



OneFIT functional and system architecture – D2.2

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:	28.02.2011
Actual Date of Delivery:	28.02.2011
Editor:	Jens Gebert (Alcatel-Lucent)
Participants:	See contributors' table
Workpackage:	WP2
Nature:	PU ¹
Version:	1.0
Total Number of Pages:	60
File:	OneFIT_D2.2_20110228.doc

Abstract

This document presents the OneFIT functional and system architecture for the management and control of infrastructure coordinated opportunistic networks (ONs). The most relevant building blocks "Cognitive management System for the Coordination of the Infrastructure" (CSCI) and the "Cognitive Management system for the Opportunistic Network" (CMON) are described.

Keywords List

Opportunistic networks, cognitive management, architecture, CSCI, CMON, C4MS

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 [1] is a collaborative research project designing and validating a managed opportunistic network (ON) solution which is coordinated by the infrastructure. The solution will provide enhanced wireless service provision and extended access capabilities for the Future Internet, through higher resource utilization, lower costs, and management decisions with a larger “green” footprint. OneFIT leads to better services for the user and creates market opportunities for manufacturers, operators and service providers. The project derived from the fifth call for proposals of the 7th framework programme (FP7) of the European Commission for research and technological development.

This document presents the OneFIT functional and system architecture for the management and control of infrastructure coordinated opportunistic networks (ONs). Opportunistic networks in the context of this project are operator-governed, temporary, coordinated extensions of the infrastructure. They are dynamically created with the support from information provided by the operator e.g. on spectrum, policies and context information, in places and at the time they are needed to deliver multimedia flows to mobile users, in an efficient manner. The ONs can comprise network elements of the infrastructure as well as terminals/devices potentially organized in an infrastructureless manner.

The most relevant building blocks for the OneFIT Functional Architecture for the cognitive management and control of infrastructure governed Opportunistic Networks as described in section 2 are

- the *Cognitive management System for the Coordination of the Infrastructure* (CSCI) which is responsible for the detection of situations where an ON is useful including the ON suitability determination;
- the *Cognitive Management system for the Opportunistic Network* (CMON) which is responsible for the creation, maintenance and termination of a given ON based on the context and policy information provided by the CSCI.

Further functionalities include the *Dynamic Spectrum Management* (DSM), the *Dynamic, Self-Organising Network Planning and Management* (DSONPM), the *Joint Radio Resources Management* (JRRM), and the *Configuration Control Module* (CCM) which are located above the underlying *Radio Access Technologies* (RATs).

The System Architecture (SA) includes a description of the mapping of the OneFIT building blocks to network entities and is described in section 3.

An introduction on *Control Channels for the Cooperation of Cognitive Management Systems* (C4MS) including the C4MS reference model is given in section 4. The C4MS can be seen as a combination and evolution of the Cognitive Pilot Channel (CPC) and the Cognitive Control Channel (CCC) concepts.

Section 5 describes Message Sequence Charts (MSCs). A differentiation is made between high-level MSCs showing only the communication between the nodes and the detailed MSCs showing also details of the communication inside nodes. At the beginning of the MSCs, there is usually an issue detected, e.g. that a mobile terminal is out of coverage, or that parts of the network are congested. Then, the ON suitability determination is started. There, other nodes can be discovered and a negotiation is made on which nodes may join an ON. After a successful negotiation, the ON will be created. During the ON establishment procedures, new links are setup and relaying functionalities are configured.

Contributors

First Name	Last Name	Affiliation	Email
Jens	Gebert	ALUD	Jens.Gebert@alcatel-lucent.com
Christian	Lange	ALUD	Christian.Lange@alcatel-lucent.com
Andreas	Wich	ALUD	Andreas.Wich@alcatel-lucent.com
Andreas	Georgakopoulos	UPRC	andgeorg@unipi.gr
Panagiotis	Demestichas	UPRC	pdemest@unipi.gr
Vera	Stavroulaki	UPRC	veras@unipi.gr
Kostas	Tsagkaris	UPRC	ktsagk@unipi.gr
Lia	Tzifa	UPRC	etzifa@tns.ds.unipi.gr
Maria	Akezidou	UPRC	akezidou@unipi.gr
Marios	Logothetis	UPRC	mlogothe@unipi.gr
Evangelos	Thomatos	UPRC	evangelos.thomatos@gmail.com
Nikos	Koutsouris	UPRC	nkouts@unipi.gr
Yiouli	Kritikou	UPRC	kritikou@unipi.gr
Aimilia	Bantouna	UPRC	abantoun@unipi.gr
Oscar	Moreno	TID	omj@tid.es
David	Visiedo	TID	dvg@tid.es
Oscar	Martin	TID	oscarmg@tid.es
Markus	Mueck	IMC	Markus.Dominik.Mueck@intel.com
Andreas	Schmidt	IMC	andreas.schmidt@intel.com
Christian	Mouton	NTUK	Christian.mouton@nectech.fr
Miia	Mustonen	VTT	miia.mustonen@vtt.fi
Marja	Matinmikko	VTT	marja.matinmikko@vtt.fi
Marcin	Filo	EIT+	Marcin.filo@eitplus.pl
Ramon	Ferrús	UPC	ferrus@tsc.upc.edu
Oriol	Sallent	UPC	sallent@tsc.upc.edu
Dragan	Boskovic	LCI	Dragan.boskovic@lacidelleing.com
Milenko	Tosic	LCI	milenko.tosic@lacidelleing.com
Paul	Bender	BnetzA	Paul.Bender@bnetza.de

Table of Acronyms

Term	Meaning
3GPP	3 rd Generation Partnership Project
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
API	Application Programmable Interface
AuC	Authentication Center
BS	Base Station
C ⁴ MS	Control Channels for the Cooperation of the Cognitive Management System
CA	Certification Authority
CCM	Configuration Control Module
CCR	Cognitive Control Radio
CMON	Cognitive Management system for the Opportunistic Network
CPC	Cognitive Pilot Channel
CSCI	Cognitive management System for the Coordination of the Infrastructure
DSM	Dynamic Spectrum Management
DSOINPM	Dynamic and Self-Organizing Network Planning and Management
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FA	Functional Architecture
GSM	Global System for Mobile communications
HLR	Home Location Register
JRRM	Joint Radio Resource Management
KPI	Key Performance Indicator
LTE	Long Term Evolution
MAC	Medium Access Control
MSC	Message Sequence Chart
ON	Opportunistic Network
OneFIT	Opportunistic networks and Cognitive Management Systems for Efficient Application Provision in the Future Internet
P2P	Peer-to-Peer
PCC	Policy and Charging Control
PKI	Public Key Infrastructure
QoS	Quality of Service
RAT	Radio Access Technology

RRC	Radio Resource Control
RRM	Radio Resource Management
RRS	Reconfigurable Radio Systems
SA	System Architecture
SAP	Service Access Point
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
WLAN	Wireless Local Area Network

Table of Contents

Contributors	3
Table of Acronyms	4
Table of Contents	6
List of Figures	7
1. Introduction	8
1.1 Summary on Scenarios.....	8
1.2 Summary on System Requirements	8
2. Functional Architecture	10
2.1 Cognitive management System for the Coordination of the infrastructure (CSCI)...	16
2.1.1 Missions and Services.....	17
2.1.2 The ON-Objective	18
2.1.3 The ON-blueprint	18
2.1.4 Detailed functions of CSCI	18
2.2 Cognitive Management system for the Opportunistic Network (CMON)	20
2.2.1 Missions	21
2.2.2 Detailed functions of CMON.....	22
3. System Architecture	23
3.1 Elements of the OneFIT system	23
3.2 Mapping of OneFIT elements to network entities.....	24
3.3 Additional OneFIT system entities	27
3.3.1 OneFIT system spectrum sensing and traffic monitoring	27
3.3.2 OneFIT system security and trust concepts	27
3.3.3 OneFIT system security and trust implementation options	29
3.3.4 OneFIT system accountability, charging and billing	31
4. Control Channels for the Cooperation of the Cognitive Management System (C4MS)....	33
4.1 C4MS layer	34
4.1.1 C4MS services	35
4.1.2 C4MS protocols	35
4.1.3 C4MS Service Access Points	36
4.2 C4MS user	36
5. Message Sequence Charts	37
5.1 MSCs on Opportunistic coverage extension	38
5.2 MSC on "Opportunistic capacity extension"	43
5.3 MSCs on Infrastructure supported opportunistic ad-hoc networking	46
5.3.1 Infrastructure initiated opportunistic ad-hoc networking	47
5.3.2 Terminal initiated opportunistic ad-hoc networking	49
5.4 MSC on opportunistic traffic aggregation in the radio access network	52
5.5 MSC on opportunistic resource aggregation in the backhaul network.....	56
6. Conclusion and Outlook	59
7. References	60

List of Figures

Figure 1: OneFIT Functional Architecture for the Management and Control of infrastructure governed Opportunistic Networks as an evolution of the ETSI/E3 FA [4]	12
Figure 2: OneFIT Functional Architecture, simplified view with combined CSCI/CMON	14
Figure 3: OneFIT Functional Architecture example where the infrastructure is not part of the ON ...	15
Figure 4: Detailed functional view of the CSCI and CMON in the terminal	15
Figure 5: Detailed functional view of the CSCI and CMON in the operator’s infrastructure.....	16
Figure 6: The “legs” of an ON.....	20
Figure 7: Mapping of the OneFIT system building blocks to the underlying network.....	25
Figure 8: Establishing security and trust between two UEs by using 3GPP procedures.....	30
Figure 9: Policy and Charging Control (PCC) [6].....	31
Figure 10: C4MS – general view.....	34
Figure 11: C4MS reference model	34
Figure 12: Syntax and colour codes used in the Message Sequence Charts	37
Figure 13: Example for Scenario 1: Opportunistic coverage extension.....	38
Figure 14: High-level MSC for Scenario 1: Opportunistic coverage extension	39
Figure 15: Detailed MSC for Scenario 1: Opportunistic coverage extension.....	41
Figure 16: Example for Scenario 2: Opportunistic capacity extension	43
Figure 17: High-level MSC for Scenario 2: Opportunistic capacity extension.....	44
Figure 18: Example for Scenario 3: Infrastructure supported opportunistic ad-hoc networking	46
Figure 19: High-level MSC for Scenario 3.1: Infrastructure initiated opportunistic ad-hoc networking	48
Figure 20: High-level MSC for Scenario 3.2: Terminal initiated opportunistic ad-hoc networking	50
Figure 21: Example for Scenario 4: opportunistic traffic aggregation in the radio access network....	52
Figure 22: High-level MSC for Scenario 4: Opportunistic traffic aggregation in the radio access network.....	53
Figure 23: Detailed MSC for Scenario 4: Opportunistic traffic aggregation in the radio access network.....	55
Figure 24: Example for Scenario 5: opportunistic resource aggregation in the backhaul network	56
Figure 25: High-level MSC for Scenario 5: Opportunistic resource aggregation in the backhaul network.....	57

1. Introduction

The OneFIT project [1] focuses on the infrastructure guided cognitive management of opportunistic networks (ONs). ONs are defined as temporary, operator-governed, coordinated extension of the infrastructure. ONs typically include user terminals and they can include infrastructure elements like a base station. Home Base Stations (e.g. a Home NodeB) can also be part of an ON.

This document describes the Functional Architecture (FA), the System Architecture (SA) and the reference points of the OneFIT solution. Further on, details are given on the two most relevant building blocks which are the Cognitive management System for the Coordination of the infrastructure (CSCI) and the Cognitive Management system for the Opportunistic Network (CMON).

The architecture is based on the business scenarios, technical challenges and system requirements as described in D2.1 [2] and summarised below:

1.1 Summary on Scenarios

Five different scenarios have been identified for OneFIT and described in detail in D2.1 [2]:

- **Scenario 1** “Opportunistic coverage extension” describes a situation in which a device cannot connect to the network operator’s infrastructure, due to lack of coverage or a mismatch in the radio access technologies. The proposed solution includes one or more additional connected users that, by creating an opportunistic network, establish a link between the initial device and the infrastructure, and act as a data relay for this link.
- **Scenario 2** “Opportunistic capacity extension” depicts a situation in which a device cannot access the operator’s infrastructure due to the congestion of the available resources at the serving access node. The proposed solution proposes the redirection of the access route through an opportunistic network that avoids the congested network segment.
- **Scenario 3** “Infrastructure supported opportunistic ad-hoc networking” shows the creation of an infrastructureless opportunistic network between two or more devices for the local exchange of information (e.g. peer-to-peer communications, home networking, location-based service providing, etc.). The infrastructure governs the ON creation and benefits from the local traffic offloading, as well as on new opportunities for service providing.
- **Scenario 4** “Opportunistic traffic aggregation in the radio access network” describes the usage of a local opportunistic network among several devices, in order to share a reduced number of infrastructure links towards a remote service-providing server or database. This situation allows some degree of traffic aggregation and caching that is useful to improve the overall network performance.
- **Scenario 5** “Opportunistic resource aggregation in the backhaul network” depicts how opportunistic networks can be used to aggregate both backhaul bandwidth and processing/storage resources on access nodes. In this case, the ON is created over Access Points (AP) rather than user terminals, thus offering a new focus on system performance improvement.

1.2 Summary on System Requirements

The system requirements for the OneFIT system are also described in D2.1. A summary of these requirements is given in Table 1. The requirements are grouped into general requirements (numbered with “G”), user and service related requirements (“U”), opportunistic network management requirements (“M”), related algorithm requirements (“A”), protocol requirements (“P”) and security requirements (“S”).

Category	Nbr.	Title of the requirement
General requirements	G1	Communication with the infrastructure
	G2	Communication between terminals
	G3	Versatile spectrum use
	G4	Versatile RAT/RAN use
	G5	Mobility
	G6	Relaying
	G7	Creation of opportunistic networks
	G8	Opportunistic Networks controllable by single operator
	G9	Preservation of legacy RAN operation
	G10	Compatibility with legacy RAN deployments
	G11	Resource efficiency
User and Service related requirements	U1	Hide complexity from the end user
	U2	User's service perception
	U3	Availability of ON-related information to the service layer
Opportunistic network Management related requirements	M1	Identification of the need for an opportunistic network
	M2	Suitability determination
	M3	Creation of opportunistic networks
	M4	Connection set-up
	M5	Maintenance of opportunistic networks
	M6	Release of opportunistic networks
	M7	Coordination of opportunistic networks with the infrastructure
	M8	Opportunistic network identification
	M9	Maximum size of an opportunistic network
	M10	Coexistence of opportunistic networks
	M11	Assignment of bandwidth
Algorithm related requirements	A1	Context awareness
	A2	Decision making
	A3	Routing
	A4	ON Advertisement
Protocol requirements	P1	Protocol usage
	P2	Broadcast/Multicast
	P3	Unicast/Dedicated addressing
	P4	Secure as well as unsecure communication
	P5	Protocol efficiency
Security requirements	S1	Security
	S2	Accountability, charging and billing
	S3	Protection of user identity
	S4	Protection of device identity

Table 1: List of the OneFIT System requirements [2]

2. Functional Architecture

The management and control functionalities for opportunistic networks shall be an addition to existing functionalities in today's networks. Thus, the OneFIT Function Architecture (FA) is an extension of an existing architecture, namely the "Functional Architecture for the Management and Control of Reconfigurable Radio Systems" as defined by ETSI in the TR 102 682[4]. The FA in ETSI has been mainly derived from the results of the E3 research project [15].

The ETSI/E3 FA is designed for a network with heterogeneous radio access technologies where the mobile devices as well as the base stations are reconfigurable. The following features are provided by the ETSI/E3 FA:

- Access Selection & Handover Decisions: Select the best radio access for a given user/session based on service requirements, radio conditions, network load, policies
- Base Station Configuration and Reconfiguration to maximise the networks efficiency
- Spectrum management for optimal, dynamic spectrum usage
- Self-Management of the Radio Network Infrastructure
- Cognition Support Mechanisms (e.g. Cognitive Pilot Channel (CPC), Spectrum Sensing).

The ETSI/E3 FA is built on top of existing Radio Access Technologies and Protocol Stacks, and therefore relies on all legacy features of operator-governed infrastructure-based networks, including credentials management, authentication, ciphering and other security-related feature.

Due to the scope of the OneFit project, the following feature is added to the FA:

- Opportunistic Networks Management to provide mechanisms for operator-governed ad-hoc extensions of infrastructure networks

This infrastructure governed Opportunistic Networks Management is divided into two building blocks, namely the "Cognitive management System for the Coordination of the infrastructure" (CSCI) and the "Cognitive Management system for the Opportunistic Network" (CMON).

For the support of Opportunistic networks, a few features need also to be added to the existing RRS/E3 FA building blocks and/or existing Radio Access Technologies (RATs), with regard to UE-UE discovery, link establishment, relay function and associated security. Some of these features are already specified in different RAT standards and are considered by the OneFIT project as implementation options.

The CSCI is mainly responsible for the activities before an ON created. This includes ON opportunity detection and ON suitability determination. The CSCI is in charge of the context acquisition, processing of the same and the determination whether or not right conditions are in place for creating the opportunistic network. When the CSCI has made a decision that an ON is suitable, the decision is then sent to the CMON.

The CMON is controlling the life cycle of the ON from creation to termination. This includes the execution of the creation procedures as well as maintenance and termination of a given ON.

A summary of this split of the functionalities for the opportunistic network coordination and management between the CSCI and CMON is shown in Table 2. The details of the functions from CSCI and CMON are explained in detail in sections 2.1 and 2.2.

	CSCI	CMON
Coordination with the Infrastructure (Infrastructure not necessarily part of the ON)	YES	-
Coordination with other nodes in the ON	-	YES
Detection of situations where an ON may be useful	YES, typically based on external triggers, e.g. information from JRRM	-
ON Suitability determination	YES	-
Execution of ON establishment/creation	-	YES
Maintenance of ON, e.g. reconfiguration	-	YES
Decision on termination of ON when ON is no longer suitable	-	YES, typically based on external triggers
Execution of ON termination	-	YES

Table 2: Functional split between CSCI and CMON

The resulting OneFIT Functional Architecture for the Management and Control of Reconfigurable Radio Systems as well as for the Management and Control of infrastructure governed Opportunistic Networks is shown in Figure 1. The main building blocks are:

- (i) the *Cognitive management System for the Coordination of the infrastructure* (CSCI) which is responsible for the detection of situations where an ON is useful, which decides on the suitability of an ON and which provides policy and context information from the infrastructure to the ON;
- (ii) the *Cognitive Management system for the Opportunistic Network* (CMON) which executes the creation, maintenance and termination of a given ON based on the decisions from the CSCI;
- (iii) the *Dynamic Spectrum Management (DSM)* which provides mid- and long-term management (e.g. in the order of hours and days) of the spectrum for the different radio systems;
- (iv) The *Dynamic, Self-Organising Network Planning and Management (DSO-NPM)* which provides mid- and long-term decisions upon the configuration and reconfiguration of the network or parts of it. The DSONPM decides for example on the configuration of a base station and then instructs the Configuration Control Module (CCM) in order to execute the reconfiguration;
- (v) The *Joint Radio Resources Management (JRRM)* which performs the joint management of the radio resources across different radio access technologies. It selects the best radio access (Access-Selection & Handover Decisions) for a given user based on the session's requested Quality of Service (QoS), radio conditions, network conditions like cell load, user preferences and network policies. The JRRM also provides Neighbourhood Information which can then be distributed via Cognitive Control Channels (CCC) or a Cognitive Pilot Channel;

- (vi) The *Configuration Control Module (CCM)* which is responsible for executing the reconfiguration of a terminal or a base station, following the directives provided by the JRRM or the DSONPM.

These building blocks act on top of existing *Radio Access Technologies (RATs)*.

Further on, an interface is defined between the DSM and an external geo-location database.

It should be noted here that the proposed functional blocks act in whole or in part in both network and terminal sides, as shown in the Figure 1 below.

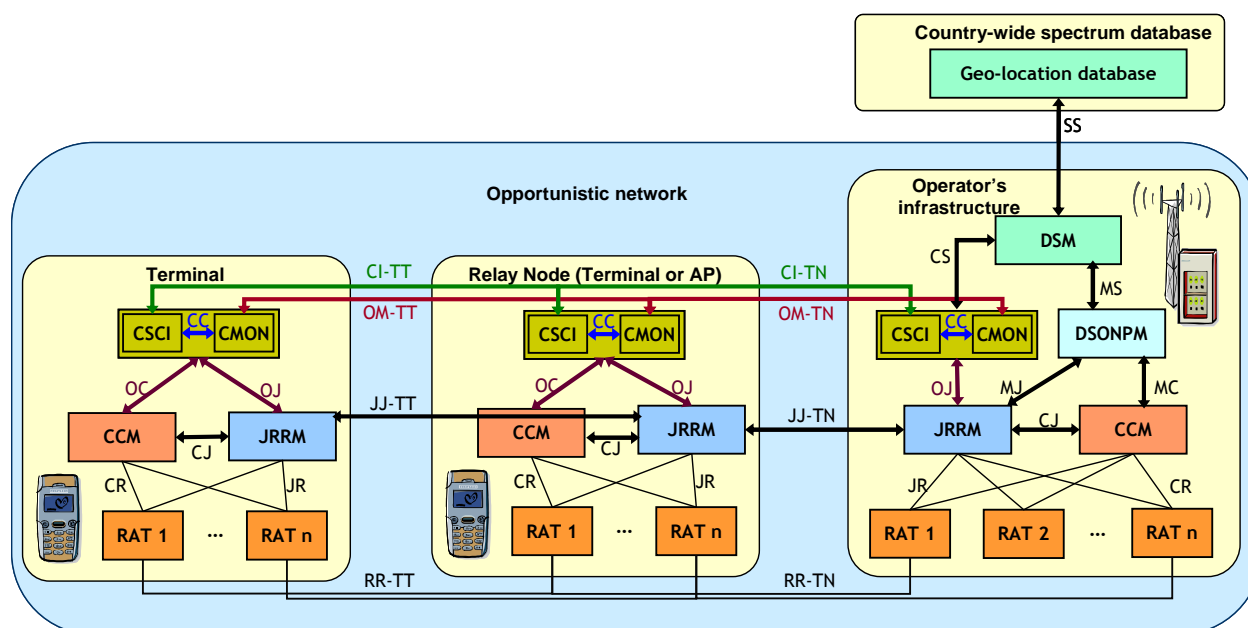


Figure 1: OneFIT Functional Architecture for the Management and Control of infrastructure governed Opportunistic Networks as an evolution of the ETSI/E3 FA [4]

The following interfaces are used in the OneFIT Functional Architecture:

- CI-Interface for the “Coordination with the Infrastructure” located between different CSCI-instances. This interface is used by the infrastructure network to inform terminals (or other infrastructure network elements) about the suitability of an ON (e.g. via an “ON-Suitability.indication message) and to provide context and policy information which are needed for the later creation and maintenance of the ON. Via this interface, the network can also collect context information from the terminals to enable the ON suitability determination. A distinction can be made between the CI-TT interface connecting the CSCI-instances of two terminals, the CI-TN interface connecting the CSCI in a terminal with the CSCI on Network side and the CI-NN interface connecting the CSCI-instances of two network entities.
- OM-Interface for the “Opportunistic Management” located between different CMON-instances. Via this interface, nodes can first negotiate about the creation of an ON. During the negotiation, node capabilities and user preferences can be exchanged and the QoS capabilities of an ON can be negotiated. After the negotiation, this interface is also used for the exchange of ON-creation, ON-maintenance and ON-release messages. A distinction can be made between the OM-TT interface connecting the CMON-instances of two terminals, the OM-TN interface connecting the CMON in a terminal with the CMON on Network side and the OM-NN interface connecting the CMON-instances of two network entities (e.g. scenario 5).

- CC-Interface connecting the CSCI in a node with the CMON in the same node. This interface is used e.g. to send a trigger for the creation of an ON from the CSCI to the CMON as well to provide information about the resources which can be used by the ON. Please note that this node interface will only exist if CSCI and CMON are implemented separately. In the case that CSCI and CMON are tightly integrated in one module, then there will be no explicit CC-interface in that node. A distinction can be made between the CC-T interface connecting the CMON and CSCI instances in a terminal, and the CC-N interface connecting the CMON and CSCI instances on network side;
- 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.
- OJ: Interface between JRRM and CSCI/CMON. Although CSCI and CMON can be separated in different blocks, it is assumed that they use both the same protocol or Application Programmable Interface (API) to exchange information with the JRRM. This interface is used to trigger the JRRM for the establishment and release of radio links during the creation, maintenance and deletion of an ON. Further on, context information e.g. on available access networks or on link performance can also be exchanged via this interface. A distinction can be made between the OJ-T interface connecting the CMON/CSCI instances with the JRRM in a terminal, and the OJ-N interface connecting the CMON/CSCI instances with the JRRM on network side
- OC: Interface between CCM and CSCI/CMON. This interface is similar to the OJ interface and may be used to obtain additional information about the current device configuration which can not be provided by the JRRM. However, it is assumed that for the normal ON management procedures, the CCM is not involved because the CMON uses the OJ-interface to trigger link setup or release procedures.
- CR: Interface between the CCM and the underlying RAT to control the reconfiguration of the radio access in a terminal or base station by the CCM;
- JR: Interface between JRRM and RAT used to report information on resource status such as cell load or link measurements towards the JRRM; Further on, this interface is used for the creation, modification and release of radio links in the underlying RATs.
- CJ: Interface between CCM and JRRM used by the JRRM to instruct the CCM on reconfigurations;
- MJ: Interface between DSONPM and JRRM used to provide status information like cell load and other Key Performance Indicators (KPIs) from the JRRM towards the DSONPM;
- MC: Interface between DSONPM and CCM used by the DSONPM to instruct the CCM on reconfigurations;
- JJ: Interface between different JRRM-instances for the exchange of JRRM related information between different nodes. A distinction can be made between the JJ-TT interface

connecting the JRRM-instances of two terminals and the JJ-TN interface connecting JRRM in a terminal with the JRRM on Network side;

- SS: Interface between different DSM instances or between the DSM and an external geo-location database;
- RR: Interface between the different RATs. This can e.g. be the interface used by a GSM, UMTS, LTE, WLAN or other protocol stack in the terminal towards a protocol stack of the same RAT in another terminal or in the network infrastructure.

The interfaces used by CSCI and CMON (CI, OM, CC, OC, OJ) are new interfaces where the details need to be developed and specified in the OneFIT project. For the other interfaces (JJ, CJ, CR, JR, MJ, MC, MS, SS), the functionality can be inherited from E3 D2.3 [16].

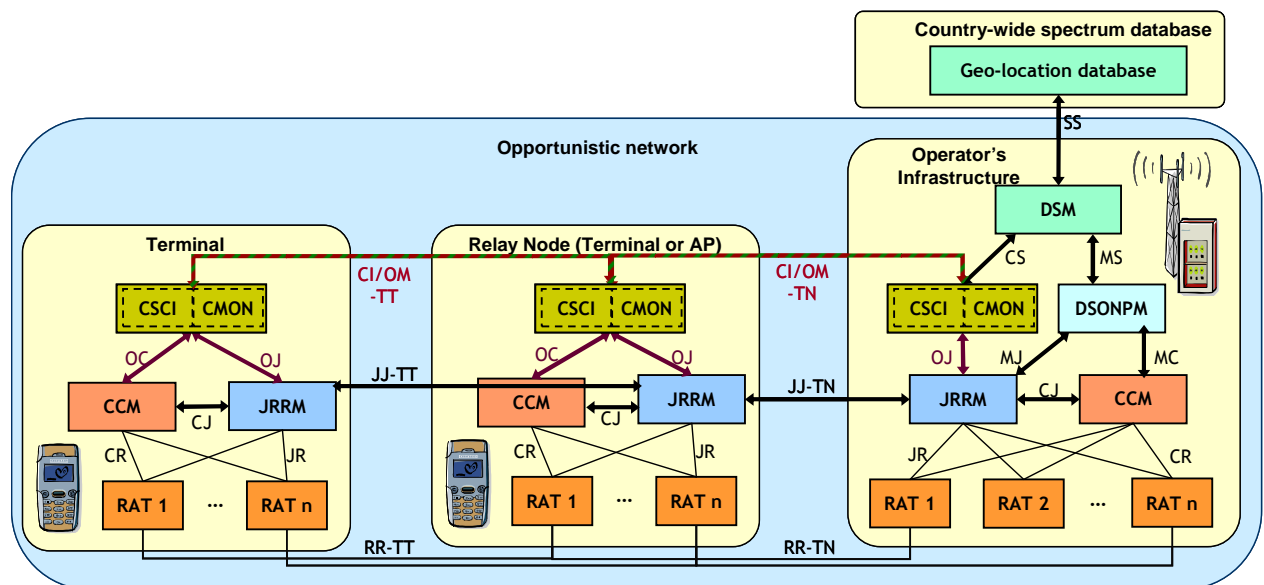


Figure 2: OneFIT Functional Architecture, simplified view with combined CSCI/CMON

As the CSCI and CMON need to interact closely and also because they act on the same context information, they can be integrated into one combined module so that the CC-interface disappears and the CI-interface and OM-interface will be a combined CI/OM interface as shown in the simplified view in Figure 2.

In the figures above, the operator's infrastructure is always part of the ON. This is typically for scenarios like coverage extension or capacity extension.

For scenarios like opportunistic ad-hoc networking between terminals, the infrastructure will not be part of the ON as shown in Figure 3. The infrastructure in such a case only provides assistance interface over the CI-TN interface, but there will be no active CMON-instance in the infrastructure.

Every node which is part of the ON must have an active CMON instance while a CSCI instance is only needed in those nodes which are coordinating with the infrastructure or which participate in the ON suitability determination.

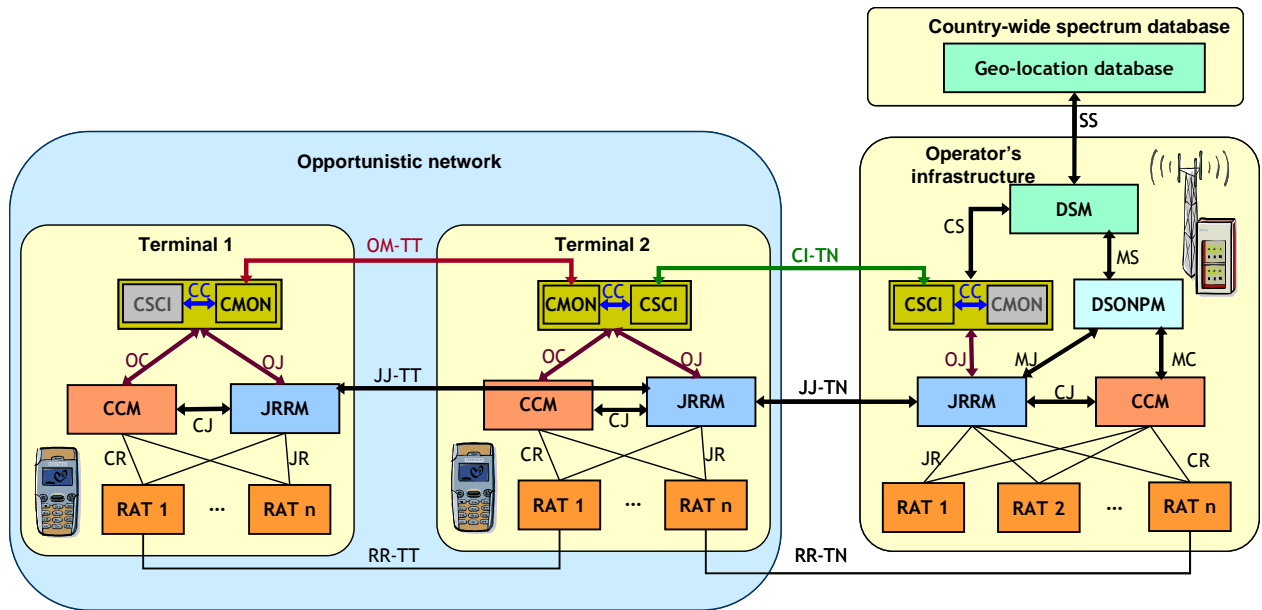


Figure 3: OneFIT Functional Architecture example where the infrastructure is not part of the ON

A more detailed functional view of CSCI and CMON is given in Figure 4 (terminal side) and Figure 5 (network infrastructure side) below.

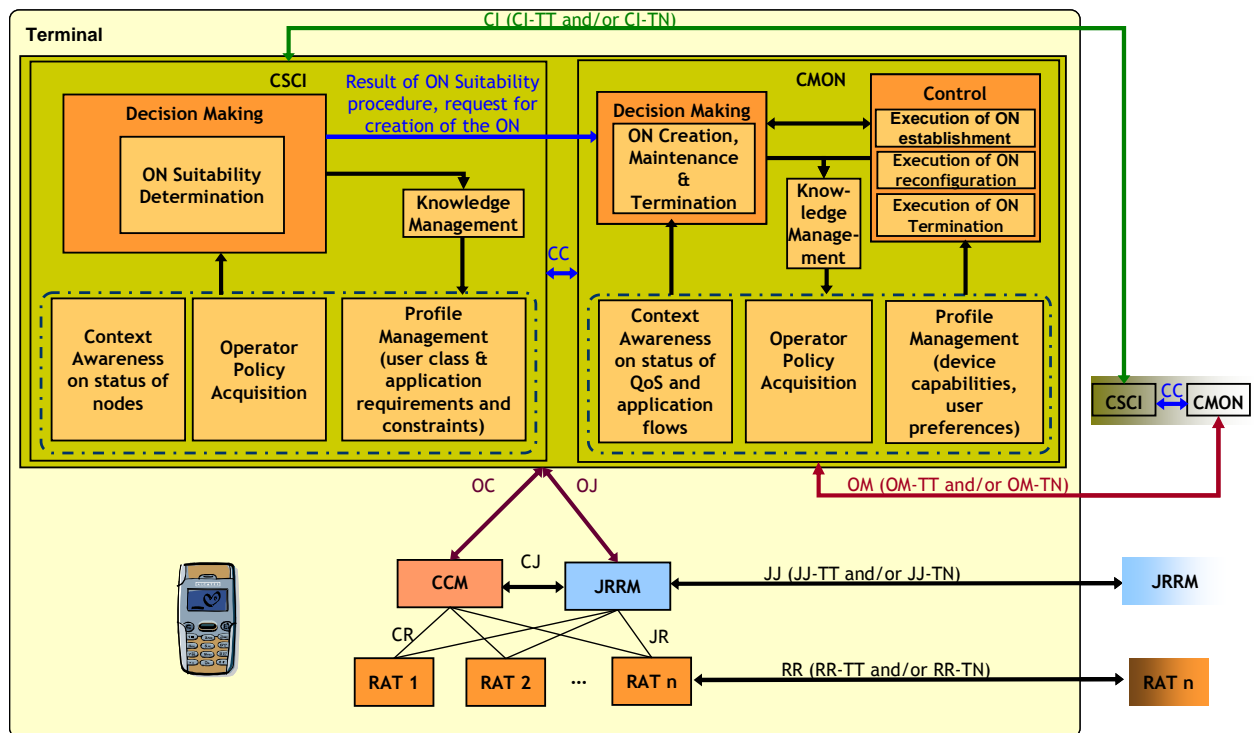


Figure 4: Detailed functional view of the CSCI and CMON in the terminal

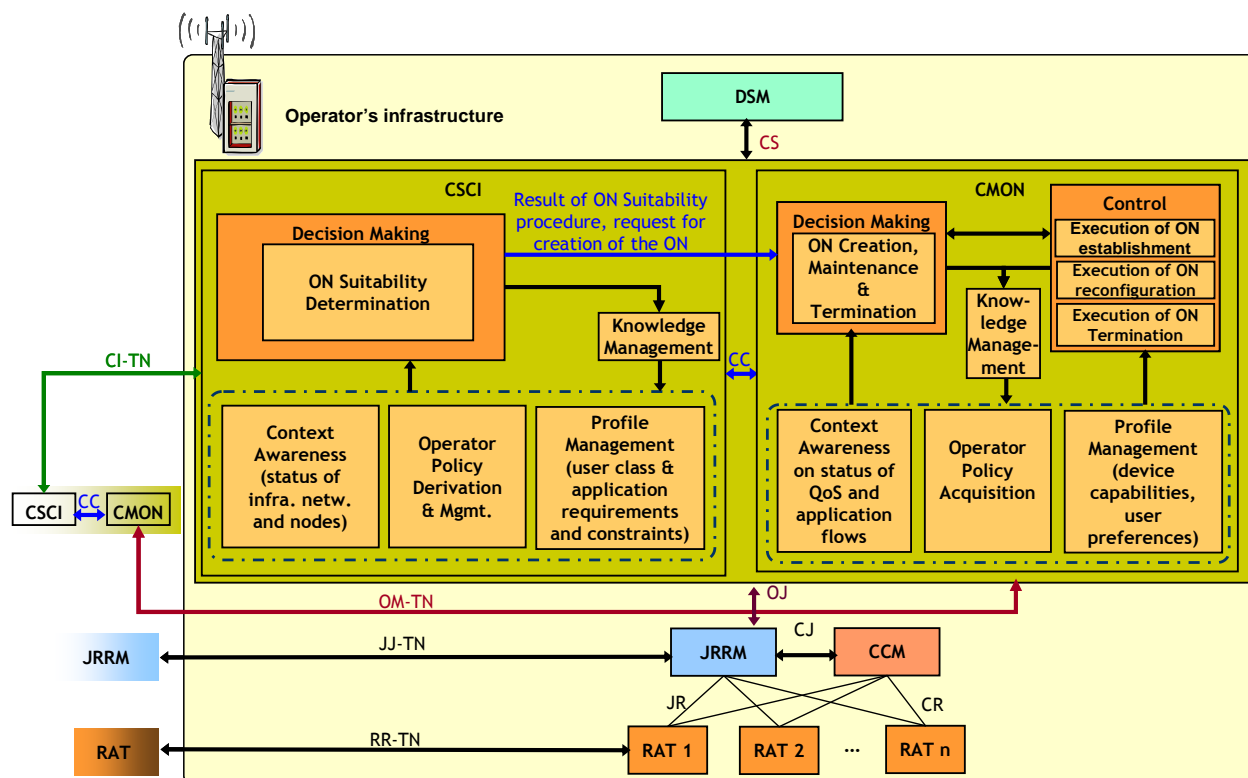


Figure 5: Detailed functional view of the CSCI and CMON in the operator's infrastructure

2.1 Cognitive management System for the Coordination of the infrastructure (CSCI)

The CSCI - *Cognitive management System for the Coordination of the infrastructure* 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.

The CSCI is responsible for the detection of situations where an ON may be useful as part of the ON suitability determination phase. The CSCI delegates the actual creation, maintenance and termination of a given ON to the associated CMON functional entity and it is located in both the operators' infrastructure side (then called "CSCI-N") and the terminal side (then called "CSCI-T").

The Suitability Determination is a centralized process, with the decision making located typically in the infrastructure but in some cases (e.g. out-of-coverage scenario) located inside a device. The decision making is based on infrastructure-level information provided by functional entities in the network and user/device-level information provided by the CSCI-T entities from a selected set of devices.

The Suitability Determination runs before the creation of an ON but also during the lifetime of the ON in order to check that context changes and ON reconfigurations (information from CMON) have not cancelled the benefit/suitability of the ON.

The CSCI-N involves context awareness, operator policy derivation and management and profile management which provide the input to the decision making mechanism. The CSCI-T involves context awareness, operator policy acquisition and profile management which provide the input to the decision making mechanism as well. 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 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 nested in the context entity which includes node's capabilities, node's status, node's location (including information from a geo-location database), node's mobility level and node's supported applications. Node information is very useful in the decision making process as it provides the necessary data of the available, candidate nodes, in order to select afterwards the best of these nodes. On the other hand, the context awareness functional entity in the CSCI-T is needed in order to acquire information for the status of nodes, which then will be used as input to the decision making mechanism.

Further on, the operator's policy derivation and 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 turn, the profile management functional entity in the CSCI includes preferences, requirements and constraints of user classes and applications which are required for the decision making. In the terminal side, the profile management functionalities are also included in order to provide details on the user class and application requirements and constraints.

In case that the conditions (dictated by the policy engine) or the potential gains by the operation of the ON are satisfied, the CSCI will come up with an ON blue print design and pass it to the CMON for the execution. To that respect, the result of the ON suitability determination phase (i.e. the request for creation of an ON) will be passed to the CMON which will handle the actual creation of the opportunistic network.

2.1.1 Missions and Services

The **missions** of the CSCI functional entity are:

- Definition of ON objectives (including QoS and security objectives)
- ON Opportunity Detection
- ON Suitability Determination (incl. compliance to network policies)
- Optimization of spectrum usage

The **services** offered by the CSCI functional entity are:

- The issuing of request for information provision:
 - To the existing network management entities, e.g. the DSM, AuC, HLR, etc...
 - To the population of mobile terminals under coverage (for "pre-ON-setup" reports), through the RAN elements (BS)
- The ON-blueprint design (see details below)
- The issuing to the CMON of requests for ON creation and extension

2.1.2 The ON-Objective

The identification of the **ON-Objective** is necessary to the CSCI to:

- Define the top-level requirements on the ON, such as QoS
- Define the criteria for ON termination.

Typical ON-Objectives are:

- “offload users A,B,C from BTS X to femto Y until BTS X is back to normal load condition”
- “connect users A,B,C through shortest possible paths until the last-but-one disconnects from the XYZ Social Network”

The detailed semantics of an ON-Objective are for further study.

2.1.3 The ON-blueprint

The ON-blueprint is designed for a given ON, meaning towards an identified ON-Objective.

The ON-blueprint is the input to the CMON process for execution of the ON creation.

The ON-blueprint is made of:

1. A set of **ON-Candidate Nodes** :
 - “Candidate” means the concerned node may or may not be eventually part of the ON, but it is part of the possible members. The final decision for inclusion during the execution of the establishment in the ON is made by the CMON entity which considers actual deployment and other optimizations (e.g. power consumption)
 - Candidate nodes have gone through the verification (by CSCI) of ON-related preferences
 - Candidate nodes have gone through the verification of “connectability” to at least one other candidate node
2. An **ON-Spectrum Allowance**
 - This allowance consists in the piece of spectrum that could be used for the ON, given the overall spectrum availability in the area and the CSCI optimization algorithm outcomes based on the ON-Objective and the considered size for the ON
 - The CMON entity (see section 2.2) will pick-up spectrum within the Spectrum Allowance
3. A set of **QoS objectives** per ON-End-user
 - These objectives are for ON-End-users, as QoS for relay nodes/links will be determined by the CMON process
 - These objectives are related to the entire path from each ON-End-user to the network access point (RAN BTS)

2.1.4 Detailed functions of CSCI

The CSCI is expected to include the following functions:

- To manage information exchange procedures between CSCI entities on the network and terminal sides related to:
 - Discovery and registration
 - Announcement of supported ON capabilities
 - Registration of CSCI-T entities with the coordinating CSCI-N

- Pairing between peer CSCI-T entities of neighbouring terminals
- Context and policy information exchanges
 - Provision of policy information from CSCI-N to CSCI-T entities.
 - Exchange of context information between CSCI entities
- In the case of CSCI-N, 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 end-points)
 - 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)
- In the case of CSCI-T, 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 local monitoring mechanisms (e.g., wide-band spectrum sensing functionality)
- To support decision-making logic for:
 - ON suitability determination
- Security management:
 - Ensure that the security mechanisms used by the underlying RAT(s) are providing the required security level from end-to-end. These security mechanisms include:
 - Authentication: Manage self identity (assigned at first provision) and authentication data needed to authenticate other entities.
 - Protection of user identity (management of user's aliases).
 - Protection of device identity (management of device's temporary identities and association to physical addresses).
 - Authorization of applications (policies and permissions for applications to use services or to access data).

- Protection of private data (storage of private user information and ciphering/deciphering of certain critical information, as defined by applications).
- Management of configuration settings related to security such as using the device as a relaying node by others.
- Accountability and billing procedures:
 - Network instances of CSCI must receive authenticated notifications of ON-related services used by the end user/applications in order to properly charge the user.
 - Terminal instances of CSCI must send authenticated notifications of the ON-related services used by the user of the terminal.

2.2 Cognitive Management system for the Opportunistic Network (CMON)

The CMON - *Cognitive Management system for the Opportunistic Network* is responsible for executing on the design obtained from the CSCI and then operationally supervising the created ON. This entity is in charge of the creation, maintenance and termination (according to the policies maintained in the CSCI) of the opportunistic network. Moreover, the CMON is responsible for the coordination of nodes in the ON. The CMON is also located in both the operators' infrastructure and the terminal side.

Generally, the CMON in the operators' infrastructure involves context awareness, policy acquisition and profile management which provide the input for the decision making mechanism. In the terminal side, the CMON 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.

In CMON, the decision-making process is a "per-leg" one: in the example below, the CMON process in UE2 must take decisions for each wireless leg (A with UE1, B with Infra):

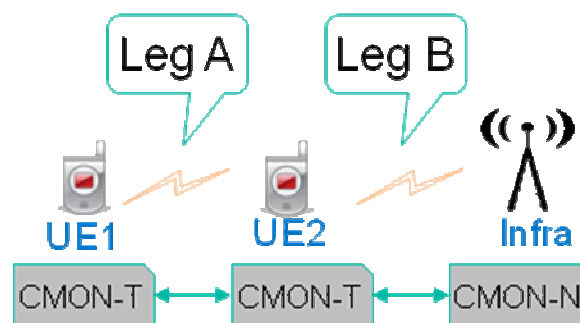


Figure 6: The "legs" of an ON

Specifically, the context awareness functional entity of the CMON in the operators' infrastructure 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). In 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 policy acquisition functional entity in both infrastructure and terminal sides, obtains and manages the policies which are being defined by the operator. Policies are used as input during the decision making mechanism for selecting the most appropriate configuration, based on the user profile (preferences) and the context. More particularly, a certain policy specifies a set of rules that the CMON must follow.

The profile management functional entity involves the device capabilities and user preferences. Indicative information includes (i) the set of potential configurations (such as the Radio Access Technologies that the device is capable of operating with, the associated spectrum and transmission power levels), (ii) the set of applications/services that can be used and the sets of QoS levels associated with the use of an application/service, and (iii) the ON-related user preferences (e.g. the utility volume/ user satisfaction) associated with the use of an application/service at a particular quality level.

Further on, the decision making functionality is present in order to handle effectively the ON creation, maintenance and ON termination according to the input from the context awareness, policy acquisition and profile management functional entities. According to the derived decision, the control entity deals with issues such as the execution of ON establishment/ creation, execution of ON reconfiguration/ maintenance or execution of ON termination. To that respect, it controls whether to proceed with an ON reconfiguration as defined in the maintenance phase or initiate the handover to infrastructure and release of resources in the case of the termination. In case a reconfiguration is deemed necessary, the CCM component will be triggered to control over terminal reconfiguration capabilities. Via the JRRM entity, CMON will control over communication protocol stacks in the terminals and infrastructure nodes by managing radio layers operation (e.g., radio link setup, radio link configuration) and network layer operation (e.g., route management internal to ON and to/from infrastructure).

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.

2.2.1 Missions

According to acquired operator's policies, context awareness and profile management, the main **missions** of the CMON functional entity are:

- Decision Making for:
 - ON creation;
 - ON reconfiguration;
 - ON termination.
- Control functionality for:
 - Execution of ON establishment/ creation;
 - Execution of ON reconfiguration;
 - Execution of ON termination.

- Knowledge management
- Security management:
 - Ensure that the security mechanisms used by the underlying RAT(s) are providing the required security level from end-to-end.

2.2.2 Detailed functions of CMON

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. Also, 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. Also, it issues commands for managing the ON operational phases (e.g., ON establishment, maintenance/ reconfiguration and termination procedures).

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).

The CMON-T has control over terminal reconfiguration capabilities and over the communication protocol stacks in the terminal by for example controlling of radio layers operation between terminals (e.g., radio link setup, radio link configuration) or controlling of network layer operation (e.g., route management internal to ON and to/ from infrastructure).

CMON-N has control over the establishment/modification/release of bearer services in the infrastructure network to support ON traffic.

Finally, with respect to security implementation related procedures, the CMON is expected to deal with security requirements in order to ensure that the security mechanisms used by the underlying RAT(s) are providing the required security (e.g. ciphering, deciphering and authentication). Further on, the CMON needs to provide relevant information for the accountability and billing procedures.

3. System Architecture

This chapter describes the high level OneFIT system architecture which has been developed based on the system requirements, the functional architecture and the proposed scenarios and use cases.

The OneFIT system (opportunistic networks and cognitive management) will be based on a framework that is compatible with the existing network and user equipment, radio spectrum, protocols and policies:

- Supported base stations will be legacy base stations, access points, femtocells and reconfigurable multi-standard base stations;
- Supported user terminals will be legacy terminals, multi-standard radio terminals and cognitive radio terminals;
- Spectrum considered suitable for ON applications includes unlicensed bands, licensed bands as well as secondary spectrum usage (e.g. UHF TV White Space bands). For each spectrum, the corresponding policies and rules about allowed channels, transmit power, radio access technology, modulation technique need to be followed.
- Protocols that can be used by the OneFIT system are legacy protocols at different layers of a system solution as well as new protocols compatible with the legacy protocols and added in order to support different phases in the ON lifetime;
- Policies and rules that have to be taken into account when building the OneFIT system are the legacy regulatory policies as well as the business policies commonly used by network operators.

3.1 Elements of the OneFIT system

The OneFIT system introduces the concept of Opportunistic Networks (ON) as coordinated extensions of the infrastructure that are built on top of existing networks (operator and user equipment) and governed by the operator. These networks will be created where and when needed, for an efficient application provisioning to requesting users.

For enabling the ON concept over existing networks, the OneFIT system requires two basic building blocks:

- Cognitive management systems;
- Control channels for coordination and cooperation of cognitive management systems.

As cognitive management systems, the CSCI and the CMON are introduced. Their algorithms, roles and relationship are to be clearly defined during this project. The difference between Self-X capabilities and the cognitive management is that Self-X capabilities of the network are based on a loop of gathering input data, processing these data and deriving optimized response to encountered changes in network environment whereas cognitive management system does this only when first time encountering specific changes in network environment. In other cases, the cognitive system will immediately respond to detected changes without the need for processing of input data.

Moreover, the OneFIT system introduces the C4MS (Control Channels for the Cooperation of the Cognitive Management Systems - see chapter 4) as main logical protocol for communication, cooperation and coordination between CSCI and CMON management entities introduced earlier. This protocol can be established over different existing radio access technologies and therefore making the OneFIT system platform/technology independent.

The CSCI, CMON and C4MS building blocks shall be self-contained functional entities which can be add-ons to the existing solutions. Equally, the adopted architectural principle ensures compatibility

with future radio access technologies and network elements. The system will use spectrum sensing and network/traffic monitoring techniques for gathering data required for cognitive management algorithms. Spectrum sensing will be used for gaining knowledge of available radio systems characteristics, condition and link quality estimation. This knowledge can be distributed between management systems or stored in databases that are to be used for gaining cognitive information about spectrum usage. This will enable efficient usage of available spectrum and therefore boost system performance and reduce interference. Network/traffic monitoring will be used for obtaining knowledge about traffic patterns, user mobility levels and application requirements. This information can be exchanged between management nodes and stored in databases of cognitive data. This will enable the system to dynamically respond on different conditions in the network and improve network usage/utilisation and application provision.

Network nodes that are to be used in the ON environment must support some kind of reconfiguration of their parameters (radio access technology specific parameters). Nodes that support multiple radio access technologies have to be capable to dynamically configure their radio interfaces to the required radio access technology.

3.2 Mapping of OneFIT elements to network entities

The OneFIT system building blocks can reside in various elements of an underlying network. If one element of network has cognitive management system(s), introduced by OneFIT, then it has to be possible to establish a C4MS based logical connection with OneFIT cognitive systems of other network nodes in order to enable an ON creation if needed. Figure 7 shows how the OneFIT system elements can be mapped onto existing network entities. As shown, the CSCI and CMON reside only in elements of the access network (base stations, access points and femto-cells) and user equipment, because these devices are under constant development and are most likely to be adapted in order to support the OneFIT system. Changing core network elements is far more demanding and represents major effort to network operators and therefore, in order to be accepted by operators, the OneFIT system has to demand as few interventions as possible on the core network.

The C4MS protocol between OneFIT cognitive systems is presented with blue dashed lines. These lines can present interfaces between CSCIs of different network nodes or interfaces between CMONs of different network nodes. The interface between CSCI and CMON inside the network nodes is not shown here.

The OneFIT system building blocks are mapped onto the existing protocol stack as introduced by the E3 project. Beside the CSCI and CMON blocks, Figure 7 shows also the JRRM, CCM and DSM blocks. There is also the SS (Spectrum Sensing) block for gaining knowledge of available radio systems by sensing, characterisation of radio conditions and radio link quality estimation. The nodes are based on existing network nodes, especially on nodes used in 3rd Generation Partnership Project (3GPP) based networks. Devices depicted in the core network correspond to the 3GPP EPC (Evolved Packet Core) network structure [7].

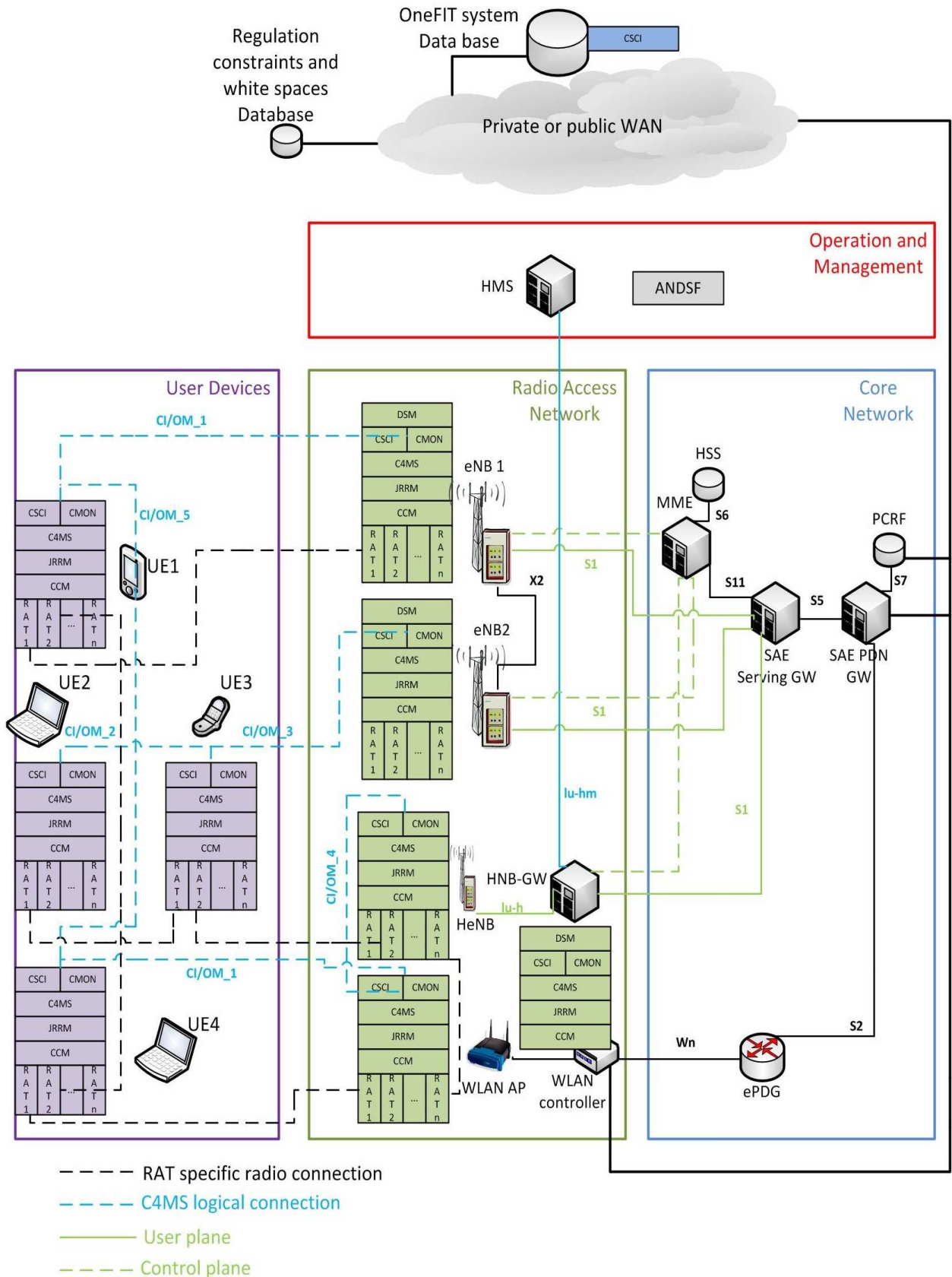


Figure 7: Mapping of the OneFIT system building blocks to the underlying network

Different options for logical and physical connections of user equipment with infrastructure nodes and among themselves are shown in Figure 7. On a logical level we have 5 different types of C4MS connections:

- CI/OM_1 represents a logical connection between the cognitive management systems of user equipment and an infrastructure node. In this case, the user is requesting a specific application and directly benefits from the ON creation. This type of C4MS connection can also be used for required signalling between infrastructure nodes and users that are exchanging data among themselves in the context of an operator governed ad-hoc networking scenario;
- CI/OM_2 is a connection between cognitive management systems of user equipment that is requesting service and user equipment that acts as relay. This type of connection is needed for coverage and capacity extension scenarios and also for the access network traffic aggregation scenario;
- CI/OM_3 is a logical connection between the OneFIT cognitive management systems of relaying user nodes and infrastructure nodes. This type of connection is needed for the same scenarios as those mentioned under CI/OM_2;
- CI/OM_4 represents a logical connection between cognitive management systems of infrastructure nodes. This type of connection is needed in scenarios where ONs are created between user nodes and more than one infrastructure node or between infrastructure nodes only for backhaul resource aggregation (scenario 5 specific);
- CI/OM_5 depicts a logical connection between cognitive management systems of user nodes that are exchanging user data among themselves. This type of connection is needed for creation of ONs in order to support operator governed ad-hoc networking of user nodes (home networking).

All these logical connections are part of the C4MS protocol and can require different control messages and user data exchange. This will be further decided during the course of the OneFIT project.

In Figure 7 it is also depicted how the OneFIT system uses multi RAT capabilities of network nodes.

In the radio access part of the infrastructure network, the OneFIT system will be mapped onto all types of radio access devices: base stations (enhanced Node B), access points (WLAN 802.11a/b/g/n, WiMAX), femto-cells (Home enhanced Node B), etc. These devices will be able to trigger the ON suitability determination, to participate in the ON creation, to forward ON parameters to other network devices, to gather spectrum sensing and traffic monitoring data for cognitive systems and to participate in the ON termination process.

A WLAN controller is introduced in the access network in order to present the fact that the OneFIT system can also be established over 802.11 networks only (a controller can be connected to the WAN cloud directly). OneFIT building blocks are placed into the controller protocol stack if WLAN APs are “thin access points” which are only radio interfaces and all logic resides in the WLAN controller. In case of “thick APs”, the OneFIT logic can reside inside them and the WLAN controller will perform its basic functions.

Parts of the CSCI may also be located in a database in a public or an operator owned WAN cloud. Cognition related information may be stored in this data base and processed in coordination with the operator and regional/country wide policies and rules on spectrum usage, application provision, QoS requirements, etc. Results of this data processing step will be a set of predefined actions and instructions how the system should react to detected changes in the network environment. Also, responses to earlier encountered triggers for ON creation will be faster. CSCI is depicted as part of this database in order to represent the fact that this data base will be able to receive cognition

related information from CSCI blocks of other network nodes but will not be part of ONs (no CMON block).

3.3 Additional OneFIT system entities

The basic OneFIT system building blocks were introduced in the previous sections. However, for a successful ON lifecycle, additional system entities have to be introduced in close cooperation with cognitive management systems. If the OneFIT system is to be recognized and accepted by the network operators, it has to address specific demands for security, trust establishment, accounting and charging policies. Some of these policies can be legacy and some of them have to be introduced by OneFIT.

3.3.1 OneFIT system spectrum sensing and traffic monitoring

Efficient spectrum sensing and network monitoring techniques have to be used by the OneFIT system in order to enable fast and accurate gathering of cognition related data and to enable the system to, as fast as possible, react to dynamic changes in the network environment.

The following spectrum sensing techniques are to be considered: waveform-based sensing, cyclostationarity-based sensing, radio identification-based sensing, TV white space detection, cooperative sensing methods, etc.

One radio interface of the infrastructure nodes could be dedicated only for spectrum sensing on different frequencies. In this way, the system will have a most realistic picture of the current state of the target spectrum. User nodes could be performing spectrum sensing in pauses between data transmissions or in some other way but battery life of user equipment is the limiting factor. Dedicated hardware for sensing can be deployed in the network.

Network monitoring will be used for surveying traffic across radio links, detecting QoE (Quality of Experience for users) and QoS, network link utilisation and performance, etc. The monitoring can be Router based (SNMP, NetFlow, Remote monitoring, etc) or non-Router based (active (ping, traceroute) and passive).

Some new metrics will be used in order to address specifics of the OneFIT system performance evaluation. These metrics will address: link availability, packet delay, packet jitter, packet reordering, packet loss, bandwidth measurements (capacity, achievable throughputs).

3.3.2 OneFIT system security and trust concepts

During the ON suitability determination phase, the CSCI is responsible to check whether the requested (by application) level of security can be provided by the underlying layers (RAT). If security cannot be provided by underlying layers, then the CSCI/CMON and C4MS have to provide the requested level of security (trust establishment and data encryption) before the ON suitability phase results in positive answer.

The security and trust establishing system as used by the underlying RATs and/or the OneFIT building blocks shall include state of the art and legacy security protocols and mechanisms for trust establishment between different network nodes and encryption of exchanged data.

Specific concepts related to secure trust establishment between users and between users and infrastructure entities are:

- Certificate: This is a public key signed by a CA (Certification Authority). By signing a public key, a CA delivers a certificate, meaning that the CA certifies that an entity is who it says it is. When an entity sends his certificate to another entity, the receiver can validate the certificate checking it against the certificate of the CA;

- Public Key Infrastructure (PKI): a PKI is an architecture of authentication based on public-private keys and certification authorities;
- Identity: In PKI's context, an identity is supported by a certificate;
- Public Key: Every entity must have a public key that can be sent to other ones. If talking about authentication, a challenge could be used to authenticate the other end, checking the result of the challenge with the help of the public key. If talking about encryption, the public key of A could be used by others to encrypt information only wanted to be read by A;
- Private Key: Every entity must have a private key that always must be kept private. It is only used for authenticating itself, to calculate the result of a challenge, or for deciphering information ciphered before using his public key;
- Certification Authority (CA): It is the trustworthy point of the PKI. Every entity must trust the CA. The CA signs the certification requests made by other entities after a procedure of identification;
- Public-Private key pair: In PKI, every entity has a public and a private key.

Each node in the ON or in the infrastructure needs to be identified uniquely. There must be, for instance, a way to verify that an entity is what it says it is. A good starting point is to use a PKI infrastructure: there is a CA that signs every identity of each entity. An entity identifies itself to other entities by using its certificate (a public key that was signed by the CA). Each entity could verify the trust of an identity by checking its certificate against the certificate of the CA (every entity must have a copy of the CA's certificate).

Every node will have a certificate (public key signed by the CA) and a private key. The private key will be used to sign packets of the protocol (to certify the issuer of the message). The public key will be used by other entities to verify the sender of a message.

After the first access of the device to the infrastructure, it is associated a temporary identity (for instance, a new public-private key with a random validity period). This will protect the device against spoofing threats and external unauthorized identification.

3.3.2.1 Protection of private data

A security function located typically at the interface between the application layer and the infrastructure must provide functionalities to cipher those data packets as instructed by the application level. The application would only concern about which of the data elements must be protected, but not how they are protected or which algorithm has been used to do that.

The protocols used for the management of opportunistic networks shall support integrity, e.g. by inclusion of an integrity check signature in those messages where needed. This signature should be based on a key and the contents of the message, and the key should be known only by those devices involved in the communication (sender, receiver and, probably, intermediates of the communication).

The integrity mechanism used should be such that a device couldn't be a target of a Denial of Service attack. The calculation of such integrity signatures should involve an appropriate amount of processing power (limited as it is in mobile devices).

3.3.2.2 Protection of user identity

User and node identity must be different. Applications should be able to know a temporary identifier of the identity of the user, but not the real identity of him. Although the infrastructure knows the real identity, the application would use an alias or a temporary identifier. It is up to the user whether

he wants to use a real identity or an alias for each application or service.

3.3.3 OneFIT system security and trust implementation options

Three solutions have been identified as possible implementation options to support the security requirements for the OneFIT system:

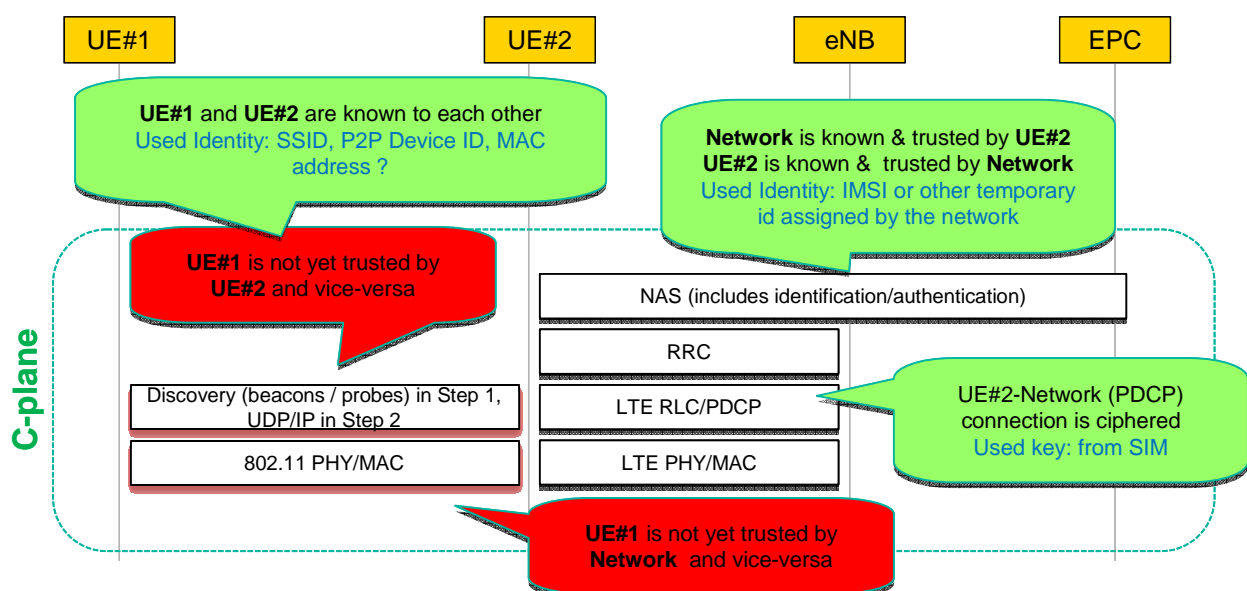
- 1- An implementation based on the existing mechanisms specified in 3GPP RAN and EPC [11][7] for providing services to “native” 3GPP mobile devices and users
- 2- An implementation based on existing mechanisms specified by 3GPP to deal with untrusted non-3GPP accesses [8][9] to the EPC services by devices/users typically making use of operator-managed WLAN Access Points
- 3- An overlay of security, built for the management of ON and making no assumption on underlying security provided by RATs

3.3.3.1 Solution “trusted 3GPP”

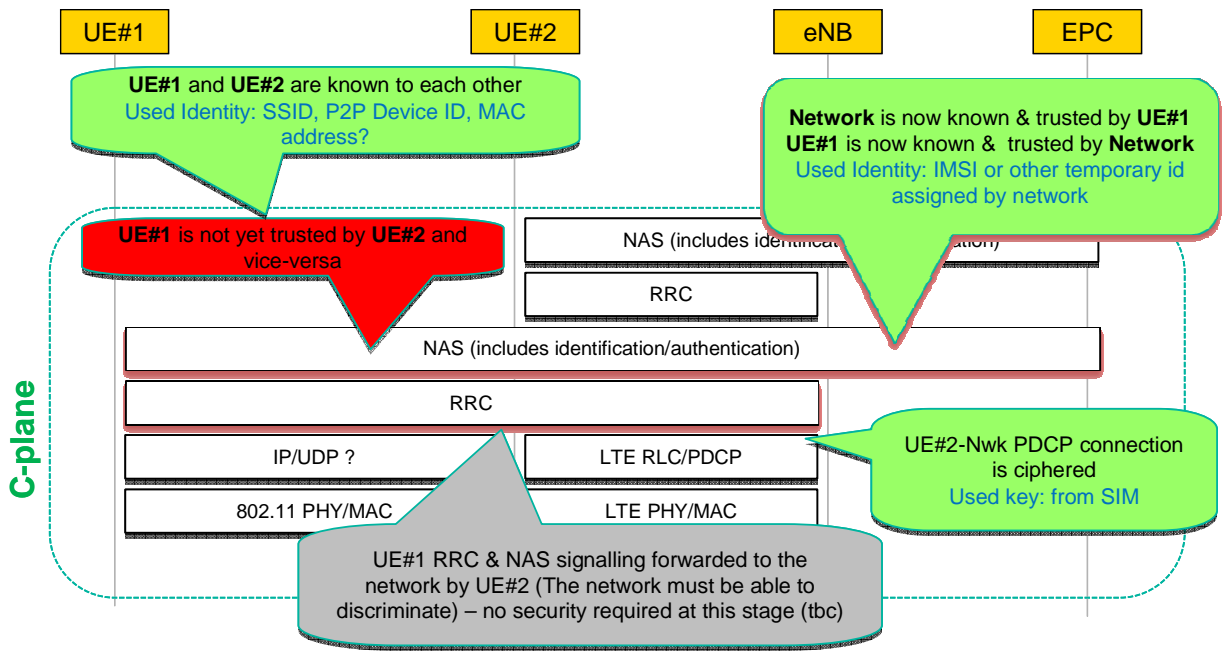
In this solution the “trusted” 3GPP mechanisms” [11][7] of authentication/ciphering are applied to all ON members, regardless of the RAT in use.

The example below shows the application of these mechanisms to the opportunistic coverage extension scenario: UE#1 is out of the coverage of the infrastructure, while UE#2 is connected to the RAN/EPC.

Step1: UE#1-UE#2 Discovery & Step2: UE#1-UE#2 Basic link establishment



Step3: UE#1-Network registration



Step4: UE#1-Network ciphering and u-plane flow start

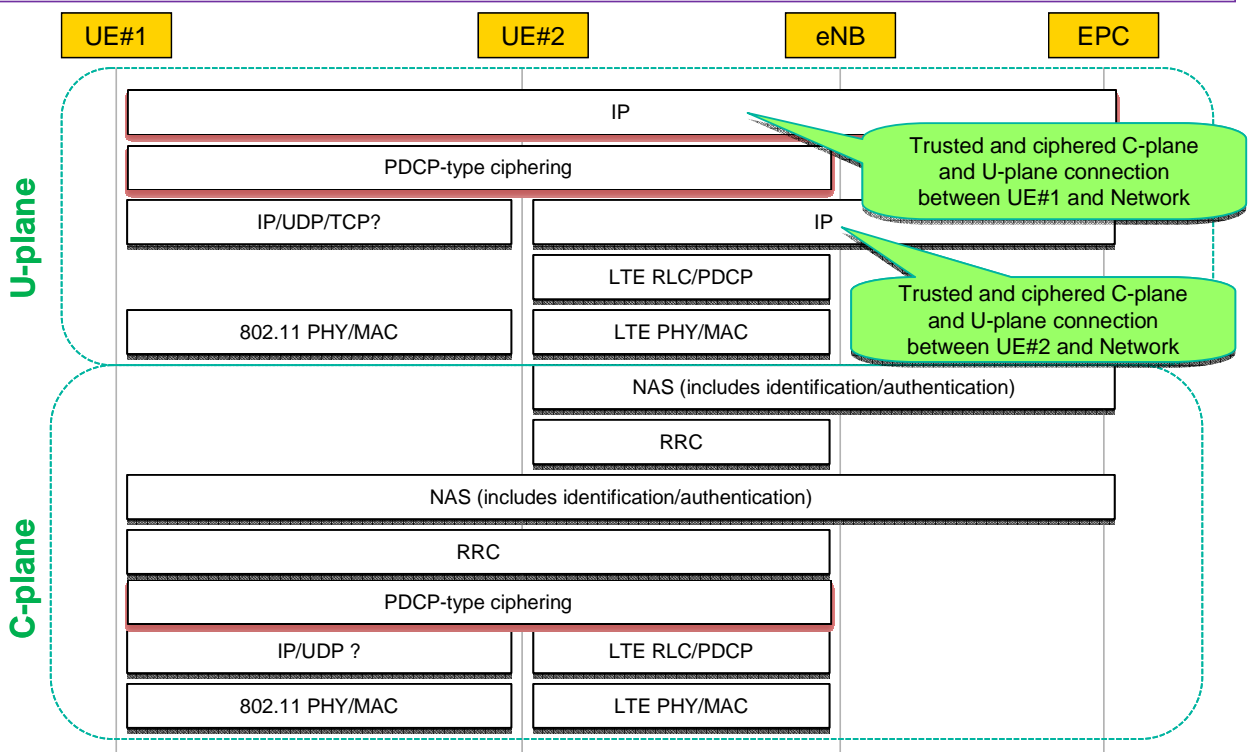


Figure 8: Establishing security and trust between two UEs by using 3GPP procedures

3.3.3.2 Solution “untrusted non-3GPP”

In this solution the mechanisms applied are the ones defined for untrusted non-3GPP access [8][9], regardless of the RAT in use.

3.3.3.3 Solution “Overlay”

In this solution, the system has an overlay of security, built for the management of ONs and making no assumption on the underlying security provided by the RATs. For this solution, a security layer must be inserted between the application and the underlying RATs in order to provide security for the user data. However, due to the effort for this solution and due to the availability of security in existing networks, it is preferred to re-use existing security functions in the underlying RATs.

3.3.4 OneFIT system accountability, charging and billing

The OneFIT system shall base its accounting and charging on operator policies. A special rewarding system for relaying user nodes will be introduced [2].

The rewarding system could be based on functionalities of the Policy and Charging Control (PCC) for non-3GPP accesses delivered by the EPC. According to [6], the PCC shall support charging models based on the volume of transmitted data, time, events, etc. One of the features of particular interest to OneFIT is the support for the “shared revenue services” for which “settlement for all parties shall be supported, including the third parties that may have been involved providing the services”. The implementation of PCC would then enable the realization of the business model in which relaying nodes receive a pay-off for providing the relaying services.

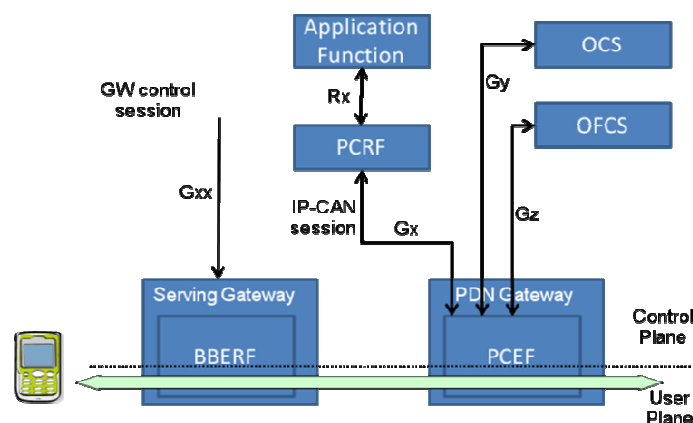


Figure 9: Policy and Charging Control (PCC) [6]

The realization of the EPC/PCC based rewarding system would require:

- Identification if a user is participating in an ON
- Identification if a user is providing support to other users, e.g. by relaying traffic of other users (type of support, amount of relayed data, etc.)
- Type of rewarding scheme the user is participating in
- Minor system modifications as described in more detail below

The introduction of the EPC based rewarding requires all the participants to be authenticated and authorized within the EPC. This can be achieved by enforcing all ON nodes that need traffic relaying to consider potential relays (i.e. other ON nodes) as untrusted non-3GPP IP access and follow the attachment procedure specified in [8] to connect and authenticate within the EPC. The alternative approach would be here to consider the relaying nodes as trusted non-3GPP IP access but due to the

security reasons and terminal complexity it was decided not to consider this approach (the relaying terminal in such a case would be additionally responsible for mobility management and authentication process).

The minor system modifications mainly concern the Evolved Packet Data Gateway (ePDG) and are necessary to allow the ePDG to be responsible for:

- Obtaining the identity of the relaying node – the procedure is required as the EPC system needs to know which user should receive the reward for providing the relaying service.
- Confirming the successful authentication of the node requesting the access to the relaying node – the procedure is required as the relaying UE needs to know if it should allow the requesting UE to transmit data. It is worth noting here that the concept is based on the assumption that the relaying node allows for an initial access to enable the authentication of the requesting node within the EPC (the relaying node could have a list of ePDG addresses and thus determine if the requesting UEs tries to access ePDG to authenticate within EPC or access other address).
- Modification of the PCC policies for the relaying node – the procedure is necessary in case the relaying UE is charged for the amount of transferred data (the procedure could decrease the charging rate, etc.).

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.

Having the identity of the user which relays the data (determined by the ePDG) and the identity of the user which requested the access, the charging system can determine the amount of transferred data (EPC monitors the amount of transferred information in the PDN Gateway) and accordingly reward the relaying user using the concept of the “shared revenue services”. It is worth noting here that the employment of the “share revenue services” concept in such a scenario may require some changes in the existing Online or Offline Charging System implementation.

4. Control Channels for the Cooperation of the Cognitive Management System (C4MS)

The exchange of information, knowledge and commands between the different CMON instances as well as between different CSCI instances relies on control channels. These “Control Channels for the Cooperation of the Cognitive Management System” C4MS can be seen as a combination and extension of the Cognitive Pilot Channel (CPC) [5] concept and the Cognitive Control Channel (CCC) concept [17].

The CPC is a (logical and optionally in part a physical) channel, which provides information from the network to the terminals, e.g. on frequency bands, available Radio Access Technologies, and spectrum usage policies. Therefore, the CPC is a basis for the coordination between infrastructure and opportunistic networks, especially the bi-directional in-band CPC. While a downlink-only CPC can provide e.g. start-up information to all terminals in a cell, a bi-directional CPC can reply to requests for terminals. The focus of the C4MS is on the bi-directional communication.

The CCC is a logical channel transporting information on top of a physical channel as e.g. provided by the Cognitive Control Radio (CCR)[17] for the peer-to-peer exchange of cognition related information between heterogeneous network nodes (e.g. between terminals).

In retrospect, the C4MS is expected to provide a common framework integrating both concepts and thus enable communication between terminals as well as between terminals and infrastructure networks (the employed mechanisms could be RAT specific or/and be RAT-independent). Additionally, C4MS should provide functionalities originally defined for CPC and CCC/CCR. These functionalities include:

- providing 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
- providing means for enabling the coexistence and coordination among different networks and devices

The basic set of functionalities inherited from the CPC and CCC/CCR concepts is to be further extended with the following OneFIT specific functionality:

- providing means for enabling the management of Opportunistic Networks

The OneFIT specific functionality makes the C4MS responsible for managing the information exchange between OneFIT functional entities located in different physical entities. In addition, the C4MS could be used to provide coordination and coexistence of different networks and devices.

The following subsections give a brief introduction to C4MS by presenting the potential services and considered C4MS components for enabling the exchange of signalling, context and policy information in heterogeneous environments.

As shown in Figure 10, different transport options are under consideration for the C4MS. The C4MS messages can be transported over IP in order to be radio access technology independent or directly over MAC or RRC [10] messages in order to enable discovery procedures or communication before an IP connection is established.

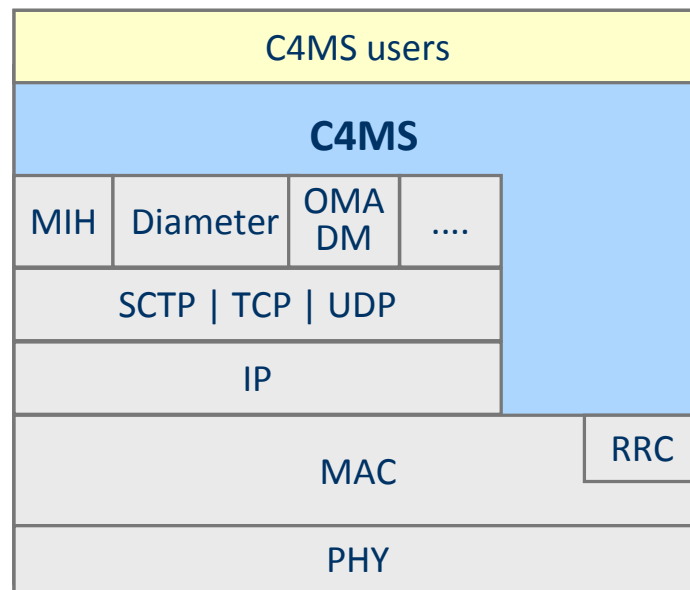


Figure 10: C4MS – general view

For the IP based transport, several options are under evaluation. These include using the 802.21 Media Independent Handover (MIH) mechanisms [12], using the IETF Diameter protocol [13] or the OMA DM Framework [14] as used by 3GPP for the Access Network Discovery and Selection Function (ANDSF) [8].

The C4MS implementation options will be further analysed in [3].

4.1 C4MS layer

The C4MS can be seen as an intermediate layer between C4MS users and the network protocol stack (see Figure 11 below) whose main role is to enable and coordinate the exchange of information between C4MS users located in different nodes. The C4MS is envisioned to enable C4MS information to be transported over different transport mechanisms (e.g. RRC, OMA DM, MIH protocol), over different layers (L2, L3 and above).

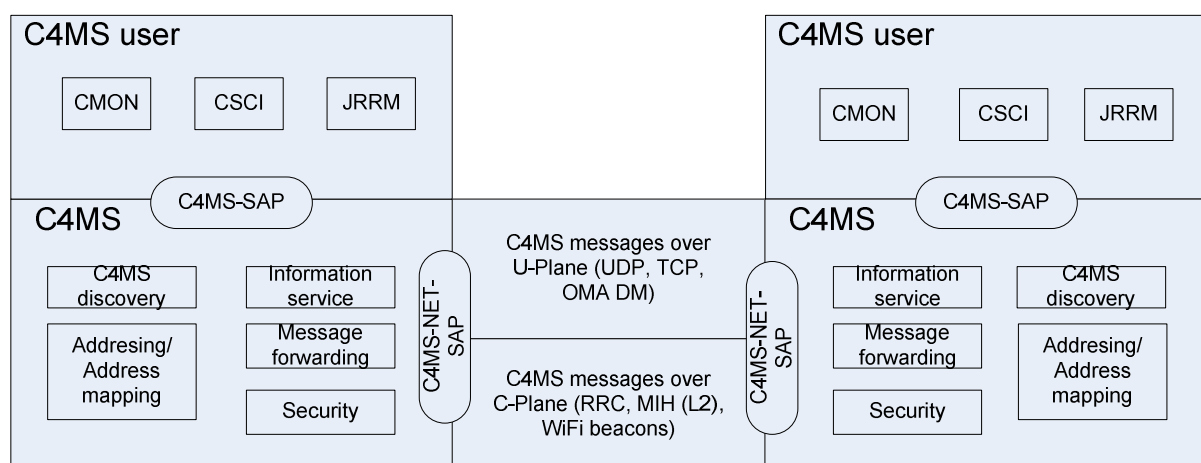


Figure 11: C4MS reference model

4.1.1 C4MS services

In order to enable the exchange of information between different C4MS users, five different services have been identified as necessary:

- Information delivery
- C4MS discovery
- Addressing/Address mapping
- Security
- Message forwarding/Routing

Information delivery: provides a framework and encompasses mechanisms responsible for the information exchange between C4MS users. It supports information pull and push modes (requests/response and notification). It allows different types of information to be exchanged (e.g. commands, events or decisions). It allows for the delivery of information in a unicast, multicast and broadcast manner.

C4MS discovery: enables discovering other C4MS users (on the terminal and network side) in case the necessary information is not provided by the lower layers (e.g. no extra information enabling discovery transmitted over beacons). Two different types of discovery mechanisms are to be supported by the C4MS: active and passive. The active discovery is based on sending ON capability requests (probes or multicast/broadcast messages) and monitoring for the ON capability responses. The passive discovery is based on passive monitoring and requires that C4MS users periodically broadcast information about their existence and their capabilities.

Addressing/Address mapping: enables determination of the correct lower layer address of the remote C4MS user (e.g. IP address and port number). This mechanism is necessary as different underlying layers can be employed for the transmission of C4MS data. The mechanism maintains a list of addresses of remote C4MS users (along with their lower layer addresses).

Security: provides means for establishing a secure connection between C4MS users belonging to the same ON. It supports mechanisms for encrypting and authenticating the exchanged messages as well as establishing a mutual authentication along with cryptographic key negotiation between C4MS users.

Message forwarding/Routing/Proxying: enables exchange of messages between C4MS users which are not directly connected (in case necessary mechanisms are not provided by the underlying layers). It allows for the concurrent employment of heterogeneous transportation mechanisms/protocols.

4.1.2 C4MS protocols

C4MS may define and support several protocols to enable information exchange between C4MS users. The protocols define message formats, including a message header and message parameters and are envisioned to provide sufficient flexibility to be transmitted over different transport mechanisms. In order to provide the reliable delivery over different transport mechanisms, the C4MS protocols will enable different modes of operation:

- Acknowledged Mode – each message needs to be acknowledged
- Unacknowledged Mode – messages does not require acknowledgments

A first set of messages has been identified for the C4MS. This messages which will be used in the message sequence charts in section 5 are:

- ON_Suitability.Indication
- ON_Discovery.Request, ON_Discovery.Answer
- 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 (ON_Negotiated, ON_Established, ON_Released)
- Spectrum_Assignment.Request, Spectrum_Assignment.Answer

4.1.3 C4MS Service Access Points

In order to enable to information exchange between C4MS users, two distinct Service Access Points (SAPs) were identified:

C4MS_SAP is a media independent SAP that provides uniform interface for C4MS users to access services delivered by C4MS. Among others, the C4MS_SAP should support generic mechanisms for the message to be sent and received.

C4MS_NET_SAP is a media dependent SAP that provides transport services over the data/control plane of the underlying layers, supporting the exchange of C4MS information and messages with the remote C4MS users. Among others, the C4MS_NET_SAP should also support C4MS discovery.

The location of these SAPs is shown in the C4MS reference model in Figure 11.

4.2 C4MS user

The C4MS user can be defined as a functional entity which uses the services provided by the C4MS entity in order to exchange the information with other C4MS users located in remote nodes. In order to access services provided by the C4MS entity, the C4MS user is required to register within its local C4MS logical entity. The two main users considered for the C4MS are CMON and CSCI, however, other functions like JRRM can also make use of the C4MS.

5. Message Sequence Charts

This section shows message sequence charts for the different OneFIT scenarios. A separation is made between high-level Message Sequence Charts (MSCs) showing only the different nodes in the network (e.g. UE, BS) and detailed MSCs showing the details inside each node (e.g. CMON, CSCI, JRRM, RAT). As shown in Figure 12, different colours are used to differentiate between the different interfaces.

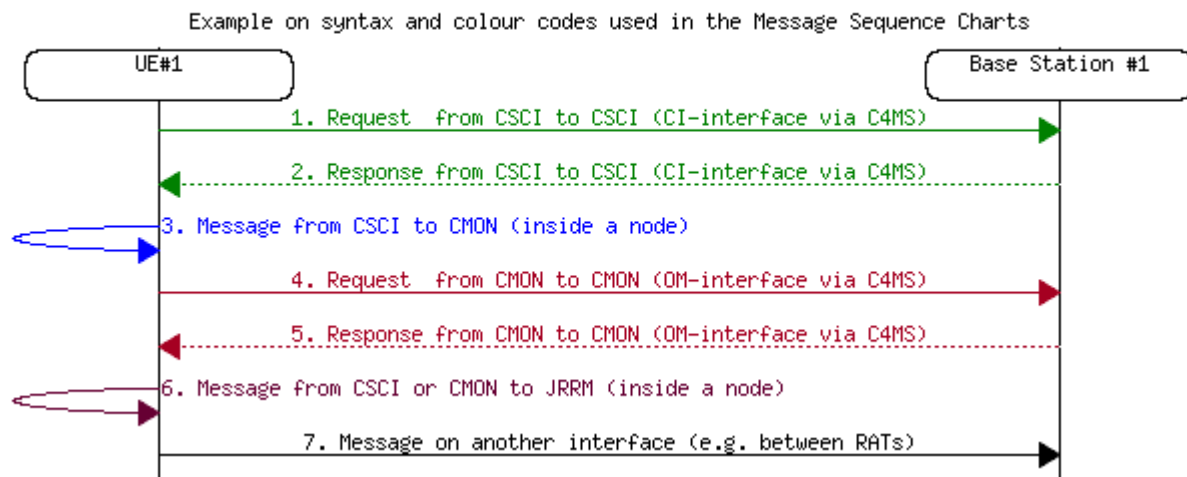


Figure 12: Syntax and colour codes used in the Message Sequence Charts

5.1 MSCs on Opportunistic coverage extension

Scenario 1 “Opportunistic coverage extension” describes a situation in which a device (here: UE#1) cannot connect to the network operator’s infrastructure, due to lack of coverage or a mismatch in the radio access technologies. In order to provide mobile access to UE#1, another node must provide a relaying service towards the infrastructure. Therefore, an ON is created. In the example shown in Figure 13, the ON consists of 3 nodes: UE#1, UE#2 (which provides the relaying service) and BS#1.

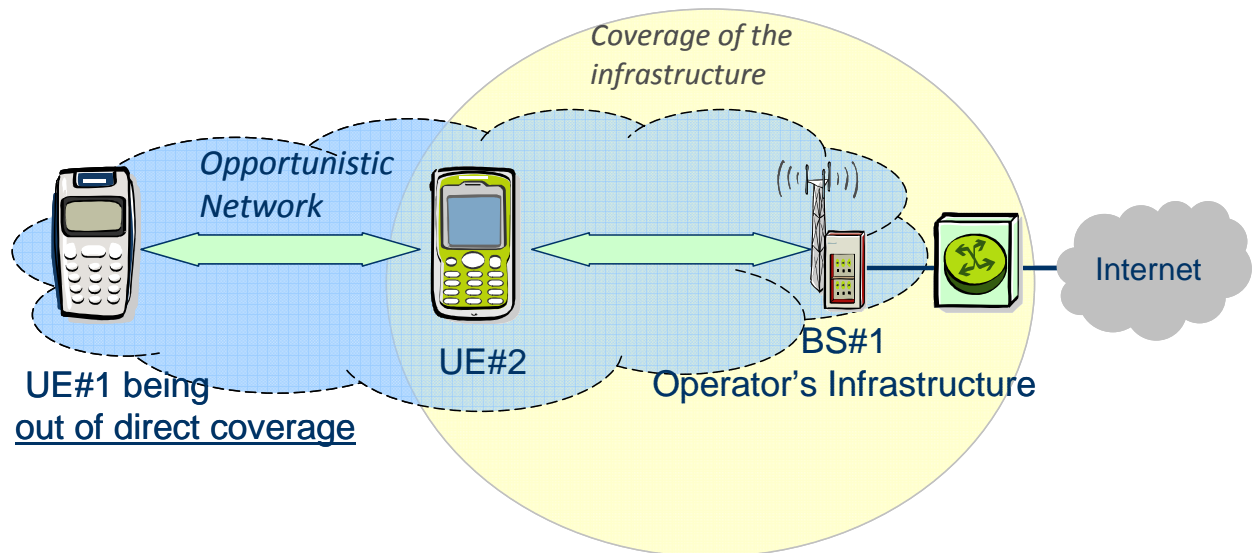


Figure 13: Example for Scenario 1: Opportunistic coverage extension

The MSC for this scenario is shown in Figure 14. After UE#1 has detected that it is out of coverage of the infrastructure, it decides to check the suitability of the creation of an ON. UE#1 discovers that UE#2 is in its vicinity and supports opportunistic networking. Thus, an ON is created and UE#1 is connected via UE#2 towards the base station BS#1.

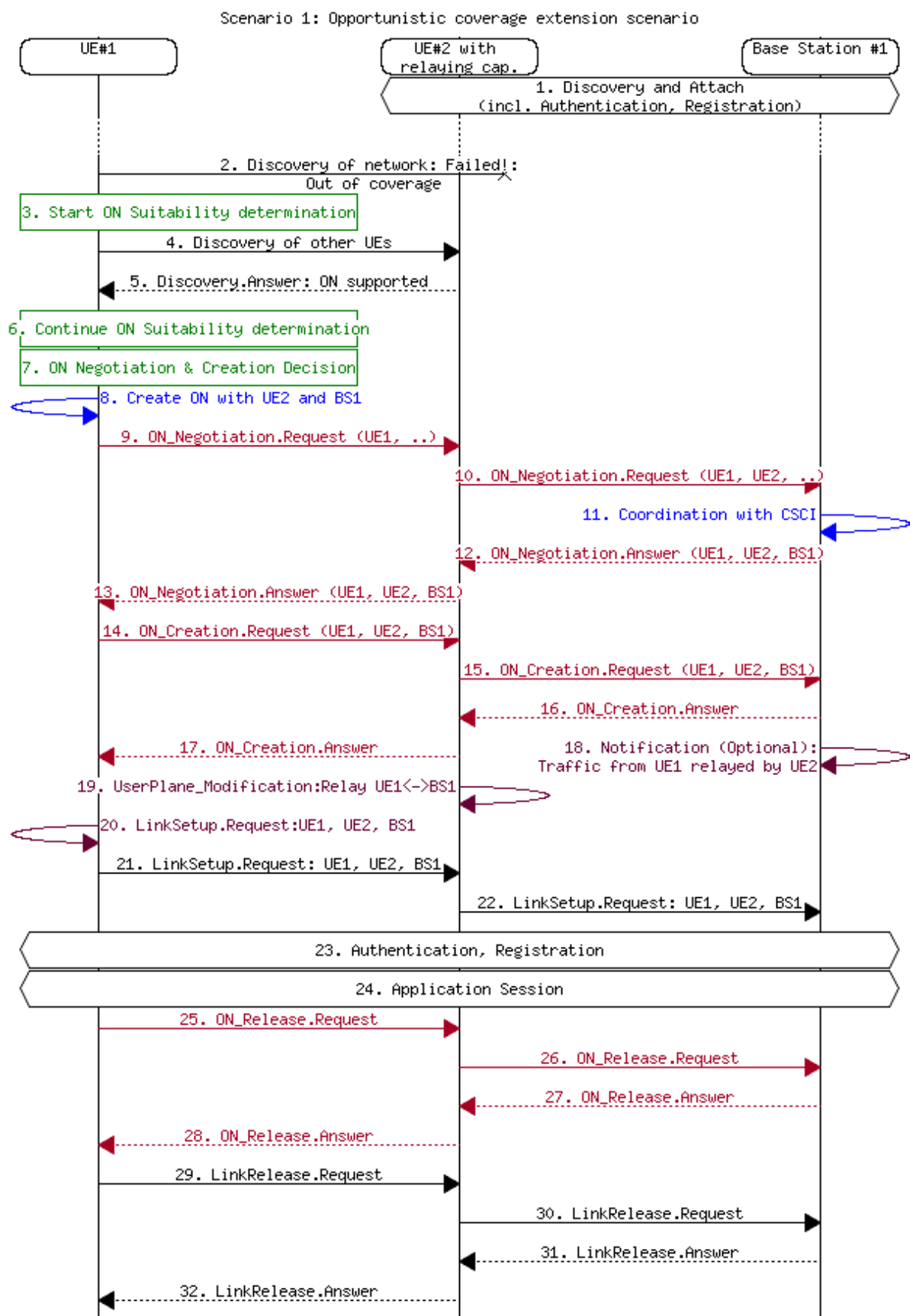


Figure 14: High-level MSC for Scenario 1: Opportunistic coverage extension

While Figure 14 shows the high-level MSC, a more detailed MSC including the node internal functions CSCI, CMON, JRRM and RAT is shown in Figure 15. Both MSCs use the same numbering for the messages, although some messages (e.g. message 2 in Figure 14) are splitted into several messages (e.g. messages 2, 2.1 and 2.2 in Figure 15). The following description of the messages is valid for both figures:

1. The UE#2 discovers the infrastructure network (e.g. by detecting signals from the broadcast channel or beacons sent out by BS#1) and attaches to the network. This procedure includes authentication and registration.
2. UE#1 initiates the discovery procedure. However, as the UE#1 is out of the coverage of the infrastructure, not broadcast signals or beacons are received. The information that there is no network discovered ("NoConnectivity.indication" in Figure 15) is sent via the JRRM towards the CSCI.
3. As the discovery procedure has failed, the CSCI in UE#1 decides to start the ON suitability determination.
4. The UE#1 initiates a discovery procedure towards other terminals. This may e.g. be done by sending probe requests or by listening to beacons from ad-hoc networks.
5. The UE#2 sends an answer to the discover request indicating that it supports ONs. Instead of an answer like answering a probe request, this could also be another message like a beacon or a broadcast message.
6. The CSCI in UE#1 continues the ON suitability determination.
7. After the CSCI in UE#1 has decided that an ON may be suitable, a decision is made that an ON shall be created.
8. The CSCI triggers the CMON in UE#1 to start the negotiation and creation of an ON. This message includes information that UE#2 shall be part of the ON.
9. An ON_Negotiation.Request including the capabilities and requirements from UE#1 is sent from UE#1 to UE#2 via C4MS.
10. UE#2 adds its own context information to the ON_Negotiation.Request and sends this message to BS#1.
11. Inside BS#1, the CMON coordinates with the CSCI in order to provide additional information from the infrastructure to the negotiation procedure. This procedure may additionally include interactions with the DSM in order to find appropriate frequencies for the ON (The interactions with the DSM are not shown in the diagram).
12. The BS#1 evaluates the ON_Negotiation.Request and sends an ON_Negotiation.Answer including a list of nodes (UE#1, UE#2 and BS#1) which should form the ON.
13. The ON_Negotiation.Answer is forwarded by UE#2 to UE#1. From the negotiation procedure, the UE#1 has now all relevant information from the involved nodes.
14. The ON_Creation.Request is sent via C4MS from the CMON in UE#1 to the CMON in UE#2.
15. The ON_Creation.Request is forwarded to BS#1.
16. The BS#1 sends an ON_Creation.Answer indicating that it is now included in the ON.
17. The UE#2 forwards the ON_Creation.Answer with an additional indication that UE#2 is now also part of the ON to UE#1.

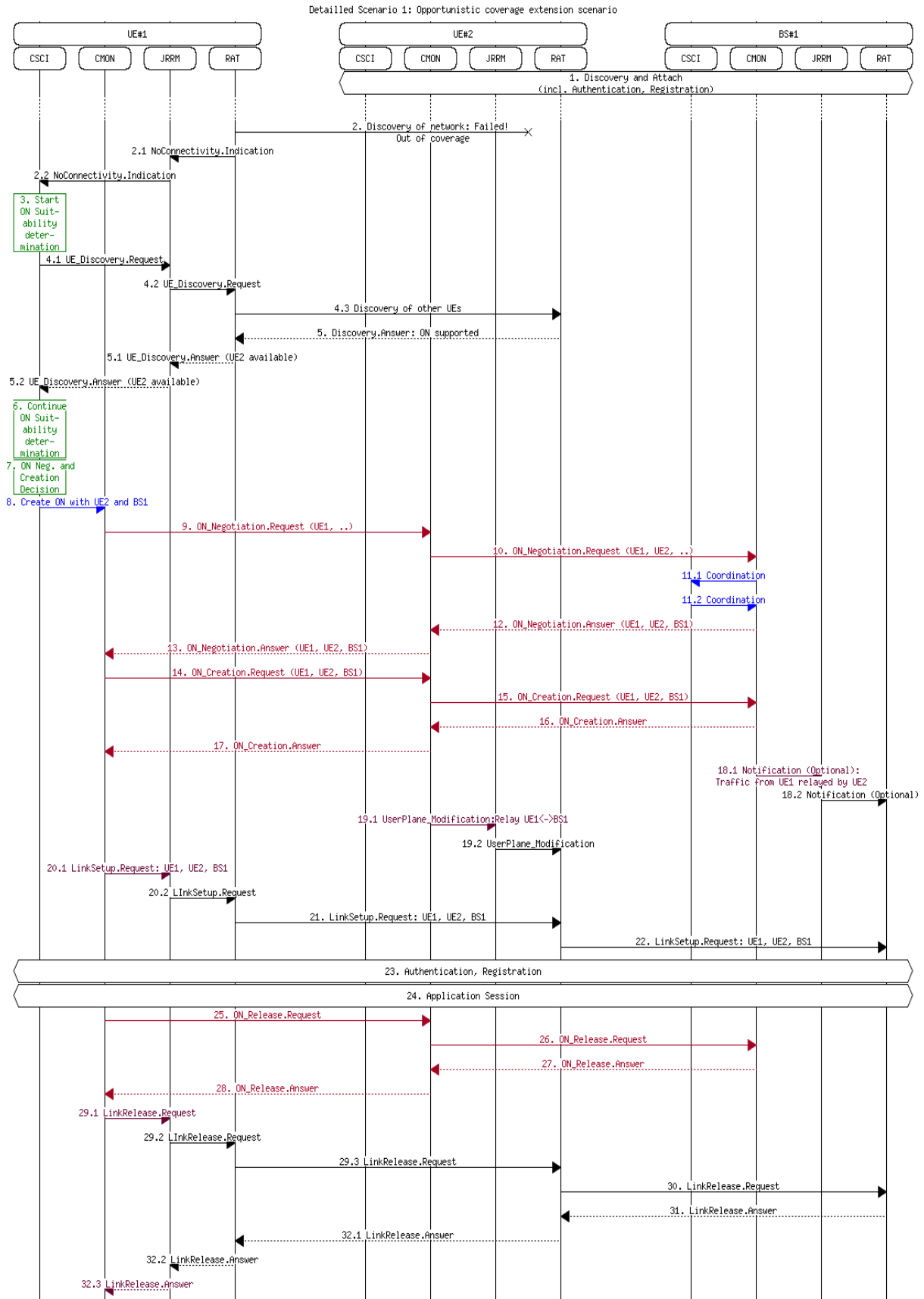


Figure 15: Detailed MSC for Scenario 1: Opportunistic coverage extension

18. If needed, the transceiver in BS#1 is configured to be able to receive traffic from UE#1 via UE#2.
19. UE#2 configures its transceiver so that traffic from UE#1 can be forwarded/relayed to BS#1 and vice versa.
20. The CMON in UE#1 initiates the setup of the user plane related radio link via the JRRM towards the underlying RAT.
21. A RAT-specific LinkSetup.Request is sent towards UE#2. In UMTS or LTE for example, this message may be a RRC Connection.Request.
22. A radio link setup or a modification of the existing link is also initiated between UE#2 and BS#1.
23. RAT-specific Authentication and Registration procedures are now being executed.
24. The Application Session is now active. At this point, radio link configurations between UE#1 and UE#2 and UE#2 and BS#1 can be modified (i.e., ON reconfiguration procedure) attending to the characteristics of the application/session being supported.
25. When the application session has ended, the CMON determines that the ON is no longer needed and an ON_Release.Request is sent from UE#1 to UE#2.
26. UE#2 forwards the ON_Release.Request to BS#1
27. BS#1 answers that the ON can be released.
28. UE#2 forwards the ON_Release.Answer to BS#1.
29. The CMON in UE#1 sends a LinkRelease.Request via JRRM towards the underlying RAT and a RAT-specific LinkRelease.Request (e.g. RRC Connection Release in UMTS) is sent to UE#2-
30. The RAT-specific LinkRelease.Request is forwarded to BS#1.
31. The BS#1 releases all resources and sends a RAT-specific LinkRelease.Answer to UE#2
32. The UE#2 releases all resources and sends a RAT-specific LinkRelease.Answer to UE#1. The UE#1 then also releases all its resources and informs the CMON. The ON is then released.

5.2 MSC on “Opportunistic capacity extension”

Scenario 2 “Opportunistic capacity extension” depicts a situation in which a part of the network (e.g. BS#1 in Figure 16) is highly loaded. Therefore, only limited service can be provided to a user at the cell edge (e.g. UE#1). As other parts of the network are less loaded (BS#2), the solution is to create an ON consisting of UE#1, UE#2 and BS#2. In that ON, UE#2 provides a relaying service between UE#1 and BS#2 and thus satisfactory QoS can be provided to UE#1.

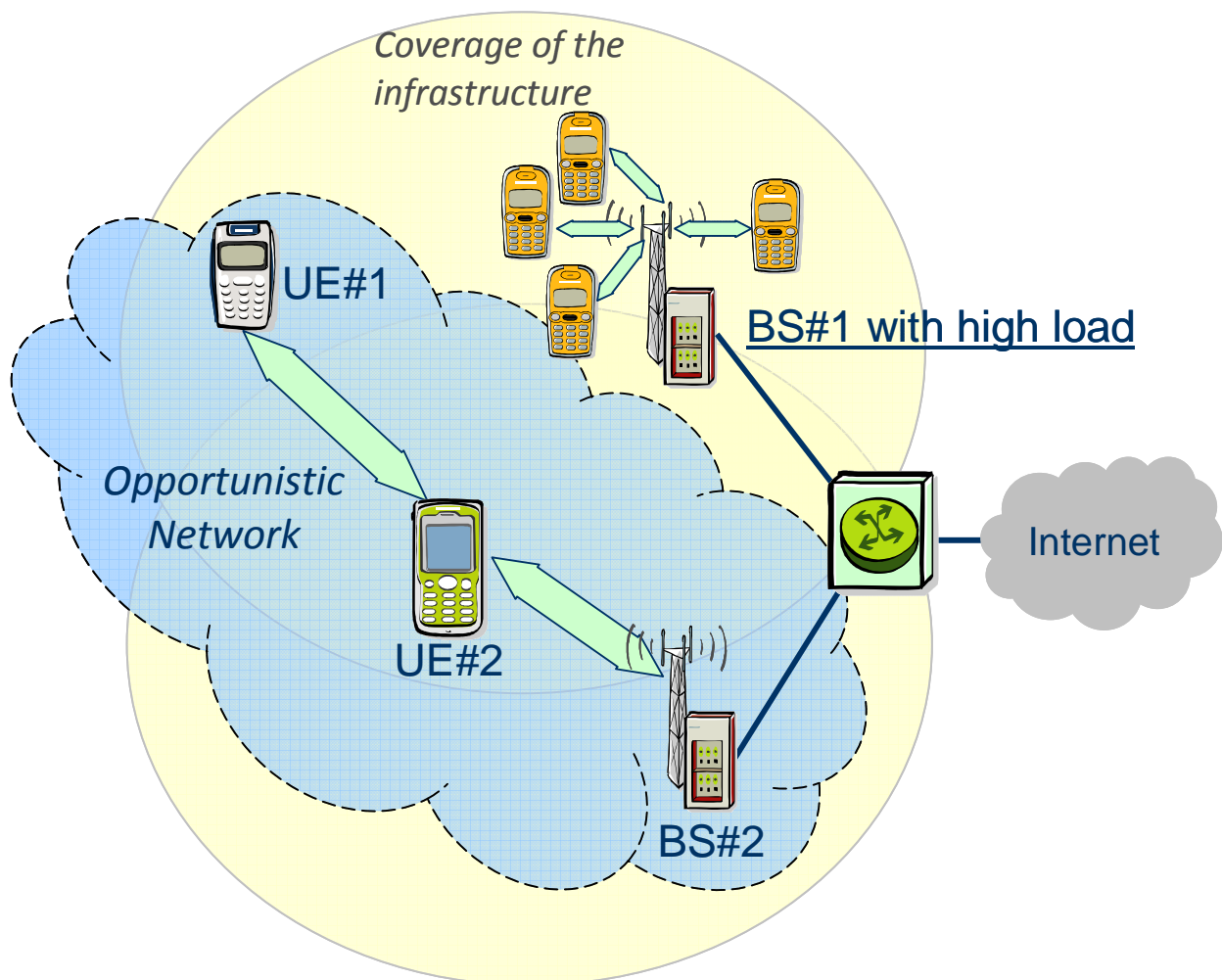


Figure 16: Example for Scenario 2: Opportunistic capacity extension

The MSC for this scenario is shown in Figure 17. There, UE#1 is first attached to the base station BS#1 while UE#2 is attached to BS#2. UE#1 established an application session but due to the fact that BS#1 in this example is highly congested, the provided QoS is insufficient. In order to improve the QoS, the UE#1 decides to check if an ON can be created. Alternatively, as the network (BS#1) is also aware of the insufficient QoS, the network may also trigger the check if an ON shall be created.

UE#1 discovers that UE#2 is in its vicinity and supports opportunistic networking, thus an ON is created between UE#1 and UE#2. After handover execution, the traffic from UE#1 is then relayed via UE#2 towards base station BS#2.

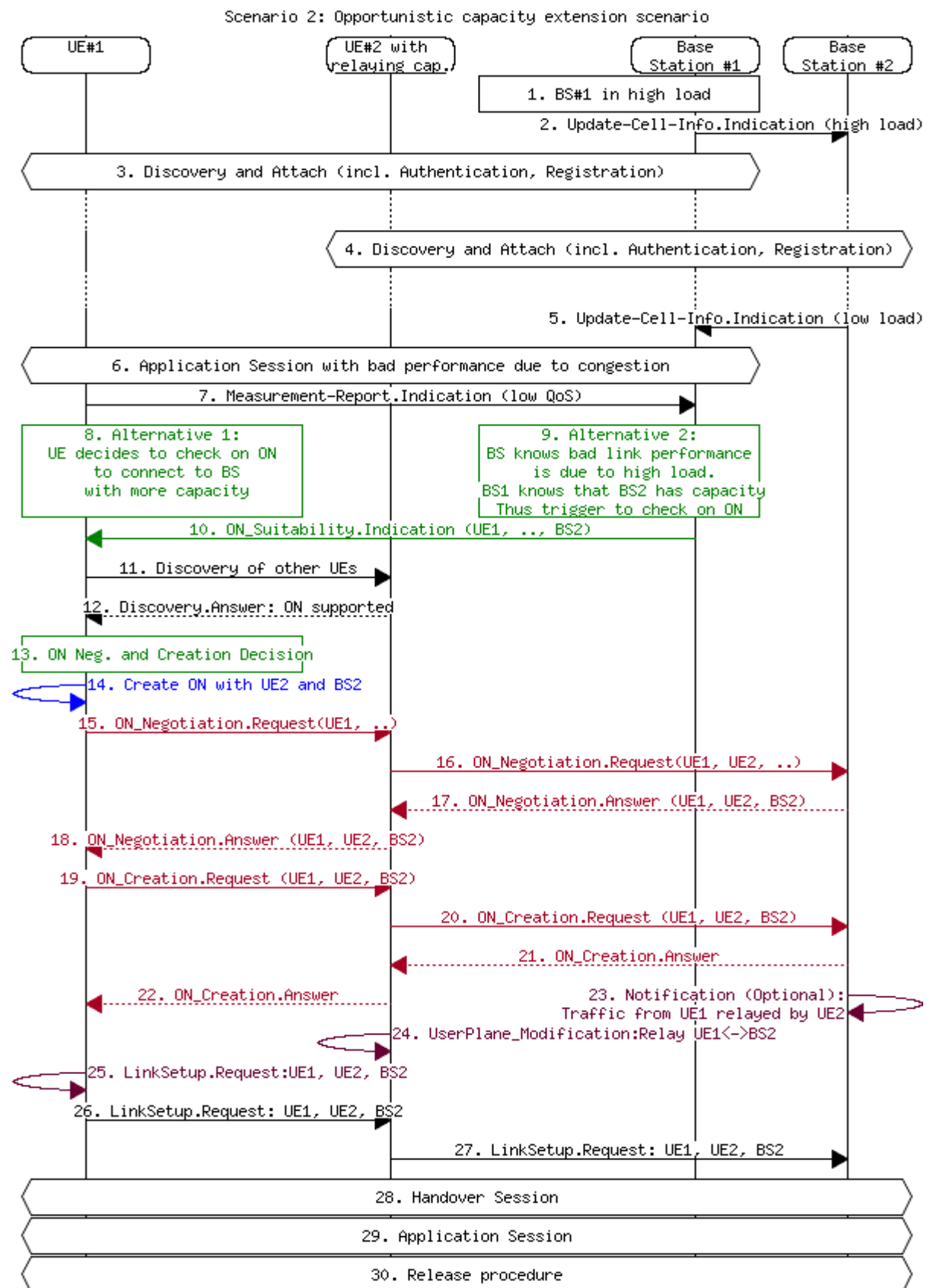


Figure 17: High-level MSC for Scenario 2: Opportunistic capacity extension

Description of the Messages used in Figure 17:

1. At the beginning of the scenario, the BS#1 is already in high load because BS#1 serves already several other users which are not shown in the MSC.
2. The BS#1 informs regularly its surrounding Base Stations, e.g. BS#2 about its load situation.
3. The UE#1 discovers and attaches to the network (via BS#1). This procedure includes authentication and registration.
4. The UE#2 discovers and attaches to the network (via BS#2). This procedure includes authentication and registration.
5. In the infrastructure network, cell load indications are regularly exchanged. Here, BS#2 informs BS#1 that it is in a low load situation.
6. UE#1 starts an application session.
7. Due to the high load in the cell of BS#1, the UE#1 experiences bad performance. A measurement report is sent to BS#1 indicating the low QoS.
- 8./9. Two options are possible on which node reacts first to improve the bad performance situation:
 - The UE#1 may decide to check if an ON can be created.
 - Alternatively, the BS#1, which has more context information about the network, e.g. that BS#2 is suitable due to its low load, can also trigger the creation of the ON.
10. In Alternative 2, the BS#1 sends an ON_Suitability.Indication to UE#1 indicating that BS#2 has been identified as a candidate for the creation of a new ON.
11. As UE#1 is out of coverage of BS#2, it has to discover other network elements or UEs which can be part of the ON.
12. UE#2 provides information that it is supporting ONs. This can either be a dedicated message or some broadcasted information.
13. The CSCI in UE#1 decides that the ON shall now be created.
14. The CSCI triggers the CMON in UE#1 to start the creation of an ON including UE#1, UE#2 and BS#2.
15. An ON_Negotiation.Request including the capabilities and requirements from UE#1 is sent from UE#1 to UE#2.
16. UE#2 adds its own context information to the ON_Negotiation.Request and sends this message to BS#2. At this point, the CMON in BS#2 may coordinate with the CSCI in BS#2 in order to provide additional information from the infrastructure to the negotiation procedure.
17. The BS#2 evaluates the ON_Negotiation.Request and sends an ON_Negotiation.Answer including a list of nodes (UE#1, UE#2 and BS#2) which should form the ON.
18. The ON_Negotiation.Answer is forwarded by UE#2 to UE#1.
19. The ON_Creation.Request is sent via C4MS from the CMON in UE#1 to the CMON in UE#2.
20. The ON_Creation.Request is forwarded to BS#2.
21. The BS#2 sends an ON_Creation.Answer indicating that it is now included in the ON.
22. The UE#2 forwards the ON_Creation.Answer with an additional indication that UE#2 is now also part of the ON to UE#1.
23. If needed, the transceiver in BS#2 is configured to be able to receive traffic from UE#1 via UE#2.

24. UE#2 configures its transceiver so that traffic from UE#1 can be forwarded/relayed to BS#2 and vice versa.
25. The CMON in UE#1 initiates the setup of the radio link for the user plane (or modification of an existing radio link) via the JRRM towards the underlying RAT.
26. A RAT-specific LinkSetup.Request is sent towards UE#2. In UMTS or LTE for example, this message may be a RRC Connection.Request.
27. A radio link setup or modification of the existing one is also initiated between UE#2 and BS#1
28. RAT-specific Session Handover procedures are now being executed.
29. After the handover, the session is continued with improved QoS.
30. After the end of the session, a release procedure is executed. This procedure is similar to the detailed release procedure described in the previous scenario described in section 5.2.

5.3 MSCs on Infrastructure supported opportunistic ad-hoc networking

Scenario 3 “Infrastructure supported opportunistic ad-hoc networking” shows the creation of an infrastructureless opportunistic network between two or more devices for the local exchange of information (e.g. peer-to-peer communications, home networking, location-based service providing, etc.).

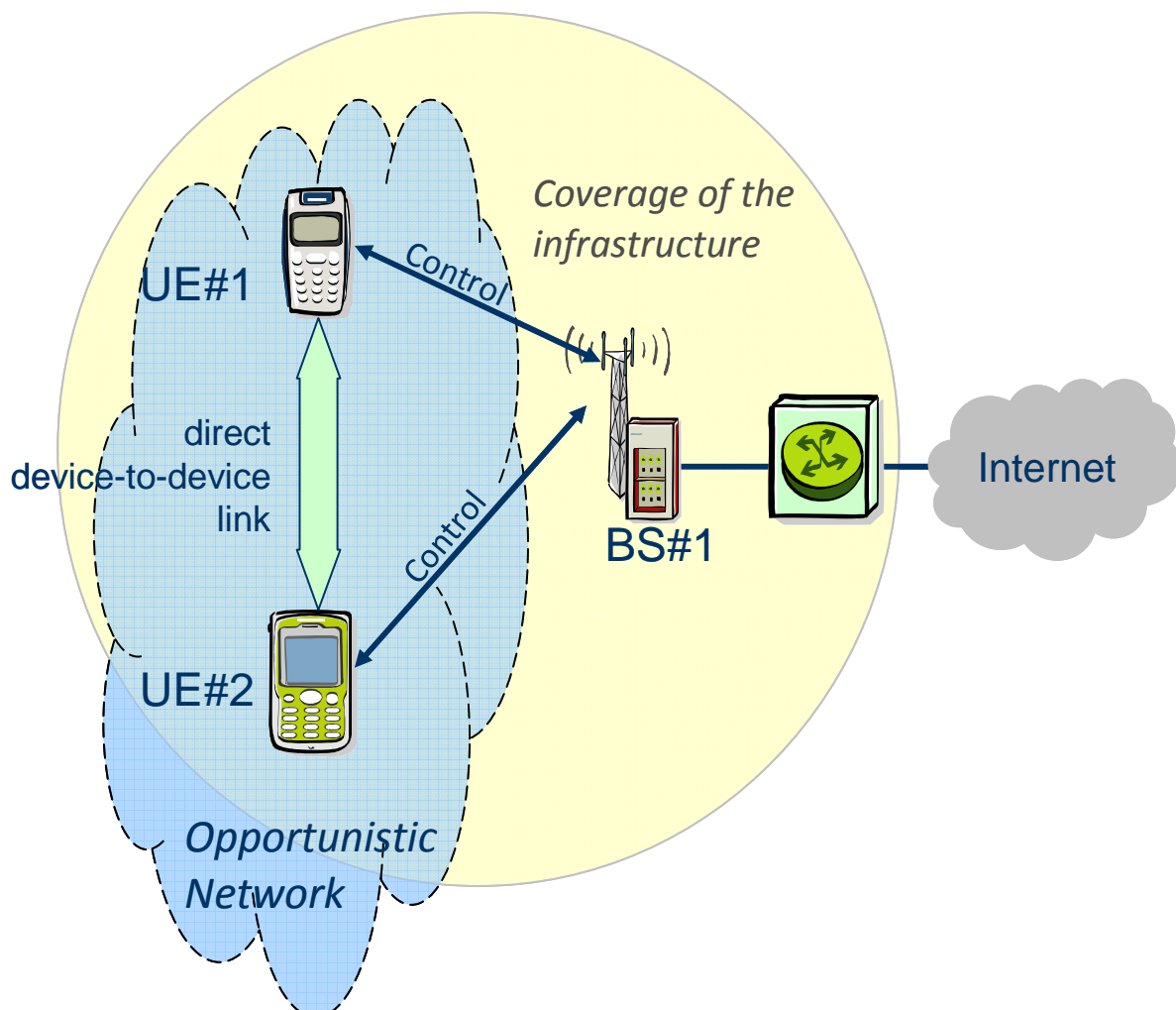


Figure 18: Example for Scenario 3:
Infrastructure supported opportunistic ad-hoc networking

As shown in Figure 18, both UE#1 and UE#2 may be attached to the infrastructure. These links to BS#1 are in this scenario only used for control signalling, e.g. indicating the suitability of an ON. The user traffic is exchanged directly between UE#1 and UE#2.

A differentiation can be made if the detection of the opportunity is inside the infrastructure as shown in section 5.3.1 below or if the detection of the opportunity is inside the user terminal as shown in section 5.3.2.

5.3.1 Infrastructure initiated opportunistic ad-hoc networking

In the MSC as shown in Figure 19, both UE#1 and UE#2 first attach to the network (Discovery, Authentication, Registration).

Then UE#1 wants to start a session towards UE#2. At this time, the UE#1 may not be aware that UE#2 is in its vicinity, so the SessionSetup.request is sent to BS#1.

The base station detects that the destination of the session (UE#2) is located in the same cell, thus a direct link may be possible. With such a direct link, the traffic can be offloaded from the network by creating an opportunistic network between UE#1 and UE#2. Therefore, BS#1 triggers UE#1 with the ON_Negotiation.Request to check if an ON between UE#1 and UE#2 can be established.

UE#1 then starts discovery procedures for UE#2 and establishes the ON. The network is notified on important events of the ON such as the establishment or the release of the ON.

Description of the Messages used in Figure 19:

1. The UE#1 discovers and registers to the network. This procedure includes authentication.
2. The UE#2 discovers and registers to the network. This procedure includes authentication.
3. 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.
4. Based on network internal information (e.g. both UE#1 and UE#2 are registered to the same BS), 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.
5. 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.
6. 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.
7. Discovery information is received from UE#2 indicating that it is supporting ONs.
8. The CSCI in UE#1 decides that the ON shall now be created. The goal of the ON is to have a direct device-to-device link between UE#1 and UE#2.
9. The CSCI triggers the CMON in UE#1 to start the creation of ON including UE#1 and UE#2.
10. An ON_Negotiation.Request including the capabilities and requirements from UE#1 is sent from UE#1 to UE#2.
11. UE#2 positively answers the negotiation and provides further context information from UE#2.
12. The CMON informs the CSCI that the negotiation was successful.
13. UE#1 provides an ON_Negotiation.Indication 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 requested in message nbr. 3.

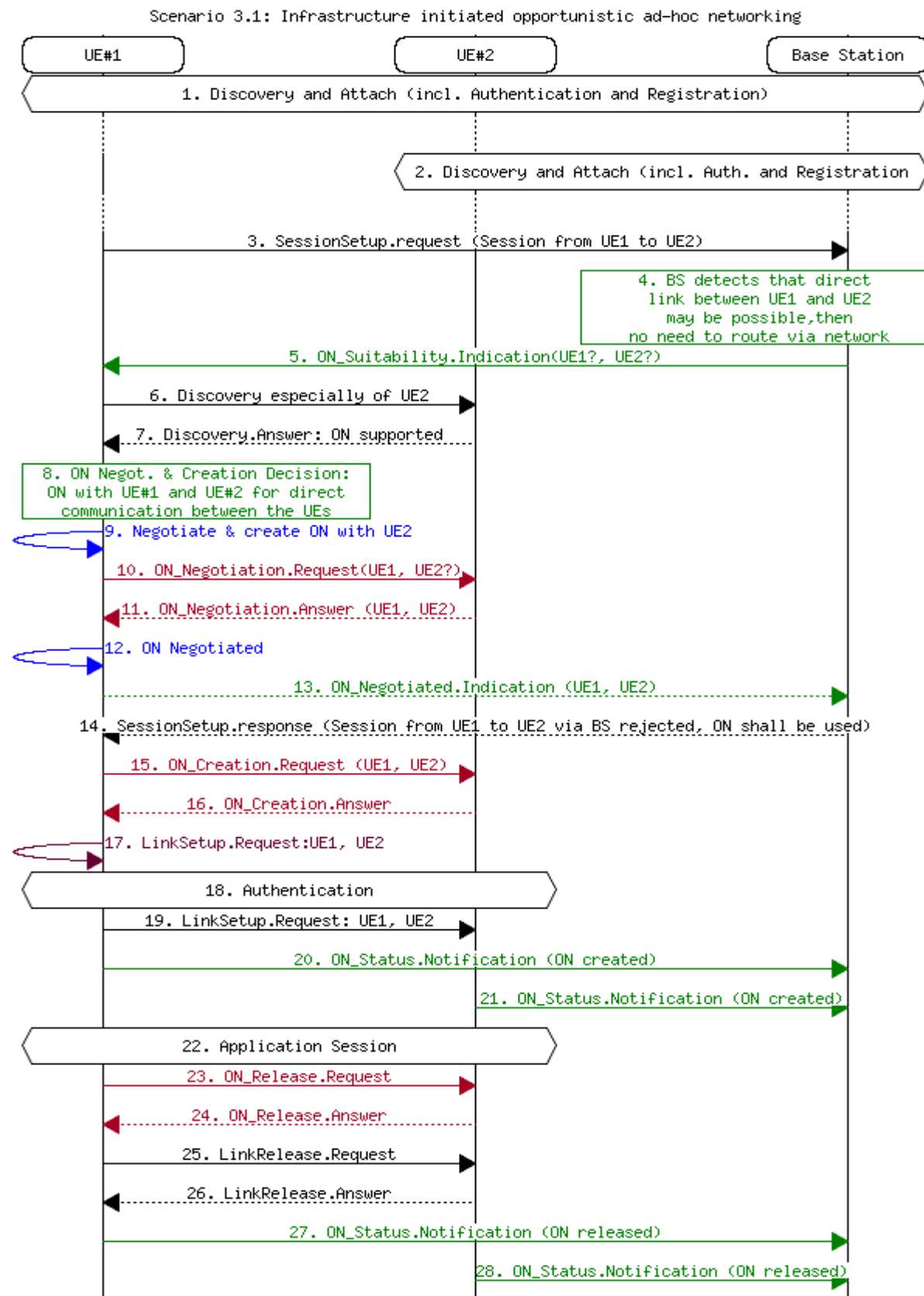


Figure 19: High-level MSC for Scenario 3.1: Infrastructure initiated opportunistic ad-hoc networking

14. The BS answers the SessionSetup.request from Msg. #3 with a SessionSetup.response that the session via the network is rejected and instead a direct link using the ON shall be used.
15. The ON_Creation.Request is sent via C4MS from the CMON in UE#1 to the CMON in UE#2.
16. The UE#2 replies with an ON_Creation.Answer.
17. The CMON in UE#1 initiates the setup of the user plane radio link via the JRRM towards the underlying RAT.
18. Authentication procedures between terminals may be executed at this point.
19. A RAT-specific LinkSetup.Request is sent towards UE#2. In UMTS or LTE for example, this message may be a RRC Connection.Request.
20. The BS is notified by UE#1 that the ON has been successfully established.
21. UE#2 also notifies the network that the ON has been successfully established.
22. The Application Session is now active.
23. After the end of the Application Session, the ON is no longer needed and an ON_Release.request is sent to UE#2.
24. UE#2 confirms the release of the ON in the ON_Release.answer.
25. The user plane link is released with a RAT-specific LinkRelease.Request
26. UE#2 confirms the release of the link.
27. UE#1 notifies the network that the ON no longer exists.
28. UE#2 also notifies the network that the ON no longer exists.

5.3.2 Terminal initiated opportunistic ad-hoc networking

In this scenario, the user's application wants to start a localised service. This service wants to exchange information with other users in the area, thus the opportunistic management is triggered to create an ON. Communication with the infrastructure takes only place to get support information from the infrastructure, e.g. on which spectrum to use. Therefore, as shown in the MSC in Figure 20, at least one UE (e.g. UE#1) is attached to the network.

Description of the Messages used in Figure 20:

1. The UE#1 discovers the network and attaches to it. This procedure includes authentication and registration.
2. An application in UE#1 wants to connect to other users in the area, e.g. to provide local services. Therefore, an ON shall be created. The CSCI is triggered to start the ON suitability determination.
3. For the coordination with the infrastructure, the CSCI in UE#1 sends a request to the infrastructure to retrieve additional information, e.g. on which spectrum to use for the ON.
4. The infrastructure provides information on which spectrum to use for the ON towards the UE#1.
5. The UE#1 starts a discovery procedure to discover other terminals in the area.

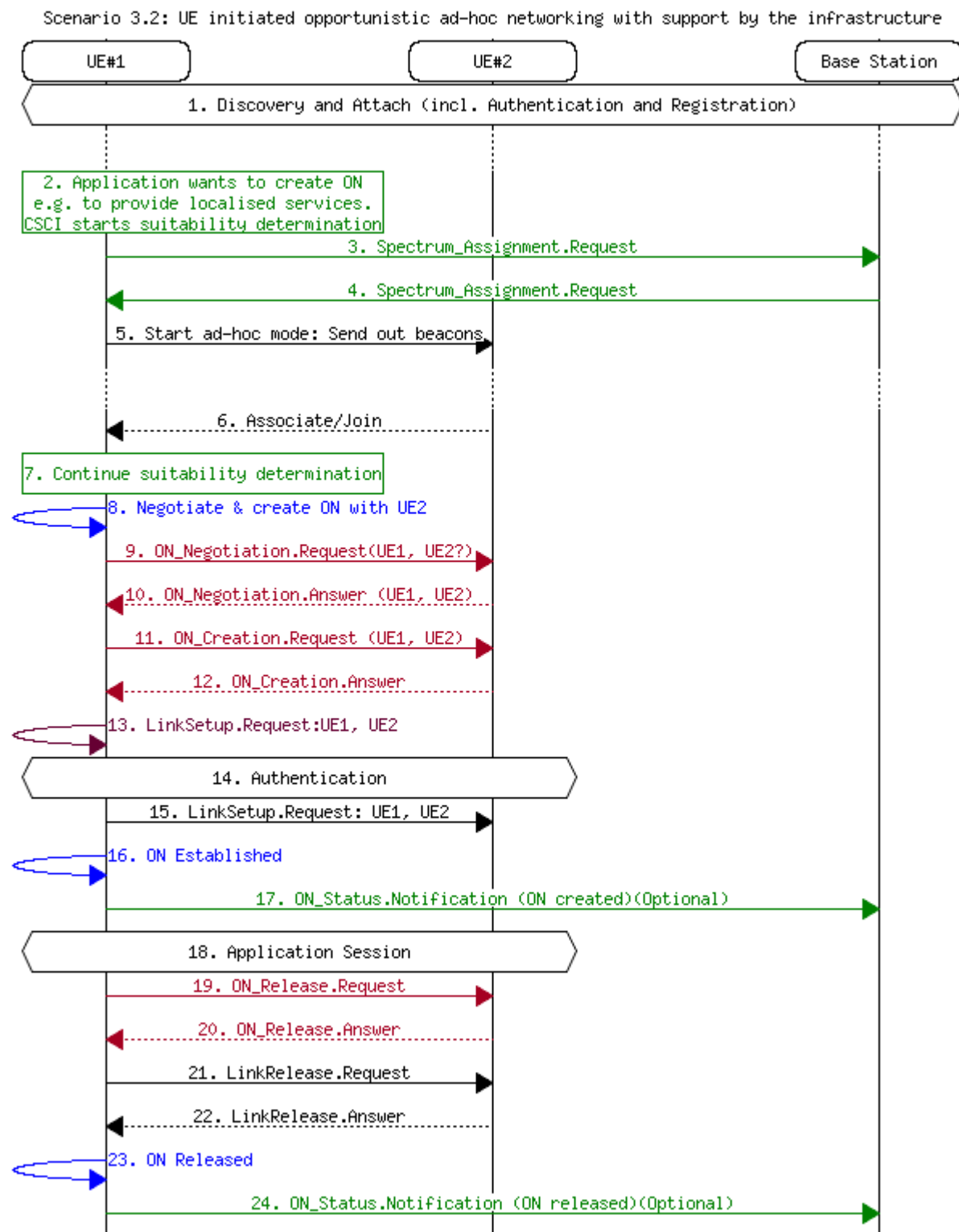


Figure 20: High-level MSC for Scenario 3.2: Terminal initiated opportunistic ad-hoc networking

6. Discovery information is received from UE#2 indicating that it is supporting ONs. This procedure may include already an RAT-specific associate/join in order to exchange further messages.
7. The CSCI in UE#1 decides that the ON shall now be created. The goal of the ON is to have a direct device-to-device link between UE#1 and UE#2.
8. The CSCI triggers the CMON in UE#1 to start the creation of the ON including UE#1 and UE#2.
9. An ON_Negotiation.Request including the capabilities and requirements from UE#1 is sent from UE#1 to UE#2.
10. UE#2 positively answers the negotiation and provides further context information from UE#2.
11. The ON_Creation.Request is sent via C4MS from the CMON in UE#1 to the CMON in UE#2.
12. The UE#2 replies with an ON_Creation.Answer.
13. So far, only Control-Plane signalling took place between the UEs. For some RATs, e.g. UMTS/LTE, a separate link is needed for the exchange of User-Plane signalling. For the creation of such a user-plane link, a LinkSetup.Request is sent from the CMON to the JRRM which forwards it to the underlying RAT.
14. Authentication procedures are executed.
15. A RAT-specific LinkSetup.Request is sent towards UE#2. In UMTS or LTE for example, this message may be a RRC Connection.Request. In other technologies where the same link can be used for control- and user-plan signalling, e.g. WLAN, this may not be necessary.
16. Inside UE#1, the CSCI is notified by the CMON that the ON has been successfully established.
17. UE#1 also notifies the network that the ON has been successfully established.
18. The Application Session is now active.
19. After the end of the Application Session, the ON is no longer needed and an ON_Release.request is sent to UE#2.
20. UE#2 confirms the release of the ON in the ON_Release.answer.
21. The user plane link is released with a RAT-specific LinkRelease.Request
22. UE#2 confirms the release of the link.
23. Inside UE#1, the CMON informs the CSCI that the ON has been released.
24. UE#1 notifies the network that the ON no longer exists.

5.4 MSC on opportunistic traffic aggregation in the radio access network

Scenario 4 “Opportunistic traffic aggregation in the radio access network” describes the usage of a local opportunistic network among several devices, in order to share a reduced number of infrastructure links towards a remote service-providing server or database. This situation allows some degree of traffic aggregation and caching that is useful to improve the overall network performance.

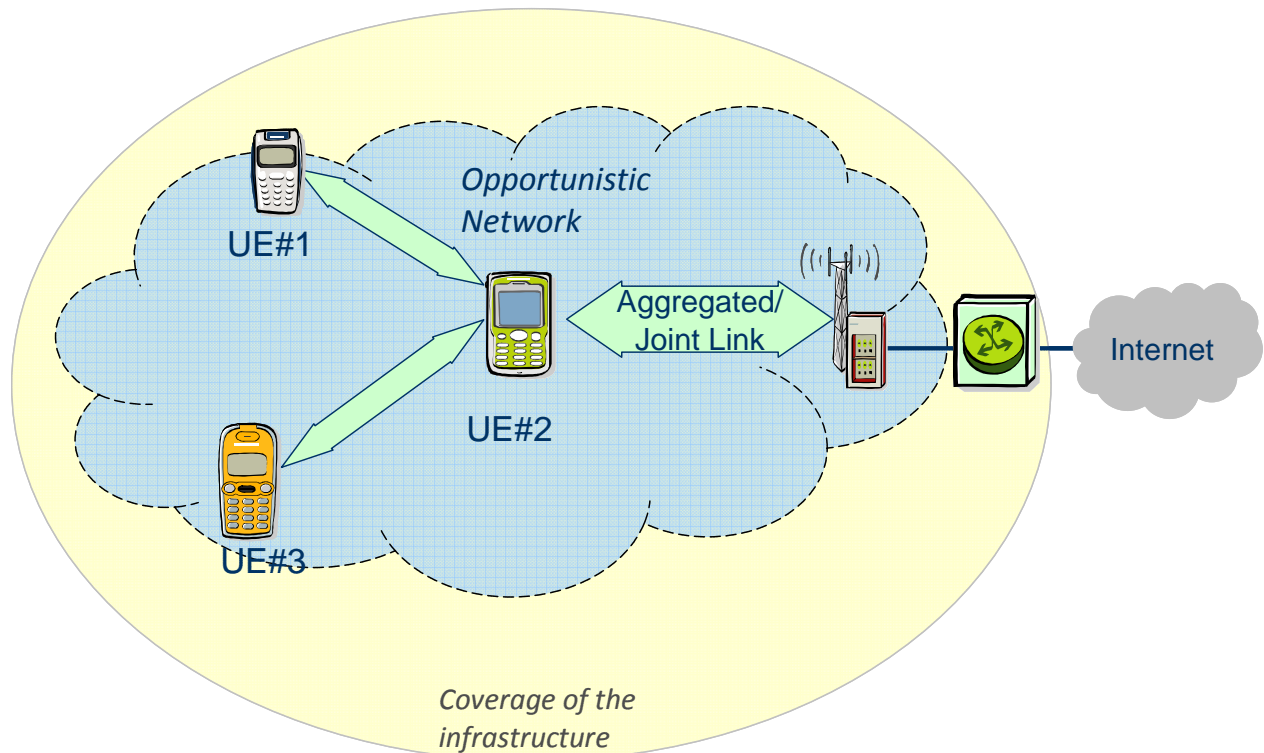


Figure 21: Example for Scenario 4: opportunistic traffic aggregation in the radio access network

UE#1 and UE#2 are attached to BS#1 to access some remote services. BS#1 discovers that UE#1 supports lower maximal bit rate than itself (alternatively, UE#1 detects that BS#1 supports higher maximal bit rate than itself) and requests UE#1 to start discovery procedures to provide it with some local context information. UE#1 discovers that UE#2 is in its vicinity and reports it to BS#1. BS#1 determines that UE#2 supports higher maximal bit rate and requests UE#1 to create an ON with UE#2. UE#1 and UE#2 establish the ON thus enabling UE#1 to be connected via UE#2 towards the base station BS#1.

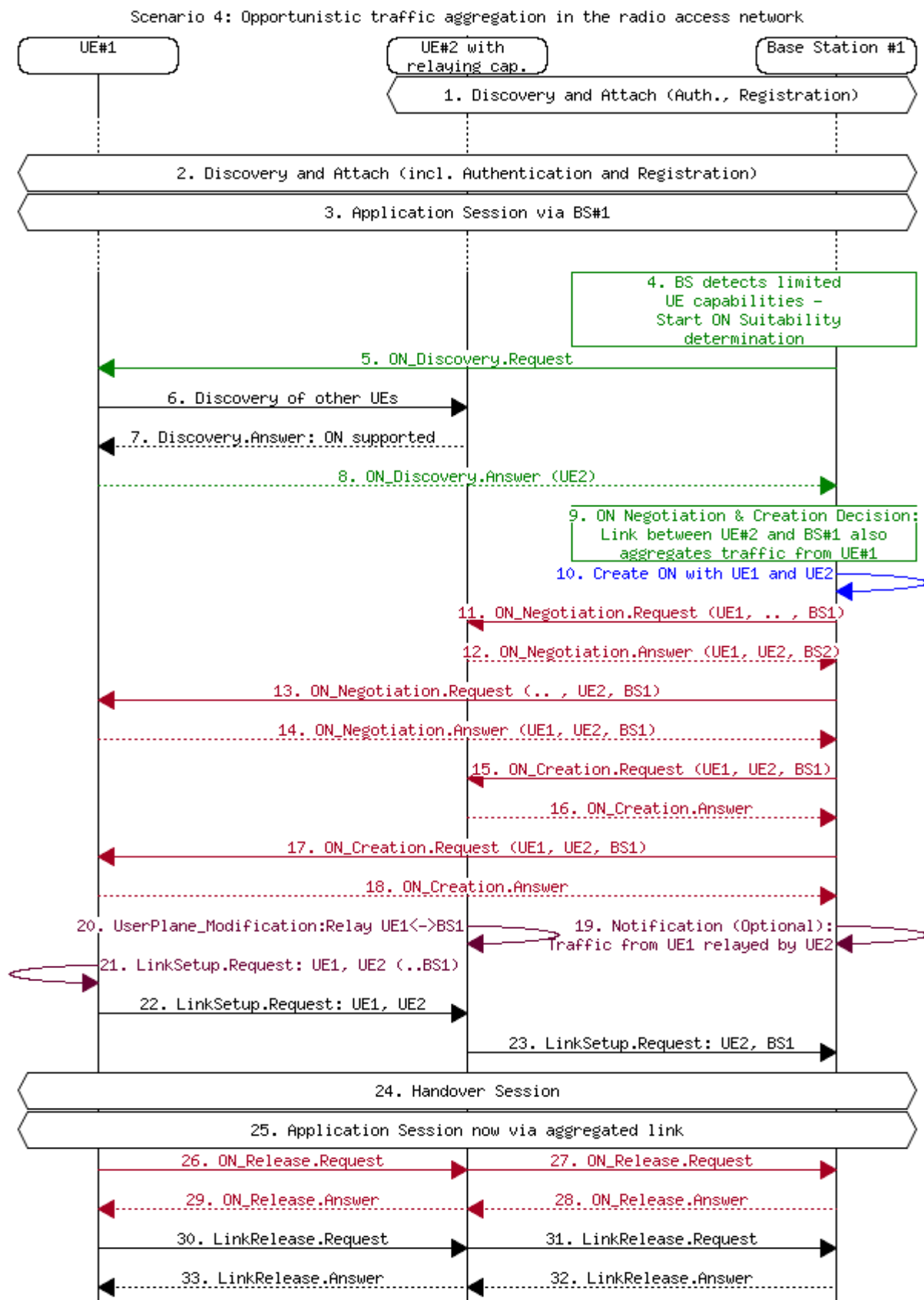


Figure 22: High-level MSC for Scenario 4: Opportunistic traffic aggregation in the radio access network

While Figure 22 shows the high-level MSC, a more detailed MSC including the node internal functions CSCI, CMON, JRRM and RAT is shown in Figure 23. Both MSCs use the same numbering for the messages, although some messages in Figure 22 are splitted into several messages in Figure 23. The following description of the messages is valid for both figures:

1. The UE#2 discovers and registers to the network. This procedure includes authentication.
2. The UE#1 discovers and registers to the network. This procedure includes authentication.
3. The UE#1 starts an Application Session using a direct link to BS#1.
4. The BS#1 detects the limited UE#1 capabilities (e.g. UE#1 does not support higher order modulation or MIMO, supported by BS#1) and starts the ON Suitability determination.
5. The BS sends an ON_Discovery.Request to UE#1 to trigger discovery procedures in UE#1. As the discovery procedure may include a reconfiguration of the transceiver, such a reconfiguration is made via the messages 5.1, 5.2, 5.3. and 5.4.
6. UE#1 initiates the discovery of other UEs in its vicinity.
7. UE#2 provides discovery information indicating that opportunistic networking is supported.
8. UE#1 answers the previous ON_Discovery.Request with an ON_Discovery.Answer towards BS#1 indicating that UE#2 is a candidate for the ON.
9. The CSCI in BS#1 continues the ON suitability determination and decides that an ON shall be created. The CSCI in the BS#1 decides that an ON will be created. The goal of the ON is to aggregate traffic from UE#1 in the existing link between UE#2 and the BS#1. In order to do so, UE#1 must setup the link towards UE#2.
10. The CSCI in BS#1 triggers the CMON to create an ON consisting of UE#1, UE#2 and BS#1.
11. BS#1 negotiates with UE#2 if UE#2 can be part of the ON.
12. UE#2 answers the ON_Negotiation indicating that it is willing to participate in the ON.
13. BS#1 negotiates with UE#1 indicating that UE#2 has agreed to be part of the ON.
14. UE#1 positively answers the ON_Negotiation.
15. The ON_Creation.Request is sent to UE#2
16. UE#2 replies with an ON_Creation.Answer.
17. The ON_Creation.Request is sent to UE#2
18. UE#2 replies with an ON_Creation.Answer.
19. Inside the BS, necessary User Plane / Transceiver modifications are performed (BS#1 is pre-configured to be able to receive/ transmit traffic from/to UE#1 via UE#2)."
20. Inside UE#2, the necessary User Plane / Transceiver modifications are also performed (UE#2 pre-configures its transceiver so that traffic from UE#1 can be forwarded/relayed to BS#1 and vice versa).
21. Inside UE#1, the CMON triggers the RAT-specific LinkSetup
22. UE#1 sends a LinkSetup.Request to UE2.
23. The LinkSetup.Request is forwarded to BS#1
24. A Handover of the session from the direct link between UE#1 and the BS#1 is made so that UE#1 now uses a link towards UE#2 which aggregates the traffic towards BS#1.
25. The Application Session continues now via the aggregated link.

26. – 32.: After the Application session has been terminated, the ON is no longer needed and the ON is released.

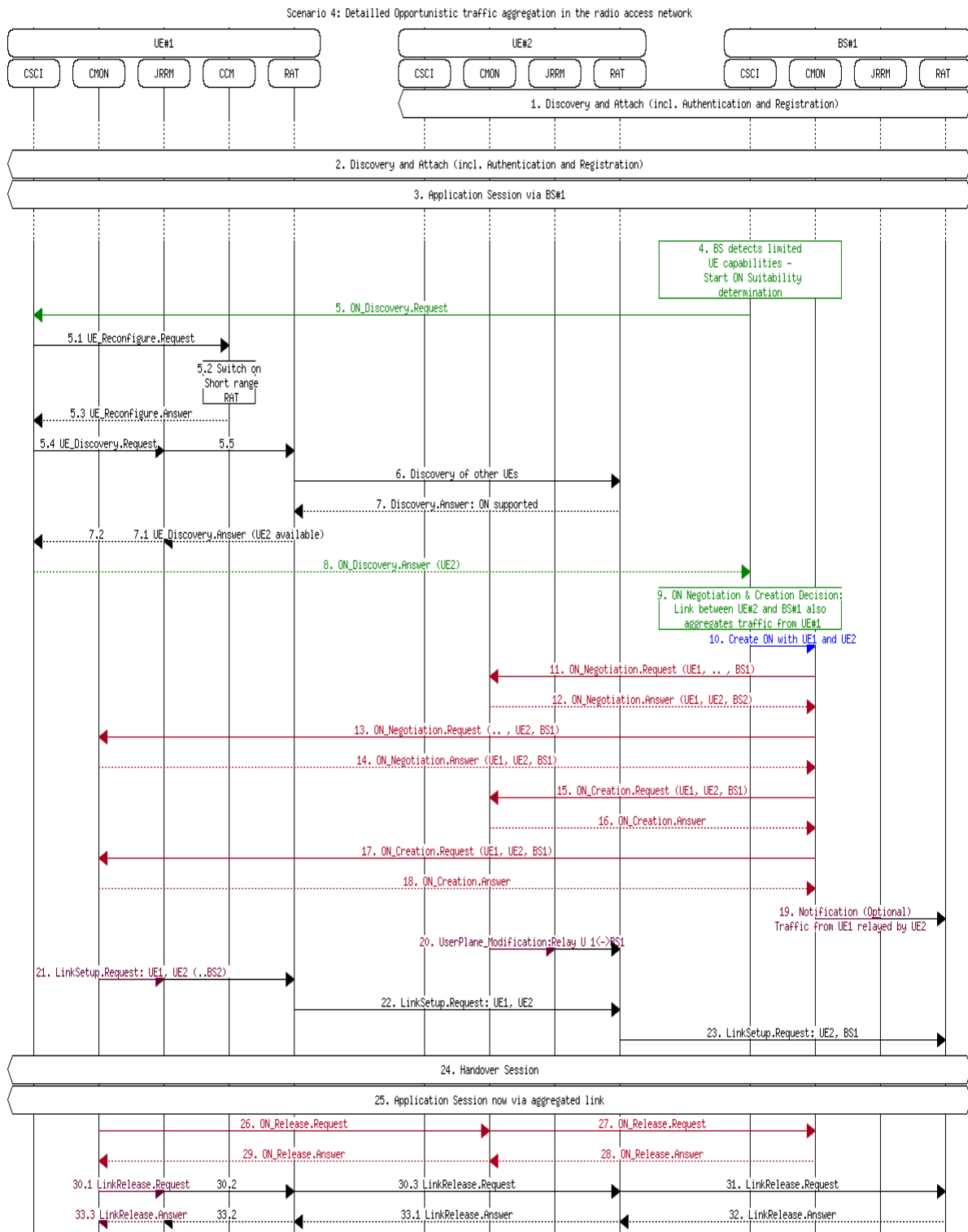


Figure 23: Detailed MSC for Scenario 4: Opportunistic traffic aggregation in the radio access network

5.5 MSC on opportunistic resource aggregation in the backhaul network

Scenario 5 “Opportunistic resource aggregation in the backhaul network” depicts how opportunistic networks can be used to aggregate both backhaul bandwidth and processing/storage resources on access nodes. In this case, the ON is created over access points rather than user terminals, thus offering a new focus on system performance improvement.

One of the use cases for the backhaul resource aggregation is depicted in figure 18. In this example base station 2 has problem with its backhaul link (it is congested or broken) and forms an ON with the neighbouring base stations in order to use their backhaul links to offload traffic from its congested backhaul link.

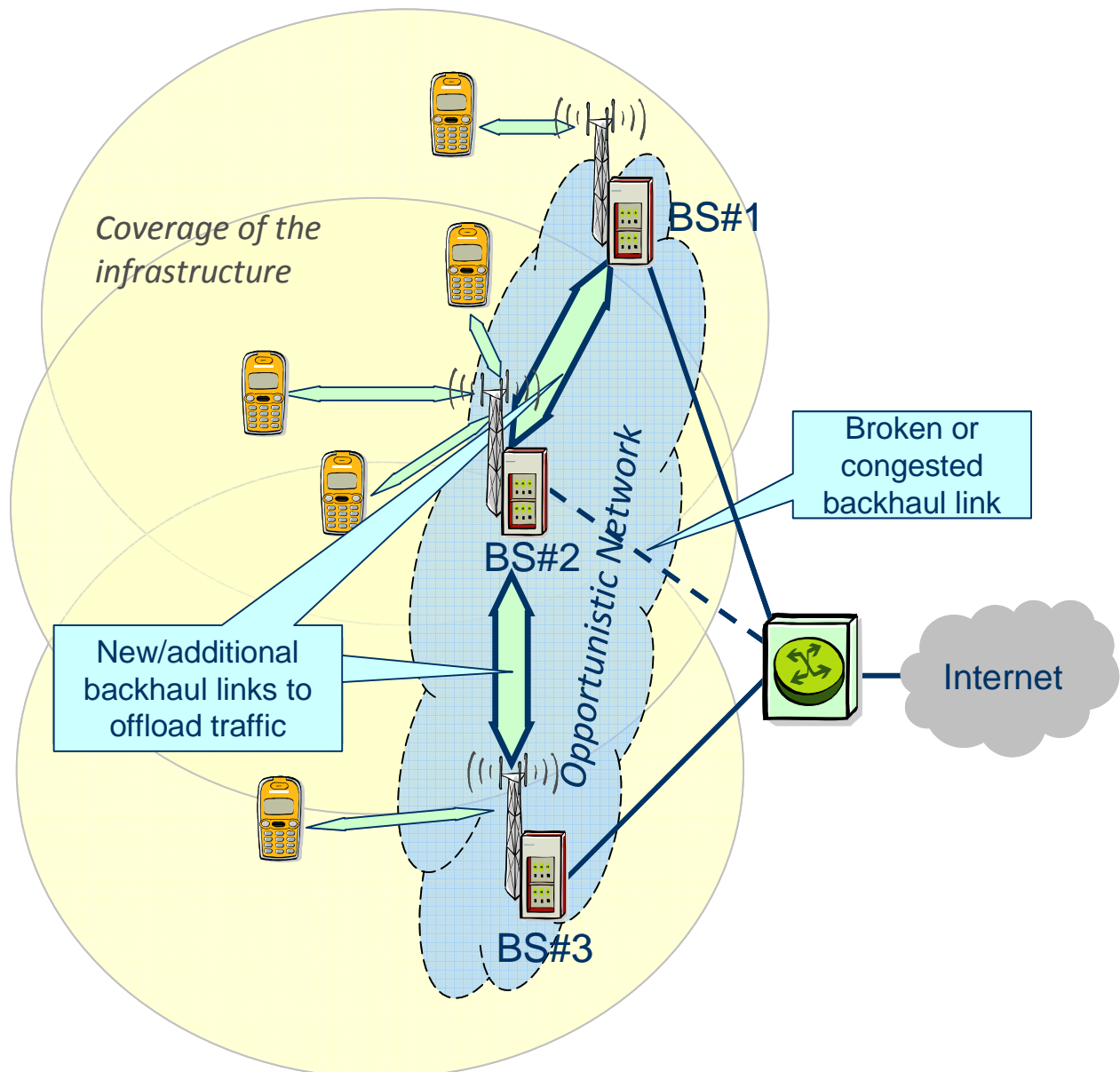


Figure 24: Example for Scenario 5:
opportunistic resource aggregation in the backhaul network

Figure 25 shows the high level MSC for the example from the Figure 24. Base stations are fixed network nodes and every one of them can store data about the neighbouring base stations that it can establish links with, so there is no need for the discovery procedure.

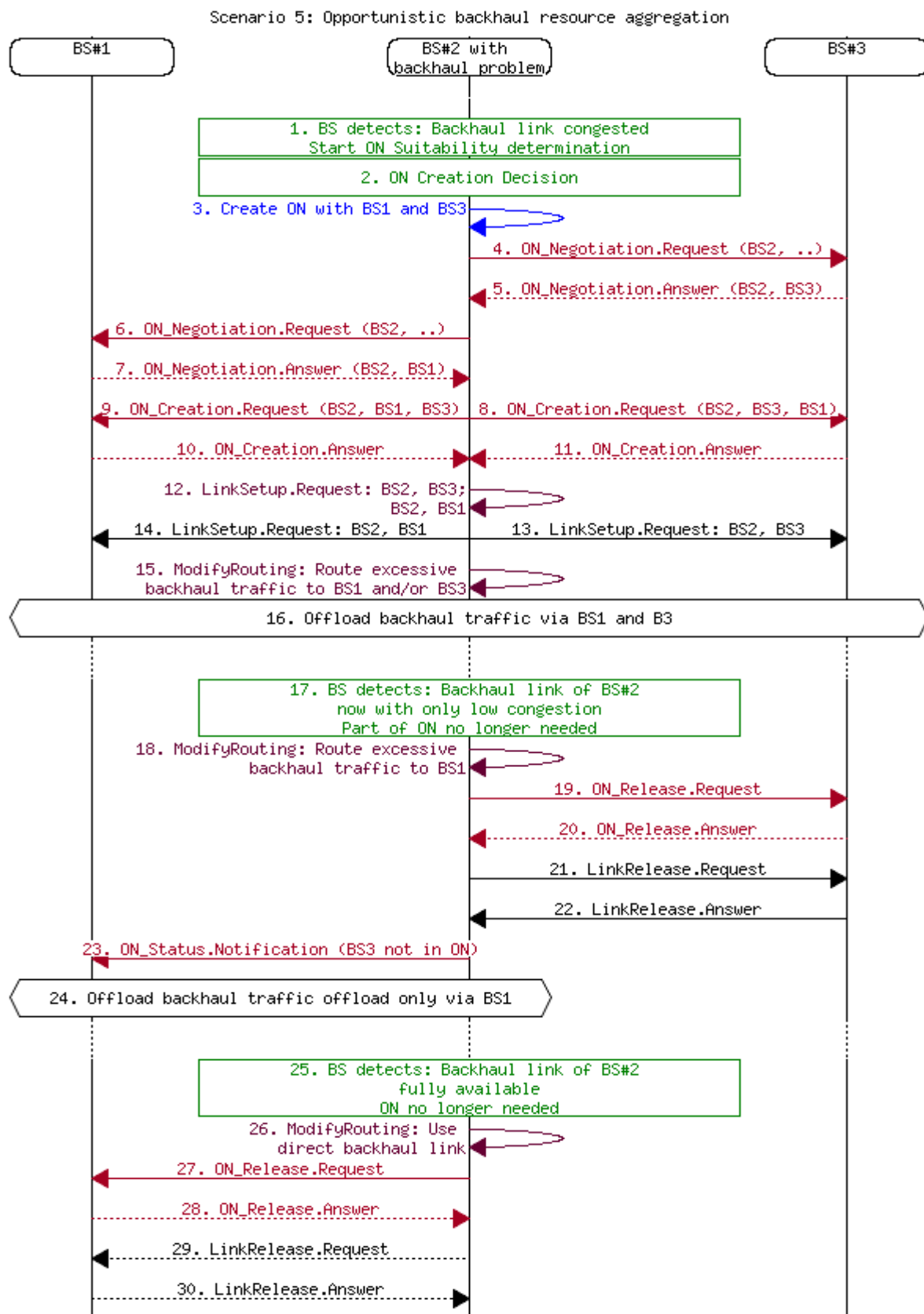


Figure 25: High-level MSC for Scenario 5: Opportunistic resource aggregation in the backhaul network

In this example, when the BS2 detects problem with its backhaul link it can immediately start the ON suitability determination procedure and start the ON negotiation with its neighbouring BSs. BS2 asks its neighbouring BSs for status and capabilities of their backhaul links and decides to create an ON with BS1 and BS3. Routing tables of the base stations that are participating in ON are updated. When the spare capacity of the BS3 backhaul link decreases below some threshold, or the backhaul traffic intensity for BS2 decreases (depicted in Figure 25), BS3 can leave the ON, which continues to exist between BS2 and BS1 while needed.

Description of the Messages used in Figure 25:

1. The BS#2 detects that the backhaul link is congested or broken. Thus, BS#2 starts the ON Suitability determination towards its neighbouring bases stations which are BS#1 and BS#3.
2. BS#2 decides to create an ON with BS#1 and BS#3.
3. Inside BS#2, the CSCI triggers the CMON to create the ON.
4. An ON_Negotiation.Request indicating that BS#2 wants to use BS#3 to backhaul it's traffic is sent to BS#3.
5. BS#3 positively replies with an ON_Negotiation.Answer.
6. A similar ON_Negotiation.Request indicating that BS#2 wants to use BS#1 to backhaul it's traffic is sent to BS#1.
7. BS#1 positively replies with an ON_Negotiation.Answer.
8. and 9.: BS#2 sends an ON_Creation.Request to BS#1 as well as to BS#3.
10. and 11.: Both BS#1 and BS#3 are replying with an ON_Creation.Answer.
12. Inside BS#2, CMON instructs JRRM to setup links towards BS#1 and BS#3
13. and 14.: LinkSetup.Requests are sent to BS#1 and BS#3.
15. Inside the BS#2, the routing is changed so that all backhaul traffic which can not be transported via the direct link is routed towards BS#1 and/or BS#3 (loadsharing).
16. The backhaul traffic is offloaded via BS#1 as well as BS#3.
17. The direct backhaul link is partially available again, thus a part of the ON can be released.
18. The routing is modified so that there will be no backhaul traffic towards BS#3.
- 19.-22.: BS#3 will be removed from the ON and the Link to BS#3 is released.
23. BS#1 is notified that BS#3 is no longer part of the ON.
24. Part of the traffic is still offloaded via BS#1.
25. The direct backhaul of BS#2 is now available with full capacity (no congestion), thus the ON is no longer needed.
26. The routing is modified so that there will be no backhaul traffic towards BS#3.
- 27.-30.: When the ON is no longer needed, the ON and the related links are released.

6. Conclusion and Outlook

This document has presented the OneFIT functional and system architecture for the management and control of infrastructure coordinated opportunistic networks (ONs).

As an important step for OneFIT, the split of the functions between the two main building blocks CSCI and CMON is described.

The CSCI (Cognitive management System for the Coordination of the infrastructure) is responsible for the detection of situations where an ON is useful, decides on the suitability of an ON and provides policy and context information from the infrastructure to the ON.

The CMON (Cognitive Management system for the Opportunistic Network) then creates and maintains an ON based on the directives from the CSCI.

Further on, Message Sequence Charts (MSCs) are described for the five main OneFIT scenarios:

- Opportunistic Coverage Extension
- Opportunistic Capacity Extension
- Infrastructure supported opportunistic ad-hoc networking
- Opportunistic traffic aggregation in the radio access network
- Opportunistic resource aggregation in the backhaul network

The architecture described in this document provides a basis for the following work in the other workpackages:

- Design and specification of the “Control Channels for the Cooperation of the Cognitive Management Systems” (C4MS) in WP3
- Algorithms for enabling opportunistic networks in WP4
- Integration of the OneFIT functions into an experimental platform where the OneFIT concepts will be validated.

7. References

- [1] ICT-2009-257385 OneFIT Project, <http://www.ict-onefit.eu/>
- [2] OneFIT Deliverable D2.1 "Business scenarios, technical challenges and system requirements", October 2010
- [3] OneFIT Deliverable D3.1 "Proposal of C4MS and inherent technical challenges", March 2011
- [4] ETSI TR 102 682 "Functional Architecture for the Management and Control of Reconfigurable Radio Systems"
- [5] ETSI TR 102 683 "Cognitive Pilot Channel"
- [6] 3GPP TS 23.203 "Policy and charging control architecture".
- [7] 3GPP TS 23.401 "GPRS enhancements for E-UTRAN access"
- [8] 3GPP TS 23.402 "Architecture enhancements for non-3GPP accesses"
- [9] 3GPP TS 24.302 "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks"
- [10] 3GPP TS 25.331 "Radio Resource Control (RRC); Protocol Specification"
- [11] 3GPP TS 33.102 "3G Security; Security Architecture"
- [12] 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
- [13] IETF RFC 3588 "Diameter Base Protocol", September 2003
- [14] OMA-ERELD-DM-V1-2: "Enabler Release Definition for OMA Device Management"
- [15] ICT-2007-216248 End-to-End efficiency (E³) Project, <https://ict-e3.eu/>
- [16] E3 Deliverable D2.3 " Architecture, Information Model and Reference Points, Assessment Framework, Platform Independent Programmable Interfaces", September 2009
- [17] E3 Deliverable D4.4 "Final solution description for autonomous CR functionalities", September 2009