Information definition and signalling flows – D3.2

Project Number:	ICT-2009-257385
Project Title:	Opportunistic networks and Cognitive Management Systems for Efficient Application Provision in the Future Internet - OneFIT
Document Type:	Deliverable

Contractual Date of Delivery:	30.9.2011
Actual Date of Delivery:	30.9.2011
Editors:	M. Mustonen, H. Sarvanko
Participants:	See contributor's list
Workpackage:	WP3
Nature:	PU[1]
Version:	1.0
Total Number of Pages:	137
File:	OneFIT_D3.2_20110930.doc

Abstract

The purpose of this deliverable is to define information to be exchanged in OneFIT system based on algorithms for the management of opportunistic networks and to design message sequence charts describing the signalling flows for supporting the management of opportunistic network. To further elaborate on the information exchange, this deliverable will introduce a preliminary state machine as well as information exchange strategies as they are envisaged in the OneFIT project.

Keywords List

Control Channels for Coordination of Cognitive Management Systems, C4MS, Opportunistic networks (ON), Parameters, Elementary procedures and messages , signalling, message sequence chart, state machine

[1] Dissemination level codes: **PU** = Public
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)

Executive Summary

The OneFIT project is a collaborative research project that aims to develop and validate a vision of opportunistic networks (ONs) managed and coordinated by the infrastructure using advanced cognitive principles. The OneFIT solution will enhance wireless service provision and extend access capabilities for the Future Internet, by enabling more efficient resource utilization, reduced costs, and management decisions with a larger "green" footprint. Additionally, the OneFIT solution will lead to enhanced services for the user and increased market opportunities for manufacturers, operators and service providers.

This deliverable describes the information exchange related to the suitability determination, creation, maintenance and termination of an ON by introducing first the models used for the information exchange and then the type of information that needs to be exchanged. The information to be exchanged in OneFIT system is based on the algorithms created for the management of opportunistic networks described in D4.1 "Formulation, implementation considerations, and first performance evaluations of algorithmic solutions" [4].

The deliverable also describes the elementary ON management procedures and message formats for the delivery of the necessary information over C4MS. Additionally, the message sequence charts describing the signalling flows between different entities of the opportunistic network are presented. Compared to the initial message sequence charts introduced in D2.2 [2], these message sequence charts provide more details on the signalling flow and they are divided into the different phases of an ON.

In order to further elaborate on the information exchange in OneFIT system, the deliverable also introduces a preliminary state machine describing the possible node and link states as well as the different triggers leading to these states. Additionally, the deliverable introduces preliminary exchange strategies for delivering information in the OneFIT system based on different types of channels. The development of state machines and exchange strategies will continue and more detailed content will be reported in the future. The deliverable also presents security aspects related to opportunistic networks in terms of potential threats as well as solutions for C4MS.

Contributors

First Name	Last Name	Affiliation	Email
Jens	Gebert	ALUD	Jens.Gebert@alcatel-lucent.com
Andreas	Wich	ALUD	Andreas.Wich@alcatel-lucent.com
Marcin	Filo	EIT+	marcin.filo@eitplus.pl
Krystian	Sroka	EIT+	Krystian.sroka@eitplus.pl
Tomasz	Wierzbowski	EIT+	tomasz.wierzbowski@eitplus.pl
Markus	Mück	IMC	markus.dominik.mueck@intel.com
Andreas	Schmidt	IMC	andreas.schmidt@intel.com
Christian	Mouton	NTUK	christian.mouton@nectech.fr
Seiamak	Vahid	UNIS	s.vahid@surrey.ac.uk
Ramon	Ferrús	UPC	ferrus@tsc.upc.edu
Jordi	Pérez-Romero	UPC	jorperez@tsc.upc.edu
Oriol	Sallent	UPC	sallent@tsc.upc.edu
Panagiotis	Demestichas	UPRC	pdemest@unipi.gr
Andreas	Georgakopoulos	UPRC	andgeorg@unipi.gr
Dimitrios	Karvounas	UPRC	dkarvoyn@unipi.gr
Marios	Logothetis	UPRC	mlogothe@unipi.gr
Vera	Stavroulaki	UPRC	veras@unipi.gr
Kostas	Tsagkaris	UPRC	ktsagk@unipi.gr
Marja	Matinmikko	VTT	marja.matinmikko@vtt.fi
Miia	Mustonen	VTT	miia.mustonen@vtt.fi
Heli	Sarvanko	VTT	heli.sarvanko@vtt.fi

Table of Acronyms

Acronym	Meaning
3GPP	3rd Generation Partnership Project
ABNF	Augmented Backus–Naur Form
ACL	Agent Communication Language
ANDSF	Access Network Discovery and Selection Function
AVP	Address Value Pair
BS	Base Station
C4MS	Control Channels for Coordination of Cognitive Management Systems
CCC	Cognitive Control Channel
CCR	Cognitive Control Radio
CMON	Cognitive systems for Managing the Opportunistic Network
CPC	Cognitive Pilot Channel
CSCI	Cognitive management Systems for Coordinating the Infrastructure
DM	Device Management
DSONPM	Dynamic and Self-Organizing Network Planning and Management
EPC	Evolved Packet Core
GSM	Global System for Mobile Communications
FIPA	Foundation for Intelligent Physical Agents
HTTP	Hypertext Transfer Protocol HTTP
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IEFT	Internet Engineering Task Force
IIOP	Internet Inter-object request broker Protocol
IMTP	Internal Message Transport Protocol
INA	Information Answer
INI	Information Indication
INR	Information Request
Leap	Lightweight Extensible Agent Platform
LTE	Long Term Evolution

MAC	Media Access Control
MIIS	Media Independent Information Service
MRA	Measurement-Answer
MRI	Measurement-Indication
MRR	Measurement-Request
MSC	Message Sequence Chart
MTP	Message Transport Protocol
NCA	Neighbour-Information-Answer
NCR	Neighbour-Information-Request
OMA	Open Mobile Alliance
ON	Opportunistic Network
ONCA	ON Creation Answer
ONCR	ON Creation Request
OneFIT	Opportunistic networks and Cognitive Management Systems for Efficient Application Provision in the Future InterneT
ONMA	ON Modification Answer
ONMR	ON Modification Request
ONNA	ON Negotiation Answer
ONNR	ON Negotiation Request
ONRA	ON Release Answer
ONRR	ON Release Request
ONSI	ON Suitability Indication
ONSN	ON Status Notification
PDU	Protocol Data Unit
QoS	Quality of Service
RAA	Re-Auth-Answer
RAR	Re-Auth-Request
RAT	Radio Access Technology
RMI	Remote Method Invocation
SAA	Spectrum-Assignment-Answer
SAE	System Architecture Evolution

SAP	Service Access Point
SAR	Spectrum-Assignment-Request
SSID	Service Set Identifier
UE	User Terminal
UMTS	Universal Mobile Telecommunications System
UWB	Ultra Wide Band
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

Table of Contents

List of Figures

1. Introduction

Opportunistic Networks (ONs) as seen by the OneFIT-project are operator-governed, temporary and coordinated extensions of the infrastructure. They are dynamically created in places and time instants in which they are needed. The OneFIT-project envisages and investigates five scenarios in which the creation of an ON can increase the performance of the network or bring a solution to a challenge faced by the network.

These five scenarios describe opportunistic coverage extension, opportunistic capacity extension, infrastructure supported opportunistic ad-hoc networking, opportunistic traffic aggregation in the radio access network and opportunistic resource aggregation in the backhaul network. Further details on these scenarios including the specific use cases, target applications and envisaged benefits can be found in D.2.1 [1]. Initial message sequence charts related to different scenarios can be found in D2.2 [2] and they are further elaborated in this deliverable in section 4.

The lifecycle of an ON consists of four different phases – suitability determination, creation, maintenance and termination. At the suitability determination phase the suitability of an ON at a specific time and place is determined based on the observed radio environment and some established criteria. Node and radio path identification as well as an assessment of potential gains are needed to support this phase. The final configuration of an ON is done in the creation phase. The selection of aspects such as involved nodes, used spectrum and routes for the ON are done based on context information and more accurate estimations of the radio environment. An ON will be dynamic and adaptable to changing conditions. At the maintenance phase monitoring will be done to ensure that the ON is still valid and efficient for what it was created for. According to the monitoring information reconfiguration or termination functionalities can be triggered. Reconfiguration will ensure the most efficient operation of the ON. When the ON operation is no longer necessary or suitable, the ON will be terminated. In case some of the services provided by an ON are still needed or termination is forced suddenly due to reasons external to the ON, there needs to be a mechanism for the ON to handover the service to the infrastructure. The information that could be exchanged in different phases of an ON are first introduced in D3.1 [3] and it will be more elaborated in this deliverable Section 3. Description of different phases of the ON lifecycle and initial algorithms created for them can be found from D4.1 [4].

The rest of the deliverable is organized as follows. Section 2 gives an overview on the OneFIT architecture and introduces aspects related to policy management and context awareness architectures (these topics are also further elaborated in Appendixes I and II, respectively). Section 3 introduces the models used for delivering the information over Control Channels for Coordination of Cognitive Management Systems (C4MS) (a more detailed description is given in Appendix V) as well as the information to be exchanged in OneFIT system. The preliminary information introduced in deliverable D3.1 [3] is limited to the set required by algorithms described in D4.1 [4]. Information to be exchanged is divided into policy information, context information, decisions, profiles and knowledge. Section 4 describes an initial idea of the elementary ON management procedures and messages to be supported over C4MS. These concepts will be further developed and described in more detail in the upcoming deliverable D3.3. The message sequence charts for OneFIT scenarios were originally presented in D2.2 [2]. In the Section 5 of this deliverable, the message sequence charts are described in more detail and they are divided into the different phases of an ON. Based on the message sequence charts, preliminary state machine describing different link and node states of the OneFIT system is introduced in Section 6. In Section 7, initial views on exchange strategies are described. This work will be used as a basis for protocol description in D3.3. Security aspects related to opportunistic networks are presented in Section 8 in terms of potential threats and solutions for C4MS. Existing security frameworks from standardization are introduced in Appendix III.

2. Overview of OneFit approach

2.1 Functional architecture

The main functional entities of the OneFIT architecture for the management and control of operator governed opportunistic networks as shown in Figure 1 are the

- Cognitive management System for Coordinating the Infrastructure (CSCI) and the
- Cognitive System for Managing the Opportunistic Network (CMON).

Further on, OneFIT uses the Control Channels for the Cooperation of Cognitive Management Systems (C4MS) to communicate between different nodes.

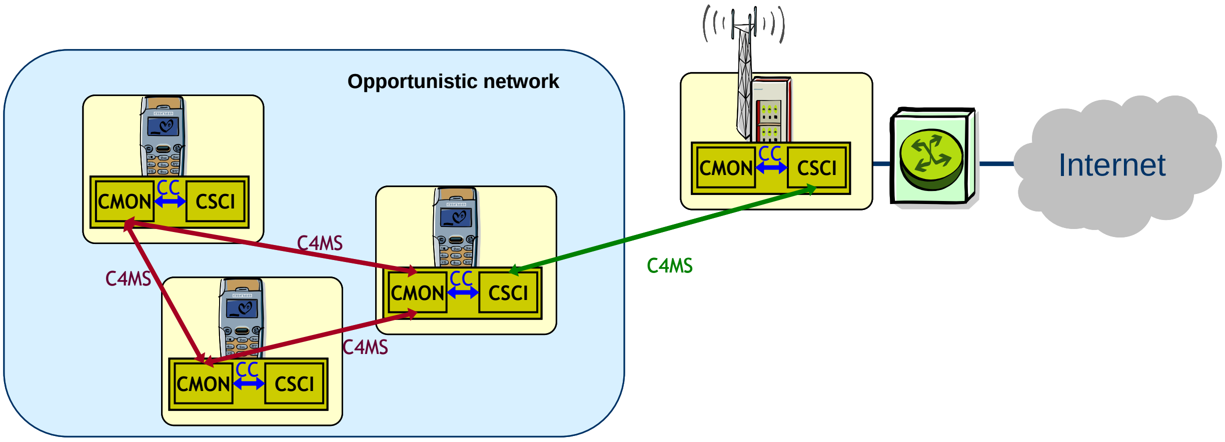


Figure 1: High level overview on the OneFIT Solution

The CSCI and CMON are management systems whereas C4MS is the main logical protocol for communication, cooperation and coordination between these management entities. The CSCI is mainly responsible for the activities before an ON is created, such as ON opportunity detection and ON suitability determination. It is in charge of the context acquisition and processing as well as gain assessment. When the CSCI has made a decision that an ON is suitable, the decision is then sent to the CMON. The CMON executes the creation, maintenance and termination of a given ON based on the information from the CSCI. The functionalities of a CMON include coordination between the nodes of the ON and reconfiguration. The OneFIT architecture including a more detailed description of the CSCI and CMON as well as an introduction of other functional entities can be found in D2.2 [2].

The C4MS is used for enabling an exchange of information such as policies, resources, node capabilities and available spectrum bands both globally and locally as well as for the purpose of managing the opportunistic networks. The C4MS inherits functionality from two well-known concepts: the Cognitive Pilot Channel (CPC) which provides information from the network to the terminals and the Cognitive Control Channel (CCC) which facilitates information exchange between heterogeneous network nodes (e.g. between terminals). A C4MS common framework integrates and further develops these two concepts in order to manage the provision of context information, policies, parameters etc. either between heterogeneous network nodes (terminals or infrastructure nodes) or between terminals and infrastructure. A detailed description of the C4MS including the implementation options can be found in D3.1 [3].

The OneFIT Functional Architecture (FA) for the Management and Control of infrastructure governed opportunistic networks is shown in Figure 2. Besides the CSCI and the CMON, the FA contains additional building blocks like the Dynamic Spectrum Management (DSM), the Joint Radio Resource Management (JRRM), the Configuration Control Module (CCM) and the Dynamic Self-Organising

Network Planning and Management (DSONPM). A description of these building blocks can be found in D2.2 [2].

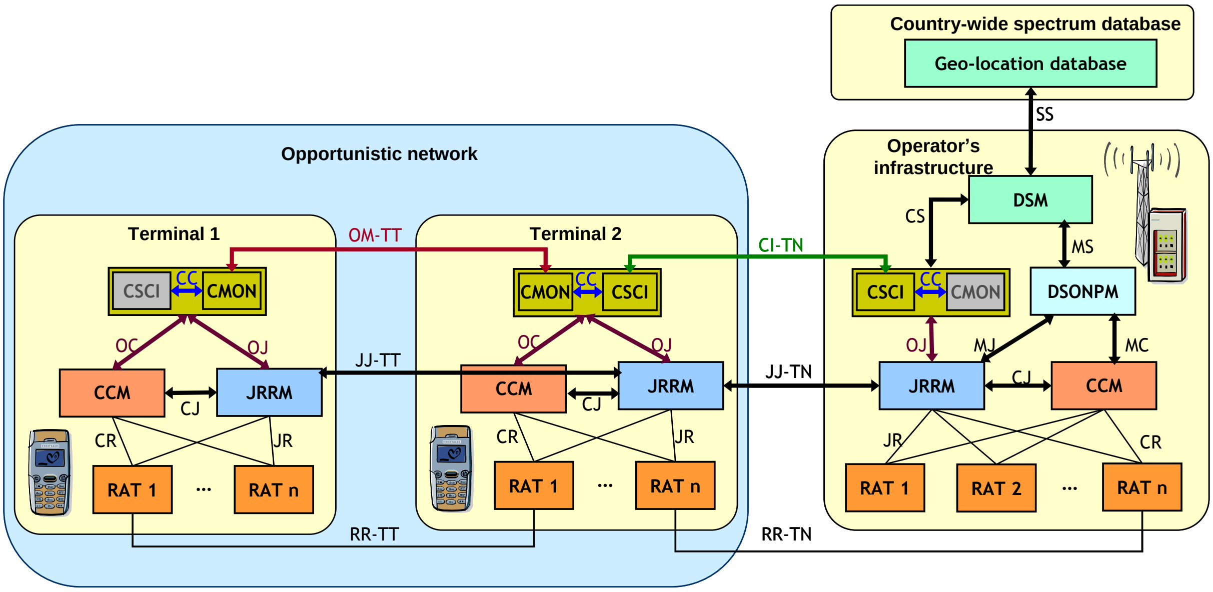


Figure 2: OneFIT Functional Architecture for the Management and Control of infrastructure governed Opportunistic Networks as an evolution of the ETSI/E3 FA [2]

2.2 Policy-based management in the OneFIT architecture

This section covers aspects related to policy-based management within the OneFIT architecture. In OneFIT, opportunistic networks, as already mentioned, are operator governed through policies. Policies are taken into account for the creation of ONs, in addition to other types of information such as profile, context, knowledge. In other words, in the scope of OneFIT policies specify rules or constraints that should be taken into account for the suitability determination, creation and set-up of an ON, refining the set of information comprised in profiles and context data.

2.2.1 Mapping onto OneFIT functional architecture

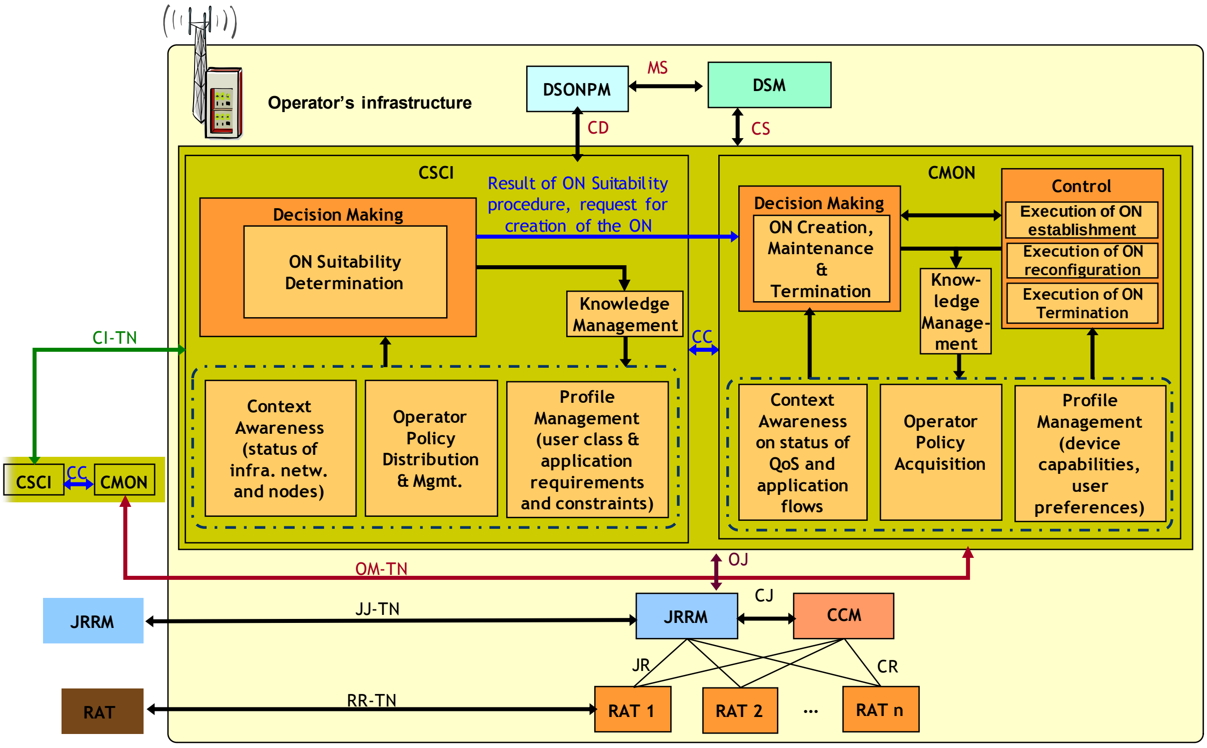
Both of the OneFIT Cognitive Management Systems, i.e. CSCI and CMON are policy-aware, meaning that both of these functional entities are able to obtain policies from other management entities e.g. DSONPM, derive the relevant information and take it into account for decision making.

As introduced in D2.2 [2], the CSCI on the infrastructure side comprises operator's policy distribution and management which designate high level rules that should be taken into account for suitability determination. Such rules are imposed by operators/regulators and refer to reconfiguration strategies, such as operator's preferences and priorities on goals to be achieved. These are related to the maximization of the QoS levels, and the minimization of cost factors (e.g. resource consumption). In the terminal side, the CSCI comprises functionality for the acquisition of policies from the operator. As regards the CMON policy-based management functionality, the policy acquisition functional entity in both infrastructure and terminal sides, obtains policies from the corresponding CSCI. These policies are used as input during the creation and set-up of an ON for selecting the most appropriate configuration, based on the user profile (preferences) and the context.

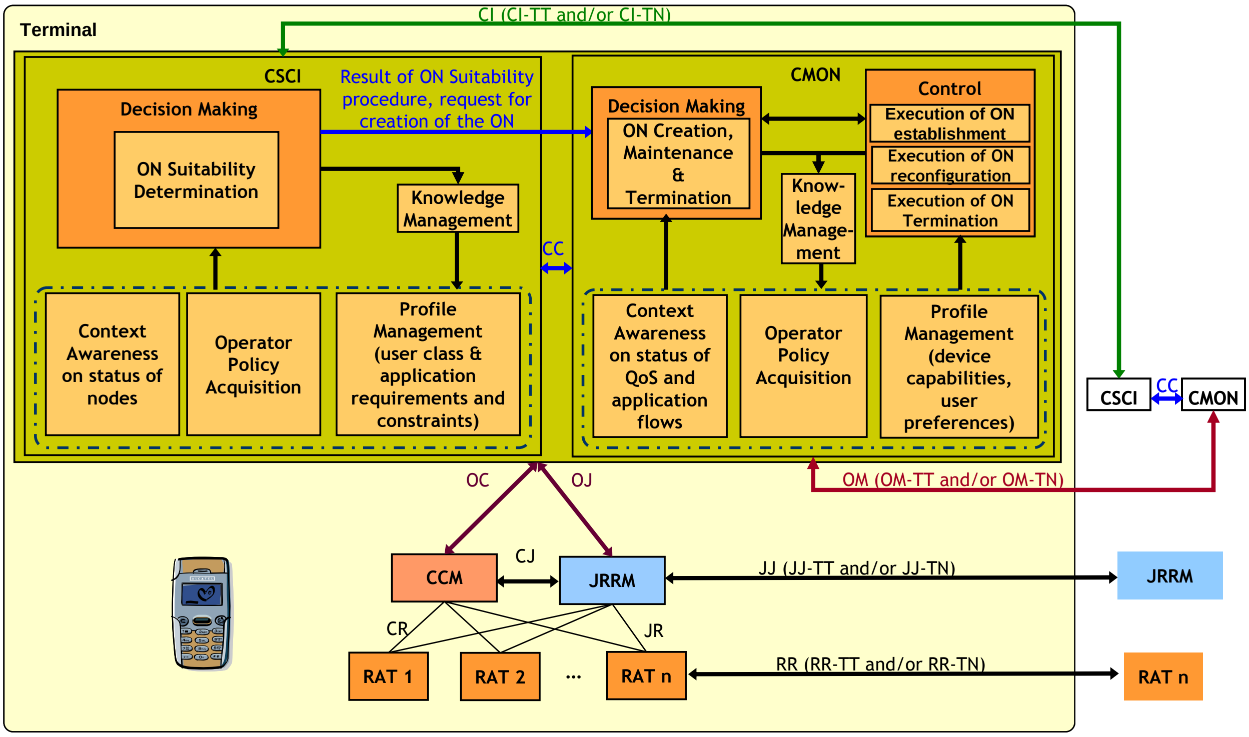
In terms of interfaces, the main interfaces of the OneFIT functional architecture (as defined in D2.2 and presented in Figure 3) are relevant:

- CI: Interface for the "Coordination with the Infrastructure" located between different CSCI-instances. This interface is used by the infrastructure network to provide terminals (or other infrastructure network elements) with policy information which is taken into account for the suitability determination;

- CC: Interface connecting the CSCI in a node with the CMON in the same node. This interface is used to provide policies from the CSCI to the CMON e.g. about the resources which can be used for the creation of the ON;
- CS: Interface between CSCI/CMON and the DSM: This interface is used by the CSCI/CMON to get information on spectrum usage and spectrum policies from the DSM. This spectrum related information can be used for the suitability determination of ONs as well as for the decision making on which spectrum shall be used in an ON. It is assumed that this interface uses identical procedures and protocols as the MS-interface;
- MS: Interface between DSONPM and DSM used by the DSONPM to get information on spectrum usage and spectrum policies from the DSM. It allows DSONPM to obtain information about the available spectrum for different RATs, unoccupied spectrum bands and spectrum opportunities.
- CD: Interface between DSONPM and CSCI/CMON. This interface can be used by the CSCI/CMON to retrieve information on the configuration of the operator's network.


Operator's infrastructure
DSONPM
MS
DSM
CD
CS
CSCI
Result of ON Suitability procedure, request for creation of the ON
CMON
Decision Making
ON Suitability Determination
Knowledge Management
Decision Making
ON Creation, Maintenance & Termination
Control
Execution of ON establishment
Execution of ON reconfiguration
Execution of ON Termination
Know-ledge Manage-ment
CC
CI-TN
Context Awareness (status of infra. netw. and nodes)
Operator Policy Distribution & Mgmt.
Profile Management (user class & application requirements and constraints)
Context Awareness on status of QoS and application flows
Operator Policy Acquisition
Profile Management (device capabilities, user preferences)
CSCI
CC
CMON
OM-TN
OJ
JRRM
JJ-TN
JRRM
CJ
CCM
JR
CR
RAT
RR-TN
RAT 1
RAT 2
...
RAT n

(a)


Terminal
CI (CI-TT and/or CI-TN)
CSCI
Result of ON Suitability procedure, request for creation of the ON
Decision Making
ON Suitability Determination
Knowledge Management
Context Awareness on status of nodes
Operator Policy Acquisition
Profile Management (user class & application requirements and constraints)
CC
CMON
Decision Making
ON Creation, Maintenance & Termination
Control
Execution of ON establishment
Execution of ON reconfiguration
Execution of ON Termination
Know-ledge Manage-ment
Context Awareness on status of QoS and application flows
Operator Policy Acquisition
Profile Management (device capabilities, user preferences)
CSCI
CC
CMON
OC
OJ
OM (OM-TT and/or OM-TN)
CCM
CJ
JRRM
JJ (JJ-TT and/or JJ-TN)
JRRM
CR
JR
RAT 1
RAT 2
...
RAT n
RR (RR-TT and/or RR-TN)
RAT n

(b)

Figure 3: Detailed functional view of the CSCI and CMON:
(a) in the infrastructure; (b) in the terminal [2]

2.2.2 Overview of state-of-art of policy based management

The literature on policy-based network management systems is quite rich (e.g. [16]-[18]). In [18]system requirements, information models, and system components for policy-based management are discussed. An approach to policy-based network management is presented that combines the business, system, and implementation spheres.

A lot of effort has also been put into standardization.

The former IETF Policy Framework working group [19] has focused on the specification of a framework for addressing issues relevant to the representation, management, sharing, and reuse of policies and policy information in a vendor-independent, interoperable, and scalable manner.

The 3GPP Access Network Discovery and Selection Function (ANDSF) [7] is an entity in the Evolved Packet Core (EPC) of the System Architecture Evolution (SAE) [8], which is responsible for the connectivity of the terminals to trusted networks including 3GPP (e.g. LTE, UMTS) and non-3GPP access networks (e.g. WiMax) and untrusted ones (e.g. WiFi). The main role of the ANDSF is to give information to the terminals about the status of these networks and provide intersystem mobility policies as well as inter-operator mobility policies.

3GPP has defined a Policy and Charging Control Architecture in TS 23.203 [6]. These policy and charging control functions are used for flow based charging, including charging control and online credit control and policy control (e.g. gating control, QoS control, QoS signalling, etc.). A short overview can be found in the Appendix I in Section 11.

The IEEE P1900.4 working group was motivated by E2R II [22] and was formed by IEEE Dynamic Spectrum Access Networks (DYSPAN) Standards Committee (formerly IEEE Standards Coordinating Committee 41 (SCC41)). The P1900.4 group has defined and standardized a policy based management framework, where a Network Reconfiguration Manager (NRM) on the network side derives radio resource selection policies for managing the behaviour of terminals, which are either cognitive radios or multimode devices operating in heterogeneous wireless environments. A Terminal Reconfiguration Manager (TRM) resides in each terminal and is responsible for receiving and implementing these policies, while at the same time it takes into account local terminal strategies. The corresponding IEEE 1900.4 standard was approved by the IEEE Standards Board on January 30th 2009 [20],[21].

Contributions to the IEEE 1900.4 were made by E3 [23]. In E3 policy acquisition and management functionality was developed on both the network as well as the user device (terminal), following an approach similar to the one defined in the IEEE 1900.4 standard. In [24]a policy is formulated as a set of a Compound Policy Condition and a Policy configuration. A Compound Policy Condition consists of a Logical Expression (e.g. AND, OR, XOR) and one or more Compound Policy Conditions or Policy Conditions. A Policy Condition comprises a Policy Expression (e.g. "equals", "greater than", "greater equal", and "less than", "less equal", etc) and a Policy Argument. A Policy Argument includes parameters such User Class, Location, and Time zone information. Information comprised in the Policy Argument indicates the devices that are affected by the specific policy. A Policy Configuration indicates the RATs that can be operated by transceivers of Access Points/Base Stations, as well as certain frequency bands per RAT in a certain service area. Moreover it also may specify the services and corresponding QoS levels that can be provided over certain RATs. This formulation may be exploited for policy-based management in OneFIT.

Further relevant activities within the DYSPAN Standards Committee include the definition of "policy-based control architectures and corresponding policy language requirements for managing the functionality and behaviour of dynamic spectrum access networks" in the scope of IEEE 1900.5. P1900.5 is planned to be published by end of 2011.

For the purposes of policy-based management in OneFIT it is mainly intended to build on existing work, mainly capitalizing on the E3 architecture and extending it as appropriate in terms both of the structure of data to be exchanged as well as enablers for exchanging the policy information.

2.3 Context awareness in the OneFIT architecture

Context-aware systems offer entirely new opportunities for application developers, system designers and for end users by gathering context data and adapting systems behaviour accordingly. Especially in combination with mobile devices these mechanisms are of high value and are used to increase usability tremendously.

2.3.1 Mapping context awareness onto OneFIT functional entities

Within OneFIT architecture, the Cognitive management Systems for the Coordination of the Infrastructure (CSCI) and the Cognitive System for Managing the Opportunistic Network (CMON) are main functional blocks involved in context management.

2.3.1.1 CSCI

CSCI is the functional entity in charge of the context acquisition, processing of the same and the determination whether or not right conditions are in place for creating an opportunistic network i.e. during ON suitability determination phase. The CSCI delegates the actual creation, maintenance and termination of a given ON to the associated CMON functional entity. The CSCI involves context awareness, operator policy distribution and profile management which provide the input to the decision making mechanism. The cognition relies on the fact that knowledge management functional entities interact with the previously mentioned entities in order to make better decisions in the future, according to the learned results.

Specifically, the context awareness functional entity of the CSCI-N (CSCI Network side) involves the monitoring of the status of the infrastructure network, in order to be aware of the necessity to create an ON. Also, node information is captured in the context entity which includes node’s capabilities, status, location (including information from a geo-location database), mobility level and supported applications. Node information is used during the decision making process as it provides the necessary data on the available nodes, used for the selection of candidate nodes. On the other hand, the context awareness functional entity in the CSCI-T (CSCI Terminal side) is needed in order to acquire information on the status of nodes, which is used as input to the decision making process.

Further on, the operator's policy management in the infrastructure side designates high level rules that should be followed in context handling. Usually, they are imposed by operators/ regulators and refer to reconfiguration strategies, such as operator's preferences and priorities on goals to be achieved. These are related to the maximization of the QoS levels, and the minimization of cost factors (e.g. resource consumption). In the terminal side, the operator's policy derivation and management is replaced by the policy acquisition from the operator which is responsible for acquiring the necessary policies from the CSCI in the infrastructure side.

In relation to "context awareness", CSCI is expected to manage information exchange procedures between CSCI entities on the network and terminal sides related to Context and policy information exchanges:

- CSCI-N is expected to manage access to policy and context information from network infrastructure elements by:
    - Obtaining spectrum assignment policies expressing the regulatory framework and operators objectives
    - Obtaining operator policies to drive ON behaviour
    - Obtaining application flows characteristics (e.g., QoS parameters, application endpoints)
    - Obtaining ON-related user preferences
    - Obtaining ON-related device capabilities
    - Obtaining geo-location coordinates for involved or candidate ON devices from location services
    - Obtaining measurements from radio link layers in infrastructure nodes
    - Obtaining context information from specific monitoring mechanisms (e.g., local sensing through interfaces to spectrum sensors)
- CSCI-T is expected to manage access to local context information from the terminal by:
    - Obtaining measurements from device radio link layers
    - Obtaining geo-location coordinates from device built-in positioning functions
    - Obtaining application flows characteristics (e.g., QoS parameters)
    - Obtaining ON-related user preferences
    - Obtaining ON-related device capabilities
    - Obtaining context information from specific

2.3.1.2 CMON

CMON is responsible for executing on the design obtained from the CSCI and then operationally supervising the created ON. The CMON is also located in both the operators' infrastructure and the terminal side.

The CMON-N in the operators' infrastructure involves context awareness, policy acquisition and profile management which provide the input for the decision making mechanism. On the terminal side, the CMON-T provides functionality for the context awareness, the policy acquisition as defined by the operator and the profile management. The cognition relies on the fact that the knowledge management functional entity interacts with the previously mentioned entities in order to make better decisions in the future, according to the learned results.

Specifically, the context awareness functional entity of the CMON-N involves QoS assessment, in order to provide constant feedback of the ON's experienced QoS and to initiate reconfiguration or termination procedures in case of a sudden drop of QoS. Also, application status monitoring is essential in order to know whether the application provision has ended, in order to terminate the ON. Resource monitoring is also included to the context entity in order to initiate reconfiguration or termination procedures in case of a sudden loss of resources. In other words, context awareness obtains the following: measurements from radio link layers, geo-location coordinates from device built-in positioning functions, application flows characteristics (e.g., QoS parameters), ON-related device capabilities and context information from specific monitoring mechanisms (e.g., wide-band spectrum sensing functionality). At the terminal side, the CMON provides functionality for the context awareness on the status of QoS and application flows which in turn, provide the input to the decision making mechanism. The decision making functionality in CMON is expected to handle effectively the ON creation, maintenance and ON termination phases according to the input from the context awareness, policy acquisition and profile management functional entities.

The contextual and performance parameters collected by the CMON during the life cycle of an ON are used for learning and improvement of its management functions/logic. Equally these data are passed onto the CSCI for improving the governance functions/logic hosted by the CSCI.

The CMON is expected to have the ability of managing information exchange with CSCI and other CMONs to allow the discovery of supported ON capabilities in neighbouring infrastructure nodes and devices through capability announcement and pairing mechanisms among peer CMONs. With respect to the context and policy information exchange, the CMON obtains context and policy information from the CSCI, provides context information to the CSCI, both by utilizing the CC interface, and obtains or provides context and policy information from/ to other CMONs by using the OM interface.

Additionally, the CMON manages access to local context information by obtaining measurements from device radio link layers, obtaining geo-location coordinates from device built-in positioning functions, obtaining application flows characteristics (e.g., QoS parameters), obtaining ON-related user preferences, obtaining ON-related device capabilities and obtaining context information from specific local monitoring mechanisms (e.g., wide-band spectrum sensing functionality).

2.3.2 Interfaces

The following two interfaces in the OneFIT Functional Architecture (also depicted in Figure 2) play main role in the provisioning of context information:

CI-Interface for the "Coordination with the Infrastructure" located between different CSCI instances. Via this interface, the network can collect context information from the terminals to enable the ON suitability determination.

OJ-Interface between JRRM and CSCI/CMON. Context information e.g. on available access networks or on link performance can also be exchanged via this interface.

2.3.3 Transport and exchange of context information

The exchange of information, knowledge and commands between the different functional entities (CMON instances as well as between different CSCI instances) relies on C4MS signalling channels. C4MS is defined to provide a common framework to enable communication between terminals as well as between terminals and infrastructure networks (the employed mechanisms could be RAT specific or/and be RAT-independent). In relation to context information, C4MS provides following functionalities:

- means for exchange of context information, policies, etc., to enable better radio resource utilization,
- provision of context information for supporting terminals in their start-up phase,
- provision of context information for supporting spectrum scanning and spectrum sensing procedures

2.3.4 Scope of context-awareness in OneFIT

Within OneFIT, context awareness and use of context-related information will be focused on:

- Realization of suitability determination and creation phases i.e. A policy driven & context-aware decision making process based on a combined knowledge of: Context information (Location & mobility, Supported Application, Transmission Power, Capability of Routing, Supported RAT, Environment Characteristics), Policies (Minimization of energy, Maximization of QoS), Profiles (Application Requirements)
- Spectrum Availability decision i.e. a context-aware decision making based on a combined knowledge of: Context information (frequency, RAT, RAT capabilities, velocity, and spectrum sensing), Policies, Profiles (bandwidth selection mechanism which takes into a consideration application requirements)
- Opportunistic Spectrum Selection i.e. a context-aware allocation of available pool of channels on a per link basis, based on a combined knowledge of: Context information (frequency, RAT, bandwidth, frequency band, maximum power, application required bit-rate and Temporal duration), Radio interface (Propagation loss, Noise and interference spectral density, Measured bit rate in the pool currently assigned), Policies, Profiles (terminal capabilities, Maximum transmit power, Supported frequency bands)
- Routing Protocols and protocol selection (context-aware routing and policy-based selection of routing techniques)
- Spectrum mobility (Context Aware vertical handover decision making)

Detailed specification of the context parameters (definition, semantics and structure) is covered in Section 3.3.

2.3.5 Overview of state-of-art

The literature on context-awareness spans European projects, standardization activities and research. In terms of European projects, the following representative (not exhaustive) sample cover many different aspects, ranging from architecture, models and applications to context information acquisition, processing, inference and learning:

An overview of context awareness in IEEE P1900.4 and ETSI RRS is given in the Appendix II in Section 12.

The E3 project [27]addressed context acquisition framework (for autonomous RAT selection) and context learning by defining context awareness related functions (Information Extraction, Collection, and Storage) within E3 functional architecture (both NRM and TRM), as well as external/internal interfaces between NRM and TRM modules related to context awareness, and exchange of context information (not part of P1900.4).

The QoSMoS project addresses context awareness for cognitive spectrum management i.e. knowledge about the operational conditions or context-awareness, is used to define the potential bands and channels that may be used opportunistically and to populate the spectrum portfolio. Project develops methodologies for context acquisition, processing and communication [28][29].

In C2POWER [30] particular interest is on context information related to energy use and consumption.

The WORKPAD project [31] focus was on providing a software and communication infrastructure supporting operators during an emergency. The objective was to investigate how to create communities of Public Safety Systems (PSSs), and how to enable mobile teams to exploit such back-end systems through the interplay of MANET technologies, process management and geo-collaboration. In order to support such a complex scenario, from the provision of data, knowledge & content to front-end teams to their process executions, different research issues were addressed such as: A peer-to-peer architecture, Novel techniques were developed for P2P data, content integration and Adaptive process management, by exploiting context-awareness and process mining, in order to manage coordination of team members.

In ARAGORN [32], focus is on developing enablers for context-sensitive applications in Cognitive Radio Networks and cognitive resource management (CRM), which is context sensitive i.e. makes use of environmental context information such as propagation conditions, existing cells, RATs, services, primary cells in addition to location information, in order to enable/support machine learning based adaptation. Main issues addressed are: context recognition, context based optimization and adaptation and Radio Environment Maps (REMs).

The vision of PERSIST [33] is of a Personal Smart Space, which is associated with the portable devices carried by the user and which moves around with him/her, providing context-aware pervasiveness to the user at all times and places. The Personal Smart Space will cater for the needs of users, adapting to their preferences and learning new ones as these arise. The objective of PERSIST is to develop Personal Smart Spaces that provide a minimum set of functionalities which can be extended and enhanced as users encounter other smart spaces during their everyday activities. They will be capable of learning and reasoning about users, their intentions, preferences and context. They will be endowed with pro-active behaviours, which enable them to share context information with neighbouring Personal Smart Spaces, resolve conflicts between the preferences of multiple users, make recommendations and act upon them, prioritise, share and balance limited resources between users, services and devices, reason about trustworthiness to protect privacy and be sufficiently fault-tolerant to guarantee their own robustness and dependability.

C-CAST [34] is aimed at emerging context-awareness technologies will act as a driving force for introduction of intelligently personalized services in smart spaces. Major novelties include highly scalable context management architecture as well as a context adaptation, representation models, reasoning, content selection and prediction methodology. The context management technology developed aims at combining mobile distribution techniques (both unicast and multicast) and context-awareness in order to optimize multimedia content distribution.

SENSEI [35] defines an architecture that fundamentally addresses the scalability problems for a large number of globally distributed wireless sensor and actuator networks devices. It provides necessary network and information management services to enable reliable and accurate context information retrieval and interaction with the physical environment. By adding mechanisms for accounting, security, privacy and trust it enables an open and secure market space for context-awareness and real world interaction. The SENSEI framework for distributed context processing allows integration of geographically distributed and heterogeneous context sources. In the existing work context processing, frameworks often target the local case with limited heterogeneity of context sources. SENSEI has implemented mechanisms for cross-layer adaptation and optimisation of context composition and processing that are able to ensure context continuity and scalability, taking into account quality of information requirements. This is because existing context frameworks have no or only limited adaptation capabilities with respect to composition and processing of context information. Context information originates from the physical environment and is captured by sensors. There are numerous types of sensors collecting information from a wide variety of physical phenomena ranging from location, temperature information to biological measurements. The system must be able to capture the context information collected from all the sensors. Moreover context information also originates from sources other than sensors such as 3G location systems or presence information from calendar systems.

The scope of context awareness in SENSEI includes modelling of context information and actuation tasks on suitable abstraction levels which includes modelling of sensors and actuators as well as context and services; developing context processing mechanisms to derive appropriate level of abstraction; defining interfaces for retrieving context information and managing actuation tasks,; and identifying quality of information and quality of actuation metrics.

ORACLE [24] defines a policy framework i.e. a support structure for operations on policies. It defines creation, storage and processing mechanisms for policies as well as tools for management and deployment of policies. A policy framework does not define algorithms for this purpose but supports any software architecture needed to implement these algorithms. The policy framework defines the supporting set of functions for processing engines and algorithms, heuristics and databases required for evaluation of policies and generation of actions needed to configure the functions of a terminal. The approach relies on a rule-based reasoning engine for processing policies. Rules are assumed to be configurable at run-time depending on the current context. A number of engines required for pre- and post-processing are also assumed to be rule-based but operate on a very limited set of mostly pre-defined rules.

Rule-based decisions are assumed to allow splitting the complex task of opportunity detection and decision taking into – ideally – mutually independent operations to be processed in consecutive steps or in parallel. The 'behaviour' of a terminal is described in a formal way by defining sets of rules to be applied to sets of input parameters in order to generate sets of output parameters, e.g., configuration parameters or parameters provided to intermediate processing steps.

Three different environments are supported by the framework: a Run-Time Environment, a Configuration-Time Environment and a Testing Environment. Common to each environment are the core processing engines for Raw Context Processing, Reasoning and the Context Watcher.

DYNAMOS project [36] aimed to make efficient use of information and services available in ubiquitous environments. Mobile users need the means for locating relevant content, where relevance has a user-specific definition. In the DYNAMOS project, a hybrid approach that enhances context-aware service provisioning with peer-to-peer social functionalities is considered/investigated.

The MobileVCE Core 4 programme [37] has looked at overcoming the challenges in development and deployment of ubiquitous services from three perspectives: user, content/service provider and network.

To reduce the perceived complexity from a user's perspective, the first innovation developed within this project is a Personal Assistant Agent (PAA) concept [38]. The PAA tailors the delivery of services and content to the most appropriate user device based on a user's personal preferences and current context. It frees users from the challenges associated with device, service and content management across not only their widely dispersed personal devices, but also shared devices to which they have been granted usage rights. Based upon a dynamic understanding of the user's context, the PAA undertakes a range of essential underlying tasks on the users' behalf - discovering and accessing services, reacting to and predicting actions. To be able to do this, the PAA builds an understanding of its surroundings and then makes informed choices about what action to take. Ontology is used to link similar concepts and characteristics to describe relationships between entities, rather than just their features.

The service/content perspective addresses the adaptation requirements, i.e. Service adaptation (Adapting how content is delivered) and Content adaptation (adapting what is delivered). To manage these adaptation requirements, the second innovation from this project is an Adaptation Management Framework (AMF) that autonomously adapts content and services based on the end user's current requirements. To correctly present a service and content to the user, the PAA and AMF between them can decide on the device and encoding to be used, based on the requirements from both the originator and user of the content, without the need for any manual intervention – reducing the management overhead for the former and the perceived complexity for the latter. The PAA and AMF communicate via the industry-standard Web Services interface and with a common OWL-DL ontology, thereby enabling users of these technologies to readily adapt or interface these solutions within the context of their own standard or proprietary technologies.

Besides major research efforts in several EU projects, in the standardization arena there have been major contributions towards enabling context-aware systems through definition and integration of required functionalities in to respective architectures, by ETSI RRS & IEEE 1900.4. The 1900.4 system architecture [20] is based on a split of functionality between terminals and the network and also the information exchange between coordinating entities for optimized resource management in a heterogeneous wireless access network. Two key entities are defined, i.e. a Network Reconfiguration Manager (NRM) and a Terminal Reconfiguration Manager (TRM). The interfaces between these management entities are also specified. Distributed radio resource usage optimization covers the optimization procedures for radio resource usage which is performed by both the network and the terminals in a distributed fashion. The system requirements are classified in three categories, one for each reconfiguration/cognition phase: obtaining context awareness information, making reconfiguration decisions, and the execution of the actual reconfiguration. In ETSI RRS [39], the requirements on functional architecture have resulted in support for Context acquisition function for supporting context awareness, within RRS FA. More specifically, context acquisition is considered as one of the inputs to the Dynamic Self-Organising Network Planning and Management (DSONPM) block, whose main function is to provide the medium and long term decision upon the reconfiguration actions a network segment should take, by considering certain input information, and by applying optimization functionality, enhanced with learning attributes. For further details see Appendix II.

Finally, the following applications of context information and usage, have also been addressed in the literature: Context-aware Scheduling, Context-aware pulse shaping, Context Aware vertical handover decision making, Context-aware end-to-end QoS diagnosis and quantitative guarantee, Context-Aware RRM for Opportunistic Content Delivery, Dynamic Geospatial Spectrum Modelling, Efficient Context-aware Service Discovery, Efficient Context-aware Node Discovery, Context-aware Routing, Context-aware Localisation.

Context management within OneFIT is expected to build on existing work, mainly based on the 1900.4 and E3 architectures and extending these as/if appropriate.

3. Information model and information to be exchanged

This section describes an information model representing an Opportunistic Network and Policies. Further on, it describes the information needed in different CMON and/or CSCI instances to make the opportunistic network related decisions, e.g. on creation, modification and termination of the ONs, including the policy and context information to be exchanged. This information may be exchanged using the C4MS but may also be exchanged by other procedures, e.g. existing RAT specific mechanisms.

3.1 Information models

The following subsection introduces a set of UML models for the OneFIT information model which is based on the E3 information model proposed in [26]. The information model describes the information that is to be managed in terms of exchange, sharing, distribution, and storage within the scope of the OneFIT project.

3.1.1 ON information model

The ON information model as shown in Figure 4 uses the Unified Modelling Language (UML) class diagram as description format.

An Opportunistic Network consists of Nodes and Links. Several links can form a path on which the application data is transported using an ON_Bearer_Service. The ON_Bearer_Service concept is based on the Bearer Service concept as defined by 3GPP e.g. in the UMTS QoS architecture [5]. A node has typically one or more network interfaces which act as endpoint for the links. A node can either be a terminal or a base station.

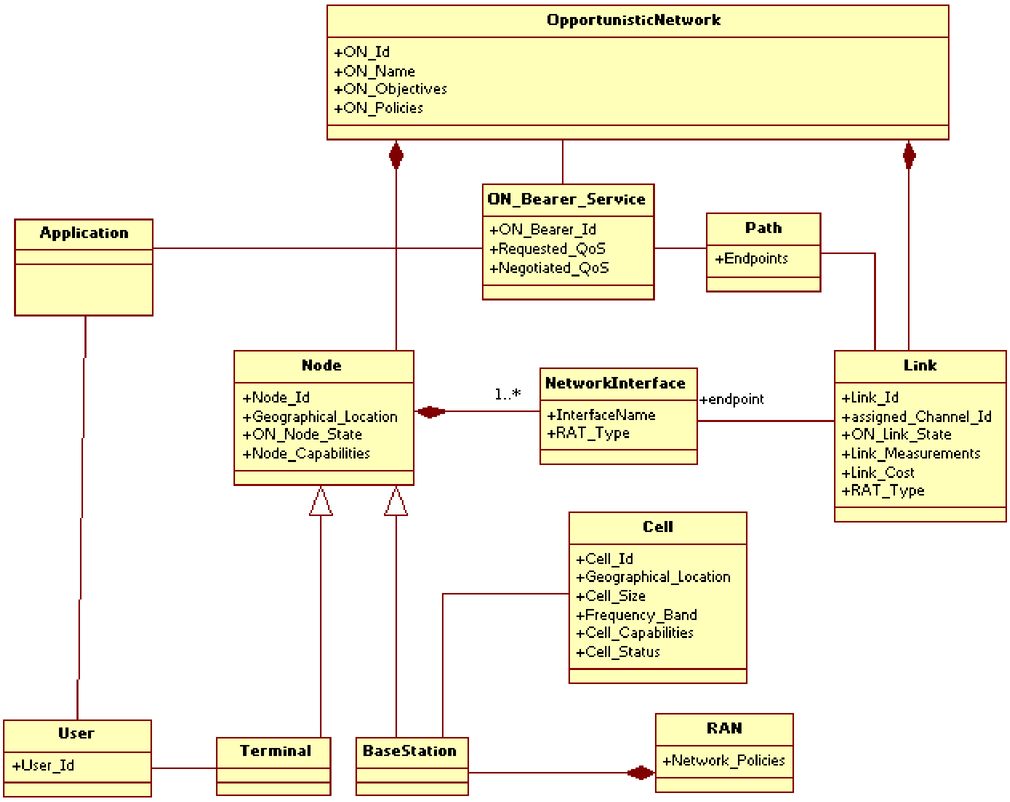


Figure 4: The ON Information Model

3.1.2 Policy information model

A policy can be defined as a set of rules related to different aspects of a system. As mentioned in [25], policies can be used to limit, steer and govern the behaviour of a system (terminals and infrastructure elements) with respect to some predefined goals or objectives.

As the OneFIT system introduces new decision-making processes and therefore multiple possible behaviours, it also creates a new field for policy-based management.

So the OneFIT project is proposing a new type of policy, specific to Opportunistic Network management, typically for the operator to be able to provide and enforce a set of rules on how and when ONs should be created, reconfigured and released.

But the OneFIT system is also requiring decision-making in areas which are already covered by state-of-the-art policy framework as defined by 3GPP or other standards, or by research projects: it has already been identified that, because OneFIT system is designed for dynamically assigned spectrum resources, it would make use of Spectrum Assignment policy. This type of policy was originally proposed within the scope of the E3 project [26] and allows an operator to control when and how spectrum can be assigned to a node (e.g. taking into account requirements for protecting legacy user) and to provide rules related to spectrum sensing aspects.

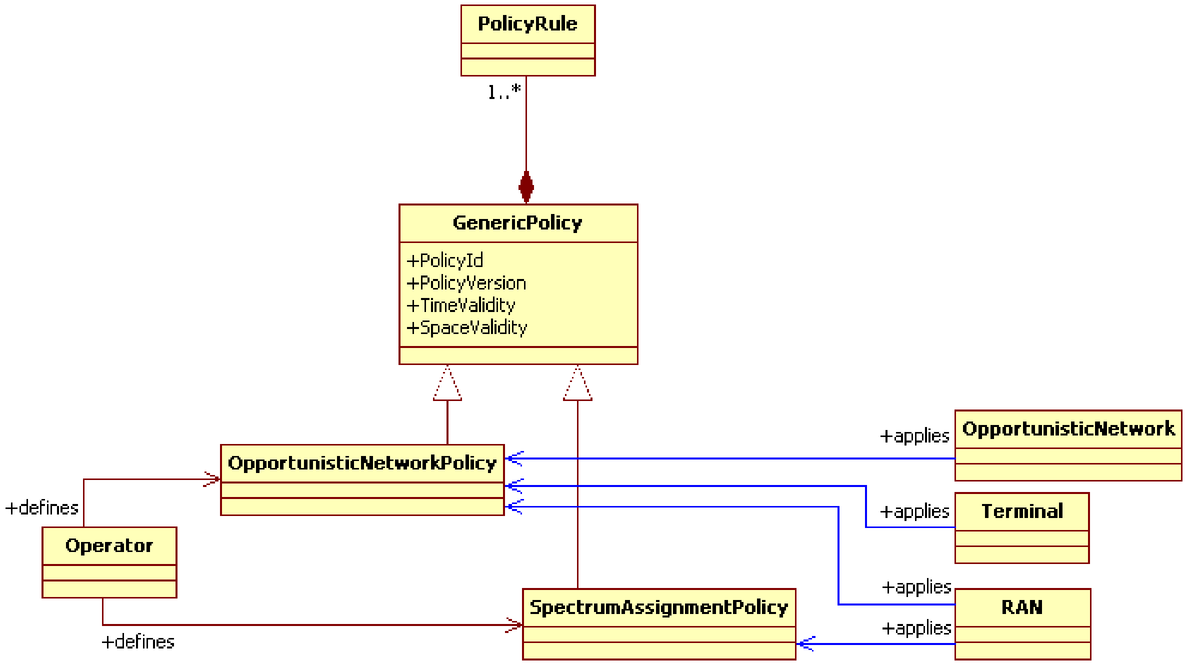


Figure 5: The Policy Information Model

3.2 Policy information to be exchanged

Depending on the scenario and the algorithm (centralized or decentralized) different policy related information may need to be exchanged over C4MS. The following section lists currently identified information.

Generic policy related information:

- Policy Identifier – as multiple policies can be considered, each policy requires a unique identifier,
- Policy Version – current version of a policy
- Time and space validity – covers information on a validity of a given policy in time and space

Opportunistic Network policy related information:

- ON Suitability determination related rule – covers aspects related to the ON suitability phase. A possible rule could e.g.:
  - define a default set of information which needs to be send by users in their beacons to enhance the suitability determination (allows to govern and limit ON related signalling during the ON suitability phase),
  - define a set of triggers which entitle a user to initiate ON suitability determination procedures (e.g. QoS degradation, high energy consumption)
  - define a minimal time which users need to spend on advertising its ON capabilities (in order to limit the energy consumption users could periodically advertise their ON capabilities, keeping their short range radios for the rest of the time switched off),
  - define a maximal time between consecutive ON advertisement periods (in order to limit the energy consumption users could periodically advertise their ON capabilities, keeping their short range radios for the rest of the time switched off),
- ON Creation related rule – covers aspects related to possible ON configurations. A possible rule could e.g.:
  - set limits on a maximal number of users in an ON or a maximal number of hops between a terminal and a base station,
  - enforce users to ignore nodes of other operators or operators with no roaming agreements (this could limit the list of potential ON candidate),
  - set limits on a maximal number of APs from which to stream cached video segments to requesting user/users (streaming a video file which is scattered among many APs requires establishment of many mini streaming sessions which could result in poor QoS)
- ON Maintenance related rule – covers aspect related to the ON maintenance such as reconfiguration procedures or ON related signalling. A possible rule could e.g.:
  - define a set of reconfiguration procedures which are allowed during the maintenance phase (some reconfiguration procedures such as spectrum reallocation may not be allowed),
  - define a minimal allowed delay between consecutive ON reconfigurations,
  - define a default set of context information that needs to be exchanged between ON participants,
  - define default exchange strategies for different types of context information and their respective settings (e.g. thresholds and hysteresis values in case for a triggered based exchange strategy)
- ON Release related rule – covers aspect related to the ON release such as ON release related conditions. A possible rule could e.g.:
  - set limits on a minimal gain which is required to sustain an ON
  - set limits of a minimal number of participants which is required to sustain an ON

Spectrum Assignment policy related information:

- Allowed frequency bands related rule – defines frequency bands which can be potentially allocated to ON participants in a given location. This information can be used by users to identify which frequency bands needs to be scanned and are allowed to be requested for allocation. This information is exchanged during ON suitability determination phase.

- Allowed bandwidth related rule – maximal bandwidth which can be requested for allocation by users in a given frequency band, in a given location. This information is exchanged during ON suitability determination phase.
- Allowed power spectral density related rule – defines a maximal power spectral density which can be used in a given frequency band, in a given location.
- Protection of legacy user related rule – a set of requirements related to the legacy user protection. This information is exchanged during ON creation phase.
    - Allowed mechanisms to obtain spectrum information – The information about spectrum usage is examined by using spectrum sensing techniques, database or control channel depending on the policies on that band
    - Probability of detection– Probability of detecting other user's signal when sensing the channel.
    - Minimum required spectrum sensing time – Time need for spectrum sensing to fulfil probability of detection requirement.
    - Level of signal to be detected – SNR of received signal. There are two levels either high or low which are used to select suitable spectrum sensing technique from three alternatives: energy detection, correlation based detection, and waveform based detection. ,
    - Minimal time between the consecutive sensing periods – Time period how often spectrum monitoring has to be done.
    - Maximal spectrum lease time – Maximum time that spectrum is allowed to be used by ON.

3.3 Context information to be exchanged

The following section describes context information which needs to be exchanged in order to enable creation and maintenance of Opportunistic Networks. The information is subdivided into three different subgroups: Network-wise context, Node-wise context, Link-wise context and Application wise context.

3.3.1 Network-wise context

Network-wise context includes information which is related to a given network. The following context information is identified:

- Congested Base Stations[2] – list of base stations which are determined to be congested.
- Non-congested Base Stations[2] – list of base stations which are determined to be not congested.
- Set of terminals in the congested area[2] -the set of terminals in the congested area which have the ability to create an ON.
- Set of terminals in neighbouring areas[2]– set of terminals in neighbouring non-congested areas that can be used as ON nodes (e.g. in order to reroute traffic to the non-congested elements). The information is collected from multiple Base Stations.

[2] This information is intended to be transferred using the CD interface (i.e. interface which connects CSCI with DSONPM)

3.3.2 Node-wise context

The following subsection provides a description of context information related to a specific node. Different types of Node-wise context information can be distinguished: Terminal specific, Base Station specific and Network interface specific.

- ON Node State – information on a node status in an Opportunistic Network
- Power consumption (average, variation) – information on the total power consumption of a node. It includes the power consumption of different network interfaces as well as the processor
- Node location – information on the geographical location of a node. This information is exchanged during ON suitability determination phase.
- Terminal specific context
    - Status of the available network interfaces (switched on/off, connected/idle) – indicates the status of the available network interfaces (in case of 3GPP interfaces, information on the connected/idle state of the interfaces could be useful to assess the time which is needed to enable service relaying).
    - Fitness value – provides an indication of the energy level, the delivery probability and the availability of a node.
    - Mobility level,
        - Direction – direction of mobile terminal,
        - Velocity (average, variation)- mobile terminal velocity, This information is exchanged during ON suitability determination phase
    - Energy/Battery level – level of the battery in the terminal,
    - Spectrum sensing results in different frequency bands, This information is exchanged during ON creation phase
        - detected energy level (average, variation), – energy level of sensed channel
        - type of detected signal – information on the type of detected signal (e.g. some spectrum sensing are capable of determining the type of the technology which generated detected signal),
        - estimated idle periods, – information on the time that channel is predicted to be vacant and available for ON usage
    - Serving Base Station (BS) (The serving BS of the node -where the node is registered to).
    - Path to serving BS – the path (full list of node ids) in order to reach a serving BS.
    - Terminal relaying capacity – this is an indication of whether a given terminal is able to relay a flow/bearer with a given QoS. This is evaluated after the QoS requirement is provided and based on local processing/queuing resources.
    - Gateway capability – denotes whether a node has an active direct link with the infrastructure and thus has the ability to serve as a gateway towards other nodes.
    - Path list – list of all possible paths from a UE to BSs. The selected path in Section 3.4, that is presented afterwards, will be a subset of this path list.
- Base station specific context

  - Broadcast transmission power – transmission power allocated to the broadcast channel (allows estimating range and coverage of a Base Station)
  - User number – number of users currently served by the BS (Idle-mode UEs are excluded).
  - User list – list of users connected to a base station.
  - User location – location of users connected to a base station.
  - Base Station load – information on the load generated by all users that are currently served by the BS.
  - Files in caching storage – information on a video chunks/files cached by a given Base Station
  - Neighbouring list – list of neighbouring base stations and femtocells. The list can be obtained from the operator or can be computed by a base station itself.
  - Current info on spectrum availability – starting time to be idle of available spectrum blocks
  - Indication of subscriber's group (for a femtocell)- e.g. Closed Subscriber Group (CSG) or Open Subscriber Group (OSG).
- Network Interface specific context
  - Transmission power – transmission power used on a given radio channel
  - Channel measurement results for a given network interface
    - Interference level in a given channel (average, variation)
    - IDs of detected devices in a given channel
    - RSSI for every detected device (average, variation)
    - SINR for every detected device (average, variation)
    - Pathloss for every detected device (average, variation)

3.3.3 Link-wise context

The following subsection describes information which is related to an established link. The following context information is identified:

- Maximal possible link capacity– information on the theoretical maximum achievable bitrate over this link (based on the Network interface capabilities and the link profile)
- RAT type – the RAT used to create a given link
- Endpoint Identifiers – identifiers of nodes which established a given link
- Frequency channel – channel used to create a given link
- Link type – type of the established link (e.g. node to node, node to infrastructure, or infrastructure to infrastructure)
- SINR (average, variation) – Signal to interference and noise ratio measured in the link. Note that received interference power spectral density, including thermal noise, could be derived from this parameter and the knowledge of the useful signal received power and the channel bandwidth.
- RSSI (average, variation) – Received Signal Strength Indication, measure of the useful signal received power in the link.

- Pathloss (average, variation) - Propagation loss of the radio channel between the two end-points of the link (this can be estimated based on a specific propagation model for the considered frequency band together with a distance associated to the terminals in the link or it can be directly measured e.g. from the useful signal received power for a given known transmit power).
- Link capacity (average, variation) – information on the link capacity in terms of achievable bitrate
- Geographical distance between each node– it can be calculated through the geographical coordinates of each node. The use of this metric could give a potential initial indication on whether it is preferable and feasible to establish links between near or far-away nodes.
- Flow specific context
    - Bitrate (average, variation) – information on the measured bitrate for a given flow
    - Latency (average, variation) – information on the measured latency for a given flow

3.3.4 App-wise context

The following section describes the semantics for the application wise context information which is necessary to be exchanged in order to allow successful operation of ON related mechanisms.

- Required QoS
    - Min bitrate – information on the theoretical minimum bit rate required to assure adequate QoS for the user running the application. This information is exchanged during ON suitability determination phase
    - Max latency – information on the theoretical maximum allowed latency to assure adequate QoS for the user running the application. This information is exchanged during ON creation phase
    - Max jitter – information on the theoretical maximum allowed jitter to assure adequate QoS for the user running the application.
- Estimated session duration - Expected temporal duration of an application session (this can be obtained from statistical observation or be a deterministic value for a given realisation of an application). This information is exchanged during ON creation phase
- Elasticity - Parameter that captures different degrees of elasticity of the application with respect to the required bitrate. A high value for this parameter means that the application is rate sensitive (e.g. voice o video traffic stream) while a low value is more representative of elastic traffic as typically generated by data-centric applications (e.g., Web, E-mail).
- Bitrate (average, variation, max value, min value) - Measured bit rate between application endpoints.
- Latency (average, variation, max value, min value) – measured packet delay between application endpoints
- Out of order packets (average, variation, max value, min value) – information on the number of packets which were dropped due to their late delivery

3.4 Decisions be exchanged

The following section describes information which is foreseen to be an outcome of different algorithms/ procedures (defined in the scope of the OneFIT project) and needs to be exchanged between different network as well as terminal entities to enable the proper operation of Opportunistic Networks. The following information is identified:

- Discovery of terminals supporting opportunistic networking related information
    - Radio Access Technologies to be used for discovering of other terminals in the vicinity
    - Selected frequencies/channels to be used for detection of other terminals in the vicinity
    - Additional information like maximum time to be spent for discovery before reporting the results can also be exchanged.
- Spectrum Opportunity Identification related information. This information is exchanged during ON creation phase
    - Selected frequency bands for scanning – information on the frequency bands to be scanned (central frequencies and bandwidths)
    - Selected spectrum sensing technique – information on the technique which needs to be used for spectrum scanning (energy-based, correlation-based, waveform-based)
    - Sensing time – information on the time which terminals need to spend on scanning the spectrum
    - Detection thresholds – information on the detection thresholds for each frequency band selected for scanning
- Spectrum Selection related information. This information is exchanged during ON creation phase
    - Selected spectrum block(s) – information on the frequency blocks selected for transmission (central frequency and bandwidth)
    - Transmission Power constraints – information on the maximum transmit power allowed in the selected spectrum block(s)
- Suitability determination related information
    - Selected candidate nodes – list of nodes that are considered as ON candidates (information allows nodes to initiate the ON creation procedures).
    - Selected Ad-hoc routing protocol – information on the selected ad-hoc routing protocol to be used in an ON to establish routes between terminals (information is sent to all nodes on the candidate list).
- Selection of nodes and routes related information
    - Selected nodes for ON creation – a subset of candidate nodes that is selected as legitimate to participate to the creation of the ON.
    - Selected path– information on a selected path. The path includes a starting point (e.g. a terminal in the congested region), an ending point (e.g. a BS), and the links that create the full path from the starting to the ending point (each link is identified by a starting point and ending point each of which is an intermediate node). Additionally, in some scenarios, the information on the selected path may also include:
        - Allocation of RATs – information on the Radio Access Technologies which are to be used to establish links between adjacent nodes in the selected route

        - Transmission power allocation – information on the transmission power which is to be used on links between adjacent nodes in the selected route
        - Spectrum/Channel allocation – information on the selected channels/spectrum which is to be used on links between adjacent nodes in the selected route
    - Assignment of users to femtocell[3] – determines which user is assigned to which femtocell (capacity extension through femtocells scenario).
    - Assignment of QoS to users[3] - the QoS that is being assigned to the users of the femtocells and to the remaining users of the previously congested BS (capacity extension through femtocells scenario).
- Ciphering key – information on the ciphering key which is to be used over the node-to-node link
- Application to route assignment – information on an assignment between an application and a route (in some scenarios a node could be reached over multiple routes)
- Selected nodes for caching – information on a caching scheme. The information includes a list of Access Points and video chunks which needs to be cached by the Access Points.
- Video Streaming schedule – information on which network nodes (APs, video servers, etc.) should be requested by a user to obtain a specific chunk of a specific video file (the information is sent to the user which requested a video streaming service)
- Selected nodes for re-caching – information on a re-caching scheme. The information includes a list of Access Points and video chunks which should be re-cached between these Access Points

3.5 Profiles, capabilities and requirements to be exchanged

The following section describes information related to profiles, requirements and capabilities which needs to be exchanged in order to enable creation and management of Opportunistic Networks.

- Terminal Capabilities
    - ON capability – indicator if a terminal supports ON
    - Supported Network Interfaces – list of supported network interfaces (supported RATs). This information is exchanged during ON suitability determination phase.
    - Routing/Relaying capability – information on the terminal routing capabilities (e.g. which ad-hoc routing protocols are supported).
    - Multiple connection capability – denotes whether a node can support multiple connections simultaneously to other nodes/terminals.
    - GPS capability – indicator if a terminal supports GPS positioning.
    - Display resolution – information on a display resolution capability of a terminal. The information is necessary to determine the most appropriate video streaming quality.
    - Spectrum sensing capability – indicator if a terminal supports spectrum sensing.
- Base station capabilities
    - ON capability – indicator if a base station supports ON.

[3] This information is intended to be transferred using the existing RAT specific signalling

  - Supported Network Interfaces – list of supported network interfaces (supported RATs).
  - Caching and streaming of video capability – indicator if a base station supports caching and streaming of video.
  - Cache size – information on a cache size of a base station.
- Network Interface capabilities[4]
  - Supported frequency bands – list of the operating frequency bands supported by the network interface (e.g. 880–915/925–960 MHz band, ISM 2.4 GHz band, etc.).
  - Supported channels – information on the supported frequency channel arrangements (carrier frequencies, channel bandwidths) in the different operating bands.
  - Maximum transmit power – information on the maximum output power supported in this interface.
  - Maximal supported velocity – information on maximal velocity that terminal's technology is assured to send and receive data without significant degradation
  - Maximal Bitrate supported – information on maximal bitrate that terminal's technology can achieve. This information is exchanged during ON suitability determination phase
  - Spectrum aggregation capabilities – an indicator if a network interface (RAT) is capable of spectrum aggregation
- Spectrum sensing capabilities[5], This information is exchanged during ON creation phase
  - Supported frequency bands – Frequency bands that are supported to be scanned by user device.
  - Energy based sensing capability – an indicator if terminal supports energy detection.
  - Correlation based sensing capability – an indicator if terminal supports correlation based detection.
  - Waveform based sensing capabilities – an indicator if terminal supports waveform based sensing capabilities.

Profile related information

- User Profile
  - Supported applications – the set of applications/services that are included in the contract of the user
  - QoS and QoE requirements – information on the end user application QoS and QoE requirements
  - ON related preferences – clarifies when and on which conditions a given user is willing to participate in an ON

[4] The exchange of network interface capabilities is necessary in case a node does not support given radio access technology and does not have any a priori information about it.

[5] The exchange of spectrum sensing capabilities is necessary as in a heterogeneous environment terminals may support different spectrum sensing techniques.

        - QoS triggering level – denotes a minimal QoS level which triggers the ON suitability determination or a minimal battery level which allows a user to participate in an ON as a relay.
        - Relaying Capacity – information on a maximal number of other user connection's which is allowed to be relayed by a given user
        - Relaying Interfaces – list of network interfaces (RATs) which are permitted be a user to be used for relaying of traffic for other users
        - Remote connection setup – denotes if other users can trigger a connection setup procedure within a terminal of a given user (in some cases users which request their traffic to be relayed could trigger a connection setup in the relaying terminal)
        - Supported Incentives – list of incentives required by a given user to provide relaying services for other ON participants
    - Video preferences
        - Video genres – list of favourite video genres
        - Video quality – list of preferred video qualities
        - Artists – list of favourite artists

3.6 Knowledge to be exchanged

The following section describes knowledge related information which can be obtained throughout the network operation and could be exchanged in order to improve the creation and management of Opportunistic Networks. The knowledge related information is briefly subdivided into ON related knowledge and spectrum related knowledge.

- Spectrum related knowledge
    - Historic info on spectrum availability – average of idle time for available spectrum blocks
    - Estimate channel availability – estimated time of channels availability according to traffic predictions This information is exchanged during ON suitability determination phase
    - PU activity level on spectrum bands – Information on the PU activity level on a specific spectrum band (duty cycle)
- Base station related knowledge
    - Historic info on base station load – Historic load information as generated by all users served by the BS
- Overall ON statistics
    - ON Location – information on the ON location (as ONs may be more likely to be created in certain locations rather than others, the exchange of knowledge related to the previous locations of ONs may improve decision making within other nodes)
    - User Resource utilization – information on the resource utilization which can be obtained when user is involved in an ON
    - ON Signalling overhead – information on the signalling overhead introduced by the ON related procedures

- Experienced QoS/QoE – application specific QoS and/or QoE reported by a user in an Opportunistic Network
- Number of rejected or accepted requests – number of requests generated by a specific user which was accepted or rejected by other users (this information could be used to assess the trustworthiness of users).
- User activity time (average, variation) – time spend by a specific user in an ON. This information can be used in order to improve the future node selection (e.g. users that disconnect form an ON just after creation may not be accepted in the future)

4. Elementary procedures

This section describes a draft version of elementary ON management procedures and messages to be supported over C4MS. The following messages are currently defined as an initial set for the interaction between CSCI/CMON entities which are C4MS users (the list is derived based on the Message Sequence Charts described in on D2.2 [2]):

- Information.Request, Information.Answer, Information.Indication
- ON_Suitability.Indication
- ON_Negotiation.Request, ON_Negotiation.Answer
- ON_Creation.Request, ON_Creation.Answer
- ON_Modification.Request, ON_Modification.Answer
- ON_Release.Request, ON_Release.Answer
- ON_Status.Notification

The Messages are specified in this section using the ABNF specification. For more details on the ABNF specification, see IETF RFC 3588 [13], Section 3.2. As a short summary, the following syntax is used to define fixed, required and optional parameters (The parameters are called Attribute-Value-Pairs (AVPs) as in [13]):

```
message = header  [ *fixed] [ *required] [ *optional][ *fixed]


fixed        = [qual] "<" avp-spec ">"
               ; Defines the fixed position of an AVP


required     = [qual] "{" avp-spec "}"
               ; The AVP MUST be present and can appear
               ; anywhere in the message (mandatory parameter)


optional     = [qual] "[" avp-name "]"
               ; The avp-name in the 'optional' rule cannot
               ; evaluate to any AVP Name which is included
               ; in a fixed or required rule.  The AVP can
               ; appear anywhere in the message.


qual         = [min] "*" [max]
               ; See ABNF conventions, RFC 2234 Section 6.6.
               ; The absence of any qualifiers depends on whether
               ; it precedes a fixed, required, or optional rule.
               ; If a fixed or required rule has no qualifier,
               ; then exactly one such AVP MUST be present.
               ; If an optional rule has no qualifier,
               ; then 0 or 1 such AVP may be present.
```

```
;
; NOTE:  "[" and "]" have a different meaning than in ABNF
; (see the optional rule, above).
; These braces cannot be used to express optional fixed
; rules (such as an optional ICV at the end).
; To do this, the convention is '0*1fixed'.
```

4.1 Information provisioning

The information provisioning procedure is used to exchange information between nodes.

This procedure can be used to exchange different types of information, e.g.:

- Neighbourhood-Information
- Node-status
- Node-capabilities
- User-profile
- Geographical-Location
- ON-Policies
- Link Measurements

Example scenarios using information request/answer and information indication are shown below in Figure 6 and Figure 7, respectively:

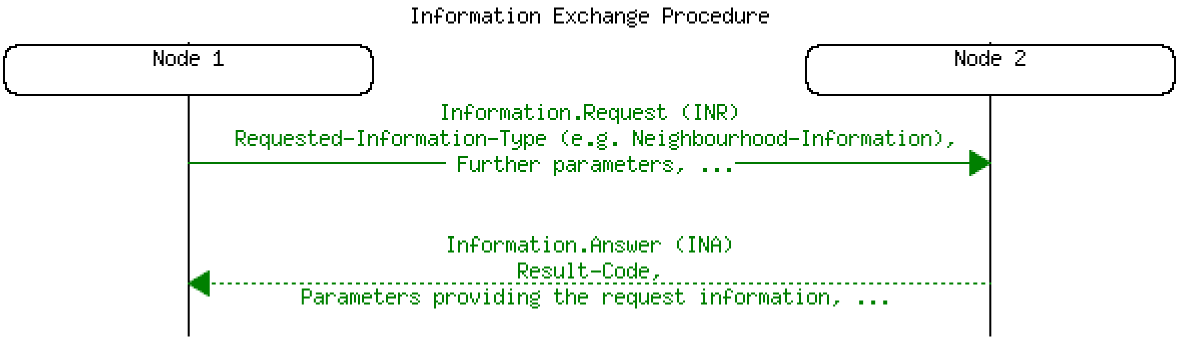

Information Exchange Procedure
Node 1
Node 2
Information.Request (INR)
Requested-Information-Type (e.g. Neighbourhood-Information),
Further parameters, ...
Information.Answer (INA)
Result-Code,
Parameters providing the request information, ...

Figure 6: Information provisioning scenario using Information.Request/Answer

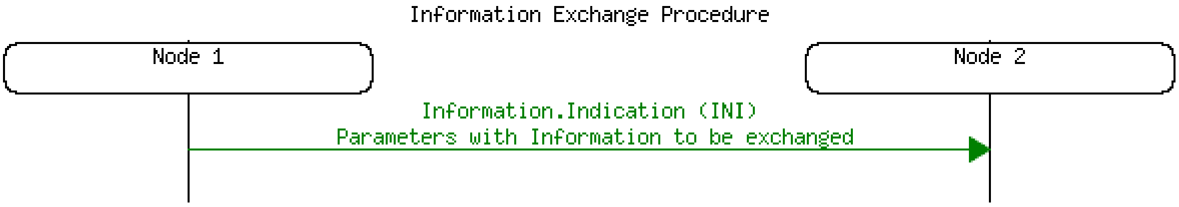

Information Exchange Procedure
Node 1
Node 2
Information.Indication (INI)
Parameters with Information to be exchanged

Figure 7: Information provisioning scenario using Information.Indication

4.1.1 Information-Request (INR)

The Information-Request (INR) may be sent by any node to retrieve information from another node.

Message Format:

```
<INR> ::= <Header>
            * { Requested-Information-Type }
            * [ AVP ]
```

4.1.2 Information-Answer (INA)

The Information-Answer (INA) is sent in response to the INR to provide the requested information or to indicate why this was not possible.

Message Format:

```
<INA> ::= <Header>
              { Result-Code }
            * [ AVP ]
              [ Error-Message ]
            * [ Failed-AVP ]
```

4.1.3 Information-Indication (INI)

The Information-Indication (INI) is used to send information to another node.

Message Format:

```
<INI> ::= <Header>
            * { Information-Type }
            * [ AVP ]
```

4.2 Node discovery

The node discovery procedure is used by a first node to discover other nodes in its vicinity. Such procedures typically exist in each RAT. For opportunistic networking, the existing node discovery procedures should be extended to indicate if a node is supporting opportunistic networking (e.g. by adding extra parameters). Then the node discovery procedure can also be used to detect ON-capable nodes. Two types of procedures typically used in existing RATs are introduced in Sections 4.2.1 and 4.2.2.

4.2.1 Listen on broadcasted information (Beacons/Broadcast channel information)

A node 1 (e.g. a terminal) listens on broadcasted information sent out by another node (e.g. a base station, a WLAN Access Point or a terminal in an ad-hoc network) as illustrated in Figure 8.

Existing broadcast information may be extended to provide additional information if opportunistic networking is supported. If such information cannot be provided in a beacon, this information must be retrieved via other procedures.

- Dependent on the radio access technology, different methods are used to broadcast information:
- Beacons are used e.g. in 802.11 WiFi networks [9]to periodically send out information like Service Set Identifier (SSID), timestamp, supported data rates and capability information.

Beacons are sent out by access points as well as typically by at least one node in an ad-hoc network.

- Broadcast messages are used by base stations (e.g. GSM, UMTS, LTE) to provide cell-related information to all users in a cell.

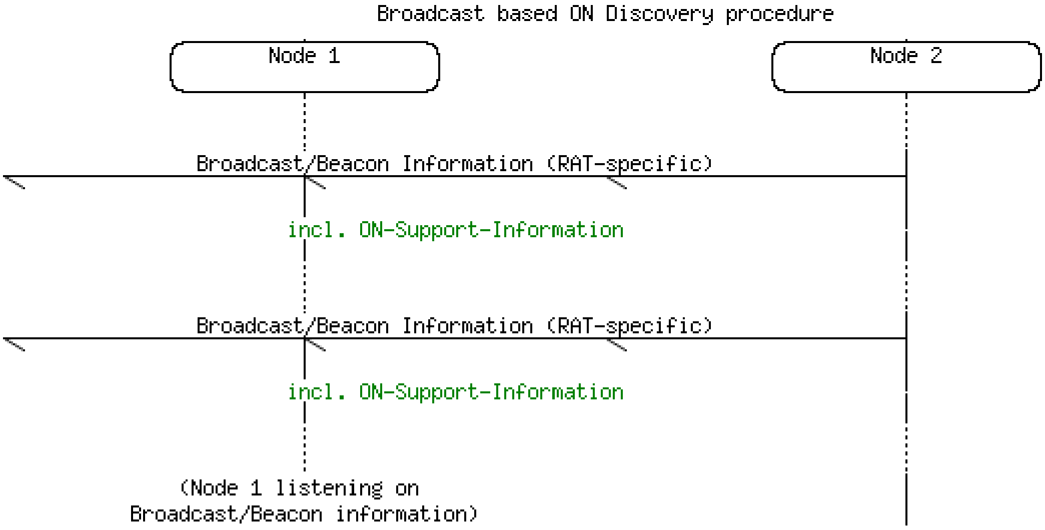

Broadcast based ON Discovery procedure
Node 1
Node 2
Broadcast/Beacon Information (RAT-specific)
incl. ON-Support-Information
Broadcast/Beacon Information (RAT-specific)
incl. ON-Support-Information
(Node 1 listening on
Broadcast/Beacon information)

Figure 8: Broadcast based ON Discovery Procedure

4.2.2 Request/response based discovery (e.g. probing)

A node 1 (e.g. a terminal) sends out a discovery-request (e.g. probe-request in 802.11) and waits for a discovery-answer (e.g. probe-response in 802.11) as shown in Figure 9. Such a discovery response contains information like capability information and supported data rates. As an extension for opportunistic network, additional information may be added to indicate if opportunistic networking is supported, e.g. by extending 802.11u [10]. If such information cannot be provided in the discovery-answer/probe-response, this information must be retrieved via other procedures.

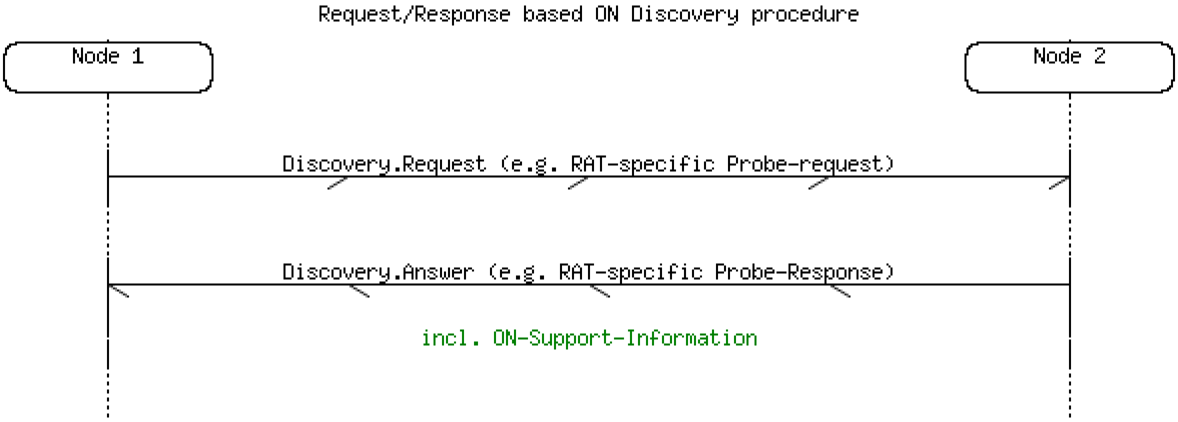

Request/Response based ON Discovery procedure
Node 1
Node 2
Discovery.Request (e.g. RAT-specific Probe-request)
Discovery.Answer (e.g. RAT-specific Probe-Response)
incl. ON-Support-Information

Figure 9: Request/response based discovery procedure

4.3 ON suitability

The ON Suitability procedure is used by a first node to initiate the ON suitability determination in a second node (see Figure 10). This procedure is typically used in scenarios where the Node 1 has discovered a situation where an ON consisting of other nodes may be suitable, but where Node 1 is not necessarily part of the ON and thus cannot decide on the suitability of an ON. Examples for such scenarios are the opportunistic capacity extension scenario (Scenario 2 in D2.2 [2]) or the infrastructure created opportunistic ad-hoc networking (Scenario 3 in D2.2).

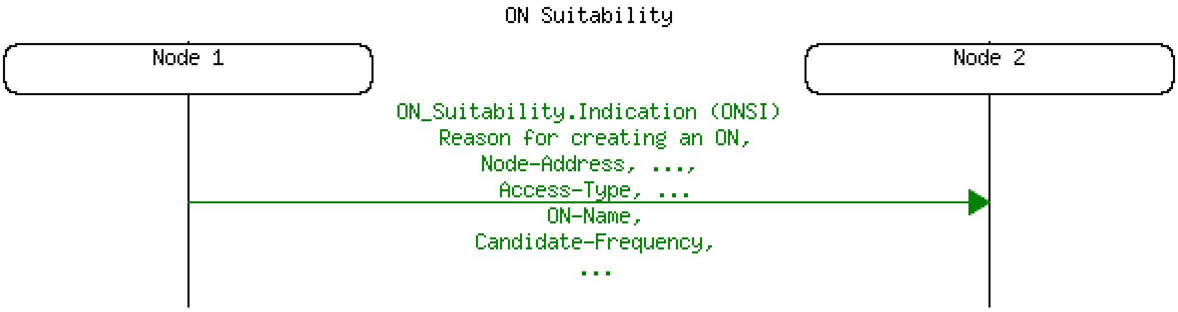


Figure 10: ON Suitability Procedure

4.3.1 ON-Suitability-Indication (ONSI)

The ON-Suitability-Indication (ONSI) shown in Figure 10 is sent by a node to initiate the ON suitability determination in another node.

Message Format:

```
<ONSI> ::= <Header>
                { Reason   }
              * { Node-Address }
              * [ Access-Type ]
              * [ Candidate-Frequency ]
              * [ AVP ]
```

Parameters:

- Reason: The reason for creating an ON e.g. low QoS or load of the surrounding BSs
- Node-Address(es): List of nodes potentially involved in an ON
- Access-Type: RAT(s) proposed for the ON. This information may be used to switch on those RATs for the discovery procedure.
- Candidate-Frequency: Allocated or candidate spectrum band(s),
- Other parameters (FFS): e.g., in the capacity extension through maximum flow scenario, it contains the list of congested and non-congested BSs, while in the capacity extension through femtocells it contains the status of congested BSs and femtocells.

4.4 ON negotiation

The ON Negotiation procedure is used to negotiate about the creation or modification of an ON, e.g. if a node is willing to join an ON, the conditions for joining and to exchange node capabilities and context information.

An example ON Negotiation is shown in Figure 11 below:

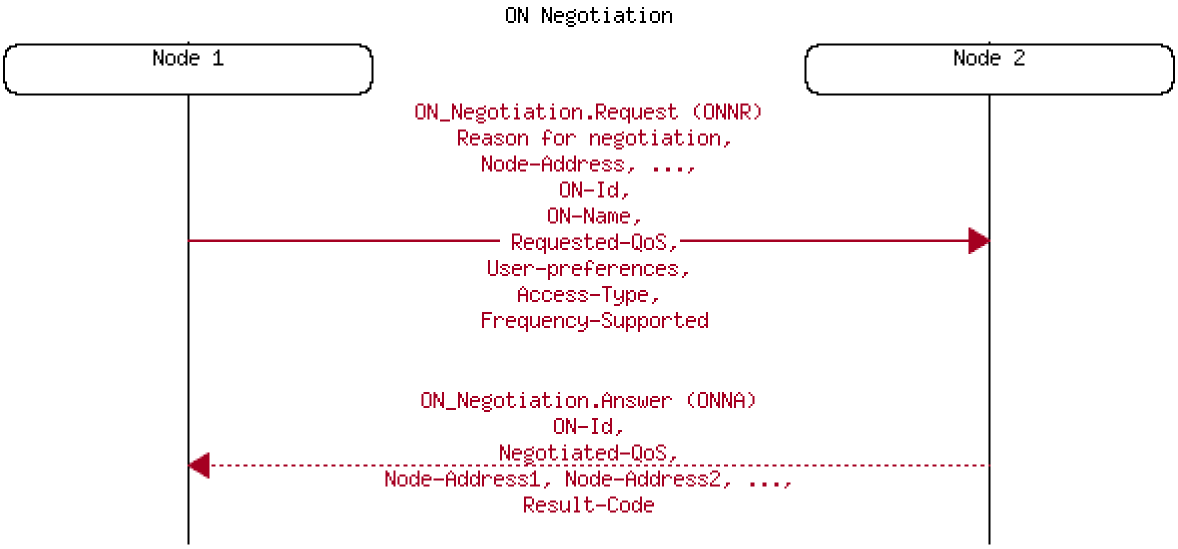


Figure 11: ON Negotiation Procedure

4.4.1 ON-Negotiation-Request (ONNR)

The ON-Negotiation-Request (ONNR) may be sent by any node to negotiate about the creation or participation in an opportunistic network.

Message Format:

```
<ONNR> ::= <Header>
                { Reason }
              * { Node-Address }
                { ON-Id }
                { ON-Name }
                [ Requested-QoS ]
                [ User-preferences ]
              * [ Access-Type ]
              * [ Frequency-Supported ]
              * [ AVP ]
```

The Node-Address may include further info, e.g. if it is a source node or a relay node.

The message contains information on capabilities (e.g. supported RATs and frequency bands, maximum transmit power) and requirements (e.g. QoS, latency, bit rate) of nodes.

4.4.2 ON-Negotiation-Answer (ONNA)

The ON-Negotiation-Answer (ONNA) is sent in response to the ONNR. The ONNR includes if a node is willing to participate in an ON.

Message Format:

```
<ONNA> ::= <Header>
               { Result-Code }
             * { ON-Id }
```

```
                * { Node-Address }
                  [ Negotiated-QoS ]
                  [ Error-Message ]
                * [ Failed-AVP ]
                * [ AVP ]
```

4.5 ON creation

The ON Creation procedure is used to create an ON after successful negotiation.

An example scenario is shown in Figure 12 below:

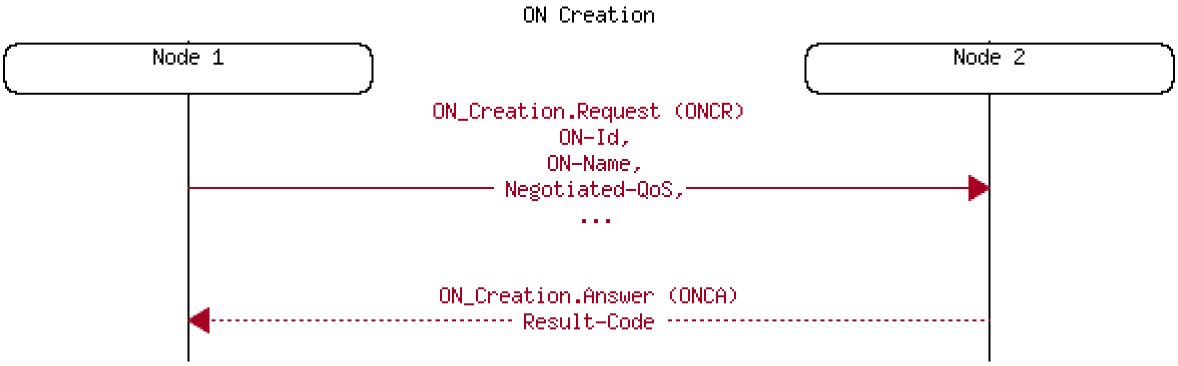


Figure 12: ON Creation Procedure

4.5.1 ON-Creation-Request (ONCR)

The ON-Creation-Request (ONCR) is sent to create an Opportunistic Network. This message can contain the detailed information of the ON such as the nodes involved and the spectrum band to be used.

Message Format:

```
<ONCR> ::= <Header>
                { ON-Id }
                { ON-Name }
              * { Node-Address }
                [ Negotiated-QoS ]
                [ Geographical-Location ]
              * [ AVP ]
```

4.5.2 ON-Creation-Answer (ONCA)

The ON-Creation-Answer (ONCA) is sent in response to the ONCR and indicates if the ON is successfully created or not.

Message Format:

```
<ONCA> ::= <Header>
                { Result-Code }
                [ Error-Message ]
```

```
                  * [ Failed-AVP ]
```

4.6 ON modification

The following procedure illustrated in Figure13 is used to enable a modification of an ON configuration. The modification can be conducted for a single node, multiple nodes or the whole ON. A negotiation procedure may be optionally executed before the ON Modification is executed.

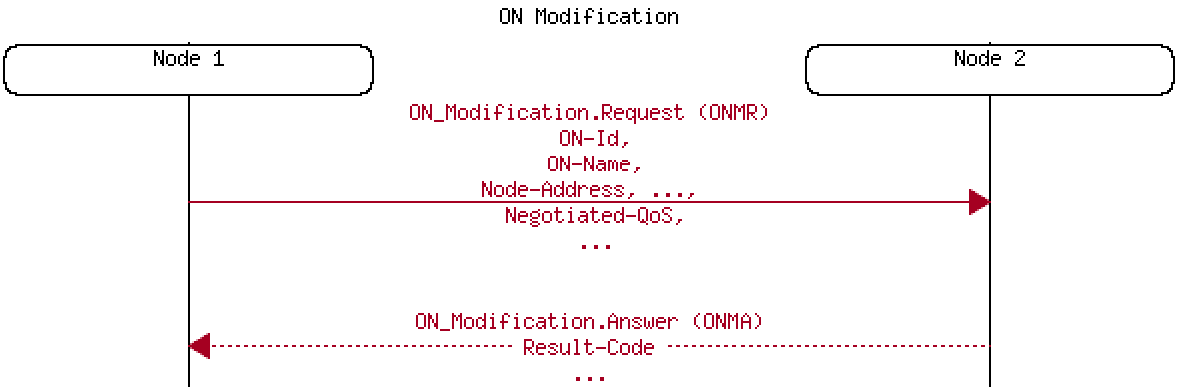


Figure13: ON Modification Procedure

4.6.1 ON-Modification-Request (ONMR)

The ON-Modification-Request (ONMR) may be sent by any node to modify the configuration of an opportunistic network.

Message Format:

```
<ONMR> ::= <Header>
                    { Reason }
                    { ON-Id }
                    { ON-Name }
                  * { Node-Address }
                    [ Negotiated-QoS ]
                  * [ AVP ]
```

4.6.2 ON-Modification-Answer (ONMA)

The ON-Modification-Answer (ONMA) is sent in response to the ONMR and indicates if the ON is successfully modified or not.

Message Format:

```
<ONMA> ::= <Header>
                    { Result-Code }
                    [ Error-Message ]
                  * [ Failed-AVP ]
```

4.7 ON release

The ON Release procedure is used to release a node from the ON or to release the complete ON. An example scenario is shown in Figure 14 below:

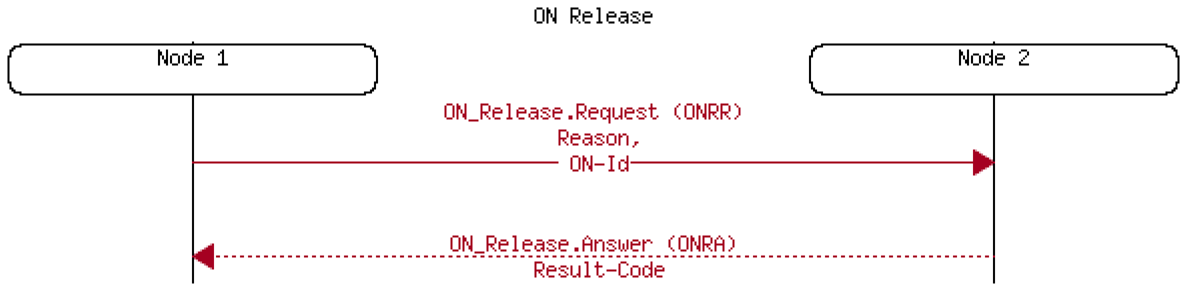


Figure 14: ON Release Procedure

4.7.1 ON-Release-Request (ONRR)

The ON-Release-Request (ONRR) is sent to release a link or a node from an ON.

Message Format:

```
<ONRR> ::= <Header>
                { Reason }
                { ON-Id }
              * [ AVP ]
```

4.7.2 ON-Release-Answer (ONRA)

The ON-Release-Answer (ONRA) is sent in response to the ONRR.

Message Format:

```
<ONRA> ::= <Header>
                { Result-Code }
                [ Error-Message ]
              * [ Failed-AVP ]
```

4.8 ON status notification

The procedure shown in Figure 15 is used by a first node to inform a second node about the status or status changes in an ON. A Notification-Event-Type describes the event to be reported, e.g.

- ON_Negotiated
- ON_Created
- ON_Modified
- ON_Released

This procedure is used for example to notify the infrastructure about creation, modification or release of an ON and may be used e.g. for accounting and billing purposes.

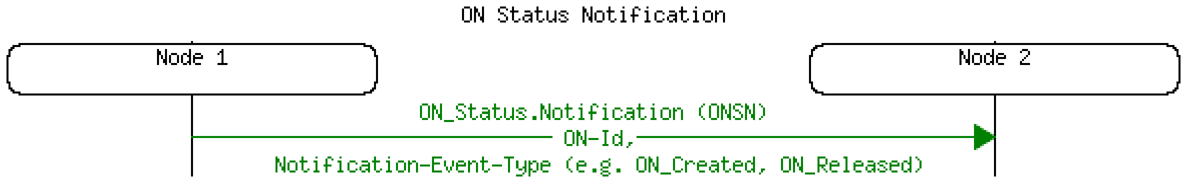

ON Status Notification
Node 1
Node 2
ON_Status.Notification (ONSN)
ON-Id,
Notification-Event-Type (e.g. ON_Created, ON_Released)

Figure 15: ON Status Notification Procedure

4.8.1 ON-Status-Notification (ONSN)

The ON-Status-Notification (ONSN) may be sent by any node to notify about a status of an ON.

Message Format:

```
<ONSN> ::= <Header>
                { ON-Id }
                { Notification-Event-Type }
              * [ AVP ]
```

Further information like involved nodes, type of applications, time and amount of exchanged data can be included in this message.

4.9 Security related procedures

4.9.1 Transmission level security

It shall be possible to transport the C4MS messages in a secured way. Dependent on the chosen approach, this can be made via RAT-specific security procedures or via higher layer procedures like IPsec [12] or TLS [11].

4.9.2 Authentication and authorization

In order to provide Authentication and Authorization, existing security mechanisms shall be reused. Dependent on the chosen approach, this can be made via RAT-specific security procedures or via higher layer procedures.

Security related parameters may be included in the previously described messages or may be exchanged using additional messages.

One example of a higher-layer Authentication and Authorization procedure using additional messages is the Re-Auth-Request/Response as defined in the Diameter base protocol [13]:

The Re-Auth-Request (RAR), may be sent by any server to the access device that is providing session service, to request that the user be re-authenticated and/or re-authorized.

Message Format:

```
<RAR>  ::= < Header >
< Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                 { Re-Auth-Request-Type }
                 [ User-Name ]
                 [ Origin-State-Id ]
               * [ Proxy-Info ]
               * [ Route-Record ]
               * [ AVP ]
```

The Re-Auth-Answer (RAA) is sent in response to the RAR. The Result-Code AVP must be present, and indicate the disposition of the request. A successful RAA message must be followed by an application-specific authentication and/or authorization message.

Message Format:

```
<RAA>  ::= <Header>
< Session-Id >
                 { Result-Code }
                 { Origin-Host }
                 { Origin-Realm }
                 [ User-Name ]
                 [ Origin-State-Id ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
               * [ Failed-AVP ]
               * [ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Host-Cache-Time ]
               * [ Proxy-Info ]
               * [ AVP ]
```

4.10 Addressing schemes

OneFIT does not intend to invent new addressing schemes but will reuse existing addressing schemes. Dependent on the selected C4MS implementation option, the C4MS shall support Layer-2 addressing schemes or Layer-3 addressing scheme or both.

4.10.1 Addressing schemes on Layer 2 and below

On Layer-2 (Data Link Layer), the addresses are (radio access) technology dependent.

The following list gives an overview on the most relevant data types used for addressing on layer 2 for OneFIT:

- MAC Address: The Media Access Control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. A MAC-address has typically 6 byte length.
- Cell-ID: Identifies a cell unambiguously within a network (e.g. a PLMN). Examples:
    - In UMTS (see 3GPP TS 25.331 Sect. 10.3.2.2) the Cell-ID can have a value from 0 to 268435455 (28 bit = 3.5 byte).
    - For WLAN, the BSSID, which contains the MAC-Address, is used as Cell-Id.
- Access-Network-ID: The network ID is used to identify the access network. Examples:
    - In UMTS, the PLMN (Public Land Mobile Network) Id contains 3 digits MCC (Mobile Country Code) and 2 or 3 digits MNC (Mobile Network Code) (See 3GPP TS 25.331)
    - For WLAN, the SSID (Service Set Identifier) contains 1..32 octets.

4.10.2 Addressing schemes on Layer 3 and above

On Layer 3 (Networking layer), the addressing scheme is independent of the underlying technology.

The following list gives an overview on the most relevant data types used for addressing on layer 3 and above for OneFIT:

- IP Address: This can either be an IPv4 or an IPv6 address
- Port Address: Used in conjunction with TCP, UDP or SCTP to address a specific port.
- Uniform Resource Identifiers (URI) as specified in IETF RFC 3305 with a syntax like "scheme://" FQDN [port] [transport] [protocol] e.g.
  - http://host.example.com:1812
  - aaa://host.example.com:6666;transport=tcp;protocol=diameter

4.10.3 Additional identifiers for opportunistic networking

In addition to the above presented addressing schemes, OneFIT introduces two additional identifiers:

- ON_Id: The “Opportunistic Network Id” is an identifier to for an opportunistic network and consists of an unsigned integer with 32 byte length.
- ON_Name: The “Opportunistic Network Name” contains a representative name of the Opportunistic Network. In this String, each Character or Digit is included in ASCII-Format.

5. Message sequence charts

Five different scenarios have been identified for OneFIT and described in detail in D2.1 [1]. Document D2.2 [2] Section 5 contains the corresponding message sequence charts (MSCs) for all of these scenarios: Message pairs exchanged over the CI-Interface via C4MS are depicted in green (the CI-Interface is used for the "Coordination with the Infrastructure"), message pairs exchanged over the OM-Interface via C4MS are depicted in red (the OM-Interface is used for the "Opportunistic Management"), and node internal messages are shown in blue. Messages and message pairs that are RAT specific are drawn in black. In this document, the same colour scheme is maintained.

The MSCs provided in this section are based on the MSCs presented in D2.2 [2] but elaborate more on each of the ON phases (i.e. Suitability determination, Creation, Maintenance, Termination), thus providing more detail. Additionally, the MSCs apply to the updated set of elementary procedures presented in Section 4.

5.1 Scenario 1: Opportunistic coverage extension

A set of message sequence charts for opportunistic coverage extension scenario is shown in this section. The proposed message sequence charts analyze different phases of the ON life cycle i.e. suitability determination, creation, maintenance and termination.

5.1.1 ON suitability determination

During the ON Suitability determination phase nodes determine if it is beneficial to establish an ON. The decision is based on some limited information which is collected by nodes from different sources (e.g. internal sensors, neighbouring nodes, operator). This information may include policies, profiles, or limited context information. As the result of the ON Suitability determination a list of potential ON candidates can be established. It is worth noting here that as nodes can join and leave an ON, the ON Suitability determination needs to be continuously conducted during the entire ON activity period.

The ON suitability determination in case of the Opportunistic coverage extension scenario can be triggered by different events. These events could include e.g. a network discovery failure or network attachment failure. The network discovery failure in this case would be triggered in case a node does not detect any suitable access network to establish a link. The network attachment failure would be triggered in case a node cannot attach to any of the discovered networks e.g. due to some temporal network overload or an authentication/authorization failure.

The following section presents message sequence charts related to the suitability determination phase. It is worth noting that the following MSCs are applicable also to scenarios with more than two UEs involved.

Initial Stage

In both use cases presented in following sub-section (network supported or terminal initiated) the MSC presented in Figure 16 is applicable. Procedure presented below, if conducted with no problems (i.e. each message was successfully received and processed) will be referred to as initial setup. Steps taken in initial setup are as follows:

1. UE#1 discovers and attaches to the infrastructure. Discovery and attach mechanisms are RAT specific. The attach mechanism can include authentication & authorisation as well as registration procedures for getting access to infrastructure network services.

2. Before starting the ON suitability determination phase, it could also happen that the BS let terminals know about its ON supported features as well as some basic ON policies. This can be achieved by means of the Information-Indication (INI) procedure.

3. Optionally, ON capabilities of the terminals and ON profiles of the users could be requested at this point by the infrastructure by means of the Information-Request (INR) procedure. This information could be used to support a network initiated ON creation, as shown in Figure 38.

4. UE#1 provides BS with the requested information by sending an Information-Answer (INA) message.

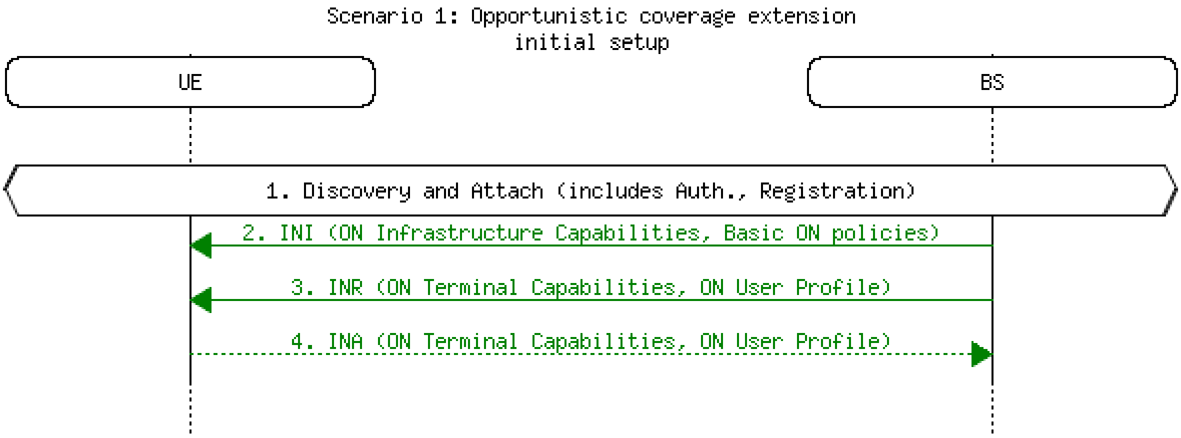

Scenario 1: Opportunistic coverage extension
initial setup
UE
BS
1. Discovery and Attach (includes Auth., Registration)
2. INI (ON Infrastructure Capabilities, Basic ON policies)
3. INR (ON Terminal Capabilities, ON User Profile)
4. INA (ON Terminal Capabilities, ON User Profile)

Figure 16: Scenario 1 – Opportunistic coverage extension – initial stage

Network Supported

The following MSC illustrates a situation in which a Base Station/Infrastructure supports UEs in suitability determination. It is worth noting here that the network support is only possible in case network is aware of out-of-coverage UEs. Such situation may happen if 1) an UE was connected to the network and was dropped due to some infrastructure element failure (e.g. a Base Station failure) or 2) an UE is connected to the network and is getting closer to an out-of-coverage area. Having knowledge about out-of-coverage UEs network operators may support establishment of ON networks in a given area.

Preconditions: Short range radios in UE#1 and UE#2 are switched on, UE#1 is registered and connected to BS#1, UE#2 is registered to BS#2

Description of the messages used in Figure 17:

1. Initial setup as specified in Figure 16 between UE#2 and BS#2

2. Initial setup as specified in Figure 16 between UE#1 and BS#1

3. UE#1 starts an application session using a direct link with BS#1

4. BS#1 shutdown/failure, UE#1 is out-of-coverage

5. UE#1 experiences a link failure.

6. BS#2 receives information from the O&M about the BS#1 failure and UEs which were connected to BS#1 and initiates suitability determination procedures.

7. As there are no other networks in the neighbourhood it switches on its short range radios and initiates ON suitability determination procedures.

8. BS#2 informs UE#2 about an out-of-coverage UE in its area using an ON_Suitability.Indication message. Additionally, BS#2 may provide support by suggesting the most appropriate short range interface, etc. The message may also carry information on the possible location of UE#1 which could have been obtained by some management system when UE#1 was connected to BS#1.

9. UE#2 switches on its short range radios to start ON Discovery mechanisms (in case UE#1 location is provided, some UEs may choose not to initiate ON Discovery procedures if the determine themselves not to be in a close proximity to UE#1).

10. UE#1 tries to discover UE#2

11. UE#1 discovers UE#2 and determines that it is ON capable. It is worth noting that passive (e.g. beaconing) as well as active (e.g. probing) discovery procedures could be used for the node discovery

12. Optionally, in case discovery procedures do not provide sufficient ON related information (e.g. in case no additional information is included in beacons or probes), UE#1 requests some basic context information from UE#2 (e.g. link quality towards infrastructure, its capabilities)

13. UE#2 provides the requested information to UE#1

14. Based on the received information, UE#1 decides to initiate the negotiation in order to create an ON which may potentially consists of UE#1, UE#2 and BS#2 (if more than one node is in range of UE#1, negotiations can be conducted with multiple nodes)

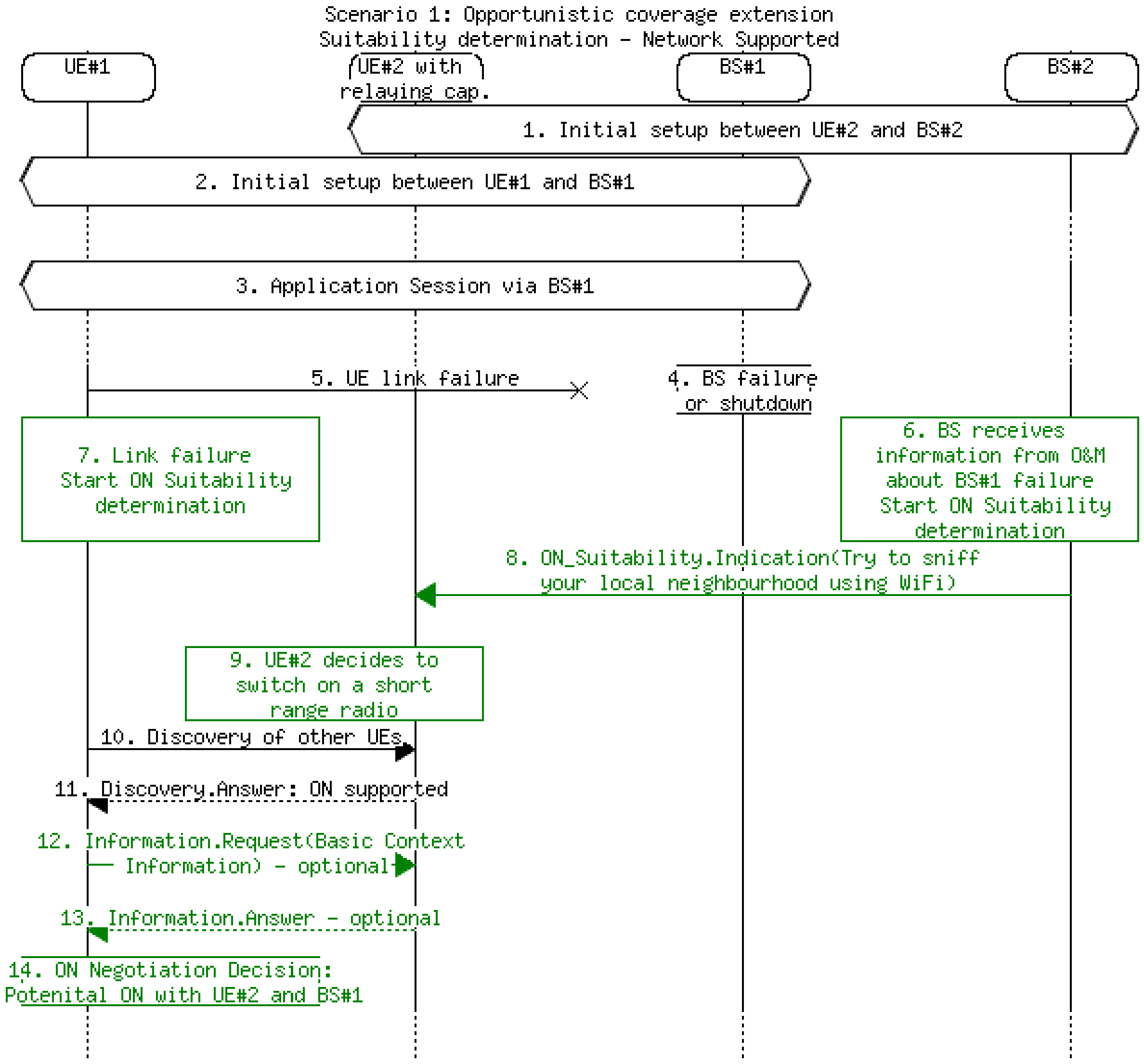

Scenario 1: Opportunistic coverage extension
Suitability determination - Network Supported
UE#1
UE#2 with relaying cap.
BS#1
BS#2
1. Initial setup between UE#2 and BS#2
2. Initial setup between UE#1 and BS#1
3. Application Session via BS#1
5. UE link failure
4. BS failure or shutdown
7. Link failure Start ON Suitability determination
6. BS receives information from O&M about BS#1 failure Start ON Suitability determination
8. ON_Suitability.Indication(Try to sniff your local neighbourhood using WiFi)
9. UE#2 decides to switch on a short range radio
10. Discovery of other UEs
11. Discovery.Answer: ON supported
12. Information.Request(Basic Context Information) - optional
13. Information.Answer - optional
14. ON Negotiation Decision: Potenital ON with UE#2 and BS#1

Figure 17: Scenario 1 - Suitability determination – Network Supported

Terminal Initiated

The following MSC illustrates a situation in which a Base Station/Infrastructure does not support UEs in suitability determination.

Preconditions: Short range radios in UE#1 and UE#2 are switched on.

Description of the messages used in Figure 18:

1. Initial setup as specified in Figure 16 between UE#2 and BS#1

2. UE#1 fails to discover BS#1 or register/attach to BS#1.

3. UE#1 does not detect any suitable access network to establish a link and initiates the suitability determination procedures.

4. UE#1 tries to discover UE#2

5. UE#1 discovers UE#2 and determines that it is ON capable. It is worth noting that passive (e.g. beaconing) as well as active (e.g. probing) discovery procedures could be used for this purpose

6. Optionally, in case discovery procedures do not provide sufficient ON related information (e.g. in case no additional information is included in beacons or probes), UE#1 requests some basic context information from UE#2 (e.g. link quality towards infrastructure, its capabilities)

7. UE#2 provides the requested information to UE#1

8. Based on the received information, UE#1 decides to initiate the negotiation in order to create an ON which consists of UE#1, UE#2 and BS#1 (if more than one node is in range of UE#1, negotiations can be conducted with multiple nodes)

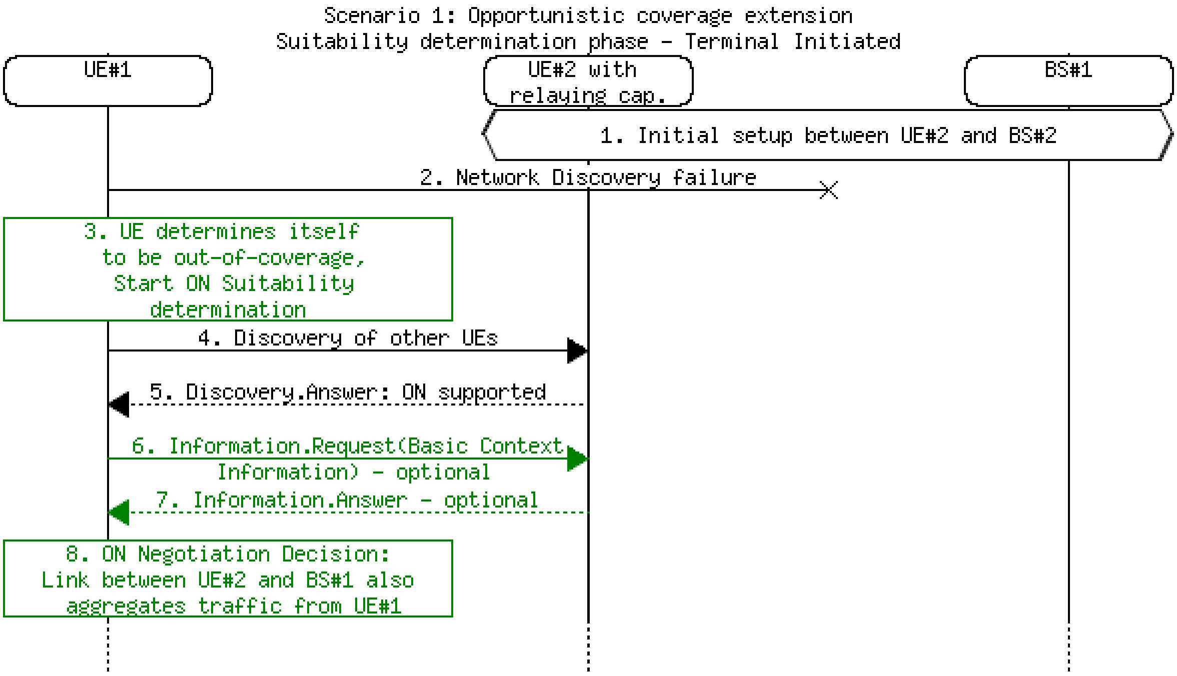

Scenario 1: Opportunistic coverage extension
Suitability determination phase - Terminal Initiated
UE#1
UE#2 with relaying cap.
BS#1
1. Initial setup between UE#2 and BS#2
2. Network Discovery failure
3. UE determines itself to be out-of-coverage, Start ON Suitability determination
4. Discovery of other UEs
5. Discovery.Answer: ON supported
6. Information.Request(Basic Context Information) - optional
7. Information.Answer - optional
8. ON Negotiation Decision: Link between UE#2 and BS#1 also aggregates traffic from UE#1

Figure 18: Scenario 1 - Suitability determination – Terminal Initiated

5.1.2 ON creation

The ON Creation phase can be subdivided into two sub-phases. During the first sub-phase the Opportunistic Network parameters are being negotiated between the ON candidates. In the result of the first sub-phase one obtains:

- confirmations from nodes about their willingness to participate in an ON (it is worth noting that not all ON candidates may be willing to participate in the ON),
- information about possible routes, possible spectrum allocation, guaranteed QoS, etc,
- ON specific measurement settings (the settings should enable proper configuration of measurements that need to be conducted when the ON is active).

Based on this information, ON creation algorithms (developed in WP4) determines an ON blue print which defines a final ON configuration (final list of ON participants, spectrum to be used, etc.). It is worth noting that in case none of the ON candidates is willing to participate in the ON or required resources cannot be provided, the ON Creation phase is terminated.

The second sub-phase of the ON Creation phase is responsible for the execution of the ON blue print and establishment of the actual ON. This sub-phase may fail in case of a link or a node failure.

The following section presents message sequence charts related to the creation phase. It is worth noting that the MSCs are applicable also to scenarios with more than two UEs and one BS involved.

Preconditions: UE#1 and UE#2 have a direct link towards BS#1. UE#1 determined UE#2 as a potential ON candidate.

Description of the messages used in Figure 19:

1. Based on the received information, UE#1 decides to initiate the negotiation in order to create an ON which consists of UE#1, UE#2 and BS#1 (if more than one node is in range of UE#1, negotiations with multiple nodes can be initiated)

2. CSCI initiates ON creation phase by sending an ON Creation trigger to CMON and passing some information about the potential ON candidates

3. An ON_Negotiation.Request including the capabilities and requirements is sent from UE#1 to UE#2.

4. UE#2 determines that it has sufficient amount of resources (e.g. high battery level) to support the ON and decides to participate in the ON

5. UE#2 sends an appropriate ON_Negotiation.Request towards BS#1 including the capabilities and requirements related to resources necessary to support the ON.

6. BS#1 determines that it has sufficient resources to support additional traffic and decides to participate in the ON. It is worth noting that BS#1 at this stage may also obtain some information on spectrum availability from a geolocation database (dedicated spectrum resources could be assigned to UE#1 and UE#2 for enabling more efficient communication between users).

7. BS#1 sends an ON_Negotiation.Answer towards UE#2. The answer includes more additional context information which could be useful in determining the most suitable route (e.g. BS load). The message may also include information on which spectrum resources are free and can be used to enable communication between UE#1 and UE#2

8. UE#2 includes additional context information (e.g. its mobility level) and forwards the received ON_Negotiation.Answer to UE#1

9. Having all the necessary context information, UE#1 determines a final configuration of the ON (e.g. routing patterns, spectrum allocation). It is worth noting that in case UE#1 negotiate with more than one UE, different ON configurations are possible. It is also worth noting that the negotiated network configuration can include measurement related parameters (types of measurements, reporting periods, etc.).

10. UE#1 sends an ON_Creation.Request towards UE#2. The message carries all the necessary information related to the configuration of the ON (e.g. spectrum allocation, measurement configuration, power allocation).

11. UE#2 forwards the received ON_Creation.Request message to BS#1.

12. BS#1 sends appropriate ON_Status.Notification(On_Created) messages to neighbouring BSs in order to reserve spectrum resources which are locally used by UE#1 and UE#2.

13. The CMON in BS#1 initiates reconfigurations according to the received ON configuration parameters (e.g. allocation of additional resources to UE#2 in order to support additional traffic).

14. BS#1 sends to UE#2 an ON_Creation.Answer acknowledging the ON creation.

15. The CMON in UE#2 initiates reconfigurations according to the ON configuration parameters carried in the ON_Creation.Request.

16. UE#2 sends to UE#1 an ON_Creation.Answer acknowledging the ON creation.

17. The CMON in UE#1 initiates the setup of the radio link for the user place (or modification of an existing radio link via the JRRM towards the underlying RAT

18. Network Attachment procedure (e.g. attachment procedure for accessing network\n over Untrusted non-3GPP IP access) or Handover procedure (e.g. handover from\n 3GPP access to Untrusted non-3GPP IP access) - see 3GPP TS 23.402 for more detail

19. Application session between UE#1 and BS#1 via UE#2 is now active

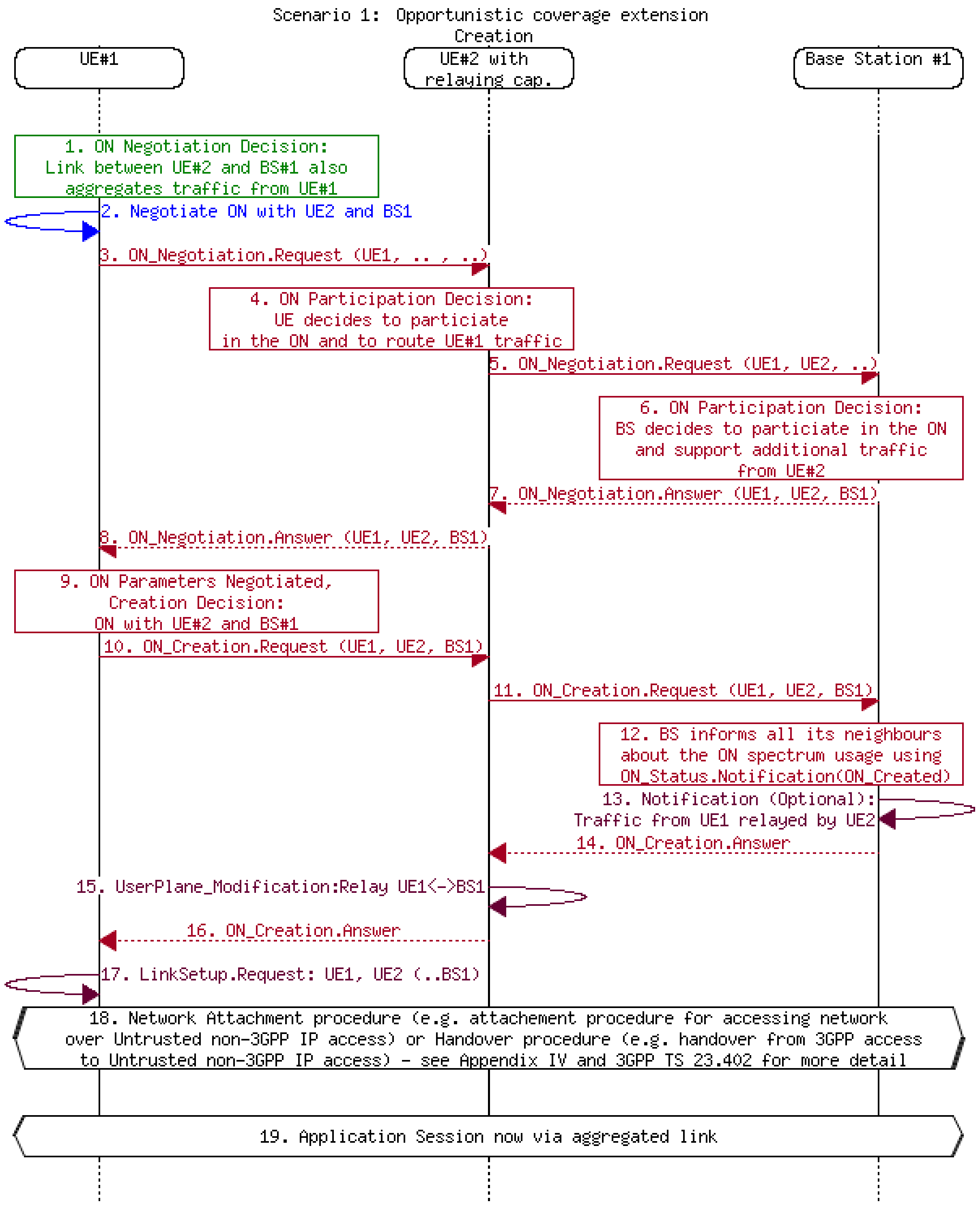

Scenario 1: Opportunistic coverage extension
Creation
UE#1
UE#2 with relaying cap.
Base Station #1
1. ON Negotiation Decision: Link between UE#2 and BS#1 also aggregates traffic from UE#1
2. Negotiate ON with UE2 and BS1
3. ON_Negotiation.Request (UE1, .. , ..)
4. ON Participation Decision: UE decides to particiate in the ON and to route UE#1 traffic
5. ON_Negotiation.Request (UE1, UE2, ..)
6. ON Participation Decision: BS decides to particiate in the ON and support additional traffic from UE#2
7. ON_Negotiation.Answer (UE1, UE2, BS1)
8. ON_Negotiation.Answer (UE1, UE2, BS1)
9. ON Parameters Negotiated, Creation Decision: ON with UE#2 and BS#1
10. ON_Creation.Request (UE1, UE2, BS1)
11. ON_Creation.Request (UE1, UE2, BS1)
12. BS informs all its neighbours about the ON spectrum usage using ON_Status.Notification(ON_Created)
13. Notification (Optional): Traffic from UE1 relayed by UE2
14. ON_Creation.Answer
15. UserPlane_Modification:Relay UE1<->BS1
16. ON_Creation.Answer
17. LinkSetup.Request: UE1, UE2 (..BS1)
18. Network Attachment procedure (e.g. attachement procedure for accessing network over Untrusted non-3GPP IP access) or Handover procedure (e.g. handover from 3GPP access to Untrusted non-3GPP IP access) - see Appendix IV and 3GPP TS 23.402 for more detail
19. Application Session now via aggregated link

Figure 19: Scenario 1 - Creation

5.1.3 ON maintenance

The following section provides several message sequence charts which describe the message flow in case of different maintenance situations. ON Maintenance phase consists of two sub-phases.

During the first sub-phase different ON relevant data is collected (e.g. mobility levels, link qualities, policy updates, profile updates). The collected data is used to monitor the ON and determine a need for the ON reconfiguration. The data can be collected from ON participants as well as from nodes which do not participate in the ON. The sub-phase is conducted continuously during the entire period of the ON activity.

The operations belonging to the second sub-phase are responsible for modification of the ON configuration. The second sub-phase starts whenever the ON reconfiguration is determined to be necessary. It is worth noting that the second sub-phase can be triggered based on the external information (e.g. low link quality of other ON participant) as well as internal information (e.g. low battery level).

During the first sub-phase information from other nodes can be collected using different delivery methods. An example of a possible delivery method is the On Demand information exchange (see Section 7 for more details). The other example of the delivery method is the Trigger based information exchange (see Section 7 for more details). The parameters related to the configuration of the Triggered based information exchange (e.g. trigger thresholds) could be established during the ON Creation phase (more specifically, during the ON negotiation sub-phase). In order to simplify, only the On Demand delivery method is considered in this sub-section (e.g. see Figure 20, steps 2, 3 and steps 4, 5).

Gateway handover

The following MSC illustrates a situation in which an UE intends to switch between UEs which serve it as relaying UEs.

Precondition: UE#1, UE#2, UE#3 and BS#1 are part of an ON. UE#2 is connected to BS#1. UE#3 is directly connected to BS#1. UE#3 is in range of UE#1 and has an active connection towards BS#1 (it is worth noting that the following MSC is also valid in case UE#2 is connected to other BS than BS#1).

Description of the messages used in Figure 20:

1. Application session between UE#1 and BS#1 via UE#2 is active

2. UE#1 requests context information from UE#2 (the procedure can be repeated periodically during the lifetime of the ON)

3. UE#2 responds with the requested context information which can be related to the link qualities, geographical location, speed, etc.

4. UE#1 requests context information from UE#3 (the procedure can be repeated periodically during the lifetime of the ON)

5. UE#3 responds with the requested context information which can be related to the link qualities, geographical location, speed, etc. (we assume that UE#3 can assess its link quality towards BS#1 (e.g. CPICH RSCP, CPICH Ec/No))

6. Based on the received information, UE#1 decides that the link towards BS#1 via UE#3 could be better that the link towards BS#1 via UE#2 and initiates the gateway handover procedure

7. UE#1 sends an ON_Modification.Request message to UE#3 to initiate the modification of the ON

8. UE#3 determines if it has sufficient amount of resources (e.g. high battery level) to support relaying of traffic for UE#1 and decides to become a gateway for UE#1

9. UE#3 forwards the received ON_Modification.Request message to BS#1 to inform it about the planned changes

10. BS#1 determines if it has sufficient resources to support additional traffic from UE#3.

11. If needed, the transceiver in BS#1 is configured to be able to receive traffic from UE#1 via UE#3

12. BS#1 acknowledges the changes by sending an ON_Modification.Answer back to UE#3

13. UE#3 configures its transceiver so that traffic from UE#1 can be forwarded/relayed to BS#1 and vice versa

14. UE#3 responds to UE#1 with an ON_Modification.Answer to acknowledge the modification.

15. The CMON in UE#1 initiates the setup of the radio link for the user place (or modification of an existing radio link via the JRRM towards the underlying RAT

16. Handover procedure is executed (e.g. handover between two Untrusted non-3GPP IP access networks - see 3GPP TS 23.402 for more detail)

17. Application session between UE#1 and BS#1 is now active via UE#3

18. BS#1 sends an ON_Status.Notification towards UE#2 to inform it about the modification and that it is no longer required to route traffic for UE#1

19. UE#2 reconfigures its transceiver so that traffic from UE#1 can no longer be forwarded/relayed to BS#1 and vice versa

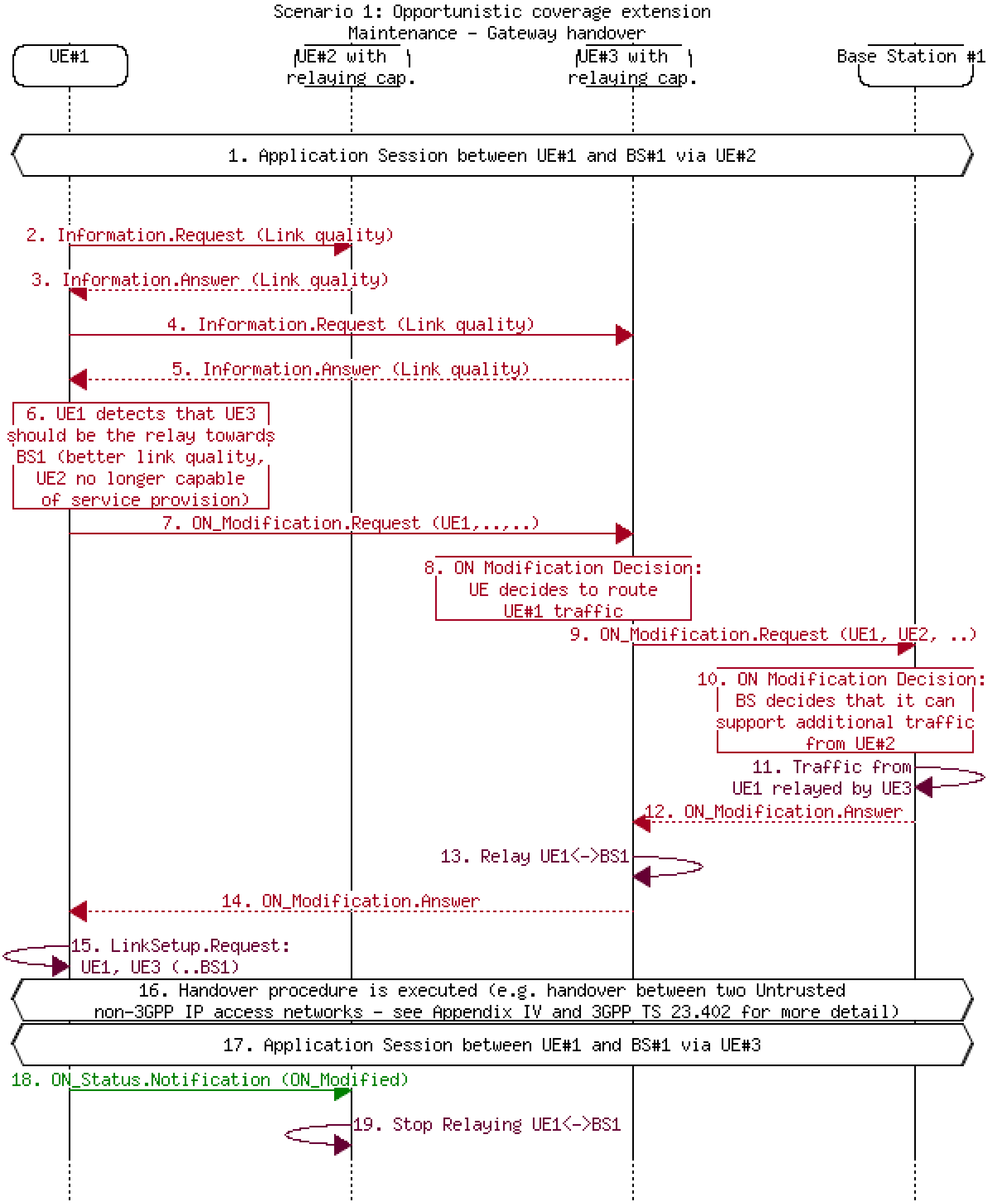

Scenario 1: Opportunistic coverage extension
Maintenance - Gateway handover
UE#1
UE#2 with relaying cap.
UE#3 with relaying cap.
Base Station #1
1. Application Session between UE#1 and BS#1 via UE#2
2. Information.Request (Link quality)
3. Information.Answer (Link quality)
4. Information.Request (Link quality)
5. Information.Answer (Link quality)
6. UE1 detects that UE3 should be the relay towards BS1 (better link quality, UE2 no longer capable of service provision)
7. ON_Modification.Request (UE1,..,..)
8. ON Modification Decision: UE decides to route UE#1 traffic
9. ON_Modification.Request (UE1, UE2, ..)
10. ON Modification Decision: BS decides that it can support additional traffic from UE#2
11. Traffic from UE1 relayed by UE3
12. ON_Modification.Answer
13. Relay UE1<->BS1
14. ON_Modification.Answer
15. LinkSetup.Request: UE1, UE3 (..BS1)
16. Handover procedure is executed (e.g. handover between two Untrusted non-3GPP IP access networks - see Appendix IV and 3GPP TS 23.402 for more detail)
17. Application Session between UE#1 and BS#1 via UE#3
18. ON_Status.Notification (ON_Modified)
19. Stop Relaying UE1<->BS1

Figure 20: Scenario 1 – ON Maintenance, Gateway handover

BS handover

The following MSC illustrates a situation in which an UE which serves as a relaying UE for another UE intends to conduct a handover from one BS to another BS. It is worth noting that as UEs can maintain connection only with a single BS at a time, the procedure needs to be guided by the infrastructure (terminals can stay connected to more than one BS at a time only in UMTS system (soft-handover)).

Precondition: UE#1, UE#2 and BS#1 are part of an ON. BS#1 can communicate with BS#2 (i.e. BS#1 and BS#2 belong to the same operator).

Description of the messages used in Figure 21:

1. Application session between UE#1 and BS#1 via UE#2 is active

2. UE#2 reports some RAT specific measurement (e.g. CPICH Ec/N0) towards BS#1 (the procedure is repeated periodically when UE#2 is connected to BS#1)

3. Based on the RAT specific measurements, BS#1 determines that UE#2 may want to handover to a new BS. Given the list of the Base Stations (extracted from the RAT specific report), BS#1 decides to include the most suitable Base Station to the ON.

4. If needed, BS#1 may request other base stations (in this case BS#2) to provide it with some basic information related to their capabilities. This step is optional as in most cases this information is made available during the infrastructure setup.

5. If needed, BS#2 provides BS#1 with the requested information

6. Based on the obtained/available information, BS#1 determines the list of potential base stations which could be included to the ON and decides to initiate the negotiation procedures.

7. CSCI initiates the ON creation phase by sending an ON Creation trigger to CMON and passing the information about the potential ON candidates.

8. BS#1 sends an ON_Negotiation.Request towards BS#2. The message includes, among others, information about the required QoS. The message is sent to all the base station on the Base Station candidate list.

9. BS#2 responds with an ON_Negotiation.Answer. The message carries information related to the outcome of the negotiation on the BS#2 side.

10. Based on the received information, BS#1 determines the most appropriate BS and decides to include it to the ON (in this case BS#2).

11. BS#1 initiates the ON Creation procedure by sending an ON_Create.Request towards BS#2

12. BS#2 responds with an ON_Create.Answer

13. BS#1 informs UE#2 about the addition of BS#2 to the ON

14. If needed, UE#2 may inform UE#1 about the addition of BS#2 to the ON

15. UE#2 decides to conduct a RAT specific handover. As BS#2 is already a part of an ON, the handover is conducted to BS#2

16. Application session is now carried over UE#2 and BS#2

17. As BS#1 is no longer actively involved in the ON it decides to leave the ON.

18. BS#1 sends an ON_Modification.Request towards BS#2. The message includes the information about BS#1 intentions.

19. BS#2 determines on the basis of RAT specific information collected from UE#2 and node configuration (e.g. timers, thresholds dependent on node parameters), if UE#2 wants to handover back to BS#1. Based on this information, BS#2 decides if BS#1 can be removed from the ON.

20. BS#2 acknowledges the request by sending an ON_Modification.Answer

21. BS#2 informs UE#2 about the ON modifications

22. If needed, UE#2 may inform UE#1 about the disconnection of BS#1

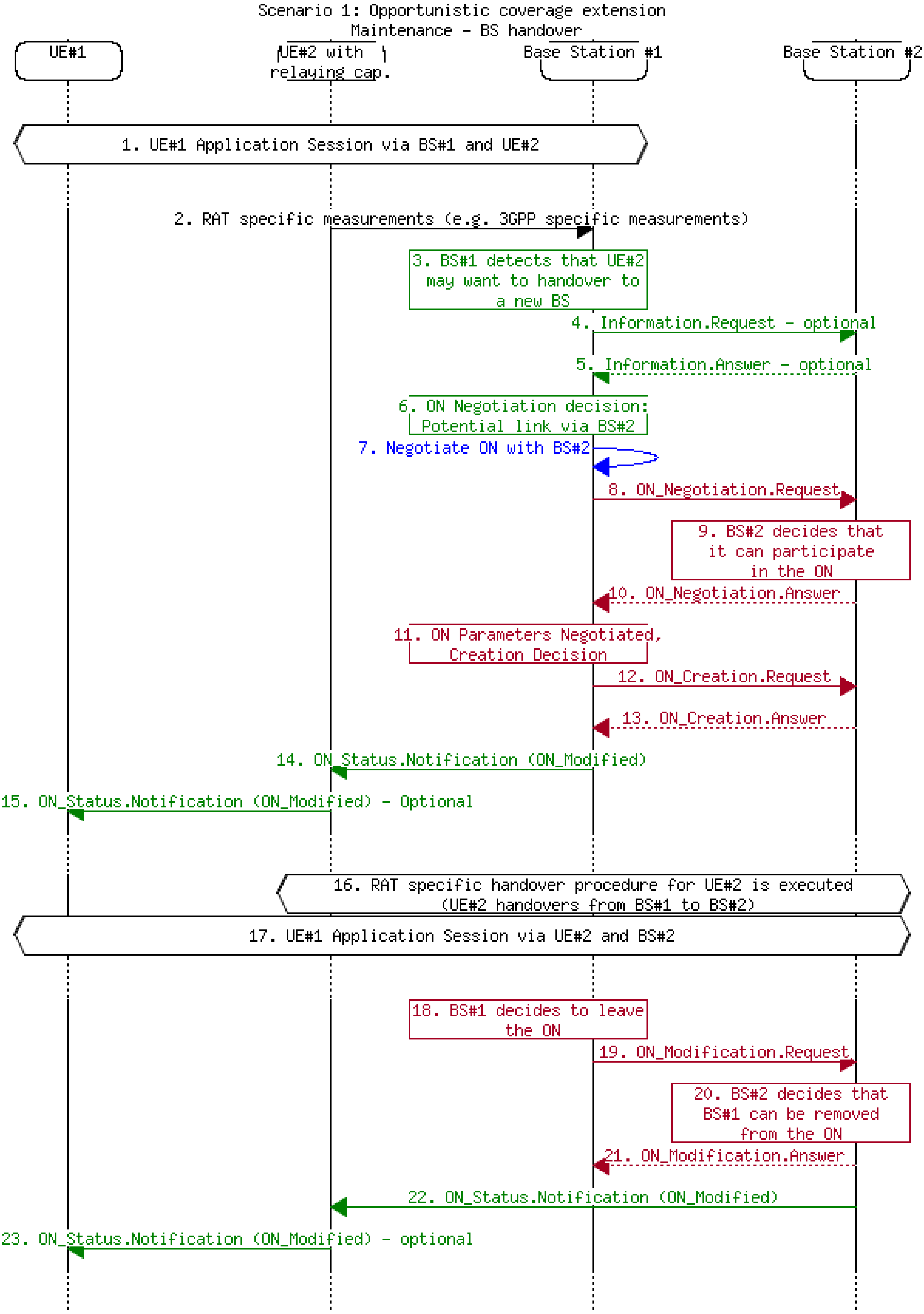

Scenario 1: Opportunistic coverage extension
Maintenance - BS handover
UE#1
UE#2 with relaying cap.
Base Station #1
Base Station #2
1. UE#1 Application Session via BS#1 and UE#2
2. RAT specific measurements (e.g. 3GPP specific measurements)
3. BS#1 detects that UE#2 may want to handover to a new BS
4. Information.Request - optional
5. Information.Answer - optional
6. ON Negotiation decision: Potential link via BS#2
7. Negotiate ON with BS#2
8. ON_Negotiation.Request
9. BS#2 decides that it can participate in the ON
10. ON_Negotiation.Answer
11. ON Parameters Negotiated, Creation Decision
12. ON_Creation.Request
13. ON_Creation.Answer
14. ON_Status.Notification (ON_Modified)
15. ON_Status.Notification (ON_Modified) - Optional
16. RAT specific handover procedure for UE#2 is executed (UE#2 handovers from BS#1 to BS#2)
17. UE#1 Application Session via UE#2 and BS#2
18. BS#1 decides to leave the ON
19. ON_Modification.Request
20. BS#2 decides that BS#1 can be removed from the ON
21. ON_Modification.Answer
22. ON_Status.Notification (ON_Modified)
23. ON_Status.Notification (ON_Modified) - optional

Figure 21: Scenario 1 – ON Maintenance, BS handover (Network Centric case)

ON Participant Disconnection

The following MSC illustrates a situation in which an UE intends to disconnect from an ON.

Precondition: UE#1, UE#2, UE#3 and BS#1 are part of an ON. UE#2 is directly connected to BS#1.

Figure 22 presents a sequence chart for a scenario in which one of UEs wants to disconnect from an ON after its application is terminated.

Description of the messages used in Figure 22:

1. Application session between UE#1 and BS#1 via UE#2 is active

2. Application session between UE#3 and BS#1 via UE#2 is active

3. UE#3 terminated the application and decides to leave the ON

4. UE#3 sends an ON_Release.Request message towards UE#2 in order to initiate the ON Disconnection procedure

5. UE#2 decides that the ON is still necessary to maintain the application session for UE#1. It decides not to initiate the ON Termination procedure

6. UE#2 allows for the disconnection of UE#3 by sending an ON_Release.Answer

7. UE#2 informs BS#1 about the disconnection of the UE#3 using an ON_Status.Notification message. The message can carry information related to the reason of the disconnection

8. If needed, UE#2 may inform UE#1 about the disconnection of UE#3 using an ON_Status.Notification message. The message can carry information related to the reason of the disconnection

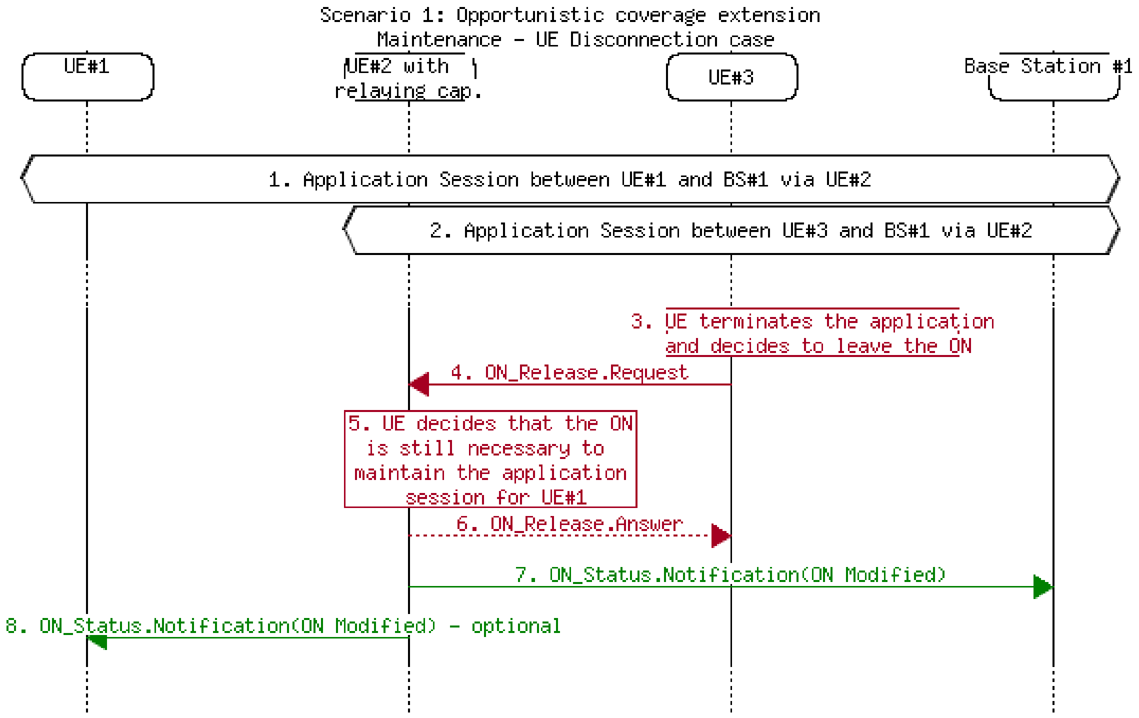

Scenario 1: Opportunistic coverage extension
Maintenance - UE Disconnection case
UE#1
UE#2 with relaying cap.
UE#3
Base Station #1
1. Application Session between UE#1 and BS#1 via UE#2
2. Application Session between UE#3 and BS#1 via UE#2
3. UE terminates the application and decides to leave the ON
4. ON_Release.Request
5. UE decides that the ON is still necessary to maintain the application session for UE#1
6. ON_Release.Answer
7. ON_Status.Notification(ON Modified)
8. ON_Status.Notification(ON Modified) - optional

Figure 22: Scenario 1 - ON Maintenance, UE disconnection

ON Gateway disconnection

The following MSC illustrates a situation in which an UE which serves as a relaying UE for another UE intends to disconnect from an ON.

Precondition: UE#1, UE#2, UE#3 and BS#1 are part of an ON. UE#2 and UE#3 are directly connected to BS#1. UE#3 is in the range of UE#1

Figure 23 presents a sequence chart for a scenario in which an UE which acts as a gateway wants to disconnect from an ON.

Description of the messages used in Figure 23:

1. Application session between UE#1 and BS#1 via UE#2 is active

2. UE#2 decides to leave the ON due to low batter level

3. UE#2 sends an ON_Release.Request message towards UE#1 in order to initiate the disconnection procedure

4. As UE#2 serves as a gateway for UE#1, UE#1 decides to initiate a gateway handover before allowing UE#2 to disconnect

5. Gateway handover procedure (see Section 5.7 for more detail)

6. Application session between UE#1 and BS#1 via UE#3 is now active

7. UE#1 sends an ON_Release.Answer to UE#2 thus allowing UE#2 to disconnect

8. UE#1 informs UE#3 about the disconnection of the UE#2 using an ON_Status.Notification message. The message can carry information related to the reason of the disconnection

9. UE#3 forwards the ON_Status.Notification towards BS#1

10. If needed, UE#2 initiates the link release procedure towards BS#1

11. BS#1 acknowledges a successful link release

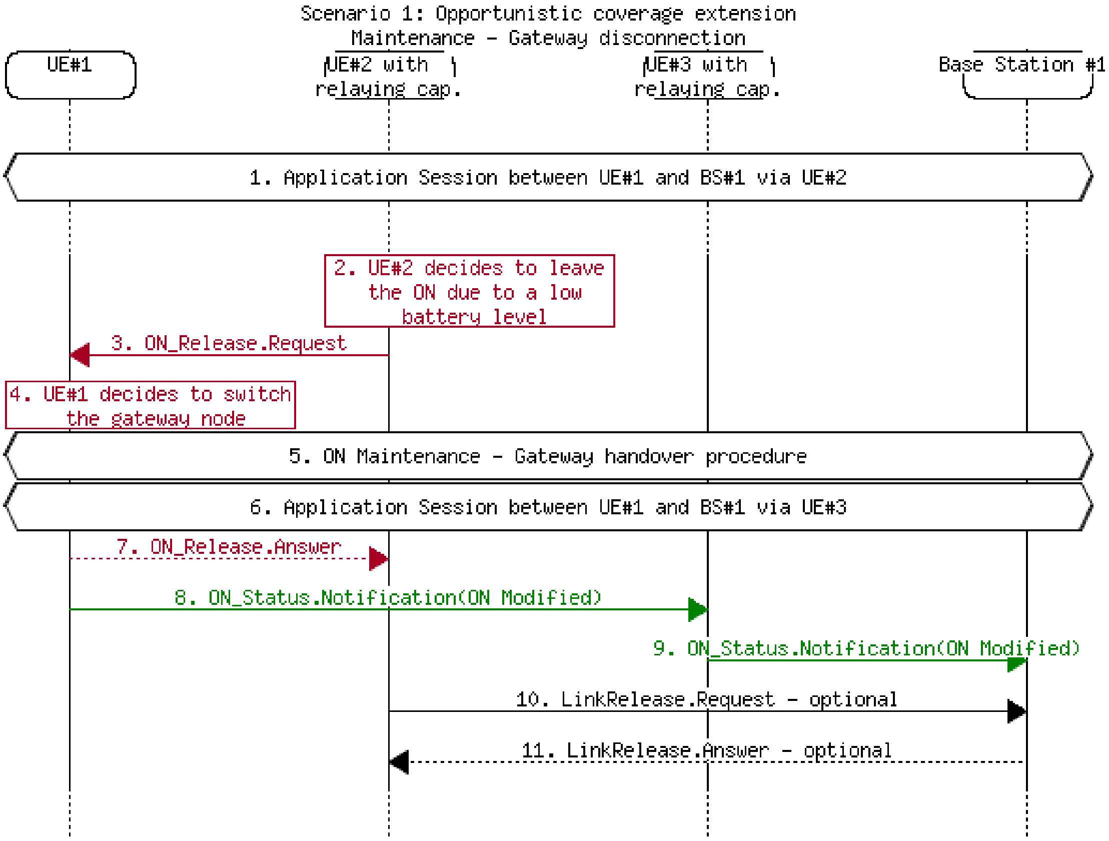

Scenario 1: Opportunistic coverage extension
Maintenance - Gateway disconnection
UE#1
UE#2 with relaying cap.
UE#3 with relaying cap.
Base Station #1
1. Application Session between UE#1 and BS#1 via UE#2
2. UE#2 decides to leave the ON due to a low battery level
3. ON_Release.Request
4. UE#1 decides to switch the gateway node
5. ON Maintenance - Gateway handover procedure
6. Application Session between UE#1 and BS#1 via UE#3
7. ON_Release.Answer
8. ON_Status.Notification(ON Modified)
9. ON_Status.Notification(ON Modified)
10. LinkRelease.Request - optional
11. LinkRelease.Answer - optional

Figure 23: Scenario 1 - ON Maintenance, Gateway disconnection

5.1.4 ON termination

The following section provides a message sequence chart describing termination of an ON. The ON Termination is conducted whenever an ON is determined to be no longer necessary. The ON termination is required in order to release some dedicated resources (e.g. spectrum, power, time, codes) allocated by the infrastructure for the purpose of serving an ON. The procedures related to the ON termination may be also used to exchange some useful ON related statistics between different ON participants.

Precondition: UE#1, UE#2 and BS#1 are part of an ON

Figure 24 presents a sequence chart for a scenario in which an ON is terminated after the application is terminated.

Description of the messages used in Figure 24:

1. Application session between UE#1 and BS#1 via UE#2 is active

2. Application session between UE#1 and BS#1 via UE#2 is terminated (e.g. user finished streaming a video)

3. As the participation in the ON is no longer beneficial for UE#1, it decides to leave the ON

4. UE#1 sends an ON_Release.Request message towards UE#2 in order to initiate the ON Disconnection procedure

6. UE#2 sends an ON_Release.Answer to UE#1, terminating UE#1 participation in the ON.

7. UE#2 determines that no other UEs (besides UE#1) were using it as a gateway and may decide to leave the ON.

8. UE#2 sends an ON_Release.Request to BS#1. The message carries information about the UE#2 intentions and disconnection of UE#1 (an alternative way for informing BS#1 about the disconnection of UE#1 would be to use the ON_Status_Indication message).

9. Based on the information received, BS#1 determines if all UEs disconnected from the ON and may decide to terminate the ON.

10. BS#1 acknowledges release of entire ONby sending ON_Release.Answer with appropriate information contents.

11. If needed, UE#2 initiates the link release procedure towards BS#1

12. BS#1 acknowledges a successful link release

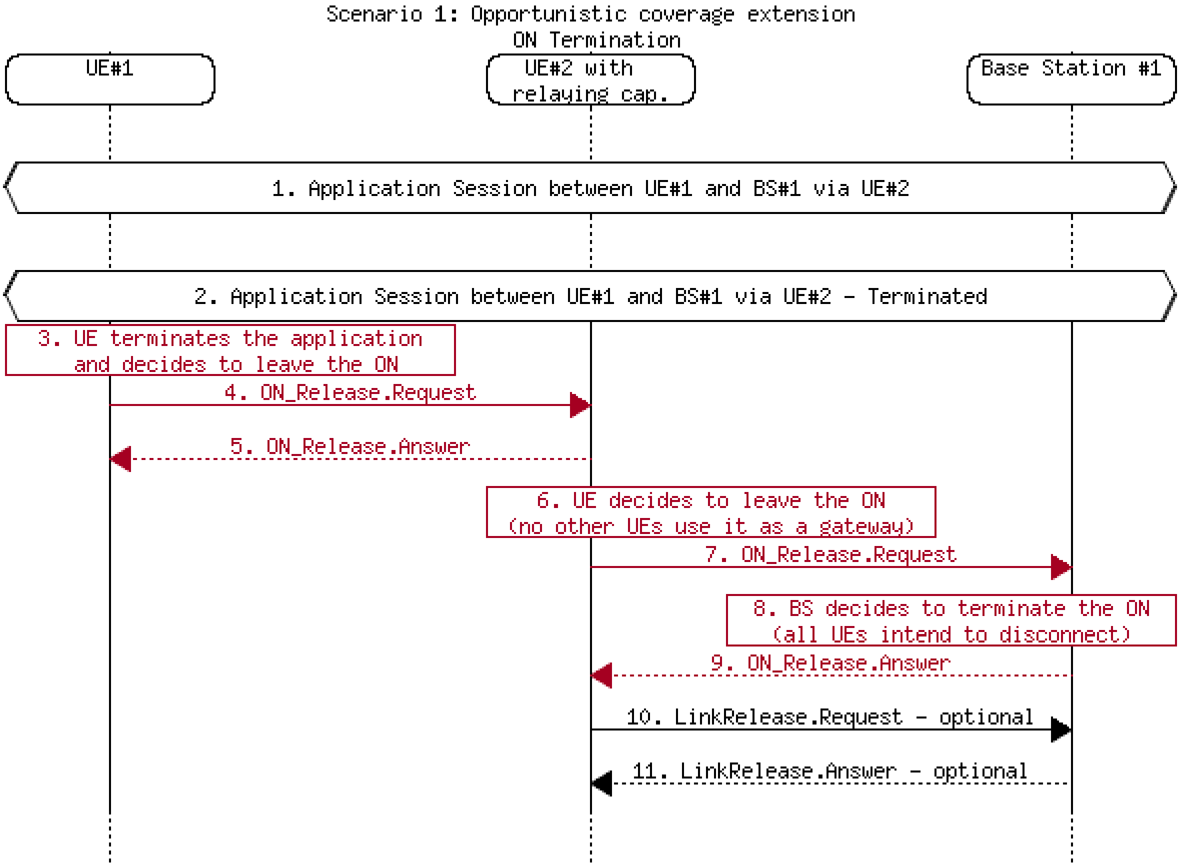

Scenario 1: Opportunistic coverage extension
ON Termination
UE#1
UE#2 with relaying cap.
Base Station #1
1. Application Session between UE#1 and BS#1 via UE#2
2. Application Session between UE#1 and BS#1 via UE#2 - Terminated
3. UE terminates the application and decides to leave the ON
4. ON_Release.Request
5. ON_Release.Answer
6. UE decides to leave the ON (no other UEs use it as a gateway)
7. ON_Release.Request
8. BS decides to terminate the ON (all UEs intend to disconnect)
9. ON_Release.Answer
10. LinkRelease.Request - optional
11. LinkRelease.Answer - optional

Figure 24: Scenario 1 - ON Termination

5.2 Scenario 2A: Opportunistic capacity extension through femtocells

A message sequence chart for opportunistic capacity extension through femtocells is shown in Figure 25 with respect to the suitability determination phase.

Figure 26 analyzes the creation phase while

Figure 27 provides messages for the maintenance phase. Finally,

Figure 28 analyzes the termination phase of an ON.

In this scenario it is assumed that an infrastructure element (i.e., BS#1) experiences congestion issues. Moreover, it is assumed that an available femtocell (i.e., BS#2) is located in the service area of the problematic BS. Available femtocells can be seen as an opportunity to provide capacity extension to overloaded infrastructure elements due to the fact that they can seize the opportunity of the radio environment (extra resources) in a specific region for a specific timeframe. In order to allow the creation of an ON, the femtocell would temporarily change to OSG mode (Open Subscriber Group) from CSG (Closed Subscriber Group) or it may temporarily add extra UEs in its subscriber group. The information whether a femtocell can change to OSG will be acquired from the suitability determination phase. Then, if the femtocell is available, the negotiation procedure will be triggered in order to become temporarily OSG from CSG or to add temporarily extra UEs.

5.2.1 ON suitability determination

1. A congestion situation is identified via the CSCI entity of the problematic infrastructure element (BS).

2. The CSCI of the Congested BS provides the information (BS context) to DSONPM.
3. The DSONPM sends a request to the CSCI entity of the neighbouring femtocell in order to acquire its context.
4. The CSCI of the femtocell answers to the DSONPM with its context and whether it can temporarily become OSG from CSG or it can add temporarily extra UEs to its subscriber group.
5. The DSONPM decides which is the most appropriate method of solving the problem. Specifically, the DSONPM identifies that an available femtocell that has the ability to become temporarily OSG from CSG or it can add temporarily extra UEs to its subscriber group, exists in the area and decides to solve the problem via the femtocell capacity extension method.
6. The DSONPM sends a message to the CSCI entity of the congested BS with the previous decision and the context of the femtocell.
7. The CSCI of the problematic BS notifies the CMON of the same element in order to trigger the solution. The message contains the context of the congested BS (BS#1) and the femtocell (BS#2) context.

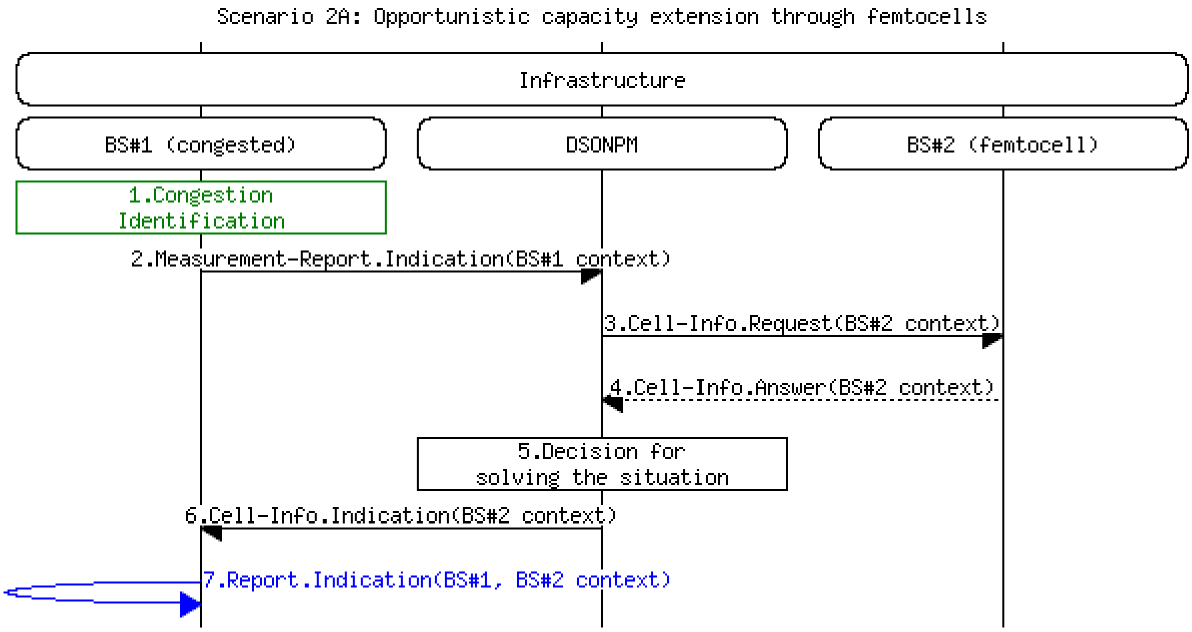

Scenario 2A: Opportunistic capacity extension through femtocells
Infrastructure
BS#1 (congested)
DSONPM
BS#2 (femtocell)
1.Congestion Identification
2.Measurement-Report.Indication(BS#1 context)
3.Cell-Info.Request(BS#2 context)
4.Cell-Info.Answer(BS#2 context)
5.Decision for solving the situation
6.Cell-Info.Indication(BS#2 context)
7.Report.Indication(BS#1, BS#2 context)

Figure 25: Scenario 2A "Opportunistic capacity extension through femtocells" -Suitability Determination phase.

5.2.2 ON creation

8. The congested BS communicates with the femtocell (ON_Negotiation.Request) in order to temporarily become OSG from CSG or temporarily add extra UEs to its subscriber group.
9. The femtocell replies back to the BS.
10. The CMON of the congested BS runs the assignment algorithm in order to redistribute terminals from the congested BS to femtocell.

11. The CMON of the congested BS sends an ON_Creation.Request message to the CMON of the femtocell in order to notify it about the UEs that will connect to it and add them temporarily to its subscriber group.
12. The CMON of the congested BS sends an ON_Creation.Request message to the CMON of the terminal in order to notify it about the femtocell to which it will be re-routed.
13. The terminal requests to connect to the femtocell.
14. The femtocell replies back to the terminal.
15. The CMON of the terminal replies back to the CMON of the congested BS (ON_Creation.Answer).
16. The CMON of the femtocell replies back to the congested BS (ON_Creation.Answer).
17. A handover of the session from the direct link between BS#1 and UE is made so that UE is now connected to BS#2. The application session is activated.

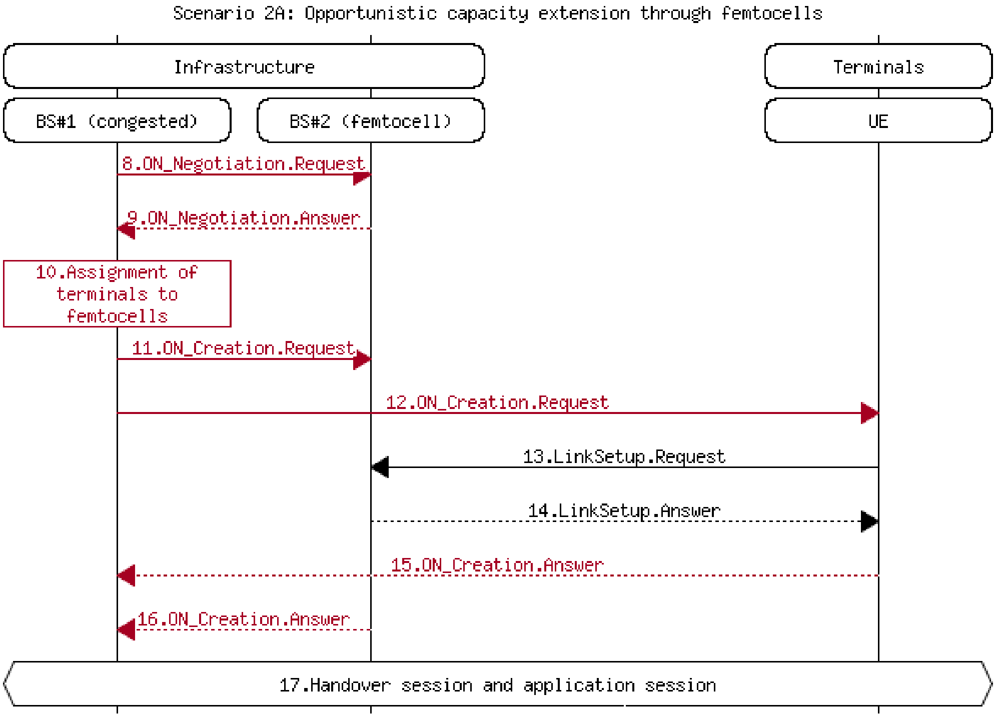


Figure 26: Scenario 2A "Opportunistic capacity extension through femtocells" –Creation phase.

5.2.3 ON maintenance

In this phase it is assumed that an ON is already created and a UE that was connected with BS#2 loses its connectivity (e.g. the UE moves out of BS's #2 coverage). Hence, the UE notifies BS#1 about the problem. After that, the modification procedure initiates.

18. The problematic situation (i.e. network failure between UE and BS#2) is discovered.
19. The UE notifies BS#1 about the problem.
20. The congested BS communicates with the femtocell (ON_Negotiation.Request) in order to temporarily become OSG from CSG or temporarily add extra UEs to its subscriber group.

21. The femtocell replies back to the BS.
22. The CMON of the congested BS sends an ON_Modification.Request message to the CMON of another femtocell (BS#3) in order to notify it about the terminal that will connect to it.
23. The CMON of the congested BS sends an ON_Modification.Request message to the CMON of the terminal in order to notify it about the femtocell to which it will be re-routed.
24. The terminal requests to connect to the femtocell.
25. The CMON of the terminal replies back to the CMON of the congested BS (ON_Modification.Answer).
26. The CMON of the femtocell replies back to the congested BS (ON_Modification.Answer).
27. A handover of the session from the link between BS#2 and UE is made so that UE is now connected to BS#3. The application session is activated.

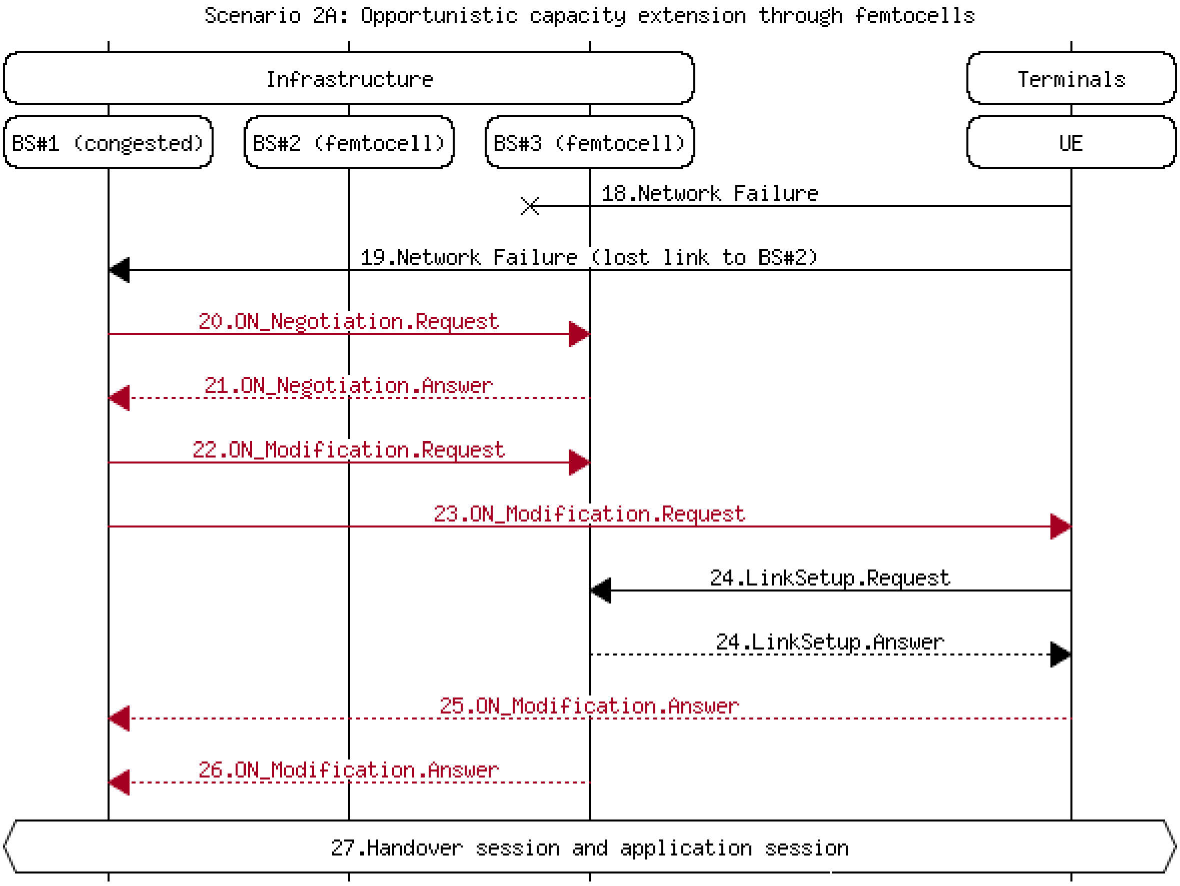

Scenario 2A: Opportunistic capacity extension through femtocells
Infrastructure
Terminals
BS#1 (congested)
BS#2 (femtocell)
BS#3 (femtocell)
UE
18.Network Failure
19.Network Failure (lost link to BS#2)
20.ON_Negotiation.Request
21.ON_Negotiation.Answer
22.ON_Modification.Request
23.ON_Modification.Request
24.LinkSetup.Request
24.LinkSetup.Answer
25.ON_Modification.Answer
26.ON_Modification.Answer
27.Handover session and application session

Figure 27: Scenario 2A “Opportunistic capacity extension through femtocells” – Maintenance phase.

5.2.4 ON termination

28. The CMON of the congested BS sends an ON_Release.Request message to the CMON of the femtocell in order to notify it about the termination of the ON, become CSG from OSG or remove the respective UEs from the subscriber list.
29. The CMON of the congested BS sends an ON_Release.Request message to the CMON of the terminal in order to notify it also about the ON termination.

30. The terminal requests to disconnect from the femtocell.
31. The CMON of the terminal replies back to the CMON of the congested BS (ON_Release.Answer).
32. The CMON of the femtocell replies back to the congested BS (ON_Release.Answer).

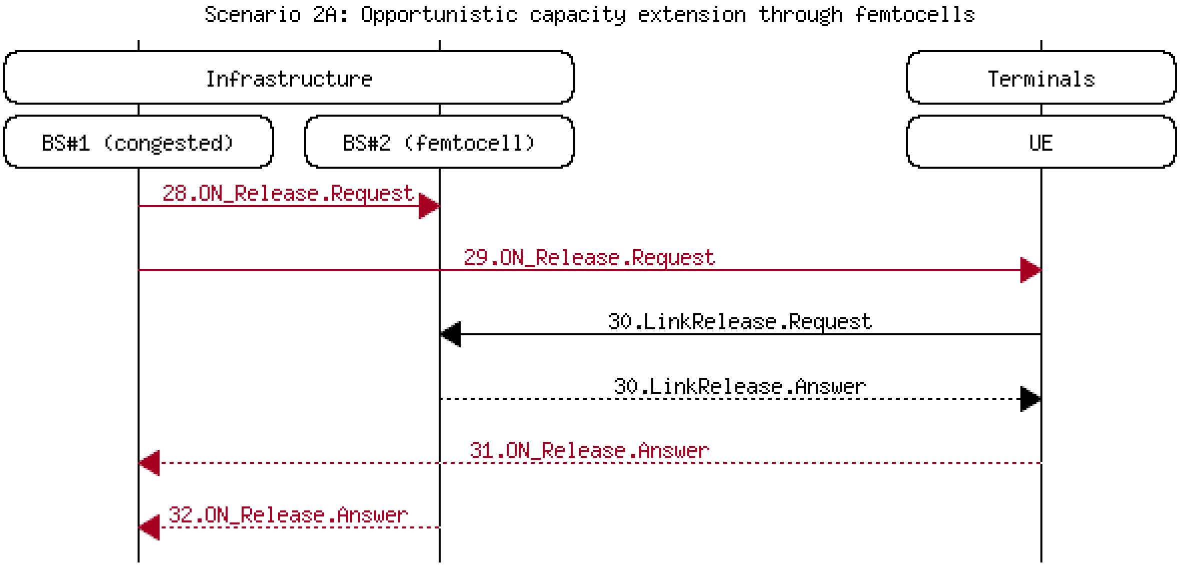


Figure 28: Scenario 2A “Opportunistic capacity extension through femtocells” – Termination phase.

5.3 Scenario 2B: Opportunistic capacity extension through maximum flow

5.3.1 Single base station experiences congestion

The opportunistic capacity extension through maximum flow scenario is depicted in this section by assuming that only one BS experiences congestion. A message sequence chart for opportunistic capacity extension through maximum flow is shown in Figure 29 with respect to the suitability determination phase. Figure 30 analyzes the creation phase while Figure 31 provides messages for the maintenance phase. Finally, Figure 32 analyzes the termination phase of an ON.

In this scenario it is assumed that a single BS experiences congestion issues. This is BS#1. Moreover, it is assumed that the terminal UE#1 is registered to the problematic BS#1. There is also a non-congested BS in the area (BS#2). Finally, it is assumed that UE#2 is close to UE#1. UE#2 is located into the non-congested area (BS#2) and can relay traffic from terminals in the congested area to terminals in the non-congested area.

5.3.1.1 ON suitability determination

1. The CSCI of the congested BS (BS#1) identifies the problematic situation.
2. The CSCI of BS#1 provides the congestion information (BS context) to DSONPM.
3. The DSONPM sends a Cell-Info.Request message to the CSCI of the non-congested neighbouring BS (BS#2) in order to acquire its context (the context contains the load parameter which needs to be retrieved).
4. An answer message containing the BS context is transmitted back to the DSONPM.

5. The DSONPM decides which is the most appropriate method of solving the problem and designates that the CSCI of the problematic BS (i.e. BS#1) will be responsible of providing the solution.

6. The DSONPM informs the CSCI of BS#1 (Cell-Info.Indication) which includes the set of congested BSs and the set of non-congested BSs.

7. The congested BS sends an information request to its terminals (e.g. UE#1) in order to acquire other terminals in a neighbouring non-congested area with ON capabilities that will help for the ON creation. Afterwards, the discovery requests and answers will identify all available neighbouring terminals that have the ability to participate to the ON. At the end, the definition of all candidate terminals that can be part of the ON is realized.

8. The CSCI of the congested BS sends the information to the selected CMON (Report.Indication), which conveys the set of congested BSs, the set of non-congested BSs, and the set of selected candidate nodes (terminals).

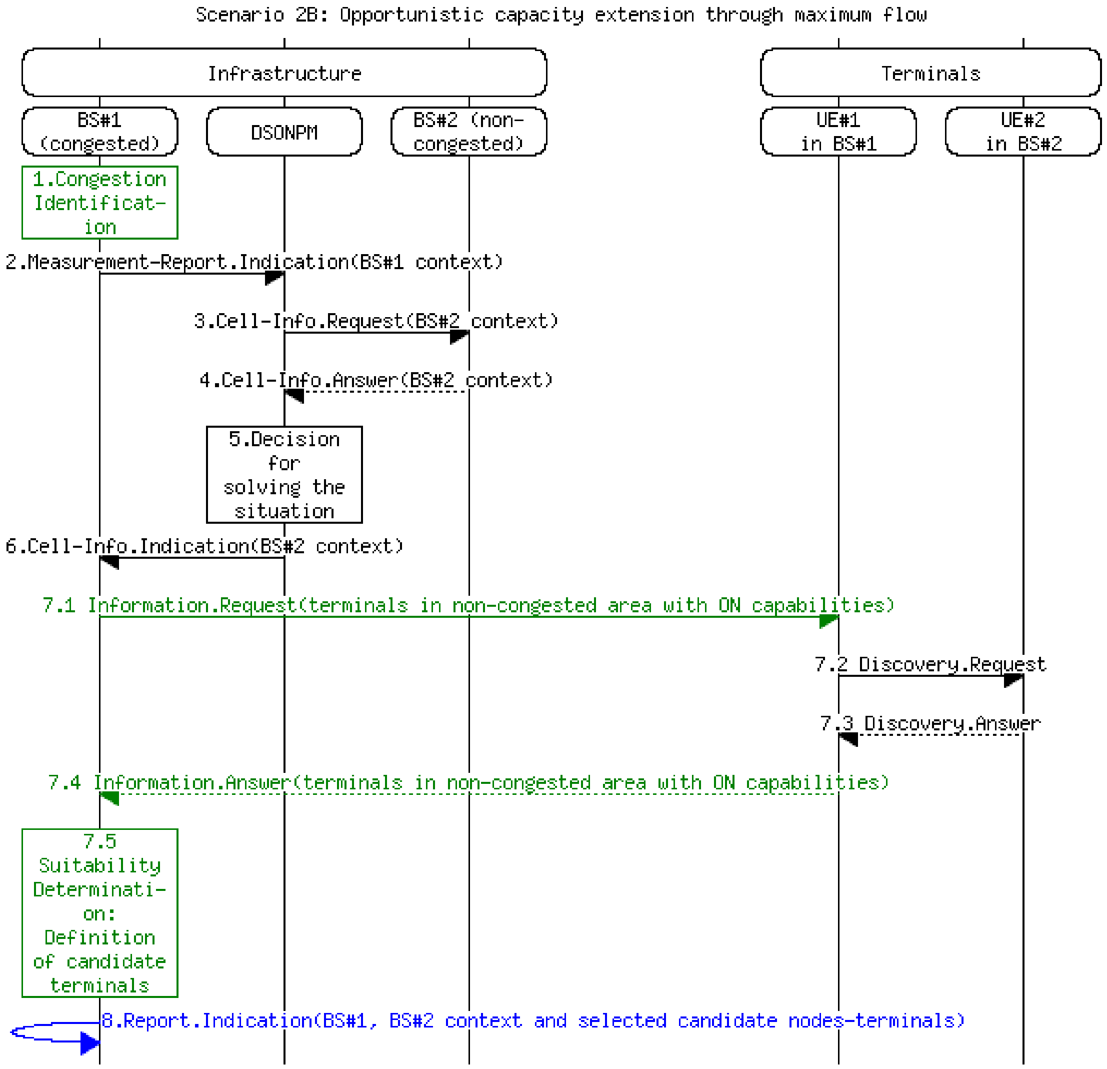

Scenario 2B: Opportunistic capacity extension through maximum flow
Infrastructure
Terminals
BS#1 (congested)
DSONPM
BS#2 (non-congested)
UE#1 in BS#1
UE#2 in BS#2
1.Congestion Identificat-ion
2.Measurement-Report.Indication(BS#1 context)
3.Cell-Info.Request(BS#2 context)
4.Cell-Info.Answer(BS#2 context)
5.Decision for solving the situation
6.Cell-Info.Indication(BS#2 context)
7.1 Information.Request(terminals in non-congested area with ON capabilities)
7.2 Discovery.Request
7.3 Discovery.Answer
7.4 Information.Answer(terminals in non-congested area with ON capabilities)
7.5 Suitability Determinati-on: Definition of candidate terminals
8.Report.Indication(BS#1, BS#2 context and selected candidate nodes-terminals)

Figure 29: Scenario 2B "Opportunistic capacity extension through maximum flow" – Single congested BS - Suitability Determination phase.

5.3.1.2 ON creation

9. The CMON of the congested BS sends an ON_Negotiation.Request message to the CMON of the terminal that is located at the problematic area, in order to acquire paths to alternate BSs.

10. The terminal communicate with its neighbouring terminals (ON_Negotiation.Request) in order to acquire paths to alternate BSs.

11. The identification of paths to alternate BSs is realized. Specifically, each terminal maintains a list of terminals and BSs to which have the ability to communicate with. Hence, through the exchange of negotiation messages, the terminals are capable of finding paths to alternate BSs.

12. The CMON of the terminal in the congested area sends an answering message to the CMON of the serving BS with the found paths.

13. The selection of nodes and routes for ON Creation takes place.

14. The CMON of BS#1 sends message (ON_Creation.Request) with the selected path to the CMON of its terminal (UE#1).

15. The terminal in the congested area sets up a link with the neighbouring terminal which is located in the non-congested area.

16. The CMON of UE#1 replies back to the CMON of its served BSs (ON_Creation.Answer).

17. A handover of the session from the direct links between BS#1 and UE#1 is made so that UE#1 now uses a link towards UE#2 which forwards traffic towards a non-congested BS (BS#2). The application session is activated.

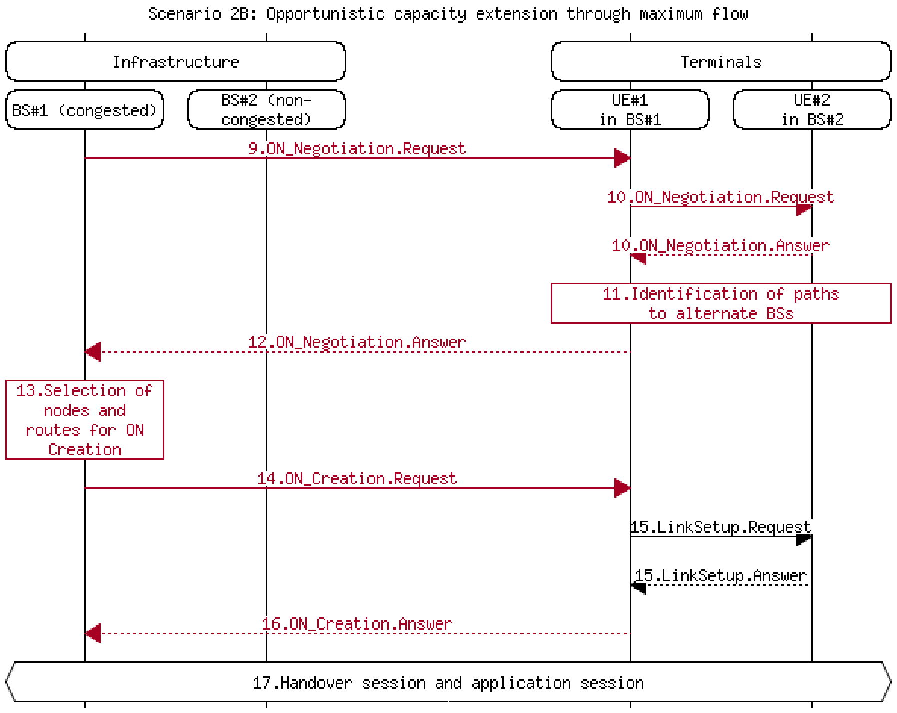


Figure 30: Scenario 2B "Opportunistic capacity extension through maximum flow" – Single congested BS – Creation phase.

5.3.1.3 ON maintenance

In this phase it is assumed that an ON is already created and UE#2 that was connected with UE#1 loses its connectivity (e.g. UE#2 left the ON). Hence, UE#1 notifies its BS (BS#1) about the problem. After that, the modification procedure initiates.

18. The problematic situation (i.e. network failure between UE#1 and UE#2) is discovered.
19. UE#1 notifies its BS (BS#1) about the problem.
20. The CMON of the congested BS (BS#1) sends a modification request to the CMON of the terminal in the congested area (UE#1).
21. The problematic terminal (UE#1) sets up a link with a neighboring terminal (UE#3).
22. The CMON of UE#1 that is in the congested area replies back to the CMON of its served BS (ON_Modification.Answer).
23. A handover of the session from the direct link between UE#1 and UE#2 is made so that UE#1 now uses a link towards UE#3 which forwards traffic towards an alternate BS. The application session is activated.

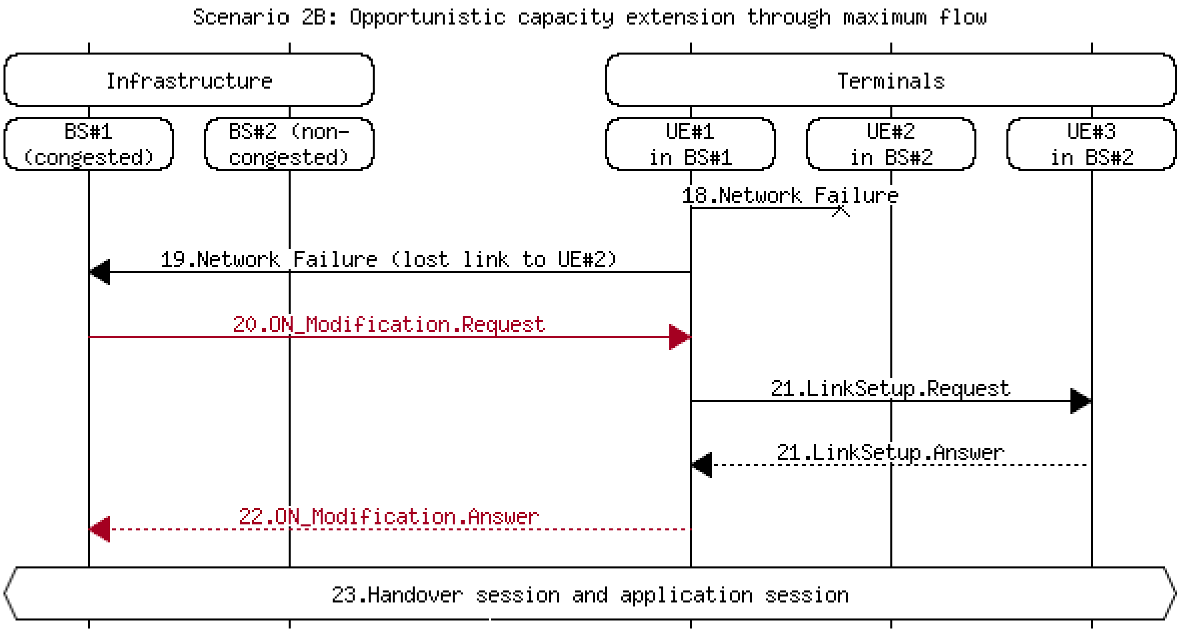

Scenario 2B: Opportunistic capacity extension through maximum flow
Infrastructure
Terminals
BS#1 (congested)
BS#2 (non-congested)
UE#1 in BS#1
UE#2 in BS#2
UE#3 in BS#2
18.Network Failure
19.Network Failure (lost link to UE#2)
20.ON_Modification.Request
21.LinkSetup.Request
21.LinkSetup.Answer
22.ON_Modification.Answer
23.Handover session and application session

Figure 31: Scenario 2B "Opportunistic capacity extension through maximum flow" – Single congested BS - Maintenance phase.

5.3.1.4 ON termination

24. The CMON of the congested BS sends a termination request (ON_Release.Request) to the CMON of its terminal.
25. The terminal in the congested area terminates the link with the neighbouring terminal.
26. The CMON of the terminal in the congested area replies back to the CMON of its served BS (ON_Release.Answer).

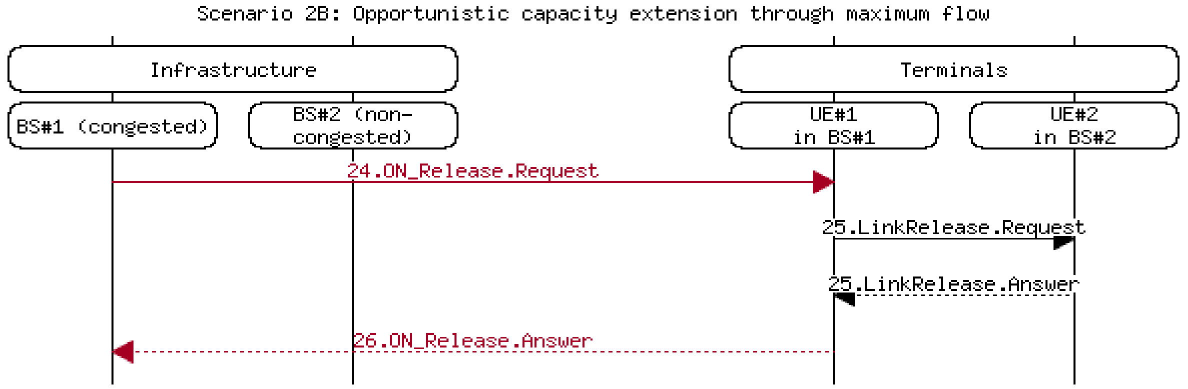


Figure 32: Scenario 2B "Opportunistic capacity extension through maximum flow" – Single congested BS - Termination phase.

5.3.2 Multiple base stations experience congestion

The opportunistic capacity extension through maximum flow scenario is also depicted in this section. This time it is assumed that more than one BSs experience congestion, in order to describe a more complex situation. A message sequence chart for opportunistic capacity extension through maximum flow is shown in Figure 33 with respect to the suitability determination phase. Figure 34 analyzes the creation phase while Figure 35 provides messages for the maintenance phase. Finally, Figure 36 analyzes the termination phase of an ON.

In this scenario it is assumed that two BSs experience congestion issues. These are BS#1 and BS#2. Moreover, it is assumed that the terminal UE#1 is registered to the problematic BS#1, while UE#3 is registered to BS#2. There is also a non-congested BS in the area (BS#3). Finally, it is assumed that UE#2 is close to UE#1 and UE#4 is close to UE#3. UE#2 and UE#4 are located into a non-congested area and can relay traffic from terminals in the congested area to terminals in the non-congested area.

5.3.2.1 ON suitability determination

1. The CSCIs of the Congested BSs identify the problematic situation.
2. The CSCIs of the Congested BSs provide the congestion information (BS context) to DSONPM.
3. The DSONPM sends a Cell-Info.Request message to the CSCIs of non-congested neighbouring BSs in order to acquire their context (the context contains the load parameter which needs to be retrieved).
4. An answer message containing the BS context is transmitted back to the DSONPM.
5. The DSONPM decides which is the most appropriate method of solving the problem and selects the CSCI that will be responsible of providing the solution (if more than one BS is in trouble). In this specific example, BS#1 acts as the selected BS which will solve the problem.
6. The DSONPM informs the selected CSCI (Cell-Info.Indication) which includes the set of congested BSs and the set of non-congested BSs.
7. The selected CSCI sends a message to the CSCIs of the congested BSs in order to acquire the list of terminals that have ON capabilities, thus they can be rerouted to alternate BSs.

8. The CSCIs of the congested BSs reply back to the selected CSCI with the list of the requested terminals.
9. The selected BS sends an information request to other congested BSs in order to acquire terminals in non-congested area with ON capabilities that will help for the ON creation. Afterwards, the discovery requests and answers will identify all available neighbouring terminals that have the ability to participate to the ON. At the end, the definition of all candidate terminals that can be part of the ON is realized.
10. The selected CSCI sends the information to the selected CMON (Report.Indication), which conveys the set of congested BSs, the set of non-congested BSs, and the set of selected candidate nodes (terminals).

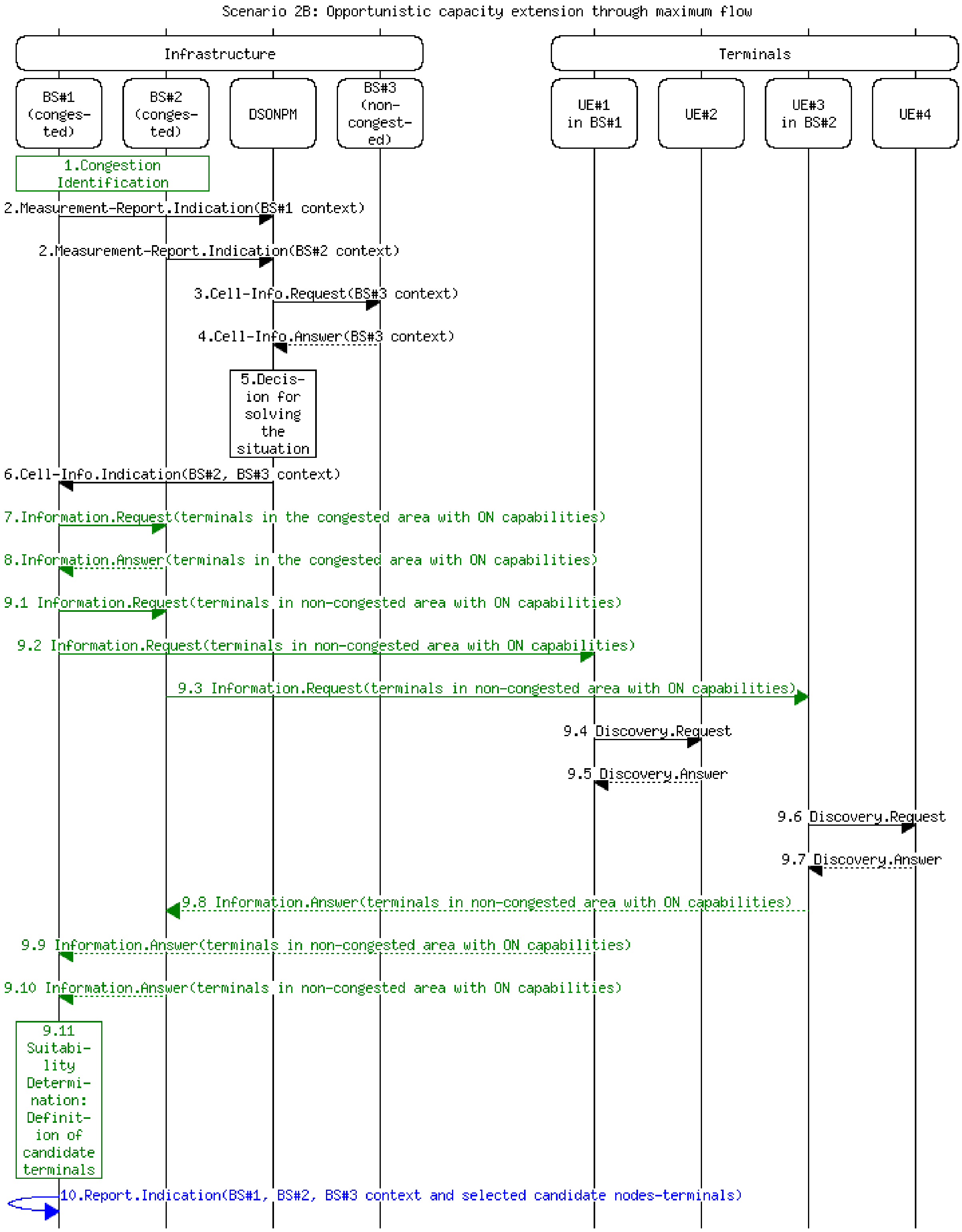

Scenario 2B: Opportunistic capacity extension through maximum flow
Infrastructure
Terminals
BS#1 (conges-ted)
BS#2 (conges-ted)
DSONPM
BS#3 (non-congest-ed)
UE#1 in BS#1
UE#2
UE#3 in BS#2
UE#4
1.Congestion Identification
2.Measurement-Report.Indication(BS#1 context)
2.Measurement-Report.Indication(BS#2 context)
3.Cell-Info.Request(BS#3 context)
4.Cell-Info.Answer(BS#3 context)
5.Decis-ion for solving the situation
6.Cell-Info.Indication(BS#2, BS#3 context)
7.Information.Request(terminals in the congested area with ON capabilities)
8.Information.Answer(terminals in the congested area with ON capabilities)
9.1 Information.Request(terminals in non-congested area with ON capabilities)
9.2 Information.Request(terminals in non-congested area with ON capabilities)
9.3 Information.Request(terminals in non-congested area with ON capabilities)
9.4 Discovery.Request
9.5 Discovery.Answer
9.6 Discovery.Request
9.7 Discovery.Answer
9.8 Information.Answer(terminals in non-congested area with ON capabilities)
9.9 Information.Answer(terminals in non-congested area with ON capabilities)
9.10 Information.Answer(terminals in non-congested area with ON capabilities)
9.11 Suitabi-lity Determi-nation: Definit-ion of candidate terminals
10.Report.Indication(BS#1, BS#2, BS#3 context and selected candidate nodes-terminals)

Figure 33: Scenario 2B “Opportunistic capacity extension through maximum flow” – Multiple congested BSs - Suitability Determination phase.

5.3.2.2 ON creation

11. The selected CMON sends a request to the CMONs of congested BSs. This message conveys the set of congested BSs, the set of non-congested BSs and the set of selected candidate nodes (terminals).

12. Each CMON of a congested BS sends an ON_Negotiation.Request message to the CMONs of the terminals located at the problematic area, in order to acquire paths to alternate BSs.

13. The terminals communicate with their neighbouring terminals (ON_Negotiation.Request) in order to acquire paths to alternate BSs.

14. The terminals communicate with their neighbouring terminals (ON_Negotiation.Request) in order to acquire paths to alternate BSs.

15. The identification of paths to alternate BSs is realized. Specifically, each terminal maintains a list of terminals and BSs to which have the ability to communicate with. Hence, through the exchange of negotiation messages, the terminals are capable of finding paths to alternate BSs.

16. Each CMON of a terminal in the congested areas sends an answering message to the CMON of the serving BS with the found paths.

17. The CMON entity of each congested BS sends an answer to the selected CMON with the requested paths.

18. The selection of nodes and routes for ON Creation takes place.

19. The selected CMON sends message (ON_Creation.Request) with the selected paths to the CMONs of the congested BSs.

20. The CMONs of the congested BSs send a message to the CMON of their terminals for the creation of the opportunistic network (ON_Creation.Request).

21. The terminals in the congested areas set up a link with the neighbouring terminals.

22. The terminals in the congested areas set up a link with the neighbouring terminals.

23. The CMONs of the terminals in the congested area reply back to the CMONs of their served BSs (ON_Creation.Answer).

24. Congested BSs reply back to the selected BS.

25. A handover of the sessions from the direct links between BS#1 and UE#1 and between BS#2 and UE#3are made so that UE#1 now uses a link towards UE#2 which forwards traffic towards non-congested BSs (e.g. BS#3). Also, UE#3 now uses a link towards UE#4 which forwards traffic towards non-congested BSs (e.g. BS#3).The application session is activated.

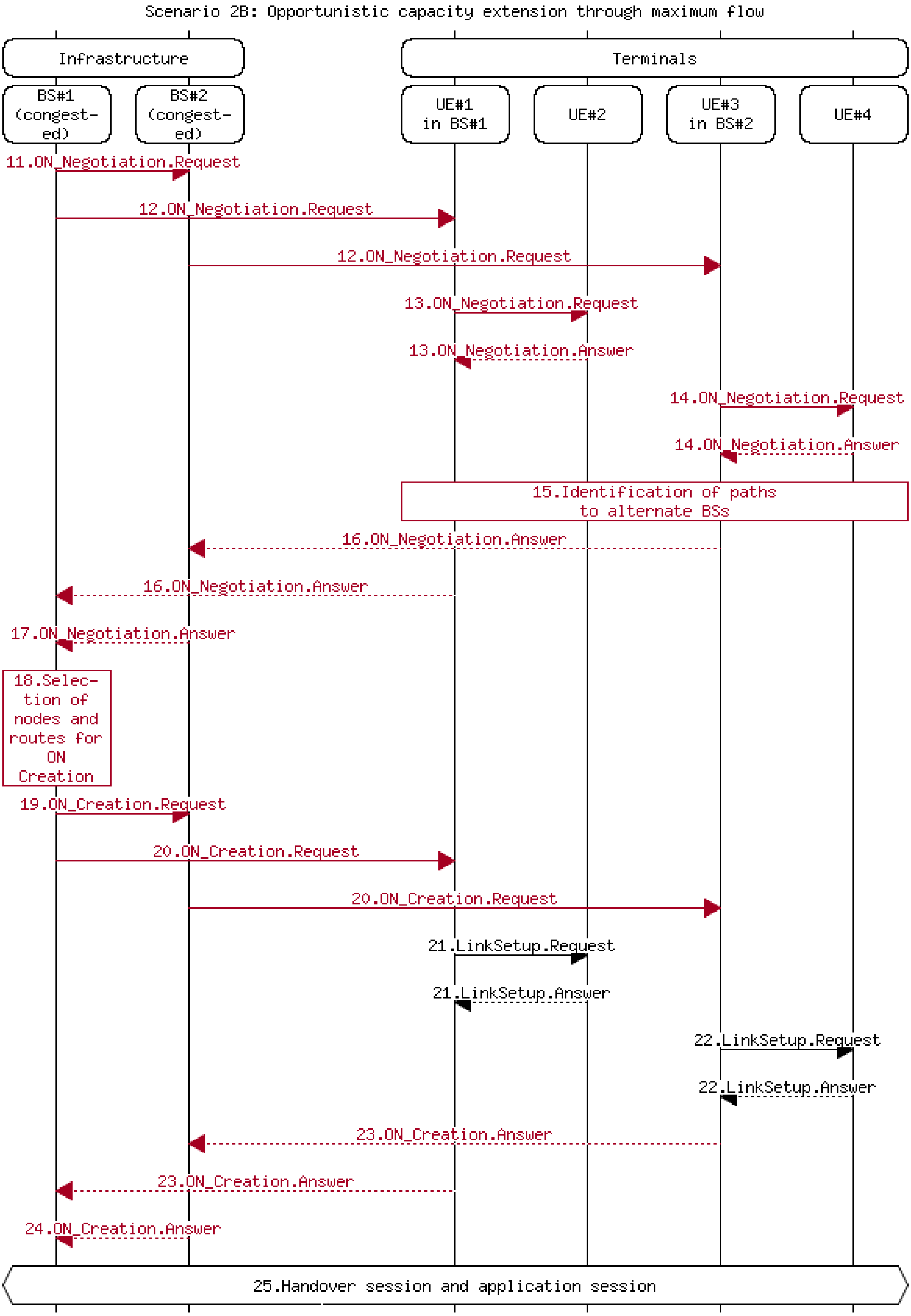


Figure 34: Scenario 2B “Opportunistic capacity extension through maximum flow” – Multiple congested BSs - Creation phase.

5.3.2.3 ON maintenance

In this phase it is assumed that an ON is already created and UE#3 that was connected with UE#4 loses its connectivity (e.g. UE#4 left the ON). Hence, UE#3 notifies its BS (BS#2) about the problem and BS#2 notifies the selected BS (BS#1). After that, the modification procedure initiates.

27. The problematic situation (i.e. network failure between UE#3 and UE#4) is discovered.
28. UE#3 notifies its BS (BS#2) about the problem and BS#2 notifies the selected BS (BS#1).
29. The CMON of the selected congested BS (BS#1) sends a modification request to the CMON of the other congested BS (BS#2). A modification request is also sent from the CMON of BS#2 to the CMONs of the terminals in the congested area (UE#3).
30. The terminal in the congested area (UE#3) sets up a link with a neighboring terminal (UE#5).
31. The CMON of the problematic terminal (UE#3) in the congested area reply back to the CMON of its served BS (ON_Modification.Answer).The congested BS replies back to the selected BS.
32. A handover of the session from the direct link between UE#3 and UE#4is made so that UE#3 now uses a link towards UE#5 which forwards traffic towards alternate BSs. The application session is activated.

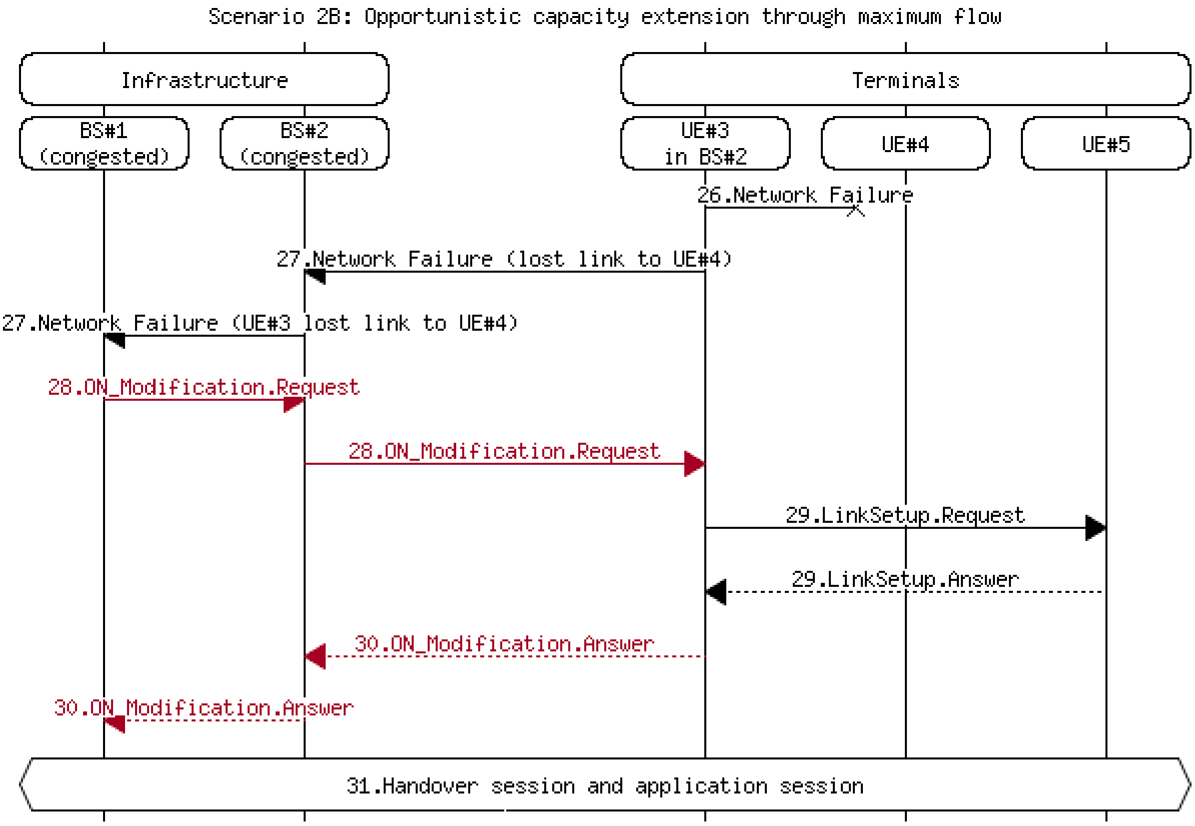

Scenario 2B: Opportunistic capacity extension through maximum flow
Infrastructure
Terminals
BS#1 (congested)
BS#2 (congested)
UE#3 in BS#2
UE#4
UE#5
26.Network Failure
27.Network Failure (lost link to UE#4)
27.Network Failure (UE#3 lost link to UE#4)
28.ON_Modification.Request
28.ON_Modification.Request
29.LinkSetup.Request
29.LinkSetup.Answer
30.ON_Modification.Answer
30.ON_Modification.Answer
31.Handover session and application session

Figure 35: Scenario 2B "Opportunistic capacity extension through maximum flow" – Multiple congested BSs - Maintenance phase.

5.3.2.4 ON termination

33. The CMON of the selected congested BS sends a termination request (ON_Release.Request) to the CMONs of other congested BSs.
34. A termination request (ON_Release.Request) is also sent from the CMONs of the congested BSs to the CMONs of their terminals.
35. The terminals in the congested area terminate the link with the neighbouring terminals.
36. The terminals in the congested area terminate the link with the neighbouring terminals.
37. The CMONs of the terminals in the congested area reply back to the CMONs of their served BSs (ON_Release.Answer).
38. Congested BSs reply back to the selected BS.

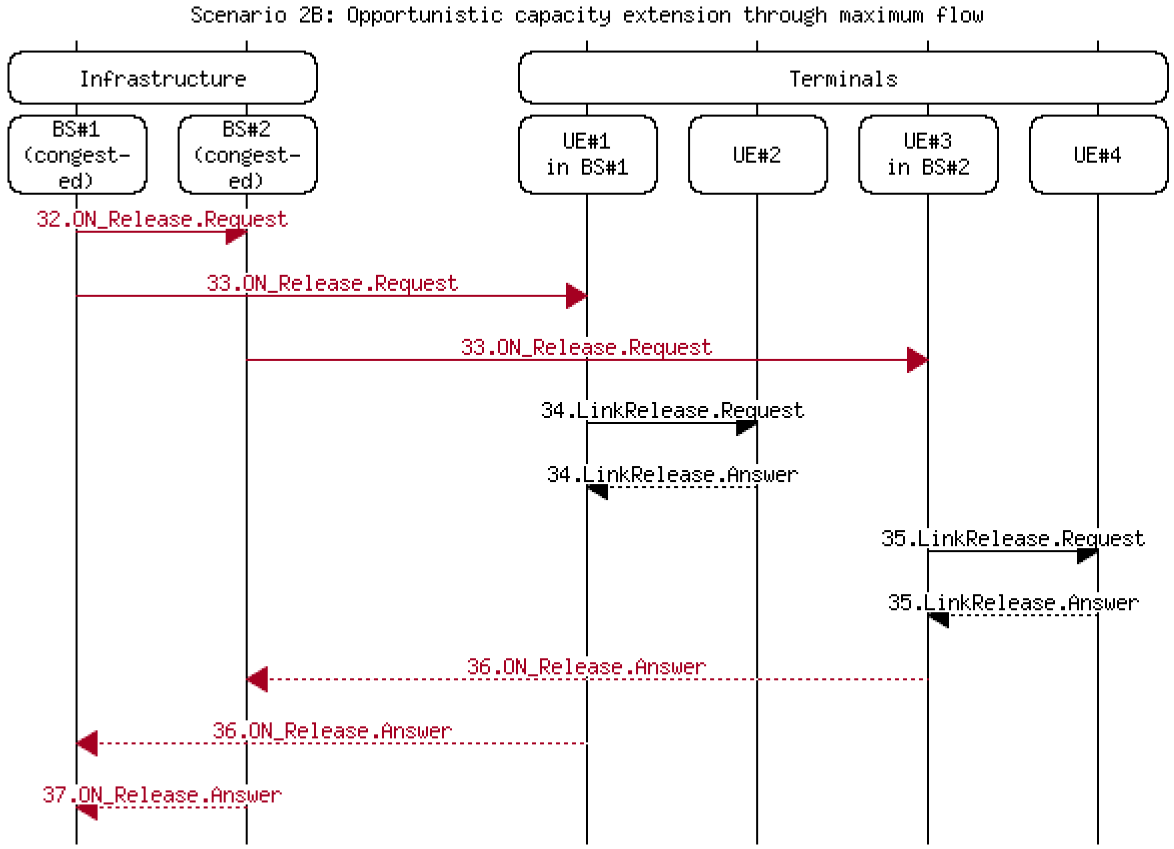


Figure 36: Scenario 2B "Opportunistic capacity extension through maximum flow" – Multiple congested BSs - Termination phase.

5.4 Scenario 3: Infrastructure supported opportunistic ad-hoc networking

In this scenario, ON functionalities are used for the infrastructure supported creation and operation of ad-hoc networks or direct short range links between nearby devices. These could be the typical situation in the uses cases "infrastructure-governed home networking" and "Opportunistic networks as platforms for location-specific services" identified under "Scenario 3: Infrastructure supported opportunistic ad-hoc networking" described in D2.1.

The considered scenario used to build the MSCs consists of two ON-enabled terminals, which could establish a short range radio link between them, and an infrastructure base station (e.g. femtocell) through which the ON services that will assist the radio link creation are offered. One illustrative example for the home networking use case could be the setup of a wireless link between e.g. a flat screen device with several wireless connectivity options and e.g. a network-attached storage (NAS) device capable of wirelessly streaming digital media content. Another example could be the case of two cellular smartphones running some type of application that is aware of the proximity of communicating users and wisely exploits the short range radio capabilities of the smartphones to establish direct radio links for the exchange of some information.

In following section a terminal centric approach is presented, in which Infrastructure provides only a limited support (i.e. initiate the suitability determination phase, provide information about the spectrum availability, allocate/assign dedicated resources, synchronize resource allocation with DSM).

Not specified hereinafter, however possible are network centric scenarios where infrastructure plays more significant role (e.g. allows for relaying C4MS messages between users, participates in decision making on ON creation, maintenance or termination).

5.4.1 ON suitability determination

Before the ON suitability determination phase is actually started, it’s assumed that both ON-enabled terminals (denoted as UE#1 and UE#2) discover the presence of the ON-enabled base station (denoted simply as BS) and attach to the infrastructure network through it. Also, announcement of ON supported capabilities and exchange of initial ON specific information can take place at this point. These initial steps before the start of the ON suitability determination phase are depicted in Figure 37 and explained in the following:

1. UE#1 discovers and attaches to the infrastructure. Discovery and attach mechanisms are RAT specific. The attach mechanism can include authentication & authorisation as well as registration procedures for getting access to infrastructure network services.

2. Before starting the ON suitability determination phase, it could also happen that the BS let terminals know about its ON supported features as well as some basic ON policies. This can be achieved by means of the Information-Indication (INI) procedure.

3. Optionally ON capabilities of the terminals and ON profiles of the users could be requested at this point by the infrastructure by means of the Information-Request (INR) procedure. This information could be used to support a network initiated ON creation, as shown in Figure 38.

4. UE#1 provides BS with the requested information by sending an Information-Answer (INA) message.

5.-8. These steps illustrate that UE#2 will also go through an identical process as the one described above for UE#1.

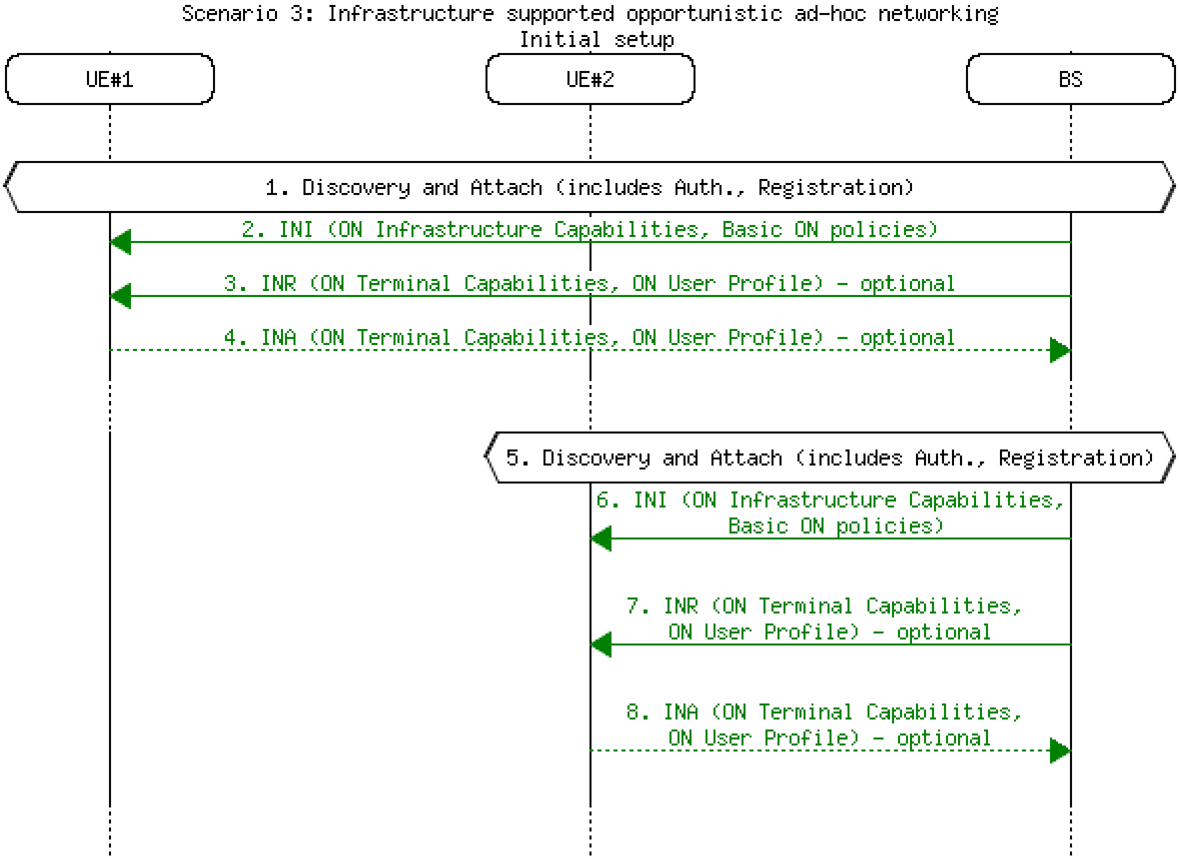

Scenario 3: Infrastructure supported opportunistic ad-hoc networking
Initial setup
UE#1
UE#2
BS
1. Discovery and Attach (includes Auth., Registration)
2. INI (ON Infrastructure Capabilities, Basic ON policies)
3. INR (ON Terminal Capabilities, ON User Profile) - optional
4. INA (ON Terminal Capabilities, ON User Profile) - optional
5. Discovery and Attach (includes Auth., Registration)
6. INI (ON Infrastructure Capabilities, Basic ON policies)
7. INR (ON Terminal Capabilities, ON User Profile) - optional
8. INA (ON Terminal Capabilities, ON User Profile) - optional

Figure 37: Scenario 3 "Infrastructure supported opportunistic ad-hoc networking" – Initial setup of the scenario.

Terminal initiated:

MSC derived in this paragraph is intended to be valid for a general case of a terminal initiated opportunistic ad-hoc network where the initial decision that triggers the ON suitability determination and negotiation is made without exclusively relying on ON functionalities (e.g. decision to establish a short range radio link made at application layer).

Once terminals are successfully registered, MSC in Figure 38 shows the steps that will form part of the ON suitability determination phase in terminal initiated case. The terminal initiated case assumes that terminals periodically scan for ON opportunities. The information on how to scan (e.g. scanning period, RAT interfaces used for scanning) could be obtained from the basic ON policies received from the infrastructure during the initial setup (see Figure 37, steps 2 and 6):

1. UE#1 periodically tries to discover ON opportunities.

2. UE#1 discovers UE#2 and determines that it is ON capable. It is worth noting that passive (e.g. beaconing) as well as active (e.g. probing) discovery procedures could be used for the purpose of node discovery. The type of discovery mechanisms could be predefined by the basic ON policies.

3. UE#1 decides that a direct radio link (e.g. Direct Wi-Fi connection) to communicate with nearby device UE#2 could be established. This decision triggers the ON suitability determination phase in order to check whether the establishment of the link can be assisted from the infrastructure.

4. Optionally, in case discovery procedures do not provide sufficient ON related information (e.g. in case no additional information can be included in beacons or probes), UE#1 initiates a INR procedure to obtain ON terminal capabilities and ON preferences related to UE#2.

5. UE#2 provides the requested information to UE#1.

6. Optionally, in case UE#1 does not already have all the necessary policies (e.g. the policies could have been already obtained) or have outdated policies, it sends an INR message to the BS for acquiring ON operational policies.

7. BS delivers the ON operational policies to UE#1 through the IAN message. These policies will allow UE#1 to determine the next steps to proceed with the establishment of a direct link.

8. Based on the received information, UE#1 decides to initiate the negotiation in order to create an ON which may potentially consists of UE#1, UE#2 (if more than one node is in range of UE#1, negotiations can be conducted with multiple nodes)

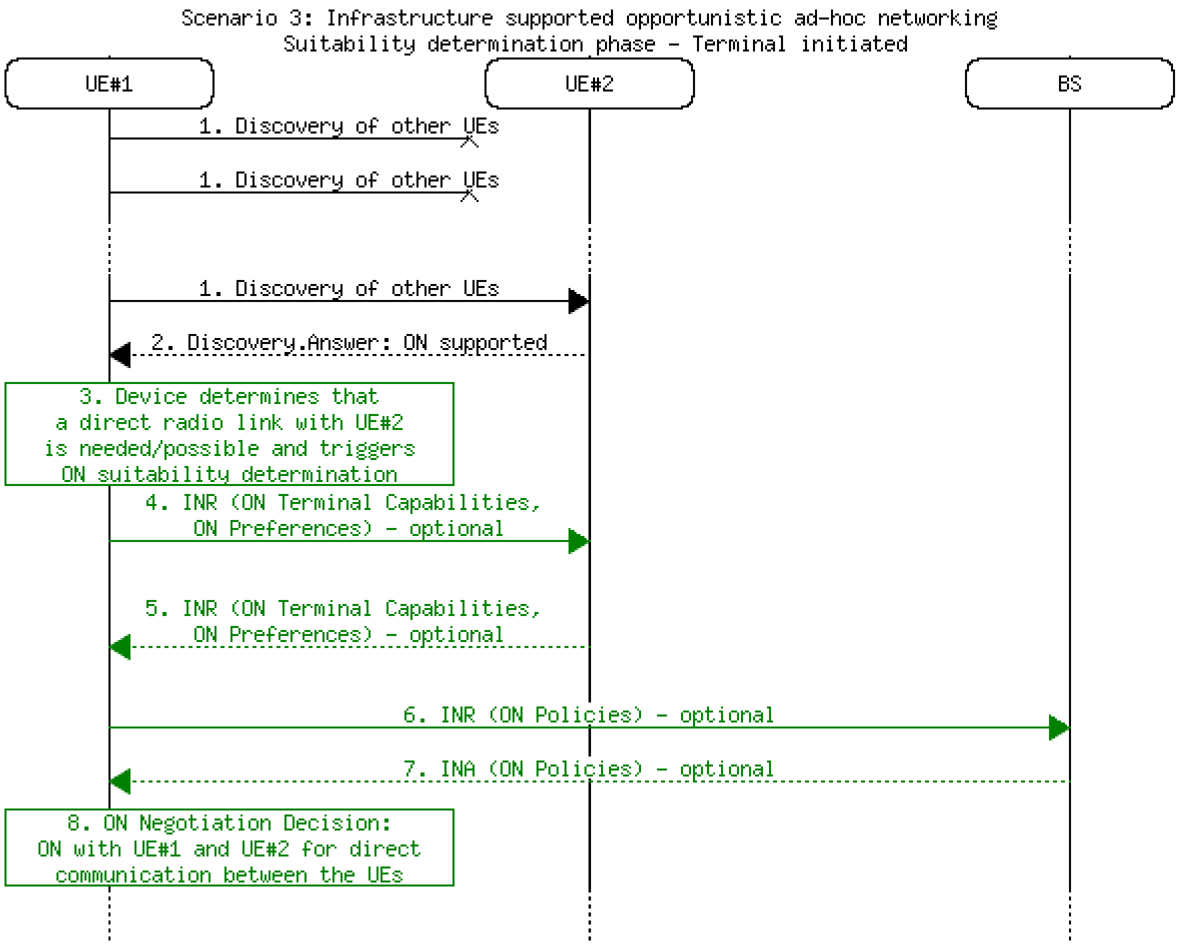

Scenario 3: Infrastructure supported opportunistic ad-hoc networking
Suitability determination phase - Terminal initiated
UE#1
UE#2
BS
1. Discovery of other UEs
1. Discovery of other UEs
1. Discovery of other UEs
2. Discovery.Answer: ON supported
3. Device determines that a direct radio link with UE#2 is needed/possible and triggers ON suitability determination
4. INR (ON Terminal Capabilities, ON Preferences) - optional
5. INR (ON Terminal Capabilities, ON Preferences) - optional
6. INR (ON Policies) - optional
7. INA (ON Policies) - optional
8. ON Negotiation Decision: ON with UE#1 and UE#2 for direct communication between the UEs

Figure 38: Scenario 3 "Infrastructure supported opportunistic ad-hoc networking" – Terminal initiated – Suitability determination phase.

Network initiated:

As an alternative to the previous MSC, the suitability for an ON may be also initiated on network side, e.g. inside the base station. For example, the base station detects that two terminals communicate with each other via the base station using cellular radio access technologies and determines that (as an optimisation) it may better to use a direct link between the terminals. After that, the BS sends an ON_Suitability.Indicaiton to UE1 indicating that an ON may be feasible between UE1 and UE2. The network support in initiating the ON suitability determination allows terminals to maintain their short range interfaces switched off and does not require them to periodically scan for ON opportunities.

In this scenario, as shown in Figure 39, the following messages are exchanged:

1. Optionally, in case UE#1 starts an application session, the SessionSetup.request is sent via RAT specific signalling towards the infrastructure network. The message may already contain information that the other communication endpoint shall be UE#2.

2. Based on information obtained during the initial setup phase (see Figure 37 steps 4, 8)[6], the network decides that a direct link between UE#1 and UE#2 may be possible and thus it is proposed to create an ON.

3. The CSCI in the BS sends an ON_Suitability.Indication towards UE#1 indicating that an ON with UE#1 and UE#2 may be possible. The message may carry some additional information such as preferred RAT interface. On the reception of this message UE#1 initiates scanning procedures in order to discover UE#2

4. The CSCI in the BS sends an ON_Suitability.Indication towards UE#2 indicating that an ON with UE#1 and UE#2 may be possible. The message may carry some additional information such as preferred RAT interface. On the reception of this message UE#2 initiates scanning procedures in order to discover UE#1.

5. UE#1 starts a discovery procedure, e.g. probing if UE#2 is in its vicinity or by listening on broadcast/beacon information from UE#2.

6. Discovery information is received from UE#2 indicating that it is supporting ONs.

7. Optionally, in case discovery procedures do not provide sufficient ON related information (e.g. in case no additional information can be included in beacons or probes), UE#1 initiates a INR procedure to obtain ON terminal capabilities and ON preferences related to UE#2.

8. UE#2 provides the requested information to UE#1.

9. Optionally, in case UE#1 does not already have all the necessary policies (e.g. the policies could have been already obtained) or have outdated policies, it sends an INR message to the BS for acquiring ON operational policies.

10. BS delivers the ON operational policies to UE#1 through the IAN message. These policies will allow UE#1 to determine the next steps to proceed with the establishment of a direct link.

11. Based on the received information, UE#1 decides to initiate the negotiation in order to create an ON which may potentially consists of UE#1, UE#2 (if more than one node is in range of UE#1, negotiations can be conducted with multiple nodes)

[6] It is assumed that both UE#1 and UE#2 are registered to the same BS

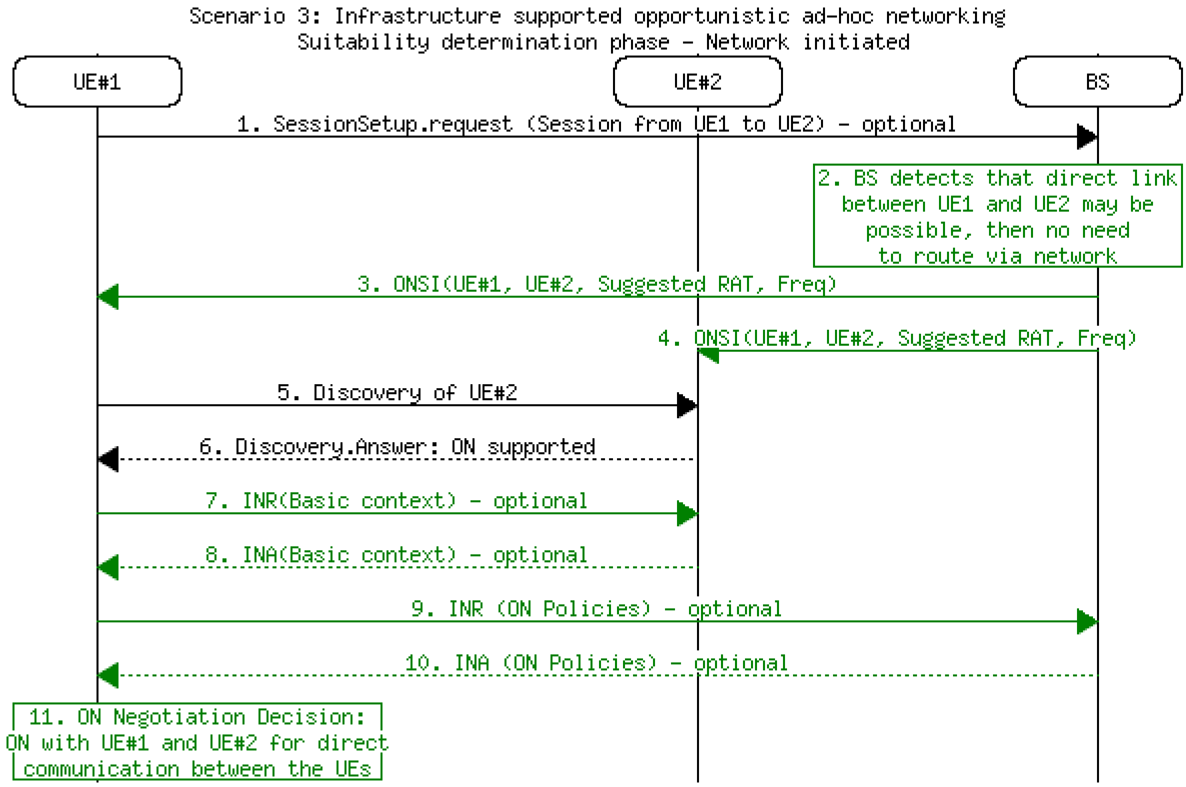

Scenario 3: Infrastructure supported opportunistic ad-hoc networking
Suitability determination phase - Network initiated
UE#1
UE#2
BS
1. SessionSetup.request (Session from UE1 to UE2) - optional
2. BS detects that direct link between UE1 and UE2 may be possible, then no need to route via network
3. ONSI(UE#1, UE#2, Suggested RAT, Freq)
4. ONSI(UE#1, UE#2, Suggested RAT, Freq)
5. Discovery of UE#2
6. Discovery.Answer: ON supported
7. INR(Basic context) - optional
8. INA(Basic context) - optional
9. INR (ON Policies) - optional
10. INA (ON Policies) - optional
11. ON Negotiation Decision: ON with UE#1 and UE#2 for direct communication between the UEs

Figure 39: Scenario 3 "Infrastructure supported opportunistic ad-hoc networking" – Suitability determination phase – Network initiated.

5.4.2 ON creation

A possible realisation of the ON creation phase for this scenario is depicted in Figure 40 where the following steps are represented:

1. As a result of the ON suitability determination phase, UE#1 has determined that the direct link establishment can be assisted by the infrastructure and that next steps to follow consists of triggering a ON Negotiation procedure to come up with the link configuration settings.

2. If necessary (e.g. ON policies may allow allocation of dedicated spectrum resources to ONs or UEs may not be capable of scanning spectrum), UE#1 sends a request to the infrastructure to determine the free spectrum resources in the area. The message may possibly indicate which terminals are involved, their location and the QoS requirements that the link is expected to support.

3. At this point, CSCI/CMON entities in the BS may determine by sending an inquiry to the Dynamic Spectrum Management (DSM) entity to the spectrum availability for the link between UE#1 and UE#2. Relevant information about involved terminals (e.g. node location, supported interfaces) as well as requested QoS could be used to enhance the accuracy of free spectrum identification. The communication with DSM is optional as CSCI/CMON entities in BS may already have enough information about the potential spectrum to be used (e.g. if the link is to be established in the ISM band, local information available at the BS about the utilisation of this band may suffice).

4. BS sends information on available spectrum back to UE#1. The information is sent using the INA message

5. The CSCI triggers the CMON in UE#1 to start the negotiation of ON between UE#1 and UE#2.

6. UE#1 sends Negotiation Request to UE#2 thus informing about the intention to establish a direct radio link between UE#1 and UE#2 and allow it to join the negotiation process for the derivation of

the radio link configuration. Some link specific requirements (required level of QoS, bit rate, frequency allocation) may be also included in this message.

7. UE#2 replies with an ON-Negotiation-Answer (ONNA) message to UE#1 by means of which it notifies its acceptance for the establishment of the link and provides some useful terminal context information to be considered in the negotiation procedure.

8. CMON in UE#1 decides that parameters of the negotiated ON fulfil its requirements and ON between itself and UE#2 shall be created.

9. The CMON informs the CSCI that the negotiation was successful.

10. UE#1 provides an ONSN to the BS indicating the successful negotiation of the ON. This means that there is no need to have the BS involved in the session. The message may also carry information on the negotiated ON configuration

11. Optionally, in case allocation of dedicated spectrum resources to ONs is supported, BS may preallocate spectrum bands which are to be used by the ON.

12. Optionally, in case the suitability determination was initiated by a SessionSetup.request (see Figure Z, step 1), a SessionSetup.response is sent to UE#1. The message informs that the session via the network is rejected and instead a direct link using the ON should be used.

13. The ON_Creation.Request is sent via C4MS from the CMON in UE#1 to the CMON in UE#2 in order to initiate the creation of the ON.

14. UE#2 replies with an ON-Creation-Answer (ONCA) message where a successful result-code is reported to indicate that the terminal is ready to establish the link. ON configuration data may also contain information about how the establishment of the link will take place (e.g. which device will adopt a master role to initiate the establishment, at which time the process will start, etc.).

15. The CMON in UE#1 initiates the setup of the user plane radio link via the JRRM towards the underlying RAT.

16. Authentication procedures between terminals may be executed at this point.

17. A RAT-specific LinkSetup.Request is sent towards UE#2. In UMTS or LTE for example, this message may be a RRC Connection.Request.

18. Finally, the creation of the ON is notified to the infrastructure from UE#1 by sending an ON-Notification-Status (ONNS) message. The final ON configuration settings are included in the message so that the infrastructure is aware of on-going ONs and their configuration..

19. Optionally, UE#2 also notifies the network that the ON has been successfully established.

20. Optionally, in case some spectrum resources were preallocated in step 11, BS allocates spectrum to the ON and informs about it the DSM

21. The Application Session is now active.

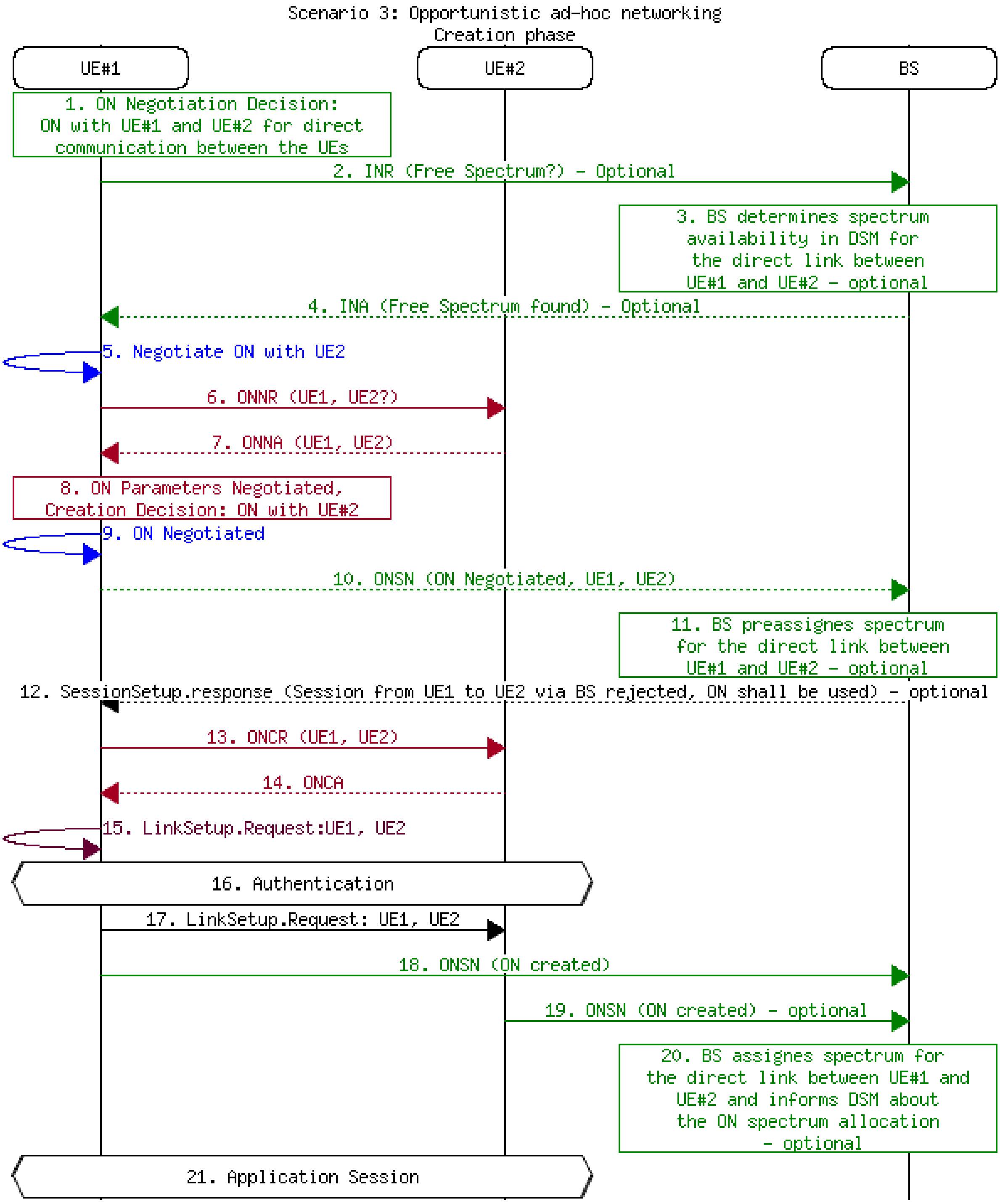

Scenario 3: Opportunistic ad-hoc networking
Creation phase
UE#1
UE#2
BS
1. ON Negotiation Decision: ON with UE#1 and UE#2 for direct communication between the UEs
2. INR (Free Spectrum?) - Optional
3. BS determines spectrum availability in DSM for the direct link between UE#1 and UE#2 - optional
4. INA (Free Spectrum found) - Optional
5. Negotiate ON with UE2
6. ONNR (UE1, UE2?)
7. ONNA (UE1, UE2)
8. ON Parameters Negotiated, Creation Decision: ON with UE#2
9. ON Negotiated
10. ONSN (ON Negotiated, UE1, UE2)
11. BS preassignes spectrum for the direct link between UE#1 and UE#2 - optional
12. SessionSetup.response (Session from UE1 to UE2 via BS rejected, ON shall be used) - optional
13. ONCR (UE1, UE2)
14. ONCA
15. LinkSetup.Request:UE1, UE2
16. Authentication
17. LinkSetup.Request: UE1, UE2
18. ONSN (ON created)
19. ONSN (ON created) - optional
20. BS assignes spectrum for the direct link between UE#1 and UE#2 and informs DSM about the ON spectrum allocation - optional
21. Application Session

Figure 40: Scenario 3 "Infrastructure supported opportunistic ad-hoc networking" – ON Creation phase.

5.4.3 ON maintenance

During the lifetime of the established radio link between both devices, context changes might occur that makes the ON to be reconfigured in order to keep fulfilling its objective. Figure 41 describes the MSC of an ON reconfiguration process that could take place during the ON maintenance phase. It is worth noting that in this MSC we assume that the ON reconfiguration is caused by the excessive interference and that UEs decide to switch to another spectrum band. The description of the different steps is as follows:

1. UE#1 requests context information from UE#2 (the procedure can be repeated periodically during the lifetime of the ON)

2. UE#2 responds with the requested context information which can be related to the link qualities, geographical location, speed, etc.

3. UE#1 detects that the radio link is not performing as expected due to a sudden increase of the interference level in the channel being used. The detection of changes in link quality is considered to be RAT specific (e.g. link level measurements) or detected at application level. Alternatively this can be also detected based on the information obtained from UE#2 in step 2. UE#1 decides to initiate procedures which would allow it to switch to another spectrum band.

4. CMON in UE#1 requests CSCI in UE#1 to inquire the infrastructure about the alternative spectrum available in the area.

5. If possible (e.g. ON policies allow allocation of dedicated spectrum resources to ONs), UE#1 sends a request to the infrastructure to determine the free spectrum resources in the area. The message may possibly indicate which terminals are involved, their location and the QoS requirements that the link is expected to support.

6. At this point, CSCI/CMON entities in the BS may determine by sending an inquiry to the Dynamic Spectrum Management (DSM) entity to the alternative spectrum for the link between UE#1 and UE#2. Relevant information about involved terminals (e.g. node location, supported interfaces) as well as requested QoS could be used here to enhance the accuracy of spectrum identification. The communication with DSM is optional as CSCI/CMON entities in BS may already have enough information about the potential spectrum to be used (e.g. if the link is to be established in the ISM band, local information available at the BS about the utilisation of this band may suffice).

7. BS sends information on available spectrum back to UE#1. The information is sent using the INA message

8. Information provided by Infrastructure to the UE#1 are transferred from CSCI to the CMON and a new configuration of ON is determined. ON reconfiguration is meant to improve link performance (e.g. level of interferences, supported QoS, bit rate etc.).

9. UE#1 sends an ON-Modification-Request (ONMR) towards UE#2 with the new ON configuration.

10. UE#2 replies with an ON-Modification-Answer (ONCA) message where a successful result-code is reported to indicate that the terminal is ready to reconfigure the link with the proposed settings.

11. The link is reconfigured at this step. This process is assumed to be RAT specific.

12. Once the link is up again with the new configuration, CMON entity in UE#1 notifies co-located CSCI entity that the configuration of the ON has changed.

13. Finally, the modification of the ON is notified to the infrastructure from UE#1 by sending an ON-Notification-Status (ONNS) message. The final ON configuration settings are included in the message so that the infrastructure is aware of the current ON configuration.

14. Optionally, in case some assignment of dedicated spectrum resources to ONs is supported, BS informs the DSM about the updates in spectrum assignment.

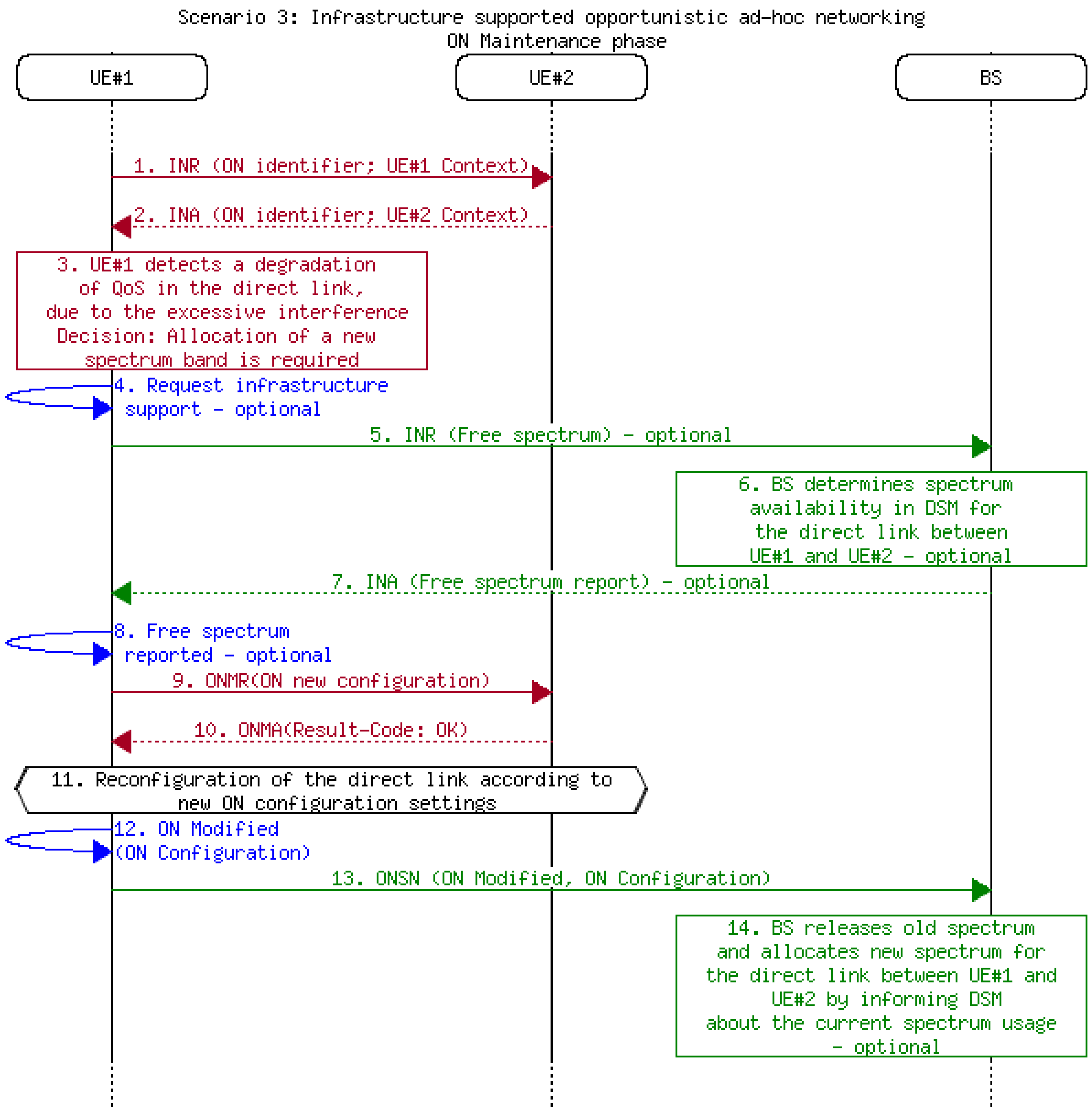

Scenario 3: Infrastructure supported opportunistic ad-hoc networking
ON Maintenance phase
UE#1
UE#2
BS
1. INR (ON identifier; UE#1 Context)
2. INA (ON identifier; UE#2 Context)
3. UE#1 detects a degradation of QoS in the direct link, due to the excessive interference Decision: Allocation of a new spectrum band is required
4. Request infrastructure support - optional
5. INR (Free spectrum) - optional
6. BS determines spectrum availability in DSM for the direct link between UE#1 and UE#2 - optional
7. INA (Free spectrum report) - optional
8. Free spectrum reported - optional
9. ONMR(ON new configuration)
10. ONMA(Result-Code: OK)
11. Reconfiguration of the direct link according to new ON configuration settings
12. ON Modified (ON Configuration)
13. ONSN (ON Modified, ON Configuration)
14. BS releases old spectrum and allocates new spectrum for the direct link between UE#1 and UE#2 by informing DSM about the current spectrum usage - optional

Figure 41: Scenario 3 "Infrastructure supported opportunistic ad-hoc networking" – ON Maintenance phase.

5.4.4 ON termination

The different steps leading to the release of the ON illustrated in this scenario are depicted in Figure 42 and explained in the following:

1. UE#1 determines that the ON is no longer needed and can be terminated. This decision can be e.g. triggered by the CMON entity when it is detected that the conditions that motivated the establishment of the ON are not valid any more (e.g. the separation of the two devices exceeds a given threshold or the application using the link was stopped).

2. An ON-Release-Request (ONRR) message is sent to UE#2.

3. UE#2 acknowledges with a ON-Release-Answer (ONRA) message.

4. The radio link is switch off at this step. This process is assumed to be RAT specific.

5. Once the link has been terminated, CMON entity in UE#1 notifies co-located CSCI entity that the associated ON has been terminated.

6. The infrastructure is notified about the ON termination through an ON-Notification-Status (ONNS) message sent by UE#1.

7. Optionally, in case some dedicated spectrum resources were assigned to the ON, BS releases the assigned spectrum resources

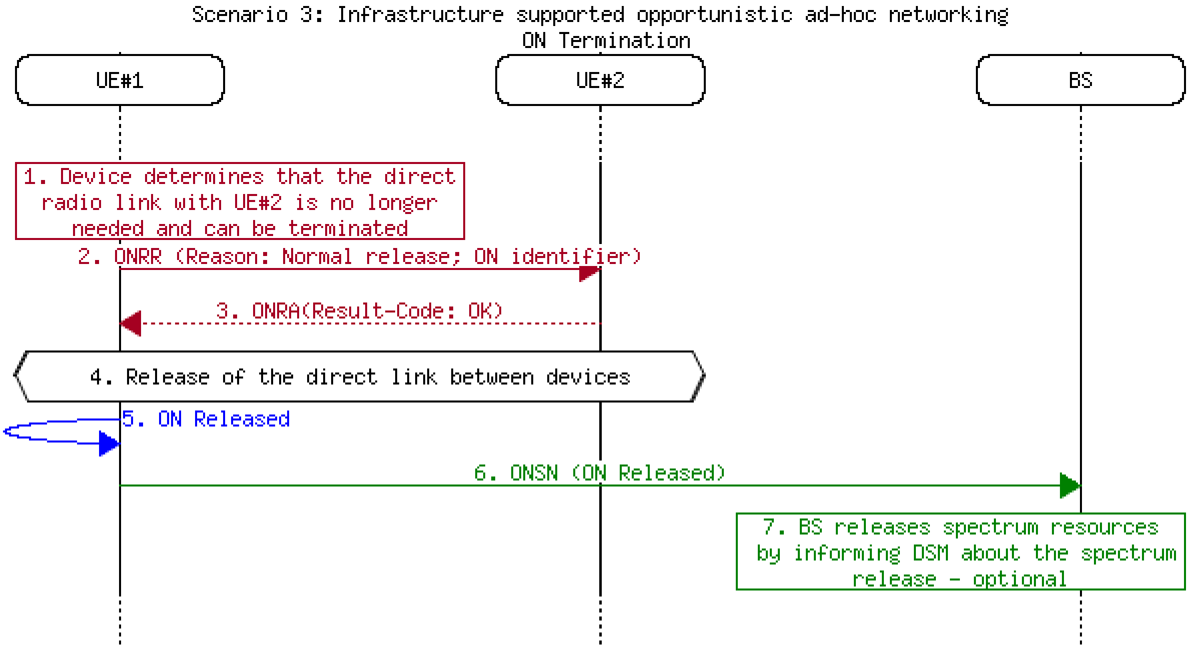

Scenario 3: Infrastructure supported opportunistic ad-hoc networking
ON Termination
UE#1
UE#2
BS
1. Device determines that the direct radio link with UE#2 is no longer needed and can be terminated
2. ONRR (Reason: Normal release; ON identifier)
3. ONRA(Result-Code: OK)
4. Release of the direct link between devices
5. ON Released
6. ONSN (ON Released)
7. BS releases spectrum resources by informing DSM about the spectrum release - optional

Figure 42: Scenario 3 "Infrastructure supported opportunistic ad-hoc networking" – ON Termination phase.

5.5 Scenario 4: Opportunistic traffic aggregation in the radio access network

A set of message sequence charts for opportunistic traffic aggregation in the radio access network scenario is shown in this section. It is worth noting here, that as the MSCs describing creation, maintenance and termination phases for Scenario 4 correspond to the MSCs developed for Scenario 1 (see Section 5.1), only the suitability determination phase is analyzed in this section.

5.5.1 ON suitability determination

During the ON Suitability determination phase nodes determine if it is beneficial to establish an ON. The decision is based on some limited information which is collected by nodes from different sources (e.g. internal sensors, neighbouring nodes, operator). The information can consist of policies, profiles, and limited context information. As the result of the ON Suitability determination a list of potential ON candidates can be established.

The ON suitability determination can be triggered by different events which could be e.g. a poor link quality towards a base station or limited capabilities of an UE (compared to the capabilities of a BS). It is worth noting that as nodes can join and leave an active ON, the ON Suitability determination needs to be continuously conducted during the entire ON activity period.

The following section presents message sequence charts related to the suitability determination phase. It is worth noting that the following MSCs are applicable also to scenarios with more than two UEs involved.

Scenarios depicted in following sub-sections (network supported or terminal initiated) are based on initial stage which is presented in Figure 43. Preceding steps are as follows:

1. Initial setup between UE#2 and BS#1 as specified in Figure 16

2. Initial setup between UE#1 and BS#1 as specified in Figure 16

3. UE#1 starts an application session using a direct link with BS#1

4. UE#1 reports some RAT specific measurement (e.g. CPICH Ec/N0) towards BS#1 (this procedure is typically conducted periodically)

5. In case UE#2 is active (i.e. it has an active connection to BS#1), it reports some RAT specific measurement (e.g. CPICH Ec/N0) towards BS#1 (this procedure is typically conducted periodically)

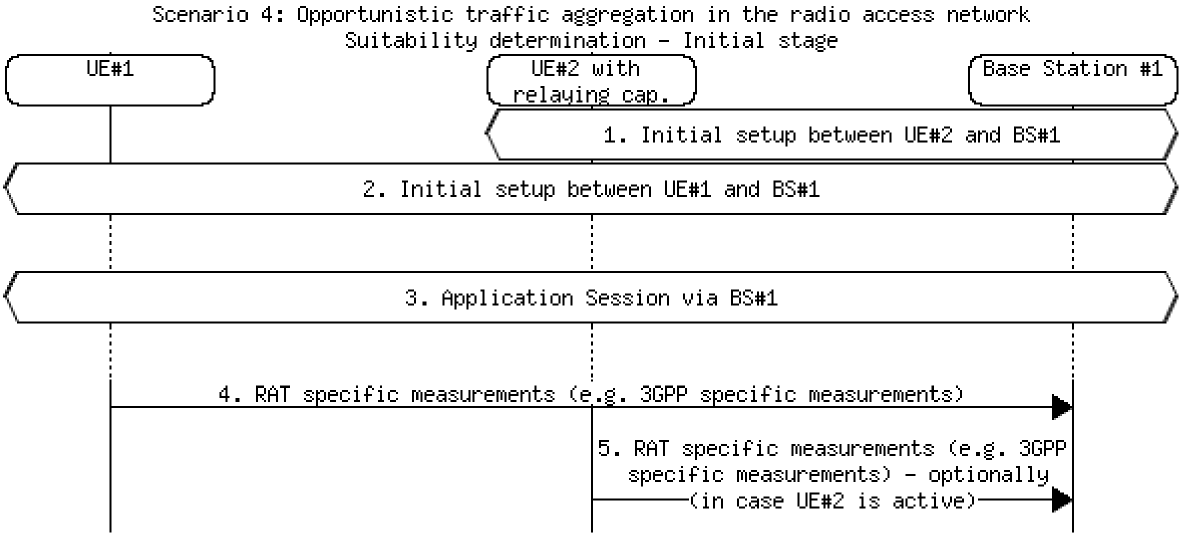

Scenario 4: Opportunistic traffic aggregation in the radio access network
Suitability determination - Initial stage
UE#1
UE#2 with relaying cap.
Base Station #1
1. Initial setup between UE#2 and BS#1
2. Initial setup between UE#1 and BS#1
3. Application Session via BS#1
4. RAT specific measurements (e.g. 3GPP specific measurements)
5. RAT specific measurements (e.g. 3GPP specific measurements) - optionally (in case UE#2 is active)

Figure 43: Scenario 4: Suitability determination – initial stage

Network Supported

The following MSC illustrates a situation in which a Base Station/Infrastructure supports UEs in suitability determination.

Preconditions: Short range radios in UE#1 and UE#2 are switched on.

Description of the messages used in Figure 44:

1. BS#1 detects e.g. poor link quality towards UE#1 (based on its own measurements and reports received from UE#1) and initiates suitability determination procedures. It is worth noting that the poor link quality is just one of the possible triggers.

2. BS#1 informs UE#1 about the potential possibility to create an ON using an ON_Suitability.Indication message. Additionally, BS#1 may provide support by suggesting the most appropriate short range interface, etc.

3. UE#1 tries to discover UE#2

4. UE#1 discovers UE#2 and determines that it is ON capable. It is worth noting that passive (e.g. beaconing) as well as active (e.g. probing) discovery procedures could be used for the node discovery

5. Optionally, in case discovery procedures do not provide sufficient ON related information (e.g. in case no additional information is included in beacons or probes), UE#1 requests some basic context information from UE#2 (e.g. link quality towards infrastructure, its capabilities)

6. UE#2 provides the requested information to UE#1

7. Based on the received information, UE#1 decides to initiate the negotiation in order to create an ON which may potentially consists of UE#1, UE#2 and BS#1 (if more than one node is in range of UE#1, negotiations can be conducted with multiple nodes)

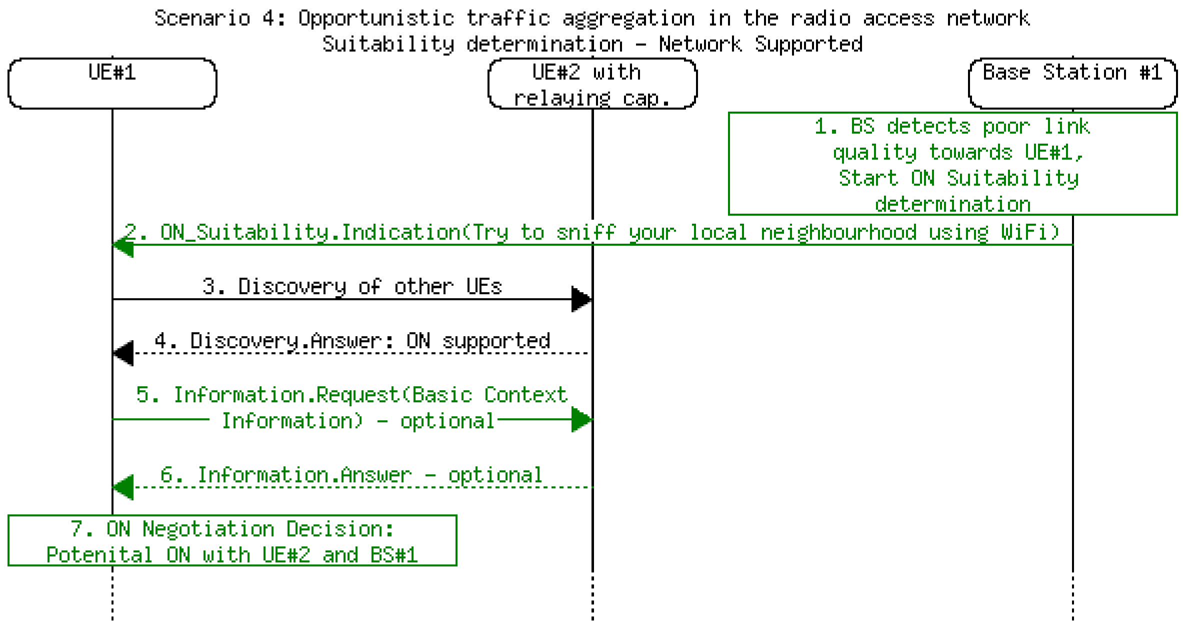

Scenario 4: Opportunistic traffic aggregation in the radio access network
Suitability determination - Network Supported
UE#1
UE#2 with relaying cap.
Base Station #1
1. BS detects poor link quality towards UE#1, Start ON Suitability determination
2. ON_Suitability.Indication(Try to sniff your local neighbourhood using WiFi)
3. Discovery of other UEs
4. Discovery.Answer: ON supported
5. Information.Request(Basic Context Information) - optional
6. Information.Answer - optional
7. ON Negotiation Decision: Potenital ON with UE#2 and BS#1

Figure 44: Scenario 4 - Suitability determination – Network Supported

The following messages slightly modify the previous MSC and are used in case users do not keep short range radio interfaces switched on in their terminals (the messages are optional). See Figure Figure 45 for the message sequence chart:

1. BS#1 detects poor link quality towards UE#1 and initiates the suitability determination procedures. It is worth noting that a poor link quality is just one of possible triggers.

2. BS#1 requests UE#1 to provide its current geographical location (this message is optional and is used in case UE#1 is GPS capable and/or infrastructure based localization via triangulation is not possible)

3. UE#1 provides its current location to BS#1 (this message is generated only in case message 11is used)

4. BS#1 sends an ON-Suitability.Indication to all UEs in its coverage. The message carries information on the location of UE#1 which is obtained in the previous step (or using infrastructure based localization via triangulation).

5. UE#2 determines itself to be in a close proximity to UE#1 (it is assumed that UE#2 can determine its own location) and it switches on its short range radio interfaces to starts ON Discovery mechanisms.

6. BS#1 informs UE#1 about the potential possibility to create an ON using an ON_Suitability.Indication message. Additionally, BS#1 may provide support by suggesting the most appropriate short range interface, etc.

7. UE#1 tries to discover UE#2

8. UE#1 discovers UE#2 and determines that it is ON capable. It is worth noting that passive (e.g. beaconing) as well as active (e.g. probing) discovery procedures could be used for this purpose

9. Optionally, in case discovery procedures do not provide sufficient ON related information (e.g. in case no additional information is included in beacons or probes), UE#1 requests some basic context information from UE#2 (e.g. link quality towards infrastructure, its capabilities)

10. UE#2 provides the requested information to UE#1

11. Based on the received information, UE#1 decides to initiate the negotiation in order to create an ON which may consists of UE#1, UE#2 and BS#1 (if more than one node is in range of UE#1, negotiations can be conducted with multiple nodes)

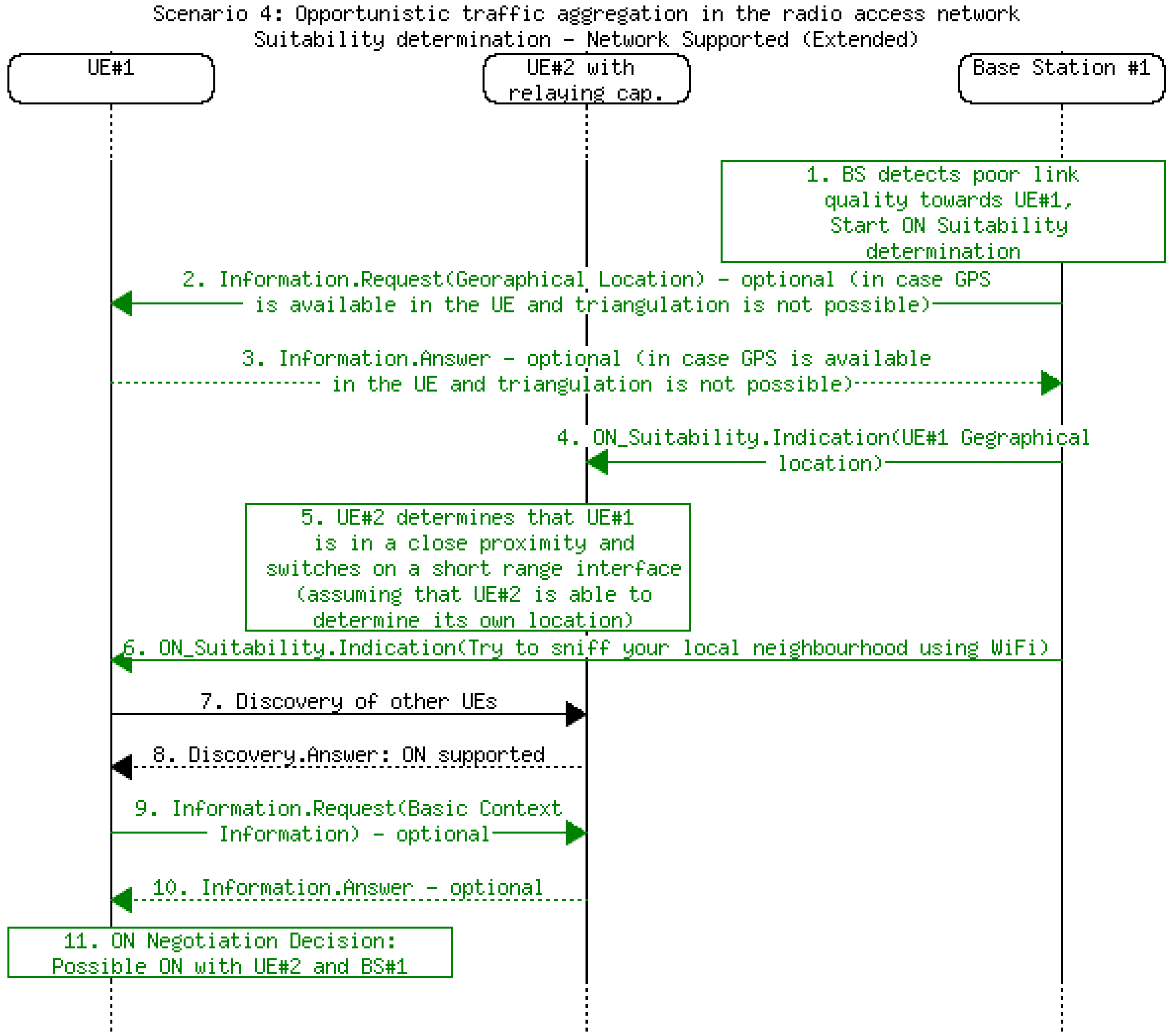

Scenario 4: Opportunistic traffic aggregation in the radio access network
Suitability determination - Network Supported (Extended)
UE#1
UE#2 with relaying cap.
Base Station #1
1. BS detects poor link quality towards UE#1, Start ON Suitability determination
2. Information.Request(Georaphical Location) - optional (in case GPS is available in the UE and triangulation is not possible)
3. Information.Answer - optional (in case GPS is available in the UE and triangulation is not possible)
4. ON_Suitability.Indication(UE#1 Gegraphical location)
5. UE#2 determines that UE#1 is in a close proximity and switches on a short range interface (assuming that UE#2 is able to determine its own location)
6. ON_Suitability.Indication(Try to sniff your local neighbourhood using WiFi)
7. Discovery of other UEs
8. Discovery.Answer: ON supported
9. Information.Request(Basic Context Information) - optional
10. Information.Answer - optional
11. ON Negotiation Decision: Possible ON with UE#2 and BS#1

Figure 45: Scenario 4 - Suitability determination – Network Supported (Extended Version)

Terminal Initiated

The following MSC illustrates a situation in which a Base Station/Infrastructure does not support UEs in suitability determination. Following steps follow after initial stage presented in Figure 43.

Preconditions: Short range radios in UE#1 and UE#2 are switched on.

Description of the messages used in Figure 46:

1. UE#1 detects poor link quality towards BS#1 and initiates the suitability determination procedures. It is worth noting that a poor link quality is just one of possible triggers.

2. UE#1 tries to discover UE#2

3. UE#1 discovers UE#2 and determines that it is ON capable. It is worth noting that passive (e.g. beaconing) as well as active (e.g. probing) discovery procedures could be used for this purpose

4. Optionally, in case discovery procedures do not provide sufficient ON related information (e.g. in case no additional information is included in beacons or probes), UE#1 requests some basic context information from UE#2 (e.g. link quality towards infrastructure, its capabilities)

5. UE#2 provides the requested information to UE#1

6. Based on the received information, UE#1 decides to initiate the negotiation in order to create an ON which consists of UE#1, UE#2 and BS#1 (if more than one node is in range of UE#1, negotiations can be conducted with multiple nodes)

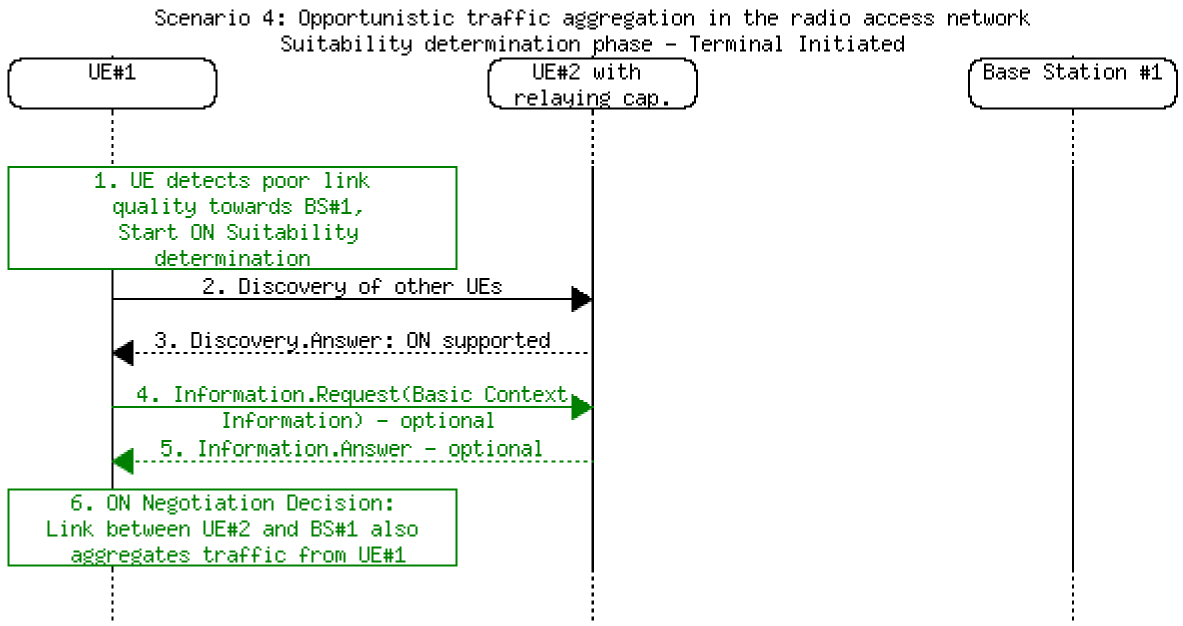

Scenario 4: Opportunistic traffic aggregation in the radio access network
Suitability determination phase - Terminal Initiated
UE#1
UE#2 with relaying cap.
Base Station #1
1. UE detects poor link quality towards BS#1, Start ON Suitability determination
2. Discovery of other UEs
3. Discovery.Answer: ON supported
4. Information.Request(Basic Context Information) - optional
5. Information.Answer - optional
6. ON Negotiation Decision: Link between UE#2 and BS#1 also aggregates traffic from UE#1

Figure 46: Scenario 4 - Suitability determination – Terminal Initiated

5.6 Scenario 5: Opportunistic resource aggregation in the backhaul network

A set of message sequence charts for opportunistic resource aggregation in the backhaul network scenario is shown in this section. The proposed message sequence charts analyze different phases of the ON life cycle i.e. suitability determination, creation, maintenance and termination.

5.6.1 ON suitability determination

During the ON Suitability determination phase BSs determine if it is beneficial to establish an ON. The decision whether to initiate the ON creation procedures is based on information which is collected by BSs from different sources (e.g. internal sensors, neighbouring BSs, operator). This information may include policies, profiles, or limited context information. As the result of the ON Suitability determination a list of potential ON candidates can be established. It is worth noting here that as BSs can join and leave an ON, the ON Suitability determination needs to be continuously conducted during the entire ON activity period.

The following section presents message sequence charts related to the suitability determination phase. It is worth noting that the following MSCs are applicable also to scenarios with more than two BSs involved.

The ON suitability determination in case of the Opportunistic resource aggregation in the backhaul network scenario can be triggered by different events. These events could include e.g. backhaul link congestion.

Description of the messages used in Figure 47:

Precondition: BS#1 and BS#2 belong to the same operator. BS#1 and BS#2 are neighbours. BS#1 and BS#2 are capable to exchange information (radio link or wire link). BS#1 and BS#2 are bootstrapped with the up-to-date ON related policies. BS#1 and BS#2 are aware of each other's capabilities.

1. Optionally, BS#1 sends RAT specific reports towards BS#2 with some measurement results (e.g. current load of BS). Such procedures are usually common in cellular networks and are typically conducted periodically. If BS#1 has more than one neighbour, the reports may be sent to multiple neighbouring base stations.

2. Optionally, BS#2 sends RAT specific reports towards BS#1 with some measurement results (e.g. current load of BS). Such procedures are usually common in cellular networks and are typically conducted periodically. If BS#1 has more than one neighbour, the reports may be sent to multiple neighbouring base stations.

3. BS#1 detects backhaul link congestion and initiates suitability determination procedures. It is worth noting here that the link congestion is just one of the possible triggers.

4. Optionally, in case RAT specific reports do not provide sufficient information to determine the ON suitability, BS#1 requests some additional context information from BS#2 (e.g. current load, cached video content). If BS#1 has more than one neighbour, additional information can be requested from multiple neighbouring base stations.

5. BS#2 provides the requested information to BS#1

6. Based on the received information, BS#1 decides to initiate the negotiation in order to create an ON which may potentially consists of BS#1 and BS#2. If more than one BS is on the candidate list, negotiations can be conducted with multiple BSs

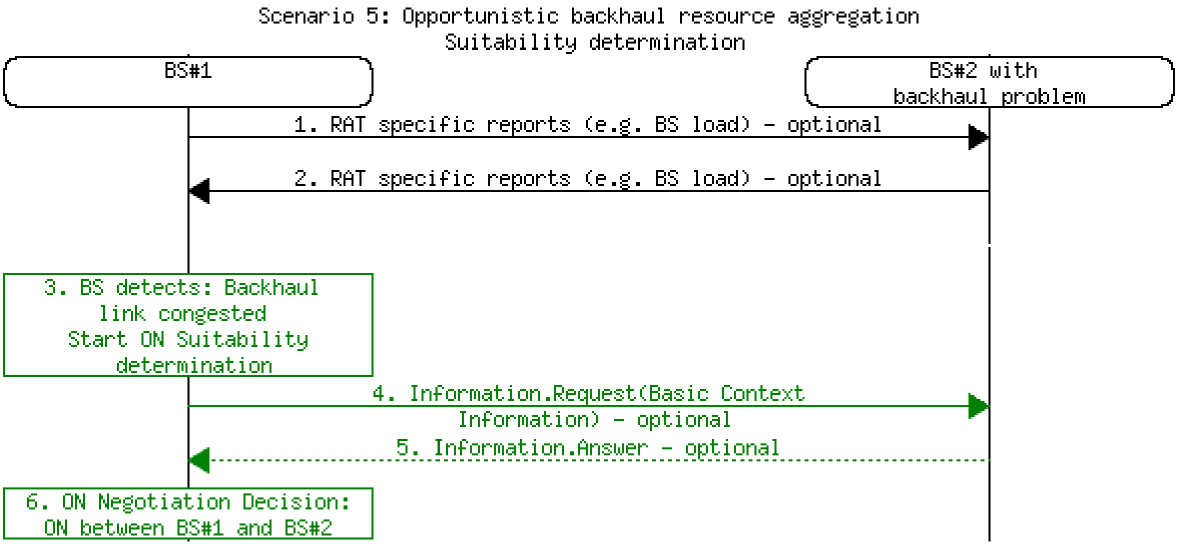

Scenario 5: Opportunistic backhaul resource aggregation
Suitability determination
BS#1
BS#2 with backhaul problem
1. RAT specific reports (e.g. BS load) - optional
2. RAT specific reports (e.g. BS load) - optional
3. BS detects: Backhaul link congested Start ON Suitability determination
4. Information.Request(Basic Context Information) - optional
5. Information.Answer - optional
6. ON Negotiation Decision: ON between BS#1 and BS#2

Figure 47: Scenario 5 – ON Suitability determination

5.6.2 ON creation

Similarly to other scenarios, the ON Creation phase can be subdivided into two sub-phases. During the first sub-phase the Opportunistic Network parameters are being negotiated between the ON candidates (in this case Base Stations). Based on the information obtained in this way, an ON blue print which defines a final ON configuration is determined (final list of ON participants, spectrum to be used, etc.). The second sub-phase of the ON Creation phase is responsible for the execution of the ON blue print and establishment of the actual ON.

The following section presents a possible realisation of the ON creation phase for this scenario. It is worth noting that the presented MSC is applicable also to scenarios with more than two BSs involved.

Preconditions: BS#1 and BS#2 are each other neighbours. BS#1 determined BS#2 as a potential ON candidate.

Description of the messages used in Figure 48:

1. Based on the received information, BS#1 decides to initiate the negotiation in order to create an ON which may potentially consists of BS#1 and BS#2. If more than one BS is on the candidate list, negotiations can be conducted with multiple BSs

2. CSCI initiates ON creation phase by sending an ON Creation trigger to CMON and passing some information about the potential ON candidates

3. An ON_Negotiation.Request including the capabilities and requirements is sent from BS#1 to BS#2.

4. BS#2 determines that it has sufficient resources to support additional traffic and decides to participate in the ON.

5. BS#2 sends an ON_Negotiation.Answer towards BS#1. The answer includes additional context information which could be useful in determining the most suitable ON configuration.

6. Having all the necessary context information, BS#1 determines final ON configuration. It is worth noting that in case BS#1 negotiate with more than one BS, different ON configurations are possible. It is also important to note that the negotiated network configuration can include parameters related to measurement settings (types of measurements, reporting periods, etc.).

7. BS#1 sends an ON_Creation.Request towards BS#2. The message carries all the necessary information related to the configuration of the ON (e.g. measurement configuration, power allocation, caching schemes).

8. The CMON in BS#2 initiates reconfigurations according to the received ON configuration parameters (e.g. reservation of resources to support additional traffic).

9. BS#2 sends to BS#1 an ON_Creation.Answer acknowledging the ON creation.

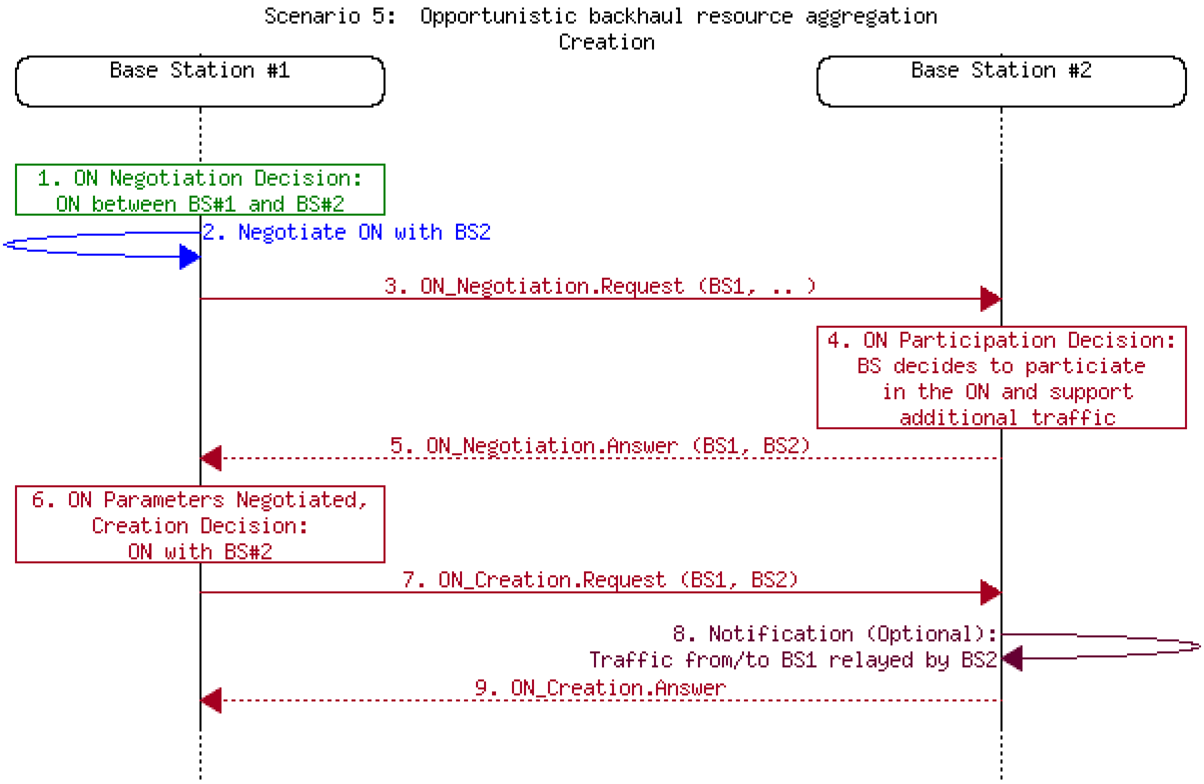

Scenario 5: Opportunistic backhaul resource aggregation
Creation
Base Station #1
Base Station #2
1. ON Negotiation Decision:
ON between BS#1 and BS#2
2. Negotiate ON with BS2
3. ON_Negotiation.Request (BS1, ..)
4. ON Participation Decision:
BS decides to particiate
in the ON and support
additional traffic
5. ON_Negotiation.Answer (BS1, BS2)
6. ON Parameters Negotiated,
Creation Decision:
ON with BS#2
7. ON_Creation.Request (BS1, BS2)
8. Notification (Optional):
Traffic from/to BS1 relayed by BS2
9. ON_Creation.Answer

Figure 48: Scenario 5 – ON Creation

5.6.3 ON maintenance

The following section provides a possible realisation of the ON management phase for scenario 5. Similarly to other scenarios, ON Maintenance phase consists of two processes. The first process is responsible for continuous collecting of different context information to monitor the ON and determine a need for the ON reconfiguration. The second process is responsible for modification of the ON configuration and it starts whenever the ON reconfiguration is determined to be necessary. It is worth noting that different external information (e.g. low link quality of other ON participant) as well as internal information (e.g. link load) can be used to trigger the reconfiguration. In order to simplify in this section only internal BS measurements are considered in this sub-section.

ON parameter modification

The following MSC (see Figure 49) illustrates a situation in which a reconfiguration of ON related parameters needs to be conducted (e.g. alteration in ON related measurements, allocation of additional resources to ON)

Precondition: BS#1, BS#2 and BS#3 are part of an ON. BS#2 and BS#3 relay traffic from/to BS#1

1. BS#1 detects that reconfiguration of ON parameters is necessary (e.g. BS#1 could experience higher backhaul link congestion) and determines the required updates.

2. BS#1 sends ON_Modification.Request message to BS#2 to inform it about the required changes (e.g. allocation of additional resources). It is worth noting here that ON_Modification.Request can be also send to other ON participants (e.g. BS#3).

3. BS#2 determines if the proposed changes are acceptable (e.g. if it can allocate more resources to support additional traffic from/to BS#1).

4. If needed, the transceiver in BS#2 is configured to be able to receive additional traffic from BS#1

5. BS#2 acknowledges the changes by sending an ON_Modification.Answer back to BS#1

6. If needed, BS#1 informs BS#3 about the updates using an ON_Status.Notification message

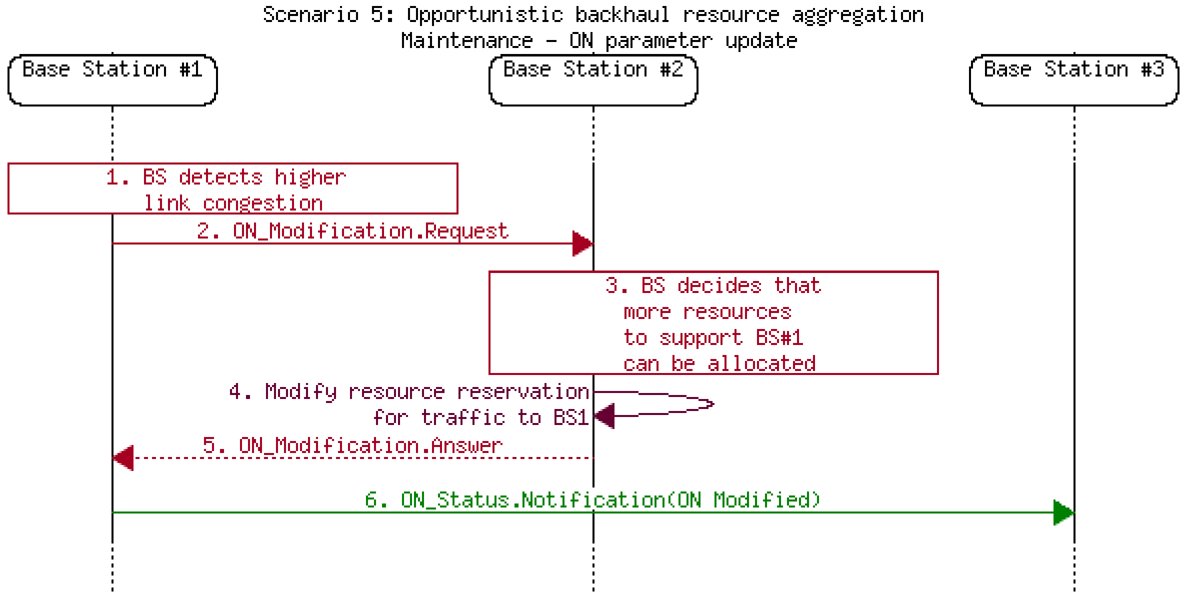

Scenario 5: Opportunistic backhaul resource aggregation
Maintenance - ON parameter update
Base Station #1
Base Station #2
Base Station #3
1. BS detects higher link congestion
2. ON_Modification.Request
3. BS decides that more resources to support BS#1 can be allocated
4. Modify resource reservation for traffic to BS1
5. ON_Modification.Answer
6. ON_Status.Notification(ON Modified)

Figure 49: Scenario 5 - ON Maintenance, ON parameter modification

ON Participant Disconnection

The following MSC (see Figure 50) illustrates a situation in which one of BSs intends to disconnect from an ON after it determines that its participation in the ON is no longer necessary or no longer feasible (e.g. due to the higher load generated by its own users).

Precondition: BS#1, BS#2, BS#3 are part of an ON. BS#2 and BS#3 relay traffic from/to BS#1.

Description of the messages used in Figure 50:

1. BS#3 determines that it can no longer relay traffic from/to BS#1 (e.g. it experiences higher load generated by its own users) and decides to leave the ON

2. BS#3 sends an ON_Release.Request message towards BS#1 in order to initiate the ON Disconnection procedure

3. BS#1 determines the necessary ON reconfigurations to compensate for disconnection of BS#3 and initiates the ON parameter modification procedure (see Figure 49 for more detail).

4. BS#1 acknowledges the disconnection of BS#3 by sending an ON_Release.Answer

5. BS#1 informs BS#2 about the disconnection of the BS#3 using an ON_Status.Notification message. The message can carry information related to the reason of the disconnection

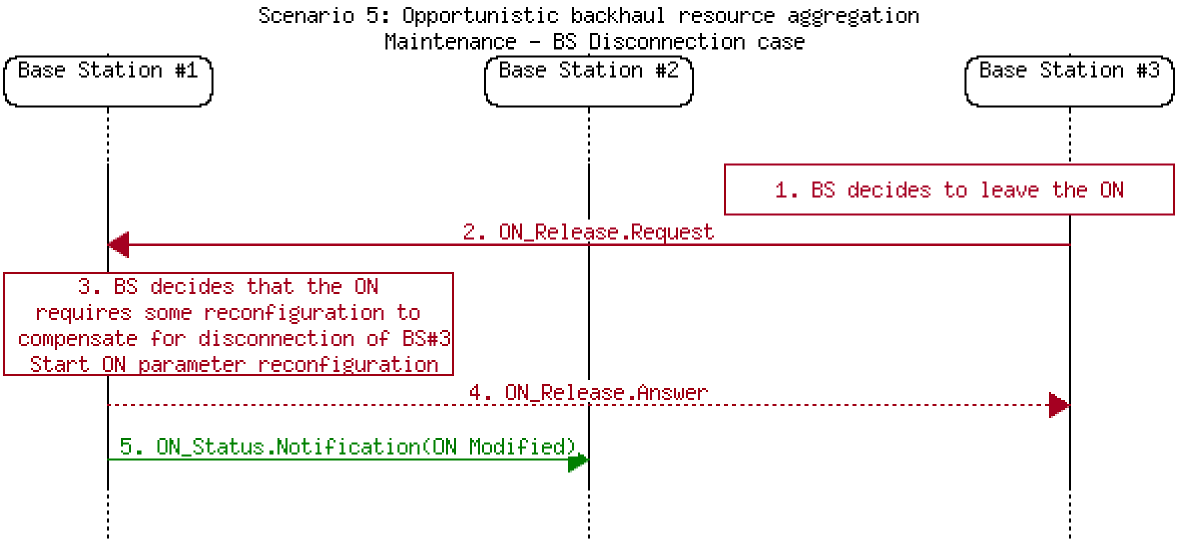

Scenario 5: Opportunistic backhaul resource aggregation
Maintenance - BS Disconnection case
Base Station #1
Base Station #2
Base Station #3
1. BS decides to leave the ON
2. ON_Release.Request
3. BS decides that the ON requires some reconfiguration to compensate for disconnection of BS#3 Start ON parameter reconfiguration
4. ON_Release.Answer
5. ON_Status.Notification(ON Modified)

Figure 50: Scenario 5 - ON Maintenance, BS disconnection

5.6.4 ON termination

The following section provides a possible realisation of the ON Termination phase for scenario 5. The ON Termination is conducted whenever all ON participants either determine it to be no longer necessary or last user disconnects form it. The ON termination is required in order to release some dedicated resources (e.g. spectrum, power, time) allocated for the purpose of serving an ON. The procedures related to the ON termination may be also used to exchange some useful ON related statistics between different ON participants.

Figure 51 presents a sequence chart for ON termination. It is worth noting that the following MSC is applicable also to scenarios with more than two BSs involved.

Precondition: BS#1, BS#2 are part of an ON

Description of the messages used in Figure 51:

1. BS#1 detects that backhaul link is no longer congested and decides to leave the ON

2. BS#1 sends an ON_Release.Request message towards BS#2 in order to initiate the ON Disconnection procedure.

3. BS#2 determines that no other BSs (besides BS#1) are using it for traffic relaying and decides to leave the ON. It is worth noting here that in case other BSs are using given ON, BS#2 may decide to remain in the ON and acknowledge the removal of BS#1 from the ON.

4. BS#2 acknowledges release of the ON by sending ON_Release.Answer.

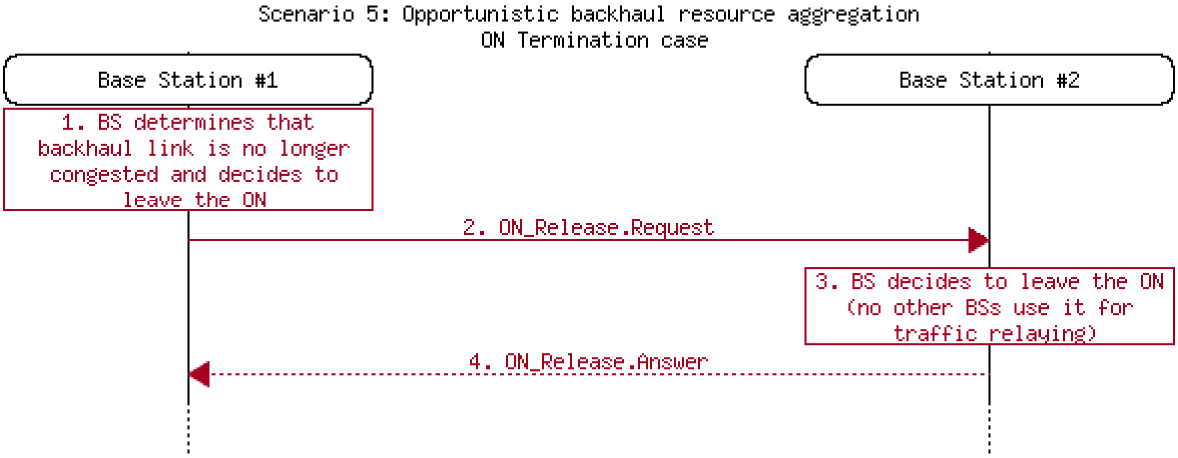

Scenario 5: Opportunistic backhaul resource aggregation
ON Termination case
Base Station #1
Base Station #2
1. BS determines that backhaul link is no longer congested and decides to leave the ON
2. ON_Release.Request
3. BS decides to leave the ON (no other BSs use it for traffic relaying)
4. ON_Release.Answer

Figure 51: Scenario 5 - ON Termination

5.7 Handover procedures

The procedures described below are for an implementation option based on extension of native 3GPP LTE signalling between UEs and eNBs, as well as between eNBs.

This is one of the possible option: another option is to re-use the 3GPP standard for “Untrusted non-3GPP IP access networks” as mentioned in some of the MSC appearing in this section and described in Appendix IV: Traffic relaying based on the standardized 3GPP solutions.

As part of OneFIT project, the 2 options are under investigation.

5.7.1 Handover from infrastructure to UE-relay

At ON creation time, active connections of some UEs need to be handed over to a UE acting as relay towards the infrastructure (via the same base station or a different one).

This is a fundamental feature of the OneFIT system, to enable operator-grade continuity of service while creating Opportunistic networks.

The way to perform this handover is deeply linked to the legacy of 3GPP networks and how these manage “normal” handovers between base stations.

The MSC shown in Figure 52 below describes a possible sequence of 3GPP native/extended signalling and ON-specific signalling that enables continuity of service, including security aspects.

In this diagram, messages with names starting with “3GPP” are legacy messages, in some case extended with some ON-specific parameters

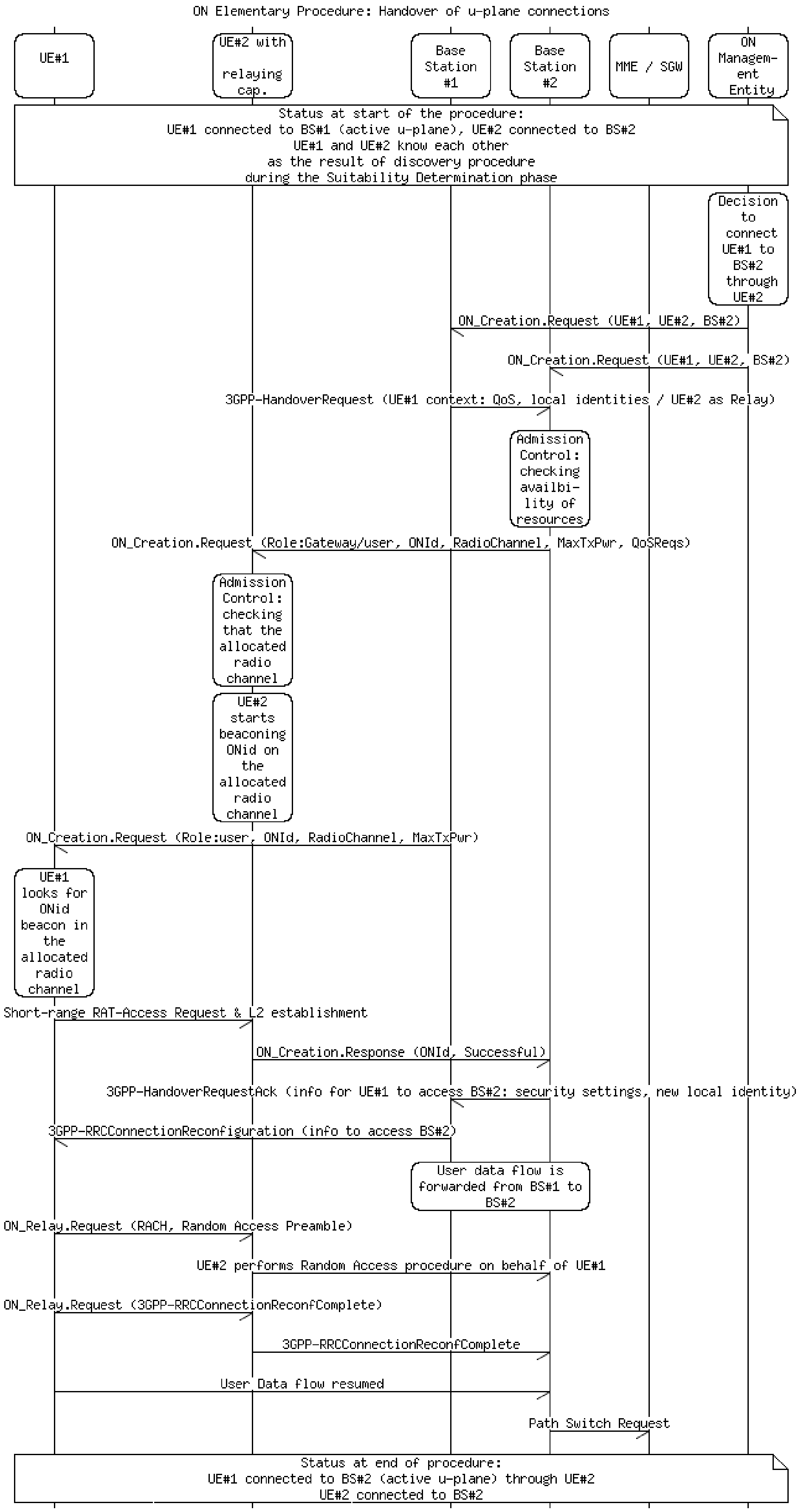

ON Elementary Procedure: Handover of u-plane connections
UE#1
UE#2 with relaying cap.
Base Station #1
Base Station #2
MME / SGW
ON Managem-ent Entity
Status at start of the procedure:
UE#1 connected to BS#1 (active u-plane), UE#2 connected to BS#2
UE#1 and UE#2 know each other
as the result of discovery procedure
during the Suitability Determination phase
Decision to connect UE#1 to BS#2 through UE#2
ON_Creation.Request (UE#1, UE#2, BS#2)
ON_Creation.Request (UE#1, UE#2, BS#2)
3GPP-HandoverRequest (UE#1 context: QoS, local identities / UE#2 as Relay)
Admission Control: checking availbi-lity of resources
ON_Creation.Request (Role:Gateway/user, ONId, RadioChannel, MaxTxPwr, QoSReqs)
Admission Control: checking that the allocated radio channel
UE#2 starts beaconing ONid on the allocated radio channel
ON_Creation.Request (Role:user, ONId, RadioChannel, MaxTxPwr)
UE#1 looks for ONid beacon in the allocated radio channel
Short-range RAT-Access Request & L2 establishment
ON_Creation.Response (ONId, Successful)
3GPP-HandoverRequestAck (info for UE#1 to access BS#2: security settings, new local identity)
3GPP-RRCConnectionReconfiguration (info to access BS#2)
User data flow is forwarded from BS#1 to BS#2
ON_Relay.Request (RACH, Random Access Preamble)
UE#2 performs Random Access procedure on behalf of UE#1
ON_Relay.Request (3GPP-RRCConnectionReconfComplete)
3GPP-RRCConnectionReconfComplete
User Data flow resumed
Path Switch Request
Status at end of procedure:
UE#1 connected to BS#2 (active u-plane) through UE#2
UE#2 connected to BS#2

Figure 52: Sequence of signalling for a handover from infrastructure to UE-Relay

6. State machines

In each node potentially participating in an ON, the CMON must have information if a node is participating in an ON or not. Further on, status information must also be stored on which other nodes are participating in the ON, especially for those nodes which have a direct link to the own node. Therefore, as shown in Figure 53, each node maintains an ON-Node-State as well as for every active link towards another node an ON-Link-State.

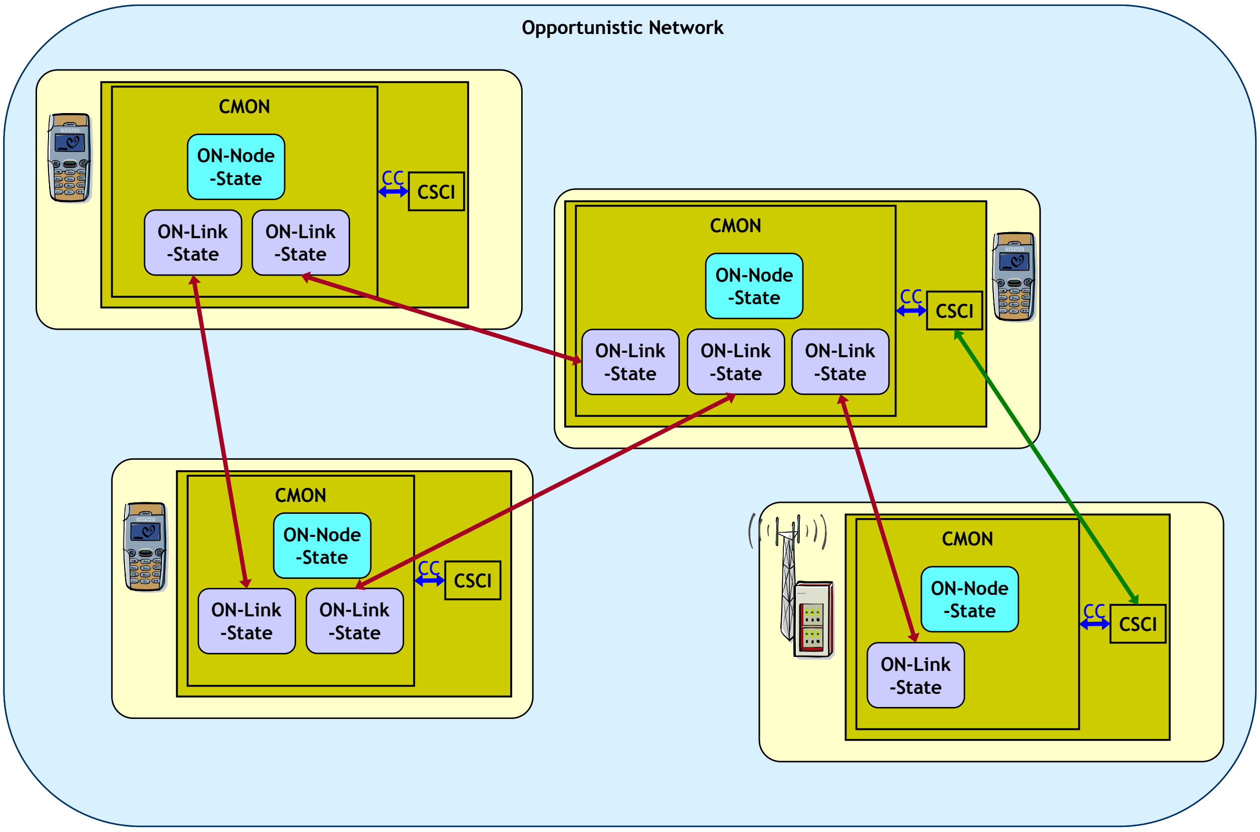


Figure 53: Location of the ON-Management related state machines inside the different nodes

Figure 54 shows the different ON-Link States. When a node has established a link towards another node, that link will initially not be able to carry ON-related traffic and the link state is “Not_in_ON”. When the ON negotiation starts over this link, either because an ON_Negotiation.request has been received or because an ON_Negotiation.request shall be sent to the other node, the state will change to “ON_Negotiating”. After successful negotiation, the ON creation will start and the state will change to “ON_Creating”. After successful creation, the link will be put into the state “ON_Active”. When the release has started, the state will be set to “ON_Releasing” and after successful release, the state is set to “Not_in_ON”.

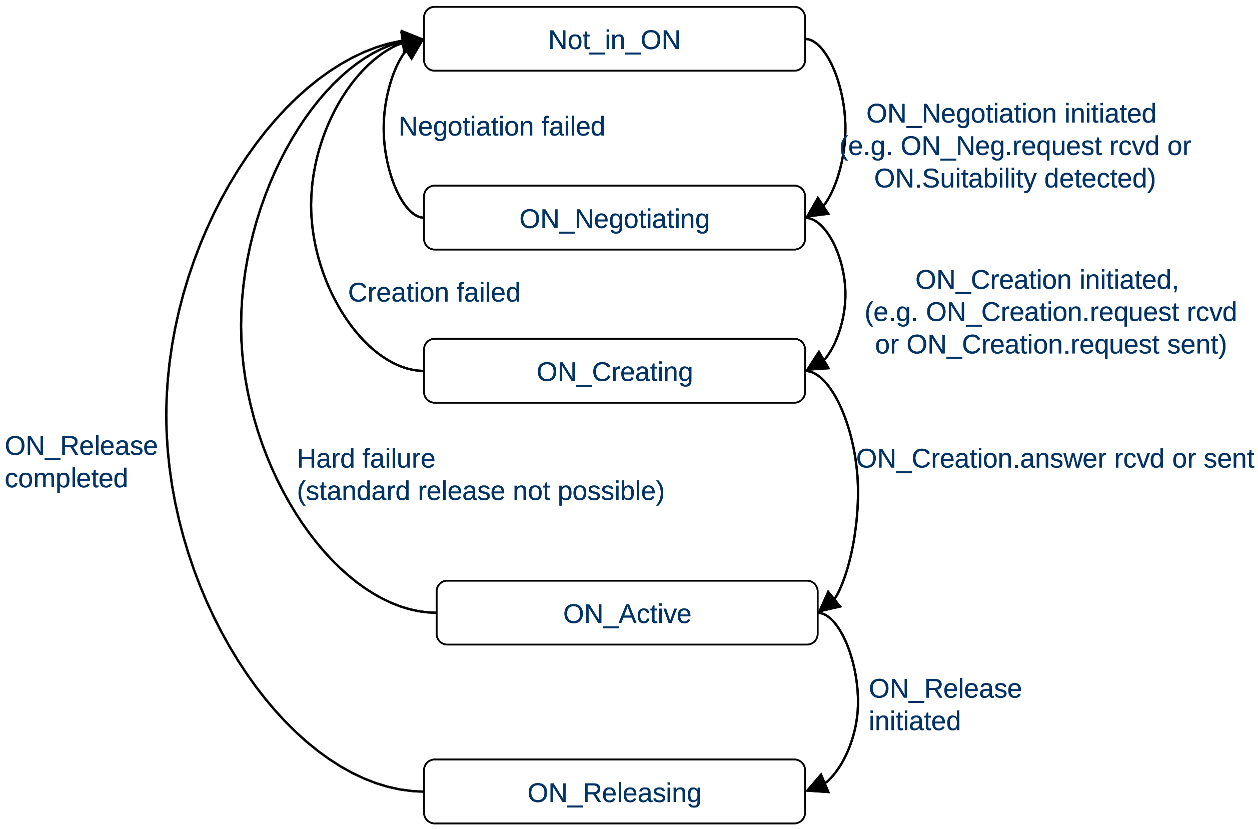

Not_in_ON
Negotiation failed
ON_Negotiation initiated (e.g. ON_Neg.request rcvd or ON.Suitability detected)
ON_Negotiating
Creation failed
ON_Creation initiated, (e.g. ON_Creation.request rcvd or ON_Creation.request sent)
ON_Creating
ON_Release completed
Hard failure (standard release not possible)
ON_Creation.answer rcvd or sent
ON_Active
ON_Release initiated
ON_Releasing

Figure 54: ON-Link-States and ON-Node-States

The ON-Node-State can take the same values as the ON-Link-State.

The ON-Node-State is created by analysing all ON-Link states:

If at least one link is in state “ON_Active” then the ON-Node state is “ON_Active”

else

If at least one link is in state “ON_Creating” then the ON-Node state is “ON_Creating”

else

If at least one link is in state “ON_Negotiating” then the ON-Node state is “ON_Negotiating”

else

If at least one link is in state “ON_Releasing” then the ON-Node state is “ON_Releasing”

else

the ON-Node state is “Not_in_ON”

Additional state machines are for further study. For example, a node may keep status for each network interface if ON-related information shall be broadcasted or not.

7. Exchange strategies

As signalling data can be exchanged using different types of channels, some overall exchange strategies which address the problem of selecting the proper channel for transmission of different signalling data could be considered. The following types of channels are available:

- Broadcast channel – logical or physical unidirectional channel which is not encrypted and is publically available to all users (connected as well as not connected). In case of WiFi (or other short range wireless technology), broadcast channel could be realized by sending data piggy-backed on beacons, and/or public management frames.
- Shared channel – logical or physical channel which is shared and available to a limited number of users (e.g. ON participants). The concept of shared channel requires that all users interested in receiving data are associated and authorized/authenticated with a network. In case of WiFi (or other short range wireless technology), shared channel could be realized by broadcasting data over a secured link that uses a common encryption key known to a limited number of users.
- Dedicated channel – logical or physical channel that permits for information exchange only between two end points. The usage of a dedicated channel requires that users are associated and authorized/authenticated with a network. For cellular networks, dedicated resources need to be allocated to the users. In case of WiFi (or other short range wireless technology), dedicated channel is realized by the exchange of unicast packets between two nodes.

Exchange strategies will determine which type of channels should be used to deliver which type of signalling data. The strategy could assume that e.g.:

- broadcast channel should be used to deliver only limited signalling data which is necessary to enable the ON Suitability determination (e.g. important policies and profiles, some limited context data),
- shared channel should be used to deliver signalling between ON participants during the ON maintenance phase (e.g. policies and context information relevant to ON participants and required to monitor ON),
- dedicated channel should be used to deliver signalling during the ON Creation and ON Termination phase (e.g. ON configuration parameters, information on the allocated/released resources).

7.1 Policy exchange strategies

As policies related to users, operators or regulators change over time, different strategies for exchange/dissemination of these policies may need to be considered. The strategies may be optimized with respect to the communication overhead, energy consumption, delay, etc. The following paragraph provides an overview of possible strategies that could be potentially employed for the exchange of information related to policies.

Assuming that users located in the same area need to follow similar policies, following methods for distribution of the policies could be considered:

- Centralized policy distribution – users request policies directly from the source of the policies (e.g. a policy server which is located in the infrastructure).
- Decentralized policy distribution – users check their local neighbourhood and (given that the neighbouring node already cached the most recent versions of policies) access the relevant

data using local connection (this method may require policies to be digitally signed in order to omit distribution of false policies by the malicious users).

A possible strategy could assume e.g. that policies are requested in the first place from the local neighbourhood (given the short-range connection is active) and in case of a failure directly from the source of the policies.

Assuming that the policy updates are related (in most cases) only to a small fraction of all available policies, some strategies related to the policy dissemination/exchange could consider different types of updating. The following methods for a policy update could be considered:

- Incremental policy update – instead of requesting the most recent set of policies, user downloads only the updates to specific policies.
- Non-incremental policy update – user requests the most recent complete set of policies.

A possible strategy could assume that the incremental policy update should be used by default. The non-incremental update would be used whenever users determine that the total number of updates which are necessary to get the most recent version of policies exceed a certain number (or size). This situation may happen in case a user 1) switches on his/her terminal for the first time, 2) switches on his/her terminal in a new location or 3) switches on his/her terminal after a long period of time.

Some strategies could also consider different methods for delivery of policies:

- Periodical policy transmission – source of the policies transmits periodically all information necessary for a user to obtain the up-to-date set of policies. Communication is not bi-directional and will allow for the reception of policy information by idle/not associated users.
- Periodical policy header transmission – source of the policies periodically transmits information which is sufficient to determine if some policy attributes have changed (e.g. policy IDs and their versions). The interested users which determine that their policies are out-of-dated (based on examination of headers) may request additional data related to specific policies (this method requires a bidirectional channel between the source of the policies and user).
- Event-Triggered policy transmission:
    - Source-initiated: policies are broadcasted by the source in case of an update,
    - User-initiated (On demand policy transmission) – exchange of the policy information is triggered by the consumer rather that the policy source. This means that the policy needs to be explicitly requested by the interested user in order to be delivered by the source e.g. upon switch-on, validity timer expiry etc.. It is worth noting that the user's request could carry information about the version of the cached policy. This would allow the source of the policy to determine if the provision of requested information is necessary.

A possible strategy could assume e.g. that: 1) most important policies should be continuously transmitted using the "periodical policy transmission", thus allowing for the delivery without any additional delay introduced by the "request-response" communication model, 2) less important policies could be delivered using the "periodical policy header transmission". Another strategy could assume that e.g. in order to decrease the overhead all policies should be delivered using the "on demand policy transmission" method (e.g. users after switching on their mobiles need to request the policies) and "triggered based policy transmission". Different possible events (besides switching on the terminal) could be potentially used to trigger the user request in case of the "on demand policy transmission". One possibility could be a policy related attribute indicating the time of the policy validity. Based on this attribute, if the policy validity expires, the policy update is requested.

7.2 Profile exchange strategies

Profiles describe system entities and may include different information ranging from device capabilities to user preferences [15]. For instance, a service/application profile could include information related to the QoS requirements of as well as the cost of the service. A device profile could include detailed device capabilities and limitations as well as current device configuration settings. As some of the properties of profiles may change over time (e.g. price of the service, configuration of the device) profiles may need to be exchanges (in some case continuously). This indicates the need for developing a set of possible strategies which could be used to optimize the process of the profile exchange.

Similar to the previous subsection, different methods for delivery of profiles could be considered. A possible strategy which considers delivery methods (see Section 7.1 for more details on delivery methods) could assume that e.g. 1) information facilitating the suitability determination are continuously transmitted using the “periodical transmission” (e.g. information related to the ON capability of devices), 2) other profile related information are exchanged explicitly using the “on-demand transmission”.

The user request in case of the “on-demand transmission” could be initiated by different events. One of the possible events could be the expiry of the profile validity. Depending on the type of the profile, different validity could be considered. Some profiles may need to be continuously exchanged during the ON operation whilst others are valid during the entire application session and thus need to be exchanged only during the ON creation.

7.3 Context information exchange strategies

The exchange of context information between different nodes allows for the implementation of different distributed as well as centralized algorithms which are responsible for suitability determination, creation and management of an ON. In order to improve the exchange of such data, limit the signalling overhead, or maintain the Quality of Context (QoC), different exchange strategies could be proposed.

Context related signalling can be delivered in a number of ways. The possible options include:

- Periodical transmission of context data – source of the context information transmits periodically context information
- Periodical transmission of context meta-data – source of the context information periodically transmits information which is sufficient to determine if some of the context data changed (the interested users may then request the source for the actual context data).
- Event-Triggered transmission of context data:
    - user-initiated (On demand transmission): context data needs to be explicitly requested by the interested user in order to be delivered by the source.
    - source-initiated: Triggered based transmission of context data – source of the context information transmits context information if some specific set of conditions is met (e.g. some threshold is exceeded).

A possible strategy which considers the above mentioned delivery mechanisms could assume e.g. that: 1) context information which is necessary for the suitability determination phase should be transmitted using the “periodical transmission” (no additional overhead introduced by the “request-response” communication model), 2) context information which is necessary during the creation phase should delivered using the “on-demand transmission” method, 3) context information necessary during the maintenance phase should be delivered using “triggered based transmission” or “periodical transmission of context meta-data” (depending on the importance of the context data).

Aggregation – aggregation of context data may effectively decrease the overhead introduced by the signalling. This is achieved by sending signalling data combined in larger packets instead of separately and thus lowering the overhead introduced by the lower layers (e.g. MAC overhead, energy overhead, call setup overhead). A possible strategy could involve aggregation of delay-tolerant signalling data during the ON maintenance phase. In such a strategy, the delay-tolerant signalling data would be transmitted only in case 1) a maximal aggregation time is exceeded, 2) aggregated information exceeds a certain size or 3) some delay-intolerant signalling is waiting to be transmitted. A possible strategy could also introduce separate queues for information addressed to different users as well as for broadcast. As the probability of the successful reception decreases with the size of the transmitted data, the strategy could determine the level of aggregation based on the link quality.

Compression/Pre-processing – compression/pre-processing of context data could be another possible way of reducing the signalling overhead. This could be achieved by reducing the volume of data to be transferred using different compression/pre-processing techniques. It is worth noting here that the context data could take advantage of more efficient (in terms of volume reduction) lossy data compression/pre-processing techniques. A possible exchange strategy which involves compression/pre-processing could alter the compression level depending on the network load and/or link quality.

Prioritization – depending on the type of context data, different Quality of Service (QoS) may be required (e.g. some context data may become out-of-dated in a short period of time). This allows context data to be subdivided into several classes. Based on this classification, an exchange strategy which introduces prioritization of QoS classes could be proposed (the exchange strategies in this case could be seen as the queuing strategies).

7.4 Decision exchange strategies

The exchange of signalling data carrying the outcome (i.e. decisions) of different algorithms responsible for suitability determination, creation and management on ONs is an important aspect of OneFIT system that enables cooperation and collaboration between different nodes. In order to ensure timely exchange of such data and at the same time limit the associated signalling overheads, different exchange strategies could be proposed.

Depending on the type of the algorithm, signalling may be assigned to different classes. A potential strategy could subdivide the signalling into two classes. The first class would comprise all the signalling data which is critical for the operation of an ON (e.g. signalling related to the emergency handover of the gateway functionality). The second class could comprise signalling which could be delayed (e.g. signalling related to optimization of ON operation). The strategy could assume a simple prioritization of one signalling class over the other.

As signalling of decisions is an important aspect of the OneFIT system, in order to provide a higher reliability, transmission of multiple copies of the same data (i.e. redundant transmission) could be considered. The method is applicable in case no lower layer acknowledgement mechanism is used (e.g. in case one broadcasts information to multiple users at once). A possible exchange strategy could involve the alteration of the “redundancy level” based on the interference levels. Such a strategy would be especially useful in case of uncoordinated short range wireless networks such as WiFi which are characterized by a high probability of collision between users.

8. Security aspects

Vision proposed by OneFIT project aims at delivering Opportunistic Networks managed and coordinated by infrastructure. As already mentioned in [1], operation of such networks needs to be conducted in a secured fashion to guarantee confidentiality and integrity of user and signaling (C4MS) data.

The following requirements, identified in [1], have impacts on the C4MS security:

- Requirement S1: Security of communication - to establish a trust relationship between the various parts of the opportunistic network by binding authentication between 1) terminals in ON, 2) authentication between RN and core network , 3) and authentication between terminal and Infrastructure via RN.
- Requirement S2: Accountability, charging and billing – to enable charging of user connected to network or rewarding RN for forwarding users' content.
- Requirement S3[7]: Protection of user identity – by using of aliases and/or temporary identities
- Requirement S4[7]: Protection of device identity – by using of aliases and/or temporary identities
- Requirement S6: Protection of private data while traversing the network – to check integrity of C4MS messages exchanged between nodes within ON as well as between user and network, and RN and network

Following section describes potential threats which emerged from the introduction of the operator governed Opportunistic Network. Additionally it briefly reviews proposed solutions for providing the necessary security mechanisms, currently under investigation in the OneFIT project[8].

8.1 System threats

The following subsection aims at identifying system threats which emerged from the introduction of the concept of operator governed Opportunistic Network. Before evaluating system threats the following assumptions are made, based on the feasibility study on the LTE relay node security [41]:

- Each ON capable node is employed with a removable UICC (Universal Integrated Circuit Card) enabling authentication between itself and the network (UICC stores user's credentials that are shared only among user and Home Subscriber Server on the infrastructure side).
- Users credentials stored in the UICC are not exchanged in unencrypted forms (only key materials created during authentication may be transmitted).
- Connection between relaying/gateway node and infrastructure network is assumed to be secured.
- Network elements (e.g. Base Stations) which are a part of operator's infrastructure are assumed to be secure and may not be compromised by potential attacker.
- Connections between network elements which are a part of operator's infrastructure are assumed to be secure.

Taking into account the above mentioned assumptions the following threats were identified:

[7] Requirements S3 and S4 are not considered in this section, as solutions have not yet been investigated.

[8] Network Domain Security, that is protection of communication between network elements on the infrastructure side, is out of scope of this document.

Man in the Middle:

Relaying/Gateway Nodes may inspect, alter, or inject traffic originated from or destined to the Client Node without the knowledge of the Client Node and the Infrastructure. Depending on the situation, user or control (C4MS) traffic may be affected resulting in the free IP connectivity.

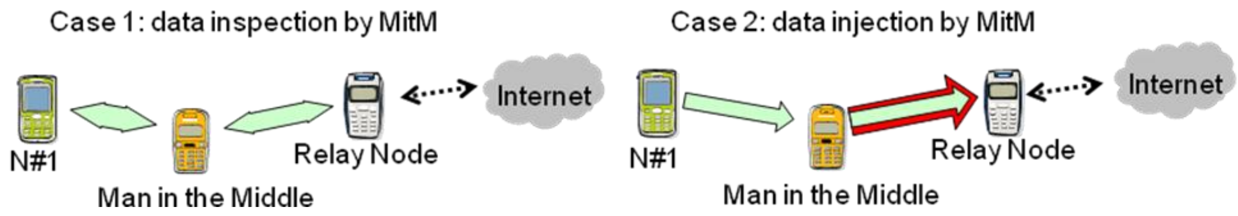


Figure 55: Scenarios with data inspection or alteration conducted by MitM; entities on the access network as well as core network have been omitted for clarity

Impersonation of other nodes:

Nodes pretend to be other nodes in order to alter or inject traffic originated from or destined to the Client or Relaying/Gateway Node without the knowledge of the parties participating in the information exchange. Depending on the situation, user or control (C4MS) traffic may be affected and may result in the initiation of different disruptive ON procedures (e.g. release of ON with an ongoing application, forcing disconnection of ON participants).

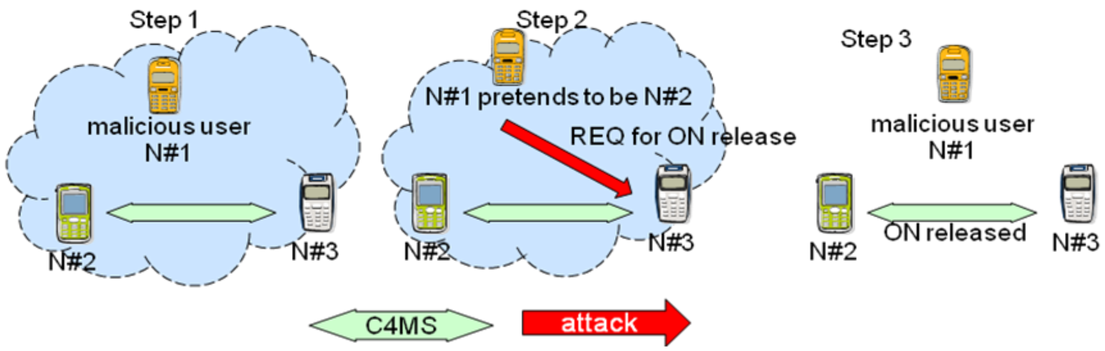


Figure 56: N#1 masquerades as N#2 and forces N#3 to release ON

User misbehaviour:

Two distinct cases of user misbehaviour can be distinguished: maliciously behaviour, and selfish behaviour (may happen in case a node is compromised).

In the first case nodes aim at deteriorating performance of other nodes. Such actions may involve saturation of C4MS by injecting a large number of C4MS messages to disturb signaling or sending false C4MS data (e.g. false spectrum avialability information) which may initate different unnecessary and disruptive ON management procedures (e.g. unnecessary reconfigurations or releases of ONs).

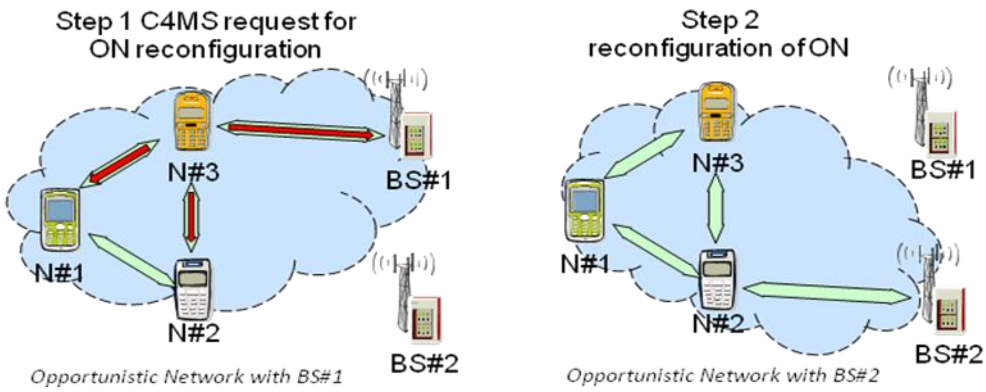

Step 1 C4MS request for ON reconfiguration
N#3
BS#1
N#1
N#2
BS#2
Opportunistic Network with BS#1
Step 2 reconfiguration of ON
N#3
BS#1
N#1
N#2
BS#2
Opportunistic Network with BS#2

Figure 57: ON participant send bogus request for reconfiguration (e.g. due to poor link quality condition to BS#1) thus force the ON reconfiguration

In the second case nodes aim at increasing their own performance by sending false C4MS context data. False context information could result in allocation of additional resources to selfish nodes (e.g. to achieve higher throughput) or prevent them from being elected as relays/gateways for other nodes towards the infrastructure (e.g. to preserve battery power).

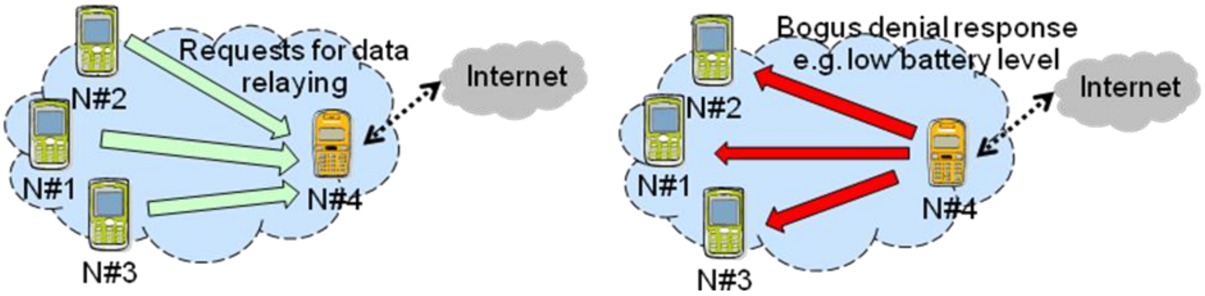

Requests for data relaying
Internet
N#2
N#1
N#4
N#3
Bogus denial response e.g. low battery level
Internet
N#2
N#1
N#4
N#3

Figure 58: ON participants request for relaying data to core/internet, while potential Relaying Node (N#4) denials to become a relay due to bogus response (e.g. low battery level); entities on the access network as well as core network have been omitted for clarity

8.2 Solution for C4MS

The principle for designing C4MS security is to ensure easy integration in the legacy 3GPP security framework for e-UTRAN/EPC, i.e. the latest generation of cellular networks. This implies to re-use as much as possible of key management principles (key hierarchy, key separation, key derivation and key provision) and authentication procedures. To be consistent with the fact that the ON is considered as an extension of the operator's network, the same level of security for C4MS as the one provided by the native 3GPP network should be granted. Security mechanisms of 3GPP and IEEE were briefly described in Appendix III of this document (Section 13).

As identified in D3.1 [3], the C4MS signalling could use various path and protocols, and may be transported between various elements of the network: UE, RAN element (e.g. eNB, DeNB, HeNB), EPC element (e.g. SGW, PGW, MME, HSS). Data integrity and confidentiality needs to be provided not only between end-to-end devices but also between devices residing in the path.

In order to address the indentified threats and comply with the identified requirements as well as the 3GPP security framework C4MS must protect integrity and confidentiality between end to end ON communicating entities. Due to the confidentiality, the entities on the path of the communication should not be able to access to the content of the message.

Generally three planes need to be protected: 1) legacy 3GPP C-plane, possibly with some ON-specific extensions, 2) additional ON-specific C-plane, e.g. over IP and 3) User plane. Additionally two new configurations introduced for ON need to be protected: 1) UE relay, 2) UE-to-UE direct communication

Moreover, before any data is exchanged between UE and the UE relay, or between UEs in ON, nodes needs to be mutually authenticated and bilaterally trusted. It needs to be noted that in real-world application UE relay would also need to be assured that by forwarding data from UE, the UE relay will be gratified[9]. On the other hand UE that is connected to core network via relay needs to be sure that relay will not be able to use UE's credentials for own purposes. e.g. IP connectivity and will not be charged for such services.

In following subsections some scenarios and use cases were identified with specification of requirements and respective solutions under investigation.

8.2.1 Mutual authentication of UEs

This use case is applicable to all scenarios and should precede any communication between nodes in ON and infrastructure.

Use case

UE#1 wishes to be given access to core network via UE relay node, i.e. UE#2.

UE#1 wishes to exchange data directly with UE#2

Detailed requirements

UE#1 c-plane and u-plane goes through UE#2 to reach eNB.

There is no direct UE#1-UE#2 u-plane.

Solution under investigation

Both UE#1 and UE#2 are needed to be authenticated by network. Such procedure may be based on 3GPP security mechanisms for both 3GPP and non-3GPP access (e.g. EAP-AKA or EAP-AKA').

Informing relaying UE about the successful authentication of UE requesting for access to core network would ensure relaying UE that UE's identity is legitimate. On the other hand, from the requesting UE's point of view, successful authentication from network would ensure that relaying UE is legitimate. In case the relaying UE had no connection to network it would not be able to provide genuine responses from the authentication server.

8.2.2 Securing direct UE-to-UE communication

This use case is applicable to all scenarios except "social network".

Use case

UE#1 and UE#2 share u-plane (application stream) while C-plane goes through UE#2 to reach eNB.

Detailed requirements

UE#1 and UE#2 must be certain of each other identity before exchanging user data.

Shared u-plane must be confidentiality protected.

Keys must be different for each UE pair.

Solutions under investigation

[9] Method used for gratification is not yet developed.

An extension of key derivation used in 3GPP scheme may be also used for WPA keys delivery from Infrastructure thus providing secure unicast and broadcast communication (as presented in Figure 63).

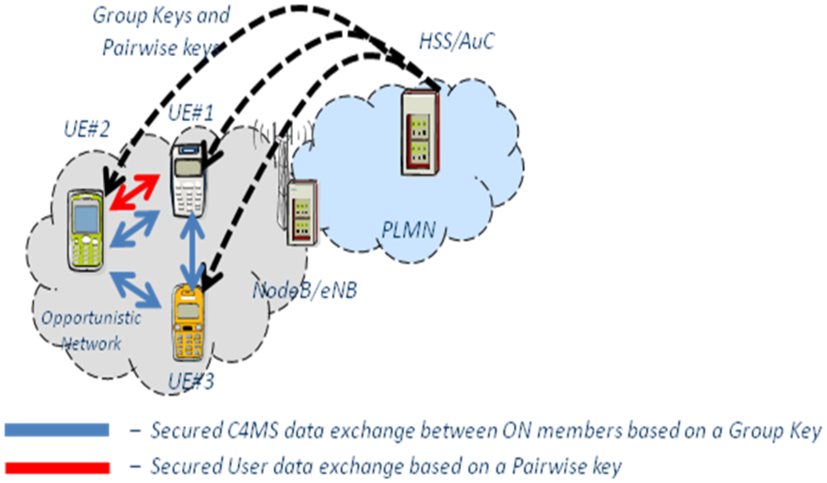

Group Keys and
Pairwise keys
HSS/AuC
UE#2
UE#1
PLMN
NodeB/eNB
Opportunistic
Network
UE#3
– Secured C4MS data exchange between ON members based on a Group Key
– Secured User data exchange based on a Pairwise key

Figure 59: Pairwise and Group key utilization in ON goverened by infrastructure where pairwise and group keys are distributed via 3GPP mechanisms

The first option applies when only point-to-point security is required (e.g. VoIP communication, dedicated C4MS signalling). In this case, mutual authentication is not required as provision/derivation of keys ensure that the users have been authenticated by the network. An additional pair of keys, one for integrity, one for confidentiality, is derived in each UE's USIM card for protecting the shared u-plane. Network's AuC provides over the secured UE-network links a UE-UE link identifier to ensure the derived keys are unique across the network's ON users. Or a UE-UE link identifier is computed by each UE based on an operator's policy or algorithm stored in the USIM card.

The second option applies when multicast/broadcast communication must be secured (e.g. network gaming, C4MS signalling). In this case, WLAN security (based on pairwise or group keys) should be used: further investigation is required to ensure feasibility and level of security.

8.2.3 Securing UE-network link across UE-relay

Although IEEE security mechanisms (e.g. pairwise keys) may be used to provide user data and signalling integrity and confidentiality between UE and relaying node, additional tunnelling (as presented in Figure 60) needs to be provided for data security between UE and closest serving Base Station. This use case is applicable to all scenarios except "social network".

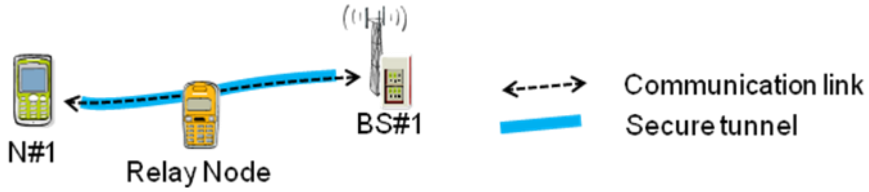


Figure 60: Due to secure tunnel Relaying Node cannot alter, inject, inspect or listen to traffic exchanged between Client and Base Station

Use case

UE#1 c-plane and u-plane goes through UE#2 to reach eNB.

No direct UE#1-UE#2 u-plane.

Detailed requirements

UE#1 <> Network c-plane and u-plane must remain integrity and confidentiality protected.

If UE#2 is attached to a different eNB than UE#1, change of keys must be performed as per a normal HO.

Solution under investigation

Two possible ways of data relaying/forwarding were investigated for proper inter-operation between ON and core network: 1) higher layer approach based on existing solutions for interworking between 3GPP and non-3GPP access networks (Figure 62, top and middle) and 2) lower layer approach based on 3GPP C-Plane and U-Plane traffic encapsulation (Figure 62, bottom).

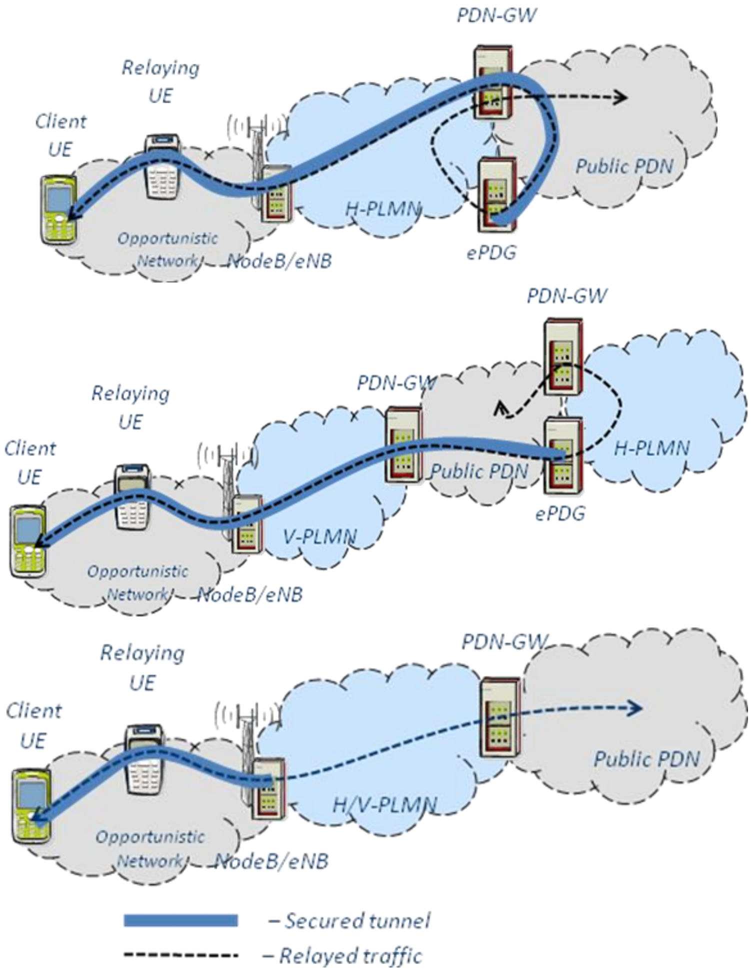


Figure 61: Approaches for data forwarding: topmost and middle – high layer approach for non-3GPP access in non-roaming and roaming scenario respectively; the lowest – lower level approach

Both investigated approaches imply some pros and cons. One of the pros of the high level approach is that it enables the reuse of existing solutions for providing the user plane security. The solution is based on EAP-AKA and IKEv2 protocols as well as IPsec tunnelling. However, as can be seen in Figure 62, the reuse of the existing solutions introduces high signalling overhead (IPsec tunnel is always setup between an end-user and ePDG). Additionally, the higher layer approach fails to provide the secured control (C4MS) plane connection. The lower layer approach on the other hand may benefit from the low signalling overhead (secured tunnel between an end-user and a base station), but requires significant specification effort to enable such relaying scheme and provide necessary security.

A potential solution to provide security for the lower layer approach could be based on the PDCP tunnelling[10] which is used to carry u-plane between UE#1 and eNB (in case of EPC). LTE "backward" (where one-way function is used before key is passed) and "forward" (MME is involved after the HO for further key passes) security schemes may be also applied for changes of keys when change of eNB. Moreover when change of eNB is needed fast-reauthentication mechanism may be used to improve time needed for U- and C-plane establishment.

8.3 Conclusions on the security aspects

Security provisioning is inevitable to provide comprehensive solution for opportunistic network creation and operation in real-world applications. Solutions for securing over-the-air C4MS and legacy c-plane in new ON configuration are under evaluation: they should require some limited extension of the existing 3GPP standards and probably use of WLAN security framework as well. Solution not integrated in 3GPP or IEEE security frameworks may also be evaluated in terms of applicability to C4MS however already standardized mechanisms are more likeable to be adopted to C4MS due to operators trust and reliability. Results presented above are just preliminaries for comprehensive C4MS security framework that should be evaluated in following research activities.

[10] specified in TS 36.323 [12]

9. Conclusions

This deliverable has provided an insight on the information exchange in OneFIT system using “Control Channels for the Cooperation of Cognitive Management Systems” (C4MS). The information to be exchanged may be related e.g. to policies, resources, node capabilities, available spectrum bands or managing opportunistic networks. The deliverable introduced the concepts of policy management and context awareness. Mapping of these concepts to the OneFIT architecture was explained. Additionally, interactions between the OneFIT policy management and the policy management of the external systems were described.

The deliverable provided an update of the information to be exchanged in OneFIT system as well as the model used for delivering this information over C4MS. In deliverable D3.1 [3], the preliminary set of information to be exchanged was introduced. Since the work on the algorithms for the OneFIT system has progressed, in this deliverable it was possible to limit the preliminary set of information to the subset which is actually required by various algorithms. The remaining issue related to classification of the identified information based on different ON phases will be covered in the next stage of work on C4MS and algorithms evaluation.

An initial proposal for the elementary ON management procedures and messages to be supported over C4MS was introduced. This work serves as ground for further development which will be described in the upcoming work as well as for future and ongoing standardization activities. The message sequence charts for all five OneFIT scenarios were originally presented in D2.2 [2]. In this deliverable, the message sequence charts were described in more detail. Especially, subdivision of each scenario to four phases was made: i.e. 1) suitability determination phase, 2) creation phase, 3) maintenance phase and 4) termination phase. Based on the provided MSCs, it can be seen that the OneFIT consortium focuses on two solutions for implementation of the OneFIT platform: terminal centric and network/infrastructure centric. In case of the terminal centric solution (e.g. SCE#3) the involvement of the infrastructure is limited to a bare minimum (e.g. allocating resources, initiating suitability determination), moving most of the burden related to the ON creation and management (i.e. decision making, signalling) to the terminal side. In case of the network/infrastructure centric solution (e.g. SCE#2) the burden is more on the infrastructure side, allowing infrastructure to participate more actively in ON related procedures (e.g. relaying C4MS messages between users, determining ON configuration).

In order to further elaborate on the changes that happen in the internal state of nodes participating in the ON as well as on the state of the links, preliminary state machine for OneFIT system was introduced. The state machine specifies ON-Link-States and ON-Node-States with corresponding action required to switch between different states. Future work may address necessity for further elaboration on state machines, but it is not yet specified if such effort will be needed.

Additionally, initial views on the information exchange strategies were described. Different strategies were identified for exchanging policies, context information, profiles and decisions. The work on exchange strategies together with definition of data structure will form a basis for the development and evaluation of C4MS. Moreover, the document addresses also basic aspects related to the security of ON operation and C4MS data exchange. Some potential threats were listed and briefly discussed. The proposals of solutions, based on the existing security framework, that may be adopted to OneFIT platform security were also presented. It needs to be noticed however, that security solution for C4MS is in preliminary phase and significant effort needs to be provided in order to address this matter thoroughly.

10. References

[1] OneFIT Deliverable D2.1 "Business scenarios, technical challenges and system requirements", October 2010.

[2] OneFIT Deliverable D2.2 "OneFIT functional and system architecture", February 2011.

[3] OneFIT Deliverable D3.1 "Proposal of C4MS and inherent technical challenges", March 2011.

[4] OneFIT Deliverable D4.1 "Formulation, implementation considerations, and first performance evaluation of algorithmic solutions", May 2011.

[5] 3GPP TS 23.107 v 10.1.0 "Quality of Service (QoS) concept and Architecture", June 2011.

[6] 3GPP TS 23.203 v 11.2.0 "Policy and Charging Control Architecture", June 2011.

[7] 3GPP TS 24.312 v 10.3.0 "Access Network Discovery and Selection Function (ANDSF) Management Object (MO)", June 2011.

[8] 3GPP TS 23.402 v 10.4.0 "3GPP System Architecture Evolution", June 2011.

[9] IEEE Std 802.11 Part 11 "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", June 2007.

[10]IEEE 802.11u Part 11 Amendment 9 "Interworking with external networks", February 2011.

[11]IETF RFC 2246 "The TLS Protocol Version 1.0", January 1999.

[12]IETF RFC 2401 "Security Architecture for the Internet Protocol", November 1998.

[13]IETF RFC 3588 "Diameter Base Protocol", September 2003.

[14]IEEE Std 802.21TM-2008, "IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services.", IEEE Computer Society, Sponsored by the LAN/MAN Standards Committee, January 2009.

[15]Z. Boufidis, N. Alonistioti, M. Stamatelatos, J. Vogler, U. Lucking, C. Kloeck, "End-to-End Architecture for Adaptive Communication Systems", *Vehicular Technology Conference*, September 2006.

[16]J. Strassner, T. Pfeifer, S. Van Der Meer, "An architecture for using metadata to manage ubiquitous communications and services: A position paper", in *IEEE International Conference on Pervasive Computing and Communications Workshops*, March 2010.

[17]X. Gu, T. Klie, L. Wolf, "A Proactive Policy-Based Management Approach Towards Autonomic Communications", in *IEEE Consumer Communications And Networking Conference*, January 2007.

[18]J. Strassner, "Policy-based network management: solutions for the next generation", (The Morgan Kaufmann Series in Networking), Morgan Kaufmann, September 2003.

[19]IETF Policy Framework Working Group charter, http://datatracker.ietf.org/wg/policy/charter/, accessed 2011.

[20]IEEE Std 1900.4™-2009, IEEE Standard for Architectural Building Blocks Enabling Network-Device Distributed Decision Making for Optimized Radio Resource Usage in Heterogeneous Wireless Access Networks, January 2009.

[21]S.Buljore, H.Harada, P.Houze, K.Tsagkaris, O.Holland, S.Filin, T.Farnham, K.Nolte, V.Ivanov, "Architecture and Enablers for Optimised Radio Resource usage: The IEEE P1900.4 Working Group" Communications Magazine, IEEE, Vol 47, no. 1, pp. 122-129, January 2009.

[22]Project "End-to-End Reconfigurability" (E2R), http://e2r2.motlabs.com, 6th Framework Programme (FP6) of the European Commission, Information Society Technologies (IST), 2007.

[23]Project End-to-End Efficiency (E3), www.ict-e3.eu, 7th Framework Programme (FP7) of the European Commission, Information and Communication Technologies (ICT), 2009.

[24]V. Stavroulaki, N. Koutsouris, K. Tsagkaris, P. Demestichas, "A Platform for the Integration and Management of Cognitive Systems in Future Networks", in *IEEE International Workshop on Management of Emerging Networks and Services*, December 2010.

[25]ORACLE Deliverable D4.1 "Draft OR Policy Framework", www.ict-oracle.eu.

[26]E3 Deliverable D2.3 "Architecture, Information Model and Reference Points, Assessment Framework, Platform Independent Programmable Interfaces", September 2009, www.ict-e3.eu.

[27]E3 Deliverable D4.5 "Final system specification for autonomous CR functions", December 2009, www.ict-e3.eu.

[28]QoSMOS Deliverable D2.1"Initial description of system architecture options for the QoSMOS system", April 2010, www.ict-qosmos.eu.

[29]QoSMOS Deliverable D6.1"Initial description of spectrum management framework, requirements analysis and approach selected", June 2010, www.ict-qosmos.eu.

[30]C2Power Deliverable D3.1 "Identification of context parameters", October 2010, www.ict-c2power.eu.

[31]WORKPAD Deliverable D1.3, "Requirements and Conceptual Framework", v2.0 March 2008, www.workpad-project.eu.

[32]ARAGORN Project, www.ict-aragorn.eu.

[33]PERSIST Project, www.ict-persist.eu.

[34]C-CAST Deliverable D6" Requirements and concepts for context casting service enablers and context management", November 2008, www.ict-ccast.eu.

[35]SENSEI Project, www.ict-sensei.eu.

[36]O. Riva and S. Toivonen. The DYNAMOS Approach to Support Context-aware Service Provisioning in Mobile Environments. *The Journal of Systems and Software*, February 2007.

[37]S. Fallis, J. Horton and W. Tuttlebee "Removing the Barriers to Ubiquitous Services", Final Overview Report, MobileVCE Core 4 Research Programme: Ubiquitous Services, December 2009.

[38]S. De and K. Moessner "Integration of PAA device-service context description with Adaptation Management Framework," Deliverable D-U3.8, MobileVCE Core 4 Research Programme: Ubiquitous Services, July 2009.

[39]ETSI TR 102 682 v1.1.1 "Reconfigurable Radio Systems (RRS); Functional Architecture (FA) for the Management and Control of Reconfigurable Radio Systems", July 2009.

[40]3GPP TS 33 401,"3GPP System Architecture Evolution (SAE); Security architecture", V10.1.1, June 2011

[41]3GPP TR 33.816, "Feasibility study on LTE relay node security", V10.0.0, March 2011

[42]3GPP TS 33.402, "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses", V10.0.0, December 2010

[43]IETF RFC 4186, “Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)”, January 2006

[44]3GPP TS 33.102, “3G security; Security architecture”, V10.0.0, December 2010

[45]IETF RFC 4187, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”, January 2006

[46]IETF RFC 5448, “Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')”, May 2009

[47]IETF RFC 5996, “Internet Key Exchange Protocol Version 2 (IKEv2)”, September 2010

11. Appendix I: Policy control in standardisation

11.1 Policy control in 3GPP

11.1.1 3GPP policy and charging control

3GPP has defined a Policy and Charging Control Architecture in TS 23.203 [6].These policy and charging control functions are used for

- Flow Based Charging, including charging control and online credit control;
- Policy control (e.g. gating control, QoS control, QoS signalling, etc.).

The main elements are the Policy and Charging Rules Function (PCRF) providing the rules which are then enforced by the Policy and Charging Enforcement Function located in the Public Date Network Gateway (PDN GW) as shown in Figure 62. The more detailed Policy and Charging Control (PCC) Architecture is shown in Figure 63.

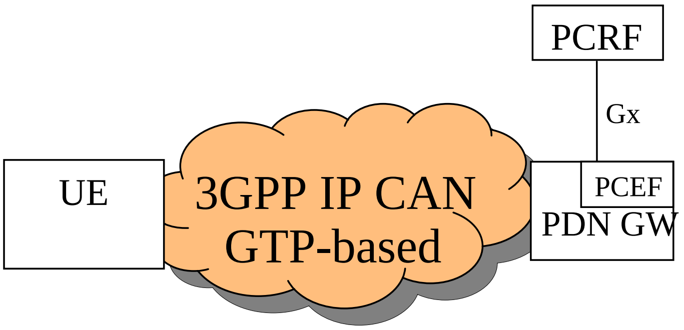


Figure 62: The 3GPP EPS IP-CAN (GTP-based) [6]

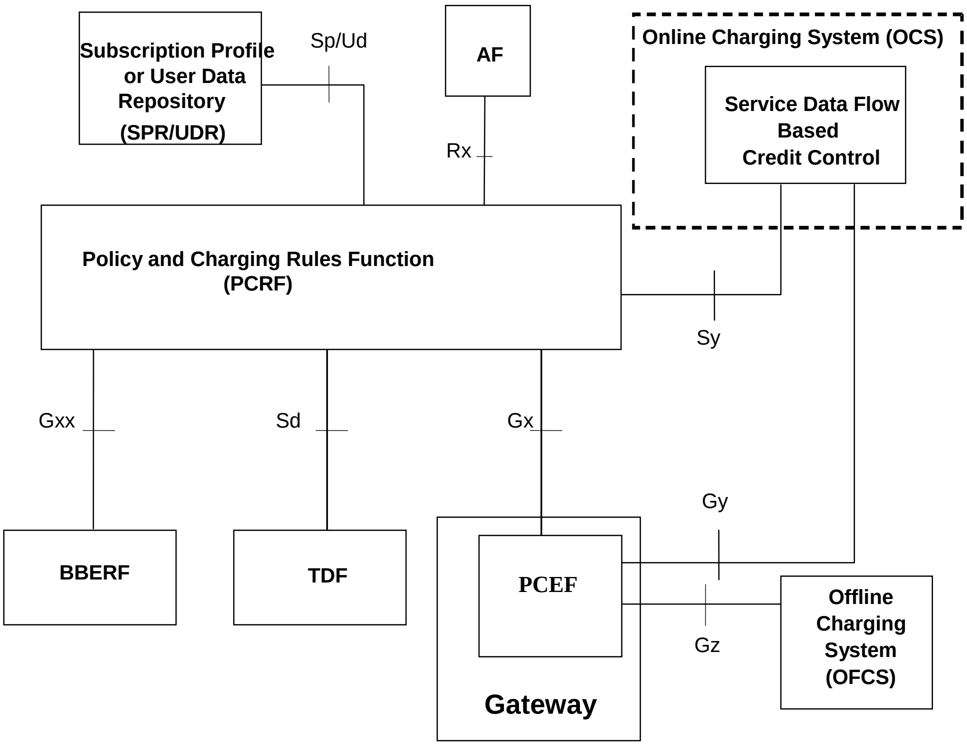

Subscription Profile or User Data Repository (SPR/UDR)
Sp/Ud
AF
Rx
Online Charging System (OCS)
Service Data Flow Based Credit Control
Policy and Charging Rules Function (PCRF)
Sy
Gxx
Sd
Gx
Gy
BBERF
TDF
PCEF
Gateway
Gz
Offline Charging System (OFCS)

Figure 63: 3GPP overall PCC logical architecture (non-roaming) [6]

11.1.2 3GPP Access Network Discovery and Selection Function (ANDSF)

The 3GPP Access Network Discovery and Selection Function (ANDSF) [7] is an entity in the Evolved Packet Core (EPC) of the System Architecture Evolution (SAE) [8], which is responsible for the connectivity of the terminals to trusted networks including 3GPP (e.g. LTE, UMTS) and non-3GPP access networks (e.g. WiMax) and untrusted ones (e.g. WiFi). The main role of the ANDSF is to give information to the terminals about the status of these networks and provide intersystem mobility policies as well as inter-operator mobility policies. An example of the ANDSF Management Object (MO) is given in Figure 64 and Figure 65.

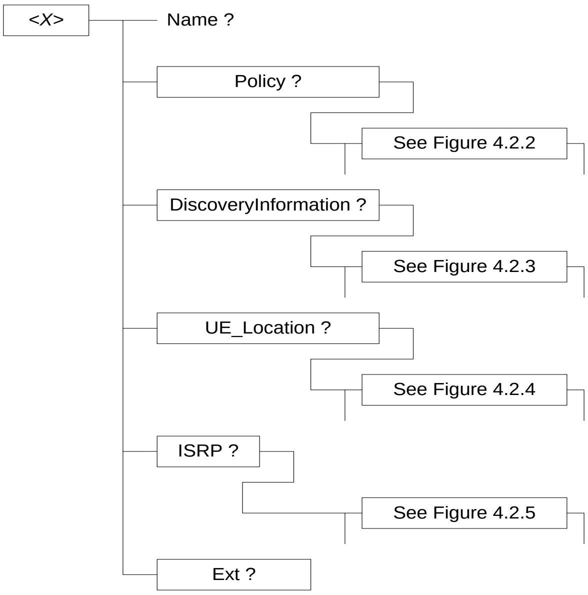


Figure 64: The ANDSF MO (Part 1: General structure) [7]

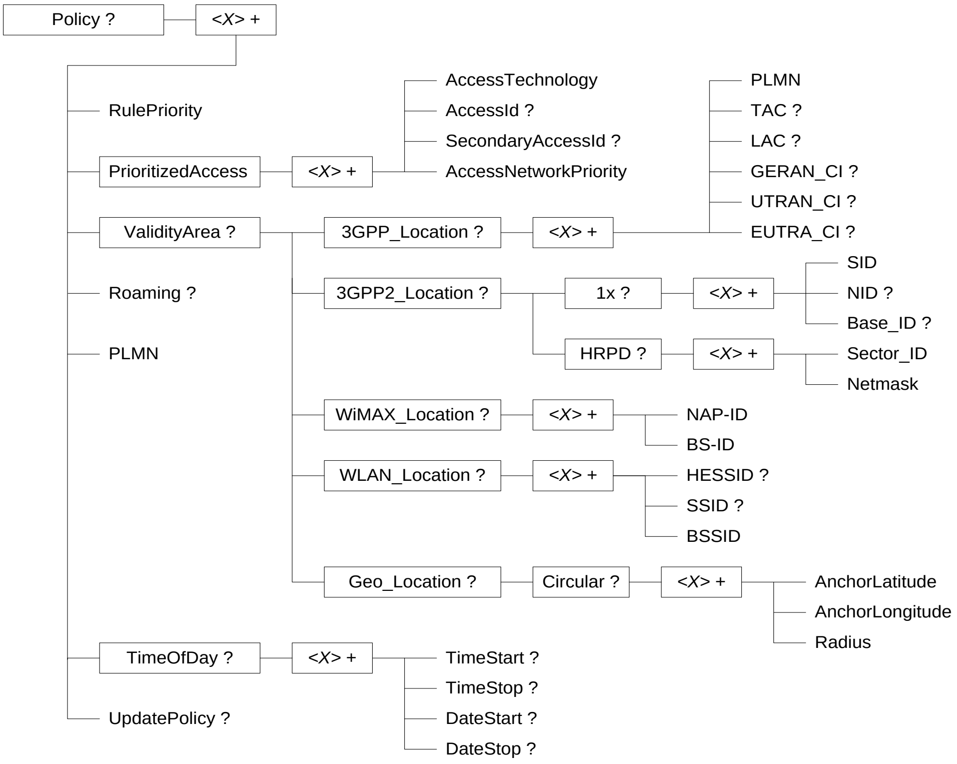


Figure 65: The ANDSF MO (Part 2: Policies) [7]

12. Appendix II: "Context-awareness" in IEEE 1900.4 & ETSI RRS

12.1 IEEE 1900.4

IEEE1900.4 standard aims to improve overall composite capacity and quality of service of wireless systems in a multiple radio access technologies environment, by defining an appropriate system architecture and protocols which will facilitate the optimization of radio resource usage, in particular, by exploiting information exchanged between network and mobile terminals, whether or not they support multiple simultaneous links and dynamic spectrum access. This is achieved by defining building blocks comprising:

- network resource managers,
- device resource managers, and
- information to be exchanged between the building blocks

thus enabling coordinated network-device distributed decision making which will aid in the optimization of radio resource usage, including spectrum access control, in heterogeneous wireless access networks. In principle, 1900.4:

- supports decision making based on policy-based management framework.
- specifies architecture and information model to enable policy-based management.
- enables to describe policies of type Event-Condition-Action
- supports radio resource selection policies create the framework to enable terminals taking reconfiguration decisions

A composite wireless network, managed by one or several operators in which P1900.4 system can operate, assumes that devices (access points and end user terminals) operating in such an environment (network comprised of several radio access networks: RANs) have multi-mode capability with advanced features, such as support for simultaneous links on different radio access technologies and corresponding spectrum bands/channels.

Three use cases are defined within IEEE P1900.4:

- *Dynamic spectrum assignment:* Frequency bands are dynamically assigned to the RANs among the participating networks in order to optimize spectrum usage. In other words, the assigned frequency bands are not fixed, and can be dynamically changed.
- *Dynamic spectrum sharing:* Frequency bands assigned to RANs are fixed. However, a particular frequency band can be shared by several RANs. In other words, the dynamic spectrum sharing use case describes how fixed frequency bands are shared and/or used dynamically by RANs and Terminals. Dynamic spectrum sharing use case includes primary/secondary spectrum usage as a special case. Figure 4 demonstrates this use case.
- *Distributed radio resource usage optimization:* Covers the process and mechanisms by which the optimization of radio resource usage is performed by the CWN and terminals in a distributed manner (Figure 5). Frequency bands assigned to RANs are fixed. Reconfiguration of RANs is not involved in this use case.

Based on the use cases above, system requirements and the corresponding system architecture are derived.

12.1.1 System requirements

The advanced spectrum management considered in IEEE 1900.4 assumes that reconfiguration of some parts of the CWN is possible (e.g., base stations and terminals). Reconfiguration usually involves three phases: obtaining the context information required for decision making, making reconfiguration decisions, and the actual reconfiguration according to the decisions made. These three categories are used to classify the system requirements of 1900.4.

Context Awareness: The standard states that there shall be entities on the network side and terminal side responsible for context information collection. Two types of context information are defined: RAN context information and terminal context information.

RAN context information may include:

- RAN radio resource optimization objectives
- RAN radio capabilities
- RAN measurements
- RAN transport capabilities.

The NRM shall be able to obtain RAN context information from context information collection entity on network side. The NRM may receive this context information periodically and/or in response to request from the NRM and/or on event. Context information collection entity on network side may be implemented in a distributed manner. Context information collection entity on terminal side shall collect terminal context information.

Terminal context information may include:

- User preferences
- Required QoS levels
- Terminal capabilities
- Terminal measurements
- Terminal geo-location information
- Geo-location-based terminal measurements.

The TRM shall be able to obtain terminal context information from context information collection entity on terminal side. The NRM and the TRM shall exchange context information. The NRM shall send RAN context information to the TRM. The NRM may send to the TRM's terminal context information related to other Terminals. The NRM may send this context information to the TRM periodically and/or in response to request from the NRM and/or on event. The TRM shall send terminal context information related to its Terminal to the NRM. The TRM may send this context information to the NRM periodically and/or in response to request from the NRM and/or on event.

Decision Making: According to the standard, there is an entity on the network side, the NRM, which is responsible for managing the CWN and terminals to achieve network terminal distributed optimization of spectrum usage. There is also an entity on the terminal side, the TRM, responsible for managing the terminal for network-terminal distributed optimization of spectrum usage. The TRM manages the terminal within the framework defined by the NRM, and in a manner consistent with user preferences and available context information.

Distributed decision making in 1900.4 is based on a policy-based management framework. Two types of policies are defined: spectrum assignment policies and radio resource selection policies. Spectrum assignment policies are based on regulations and express operator objectives related to dynamic spectrum assignment. These policies are generated by another entity on the network side and transmitted from this entity to the NRM. Radio resource selection policies guide terminals in their reconfiguration decisions, and are generated by the NRM and transmitted from the NRM to TRMs in terminals. Spectrum assignment policies are mandatory for the NRM, while radio resource selection policies are mandatory for the TRMs.

12.1.2 Functional architecture

The functional architecture defined in the IEEE 1900 standard is shown in Figure 60 below. The functionalities of the OSM, RMC, RRC, TMC, and TRC are well defined in 1900.4. However, as the NRM and TRM are the key decision making entities in the standard, this section focuses on the functionalities associated with these two important entities.

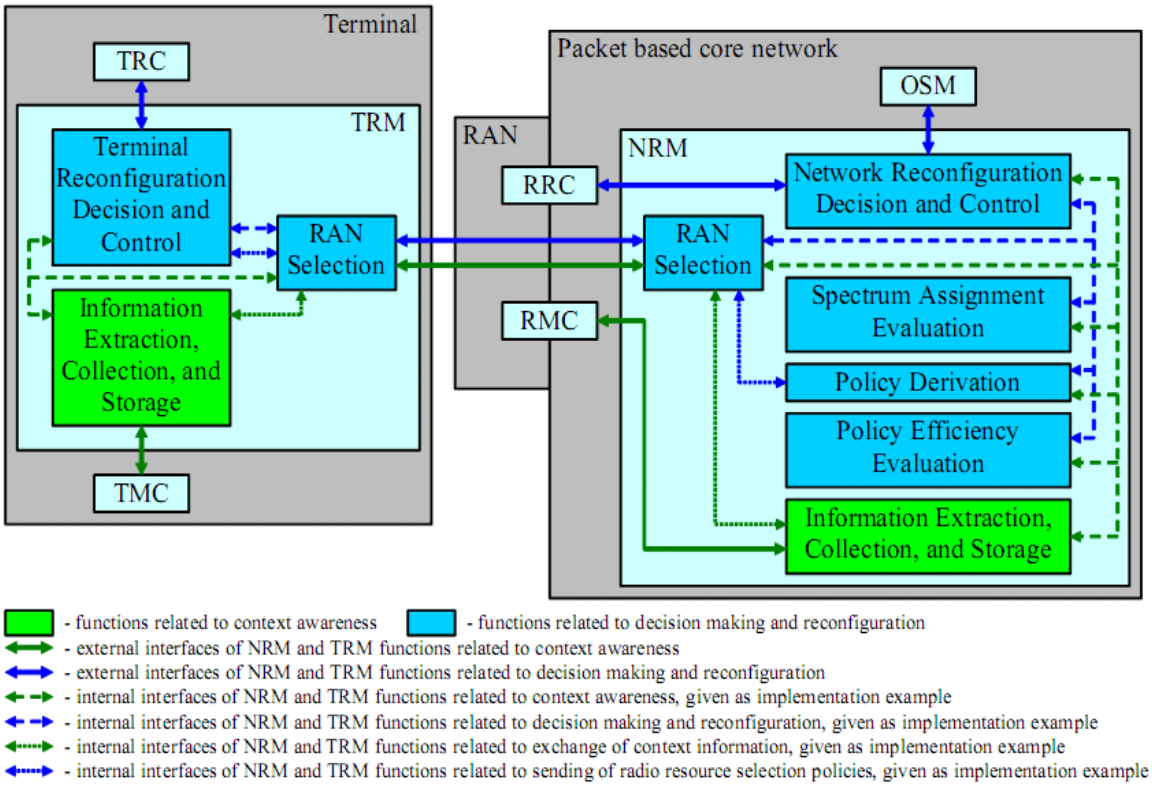

Terminal
TRC
TRM
Terminal Reconfiguration Decision and Control
RAN Selection
Information Extraction, Collection, and Storage
TMC
RAN
RRC
RMC
Packet based core network
OSM
NRM
Network Reconfiguration Decision and Control
RAN Selection
Spectrum Assignment Evaluation
Policy Derivation
Policy Efficiency Evaluation
Information Extraction, Collection, and Storage
- functions related to context awareness
- functions related to decision making and reconfiguration
- external interfaces of NRM and TRM functions related to context awareness
- external interfaces of NRM and TRM functions related to decision making and reconfiguration
- internal interfaces of NRM and TRM functions related to context awareness, given as implementation example
- internal interfaces of NRM and TRM functions related to decision making and reconfiguration, given as implementation example
- internal interfaces of NRM and TRM functions related to exchange of context information, given as implementation example
- internal interfaces of NRM and TRM functions related to sending of radio resource selection policies, given as implementation example

Figure 66: IEEE 1900.4 Functional Architecture

The standard defines six functions inside NRM:

- Policy Derivation
- Policy Efficiency Evaluation
- Network Reconfiguration Decision and Control
- Spectrum Assignment Evaluation
- Information Extraction, Collection, and Storage
- RAN Selection

Policy Derivation function generates radio resource selection policies that guide TRMs in Terminals reconfiguration decisions. The policy derivation function generates radio resource selection policies that guide TRMs in terminals’ reconfiguration decisions. The radio resource selection policies are derived using the context information from the information extraction, collection, and storage function.

The policy efficiency evaluation function evaluates the efficiency of current radio resource selection policies. Evaluation results are used by the policy derivation function in generating radio resource selection policies. The network reconfiguration decision and control function makes decisions on RANs reconfiguration compliant with spectrum assignment policies received from OSM. After making these decisions, this function sends corresponding reconfiguration commands to RRC. Also, this function sends information on made decisions to OSM. The spectrum assignment evaluation function evaluates the efficiency of spectrum usage under the current spectrum assignment. Evaluation results are used by the network reconfiguration decision and control function in making decisions on RAN reconfiguration.

The NRM information extraction, collection, and storage function receives, processes, and stores RAN context information and terminal context information. RAN context information is received from the RMC, while terminal context information is received from the TRM. The NRM information extraction, collection, and storage function provides information to functions inside the NRM. It forwards RAN context information to the TRM and may forward terminal context information, related to other terminals, to the TRM. The NRM RAN selection function selects RANs for exchanging radio resource selection policies and context information between the NRM and TRM. This is done to minimize signalling overhead, and ensure timely and reliable delivery of radio resource selection policies and context information.

The standard also defines three functions inside the TRM:

- Terminal reconfiguration decision and control,
- Information extraction, collection, and storage,
- RAN selection functions

The terminal reconfiguration decision and control function makes decisions on terminal reconfiguration. These decisions are made within the framework determined by the radio resource selection policies received from the NRM. After making these decisions, this function sends corresponding reconfiguration commands to the TRC. The TRM information extraction, collection, and storage function receives, processes, and stores terminal context information and RAN context information.

Terminal context information is received from the TMC. Terminal context information regarding other terminals may be received from the NRM. RAN context information is received from the NRM. The TRM information extraction, collection, and storage function provides information to functions inside the TRM. Also, it forwards terminal context information to the NRM. The TRM RAN selection function selects RANs for exchanging radio resource selection policies and context information between the NRM and TRM.

12.1.3 Interfaces

The following interfaces in the 1900.4 Functional Architecture play main role in the provisioning of context information:

- **Interface between the TRM and the TMC -** Interface between the TRM and the TMC is used to transmit the following:

  From TRM to TMC:

  - Terminal context information requests

  From TMC to TRM:

  - Terminal context information
- **Interface between the NRM and the TRM -** Interface between the NRM and the TRM is used to transmit the following:

From NRM to TRM:

- Radio resource selection policies
- RAN context information
- Terminal context information

From TRM to NRM:

- Terminal context information related to Terminal of this TRM

- **Interface between the NRM and the RMC -** Interface between the NRM and the RMC is used to transmit the following:

  From NRM to RMC:

  - RAN context information requests

  From RMC to NRM:

  - RAN context information

- **Interface between several NRMs -** If there are several NRMs, a corresponding interface may be defined between these NRMs. This interface is used to transmit the following:
  - RAN context information
  - Terminal context information
  - Spectrum assignment policies
  - RAN reconfiguration decisions
  - Radio resource selection policies

12.2 ETSI RRS

12.2.1 System requirements

Requirements pertaining to context information and management within ETSI RRS functional architecture are as follows:

- Ability to provide the terminals with information on which radio accesses may be available at the current location of the terminal. Such information can help the terminal to make a more efficient detection of the available radio accesses and thus may improve the time for the detection of the radio accesses and may also reduce the energy consumption in the terminal used for this procedure.

- Ability to provide the terminals with access selection information on which of the available accesses to use for a session. This access selection information can either be policies, recommendations or commands provided by the network to the terminal.

- Support of mechanisms to provide user and terminal related information from the terminal to the network. Such information may include terminal capabilities, user preferences, the session's QoS information and information about detected radio accesses.

Support of mechanisms to provide base station and cell related information from the base stations to the network. Such information may include base station capabilities, current configuration, cell capabilities and cell load.

The aforementioned requirements have resulted in a set of functions that management and control systems (such as the one represented through the FA) should support, namely:

- Context acquisition functions for supporting context awareness.

- Profile management for supporting the requirement for personalization and pervasive computing.

- Policies derivation functions for offering rules necessary for always-best connectivity.
- Knowledge acquisition based on learning functionality, which is essential for addressing complexity and scalability.

12.2.2 Functional architecture

The ETSI RRS FA concentrates on the network aspects, and in particular on the different optimization needs within a composite radio environment. In this respect, the FA constitutes an amalgamation of different advanced resource management mechanisms represented as functional blocks, each of which can be considered as a wrapper to the functions deriving from the requirements mentioned above. Those blocks include:

- Dynamic, Self-Organising Planning and Management (DSONPM);
- Dynamic Spectrum Management (DSM);
- Joint Radio Resources Management (JRRM);
- Configuration Control Module (CCM).

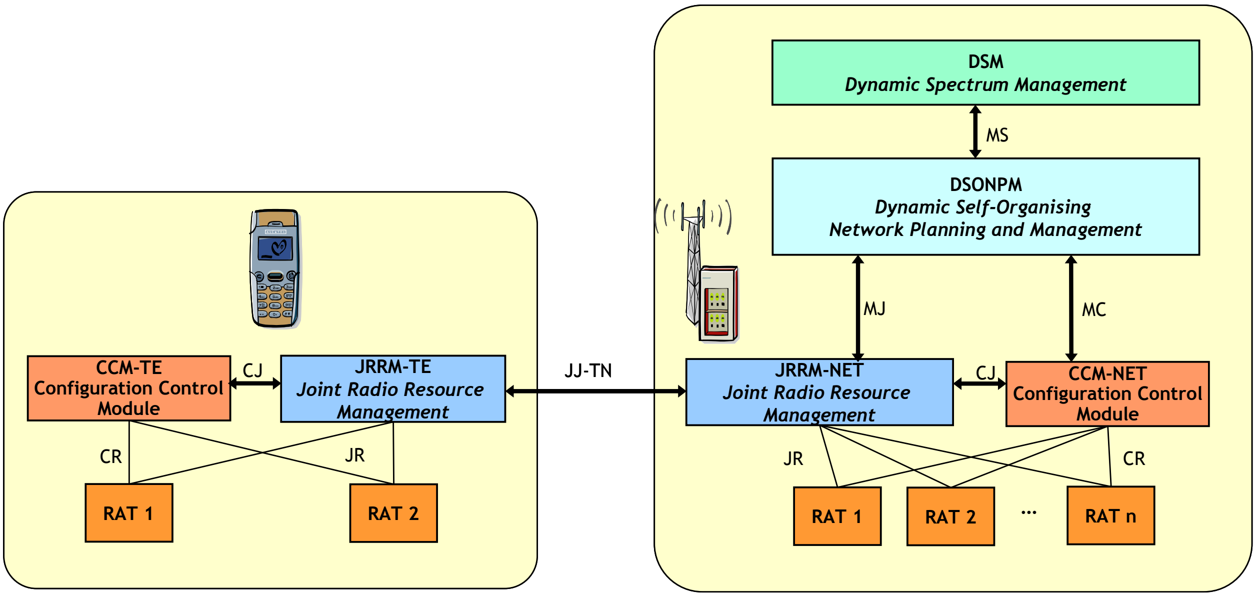

CCM-TE
Configuration Control Module
CJ
JRRM-TE
Joint Radio Resource Management
CR
JR
RAT 1
RAT 2
JJ-TN
DSM
Dynamic Spectrum Management
MS
DSONPM
Dynamic Self-Organising Network Planning and Management
MJ
MC
JRRM-NET
Joint Radio Resource Management
CJ
CCM-NET
Configuration Control Module
JR
CR
RAT 1
RAT 2
...
RAT n

Figure 67: High level view of the FA for the Management and Control of Reconfigurable Radio Systems (single-operator viewpoint)

12.2.2.1 Dynamic Self-Organising Network Planning and Management (DSONPM)

The objective of the DSONPM block is to provide the medium and long term decision upon the reconfiguration actions a network segment should take, by considering certain input information, and by applying optimization functionality, enhanced with learning attributes.

Input to DSONPM

"Context acquisition" reflects the status of the elements of the network segment, and the status of their environment. Essentially, each element uses monitoring and discovery (sensing) procedures. Monitoring procedures provide, for each network element of the segment, and for a specific time period, the traffic requirements, QoS levels offered, the mobility conditions, the interference levels, the configuration used by the transceivers (operating RATs, spectrum bands, radio parameters), and the QoS levels offered. Discovery procedures provide information on the QoS that can be achieved by alternate configurations, as well as the expected blocking probability, delays, handover blocking,

outage probability, etc. Context information will be used from the system to provide the current view of the service area that can be translated to a well specified pattern.

"Profiles management" provides information on the capabilities of the elements and terminals of the segment (at both, a software and a hardware level), as well as the behaviour, preferences, requirements and constraints of users and applications. Essentially, it also designates the configurations that will be checked for network elements and terminals. For users this part designates the applications required, the preferred QoS levels and the constraints regarding costs. This information is necessary during the optimization procedure in order to decide the most appropriate configuration considering current context information.

"Policies derivation" adheres to the fact that management decisions should not only be feasible from technological perspective but also have to be aligned with operator strategies. Policies information designates rules and functionality (optimization and negotiation algorithms) that should be followed in context handling. Sample rules can specify allowed (or suggested) QoS levels per application, preferred allocations of applications to RATs and assignments of configurations to transceivers. Additionally, policies also refer to the selection of the appropriate algorithm, among a family of algorithms, which is appropriate for handling the certain context. This implies the placing of utility weights (based on the offered QoS levels) that differentiate the functions used for reaching a decision. Furthermore, an operator might choose to apply load balancing among their RATs, or select other criteria, or he could choose the number of transceivers to be used (judging from their cost), the priorities of the available RATs, as well as the weights with regards to the desirable radio parameters values.

Output of DSONMP

The decision of the optimization procedure that accompanies Dynamic and Self-Organizing Network Planning and Management (DSONPM) is manifold and can be split as follows:

- General Application layer:
    - QoS assignment (e.g. maximum/guaranteed bit-rate per QoS Class per cell).
- Network layer related:
    - Distribution of traffic to RATs and networks
    - Network performance (e.g. HO parameter optimization, Load balancing, Interference control, etc.).
    - Element interconnections (backhaul selection and mesh aspects to be supported).
- PHY/MAC related:
    - Number of network element transceivers involved in decisions
    - RATs to be activated in the selected transceivers
    - Spectrum selection
    - Radio parameters configuration per RAT (e.g. maximum power level per carrier, Antenna tilt, channel selection, etc.).

It should be noted that the decisions should take into account some green aspects, i.e. they should target the minimization of the number of transceivers that are active, the minimization of the generated interference, as well as the minimization of the overall consumed power.

12.2.2.2 Interfaces

The following interfaces in the ETSI RRS Functional Architecture as depicted in Figure 67, play main role in the provisioning of context information:

- **MJ-Interface** (between DSONPM and JRRM) - The MJ interface is used by the JRRM towards the DSONMP to send information on the current context, i.e. the amount of resources used in each RAT and cell as well as other relevant context and status information.

- **JJ-TT interface** (between JRRM instances in different terminals) - The purpose of the JJ-TT interface is to support the information exchange between JRRM instances in different terminals having direct communication with each other. Such information could include context information (measurements, spectrum sensing results, etc.). Also via this interface JRRM modules could negotiate on their terminals reconfiguration. The other purpose of the JJ-TT interface is in the case of a multi-hop scenario to extend the JJ-TN interface to the terminals that do not have a direct communication with the network side, in case of multi-hop communication. In this case a part of information exchanged via JJ-TN interface is also exchanged via JJ-TT interface, where the intermediate terminal serves as a relay. This optional interface may be used when terminals have direct communication with each other.
- **JR interface** (between JRRM and the underlying RATs) - The JR interface is used to report information on the resource status like cell load or measurements of the current active links as well as candidate links to the JRRM. Please note that this interface is used on the terminal side as well as on the network side.

On the terminal side, the JRRM may request measurements of the link performance from the underlying RATs. The underlying RATs may then execute the measurements and report the results back. It is recommended that the measurements are described in an abstracted format, e.g. describing the available/expected bit rate, bit error rate and Delay (minimum, maximum, expected average, expected variation) instead of using RAT-specific parameters like Received Signal Strength Indicator (RSSI), Signal to Interference and Noise Ratio (SINR) or Channel Quality Indicator (CQI). *On network side*, the same or similar information about the link performance may be exchanged between the underlying RATs and the JRRM. Additionally, this interface is used on network side to exchange information about the resource usage in the network, e.g. cell capacity and current cell load.

13. Appendix III: Security frameworks

13.1 3GPP e-UTRAN/EPC security framework

This framework introduces a single authentication procedure to independently secure three different over-the-air streams[11]:

- C-plane (signalling) Non Access Stratum stream between UE and MME: integrity and confidentiality protected
- C-plane (signalling) Access Stratum stream between UE and eNB: integrity and confidentiality protected
- U-plane (user data) stream between UE and eNB: confidentiality protected

All keys are derived through a hierarchical scheme from a shared key in AuC and user's USIM card, and this is done on a per-user/per-NAS attachment basis but can be changed also on eNB change.

Authentication challenge on UE-side is performed in USIM card.

Key derivation on UE side is performed partly in the USIM card, partly in the device.

The 3GPP security framework also defined means to perform "fast" re-authentication because of timing constraints (e.g. HO delay) linked to mobility.

Main features that are defined for providing secure network access are: user identity confidentiality, user authentication, network authentication, confidentiality of user data, confidentiality of signalling data, and integrity and origin authentication of signalling data.

Security key hierarchy in EPS[12] is presented below with key description presented afterwards [40].

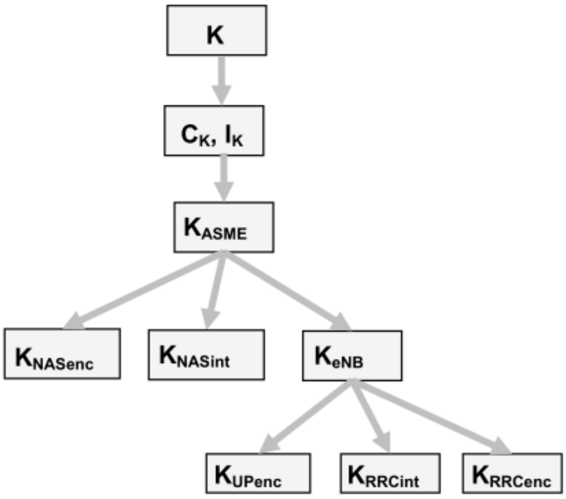


Figure 68: Security key hierarchy in EPS [40].

K: long term credential, shared between UE and AuC (Authentication Center);

C_K : ciphering key: result of an EPS AKA run; shared between UE and HSS (Home Subscriber Server);

I_K : integrity key: result of an EPS AKA run; shared between UE and HSS;

[11] Security between infrastructure equipment (e.g. eNB and MME) for C4MS signalling is out of scope of the section.

[12] EPS is Evolved Packet System, which is composed of Evolved Packet Core and Radio Access Network.

K_{ASME} : key for access security management entity (corresponds to MME), derived from C_K , I_K by an EPS specific key derivation function; shared between UE and MME;

K_{eNB} : key for eNB security from which further E-UTRAN specific keys are derived; shared between UE and MME;

K_{NASenc} : key for NAS encryption in EPS, specific per selected encryption mechanism; shared between UE and MME;

K_{NASint} : key for NAS integrity protection in EPS, specific per selected integrity protection mechanism; shared between UE and MME;

K_{Upenc} : key for user plane encryption on LTE-Uu; shared between UE and eNodeB;

K_{RRCenc} : key for RRC message encryption, specific per selected encryption mechanism; shared between UE and eNodeB;

K_{RRCint} : key for RRC message integrity protection, specific per selected integrity protection mechanism; shared between UE and eNodeB.

It needs to be noted that services provided by the 3GPP networks can be also accessed from the non-3GPP access networks. Although different approaches were developed for that purpose (e.g. I-WLAN, GAN, Untrusted/Trusted non-3GPP IP Access), basic assumptions regarding security framework and keys hierarchy for these approaches remained unchanged compared to 3GPP RAN networks.

Several methods applicable for Authentication and Key Agreement procedures (*-AKA procedures) may be used to gain access from 3GPP access and non-3GPP acccess networks. Corresponding methods for AKA procedures are presented in following documents:

- In case of connection from E-UTRAN to EPC – EPS-AKA is used – specified in [40]
- In case of connection from GERAN/UTRAN to EPC – GSM/UMTS – AKA is used – presented in [43] and [44] respectively.
- In case of connection from untrusted 3GPP-access network to EPC – EAP-AKA is used – specified in [45].
- In case of connection from trusted 3GPP-access network to EPC – EAP AKA' (aka EAP AKA Prime) is used – specified in [46].

It needs to be noted that in case of non 3GPP-access networks additional security mechanisms needs to be used to provide a secured connection between UE and authenticatior[13]. This is achieved via IPsec tunnel, which can be setup using EAP-AKA encapsulated in IKEv2 protocol [47].

The 3GPP security framework also defined means to perform "fast" re-authentication because of timing constraints (e.g. HO delay) linked to mobility, in such case no full AKA procedure needs to be applied.

In the IP Multimedia Subsystem (IMS), the IETF DIAMETER protocol is used with 3GPP specific extensions as the primary signalling protocol for Authentication, Authorisation and Accounting (AAA) and for the User Profile retrieval, e.g. between the CSCF and the HSS, between the SIP Application Server and the HSS and between the CSCF and Charging Data Collection Functions.

[13] In untrusted non-3GPP access Network EPC authenticator resides in ePDG (evolved Packet Data Gateway)

13.2 IEEE-based security

IEEE security framework is based on two approaches. Firstly WPA (WiFi Protected Access) has been announced by WiFi-Allience and afterwards additional set of mechanisms named WPA2 was specified and ratified in IEEE 802.11i standard (802.11i specifies a framework called RSN (Robust Security Network) that integrates WPA and WPA2 mechanisms). The newest IEEE 802.11:2007 standard has embedded RSN as mandatory [9]. WPA and WPA2 share common architecture and approach, however WPA supports TKIP cipher algorithm, when WPA2 may also use AES.

Similarly to 3GPP, IEEE decided to use EAP mechanisms to communicate between STA (supplicant), an authenticator (usually an AP) and authentication server using a 4-way handshake. 802.11i uses 802.1X model with corresponding mechanisms of EAPOL (EAP Over LAN) and additional protocols like RADIUS for data exchange and authentication.

Keys used for data encryption and integrity are derived from PTK - Pairwise Transient Keys (and afterwards GTK - Group Transient Key) which is firstly based on Pairwise Master Keys (PMK). Master Key may be stored in a smart card, device disk or remembered by user. In case of upper-layer authentication, key supplied as Master Key needs to be securely transferred to STA. However specification does not impose which scheme shall be used (e.g. TLS, Kerberos or Cisco Light EAP may be used) for providing a key to user. When pre-shared keys are used, a pre-shared key is straightforwardly used as PMK.

Both approaches use key hierarchy and distinction between pairwise and group keys. Pairwise keys are shared only between two communicating devices (i.e. station (STA) and AP in infrastructure mode, or two STAs in ad-hoc mode), hence enabling unicast communication. On the other hand a group key enables to reach all STAs in radio range. Group key in infrastructure mode may be only used by AP. When node wishes to send broadcast message to all nodes in its Basic Service Set (BSS) first a unicast message to AP is sent and afterwards AP broadcast a message protected by Group Key to all STAs. In ad-hoc mode each node needs to establish a secure unicast connection with its neighbours. Afterwards a Group Key is generated and sent by unicast communication only to those STAs that a sending node wishes to grant access to a group (hence such communication is more like multicast rather than broadcast). Group key in non-infrastructure mode is unique for every transmitting node.

Based on PMK and other entries following pairwise keys are derived:

- Data Encryption key (128 bits)
- Data Integrity key (128 bits) [14]
- EAPOL-Key Encryption key (128 bits)
- EAPOL-Key Integrity key (128 bits)

Based on GMK (which is arbitrarily chosen by a device) two group keys are derived:

- Group Encryption key (128 bits)
- Group Integrity key (128 bits)[8]

Unicast or broadcast/multicast keys are changed each time when an STA connects to an AP. As an enhancement towards nodes mobility, a fast authentication may be applied when STA handoffs from one AP to another by distributing security context from one AP to another. However such scheme reduces the overall system security as such transactions may be compromised.

[14] In WPA2 one key is used for both encryption and integrity key.

14. Appendix IV: Traffic relaying based on the standardized 3GPP solutions

The original motivation behind the introduction of different solutions for interworking of non-3GPP technologies with 3GPP networks was the extension of the 3GPP network coverage by enabling access to 3GPP services over WLAN APs or WiMax base stations. In OneFIT we propose to further extend this concept and enable access to 3GPP services also over user terminals (more specifically over short range radios supported by user terminals). This means that in OneFIT user terminals would be treated by other user terminals as points of attachment that may provide access to 3GPP network.

In general, 3GPP standardized four approaches for interworking of non-3GPP technologies with legacy 3GPP technologies. These approaches include GAN (Generic Access Network), which is often called UMA (Unified Mobile Access), I-WLAN (Interworking WLAN) and Untrusted/Trusted Non-3GPP IP Access. The first two approaches (i.e. GAN and I-WLAN) were developed to enable interworking of non-3GPP networks with the pre-release 8 3GPP networks. The other two approaches i.e. Untrusted and Trusted non-3GPP IP access were introduced in the later releases, along with the introduction of EPC (Evolved Packet Core) which is an all-IP core network.

In this section we will mainly focus on Untrusted non-3GPP IP access but it needs to be noted that similar extensions can be proposed for I-WLAN (I-WLAN is considered to be the predecessor of Untrusted/Trusted non-3GPP IP access) and GAN/UMA. We do not consider in this section Trusted non-3GPP IP access as relaying user terminals in this case would need to be responsible for handling authentication and authorization processes for the client terminal (relaying terminals would need to act as typical Gateways in Trusted non-3GPP IP access). This obviously would jeopardize the overall security of the system.

The following section provides an overview of a concept for enabling traffic relaying, based on the solutions for connecting non-3GPP networks to PLMN. The section briefly introduces the basic approach, highlights some of the existing problems and identifies the necessary extensions.

14.1 General considerations on untrusted non-3GPP IP access

As already mentioned, Untrusted non-3GPP IP network access solution was proposed in order to enable interworking of non-3GPP networks with PLMNs. Similarly to other approaches (I-WLAN, GAN/UMA and Trusted non-3GPP IP access), Untrusted non-3GPP IP access enables 3GPP-based access control, 3GPP-based charging, access to 3GPP PS based services (e.g. IMS calls) and seamless mobility between different systems. Moreover, it does not impose any limitation with respect to the technologies that can be used to access the 3GPP network [8]. This means that any existing short range radio technology employed by a user terminal could be potentially reused for the purpose of accessing the 3GPP network.

The main building block of the interworking architecture for the Untrusted non-3GPP IP access is ePDG (evolved Packet Data Gateway) which is responsible for IPSec tunnel handling, mobility (in case of S2b), tunnel authentication and authorization, enforcement of QoS, lawful interception, etc. It is important to note that the ePDG allows the local access router (relaying terminal in our case) not to be involved in the higher layer procedures such as: initial terminal attachment, terminal detachment or terminal handover. The responsibilities of the local access router (relaying terminal in our case) are thus limited to local IP address management, and routing of client traffic to ePDG.

In OneFIT we try to reuse the procedures and the above mentioned features provided by the Untrusted non-3GPP IP access for realization of traffic relaying which is a necessary functionality for most of the proposed scenarios (e.g. SCE#1, SCE#2, SCE#4). Our basic idea is to further extend the concept of Untrusted non-3GPP IP access and enable access to 3GPP networks also via user terminals (more specifically via short range radios supported by user terminals). This means that in OneFIT user terminals would be treating each other as potential points of attachment that may provide access to the 3GPP network services. Figure 69 depicts a possible path of data relayed by the relaying terminal. As seen, the traffic of the client terminal is routed via relaying terminal's PLMN up to the PDN Gateway of the relaying terminal. From that point, the traffic of the client terminal is routed over public network towards the ePDG of the client terminal and then over the PLMN of the client terminal to PDN Gateway.

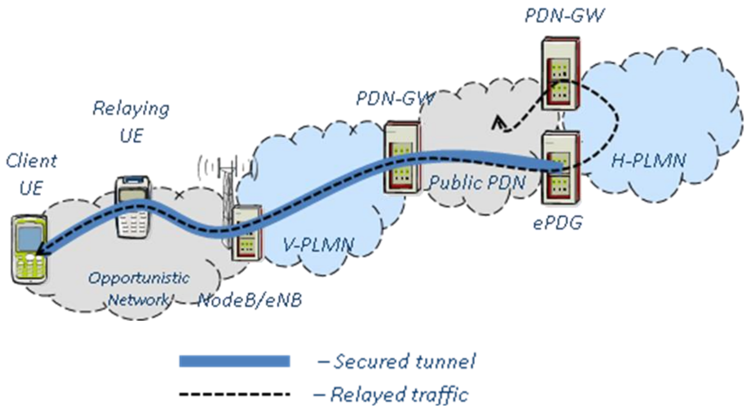


Figure 69: Traffic relaying based on Untrusted non-3GPP IP access for non-roaming (top) and roaming (bottom) scenario – simplified vision

It is worth noting here that the concept is based on the assumption that the relaying terminal allows for an initial access to enable the authentication of the requesting node within the EPC. In order to realize that the relaying terminal could have a list of ePDG addresses and thus determine if the client terminal accesses ePDG to authenticate, or tries to access other services.

14.2 Shortcomings and necessary extensions

Although the concept of Untrusted non-3GPP IP access seems to provide all the necessary procedures (e.g. terminal attachment, detachment, authentication, charging) and features (e.g. seamless mobility which is a necessary condition to provide QoS, charging, access control), several shortcomings which may not allow the full application of the scenarios proposed in OneFIT could be identified. The identified shortcomings include:

- no decision making logic on the terminal side – there are no mechanisms which would allow terminals to determine when to relay, how to choose terminals for relaying, etc.,
- no resource reservation procedures for services relayed over other terminals – there are no procedures which would be responsible for reconfiguration of the existing links between the infrastructure and the relaying terminal. This is necessary in case a terminal starts relaying traffic for other terminals and higher QoS is required,
- no procedures to guarantee QoS for services running on relaying terminal – there are no procedures on the terminal side which would guarantee QoS in case terminal starts to relay traffic for other users,
- no local breakout function to optimize routing – there are no procedures which would allow to optimize routing in case PDN-GWs for the client terminal and relaying terminal are the same entity (see Figure 69)
- no mechanisms for supporting PCC based rewarding system [2] – there are no mechanisms for identification if a user is relaying traffic, or for identification if a user is using other user as a relay,

In order to address the above mentioned shortcomings, new functionalities need to be implemented on the terminal side as well as on the network side. In case of the terminal side, the new functionalities will be developed in WP4 (ON Suitability determination algorithms, ON Maintenance algorithms, etc.).

In case of the network side the required functionalities could be achieved by introducing some minor system modifications which would mainly concern the evolved Packet Data Gateway (ePDG). The modifications should allow ePDG to:

- Obtain the identity of the relaying user – the procedure is required as the system needs to know which user should receive the reward for providing the relaying service.
- Confirm the successful authentication of the user requesting the access to the relaying user – the procedure is required as the relaying user needs to know if it should relay traffic for a specific user.
- Modify the PCC policies for the relaying node – the procedure is necessary in case a link between a relaying node and infrastructure needs to provide higher QoS.

Obtaining the identity of the relaying node as well as sending confirmation about the authentication result to the relaying node seems to be straight forward (ePDG knows the IP address of the relaying UE and can use it to determine the user identity). The modification of the PCC policies may be however more challenging.

15. Appendix V: Information model concepts

The following section introduces a set of UML models which provide a more detailed view on the ON information model proposed in Section 3. As the proposed information model, in general, extends the E3 information model (see [26]), only the UML models for the new concepts or concepts which require extension/alteration are depicted in this section.

Firstly basic concepts of User, Terminal and Application is presented. Afterwards a Base Station model is depicted. With those elements specified a concept of Network Interface and Link models are shown enabling a inter-device communication and data exchange.

15.1 User concept

A user concept of OneFIT may be seen as a simplified version of E3 approach [26]. User model consist of one or more User Profile and corresponding User preferences. As presented in UML model for the OneFIT User concept (see Figure 70) a Users Preferences may also incorporate User Requirements, ON Preferences or Video Preferences.

A user in OneFIT system with corresponding information about supported Applications (based on Profile class) and set of preferences (based on combination of three classes merged and given a description of Preference Id) forms a basic network element.

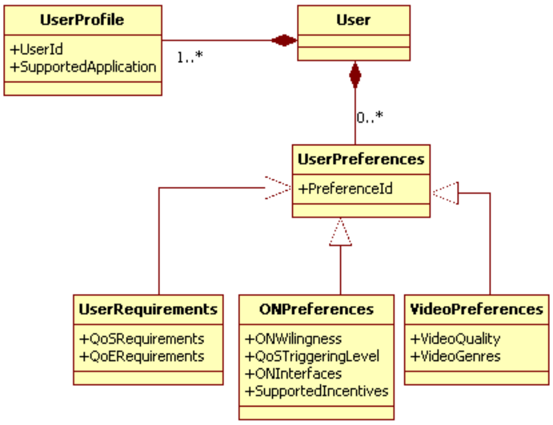


Figure 70: UML model for the OneFIT User concept

15.2 Terminal concept

The terminal concept proposed for OneFIT describes a generic approach for ON-enabled entity that include Application model (specified in section 15.3), User (concept depicted in section 15.1), Terminal Profile, Terminal Measurements, Terminal Configuration and Terminal Capabilities.

As presented in Figure 71 Terminal Configuration may be also extended by information from many Geolocation Databases (e.g. Databases regarding different regions and locations, or geolocation from one region but more than one geolocation system) and information about Spectrum Sensing. Capabilities of a Terminal are also extended by Geolocation Database Capabilities (distinguishing Database Protocols and Operators) and Spectrum Sensing Capabilities (that inform about supported spectrum sensing techniques or available/feasinble frequency range for sensing).

As presented below (in Figure 71) a Terminal may incorporate none or many Applications (depicted in next sub-section) but at least one User needs to own a Terminal.

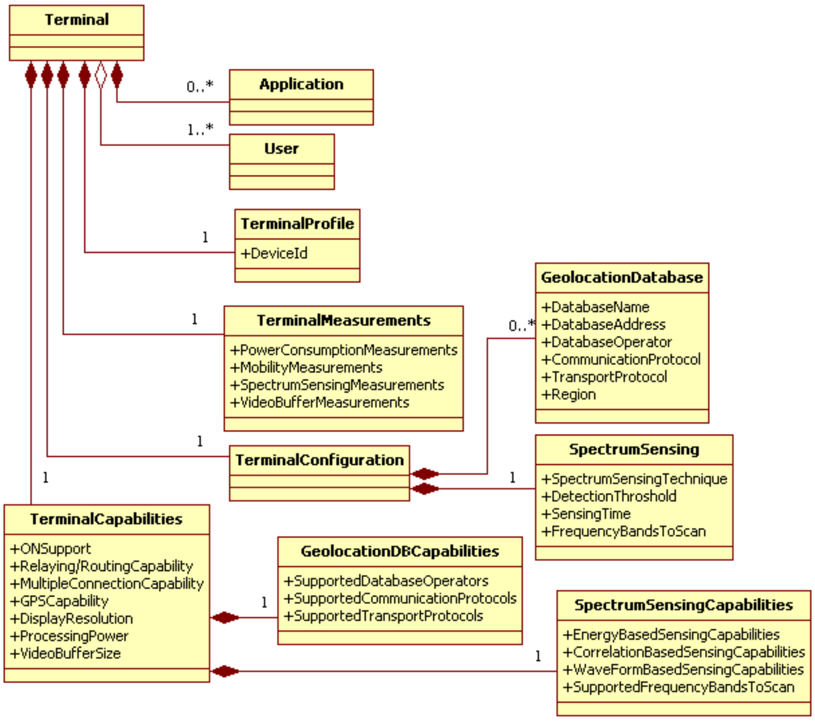


Figure 71: UML Model for the OneFIT Terminal concept

15.3 Application concept

An Application is a building block of a Terminal, however more than one Application may be run in Terminal. Application is described in following figure (Figure 72) by three sub-classes: Application Measurements, Application Profile and Application Capabilities. Each sub-class unequally characterize an Application and cannot be omitted in Application class description.

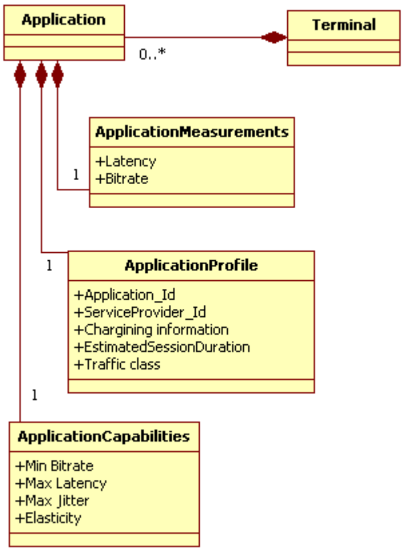


Figure 72: UML Model for the OneFIT Application concept

15.4 Base station concept

Similarly to [26], the term Base Station is used to refer to any radio node on the network side. Each standard introduces common names for Base Station entities, e.g. eNodeB in LTE, NodeB in UMTS, Access Point in IEEE Standard 802.11 or Base Station in GSM thus providing distinguishable names for specific technology. Concept of the Base Station consist of Base Station Profile, Base Station

Measurements, Base Station Configuration (regarding Power Allocation, operating Frequency Bands, Connected Users and Neighbouring list) and Base Station Capabilities (with parameters allocated to Opportunistic Network Support and maximum number of served Users). Base Station Capabilities are extended by Caching Capabilities as described in Figure 73.

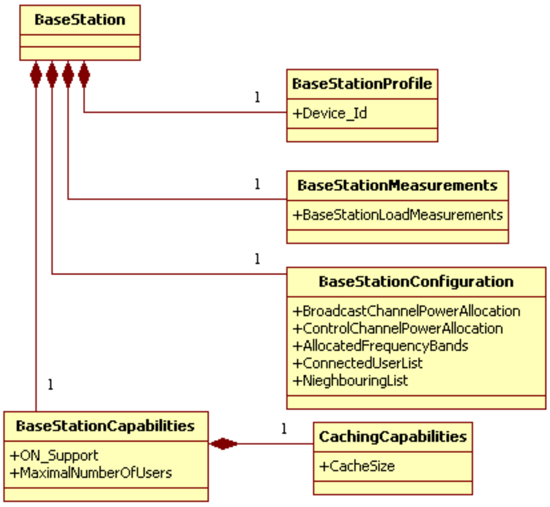


Figure 73: UML Model for the OneFIT Base Station concept

15.5 Link concept

A link is an entity that enables communication between elements of a communication system (e.g. Base Stations and Terminals). Link is characterized by three classes: 1) Link Profile specifying Profile characteristics like destination, state of a link, used frequency or type of a link (e.g. link to infrastructure or link between terminals), 2) Link Capabilities describing Maximum Link Capacity and 3) Measurements of a Link thus providing information about actual Link parameters as RSSI (Received Signal Strength Indication), SINR (Signal to Noise Ratio), Bit rate or Latency.

As presented in Figure 74 a Link associates with Network Interface (described by RAT identity and Transmission Power) in relation from none to many.

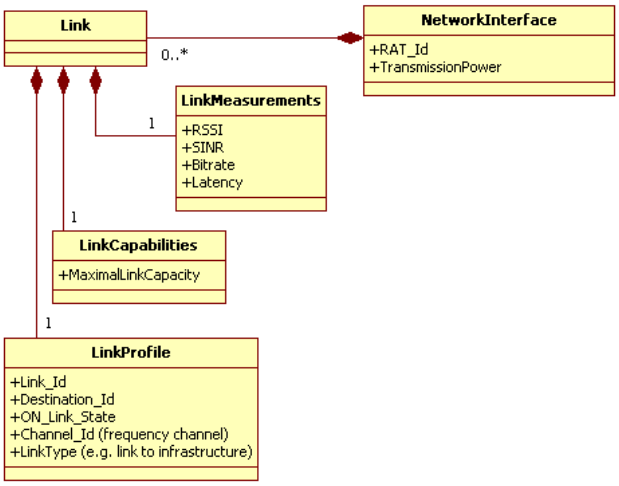


Figure 74: UML Model for the OneFIT Link concept

15.6 Network interface concept

The following subsection provides more detailed description of the Network Interface concept. Network Interface is composed form several classes: 1) a profile characterizing RAT Id, 2) Network Interface Measurements by providing information about current interface load extended by Channel

Measurements, 3) Network Interface Configuration with a specified RAT Id, Transmission Power and Gateway Mode status and 4) Capabilities of a Network Interface regarding interface specific information (e.g. supported bit rate or channels, Energy Consumption etc.). As depicted in Figure 75 Node may incorporate one or more Network Interfaces.

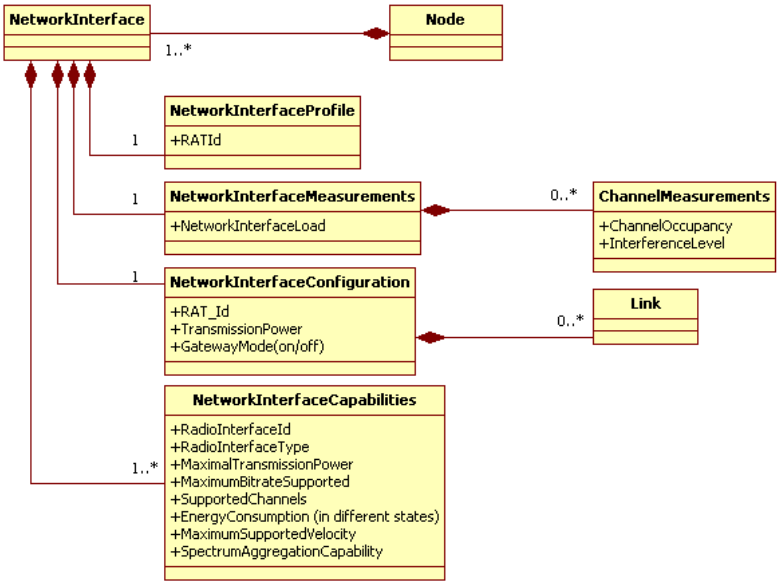


Figure 75: UML Model for the OneFIT Network Interface concept