3GPP TR 29.839 V11.0.0 (2012-06)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP system - fixed broadband access network interworking; Home (e)Node B - security gateway interface (Release 11)

Keywords
access, packet mode, 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

Contents

Foreword

This Technical Report 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 [3].

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 TR 41.001: "GSM Release specifications".

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

[4] 3GPP TR 24.820: "3GPP System-Fixed Broadband Access Network Interworking; 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 5996: " Internet Key Exchange Protocol Version 2 (IKEv2)".

[7] Void

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

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

[10] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

3 Definitions, symbols 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: 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 [3].

H(e)NB local IP address Info: 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 Symbols

For the purposes of the present document, the following symbols apply:

Editor note: adding symbols if there is any.

3.3 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].

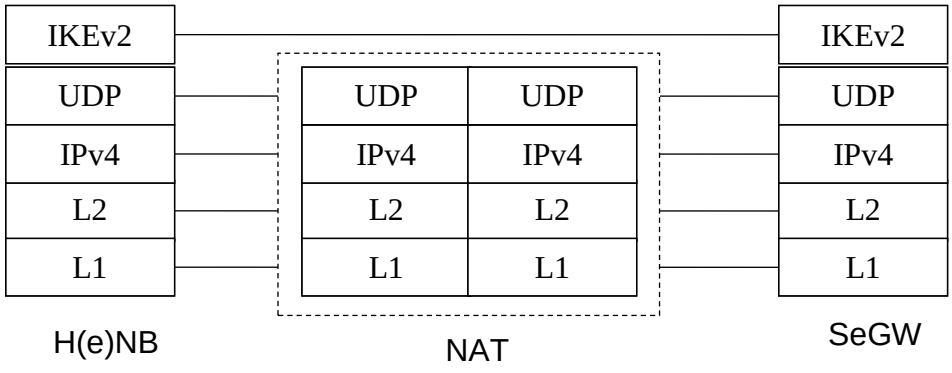
DSCP	Differentiated Services Code Point
H(e)NB	Home (e)NodeB
NAT	Network Address Translation
NAT-T	NAT Traversal
SeGW	Security Gateway

4 General

Editor note: general information

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 [6].

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 [6].

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 [5].

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 TR 24.820 [4].

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 [3].

6 Tunnel Management

6.1 General

The tunnel is an IPsec tunnel established via an IKEv2 protocol exchange IETF RFC 5996 [6] between the H(e)NB and the SeGW which is through the Fixed Broadband Access Network.

In an IPv4 Fixed Broadband Access Network, NAT may be deployed, e.g. RG. 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 [6]. When NAT is detected during IKEv2 procedure, the H(e)NB local IP address info (i.e. IP address and possible UDP port number) shall be provided to by the SeGW using IKEv2 signalling as specified in 3GPP TS 23.139 [3].

6.2 H(e)NB procedures

6.2.1 Tunnel establishment

6.2.1.1 IP address allocation

The IP address shall be allocated by the SeGW 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 [6] after reception of the IKE_SA_INIT response from the SeGW.

Editor note: It is FFS if the static IP address needs to be specified.

6.2.1.2 NAT Traversal

NAT may be deployed in an IPv4 Fixed Broadband Access Network. IKEv2 NAT Traversal specified in section 2.23 of IETF RFC 5996 [6] 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 [6];
- 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 [8];

NOTE: M is a locally configurable parameter with a default value of 20 seconds as defined in the IETF RFC 3948 [8].

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 in the CFG_REQUEST Configuration Payload within the IKE_AUTH request message. If the EXTERNAL_SOURCE_IP4_NAT_INFO attribute in the CFG_REQUEST Configuration Payload is received from the SeGW, the H(e)NB shall report the H(e)NB local IP address information to the MME. The format of the EXTERNAL_SOURCE_IP4_NAT_INFO attribute is shown in Figure A.1-1.

6.2.2 Tunnel modification

NAT mappings may 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, the H(e)NB may handle this case in following three ways:

- Tunnel re-setup. The H(e)NB tears down the IKEv2 SA and re-initiate the tunnel establishment procedure as specified in 6.2.1.
- Dynamic address update.
- MOBIKE. The H(e)NB uses MOBIKE for recovering the IKEv2 SA as specified in IETF RFC 4555 [9].

Editor's note: Whether MOBIKE needs to be required for H(e)NB is FFS.

If MOBIKE is supported by the H(e)NB, the following procedures of tunnel modification shall be performed:

- the H(e)NB shall include the MOBIKE_SUPPORTED notification in the IKE_AUTH request message;
- the H(e)NB performs Dead Peer Detection (DPD) to detect if NAT mapping have changed as specified in IETF RFC 4555 [9];

- if NAT remapping is detected, the H(e)NB shall update the IKE security association with the new address, and shall then send an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification to the SeGW;

- when the H(e)NB receives an INFORMATIONAL request with a COOKIE2 notification present, the H(e)NB shall copy the notification to the COOKIE2 notification of an INFORMATIONAL response and send it to the SeGW.

Editor's note: How the H(e)NB gets the modified NATed IP address information and inform the changes to the network after NAT remapping is FFS.

6.2.3 Tunnel disconnection

The H(e)NB shall use the procedures defined in IETF RFC 5996 [6] 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 may be deployed in an IPv4 Fixed Broadband Access Network. IKEv2 NAT Traversal specified in section 2.23 of IETF RFC 5996 [6] 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 [6].

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

If NAT is detected between the H(e)NB and SeGW, the SeGW shall provide the H(e)NB local IP address information to the H(e)NB by including the EXTERNAL_SOURCE_IP4_NAT_INFO attribute in the CFG_REQUEST Configuration Payload within the IKE_AUTH response message.

6.3.2 Tunnel modification

NAT mappings may change when the UDP port number is reassigned by the NAT. If NAT remapping is detected, the SeGW may handle this case in following three ways:

- Tunnel re-setup. The SeGW tears down the IKEv2 SA; or

- Dynamic address update.

- MOBIKE. The SeGW uses MOBIKE for recovering the IKEv2 SA as specified in IETF RFC 4555 [9].

Editor's note: Whether MOBIKE needs to be supported for SeGW is FFS.

If MOBIKE is supported by the SeGW the following procedures of tunnel modification shall be performed:

- when receiving an INFORMATIONAL request containing the UPDATE_SA_ADDRESSES notification, the SeGW shall check the validity of the IP address and update the IP address in the IKE security association with the values from the IP header, and shall reply with an INFORMATIONAL response;

- the SeGW may initiate a return routability check for the new address provided by the H(e)NB, by including a COOKIE2 notification in an INFORMATIONAL request and send it to the H(e)NB;
- when the SeGW receives the INFORMATIONAL response from the H(e)NB, it shall check that whether the COOKIE2 notification payload is the same as the one it sent to the H(e)NB. If it is different, the SeGW shall close the IKE security association by sending an INFORMATIONAL request message including a "DELETE" payload;
- If no return routability check is initiated by the SeGW, or if a return routability check is initiated and is successfully completed, the SeGW shall update the IPsec security associations associated with the IKE security association with the new address.

6.3.3 Tunnel disconnection

The SeGW shall use the procedures defined in IETF RFC 5996 [6] to disconnect an IPsec tunnel to the H(e)NB.

7 Conclusion

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

The followings are the open issues which shall be solved in the normative work:

- It's FFS if MOBIKE needs to be supported by H(e)NB and SeGW for tunnel management procedure at NAT remapping.
- If SA2 indicates that network based approach for NAT public address discovery is needed, Tunnel management procedure needs to be updated accordingly.
- It is FFS to define the IKEv2 extensions for NAT public address discovery and whether this is done either in IETF or 3GPP.

This conclusion is based on the current stage 2 agreement and this may change if any further changes are made by SA2 to the Stage 2

Annex A:
A.1 EXTERNAL_SOURCE_IP4_NAT_INFO attribute

The format of the EXTERNAL_SOURCE_IP4_NAT_INFO attribute is shown in figure A.1-1. The length of the EXTERNAL_SOURCE_IP4_NAT_INFO attribute is 4 or 6 bytes. The UDP Port number field is optional.

Editor's note: It is FFS the EXTERNAL_SOURCE_IP4_NAT_INFO attribute is defined in 3GPP or IETF.

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

Figure A.1-1: EXTERNAL_SOURCE_IP4_NAT_INFO attribute

Annex B:
Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2012-06	CT#56	CP-120256			Presented for information and approval	1.0.0	11.0.0