ETSI TS 129 139 V14.0.0 (2017-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
3GPP system - fixed broadband access network interworking;
Home (e)Node B - security gateway interface
(3GPP TS 29.139 version 14.0.0 Release 14)

Reference
RTS/TSGC-0429139ve00

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

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 (https://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.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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 H(e)NB – SeGW interface. The interface is used for the interworking between a 3GPP system and a Fixed Broadband Access network defined by Broadband Forum. The interworking procedure provides the IP connectivity to a 3GPP UE using a H(e)NB connected to a Fixed Broadband Access network as specified in 3GPP TS 23.139 [2].

The specification covers the QoS aspects and Tunnel management procedures.

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; Stage 2".

[3] 3GPP TS 24.139: "3GPP System-Fixed Broadband Access Network Interworking; Stage 3".

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

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

[6] IETF RFC 3948: "UDP Encapsulation of IPsec ESP Packets".

[7] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

3 Definitions and abbreviations

3.1 Definitions

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

H(e)NB Reflective QoS function: H(e)NB Reflective QoS function is a H(e)NB function in order to support QoS for uplink traffic over a Fixed Broadband Access network as specified in 3GPP TS 23.139 [2].

H(e)NB local IP address Info: H(e)NB local IP address Info is defined as either the public IPv4 address or IPv6 address assigned to the H(e)NB by the Fixed Broadband Access Network domain, or the public IPv4 address and the UDP port number used by the NATed RG that is used for this H(e)NB. The public IPv4 address used by the NATed RG is assigned by the Fixed Broadband Access Network domain.

3.2 Abbreviations

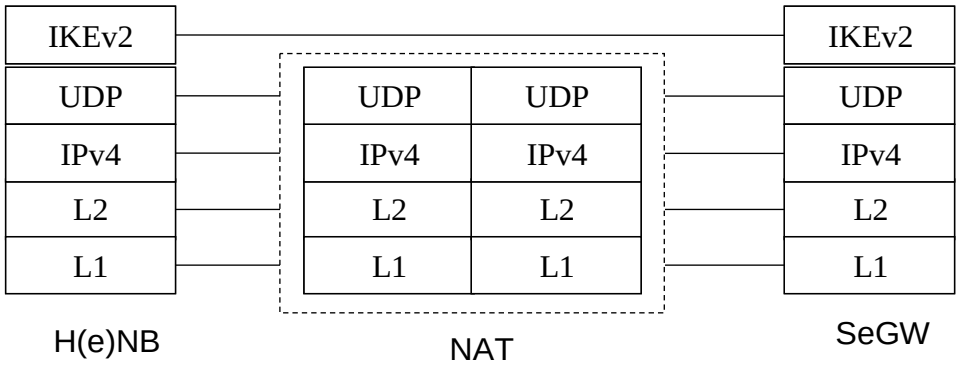
For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

DSCP	Differentiated Services Code Point
H(e)NB	Home (e)NodeB
NAT	Network Address Translation
NAT-T	NAT Traversal
SeGW	Security Gateway

4 General

4.1 Protocol Stack

4.1.1 Control Plane for H(e)NB – SeGW



Legend:

- **IKEv2 Protocol**: This protocol is used to between H(e)NB and SeGW. The IKEv2 protocol is defined in IETF RFC 5996 [5].

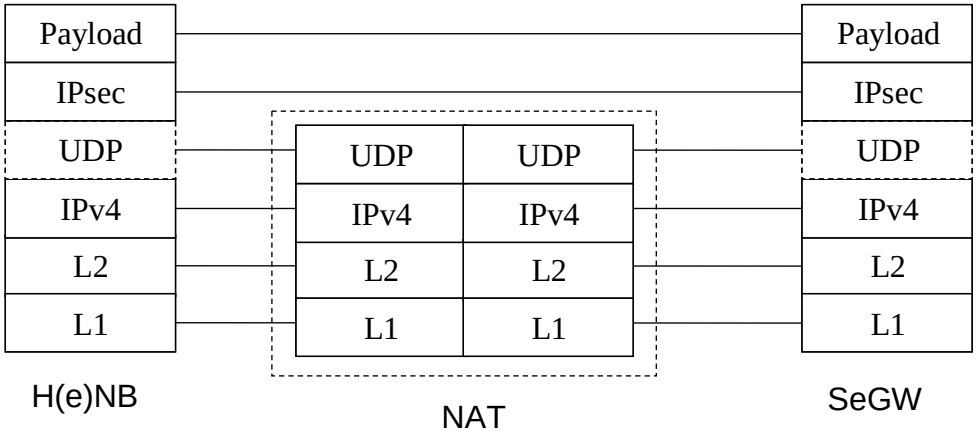
Figure 4.1.1-1: Control Plane for H(e)NB - SeGW Interface over IPv4 transport network

Legend:

- **IKEv2 Protocol:** This protocol is used to between H(e)NB and SeGW. The IKEv2 protocol is defined in RFC 5996 [5].

Figure 4.1.1-2: Control Plane for H(e)NB - SeGW Interface over IPv6 transport network

4.1.2 User Plane for H(e)NB – SeGW



Legend:

- **UDP:** UDP encapsulation is used if NAT is detected between the H(e)NB and the SeGW.

Figure 4.1.2-1: User Plane for H(e)NB - SeGW Interface over IPv4 transport network

Figure 4.1.2-2: User Plane for H(e)NB - SeGW Interface over IPv6 transport network

5 Supporting QoS

5.1 General

At interworking with a Fixed Broadband Access network, QoS is provided by DSCP marking as specified in IETF RFC 2474 [4].

5.2 H(e)NB procedures

5.2.1 General

The H(e)NB shall support DSCP marking on the IPsec header when forwarding the UE uplink traffic.

Based on H(e)NB configuration either the QCI mapping or the Reflective QoS may be used.

5.2.2 QCI mapping

The QCI mapping table contains a one-to-one mapping from QCI value to DSCP marking value. The QCI mapping table is configured in the H(e)NB by the operator.

When forwarding an uplink IP packet, the H(e)NB shall perform a lookup in the QCI mapping table based on the QCI value of the EPS bearer/PDP context before the IPsec tunnel encapsulation. The H(e)NB shall set the DSCP marking value of the IPsec header according to the matched QCI mapping table entry.

5.2.3 Reflective QoS

To support the H(e)NB Reflective QoS function for uplink traffic, the H(e)NB shall create and maintain the uplink DSCP marking rules for each active PDN connection as specified for UE Reflective QoS function in 3GPP TS 24.139 [3].

When forwarding an uplink IP packet, the H(e)NB shall perform a lookup in the DSCP marking table based on the n-tuple of the IP header before the IPsec tunnel encapsulation. If a matching entry is found, the H(e)NB shall set the DSCP marking value of the IPsec header according to the matched DSCP marking rule. If no matching entry is found, the H(e)NB shall copy the DSCP field of the outer IP header into the IPsec header before forwarding to the SeGW.

5.3 SeGW procedures

When receiving a downlink data packet, the SeGW shall copy the DSCP marking value from the outer IP header into the IPsec header before forwarding to the H(e)NB using the IPsec tunnel, as specified in 3GPP TR 23.139 [2].

6 Tunnel Management

6.1 General

The tunnel is an IPsec tunnel established via an IKEv2 protocol exchange IETF RFC 5996 [5] between the H(e)NB and the SeGW which is through the Fixed Broadband Access Network.

In an IPv4 Fixed Broadband Access Network, NAT can be deployed between the H(e)NB and the SeGW, e.g. in a Residence Gateway. A H(e)NB behind the NAT shall invoke the NAT traversal procedure for IKEv2. The IPsec tunnel is encapsulated over UDP in the Tunnel-Mode as specified in IETF RFC 5996 [5].

6.2 H(e)NB procedures

6.2.1 Tunnel establishment

6.2.1.1 IP address allocation

The SeGW shall provide the IP address to the H(e)NB for the communication with the EPC network.

For dynamic IP address allocation, the H(e)NB shall include the requested IP address type (IPv4 address or IPv6 address) that needs to be configured in an IKEv2 CFG_REQUEST Configuration Payload in the IKE_AUTH request message as defined in IETF RFC 5996 [5] after reception of the IKE_SA_INIT response from the SeGW.

6.2.1.2 NAT Traversal

NAT can be deployed in an IPv4 Fixed Broadband Access Network. IKEv2 NAT Traversal specified in section 2.23 of IETF RFC 5996 [5] shall be supported by H(e)NB.

If NAT is detected between the H(e)NB and SeGW, the following procedures shall be performed:

- UDP-Encapsulated ESP as defined in IETF RFC 5996 [5];
- sending the NAT-keepalive packet to keep NAT mapping alive if no other packet to the SeGW has been sent in M seconds as defined in the IETF RFC 3948 [6];

NOTE: M is a locally configurable parameter with a default value of 20 seconds as defined in the IETF RFC 3948 [6].

6.2.1.3 H(e)NB NATed Tunnel-IP address discovery

If NAT is detected between the H(e)NB and SeGW, the H(e)NB shall request the SeGW to return the H(e)NB local IP address information by including the EXTERNAL_SOURCE_IP4_NAT_INFO attribute as defined in subclause 7.1.1.1 in the CFG_REQUEST Configuration Payload within the IKE_AUTH request message. The length field of the attribute shall be set to zero. The NATed IPv4 Address field and UDP Port number field shall be absent.

If the H(e)NB subsequently receives the EXTERNAL_SOURCE_IP4_NAT_INFO attribute in the CFG_REPLY configuration payload from the SeGW, the H(e)NB shall report the IP address received in EXTERNAL_SOURCE_IP4_NAT_INFO attribute as the H(e)NB local IP address to the MME/SGSN.

6.2.2 Tunnel modification

NAT mappings can change when the UDP port number is reassigned by the NAT, and/or H(e)NB local IP address is reallocated due to NAT restart.

Upon NAT remapping, the SeGW initiates the tunnel disconnection procedure as specified in subclause 6.3.3. Then the H(e)NB shall re-initiate the tunnel establishment procedure as specified in sub-clause 6.2.1.

6.2.3 Tunnel disconnection

The H(e)NB shall use the procedures defined in IETF RFC 5996 [5] to disconnect an IPsec tunnel to the SeGW.

6.3 SeGW procedures

6.3.1 Tunnel establishment

6.3.1.1 IP address allocation

For dynamic IP address allocation, upon receipt of an IKE_AUTH request message from the H(e)NB requesting the IP address, the SeGW shall include the remote IP address information in the IKEv2 Configuration Payload (CFG_REPLY)

of the final IKE_AUTH response message to the H(e)NB. The SeGW shall assign either an IPv4 or an IPv6 address to the H(e)NB via a single CFG_REPLY Configuration Payload.

6.3.1.2 NAT Traversal

NAT can be deployed in an IPv4 Fixed Broadband Access Network. IKEv2 NAT Traversal specified in section 2.23 of IETF RFC 5996 [5] shall be supported by SeGW.

If NAT is detected between the H(e)NB and SeGW, the SeGW shall use UDP-Encapsulated ESP as defined in IETF RFC 5996 [5].

6.3.1.3 H(e)NB NATed Tunnel-IP address discovery

If the SeGW receives the EXTERNAL_SOURCE_IP4_NAT_INFO attribute as defined in subclause 7.1.1.1 in the CFG_REQUEST configuration payload within IKE_AUTH request message, the SeGW shall provide the H(e)NB local IP address information (i.e. NATed IPv4 address and UDP port number) to the H(e)NB by including the EXTERNAL_SOURCE_IP4_NAT_INFO attribute in the CFG_REPLY configuration payload within the IKE_AUTH response message.

6.3.2 Tunnel modification

NAT mappings can change when the UDP port number is reassigned by the NAT, and/or H(e)NB local IP address is reallocated due to NAT restart.

If NAT remapping is detected by the SeGW, the SeGW shall initiate the tunnel disconnection procedure (see subclause 6.3.3).

NOTE: No procedures are defined in current release of specification to enable the SeGW to send the modified H(e)NB local IP address information to the H(e)NB during the lifetime of IKEv2 security association.

6.3.3 Tunnel disconnection

The SeGW shall use the procedures defined in IETF RFC 5996 [5] to disconnect an IPsec tunnel to the H(e)NB.

7 PDUs and parameters specific to the present document

7.1 IETF RFC coding information defined within present document

7.1.1 IKEv2 Configuration Payloads attributes

7.1.1.1 EXTERNAL_SOURCE_IP4_NAT_INFO attribute

The format of the EXTERNAL_SOURCE_IP4_NAT_INFO attribute follows the definition of Configuration Attributes as specified in IETF RFC 5996 [5], section 3.15.1. The format is shown in figure 7.1.1.1-1 as below. The length of the EXTERNAL_SOURCE_IP4_NAT_INFO attribute is 0 or 6 bytes.

7	6	5	4	3	2	1	0	Octets
R	Attribute Type							1
Attribute Type								2
Length								3, 4
NATed IPv4 Address								5 - 8
UDP Port number								9 - 10

Figure 7.1.1.1-1: EXTERNAL_SOURCE_IP4_NAT_INFO attribute

The R bit in the first octet is as defined in IETF RFC 5996 [5].

The Attribute Type indicating EXTERNAL_SOURCE_IP4_NAT_INFO is of the value 23.

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2012-12	CT#58	CP-120895			V2.0.0 presented for approval	2.0.0	11.0.0
2012-12	CT#58	CP-120697	0001	-	Removal of invalid reference and editor's note	11.0.0	11.1.0
2014-09	-	-	-	-	Update to Rel-12 version (MCC)	11.1.0	12.0.0
2015-12	-	-	-	-	Update to Rel-13 version (MCC)	12.0.0	13.0.0
2016-03	CT#71	CP-160019	0004	1	Complete the EXTERNAL_SOURCE_IP4_NAT_INFO attribute information according to IANA registration	13.0.0	13.1.0
2017-03	CT#75	-	-	-	Update to Rel-14 version (MCC)	13.1.0	14.0.0

History

Document history		
V14.0.0	April 2017	Publication