATA and QOSS, as depicted in the figure, or (b) by sending an indication to the FLAVIA Control containing a configuration update.

Finally, the bottom of the diagram in Figure 46, depicts the case in which the optimization routine would detect the presence of traffic flows that can be dealt with by means of a new traffic class. As a consequence, AOPS would automatically determine the parameters to be used for the new traffic class, and interface to DATA and QOSS services in order to deploy the new traffic class (alternatively, as explained before, AOPS can ask the FLAVIA Control to deploy the traffic class).

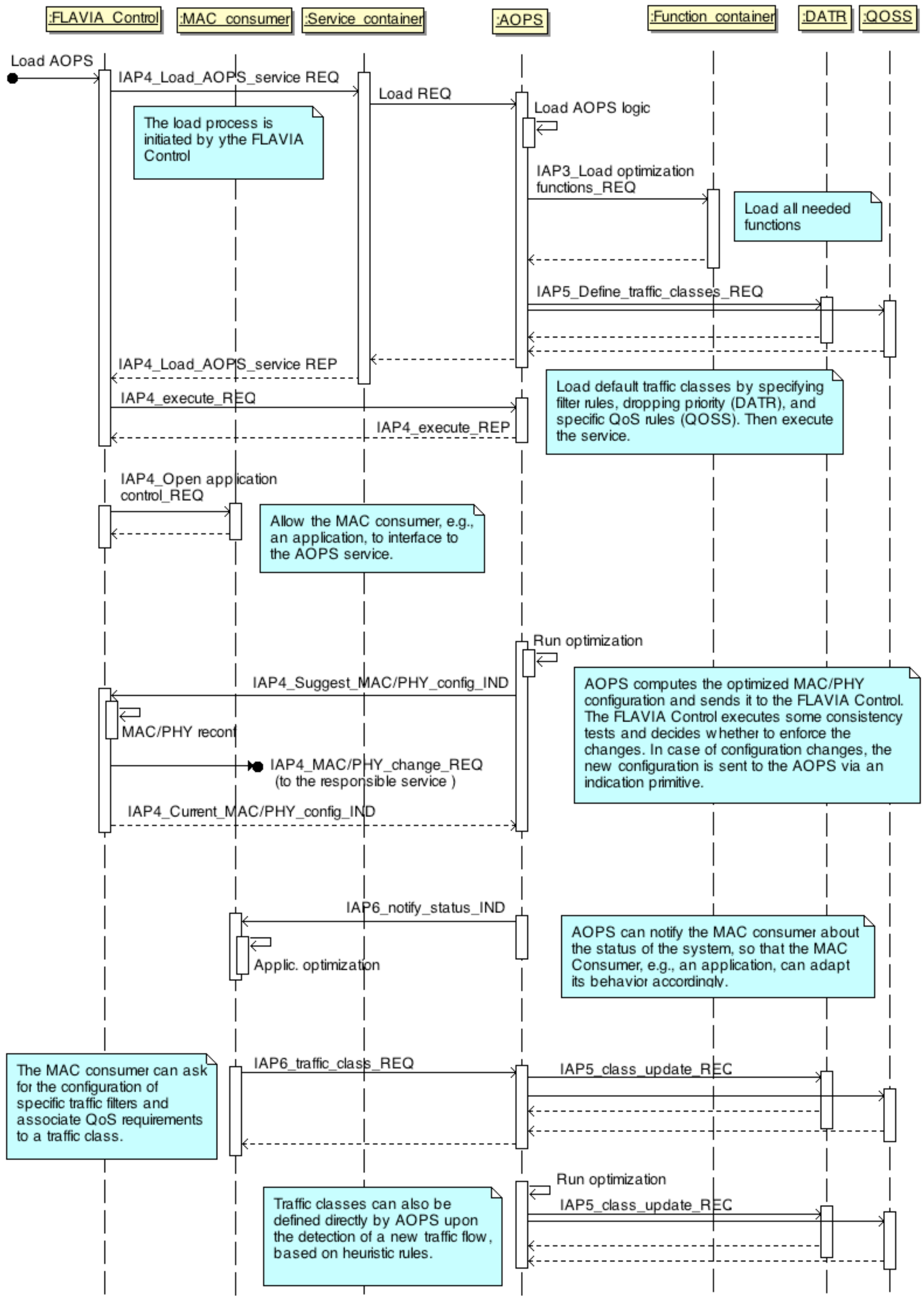


Figure 46: AOPS loading and basic operation. AOPS is loaded by the FLAVIA Control, then it starts interacting with the FLAVIA Control and the MAC Consumer (I.e., the applications running on top of the MAC)

5 Conclusions

This third WP3 deliverable provides the updated specification of the functional architecture, including services and interfaces, required for the implementation of a scheduled-based (802.16) FLAVIA node.

In D3.1.1, the first deliverable of WP3, we had identified a set of main services including "classical" services that are currently available in "legacy" 802.16 nodes, e.g., data transport or link adaptation, as well as new services, i.e., SSON service and Inter-Cell Cooperation and Coordination. D3.1.1 aimed to define services and interfaces and self-contained yet small modules, such that will support modularity and plug-and-play operation. Interface Access Points (IAPs) inside and outside the MAC were defined. For every IAP a list of primitives were specified for each service. Different types of primitives were defined to allow inter-module communication according to the request/replay paradigm as well as to the event notification paradigm.

In D3.2 we designed a prototype that will be used as validation platform of the conceptual architecture described in D3.1.1. The prototype was based on standard 802.16 as paradigm of current scheduled systems. The prototype followed the architecture obtained in D3.1.1

This document D3.1.2 is a revision of D3.1.1. In D3.1.2 we compared the conceptual model of architecture for scheduled systems depicted in D3.1.1 with the design of the validation platform described in D3.2 and, based on the constraints of such real-world example, we updated the relevant definition of services and interfaces.

The final result is an architecture that is still able to show the modularity, flexibility and virtualization capabilities of FLAVIA's approach. For example, the proposed architecture is able to dynamically modify the scheduling strategy used. The decision to modify the scheduling strategy can be taken automatically by the system based on the detected traffic's behavior but can also be taken by the network operator that can decide to re-configure based on strategic reasons.

6 References

[1]FLAVIA Project Deliverable D.2.1.1 - Report on Scenarios, Services and Requirements, January 2011, available online at http://www.ict-flavia.eu

[2]FLAVIA Project Deliverable D.2.2.1 - *Architecture Specification*, May 2011, available online at http://www.ict-flavia.eu

[3]IEEE, "IEEE 802.16m-07/002r10, IEEE 802.16m System Requirements", Jan. 2010.

[4]3GPP, "3GPP TS 36.201 V8.0.0, Evolved Universal Terrestrial Radio Access (E-UTRA); Long Term Evolution (LTE) physical layer; General description (Release 8)", Sept. 2009

[5]R1-090647, "Downlink Control Structure for LTE-Advanced System," Feb. 2009

[6]Liu, C.L. and Layland, J.W., "Scheduling algorithms for multiprogramming in a hard real time environment", Journal of the Association for Computing Machinery, Vol.20, no. 1,pp. 44–61, Jan., 1973.

[7]Jalali, A., Padovani, R. and Pankaj, R., "Data throughput of CDMA-HDR a high efficiency-high data rate personal communication wireless system," Proc. IEEEE VTC pp. 1854–1858, 2000, Tokyo, Japan.

[8]IEEE Std 802.16-2009, IEEE Standard for Local and Metropolitan Area Networks – PART 16: Air Interface for Broadband Wireless Access Systems, May 2009.

[9]Sally Floyd, Van Jacobson. Random Early Detection Gateways for Congestion Avoidance (1993). IEEE/ACM Transactions on Networking, vol.1 (4): pp.397–413.

[10] F. Kelly, Charging and rate control for elastic traffic, European Trans. On Telecommunications, No. 8, pp. 33–37, 1997.

[11] FLAVIA Project Deliverable D.3.1.1 - *802.16 architecture and interfaces specification*, May 2011, available online at http://www.ict-flavia.eu

[12] FLAVIA Project Deliverable D.3.2 - *802.16 modules specification*, January 2012, available online at http://www.ict-flavia.eu

7 Appendix

7.1 Data packet representation in different services

This section details the flow of DL data packets during the scheduling process and shows which information is available and manipulated in the individual services. The following description is based on the scenario introduced in 3.3.1 and the individual stages are illustrated in Figure 47.

1. Data Transport holds DL SDU descriptors consisting of a pointer to the SDU content and information for manipulating the SDU (e.g. fragments serial number)
2. QoS Strategy holds virtual packets for DL/UL bandwidth requests, including information required for QoS Scheduling, such as size and timestamp.
3. Scheduling Strategy receives a candidates list. Each candidate is a quota for a specific connection, comprised of QoS header with QoS attributes/metric (e.g. "under/above guaranteed rate", QoS type, traffic priority) and virtual packets.
4. Scheduling Strategy decides about allocation size and resources assignment. Hence, the resulting allocation quotas include allocation size in bytes/slots and resource assignments. Scheduling Strategy may decide to allocate only parts of the packets (e.g. caused by multi-user allocation for collaborative MIMO) and therefore virtual packets may have a different size compared to the original one.
5. Data Transport should fulfil the allocation quota with the corresponding SDUs. The actual size of the transmitted SDUs is calculated by Data Transport since it is responsible to attach relevant headers (packing/fragmentation) and to build PDUs.
6. A feedback about the actually transmitted/allocated data should be provided to QoS Strategy and Scheduling Strategy.

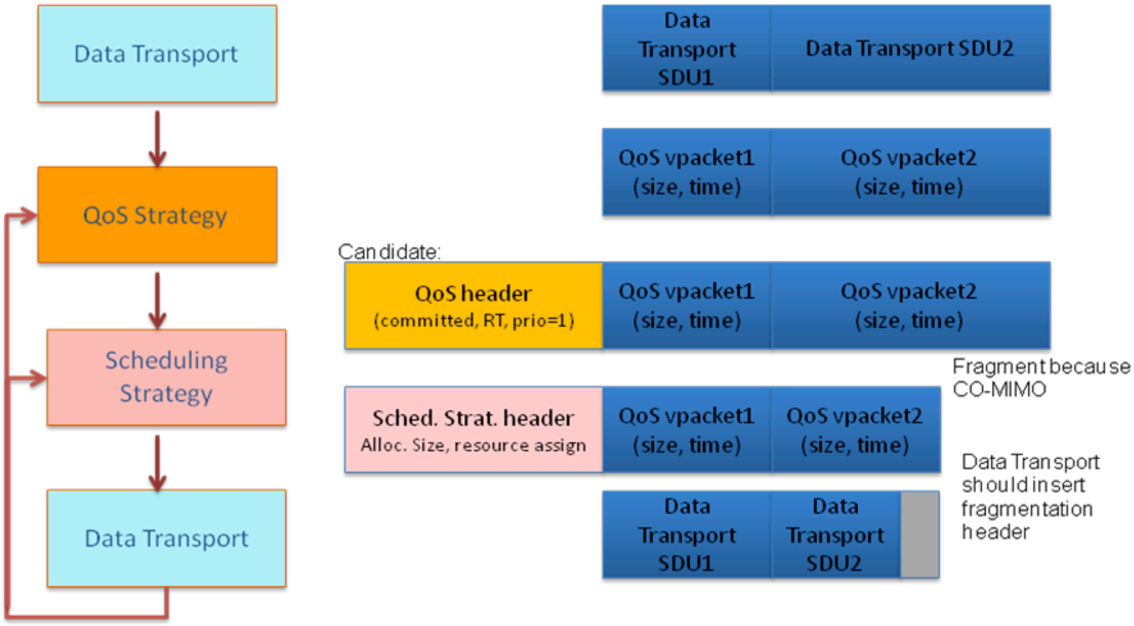


Figure 47: Data packet representation in different services.