3GPP2 X.S0054-210-0
Version 1.0
Date: December 19, 2007

CMIP based Inter-AGW Handoff

This page is left blank intentionally.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

No table is described in this document.

REVISION HISTORY

Revision	Date	Remarks
0	December, 2007	Initial release

FOREWORD

(This foreword is not part of this Standard.)

This document was prepared by 3GPP2 TSG-X.

This document is a new specification.

This document is part of a multi-part document consisting of multiple parts that together describes Converged Access Network.

This document is subject to change following formal approval. Should this document be modified, it will be re-released with a change of release date and an identifying change in version number as follows:

X.S0054-210-X version n.0

where:

- X an uppercase numerical or alphabetic character [0, A, B, C, …] that represents the revision level.
- n a numeric string [1, 2, 3, …] that indicates an point release level.

This document uses the following conventions:

- “Shall” and “shall not” identify requirements to be followed strictly to conform to this document and from which no deviation is permitted.
- “Should” and “should not” indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.
- “May” and “need not” indicate a course of action permissible within the limits of the document.
- “Can” and “cannot” are used for statements of possibility and capability, whether material, physical or causal.

This page is left blank intentionally.

1 Introduction

This document describes inter-AGW handoff operation using Mobile IP (e.g., the AT implements MIP client functionality, called CMIP) for layer 3 mobility, for both active and idle handoffs. The seamless inter-AGW handoff is achieved using CMIP4 [7] and L2 tunneling between the eBSs that are connected to the Source AGW and Target AGW as specified in [2].

1.1 Scope

This document is part of a multi-part document consisting of multiple parts that together describes Ultra Mobile Broadband Wireless IP Network operation.

The scope of this document covers support for CMIP4 based Inter-AGW handoff.

2 References

2.1 Normative References

[1] 3GPP2: C.S0084-0 v2.0, “Ultra Mobile Broadband (UMB) Air Interface”, September 2007.

[2] 3GPP2: A.S0020-0 v1.0, “Interoperability Specification (IOS) for Ultra Mobile Broadband (UMB) Radio Access Network Interfaces”, November 2007.

[3] 3GPP2: X.S0054-100-0 v1.0, “ Basic IP Service for Converged Access Network Specification”, December 2007.

[4] 3GPP2: X.S0054-110 v1.0, “ MIP4 Specification in Converged Access Network Specification”, December 2007.

[5] IETF: IETF: draft-leung-mip4-proxy-mode

[Editor Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor’s Note is removed, the inclusion of the above document is for informational purposes only.]

[6] IETF: draft-yegani-gre-key-extension

[Editor Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor’s Note is removed, the inclusion of the above document is for informational purposes only.]

[7] IETF: RFC3344, Parkins, “IP Mobility Support for IPv4”, August 2002.

[8] 3GPP2: X.S0054-400-0, v1.0, “Converged Access Network Accounting Specification”, December 2007.

2.2 Informative References

This section provides references to other documents that may be useful for the reader of this document.

<1> 3GPP2: X.S0054-000-0 v1.0, “CAN Wireless IP Network Overview and List of Parts”, December 2007.

<2> 3GPP2: X.S0054-102-0 v1.0, “Multiple-Authentication and Legacy Authentication Support for CAN”, December 2007.

<3> 3GPP2: X.S0054-220-0 v1.0, “Network PMIP Support”, December 2007.

<4> 3GPP2: X.S0054-300-0 v1.0, “QoS Support for Converged Access Network Specification”, December 2007.

<5> 3GPP2: X.S0054-910-0 v1.0, “CAN Data Dictionary”, December 2007.

3 Inter-AGW Active Handoff

Mobility in the CAN network architecture is achieved via handoffs. A handoff between eBSs with connectivity to the same AGW such that the Source AGW remains the same before, during, and after handoff, is called Intra-AGW handoff. When the AT has an active session, a newly added eBS in the Route Set should be able to connect to the existing AGW. Therefore Intra-AGW handoff normally occurs. The intra-AGW handoff is specified in [2].

In some cases, inter-AGW Handoff occurs when the AT has an active session and a newly added eBS needs to connect with a different AGW from the Source AGW. This section addresses this scenario.

In this scenario, a different LinkID (which represents the new AGW that assigns the new CMIP4 care of address (e.g., CMIP4 FA CoA) is presented to the AT after the new eBS which is connected to a new AGW is added in the Route Set and after EAP Access Authentication is performed successfully. Once the new primary RAN PMIP4 tunnel is established between the new eBS and new AGW (Target AGW) the AT presents the new IP interface to upper layer which triggers CMIP4 binding update. See [2] for the details.

A new CMIP4 FA CoA is assigned to the AT and is associated with the newly established primary PMIP4 tunnel with the new AGW. A Client initiated CMIP4 binding is then performed. The primary PMIP4 tunnel from the previous DAP to the previous AGW is kept alive until that PMIP4 tunnel life-time expires or the AGW receives PMIP4 deregistration for the primary PMIP4 tunnel. The reverse link bindings to the previous AGW (if any) are also kept alive until the reverse link PMIP4 bindings life-times expire or the AGW receives PMIP4 deregistration for the reverse link PMIP4 tunnel.

During inter-AGW handoff, the AT keeps each IP interface (e.g., both CMIP4 FA CoAs under Source AGW and Target AGW) until all eBSs associated with that particular IP interface are dropped from the Route Set. This is so that the AT can receive/send the data from/to both IP interfaces during inter-AGW handoff period. Inter-AGW handoff is a Make-Before-Break process.

Figure 1 shows an example of inter-AGW handoff. In the figure, eBS0 and eBS1 are under AGW1 (associated with LinkID1) and eBS2 and eBS3 are under AGW2 (associated with LinkID2) and Mobile IP (e.g., CMIP4 as specified in [7]) is used for inter-AGW handoff. The AT has been in communication with eBS1 (DAP/FLSE/RLSE) connected with AGW1. The AT has just added eBS2 and eBS2 sent LinkID2 representing AGW2 to the AT. Due to radio conditions, the FLSE/RLSE is switched to eBS2.

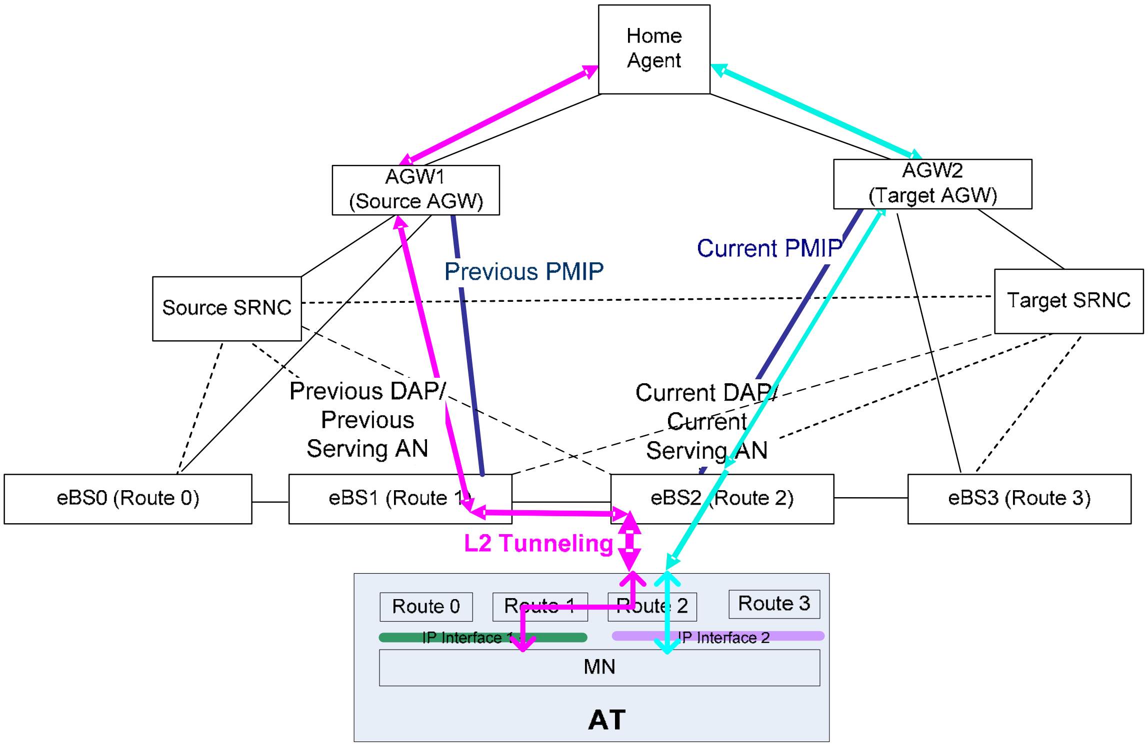

Figure 1 **An Example of Inter-AGW HO based on CMIP**

3.1 Reverse Link Operation

In Figure 1 , before handoff CMIP4 binding uses IP interface 1. When the application in the AT generates data, the MN in the AT sends the data to IP interface 1 associated with the LinkID 1 (which is associated with AGW1, called the Source AGW). The AT can use any stack associated with LinkID1 (e.g., Route 0 or Route 1 in Figure 1).

Since current RLSE (eBS2 in the figure) is not associated with LinkID1, the AT sends the packets to Route 1, which processes the packet and perform regular operation for sending it over the air, i.e., eBS1 is not the RLSE so the packet is sent to the IRTP protocol in Route 2 as specified in [1] to be tunneled through the Link-Layer Tunnel to eBS1. Once eBS1 receives the packet, it processes the packet and sends it to AGW1 (Source AGW).

This process continues as long as eBS2 is the RLSE and eBS1 is in the route set.

In parallel with previous steps, , the Target SRNC triggers EAP Access Authentication and Authorization to the AT. UponOnce successful EAP Authentication and Authorization is performed and the session configuration is completed, among AT, Target SRNC, Target AGW, and HAAA, eBS2 sends a new Link ID (LinkID2) to the AT. When eBS2 becomes DAP, the AT presents IP interface to the upper layer, which triggers the AT to retrieve a new IP address from the Target AGW (e.g., AT sends Agent Solicitation to retrieve a CMIP4 FA CoA for Interface 2.

eBS2 also forwards the IP packets received from the Target AGW to AT using Route2. See [2] for the details.

3.2 Forward Link Operation

On the forward-link, before handoff, the Mobile IP Home Agent sends data to the Source AGW. The Source AGW sends packets to eBS1 which is the DAP for the Source AGW (AGW1).

When eBS1 receives a packet for the AT from AGW1 (and the FLSE is eBS2 under AGW2), it uses its route (Route 1) to send the packet to eBS2 via Link-Layer tunneling protocol. Once the packet is transmitted from eBS2 to the AT, the AT processes the IP packet on the associated IP interface with Route 1 (IP interface 1 in Figure 1).

For CMIP4, after Mobile IP registration is successfully performed between the AT and HA, the Home Agent starts sending data to AGW2, which forwards packets to eBS2 (DAP under AGW2).

When eBS2 receives an IP packet for the AT from AGW2 (and the FLSE is eBS2), eBS2 uses its route (Route 2) to send the IP packet to the AT. Upon receipt of the packet, the AT uses the associated IP interface with Route 2 (i.e., IP interface 2) to process the packet.

3.3 AGW Requirements

The Source AGW shall clean up its resource when the primary PMIP4 lifetime expires and process remaining accounting messages per [8]. The Target AGW shall follow the requirement as specified in [3] for Access Authentication and Authorization and RAN PMIP4 tunnel operation. If the AGW receives AAA-Session-ID in the AAA message received from SRNC, the AGW shall include it in the AAA messages sent to the AAA during Access Authentication and Authorization procedures. For CMIP4 FA CoA address assignment, the Target AGW shall follow the requirements as specified in [4] for CMIP4 IP address assignment and CMIP4 registration procedure.

3.4 eBS Behavior

During inter-AGW handoff, the RAN PMIP4 tunnel between the source DAP and source AGW and the RAN PMIP4 tunnel between the target DAP (new DAP) and Target AGW are maintained simultaneously. The detailed requirements for the eBS are specified in [2].

3.5 SRNC Requirements

SRNC shall trigger EAP authentication by sending EAP Request/Identity to the AT as specified [3]. When the Target SRNC sends a AAA message to the AGW for EAP authentication, it shall include the AAA-Session-ID received from Source SRNC (for details on SRNC transfer refer to [2] in the AAA message as specified in [3]. The detailed requirements for SRNC are specified in [2] and [3].

3.6 AT Requirements

The AT shall support multiple IP interfaces as specified in [1]. When the AT is presented a new IP interface, the AT shall follow the requirement as specified in [4] for CMIP4 IP address assignment and CMIP4 registration procedures.

3.7 HAAA Requirements

If the HAAA receives AAA-Session-ID during EAP Access Authentication procedures from a different AGW, the HAAA determines the CAN Access session has not been terminated. Since the session is continued with the new AGW, the HAAA shall return the same AAA-Session-ID to the AGW in the AAA messages specified in [3] during Access Authentication and authorization procedures.

4 Inter-AGW AT Idle Handoff

This section describes Inter-AGW idle handoff. In this case, the Session Anchor is in Source SRNC, and Source SRNC is under Source AGW. Before AT performs the handoff, it is in idle state. Later, when AT crosses the AGW's boundary, the Session Anchor is moved to Target SRNC, Target AGW becomes a serving gateway for the AT. Client Mobile IPv4 is used to achieve seamless inter-AGW Idle handoff.

See [2] for the details.

4.1 AGW Requirements

See section 3.3.

4.2 SRNC Requirements

See section 3.5.

4.3 AT Requirements

See section 3.6.

4.4 HAAA Requirements

See section 3.7.

5 Call Flows

5.1 Inter-AGW Handoff

Figure 2 illustrates an example call flow for client CMIP4 based inter-AGW Handoff.

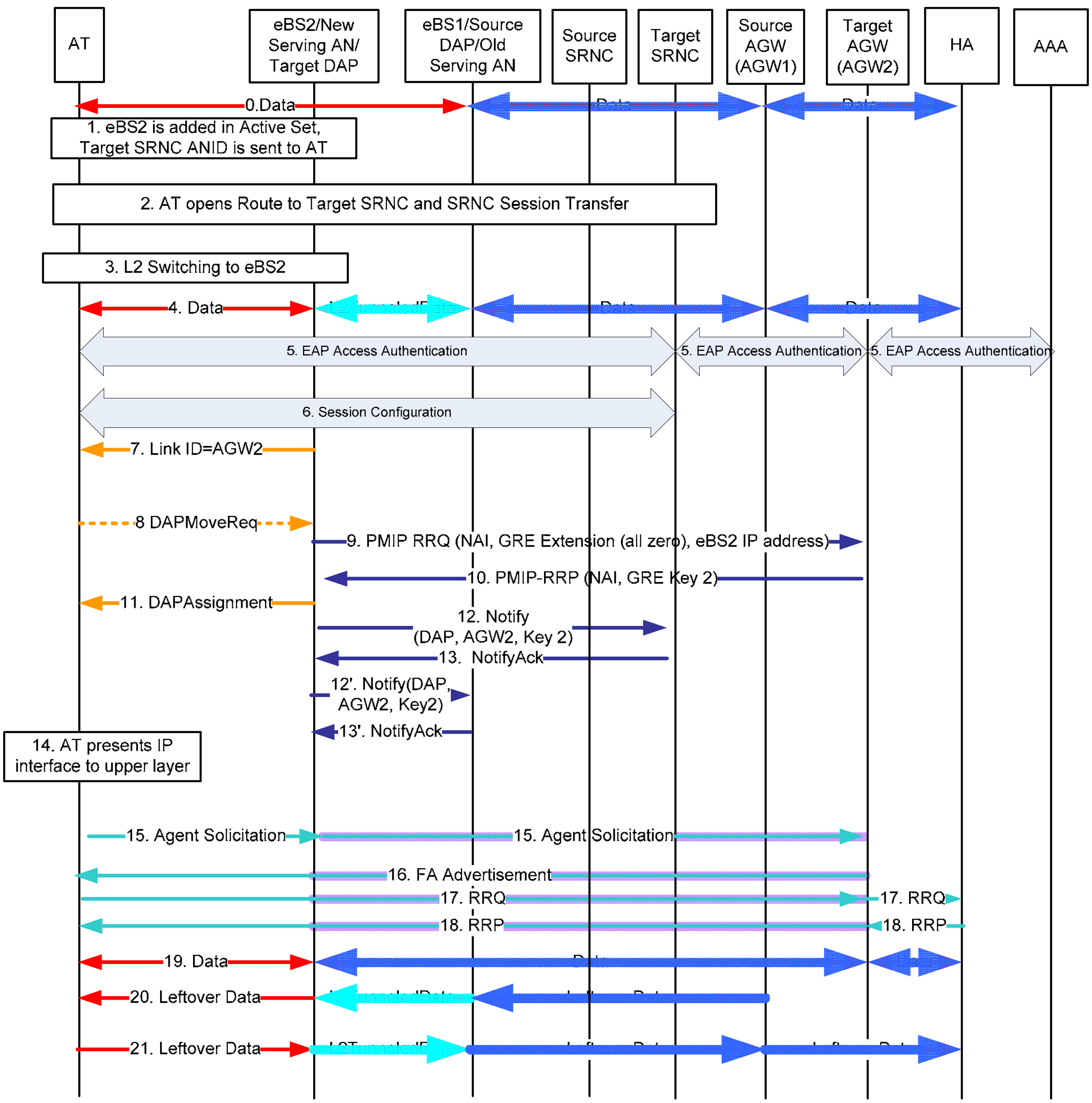

Figure 2 **An example call flow for client CMIP4 based inter-AGW Handoff**

The steps in Figure 2 are described below:

0. The AT sends/receives IPv4 packets to/from the HA through the CMIP4 tunnel between the HA and source AGW (AGW1) and the tunnel between eBS1 (that serves as both Serving eBS and DAP) and AGW.
1. The AT requests to add eBS2 in the Route Set. In this example, eBS2 is connected to AGW2 and Target SRNC. The target SRNC ANID is sent to the AT.
2. The AT opens Route to the Target SRNC and the SRNC session transfer is performed. The target SRNC assigns a new UATI to the AT. As a part of UATI assignment, the Target SRNC fetches session information from Source SRNC. See IOS document for the details.
3. The AT performs L2 fast switching to eBS2.
4. The AT sends/receives IPv4 packets to/from the HA through the CMIP4 tunnel between the HA and source AGW (AGW1), the GRE tunnel between eBS1 (that serves as both Serving eBS and DAP) and AGW, and the L2 tunnel between eBS1/DAP and eBS2.
5. The Target SRNC triggers full EAP Access Authentication and Authorization. (See [3] on Access Authentication and Authorization call flow.)
6. The Target SRNC sends session information to eBS2 through IOS signaling in which AGW2 IP address, LinkID, NAI, AAA-Session-ID, and PMN-AN-HA1 key are sent to eBS2. (See [2] for the details.)
7. eBS2 presents link ID to the AT. The link ID represents the IP interface that the AT creates to talk to IP layer.
8. This step is optional. It is performed only for AT assisted DAP move (see [2]). The AT sends DAPMoveReq message to eBS2.
9. Since eBS2 doesn't have the GRE key associated with AGW2, eBS2 sends a RAN PMIP4 RRQ (see [5]) to AGW2 which includes GRE Extension (all zero), NAI (formatted as AAA-Session-ID@Realm, where AAA-Session-ID is received from SRNC at step 6, and Realm is the Realm portion of NAI received from SRNC at step 6) eBS2's IP address, and MN-HA authentication extension calculated by using PMN-AN-HA1 key received from step 6.
10. AGW2 selects a GRE key 2 associated with this NAI and includes it through GRE extension (see [6]) in the RAN PMIP4 RRP sent to eBS2.
11. eBS2 sends DAP Assignment to the AT.
12. eBS2 notifies other Route Set members (SRNC, eBS1) of AGW2 IP address and GRE key 2 through IOS signaling (see [2] for the details.)
13. The SRNC and eBS1 send Notify Ack back to eBS2.
14. The AT presents the link ID to the upper IP layer. The upper IP layer compares the link ID with its current link ID. Since it is different from its current link ID, it triggers IP Address assignment procedures.
15. The AT sends Agent Solicitation Message to AGW2 via eBS2 (assuming the CMIP4 application in this call flow).
16. AGW2 sends a Foreign Agent Advertisement message to the AT containing a new FA CoA.
17. The AT sends an RRQ which includes its current HoA to the AGW2 and the AGW2 forwards it to the HA to bind its HoA with the new FA CoA.

18. The HA sends RRP back to the AT through AGW2.

19. Now the AT sends/receives IPv4 packets to/from the HA through the CMIP4 tunnel between the HA and Target AGW (AGW2) and the tunnel between eBS2 (that serves as both Serving eBS and DAP) and AGW2..

20. On forward link, there might be some leftover data sent from the source AGW (AGW1) to the AT through the tunnel between AGW1 and the source DAP and L2 tunnel between eBS1 and eBS2.

21. On reverse link, there might be some leftover data sent from the AT's IP interface 1 to the HA through L2 tunnel between eBS1 and eBS2, the tunnel between eBS1 and AGW1, and the CMIP4 tunnel between AGW1 and HA. During this period of time, the HA may bi-receiving the data from both AGW1 and AGW2.