

# 3GPP TR 24.820 V11.0.0 (2012-06)

---

*Technical Report*

## **3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP system to fixed broadband access network interworking (Release 11)**



The present document has been developed within the 3<sup>rd</sup> Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented. This Report is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

---

Keywords

---

access, packet mode, broadband access,  
interworking, UMTS, LTE

**3GPP**

Postal address

---

3GPP support office address

---

650 Route des Lucioles - Sophia Antipolis  
Valbonne - FRANCE  
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

---

<http://www.3gpp.org>

---

**Copyright Notification**

---

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2012, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TTA, TTC).  
All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
GSM® and the GSM logo are registered and owned by the GSM Association

# Contents

Foreword .....	5
1 Scope .....	6
2 References.....	6
3 Definitions and abbreviations .....	7
3.1 Definitions .....	7
3.2 Abbreviations .....	7
4 General.....	7
5 Network Discovery and Selection.....	7
5.1 Access network discovery and selection procedures.....	7
5.2 EPC network selection.....	8
5.3 Access Network reselection.....	8
5.4 Data traffic routing of IP flows .....	8
6 UE – EPC Network Protocols .....	8
6.1 General .....	8
6.2 Trusted and Untrusted Accesses .....	8
6.3 IP Mobility Mode Selection.....	8
6.4 Authentication and Authorization.....	8
7 Support of QoS .....	8
7.1 General .....	8
7.2 UE reflective QoS procedures .....	9
7.2.1 General.....	9
7.2.2 DSCP marking rule .....	9
7.2.3 Maintaining DSCP marking rules .....	9
7.2.4 Receiving an IP packet .....	10
7.2.5 Sending an IP packet .....	10
7.3 Network procedures for supporting QoS.....	10
7.4 Enabling UE reflective QoS function .....	10
7.4.1 General.....	10
7.4.2 UE procedure .....	11
7.4.2.1 Sending Reflective QoS Indication (RQSI) to 3GPP AAA server.....	11
7.4.2.2 Receiving the RQSI from 3GPP AAA server.....	11
7.4.3 Network procedure.....	12
7.4.3.1 RQSI from 3GPP AAA server to UE.....	12
8 UE – EPC Network Procedures for Fixed Broadband Access network over S2b.....	12
8.1 General .....	12
8.2 Tunnel management procedures .....	12
8.2.1 UE procedure .....	12
8.2.1.1 Tunnel establishment.....	12
8.2.1.2 Tunnel modification .....	13
8.2.1.3 Tunnel disconnection .....	13
8.2.2 ePDG procedure .....	13
8.2.2.1 Tunnel establishment.....	13
8.2.2.2 Tunnel modification .....	13
8.2.2.3 Tunnel disconnection .....	13
8.3 WLAN offloading .....	13
8.4 Supporting QoS with S2b procedure.....	13
8.4.1 UE procedure .....	13
8.4.2 ePDG procedure .....	14
9 UE – EPC Network Procedures for Fixed Broadband Access network over S2c .....	14
9.1 General .....	14
9.2 Procedures for trusted Fixed Broadband Access network over S2c .....	14

9.2.1	Supporting QoS with S2c procedure over trusted access .....	14
9.2.1.1	UE procedure .....	14
9.2.1.2	HA procedure .....	14
9.2.2	NAT traversal with S2c procedure over trusted access .....	14
9.2.2.1	General .....	14
9.2.2.2	UE procedure .....	14
9.2.2.3	HA procedure .....	15
9.2.3	UE local IP address change .....	15
9.2.3.1	General .....	15
9.2.3.1	UE procedure .....	15
9.2.3.2	HA procedure .....	15
9.3	Procedures for untrusted Fixed Broadband Access network over S2c .....	15
9.3.1	Supporting QoS with S2c procedure over untrusted access .....	15
9.3.1.1	UE procedure .....	15
9.3.1.2	HA procedure .....	15
9.3.1.3	ePDG procedure .....	15
9.3.2	UE local IP address change .....	16
9.3.2.1	General .....	16
9.3.2.1	UE procedure .....	16
9.3.2.2	ePDG procedure .....	16
9.3.2.2	HA procedure .....	16
10	UE – EPC Network Procedures for Fixed Broadband Access network using H(e)NB .....	16
10.1	General .....	16
10.2	Tunnel management procedures .....	16
10.2.1	General .....	16
10.2.2	Impacts to CT1 .....	17
10.3	Supporting QoS with H(e)NB procedure .....	17
10.3.1	General .....	17
10.3.2	Impacts to CT1 .....	17
10.4	Supporting CS domain services with HNB procedure .....	17
10.4.1	General .....	17
10.4.2	Impacts to CT1 .....	17
11	UE – EPC Network Procedures for Fixed Broadband Access network over S2a .....	18
12	Non-seamless WLAN offload traffic .....	18
12.1	General .....	18
12.2	UE procedure .....	18
12.3	Network procedure .....	18
13	PDU and parameters specific to the present document .....	18
13.1	IETF RFC coding information defined within present document .....	18
13.1.1	RQSI attributes .....	18
13.1.1.1	AT_RQSI_IND attribute .....	18
13.1.1.2	AT_RQSI_RES attribute .....	19
14	Conclusion .....	19
<b>Annex A (informative): Change history .....</b>		<b>21</b>

---

# Foreword

This Technical Report has been produced by the 3<sup>rd</sup> Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

---

# 1 Scope

The present document studies the additional UE – EPC procedures within the scope of 3GPP TS 24.302 [2] and 3GPP TS 24.229 [3], for the interworking between a 3GPP system and a Fixed Broadband Access network defined by Broadband Forum to provide the IP connectivity to a 3GPP UE using a WLAN and a H(e)NB connected to a Fixed Broadband Access network.

The report covers the discovery and network selection procedures, QoS aspects, Tunnel management procedures, selection of the IP mobility mode, Authentication and Access Authorization using Authentication, Authorization and Accounting (AAA) procedures, and IP CAN session impacts.

The present document is applicable to the UE and the network. In this technical specification the network is the 3GPP EPC.

---

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 23.139: "3GPP System-Fixed Broadband Access Network Interworking".
- [2] 3GPP TS 24.302: "Access to the Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".
- [3] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".
- [4] IETF RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".
- [5] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [6] IETF RFC 2474 (December 1998): "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".
- [7] IETF RFC 4301 (December 2005): "Security Architecture for the Internet Protocol".
- [8] Broadband Forum TR-058: "Multi-service Architecture and Framework Requirements", September 2003.
- [9] Broadband Forum TR-101: "Migration to Ethernet-based DSL Aggregation", July 2011.
- [10] Broadband Forum WT-134: "Policy Control Framework" (work in progress).
- [11] Broadband Forum WT-203: "Interworking between Next Generation Fixed and 3GPP Wireless Access" (work in progress).
- [12] Broadband Forum TR-059: "Architecture Requirements for the Support of QoS-Enabled IP Service", September 2003.
- [13] Broadband Forum WT-145: "Multi-service Broadband Network Functional Modules and Architecture" (work in progress).

- [14] 3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6; Stage 3".
- [15] Broadband Forum WT-146: "Subscriber Sessions", January 2012.
- [16] IETF RFC 5996 (September 2010): "Internet Key Exchange Protocol Version 2 (IKEv2)".
- [17] IETF RFC 4555 (June 2006): "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".
- [18] IETF RFC 3948 (January 2005): "UDP Encapsulation of IPsec ESP Packets".
- [19] IETF RFC 4303 (December 2005): "IP Encapsulating Security Payload (ESP)".
- [20] 3GPP TR 29.839: "3GPP System-Fixed Broadband Access Network Interworking; Home (e)Node B – Security Gateway Interface; Stage 3".

---

## 3 Definitions and abbreviations

*Editor's note: description of additional definitions and abbreviations to 3GPP TS 24.302 [2].*

### 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [5] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [5].

**Fixed Broadband Access Network:** This refers to the Fixed BBF access network defined by BBF TR-058 [8], BBF TR-059 [12], BBF TR-101 [9], BBF WT-134 [10], BBF WT-145 [13], and BBF WT-203 [11].

**UE reflective QoS function:** A UE function that supports Reflective QoS for uplink traffic over a Fixed Broadband Access network as specified in 3GPP TS 23.139 [1].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.303 [14] subclause 3.1 apply:

**Home Agent (HA)**

### 3.2 Abbreviations

DSCP	Differentiated Services Code Point
NAT	Network Address Translation
P-GW	PDN Gateway
QoS	Quality of Service
RQSI	Reflective QoS Indication

---

## 4 General

*Editor's note: additional general information to 3GPP TS 24.302 [2]*

---

## 5 Network Discovery and Selection

### 5.1 Access network discovery and selection procedures

When interworking with Fixed Access Broadband, the access network discovery and selection procedures specified in 3GPP TS 24.302 [2] shall be used.

## 5.2 EPC network selection

When interworking with Fixed Access Broadband, the EPC network selection procedures specified in 3GPP TS 24.302 [2] shall be used.

## 5.3 Access Network reselection

When interworking with Fixed Access Broadband, the access network reselection procedures specified in 3GPP TS 24.302 [2] shall be used.

## 5.4 Data traffic routing of IP flows

When interworking with Fixed Access Broadband, the data routing of IP flows procedures specified in 3GPP TS 24.302 [2] shall be used.

---

# 6 UE – EPC Network Protocols

## 6.1 General

## 6.2 Trusted and Untrusted Accesses

When interworking with Fixed Access Broadband, the UE-EPC Network protocols related to trusted and untrusted access procedures specified in 3GPP TS 24.302 [2] shall be used.

## 6.3 IP Mobility Mode Selection

When interworking with Fixed Access Broadband, the UE-EPC Network protocols related to IP Mobility Mode Selection procedures specified in 3GPP TS 24.302 [2] shall be used.

## 6.4 Authentication and Authorization

When interworking with Fixed Access Broadband, the UE-EPC Network protocols related to Authentication and Authorization procedures specified in 3GPP TS 24.302 [2] shall be used.

---

# 7 Support of QoS

## 7.1 General

When interworking with a Fixed Broadband Access network, DSCP marking is used for setting QoS as specified in IETF RFC 2474 [6].

For downlink traffic, the 3GPP network sets the DSCP value on the outer header of each IP packet at per-flow basis. When tunnelling the IP packet to the UE, the network copies the DSCP value from the inner IP header to the new outer IP header.

For uplink traffic, the reflective QoS on uplink traffic is optionally supported by the UE when accessing a Fixed Broadband Access network. The reflective QoS is achieved by creating a DSCP marking rule based on the received downlink traffic.

The BBF network may perform QoS treatment and QoS remapping based on DSCP value of the outer IP header.



## 7.2 UE reflective QoS procedures

### 7.2.1 General

A UE may support the UE reflective QoS function for uplink traffic.

For a UE supporting UE reflective QoS function, once the UE reflective QoS function is enabled by the network, the UE shall create uplink DSCP marking rules based on the received downlink traffic. Each uplink DSCP marking rule contains a n-tuple rule which is created based on the corresponding n-tuple of the received downlink traffic. The UE shall use the uplink DSCP marking rules to set the DSCP field of the outer IP header of the outgoing IP packets.

The UE reflective QoS function may be enabled by the network as specified in subclause 7.4.

### 7.2.2 DSCP marking rule

The DSCP marking rules contains following parameters:

- Source IP address;
- Destination IP address;
- Source port number;
- Destination port number;
- Protocol type;
- DSCP marking value; and
- Timestamp.

The source IP address refers to the IP address used by the UE as source IP address when generating IP traffic.

The destination IP address refers to the IP address of the data packets destined for the UE.

The source port number refers to the port number used by the UE as source port number when generating IP traffic.

The destination port number refers to the port number of the data packets destined for the UE.

The protocol type is a value among the internet protocol numbers as defined in IANA. In case of IPv4, the protocol type value is the value of the last protocol type field. In case of IPv6, the protocol type value is the value of the last next header field.

The timestamp is the time that the DSCP marking rule was created or the last time the DSCP marking rule was used.

### 7.2.3 Maintaining DSCP marking rules

The DSCP marking table is created when the first DSCP marking rule is created based on the received downlink IP packet.

Depends on the protocol type, the n-tuple is either a 5-tuple (including: source IP address, destination IP address, source port number, destination port number, and protocol type) or a 3-tuple (including source IP address, destination IP address, and protocol type).

The lifetime of the DSCP marking table is same as the associated PDN connection.

A UE may remove the expired entries from the table based on the timestamp. How long the entry shall be maintained in the table is an implementation specific value.

## 7.2.4 Receiving an IP packet

When receiving an IP packet, the UE shall perform a lookup in the DSCP marking table based on the n-tuple of the IP header. If tunnel is established between the UE and the network, the lookup is performed after the tunnel de-capsulation.

If no matching entry is found, a new entry shall be created as followings:

- The source IP address of the new entry is the destination IP address of the received packets;
- The source port number of the new entry is the destination port number of the received packets;
- The destination IP address of the new entry is the source IP address of the received packets;
- The destination port number of the new entry is the source port number of the received packets;
- The protocol type value is either the value of the last protocol type field in IPv4 case, or the value of the last next header field in case of IPv6;
- The DSCP field is set as same as the DSCP field of the received outer IP header; and
- The timestamp is set.

If a matching entry is found, the timestamp shall be set.

## 7.2.5 Sending an IP packet

When sending an IP packet, the UE shall perform a lookup in the DSCP marking table based on the n-tuple of the IP header. If tunnel is established between the UE and the network, the lookup is performed before the tunnel encapsulation.

If a matching entry is found, the UE shall set the DSCP marking value of the outer IP header according to the matched DSCP marking rule and set the timestamp of the entry. If there is already a value of the DSCP field in the outer IP header set by the UE application, it shall be overwritten by the DSCP marking value from the DSCP marking rule.

If no matching entry is found, the UE shall not modify the DSCP field of the outer IP header.

## 7.3 Network procedures for supporting QoS

The 3GPP network shall create DSCP marking rules per QoS flow based on policies as defined in 3GPP TS 23.139 [1].

When tunnelling the UE downlink traffic, the network shall copy the DSCP value from the received IP header into the new outer header before forwarding to the UE.

Optionally, the network may perform DSCP marking remapping based on the operator's policy.

## 7.4 Enabling UE reflective QoS function

### 7.4.1 General

The UE indicates its support of UE reflective QoS function to the network. When the UE explicit indication is received, the network provides the reflective QoS Indication to the UE which indicates that the UE reflective QoS function shall be enable or disabled.

For trusted Fixed Broadband Access network, the indication is provided at 3GPP based access authentication before an IP address is allocated to the UE. For un-trusted Fixed Broadband Access network, if the 3GPP based access authentication is performed the indication is provided at 3GPP based access authentication before an IP address is allocated to the UE, or it is provided during IKEv2 signalling for IPsec tunnel establishment with the ePDG. For DSMIPv6 based access procedure, the indication is provided during IKEv2 signalling for IPsec tunnel establishment with the PDN-GW/HA.

## 7.4.2 UE procedure

### 7.4.2.1 Sending Reflective QoS Indication (RQSI) to 3GPP AAA server

During EAP-AKA and EAP-AKA' based authentication, UE may provide an explicit indication to the 3GPP AAA server about the supporting of UE reflective QoS function. The explicit indication is sent using an attribute in the EAP-AKA and EAP-AKA' protocols, to extend these protocols as specified in subclause 8.2 of IETF RFC 4187 [4]. This attribute is provided in EAP-Response/AKA-Challenge and corresponding EAP-AKA' message payload.

If the UE reflective QoS function is supported, the UE shall provide the RQSI using AT\_RQSI\_IND attribute in EAP-AKA or EAP-AKA'. The indication is provided if the UE receives the AT\_RESULT\_IND attribute within the EAP-Request/AKA-Challenge message, or the EAP-Request'/AKA-Challenge' message when EAP-AKA' is used. If the UE provides the AT\_RQSI\_IND attribute within the EAP-Response/AKA-Challenge message payload, or the EAP-Response'/AKA-Challenge' message payload when EAP-AKA' is used, the UE shall also provide the AT\_RESULT\_IND attribute within the message.

The detailed coding of this attribute is described in subclause 13.1.1.

### 7.4.2.2 Receiving the RQSI from 3GPP AAA server

The UE shall only enable the UE reflective QoS function if enabled by the network.

If the Reflective QoS Indication is received at 3GPP based access authentication which indicates the UE reflective QoS function is enabled, the UE may:

- perform the UE reflective QoS function on all traffic for the attached Fixed Broadband Access network that enabled the UE reflective QoS function; and
- disable the UE reflective QoS function, when:
  - a) the UE/network initiated detachment from the attached Fixed Broadband Access network; or
  - b) the UE moves away from the attached Fixed Broadband Access network coverage.

If the Reflective QoS Indication is received at 3GPP based access authentication during the attachment of the Fixed Broadband Access network:

- the UE need not provide an explicit indication during IKEv2 signalling for IPsec tunnel establishment with ePDG or DSMIPv6 over a trusted Fixed Broadband Access network; and
- the UE shall ignore the Reflective QoS Indication if it is received during IKEv2 signalling for IPsec tunnel establishment with ePDG or DSMIPv6 over a Fixed Broadband Access network.

If the Reflective QoS Indication is received during IKEv2 signalling for IPsec tunnel establishment with ePDG which indicates that the UE reflective QoS function is enabled, the UE may:

- perform the UE reflective QoS function on all tunneled traffic for the attached ePDG that enabled the UE reflective QoS function; and
- disable the UE reflective QoS function, when:
  - a) the PDN connection over the attached ePDG is released or handover to another access network;
  - b) the UE/network initiated detachment from the attached Fixed Broadband Access network; or
  - c) the UE moves away from the attached Fixed Broadband Access network coverage;

For DSMIPv6 over a trusted Fixed Broadband Access network, if the Reflective QoS Indication is received during DSMIPv6 bootstrapping with PDN-GW/HA which indicates that the UE reflective QoS function is enabled, the UE may:

- perform the UE reflective QoS function for all DSMIPv6 traffic for the attached PDN-GW/HA that enabled the UE reflective QoS function; and
- disable the UE reflective QoS function, when:

- a) the PDN connection with the attached PDN-GW/HA is released or handover to another access;
- b) the UE/network initiated detachment from the attached Fixed Broadband Access network; or
- c) the UE moves away from the attached Fixed Broadband Access network coverage;

The UE shall not enable the UE reflective QoS function, if:

- the received Reflective QoS Indication indicates that the UE reflective QoS function is disabled; or
- the Reflective QoS Indication is not received from the 3GPP AAA.

If the UE reflective QoS function is not enabled, the DSCP marking value of the outer IP header performed by the UE is implementation specific.

## 7.4.3 Network procedure

### 7.4.3.1 RQSI from 3GPP AAA server to UE

A 3GPP AAA server supporting RQSI, shall include the AT\_RESULT\_IND attribute within the EAP-Request/AKA-Challenge and corresponding EAP-AKA' message payload.

If the UE provided an explicit indication as described in subclause 7.4.2.1, the 3GPP AAA server shall inform the UE of its decision of the UE reflective QoS function by invoking an EAP-Request/AKA-Notification dialogue when EAP-AKA is used or an EAP-Request/AKA-Notification' dialogue when EAP-AKA' is used. The UE reflective QoS function decision is sent to the UE by using the AT\_RQSI\_RES attribute.

The UE reflective QoS function decision is made by the 3GPP AAA server based on the capabilities of the UE, the type of access, the access identity and local policies.

The detailed coding of this attribute is described in subclause 13.1.1.

---

# 8 UE – EPC Network Procedures for Fixed Broadband Access network over S2b

## 8.1 General

During the procedure of initial attach for Fixed Broadband Access network over S2b, the UE shall initiate the IKEv2 tunnel establishment as defined in IETF RFC 5996 [16] with the ePDG through the Fixed Broadband Access Network. In an IPv4 Fixed Broadband Access Network, NAT may be deployed, e.g. RG. If NAT is deployed, the UE behind the NAT shall invoke the NAT traversal procedure for IKEv2.

## 8.2 Tunnel management procedures

### 8.2.1 UE procedure

#### 8.2.1.1 Tunnel establishment

Once the ePDG has been selected, the UE shall initiate the IPsec tunnel establishment procedure using the IKEv2 protocol as defined in 3GPP TS 24.302 [2] with the following additions:

- a) if the UE supports Reflective QoS, the UE shall provide the RQSI using AT\_RQSI\_IND attribute as defined in subclause 13.1.1.1 within the IKE\_AUTH request message;
- b) the UE shall support the NAT detection function as defined in section 2.23 of IETF RFC 5996 [16]; and
- c) if NAT is detected between the UE and the ePDG,

- the UE shall use UDP encapsulated for ESP as defined in IETF RFC 5996 [6]; and
- the UE may send the NAT-keepalive packet to keep NAT mapping alive as defined in the IETF RFC 3948 [18].

### 8.2.1.2 Tunnel modification

This procedure is used if MOBIKE as defined in IETF RFC 4555 [31] is supported by the UE. The tunnel modification procedure is as specified in 3GPP TS 24.302 [2] subclause 7.2.3 with the following additions:

- a) the UE should support the NAT re-mapping detection function as defined in IETF RFC 4555 [17]; and
- b) if the NAT re-mapping (i.e. the IP address or the UDP port number or both are reallocated) is detected, the UE shall send an INFORMATIONAL request containing the UPDATE\_SA\_ADDRESSES notification to the ePDG as defined in IETF RFC 4555 [17].

### 8.2.1.3 Tunnel disconnection

The procedure of tunnel disconnection initiated by the UE is as specified 3GPP TS 24.302 [2].

## 8.2.2 ePDG procedure

### 8.2.2.1 Tunnel establishment

Upon receipt of an IKE\_AUTH request message from the UE requesting the establishment of a tunnel, the ePDG shall proceed with authentication and authorization as specified in 3GPP TS 24.302 [2] with the following additions:

- a) the ePDG shall support the NAT detection function as defined in section 2.23 of IETF RFC 5996 [16];
- b) if NAT is detected between the UE and the ePDG, the ePDG shall use UDP encapsulated for ESP as defined in IETF RFC 5996 [16]; and
- c) the ePDG shall send the RQSI on whether Reflective QoS shall be applied within the IKE\_AUTH response message to the UE if receiving from the 3GPP AAA Server.

### 8.2.2.2 Tunnel modification

The ePDG tunnel modification procedure is as specified in 3GPP TS 24.302 [2].

### 8.2.2.3 Tunnel disconnection

The procedure of tunnel disconnection initiated by the ePDG is as specified 3GPP TS 24.302 [2].

## 8.3 WLAN offloading

**Editor's note: WLAN offloading requirements over an untrusted Fixed Broadband Access network**

## 8.4 Supporting QoS with S2b procedure

### 8.4.1 UE procedure

The UE may support reflective QoS for uplink traffic as specified in subclause 7.2.

If reflective QoS is supported and anti-replay feature is implemented, the UE should create dedicated child SA for each IP flow which has the same DSCP marking value.

## 8.4.2 ePDG procedure

When receiving a downlink data packet for a UE, the ePDG shall copy the DSCP marking value from the received IP header into the new IPsec header before forwarding to the UE, as specified in subclause 7.3.

If the anti-replay feature is implemented, the ePDG should create dedicated child SA for each IP flow which has the same DSCP marking value.

Optionally, the ePDG may perform DSCP marking remapping based on the operator's policy.

---

# 9 UE – EPC Network Procedures for Fixed Broadband Access network over S2c

## 9.1 General

*Editor's note: UE- EPC function description and procedure of 3GPP access and Fixed Broadband Access network interworking using S2c DSMIPv6.*

## 9.2 Procedures for trusted Fixed Broadband Access network over S2c

*Editor's note: UE- EPC function description and procedure of 3GPP access and trusted Fixed Broadband Access network interworking using S2c DSMIPv6.*

### 9.2.1 Supporting QoS with S2c procedure over trusted access

#### 9.2.1.1 UE procedure

The UE may support UE Reflective QoS function for uplink traffic as specified in subclause 7.2.

If UE Reflective QoS function for uplink traffic is enabled, S2c data integrity protection is used and the IPsec anti-replay feature specified in IETF RFC 4301 [7] is implemented, the UE should create dedicated child SA for each IP flow which has the same DSCP marking value.

#### 9.2.1.2 HA procedure

The HA shall set per QoS flow DSCP marking on IP outer header as specified in subclause 7.3.

If S2c data integrity protection is used and the IPsec anti-replay feature specified in IETF RFC 4301 [7] is implemented,

### 9.2.2 NAT traversal with S2c procedure over trusted access

#### 9.2.2.1 General

During the procedure of initial attach for trusted Fixed Broadband Access network over S2c, the UE shall initiate the IKEv2 tunnel establishment with the HA for negotiating the IPsec security association to secure DSMIPv6 signalling as specified in 3GPP TS 24.303 [14] through the Fixed Broadband Access Network. In an IPv4 Fixed Broadband Access Network, NAT may be deployed, e.g. RG. In this case, the UE behind the NAT shall invoke the NAT traversal procedure for IKEv2.

#### 9.2.2.2 UE procedure

The UE shall support the NAT detection function as defined in the section 2.23 of IETF RFC 5996 [16].

If NAT is detected between the UE and HA, the following procedures shall be performed:

- the UE shall use UDP-Encapsulated ESP as defined in IETF RFC 5996 [16]; and
- the UE may send the NAT-keepalive packet to keep NAT mapping alive as defined in the IETF RFC 3948 [18].

### 9.2.2.3 HA procedure

Upon receipt of an IKE\_AUTH request message from the UE requesting the establishment of a tunnel, the HA shall proceed with authentication and authorization as specified in 3GPP TS 24.303 [14] with the following additions:

- the HA shall support the NAT detection function as defined in section 2.23 of IETF RFC 5996 [16]; and
- if NAT is detected between the UE and the HA, the HA shall use UDP-Encapsulated ESP as defined in IETF RFC 5996 [16].

## 9.2.3 UE local IP address change

### 9.2.3.1 General

If the UE receives a new local IP address from the Fixed Broadband Access network, the UE needs to update the mobility tunnel with the HA.

### 9.2.3.1 UE procedure

The UE shall perform the Dual-Stack Mobile IPv6 handover procedure as defined in 3GPP TS 24.303 [14], subclause 5.2.2.

### 9.2.3.2 HA procedure

The HA shall perform the Dual-Stack Mobile IPv6 handover procedure as defined in 3GPP TS 24.303 [14], subclause 5.2.3.

## 9.3 Procedures for untrusted Fixed Broadband Access network over S2c

*Editor's note: UE- EPC function description and procedure of 3GPP access and untrusted Fixed Broadband Access network interworking using S2c DSMIPv6.*

### 9.3.1 Supporting QoS with S2c procedure over untrusted access

#### 9.3.1.1 UE procedure

The UE may support reflective QoS for uplink traffic as specified in subclause 7.2.

If the anti-replay feature is implemented, the UE should create dedicated child SA for each IP flow which has the same DSCP marking value.

#### 9.3.1.2 HA procedure

The HA shall set per QoS flow DSCP marking on IP outer header as specified in subclause 7.3.

#### 9.3.1.3 ePDG procedure

When receiving a downlink data packet for a UE, the ePDG shall copy the DSCP marking value from the received IP header into the new IPsec header before forwarding to the UE, as specified in subclause 7.3.

If the anti-replay feature is implemented, the ePDG should create dedicated child SA for each IP flow which has the same DSCP marking value.

Optionally, the ePDG may perform DSCP marking remapping based on the operator's policy.

## 9.3.2 UE local IP address change

### 9.3.2.1 General

If the UE receives a new local IP address from the Fixed Broadband Access network, the UE needs to update the IPsec tunnel with the ePDG.

#### 9.3.2.1 UE procedure

If the UE supports MOBIKE, the UE shall perform the tunnel modification procedure as defined in 3GPP TS 24.302 [2], subclause 7.2.3.

NOTE 1: in this case UE's Care-of Address remains unchanged and an update of the mobility tunnel towards the HA is not needed.

If the UE does not support MOBIKE, the UE shall perform the UE initiated disconnection procedure as defined in 3GPP TS 24.302 [2], subclause 7.2.4, followed by the tunnel establishment procedure, as defined in 3GPP TS 24.302 [2], subclause 7.2.2 and the Dual-Stack Mobile IPv6 handover procedure as defined in 3GPP TS 24.303 [14], subclause 5.2.2.

#### 9.3.2.2 ePDG procedure

If MOBIKE applies, the ePDG shall perform the tunnel modification procedure as defined in 3GPP TS 24.302 [2], subclause 7.4.2. If MOBIKE does not apply, the ePDG shall perform the procedure for UE initiated disconnection as defined in 3GPP TS 24.302 [2], subclause 7.4.3.2, and the tunnel establishment procedure as defined in 3GPP TS 24.302 [2], subclause 7.4.1.

#### 9.3.2.2 HA procedure

If triggered by the procedure in subclause 9.3.2.1, the HA shall perform the Dual-Stack Mobile IPv6 handover procedure as defined in 3GPP TS 24.303 [14], subclause 5.2.3.

NOTE: If the UE does not support MOBIKE, UE's Care-of Address will change during the procedure described in subclause 9.3.2.1.

---

## 10 UE – EPC Network Procedures for Fixed Broadband Access network using H(e)NB

### 10.1 General

This clause is related to the procedures of 3GPP system and Fixed Broadband Access network interworking for H(e)NB case and potential impacts to CT1 Specification.

### 10.2 Tunnel management procedures

#### 10.2.1 General

The IPsec tunnel is established using the IKEv2 protocol as defined in IETF RFC 5996 [16] between the H(e)NB and the SeGW. The IPsec ESP is supported (see IETF RFC 4303 [19]) in order to provide secure tunnels between the H(e)NB and the SeGW.



If NAT is deployed in an IPv4 Fixed Broadband Access Network, the H(e)NB behind the NAT uses the NAT traversal for IKEv2. The IPsec tunnel is encapsulated over UDP in the Tunnel-Mode as specified in IETF RFC 5996 [16]. The H(e)NB can request the SeGW to return the H(e)NB local IP address as described in 3GPP TR 29.839 [20].

All the above means that there is not impact to the tunnel management procedures defined by the subclause 8.2 when H(e)NB is used.

## 10.2.2 Impacts to CT1

There is no identified impact to CT1 by using tunnel management procedures via the H(e)NB and the SeGW for 3GPP access and Fixed Broadband Access network interworking.

## 10.3 Supporting QoS with H(e)NB procedure

### 10.3.1 General

When forwarding the UE uplink traffic, the H(e)NB supports DSCP marking on the outer IP header. Based on H(e)NB configuration either the QCI mapping or the Reflective QoS may be used as described in 3GPP TR 29.839 [20].

If the anti-replay feature is implemented, the H(e)NB(uplink) creates dedicated child SA for each IP flow which has the same DSCP marking value. The H(e)NB should map IP flows of different DSCP to different child SA.

When receiving a downlink data packet for a UE, the SeGW copies the DSCP value from the received IP header into the new IPsec header before forwarding to the H(e)NB using the IPsec tunnel, as specified in the subclause 7.3.

For the control-plane downlink traffic, the relevant message can be marked with the appropriate DSCP by the relevant network entity (e.g. H(e)MS, MME/SGSN) according to the preconfigured QoS. The SeGW copies this DSCP if it exists from the received IP header into the new IPsec header.

Optionally, the SeGW may perform DSCP marking remapping based on the operator's policy.

If the anti-replay feature is implemented, the SeGW (downlink) should create dedicated child SA for each IP flow which has the same DSCP marking value. The SeGW should map IP flows of different DSCP to different child SA.

All the above means that the QCI mapping and the Reflective QoS is achieved by the H(e)NB. Furthermore, the SeGW performs copy of the per-flow DSCP marking to the new outer header unless DSCP remapping is performed.

### 10.3.2 Impacts to CT1

There is no identified impact to CT1 by the use of QCI mapping and Reflective QoS via the H(e)NB and the SeGW for 3GPP access and Fixed Broadband Access network interworking.

## 10.4 Supporting CS domain services with HNB procedure

### 10.4.1 General

In the CS domain services with HNB procedure, at call setup procedures, the HNB GW can intercept the RAB assignment message received from MSC and send HNB information and correlated QoS requirement to the PCRF. Then the PCRF can notify the BPCF to modify the Fixed Broadband Access resource to support the CS service for the UE. The corresponding procedures are specified in 3GPP TS 23.139 [1]. Hence, there is no change in the procedures or signalling between the UE and the core-network in order to support CS domain services for 3GPP access and Fixed Broadband Access network interworking.

### 10.4.2 Impacts to CT1

There is no identified impact to CT1 by supporting CS via S15 session management between HNB Gateway and PCRF for 3GPP access and Fixed Broadband Access network interworking.

---

## 11 UE – EPC Network Procedures for Fixed Broadband Access network over S2a

*Editor's note: UE- EPC function description and procedure of 3GPP access and trusted Fixed Broadband Access network interworking using S2a.*

---

## 12 Non-seamless WLAN offload traffic

### 12.1 General

A non-seamless offload capable UE selects a Fixed Broadband Access for non-seamless WLAN offload as specified in 3GPP TS 24.302 [2].

### 12.2 UE procedure

The UE may use any local IP address(es) for non-seamless WLAN offload traffic. The UE local IP address allocation procedure is specified in BBF WT-146 [15].

The UE may support the UE reflective QoS for non-seamless WLAN offload uplink traffic as specified in subclause 7.2. The UE reflective QoS function may be enabled by the network at 'EAP-AKA and EAP-AKA' based access authentication as specified in subclause 7.4.

### 12.3 Network procedure

The Fixed Broadband Access may provide QoS on the non-seamless WLAN offload traffic if the 3GPP based access authentication is performed. If NAT between the UE and the network is detected, only default QoS is applied.

When forwarding a downlink data packet to a UE, the Fixed Broadband Access network may set the DSCP value on the outer header of each IP packet at per-flow basis as specified in subclause 7.3.

---

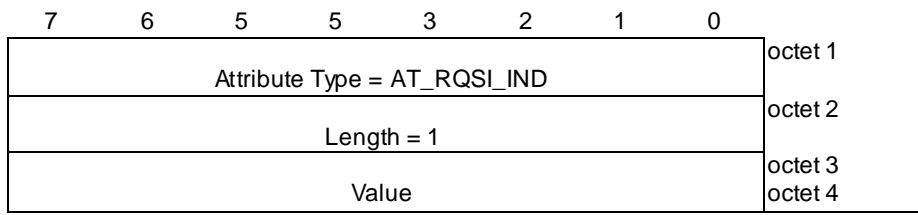
## 13 PDUs and parameters specific to the present document

*Editor's note: description of additional parameters to 24.302*

### 13.1 IETF RFC coding information defined within present document

#### 13.1.1 RQSI attributes

##### 13.1.1.1 AT\_RQSI\_IND attribute

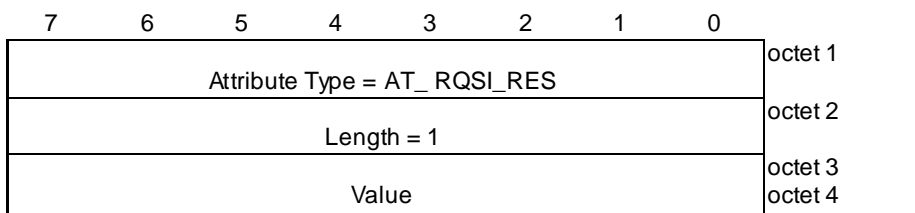


**Figure 13.1.1.1: AT\_RQSI\_IND attribute**

**Table 13.1.1.1: AT\_RQSI\_IND attribute**

<p>Octet 1 indicates the type of attribute as AT_RQSI_IND with a value of xxx1.  <b>Editor note's: the value of this attribute needs to be allocated by IANA.</b></p>								
<p>Octet 2 is the length of this attribute which shall be set to 1 as per IETF RFC 4187 [4]</p>								
<p>Octet 3 and 4 is the value of this attribute. Octet 3 is reserved and shall be coded as zero. Octet 4 shall be set as follows. All other values are reserved.</p>								
<b>7</b>	<b>6</b>	<b>4</b>	<b>5</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>0</b>	Protocol Supported
0	0	0	0	0	0	0	1	reflective QoS function is supported
0	0	0	0	0	0	1	0	reflective QoS function is not supported

13.1.1.2 AT\_RQSI\_RES attribute



**Figure 13.1.1.2: AT\_RQSI\_RES attribute.**

**Table 13.1.1.2: AT\_RQSI\_RES attribute**

<p>Octet 1 indicates the type of attribute as AT_RQSI_RES with a value of xxx2.  <b>Editor's note: the value of this attribute needs to be allocated by IANA.</b></p>								
<p>Octet 2 is the length of this attribute which shall be set to 1 as per IETF RFC 4187 [4]</p>								
<p>Octet 3 and 4 is the value of this attribute. Octet 3 is reserved and shall be coded as zero. Octet 4 shall be set as follows. All other values are reserved.</p>								
<b>7</b>	<b>6</b>	<b>4</b>	<b>5</b>	<b>3</b>	<b>2</b>	<b>1</b>	<b>0</b>	Protocol Selected
0	0	0	0	0	0	0	1	Enabling the UE reflective QoS function
0	0	0	0	0	0	1	0	Disabling the UE reflective QoS function

---

## 14 Conclusion

The TR is ready for normative text work and a new TS is required.

The following procedures shall be moved into the normative text:

- General (Subclause 4, 5 and 6 of this TR)
- Support of QoS (Subclause 7 of this TR)
- Additional Tunnel management procedure (Subclause 8 and 9 of this TR)
- Non-seamless WLAN Offload (Subclause 12 of this TR)
- PDUs and parameters specific to the present document (Subclause 13 of this TR)

The following procedures will not be moved into the normative text:

- UE – EPC Network Procedures for Fixed Broadband Access network using H(e)NB (Subclause 10 of this TR)
- UE – EPC Network Procedures for Fixed Broadband Access network over S2a (Subclause 11 of this TR)

## Annex A (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2011-10					Draft skeleton provided in C1-114416 by rapporteur to CT1#74.		0.0.1
2011-10	CT1#74				Includes the following contribution agreed by CT1 at CT1#74: C1-114415	0.0.1	0.1.0
2011-11	CT1#75				Includes the following contribution agreed by CT1 at CT1#75: C1-114996, C1-114997, C1-115346.	0.1.0	0.2.0
2012-02	CT1#76				Includes the following contribution agreed by CT1 at CT1#76: C1-120512, C1-120513, C1-120834, C1-120835, C1-120836	0.2.0	0.3.0
2012-04	CT1#77				Includes the following contribution agreed by CT1 at CT1#76: C1-121519, C1-121520, C1-121521, C1-121522, C1-121652, C1-121727	0.3.0	0.4.0
2012-05	CT1#78				Includes the following contribution agreed by CT1 at CT1#78: C1-122039, C1-122192, C1-122197, C1-122198, C1-122199, C1-122425, C1-122196	0.4.0	0.5.0
2012-06	CT-56	CP-120282			V1.0.0 created by MCC for presentation to CT-56 for information and approval	0.5.0	1.0.0
2012-06	CT-56				V11.0.0 created by MCC after approval at CT-56	1.0.0	11.0.0