ETSI TS 124 139 V11.0.0 (2012-10)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP System - Fixed Broadband
Access Network Interworking;
Stage 3
(3GPP TS 24.139 version 11.0.0 Release 11)

Reference
DTS/TSGC-0124139vb00

Keywords
LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

ETSI

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

This Technical Specification has been produced by the 3rd 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 specifies the UE – EPC procedures for accessing 3GPP Evolved Packet Core (EPC) via a Fixed Broadband Access network.

The specification covers the Support of QoS, Tunnel management procedures including the support of NAT traversal, and non-seamless offloading 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2]   3GPP TS 23.139: "3GPP System-Fixed Broadband Access Network Interworking".

[3]   3GPP TS 24.302: "Access to the Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[4]   3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6; Stage 3".

[5]   IETF RFC 2474 (December 1998): "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[6]   IETF RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[7]   IETF RFC 5996 (September 2010): "Internet Key Exchange Protocol Version 2 (IKEv2)".

[8]   IETF RFC 4555 (June 2006): "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[9]   IETF RFC 3948 (January 2005): "UDP Encapsulation of IPsec ESP Packets".

[10]   IETF RFC 4301 (December 2005): "Security Architecture for the Internet Protocol".

[11]   Broadband Forum TR-058: " Multi-service Architecture and Framework Requirements", September 2003.

[12]   Broadband Forum TR-059: "Architecture Requirements for the Support of QoS-Enabled IP Service", September 2003.

[13]   Broadband Forum TR-101: "Migration to Ethernet-based DSL Aggregation", July 2011.

[14]   Broadband Forum WT-134: "Policy Control Framework" (work in progress).

Editors note: The above BBF specification works in progress. It cannot be formally referenced until it is published by BBF.

[15]   Broadband Forum WT-145: "Multi-service Broadband Network Functional Modules and Architecture" (work in progress).

Editors note: The above BBF specification works in progress. It cannot be formally referenced until it is published by BBF.

[16]   Broadband Forum WT-203: "Interworking between Next Generation Fixed and 3GPP Wireless Access" (work in progress).

Editors note: The above BBF specification works in progress. It cannot be formally referenced until it is published by BBF.

[17]   Broadband Forum WT-146: "Subscriber Sessions", Revision 22 – July 2012 (work in progress – Straw ballot).

Editors note: The above BBF specification is in straw ballot. It cannot be formally referenced until it is published by BBF.

3   Definitions and abbreviations

3.1   Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] 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 [1].

Fixed Broadband Access network: Fixed Broadband Access network is a type of high-speed Internet access for multi-service broadband packet networking. The Fixed Broadband Access system is specified by the Broadband Forum in BBF TR-058 [11], BBF TR-059 [12], BBF TR-101 [13], BBF WT-134 [14], BBF WT-145 [15], and BBF WT-203 [16].

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 [2].

Non-seamless WLAN offload (NSWO): NSWO is a capability of a UE supporting routing specific IP flows over the WLAN access without traversing the EPC as defined in 3GPP TS 23.139 [2].

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.303 [4] subclause 3.1 apply:

   Home Agent (HA)

3.2   Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

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

4 General

4.1 Support of Fixed Broadband Access Network Interworking

The support of fixed broadband access network is based on the network configuration as specified in 3GPP TS 23.139 [2]. The fixed broadband access network interworking related functions are triggered by the network if the network knows the UE local access network is a fixed broadband access network. For instance, the network can be statically configured with a mapping between the UE local IP address and the local access network type.

For access to 3GPP Evolved Packet Core (EPC) via a fixed broadband access network or non-seamless WLAN offload at a fixed broadband access network or both, the EPC network procedures and the UE procedures are specified in this document. In all other cases, the EPC network procedure and the UE procedures are specified in 3GPP TS 24.302 [3] and 3GPP TS 24.303 [4].

4.2 Network Discovery and Selection

4.2.1 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 [3] is applied.

4.2.2 EPC network selection

When interworking with Fixed Access Broadband, the EPC network selection procedures specified in 3GPP TS 24.302 [3] is applied.

4.2.3 Access Network reselection

When interworking with Fixed Access Broadband, the access network reselection procedures specified in 3GPP TS 24.302 [3] is applied.

4.2.4 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 [3] is applied.

4.3 UE – EPC Network Protocols

4.3.1 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 [3] is applied.

4.3.2 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 [3] is applied.

4.3.3 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 [3] is applied.

5 Supporting QoS

5.1 General

When interworking with a fixed broadband access network, DSCP marking is used for setting QoS as specified in IETF RFC 2474 [5].

For downlink traffic, the 3GPP network sets the DSCP value on the outer header of each IP packet on a 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 performs QoS treatment and QoS remapping based on DSCP value of the outer IP header.

5.2 UE reflective QoS procedures

5.2.1 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 is enabled by the network as specified in subclause 5.4.

5.2.2 DSCP marking rule

The DSCP marking rules contains following parameter values:

- 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 outer IP header 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 applied.

5.2.3 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.

Depending 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.

5.2.4 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 follows:

- 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.

5.2.5 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 a 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 IP header of the packet 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 IP header of the packet 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 IP header of the packet.

If a tunnel is established between the UE and the network, the UE shall copy the DSCP value from the IP header of the original packet into the new outer header at the tunnel encapsulation before forwarding it to the network.

5.3 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 [2].

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.

5.4 Enabling UE reflective QoS function

5.4.1 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.

5.4.2 UE procedure

5.4.2.1 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, which extends these protocols as specified in subclause 8.2 of IETF RFC 4187 [6]. This attribute is provided in EAP-Response/AKA-Challenge and the 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'. This 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 8.1.1.

5.4.2.2 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 occurs;

    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 occurrs;

    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.

5.4.3 Network procedure

5.4.3.1 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 5.4.2.1, 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 8.1.1.

6 Tunnel management procedure

6.1 Tunnel management procedures over S2b

6.1.1 General

The purpose of tunnel management procedures is to establish or disconnect an end-to-end tunnel between the UE and the ePDG for S2b access to 3GPP Evolved Packet Core (EPC) via a fixed broadband access network.

The tunnel management procedures specified in 3GPP TS 24.302 [3] subclause 7 are applied. In addition, the procedures specified in this subclause shall be supported.

6.1.2 UE procedures

6.1.2.1 Tunnel establishment

Once the ePDG has been selected, the UE shall initiate the IPsec tunnel establishment procedure using the IKEv2 protocol as specified in 3GPP TS 24.302 [3] subclause 7.2.2 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 8.1.1.1 within the IKE_AUTH request message;

b) if MOBIKE is supported, the UE shall include the MOBIKE_SUPPORTED notification in the IKE_AUTH request message;

c) in an IPv4 fixed broadband access network, NAT may be deployed, e.g. a UE may behind a Residence Gateway which has a NAT function enabled. The UE shall support the NAT detection function as specified in IETF RFC 5996 [7]; and

d) if NAT is detected between the UE and the ePDG,

- the UE shall invoke the IKEv2 NAT traversal procedure as specified in IETF RFC 5996 [7];

- the UE shall use UDP encapsulated for ESP as specified in IETF RFC 5996 [7]; and

- the UE may send the NAT-keepalive packet to keep NAT mapping alive as defined in the IETF RFC 3948 [9].

6.1.2.2 Tunnel modification

The UE shall support the tunnel modification procedure specified in 3GPP TS 24.302 [3] subclause 7.2.3.

The tunnel modification procedure may be triggered if the UE local IP address or the NAT UDP port number or both have been reassigned. For instance, the Residence Gateway NAT function may be restarted for some reasons. As the result of the NAT restart, the UE local IP address and the mapping of the NAT UDP port number may be reassigned.

If the UE detects that the local IP address or the NAT UDP port number or both are reassigned, the UE shall:

- disconnect the tunnel as specified in subclause 6.2.3 and re-initiate the tunnel establishment procedure as specified in subclause 6.2.1; or

- use MOBIKE for recovering the IKEv2 SA as specified in IETF RFC 4555 [8].

If MOBIKE is supported, the UE shall support the tunnel modification procedure specified in 3GPP TS 24.302 [3] subclause 7.2.3 with the following additions:

- the UE shall perform the Dead Peer Detection (DPD) procedure to detect if NAT mapping have changed as specified in IETF RFC 4555 [8];

- if NAT remapping is detected, the UE shall update the IKEv2 security association with the new address, and shall then send an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification to the ePDG; and

- when the UE receives an INFORMATIONAL request with a COOKIE2 notification present, the UE shall copy the notification to the COOKIE2 notification of an INFORMATIONAL response and send it to the ePDG.

6.1.2.3 Tunnel disconnection

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

6.1.2.4 Support of reflective QoS

The UE may support reflective QoS for uplink traffic as specified in subclause 5.2.

If reflective QoS is supported and IPsec anti-replay feature specified in IETF RFC 4301 [10] is implemented, the UE should create dedicated child SA for each IP flow which has the same DSCP marking value. If not, the UE may choose

to increase the IPsec anti-replay window size or use any other implementation-specific method to avoid the sequence issue.

6.1.3 ePDG procedure

6.1.3.1 Tunnel establishment

Upon receipt of an IKE_AUTH request message from the UE requesting the establishment of a tunnel, the ePDG shall perform the tunnel establishment procedure as specified in 3GPP TS 24.302 [3] with the following additions:

a) the ePDG shall support the NAT detection function as defined in section 2.23 of IETF RFC 5996 [7];

b) if MOBIKE_SUPPORTED notification is received, the ePDG shall include the MOBIKE_SUPPORTED notification in the IKE_AUTH response message;

c) if NAT is detected between the UE and the ePDG, the ePDG shall use UDP encapsulated for ESP as defined in IETF RFC 5996 [7]; and

d) 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.

6.1.3.2 Tunnel modification

If MOBIKE applies, the ePDG shall perform the tunnel modification procedure as defined in 3GPP TS 24.302 [3], 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 [3], subclause 7.4.3.2, followed by the tunnel establishment procedure as defined in 3GPP TS 24.302 [3], subclause 7.4.1.

6.1.3.3 Tunnel disconnection

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

6.1.3.4 Support of QoS

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 5.3.

If the anti-replay feature specified in IETF RFC 4301 [10] is implemented, the ePDG should create a dedicated child SA for each IP flow which has the same DSCP marking value; or, the ePDG may choose to increase the IPsec anti-replay window size or use any other implementation-specific method to avoid the out of sequence issue.

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

6.2 Tunnel management procedure over S2c

6.2.1 S2c procedure over trusted fixed broadband access network

6.2.1.1 General

The purpose of tunnel management procedures is to establish or disconnect an end-to-end tunnel between the UE and the HA for S2c access to 3GPP Evolved Packet Core (EPC) via a trusted fixed broadband access network.

The tunnel management procedures specified in 3GPP TS 24.303 [4] clause 5 are applied. In addition, the procedures specified in this subclause shall be supported.

6.2.1.2 UE procedure

6.2.1.2.1 Dual-Stack Mobile IPv6 initial attach

Once the HA has been selected, the UE shall initiate the Dual-Stack Mobile IPv6 initial attach procedure specified in 3GPP TS 24.303 [4], subclause 5.1 with the following additions:

a) if the UE supports Reflective QoS, the UE may provide the RQSI using AT_ RQSI_IND attribute as defined in subclause 8.1.1.1 within the IKE_AUTH request message;

b) If MOBIKE is supported, the UE shall include the MOBIKE_SUPPORTED notification in the IKE_AUTH request message;

c) in an IPv4 fixed broadband access network, NAT may be deployed, e.g. a UE may behind a Residence Gateway which NAT function is enabled. The UE shall support the NAT detection function as specified in IETF RFC 5996 [7] and IETF RFC 4555 [8];

d) If NAT is detected between the UE and the HA,

  - the UE shall invoke the IKEv2 NAT traversal procedure as specified in IETF RFC 5996 [7];

  - the UE shall use UDP-Encapsulated ESP as defined in IETF RFC 5996 [7] and IETF RFC 4555 [8]; and

  - the UE may send the NAT-keepalive packet to keep NAT mapping alive as defined in IETF RFC 3948 [9] and IETF RFC 4555 [8].

6.2.1.2.2 Dual-Stack Mobile IPv6 handover

The Dual-Stack Mobile IPv6 handover procedure shall be triggered if the UE local IP address has been reassigned, or the UE moves from one link to another link.

The UE procedure of Dual-Stack Mobile IPv6 handover is specified in 3GPP TS 24.303 [4], subclause 5.2.

If the UE detects that the local IP address or the NAT UDP port number or both are reassigned, the UE shall update the mobility tunnel with the HA by initiating the Dual-Stack Mobile IPv6 handover.

6.2.1.2.3 Dual Stack Mobile IPv6 Re-Registration

The UE procedure of Dual-Stack Mobile IPv6 Re-Registration is specified in 3GPP TS 24.303 [4], subclause 5.3.

6.2.1.2.4 Dual-Stack Mobile IPv6 detach

The UE procedure of Dual-Stack Mobile IPv6 detach is specified in 3GPP TS 24.303 [4], subclause 5.4.

6.2.1.2.5 Support of reflective QoS

The UE may support UE Reflective QoS function for uplink traffic as specified in subclause 5.2.

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 [10] is implemented, the UE should create dedicated child SA for each IP flow which has the same DSCP marking value; or, the UE may choose to increase the IPsec anti-replay window size or use any other implementation-specific method to avoid the sequence issue.

6.2.1.3 HA procedure

6.2.1.3.1 Dual-Stack Mobile IPv6 initial attach

Upon receipt of an IKE_AUTH request message from the UE requesting the establishment of a tunnel, the HA shall perform the Dual-Stack Mobile IPv6 initial attach procedure as specified in 3GPP TS 24.303 [4], subclause 5.1 with the following additions:

a) the HA shall support the NAT detection function as defined in section 2.23 of IETF RFC 5996 [7] and in IETF RFC 4555 [8];

b) if MOBIKE_SUPPORTED notification is received, the HA shall include the MOBIKE_SUPPORTED notification in the IKE_AUTH response message; and

c) if NAT is detected between the UE and the HA, the HA shall use UDP encapsulated for ESP as defined in IETF RFC 5996 [7].

6.2.1.3.2 Dual-Stack Mobile IPv6 handover

The Dual-Stack Mobile IPv6 handover procedure shall be triggered if the UE local IP address has been reassigned, or the UE moves from one link to another link.

The HA procedure of Dual-Stack Mobile IPv6 handover is specified in 3GPP TS 24.303 [4], subclause 5.2.

6.2.1.3.3 Dual Stack Mobile IPv6 Re-Registration

The HA procedure of Dual-Stack Mobile IPv6 Re-Registration is specified in 3GPP TS 24.303 [4], subclause 5.3.

6.2.1.3.4 Dual-Stack Mobile IPv6 detach

The HA procedure of Dual-Stack Mobile IPv6 detach is specified in 3GPP TS 24.303 [4], subclause 5.4.

6.2.1.3.5 Support of QoS

The HA shall set per QoS flow DSCP marking on the IP outer header as specified in subclause 5.3.

If S2c data integrity protection is used and the IPsec anti-replay feature specified in IETF RFC 4301 [10] is implemented, the HA should create a dedicated child SA for each IP flow which has the same DSCP marking value. Or, the UE may choose to increase the IPsec anti-replay window size or use any other implementation-specific method to avoid the out of sequence issue.

6.2.2 S2c procedure over un-trusted fixed broadband access network

6.2.2.1 General

The purpose of tunnel management procedures is to establish or disconnect an end-to-end tunnel between the UE and the HA for S2c access to 3GPP Evolved Packet Core (EPC) via an un-trusted fixed broadband access network.

The tunnel management procedures specified in 3GPP TS 24.303 [4] clause 5 are applied. In addition, the procedures specified in this subclause shall be supported.

6.2.2.2 UE procedure

The UE tunnel management procedure of the IPsec tunnel with ePDG is specified in subclause 6.1.2.

The UE tunnel management procedure of Dual-Stack Mobile IPv6 tunnel with the HA is specified in subclause 6.2.1.2.

The UE may support the UE reflective QoS for uplink traffic on the IPsec header as specified in subclause 6.1.2.4.

6.2.2.3 ePDG Procedure

The ePDG tunnel management procedure of the IPsec tunnel is specified in subclause 6.1.3.

The ePDG procedure for the support of QoS is specified in subclause 6.1.3.4.

6.2.2.4 HA Procedure

The HA tunnel management procedure of Dual-Stack Mobile IPv6 tunnel is specified in subclause 6.2.1.3.

The HA procedure for the support of QoS is specified in subclause 6.2.1.3.5.

7 Non-seamless WLAN Offload

7.1 General

A non-seamless offload capable UE selects a fixed broadband access network for non-seamless WLAN offload as specified in 3GPP TS 23.139 [2].

7.2 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 [17].

The UE may support the UE reflective QoS for non-seamless WLAN offload uplink traffic as specified in subclause 5.2. The UE reflective QoS function may be enabled by the network at EAP-AKA and EAP-AKA' based access authentication as specified in subclause 5.4.

7.3 Network procedure

The fixed broadband access network 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. How the NAT is detected by the UE and the network is out of the scope of this document.

When forwarding a downlink data packet to a UE, the fixed broadband access network may set the DSCP value on the outer IP header of each IP packet at per-flow basis as specified in subclause 5.3.

8 PDUs and parameters specific to the present document

8.1 IETF RFC coding information defined within present document

8.1.1 RQSI attributes

8.1.1.1 AT_RQSI_IND attribute

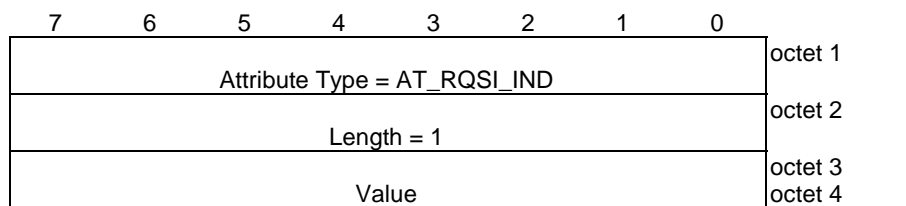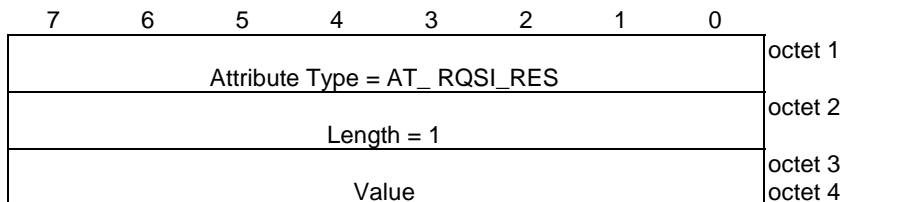| 7	6	5	4	3	2	1	0	
Attribute Type = AT_RQSI_IND								octet 1
Length = 1								octet 2
Value								octet 3
								octet 4

Figure 8.1.1.1-1: AT_RQSI_IND attribute

Table 8.1.1.1-1: AT_RQSI_IND attribute

Octet 1 indicates the type of attribute as AT_RQSI_IND with a value of xxx1.								
Editor note: the attribute shall be defined as a skippable attribute. The value of this attribute needs to be allocated by IANA.								
Octet 2 is the length of this attribute which shall be set to 1 as per IETF RFC 4187 [6]								
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.								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	Support of reflective QoS
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

8.1.1.2   AT_ RQSI_RES attribute

Figure 8.1.1.2-1: AT_ RQSI_RES attribute.

Table 8.1.1.2-1: AT_ RQSI_RES attribute

Octet 1 indicates the type of attribute as AT_ RQSI_RES with a value of xxx2.								
Editor note: the attribute shall be defined as a skippable attribute. The value of this attribute needs to be allocated by IANA.								
Octet 2 is the length of this attribute which shall be set to 1 as per IETF RFC 4187 [6]								
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.								
7	**6**	**5**	**4**	**3**	**2**	**1**	**0**	Reflective QoS decision
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

Annex A (informative):
Change history

					Change history		
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2012-05					Version 0.0.1: Preliminary proposal		0.0.1
2012-05	CT1#78				Includes the following contribution agreed by CT1 at CT1#78: C1-122424, C1-122484	0.0.1	0.1.0
2012-08	CT1#79				Includes the following contribution agreed by CT1 at CT1#79: C1-123080, C1-123082, C1-123083, C1-123084, C1-123085, C1-123366	0.1.0	0.2.0
2012-09	CT-57	CP-120607			Version 1.0.0 created by MCC for presentation at CT-57 for information and approval	0.2.0	1.0.0
2012-09	CT-57				Version 11.0.0 created by MCC after approval at CT-57	1.0.0	11.0.0

History

Document history		
V11.0.0	October 2012	Publication