WiMAX Forum Network Architecture

(Stage 2: Architecture Tenets, Reference Model and Reference Points)

[Part 2]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

Copyright © 2005-2007 WiMAX Forum.   All Rights Reserved.

Table of Contents

1 **TABLE OF FIGURES**

1 **LIST OF TABLES**

12

7. Functional Design and Decomposition

Unless specified otherwise, call flows and messages defined in this section are superseded by corresponding definitions in Stage 3.

> **Note:** See §3.0 References in *WiMAX Forum Network Architecture [Part 1]* for references cited in this document.

7.1 Network Entry Discovery and Selection/Re-selection

7.1.1 Functional Requirements

    a) The solution architecture SHALL accommodate Nomadic, Portable, and fully mobile deployment scenarios.

    b) The solution architecture SHALL accommodate "NAP sharing" and "NAP+NSP" deployment models.

    c) The solution architecture SHOULD support Licensed and License-Exempt (LE) deployments.

    d) The solution architecture SHOULD support both manual [1] and automatic [2] NSP selection.

7.1.2 Use Case Scenarios

NSP discovery and selection procedures are typically executed on a first time use, initial network entry, network re-entry, or when an MS transitions across NAP coverage areas. This subsection describes all four use case scenarios.

7.1.2.1 Use-case Scenario 1—First-Time Use without NAP/NSP Configuration Information Stored on MS

    a) MS detects one or more available WiMAX NAPs.

    b) MS discovers available NSPs associated with one or more NAPs.

    c) MS identifies all accessible NSPs and selects an NAP and an NSP based on some preference criteria.

    d) MS performs more concrete processes procedure with a NAP.

    e) MS becomes authorized on the selected NSP for service subscription purposes only to create a business relationship with the selected NSP.

    f) MS creates a business relationship enabling access via the selected NSP.

    g) MS acquires and stores the configuration information.

7.1.2.2 Use-case Scenario 2—Initial Network Entry or First-Time Use with NAP/NSP Configuration Information

a) MS detects, using the stored configuration information, one or more available WiMAX NAPs.

b) MS discovers available NSPs associated with one or more NAPs.

c) MS identifies all accessible NSPs and, using the stored configuration information, selects or allows a subscriber to select an NSP based on some preference criteria.

---

[1] In manual selection, the user must be able to receive the information about all available NSPs, and indicate its NSP preference to the network manually.

[2] In automatic selection, the MS will automatically make the NSP selection decision based on the detected wireless environment and configuration file information without the user's intervention.

d) MS performs initial network entry procedure with a NAP that has a business relationship enabling access via the selected NSP.

In case of failure, MS reverts to Use Case Scenario 1.

7.1.2.3   Use-case Scenario 3—Network Re-entry

Network re-entry is equivalent to establishing connection with the same or another BS in a previously discovered WiMAX NAP. Scenario 3 mechanics assumes that NAP and NSP geographic coverage are synonymous in this context.

In case of failure, MS reverts to scenario 2.

7.1.2.4   Use-case Scenario 4—MS Transitions Across NAP Coverage Areas

a) MS has previously completed network entry and is in normal operation with its NSP on a WiMAX NAP.

b) MS discovers, using the stored configuration information, one or more available neighboring WiMAX NAP(s)[3].

c) MS discovers NSPs associated with one or more NAPs, which MAY include its currently authorized NSP [3].

d) Due to user movement or other confounding factor, MS elects to transition to another NAP.

e) MS identifies all accessible NSPs and, using the stored configuration information, selects an NSP based on some preference criteria.

f) MS performs network re-entry with a NAP that has a business relationship enabling access via the selected NSP. This network re-entry will involve a full authentication. Optimized handover on all other network re-entry steps is not possible.

In case of failure, MS reverts to scenario 2.

7.1.3   NAP, NSP Domains

The adopted NWG reference model enables deployments wherein an MS may encounter one or more of the following situations:

a) An Access Service Network (ASN) managed/owned by a single NSP administrative domain (also referred to as "NAP+NSP" deployment case).

b) An ASN managed by a NAP but shared by two or more NSPs (also referred to as "NAP sharing" deployment case).

c) A physical geographic region covered by two or more ASNs, representing either a "NAP+NSP" or "NAP sharing" scenario.

NOTE: "NAP sharing" is referred to the ASN deployment scenario when it has the management plane, control plane and data plane connectivity shared directly with more than one NSP;   i.e. this is not the same as the roaming scenario, where multiple NSPs may be accessible via the ASN, but are accessible indirectly through one (or more) of the NSPs attached to that specific ASN.

The requirement is to enable the MS to discover all accessible NSPs, and to indicate the NSP selection during connectivity to the ASN. The actual NSP selection mechanism employed by the MS may be based on various preference criteria, possibly depending on the presence on the MS of configuration information. Configuration information SHALL include:

a) information useful in MS discovery of NAP including channel, center frequency, and PHY profile,

---

[3] Steps b and c of Scenario 4 may occur either before or after step 4 without affecting performance.

1   b)   information useful in MS decision mechanism to discriminate and prioritize NSPs for service selection
2   including a list of authorized NAP(s) and a list of authorized NSP(s) with a method of prioritization for the
3   purpose of automatic selection,

4   c)   a list of authorized 'share' or 'roaming' affiliation relationships between authorized NAP(s) and NSP(s)
5   and partner NAP(s) and NSP(s), with a method of prioritization for the purpose of automatic selection,

6   d)   identity/credentials provided by NSP(s) to which the MS has a business relationship, and

7   e)   the mapping relation table between 24-bit NSP identities and corresponding realms of the NSPs.

8 Configuration information may be provided on a pre-provisioned basis or at time of MS dynamic service
9 subscription and may be subject to periodic update in a method outside the scope of this standard.

10
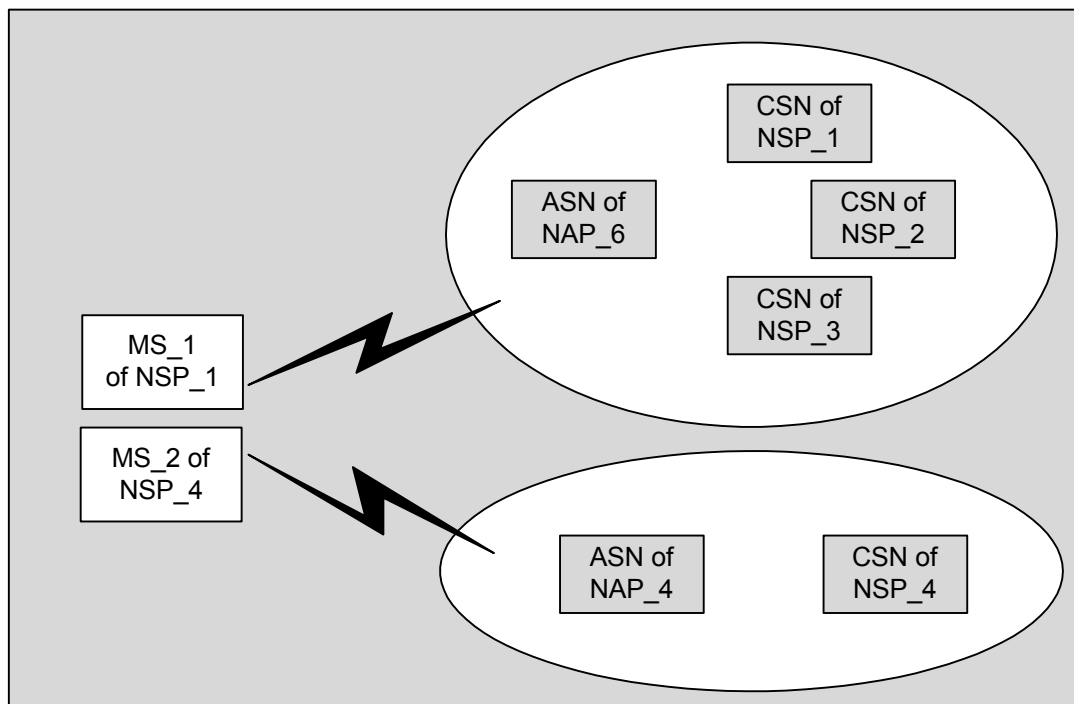
11 **Figure 7-1 - Coverage Area with Overlapping ASNs**

12 For example, as shown in Figure 7-1, MS_1 and MS_2 discover available NSPs and select one based on its
13 configuration information. More specifically, MS_1 prefers to connect to ASN of "NAP_6" because it is directly
14 affiliated with MS_1's home NSP through NAP sharing. And, MS_2 prefers to connect to ASN of "NAP_4"
15 because it is owned by MS_2's home NSP (i.e., NSP_4).

16 There is a need for a solution framework that enables an MS to discover identities of available NSP(s) in a WiMAX
17 coverage area, and indicate its selected NSP to the ASN. While the general method for MS selection of NSP for
18 attachment is provided as part of Release 1.0.0, the specific mechanisms that an MS MAY use to select a particular
19 NSP from the list of discovered NSPs are out of scope of Release 1.0.0, but would likely include reference to
20 configuration information.

21 **7.1.4   NAP, NSP Discovery and Selection**

22 This subsection provides an overview of a solution for NAP, NSP discovery and selection.

23 The solution consists of four procedures:

24   a)   NAP Discovery

25   b)   NSP Discovery

26   c)   NSP Enumeration and Selection

1   d)   ASN Attachment

2   *WiMAX NAP Discovery* refers to a process wherein an MS discovers available NAP(s) in a detected wireless
3   coverage area. *NSP* Access *Discovery* refers to a process wherein an MS discovers available NSP(s) in a coverage
4   area. *NSP Enumeration and Selection* refers to a process of choosing the most preferred NSP and a candidate set of
5   ASNs to attach, based on the dynamic information obtained during the discovery phase and stored configuration
6   information. *ASN Attachment* based on *NSP Enumeration and selection* refers to a process wherein the MS
7   indicates its selection during registration at ASN associated with the selected NSP by providing its identity (in the
8   form of NAI [60]). The enumerated steps are not sequential and need not be completed in their entirety. That is, *NSP*
9   *Access Discovery* and *NSP Enumeration and Selection MAY* well occur concurrent to *WiMAX NAP Discovery*. Also,
10 there is no requirement that an MS discover **all** NAPs and NSPs in the available environment. An MS MAY stop the
11 discovery process on discovery of a NAP and NSP meeting the MS *NSP Enumeration and Selection* criteria and
12 proceed to *ASN Attachment*.

13 7.1.4.1   WiMAX NAP Discovery

14 An MS detects available NAP(s) by scanning and decoding DL-MAP of ASN(s) on detected channel(s). The 24-bit
15 value of the "operator ID" (see 6.3.2.3.2 of IEEE Std 802.16) within the "Base Station ID" parameter in the DL-
16 MAP message is the NAP Identifier and is used to indicate the ownership of the ASN. The value of the 24-bit
17 "operator ID" shall be assigned as an IEEE 802.16 Operator ID by the IEEE Registration Authority[4]. Operator
18 ID/NAP ID allocation and administration method, and field formatting are defined in IEEE Std 802.16. If
19 information useful in MS discovery of NAP is available in configuration information, it may be used to improve
20 efficiency of NAP discovery.

21 7.1.4.2   NSP Access Discovery

22 The NAP SHALL be served by one or more NSPs. In NSP discovery, an NSP identifier can be presented to the MS
23 as a unique 24-bit NSP identifier. The value of the 24-bit NSP ID (i.e., NSP Identifier) SHALL be issued by a
24 namespace authority to guarantee global uniqueness. NSP ID allocation and administration are managed by the
25 IEEE RAC. NSP ID may either be a 22-bit globally-assigned ID or a combined MCC+MNC as described in ITU-T
26 Recommendation E.212. Selection of the method used for NSP ID format is implementation specific.

27 During scanning, if the MS cannot deduce available NSP(s) from the NAP identifier based on the NSP Identifier
28 Flag, detected NAP IDs, and the configuration information, then it SHOULD try to dynamically discover a list of
29 NSPs supported by the NAP.

30 If the NAP and NSP are the same (i.e. there is a one-to-one relationship between these IDs), the network MAY
31 advertise only the NAP ID and not separately present any NSP identifiers (NSP IDs). The NAP SHALL identify
32 this case by setting the least significant 1st bit (1st LSB; the 25th bit of Base Station ID; the NSP Identifier Flag) of
33 the Base Station ID to a value of '0'. For this case, the MS SHALL assume that the NSP ID is the same ID presented
34 as NAP ID.

35 In the event that more than one NSP is served by a detected NAP, or that some regulatory or deployment
36 requirement compels separate presentation of one or more NSP IDs, the NAP MAY transmit the NSP ID list as part
37 of the Service Information Identity (SII-ADV) broadcast MAC management message. Also, the BS SHALL transmit
38 the list of NSP IDs as part of SBC-RSP in response to an MS request through SBC-REQ. The NAP shall identify the
39 presentation of a separate list of NSP IDs by setting the NSP Identifier Flag to a value of '1'

40 In this phase, if the list of NSP identifiers supported by a NAP does not exist in the configuration information of the
41 MS, or the list of NSP identifiers supported by a NAP is changed, e.g. the optional NSP Change Count TLV (NSP
42 Change Count TLV is described in the IEEE Std 802.16) obtained from the network as part of obtaining the NSP ID
43 list, is different with that stored in the configuration information of the MS, the MS SHOULD get the list from the
44 network. Otherwise, available NSP(s) associated with a NAP SHALL be enumerated locally based on the
45 configuration information of the MS.

46 24-bit NSP identities received in this phase SHALL be mapped into realms of corresponding NSPs.

---

[4] The IEEE Registration Authority is a committee of the IEEE Standards Association Board of Governors. General information as well as details on the allocation of 802.16 Operator IDs can be obtained at http://standards.ieee.org/regauth.

7.1.4.3   NSP Enumeration and Selection

For automatic selection, an MS makes its NSP selection decision based on the dynamic information obtained within a coverage area (e.g., a list of available NSP Identifiers offering services), and configuration information. The specific algorithms that an MS MAY use to select the most preferred NSP from the list of discovered NSPs are out of scope of Release 1.0.0.

For manual selection, the user manually selects the most preferred NSP based on the dynamic information obtained within the coverage area. Manual selection can also enable use scenarios where a non-subscribed user wants to connect to a detected network. For example, the user wants to exercise an initial provisioning procedure with a specific NSP, or it wants to use the network on "pay for use" basis.

7.1.4.4   ASN Attachment Based on NSP selection

Following a decision to select an NSP, an MS indicates its NSP selection by attaching to an ASN associated with the selected NSP, and by providing its identity and home NSP domain in the form of NAI. The ASN uses the realm portion of the NAI to determine the next AAA hop to where the MS's AAA packets SHOULD be routed. The MS MAY use its NAI with additional information (also known as decorated NAI— described in section 2.7 of [48]) to influence the routing choice of the next AAA hop when the home NSP realm is only reachable via another mediating realm (e.g., a visited NSP). For example, as shown in Figure 7-2, MS_1 uses a normal/root NAI (i.e., user-name@NSP_1.com) as the AAA packets can be directly routed to the AAA server in NSP_1. Whereas, MS_2 needs to construct a decorated NAI (e.g., NSP_4!user-name @NSP_1.com) as the AAA packets cannot directly be routed to the home NSP (i.e., NSP_4). The specific use of realm is defined in section 7.3.7.
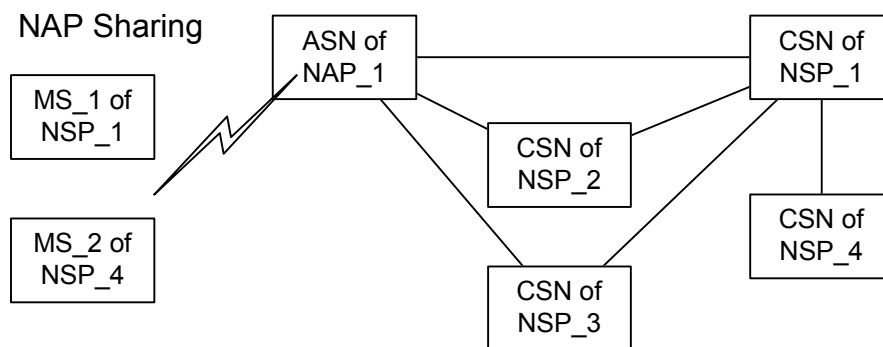
Figure 7-2 - Deployment example with NAP sharing

7.2   IP Addressing

This section defines IP addressing for both IPv4 and IPv6 protocols. IPv4 addressing details are described in Stage 2 section 7.2.1 and IPv6 addressing details are described in Stage 3 section 5.11.8

7.2.1   IPv4 address Management

IP address allocation refers to the Point of Attachment (PoA) address delivered to the MS. The discussion below refers primarily to allocation of Dynamic IP addresses. From the perspective of the MS, for MS that do not support Client MIP, DHCP [11] is used as the mechanism of dynamic IP address allocation. The home CSN may employ alternate techniques such as IP address assignment by a AAA server and deliver it to the MS via DHCP. Details of such alternate mechanisms for IP address allocation are out of scope of Release 1.0.0. These alternate techniques MAY include allocation of addresses between the home CSN and the ASN via AAA. Alternatives for DNS discovery include the use of DHCP or the use of Mobile IP extension as defined in IETF draft-ietf-mip4-gen-ext-00.txt. The following discussion focuses on the usage of DHCP to allocate PoA address to the MS. In the context of this section (and R3 Mobility Management section) PoA address corresponds to the HoA (Home Address).

7.2.1.1 Functional Requirements

Note - Considerations for overlapping IP addresses in the ASN is beyond the scope of Release 1.0.0.

a) When an MS is an IP gateway, a Point-of-Attachment IP address (PoA address) SHALL be allocated to the IP gateway. When MS is an IP host, a PoA address SHALL be allocated to the IP host.

b) For fixed and nomadic access, the PoA IP address has to be routable in the CSN and ASN and the PoA address SHALL be assigned from the CSN address space.

For portable and mobile access, the PoA address SHALL be assigned from the address space of CSN of either Home-NSP or Visited NSP depending on:

   o   Roaming agreement between Home NSP and Visited NSP.

   o   User subscription profile and policy in Home NSP.

c) For fixed access, the PoA address allocated to MS MAY be static or dynamic.

d) The allocation of PoA address SHALL NOT preclude allocation of additional tunnel IP address to access specific applications (i.e., inner tunnel IP address allocated for VPN, etc.).This requirement is also applicable for overlay mobility based on MIP.

e) For billable IP services, a Point-of-attachment IP address SHALL be allocated to MS only after successful user/MS authorization. The allocated addresses SHALL be bound to the authorized user/MSs for the duration of the session. The binding MAY be maintained by an Address Allocation Server (e.g., a DHCP server or AAA server).

f) For mobile access (Proxy MIP and Client MIP), a PoA address (MIP home address, See note1[5]), routable in CSN domain SHALL be allocated to MS.

7.2.1.1.1 Fixed Access Scenario

Fixed usage scenario SHALL allow two types of PoA IP address allocations, static and dynamic. In both cases the PoA address SHALL be routable in the CSN:

a) Static IP address: static IP addresses MAY be assigned by manual provisioning in the MS or via DHCP.

b) Dynamic IP address: Dynamic IP address assignment is based on DHCP. The DHCP server SHALL reside in CSN domain that allocates the PoA address. A DHCP relay SHALL exist in the network path to the CSN.

The DHCP proxy MAY reside in ASN and retrieves IP host configuration information during access authorization (i.e. during AAA exchange).

7.2.1.1.2 Nomadic Access Scenario

Nomadic access scenario SHALL be based on dynamic IP address assignment. It SHALL be the default for nomadic access deployment scenarios. Static IP address assignment MAY be used; however details on use of static IP address assignment are beyond the scope of Release 1.0.0. Dynamic IP address assignment SHALL be based on DHCP. The DHCP server SHALL reside in home or visited CSN domains. The DHCP proxy MAY reside in ASN and retrieves IP host configuration information during access authorization (i.e. during AAA exchange).

7.2.1.1.3 Mobile Access Scenario

Mobile access scenario SHALL allow PoA IP address assignment based on DHCP for Proxy-MIP based SS/MSs. The DHCP server MAY reside in CSN domain. In this case, the PoA address (i.e., Mobile IP home address) and IP host configuration information SHALL be derived using DHCP. Alternatively, the DHCP proxy MAY reside in ASN, wherein it retrieves IP host configuration information and home address during Access Authentication AAA exchange with home NSP.

For CMIP-based mobile SS/MSs, MIP [43] based IP addressing SHALL be used instead of DHCP.

---

[5] Note 1: In this case, PoA=HoA

1 **7.2.1.2   Functional Decomposition**

2 As per WIMAX reference model, functional decomposition for MS IP address management feature SHALL be done
3 across the following reference points:

4   a)   R1

5   b)   R3

6   c)   R5, if applicable

7 Reference points for PoA IP address are shown in Figure 7-3 and Figure 7-4:

8   •   When PoA address is allocated by visited NSP, the Address Allocation Server, located in visited CSN,
9   allocates PoA from its pool of addresses (as per roaming agreement with Home NSP). This case is shown
10   in Figure 7-3.

11   •   When PoA address is allocated by Home NSP, the Address Allocation Server, located in Home CSN,
12   allocates PoA from its pool of addresses. This case is shown in Figure 7-4.

13   •   In addition to the figures below, with the Ethernet case acting as a layer-2 MS, the DHCP client MAY
14   reside in the hosts behind the MS. In this case, the MS simply forwards the DHCP messages between the
15   hosts and Address Allocation Server.

16

Note: The DHCP client shown above may reside inside the SS/MS or behind the SS/MS

17

18   **Figure 7-3 - Functional Decomposition for PoA from Visited NSP**
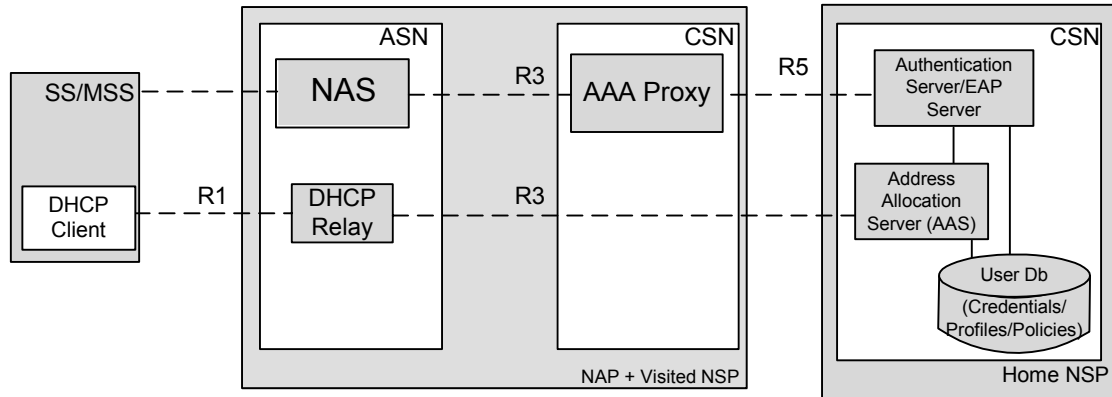
Note: DHCP Client shown above may reside inside the SS/MS or behind the SS/MS

1

2 **Figure 7-4 - Functional Decomposition for PoA from Home NSP**

3 **7.2.1.3 Dynamic IP Configuration Setup for Fixed and Nomadic Access Scenarios**

4 This section defines the dynamic IP configuration setup for fixed and nomadic access. IP configuration for mobile
5 access with in CMIP and PMIP is provided in [ref to section 7.8.1.8] and [ref to section 7.8.1.9], respectively. The
6 following signaling flow describes IP configuration setup phase using AAA. In this flow, DHCP relay is located in
7 the ASN and DHCP server is located in the CSN.

8
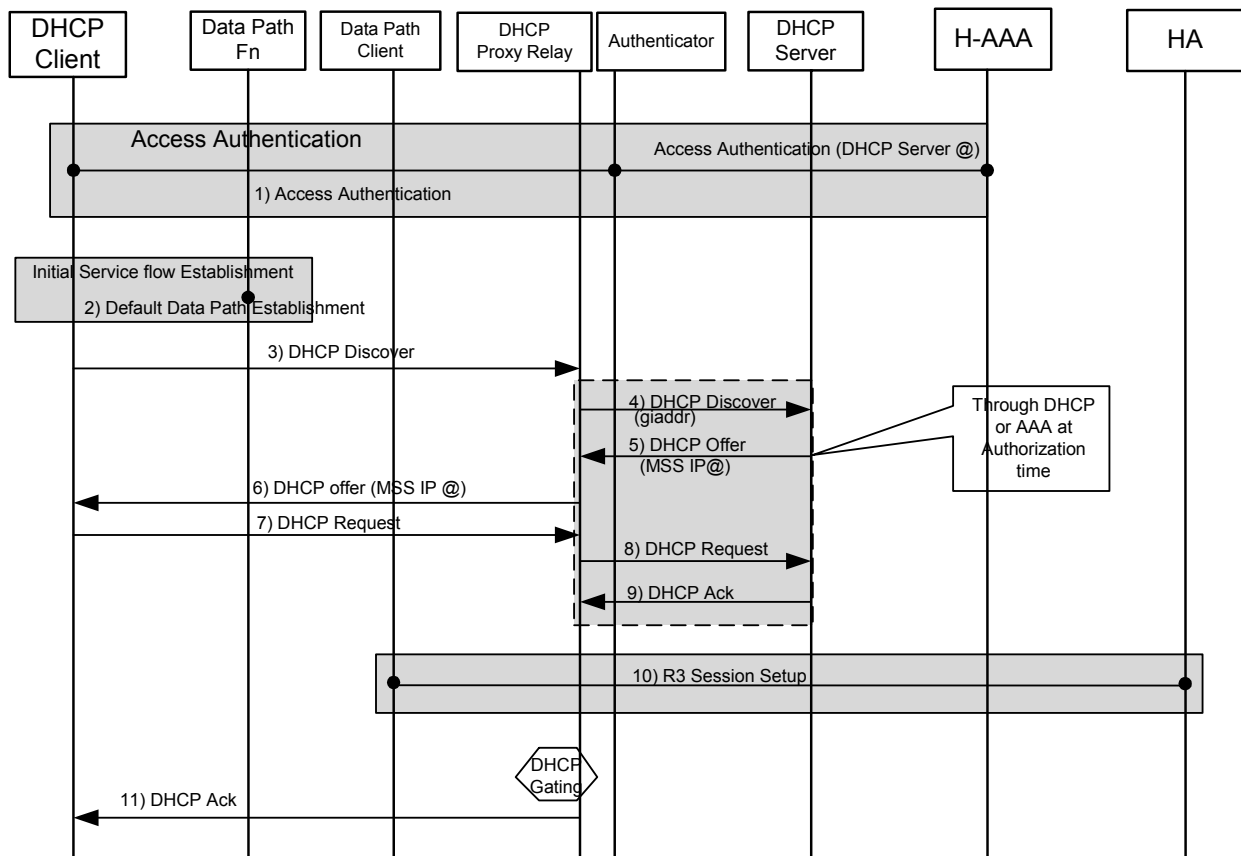
9 **Figure 7-5 - MS IPv4 Address Management**

1 The functional entity residing in ASN is a DHCP Proxy. However, when a PoA address is delivered via RADIUS
2 access authentication, the functional entity in ASN is DHCP proxy.

3 The essential phases of the process shown in Figure 7-5, appear as follows:

4 1) *Access authentication*: During access level authentication— e.g., based on EAP-over-PKMv2— the network
5 assigning the PoA address is determined. The DHCP server address is retrieved from the AAA access authentication
6 or configured locally at the ASN. The DHCP relay in ASN is configured with the appropriate DHCP server address.
7 The relay function in ASN can direct the DHCP messaging to the specific DHCP server selected based on the CSN
8 membership of the MS.

9 2) At the completion of authentication and registration (.16e), an Initial Service flow (ISF) is established for the MS
10 within the ASN. The ISF can be used for IP configuration of the host. DHCP messages can be transported over the
11 ISF associated with the MS.

12 3–9) *IP address assignment and IP Host configuration:* After successful establishment of the ISF, the MS sends a
13 DHCP discover message. Upon receiving a DHCP discover message the BS forwards the DHCP discover message
14 to DHCP Proxy in ASN. The DHCP relay in ASN manages the DHCP exchange with the DHCP server.

15 Alternatively, the DHCP Relay in ASN can return the complete IP configuration to the MS. In this case the IP
16 configuration including the PoA address data at the DHCP server is provided by the NSP through the access
17 authentication AAA exchange. In the case of mobile node with PMIP, the address obtained using DHCP SHALL be
18 the home address of MS. Dynamic Home Agent address assignment MAY be supported in compliance with RFC
19 4433

20 10) The PMIP Client and the HA complete R3 session setup.

21 11) *DHCP Ack*: Following step 10, the DHCP function relays the DHCP ACK to the MS.

22 For mobile access, detailed IP address assignment procedures for Proxy MIP and Client MIP are specified in Section
23 7.8.1.8 and Section 7.8.1.9.

24 ### 7.2.1.4   IP Address Renewal

25 IP address renewal is initiated by the DHCP client in the MS.

26 The triggers which cause IP address renewal could be based on events such as :

27 - Address lease lifetime expiry threshold reached

28 - Inability to send packets using the address assigned

29 - Indication of network failure

30 - MS specific trigger

31

32 DHCP renewal messages are sent directly from the MS to the DHCP server without the need for relaying in the
33 ASN since the MS obtains the IP address of the DHCP server from the siaddr address field in the DHCP Ack
34 message during connection setup time.

35

36 ### 7.2.2   IPv6

37 IPv6 in WiMAX can be operated in multiple ways. The packet convergence sublayer (CS) specified in the IEEE
38 802.16d/e specification is used for transport of all packet based protocols such as Internet protocol, IEEE Std
39 802.3/Ethernet and, IEEE Std 802.1Q. IPv6 can be run over the IP specific part of the packet CS or alternatively
40 over the Ethernet (802.3/802.1Q) specific part of the packet CS. The operation of IPv6 over the IP specific part of
41 the Packet CS is specified in [Reference to IETF I-D: draft-ietf-16ng-ipv6-over-ipv6cs-01] and should be referred to
42 for understanding the basic mechanism. This section provides additional information about IPv6 operation that is
43 WiMAX specific. IPv6 over 802.3 and 802.1Q specific parts of the packet CS are described in [REF draft-riegel-
44 16ng-ip-over-eth-over-80216-01.txt]. It should be noted that only the IP specific part of the packet CS is a
45 mandatory requirement and support for 802.3 and 802.1Q parts of the packet CS is optional.

1   ### 7.2.2.1   Link Model

2   The MS and the IPv6 AR are connected at the IPv6 layer by a point-to-point link. The combination of the transport
3   connection over the air interface (R1) between the MS and the BS and, a GRE tunnel between the BS and the IPv6
4   AR (R6 in the case of profiles A and C) creates a point-to-point link. Each MS is assigned a unique IPv6 prefix(es)
5   by the AR. In the case of Profiles A and C the AR is a function at the ASN-GW. The IPv6 AR is a function within
6   the ASN in the case of profile B. A GRE tunnel, the granularity of which is on a per-MS or a per-service flow basis
7   is established between the BS and the AR. In the case of profile B the link between the BS and the AR is
8   unspecified. The figure below shows the link model in profiles A and C:

9
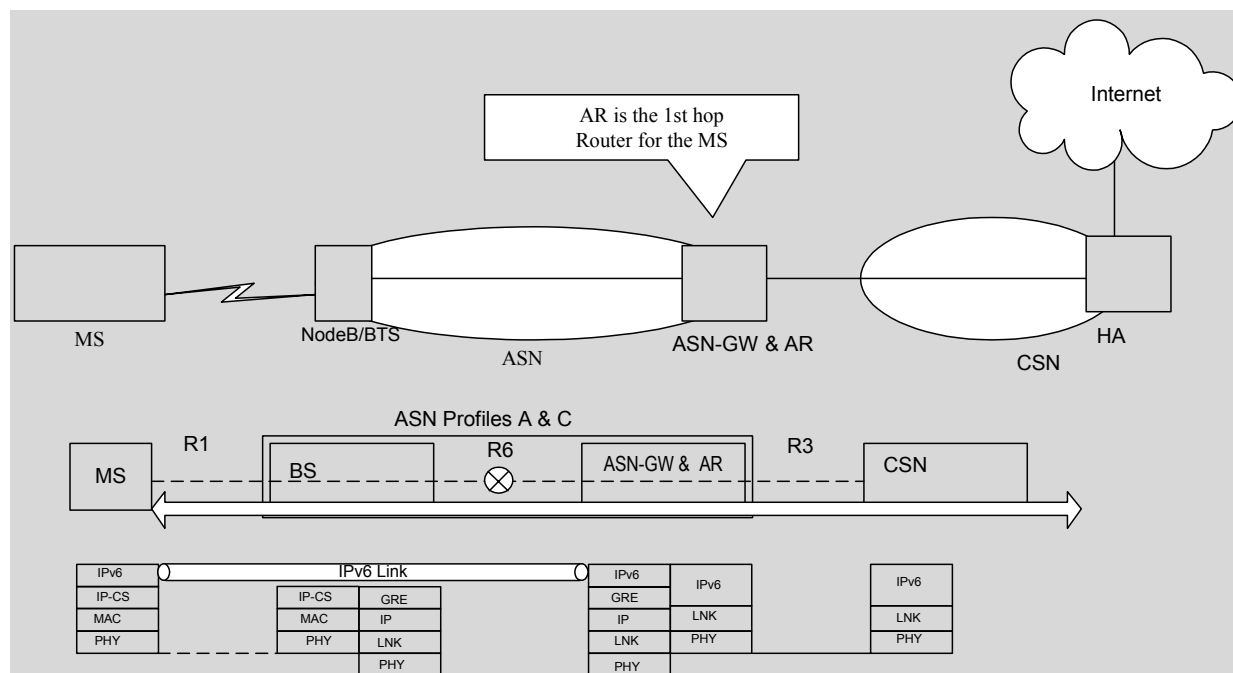
10   **Figure 7-6 - IPv6 link model for Profiles A and C**

11

12
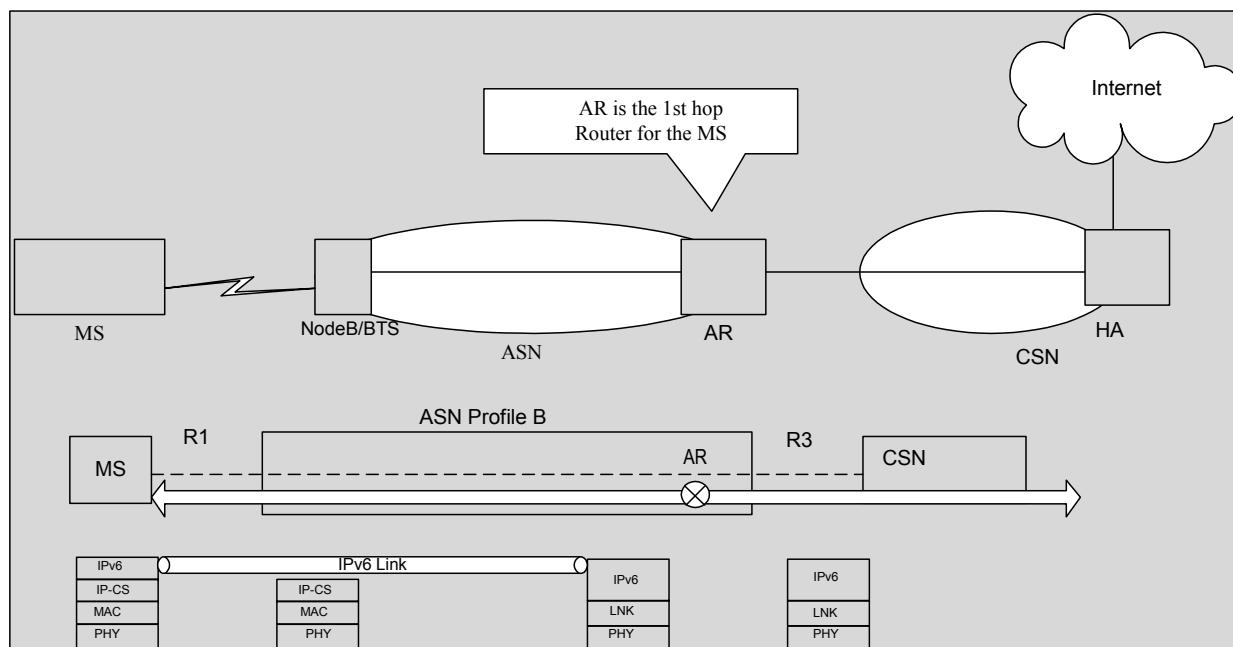
1   **Figure 7-7 - IPv6 link model for Profile B**

2   **7.2.2.2   IPv6 Address Management**

3 The PoA address in the context of Mobile IPv6 can be either the CoA or the HoA. The CoA is the address whose
4 scope is at the IPv6 AR in the ASN. The HoA is the address whose scope is at the MS' home agent. Only a MIP6
5 MS has an HoA and a CoA. The MIP6 MS can use either the HoA or the CoA for its IP sessions. All IPv6 MS' that
6 attach to the network and establish an IPv6 connection have a prefix assigned by the IPv6 AR. The address
7 associated with the AR can be used by an MS for IP sessions. A MIP6 MS also uses this address to register it with
8 the HA in the binding update message. The PoA address for an MS that does not use MIP6 is the address obtained
9 via DHCPv6 or the address generated by stateless address autoconfiguration based on the prefix advertised to the
10 MS by the IPv6 AR.

11 IPv6 address assignment requirements and procedures are detailed in the following sections:

12   **7.2.2.2.1   MS Functional Requirement**

13   a)   For fixed/nomadic access, a MS MAY be allocated a PoA address for simple IP connectivity by either
14   static, stateless address autoconfiguration (SLAAC) means or stateful DHCPv6 [42] assignment.

15   b)   MS should support static, stateless or stateful [42] address assignment for home address assignment.

16   c)   MS should support stateful address autoconfiguration [42] or stateless autoconfiguration ([16] and [30]) for
17   CoA allocation.

18   d)   For nomadic access, MS MAY be allocated a PoA address for IP connectivity by stateless address
19   autoconfiguration ([16] and [30]) or DHCPv6.

20   e)   MS SHALL use DHCPv6 [42] to determine system configuration information such as DNS servers, NTP
21   servers, etc.

22   f)   MS SHALL support the ability for multiple CoAs as per the description in Section 11.5.3 of [54].

23   g)   Allocation of PoA SHALL NOT preclude the allocation of additional tunnel IP addresses to access
24   applications (i.e., VPN).

25   h)   For billable IP services, the PoA SHALL be allocated only after successful user/device authorization.

26   i)   PoA SHALL be bound to user/device for the duration of the session.

27   j)   When PoA=CoA, it SHALL always be allocated by the serving network (visited or home).

28   k)   MS MAY use Neighbor Discovery [15] to acquire IP configuration information such as prefix, router
29   address, etc.

30   **7.2.2.2.1.1   Fixed Access /Stationary Networks Scenario**

31 Fixed usage SHALL allow two types of PoA IP address allocations via static/manual configuration, DHCPv6 and
32 stateless address autoconfiguration (SLAAC):

33   •   Static IP address: An MS may be provisioned with a static IPv6 address. In the case of an MS operating IPv6
34   over IPv6CS, the IPv6 AR is located in the ASN and the address assigned to the SS is based on the
35   prefix/subnet of the AR. In the case of IPv6 over Ethernet CS, the address pool comes from an AR that acts as
36   the 1st hop router for the SS. An example of such an AR would be the BRAS in a DSL type of deployment.

37   •   Stateful address autoconfiguration: Stateful address autoconfiguration is based on DHCPv6 [42]. The DHCPv6
38   server SHALL reside in the Visited CSN domain that allocates the PoA address. A DHCPv6 relay MAY exist
39   in the network path to the CSN

40   •   Stateless address autoconfiguration (SLAAC): An SS at the completion of the establishment of the initial
41   service flow (ISF) sends a router solicitation to the all-routers multicast address. The AR in the ASN can also
42   send an unsolicited router advertisement to the SS on completion of the ISF establishment. The AR in the ASN
43   responds to the router solicitation with a router advertisement which contains the prefix(es) that can be used by
44   the SS to do SLAAC. The SS SHALL perform DAD on the address that it autoconfigures.

7.2.2.2.1.2   Nomadic Access Scenario

Nomadic access SHALL allow two types of PoA IP address associations.

- Stateful address autoconfiguration: Stateful address autoconfiguration is based on DHCPv6 [42]. The DHCP server SHALL reside in the Visited CSN domain that allocates the PoA address. A DHCP relay SHALL exist in the network path to the CSN.

- Stateless address autoconfiguration: The SS/MS sends a router solicitation to the all-routers multicast address at the completion of the establishment of the ISF. The AR in the ASN responds with a router advertisement which includes the prefix(es) that can be used to autoconfigure an address. The MS SHALL perform DAD on the address that it autoconfigures. The AR should also send an unsolicited router advertisement to the MS at the completion of the establishment of the ISF.

7.2.2.2.1.3   Portable, Simple and Full-Mobility Access Scenario

Mobility (R3 mobility) in the case of IPv6 is enabled via Mobile IPv6. IPv6 in Release 1.0.0 is an optional feature. Mobile IPv6 is hence an optional feature as well. Mobile IPv6 in Release 1.0.0 is as per RFC 3775. Mobility service requires the MS having a home address (HoA) and at least one care-of-address (CoA). Both addresses are globally routable. CoA is the address whose scope belongs to the AR in the ASN. The HoA is the address the scope of which is at the MIP6 Home Agent. Address assignment is via stateful and SLAAC means. The HoA may also be statically configured at the MS. The CoA address allocation occurs as follows:

- SLAAC: An Initial Service flow (ISF) is established on completion of .16e Registration by the MS. The MS sends a Router solicitation to the AR. The AR in the ASN responds with a router advertisement (RA) which includes the prefix(es) that enable the MS to autoconfigure an address. The AR should also send an unsolicited RA on completion of the establishment of an ISF for an MS.

- Stateful address autoconfiguration: The MS acquires an address from the ASN via DHCPv6. DHCPv6 is initiated only after the establishment of the ISF.

The HoA for an MS is assigned as follows (RFC 3775 and related IETF standards):

- Stateless DHCP : During initial access authentication, the Home AAA determines the MS is authorized for MIP6 service and sends the bootstrap parameters required by the MS in the Access Accept message to the visited AAA in the ASN. The ASN inserts the MIP6 bootstrap parameters which include the address of the HA, the home link prefix or the HoA in the stateless DHCPv6 server in the ASN. On completion of the establishment of the ISF, the MS sends a DHCPv6 query to the DHCP server in the ASN and receives the MIP6 bootstrap parameters. If the MS receives the Home link prefix, the MS does SLAAC to configure the home address. If the DHCP response includes the HoA then the MS uses the HoA in the binding update to the HA. If the Home AAA does not provide either the home link prefix or the HoA, the MS can send a binding update to the HA with the HoA set to the unspecified address. In such a case the HA will assign the MS an HoA in the binding Ack.
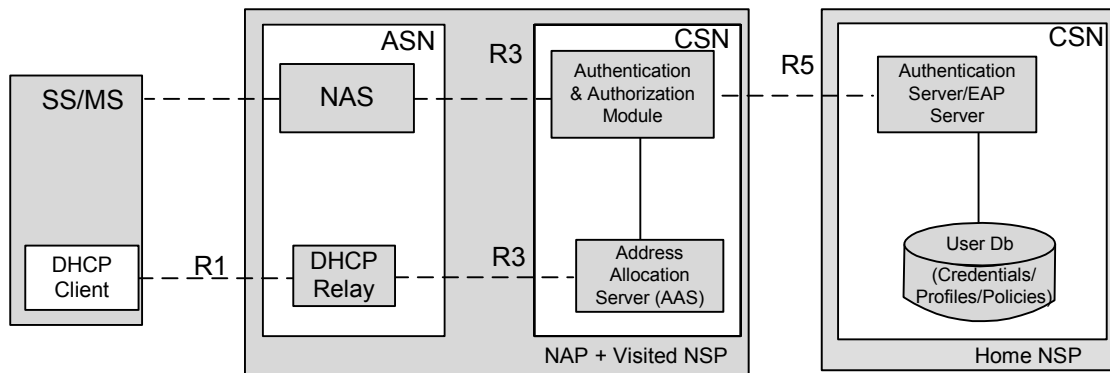
7.2.2.2.2   Functional Decomposition

As per WIMAX reference model, functional decomposition for MS PoA IP address management feature SHALL be done across the following reference points:

    a) R1

    b) R3

    c) R5 if applicable
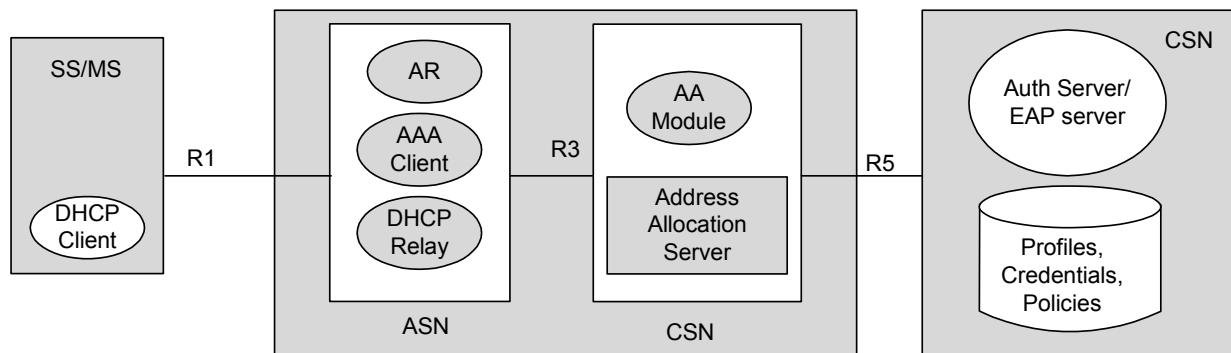
Figure 7-8 - Stateful MS IPv6 Address Management

There are two methods for address allocation:

- The PoA address MAY be allocated by the Address Allocation Server in the Serving Network [42]. This could be in the home network if the device is not roaming or in the visited network if the device is roaming (as per roaming agreement with the Home NSP).

- The PoA MAY be derived using SLAAC. The CoA prefix belongs to the address range assigned to and managed by the V-NSP.

The link-local address is always autoconfigured by the MS as soon as the IPv6 radio bearer is established. Link-local address is formed by using the MS MAC address and the well-known link-local prefix, as described in [15] and [16]. The MS SHALL perform duplicate address detection on its link-local address [16]. If later the MS autoconfigures a CoA by combining the same interface identifier it used for link-local address with an advertised prefix, the MS doesn't need to perform duplicate address detection process for such address. The MS will use its link local address as source address in any IPv6 datagrams that it sends before it has acquired a global address.

7.2.2.3   IP Address Renewal

An MS that is assigned an address via DHCPv6 should renew the address when the lease lifetime nears expiry. The MS triggers DHCP renewal and the process is as per [42].

If an MS has an address that is acquired via SLAAC, the MS needs to renew the address by sending a neighbor solicitation to the AR.

7.2.2.4   DNS discovery

The MS can discover the address of the DNS via either one of the following methods:

- o   DHCPv6

- o   Well known DNS address

- o   Address of the DNS server in the router advertisement

7.3   AAA Framework

The WiMAX AAA framework is based on IETF specifications, in particular on [23] and [24]. The term AAA is used to refer to the AAA protocols, RADIUS or Diameter.

The AAA framework provides the following services to WiMAX:

- Authentication Services. These include device, user, or combined device and user authentication.

- Authorization Services. These include the delivery of information to configure the session for access, mobility, QoS and other applications.

- • Accounting Services. These include the delivery of information for the purpose of billing (both prepaid and post paid billing) and information that can be used to audit session activity by both the home NSP and visited NSP. Accounting is described in section 7.5.

7.3.1 Functional Requirements

The following functional requirements are considered:

a) The AAA framework SHALL support global roaming across WiMAX operator networks, including support for credential reuse and consistent use of authorization and accounting.

b) The AAA framework SHALL support roaming between home and visited NSPs.

c) The AAA framework SHALL be based on use of RADIUS or Diameter in the WiMAX ASN and CSN. Where applicable, an Interworking gateway SHALL translate between either of these Diameter and RADIUS protocols. As well an interworking function maybe required for translating between one of these protocols and a legacy domain-specific protocol.

d) The AAA framework SHALL be compatible with the AAA 3-party scheme — with an MS as a "Supplicant," "Authenticator" in ASN, and an AAA backend as an "Authentication Server."

e) The AAA framework SHALL be compatible with AAA authorization requirements as per [27].

f) The AAA framework SHALL accommodate both Mobile IPv4 and Mobile IPv6 Security Association (SA) management.

g) The AAA framework SHALL accommodate all the scenarios of operation from fixed to full mobility as defined in WiMAX Forum Stage 1 document [79].

h) The AAA framework SHALL provide support for deploying MS authorization, user and mutual authentication between MS and the NSP based on PKMv2.

i) In order to ensure inter-operability, the AAA framework SHALL support EAP-based authentication mechanisms that MAY include but are not limited to the following: passwords or shared secrets, Subscriber Identity Module (SIM), Universal Subscriber Identity Module (USIM), Universal Integrated Circuit Card (UICC), Removable User Identity Module (RUIM), and X.509 digital certificates.

j) AAA framework SHALL provide appropriate support for policy provisioning at ASN or CSN, for instance by carrying policy related information from AAA server to ASN or CSN.

k) The AAA framework SHALL support dynamic change of authorization updates e.g. as described in [48]. This information includes but not limited to the identity of the visited network, and the location of the MS as known by the ASN.

l) The AAA framework SHALL be capable of providing the Visited CSN or ASN with a "handle" that represents the user without revealing the user's identity. This handle MAY be used by entities external to the Home CSN for billing and for enforcement of service level agreements.

m) In order to support some applications such as dynamic authentication, the AAA framework MAY be required to maintain session state. In the case of RADIUS [23] (a stateless protocol) the maintenance of session state is an implementation detail.

7.3.2 Reference Point Security

In order to ensure end-to-end security of the NWG architecture, security of each reference point must be considered. Privacy, authentication, integrity and replay protection must be ensured either at the lower layers (phy, mac, or network layer) or at the higher layers. Security at the lower layers comes in the form of a secure channel that can be utilized by any one of the signaling protocols and data traffic running above it.

It should be noted that the lower layer security and the higher layer security are complementary. Absence of one should be compensated by the presence of the other. At times both may be present. Lower layer security between two end points can be a substitute for the higher layers that terminate on the same end points. If the end points are different, the substitution may not apply. For example, a secure channel between the BS and the ASN GW alleviates the need to secure any R6 signaling, but pass-through R2 signaling cannot rely on this security.

1 Deployments must be aware of the necessity and availability of layered-security for each reference point. This
2 section provides a guideline to deployments.

3 **R1** – The 802.16 primary management connection over R1 is authenticated, integrity and replay protected at the
4 IEEE 802.16 MAC layer upon successful Device Authentication. All the subsequent R1 messaging over these
5 connections can rely on this lower-layer cryptographic security. On the other hand, transport connections may not be
6 crypto-protected at all. For that, any signaling protocol and data traffic that run above these connections shall
7 provide their own security when necessary. (Note: Although enabling security on the transport connections is
8 optional, it is recommended that deployments take advantage of this feature).

9 **R2** - This reference point may not have an end-to-end secure channel. It shall be assumed that the lower-layers are
10 insecure and the signaling protocols and data traffic shall provide their own security when necessary.

11 **R3** - This reference point may not have an end-to-end secure channel. It shall be assumed that the lower-layers are
12 insecure and the signaling protocols and data traffic shall provide their own security when needed. Examples:
13 Mobile IPv4 using authentication extensions, RADIUS using authentication attribute, etc.

14 **R4** - This reference point has an end-to-end secure channel, including privacy. The channel security may be
15 implemented using physical security, IPsec or SSL VPNs, etc. The VPN end points may be collocated with the R4
16 end points, or be on-path between the two to ensure end-to-end security.

17 **R5** - This reference point may not have an end-to-end secure channel. It shall be assumed that the lower-layers are
18 insecure and the signaling protocols and data traffic shall provide their own security when needed. Examples:
19 RADIUS authentication attribute, etc.

20 **R6** - This reference point has an end-to-end secure channel, including privacy. The channel security may be
21 implemented using physical security, IPsec or SSL VPNs, etc. The VPN end points may be collocated with the R6
22 end points, or be on-path between the two to ensure end-to-end security.

23 **R8** - This reference point has an end-to-end secure channel, including privacy. The channel security may be
24 implemented using physical security, IPsec or SSL VPNs, etc. The VPN end points may be collocated with the R8
25 end points, or be on-path between the two to ensure end-to-end security.

26 ### 7.3.3 Functional Decomposition

27 RFC2904 [25], presents three models for deploying AAA framework namely, Agent sequence/model, Pull
28 sequence/model and Push sequence/model. The models mainly differ in two aspects namely, a) how the supplicant
29 and authentication server communicate and b) how the control information (e.g., keys, policy details) are configured
30 into the bearer plane MSs. The [25] does not recommend one model over another. On the contrary it suggests that it
31 is appropriate to deploy a hybrid model. A related [26] provides examples of various key applications deployed
32 using the models defined in [25]. As per examples in the [25], the pull model is a preferred model for deploying
33 AAA framework and other models can be mixed in when required. Pull model is recommended for AAA
34 deployments within WiMAX networks. For more details on these models and terms like supplicant, authentication
35 server please refer to [25].

36 The NAP MAY deploy an AAA proxy between the Network Access Server NAS(s) in the ASN and the AAA in the
37 CSN in order to provide security and enhance maintainability. This is particularly the case where the ASN has
38 many NASs and the CSN is in another administrative domain. In this case, the AAA proxy will make it easier to
39 configure the AAA infrastructure between the NAP and the visited CSN, reducing the number of shared secrets that
40 need to be configured and making it easier to configure the network for failover. The AAA proxy will also allow the
41 NAP to police the AAA attributes received from the visited CSN and add additional AAA attributes that MAY be
42 required by the NASs in the ASN. Note: This Proxy AAA is not shown in the subsequent figures in this section.

43 #### 7.3.3.1 Non-Roaming Pull Model

44 Figure 7-9 shows the non-roaming pull model as per [25].

1
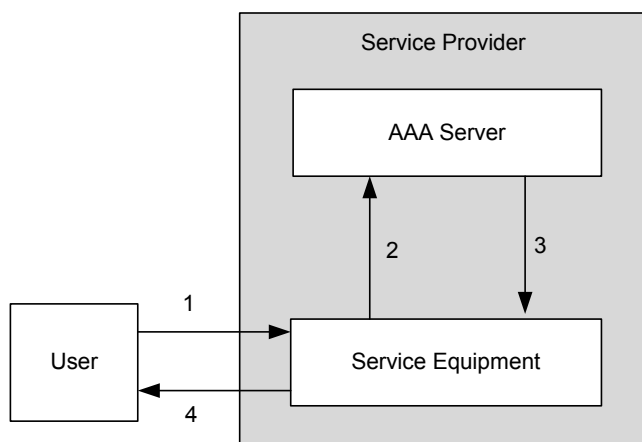
2 **Figure 7-9 - Generic Non-roaming AAA Framework**

3 The User (e.g., MS) sends a request to the Service Equipment (e.g., Network Access Server—NAS).

4 The Service Equipment forwards the request to the Service Provider's AAA Server.

5 Service Provider's AAA server evaluates the request and returns an appropriate response to the Service Equipment.

6 Service Equipment provisions the bearer plane and notifies the user that it is ready.

7 Figure 7-10 shows the non-roaming pull model mapped to the WiMAX non-roaming reference model.

8
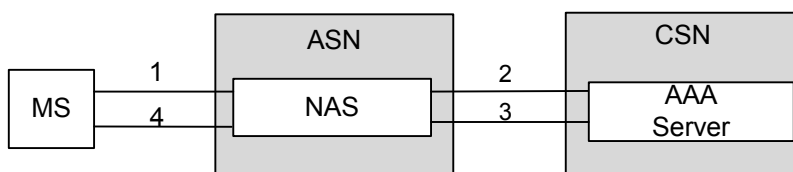
9 **Figure 7-10 - Greenfield Non-roaming AAA Framework**

10 For more details on WiMAX reference model, please refer to Section 6. As shown in Figure 7-10, the Service
11 Provider is split into ASN and CSN, while the Service Equipment in the ASN becomes a NAS. The CSN hosts the
12 AAA server whereas the ASN hosts one or more NASs.

13 Figure 7-11 shows the corresponding WIMAX non-roaming reference model when the CSN is belonging to an
14 incumbent NSP whose authorization and authentication backend is not AAA protocol compliant. The
15 incompatibility can be at the protocol level or at attributes level, etc.

16
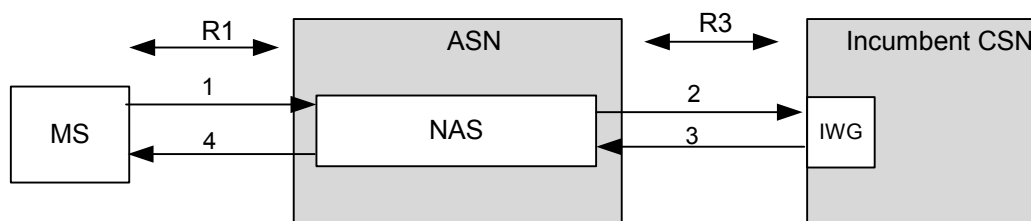
17 **Figure 7-11 - Non AAA Compliant Incumbent Non-roaming AAA Framework**

18 In this scenario, the CSN of an incumbent NSP needs to host an internetworking gateway (IWG) to map AAA
19 protocols and attributes to incumbent NSP specific protocols and attributes and vice-versa Since the IWG translates
20 the AAA protocol the Incumbent Non-roaming case is functionally identical to the Non-roaming case presented
21 earlier.

1 **7.3.3.2   Roaming Pull Model**

2 Figure 7-12 shows the roaming pull model as per [25].

3
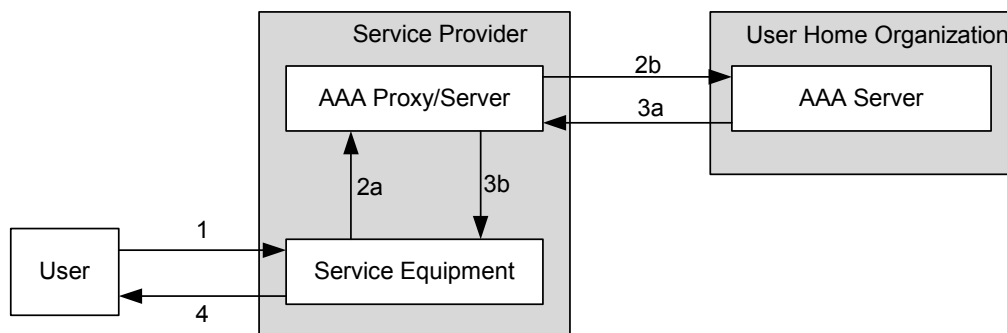
4 **Figure 7-12 - Generic Roaming AAA Framework**

5 Figure 7-13 shows the corresponding WiMAX roaming reference model.

6
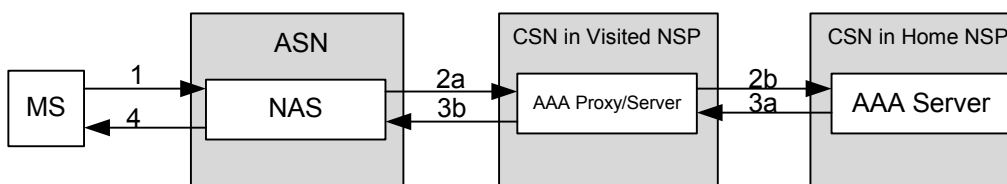
7 **Figure 7-13 - Greenfield Roaming AAA Framework**

8 In case of roaming deployments, optionally one or more AAA proxy/server entities exist between ASN and the
9 home CSN.

10 Figure 7-14 shows the corresponding WiMAX roaming reference model when CSN is in an incumbent home NSP
11 whose authorization and authentication backend is not RADIUS compliant. As in the non-roaming case, the
12 incumbent home NSP will host an IWG to map the AAA protocols and attributes to incumbent NSP specific
13 protocols and attributes, and vice-versa.

14

15 **Figure 7-14 - Non AAA Complaint Incumbent Roaming AAA Framework**

16 **7.3.3.3   Decomposition of AAA in the ASN**

17 As was shown in the above diagrams, the ASN is composed of one or more NASs. A NAS is considered as the first
18 AAA client where AAA messages originate and authentication and authorization attributes are delivered to. It is also
19 one source of accounting information (the accounting client may also be located in the CSN/Home Agent).

20 The Authentication and authorization attributes are delivered to AAA "Applications" such as, the Authenticator,
21 mobility applications (PMIP, FA), prepaid applications, QoS applications, which collectively are assumed to live in
22 the NAS.   With respect to the implementation of the ASN, these applications MAY actually reside in different
23 physical elements in the ASN. That is, the NAS MAY be implemented on multiple physical functional entities in
24 the ASN.

7.3.4 RADIUS Reference Protocol Stack

The following figure describes the RADIUS Reference Protocol Stack.
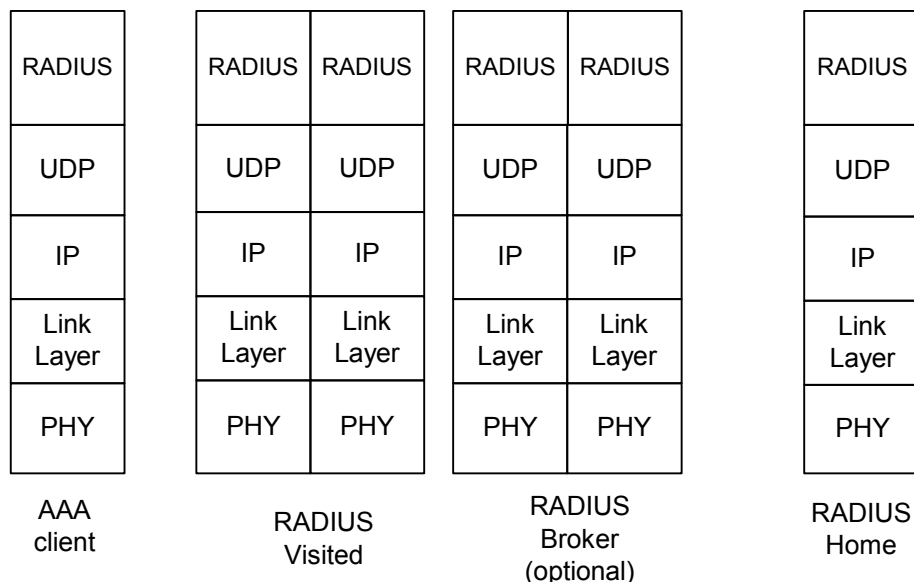
Figure 7-15 - RADIUS Reference Protocol Stack.

As shown RADIUS is based on UDP protocol and as such RADIUS protocol uses a handshake (request reply) to provide its own robustness. Retry and Failover mechanisms are left as an implementation detail.

Therefore, the WiMAX network should define a retransmission strategy that reacts to network congestion and thus does not contribute to the congestive collapse of the network.

7.3.5 Routing of AAA messages

As specified above, AAA protocols are hop by hop protocols. During operations the AAA messages SHALL be routed between the NAS and the home AAA server. In RADIUS, the routing of the messages typically depends on the NAI but MAY also depend on other attributes in the RADIUS packets. Each RADIUS based operational scenario SHOULD discuss how messages are routed.

7.3.6 AAA Security

The IETF AAA protocols are hop-by-hop secure.   That is, the AAA nodes are assumed to be trustworthy.

The AAA protocols provide protection against multiple types of external threats e.g. man-in-middle attacks. In RADIUS the protocol provides a mechanism to provide integrity protection, privacy, and protection against replay attacks. This mechanism is protected by a key that is shared between the RADIUS hops.

RADIUS may also be protected using IPsec. However, IPsec is not part of the RADIUS protocol.

This specification strongly recommends to protect the reference points and interfaces between all interconnected RADIUS client, proxy and server entities; however, the decision on a specific protection method remains a deployment-specific decision.

RADIUS uses a number of data stores. These include the user's identity store, policy stores, and an accounting store that contains accounting information collected for a period of time. These stores must be secured and maintained. The procedures for provisioning, maintaining, and securing these stores are not part of this specification.

7.3.7 Authentication and Authorization Protocols

IEEE 802.16-2004 October 2004, and IEEE 802.16e-2005 March 2006 specify PKMv1 and PKMv2 with Extensible Authentication Protocol (EAP) for user authentication and MS authorization. PKMv1 provides support for only Device Authentication whereas PKMv2 provides a flexible solution that supports device and user authentication between MS and home CSN.

1 In the architecture specified within this document, authentication and authorization must be based on EAP
2 (Extensible Authentication Protocol, compliant to [52]). In order to work with EAP, IEEE Std 802.16e PKMv2 must
3 be used between MS and ASN. Within the ASN, Intra ASN security describes additional steps to transfer EAP
4 messages and keys within the ASN entities. Between AAA server and authenticator in ASN, EAP runs over
5 RADIUS [49].

6 The AAA framework used for network access authentication and authorization can transparently support different
7 EAP methods. However, all EAP methods

8 • must fulfill the requirements to EAP methods specified in 802.16e for PKMv2 (e.g. those related to [81]),

9 • must generate MSK and EMSK as required by [52], and

10 • have to be chosen to support the provisioned credential types (details of allowed credential type mappings
11 to specific authentication modes (user/device/user and device) and the location of the EAP server
12 (ASN/Visited CSN/home CSN) are provided as part of the WiMAX Stage-3 specifications.

13 The different credential types supported in WiMAX network access authentication and authorization are listed in
14 Table 7-1.

15 **Table 7-1 - Credential Types for User and Device Authentication**

Credential	Instances	Description
SUBC	0-1	The Subscriber Root Key (SUBC) is used to authenticate the subscriber. The size of the SUBC is EAP-method specific. The SUBC is also known by the HAAA. This is a long term key. If device-Only authentication is performed, then the SUBC need not be provisioned. The SUBC must be stored securely and is never transported from the user or the HAAA.
Device-Cert	1	Private/Public Certificate based keys used to authenticate the device. The certificate conforms to X.509. This is a long term credential. The Private/Public Certificate based keys are configured at the device. The private key must be stored securely and is never transported outside the device.
Device-PSK	0-n	Preshared Key (PSK) used to authenticate the device. The PSK is also provisioned at the realm responsible for authenticating the device. There may be a PSK provisioned for each realm or PSK maybe shared by more then one realm. The later case should be avoided since sharing of the PSK increase security risk. The PSK is indexed by a NAI used during the EAP authentication. This PSK must be stored securely.

16 The provisioning of such credentials is not in scope of this document.

17 **7.3.7.1 User Authentication**

18 PKMv2 must be used to perform over-the-air user authentication. PKMv2 transfers EAP over the IEEE 802.16 air
19 interface between MS and BS in ASN. Depending on the Authenticator location in the ASN, a BS may forward
20 EAP messages over Authentication Relay protocol (e.g. over R6 reference point) to Authenticator. The AAA client
21 on the Authenticator encapsulates the EAP in AAA protocol packets and forwards them via one or more AAA
22 proxies to the AAA Server in the CSN of the home NSP, which holds the subscription with the Supplicant. In
23 roaming scenarios, one or more AAA brokers with AAA proxies may exist between Authenticator and AAA Server.
24 All AAA sessions always exist between the Authenticator and AAA server with optional AAA brokers just
25 providing conduit for NAI realm based routing.

1   Figure 7-15 illustrates the layering of user/Device Authentication protocols.
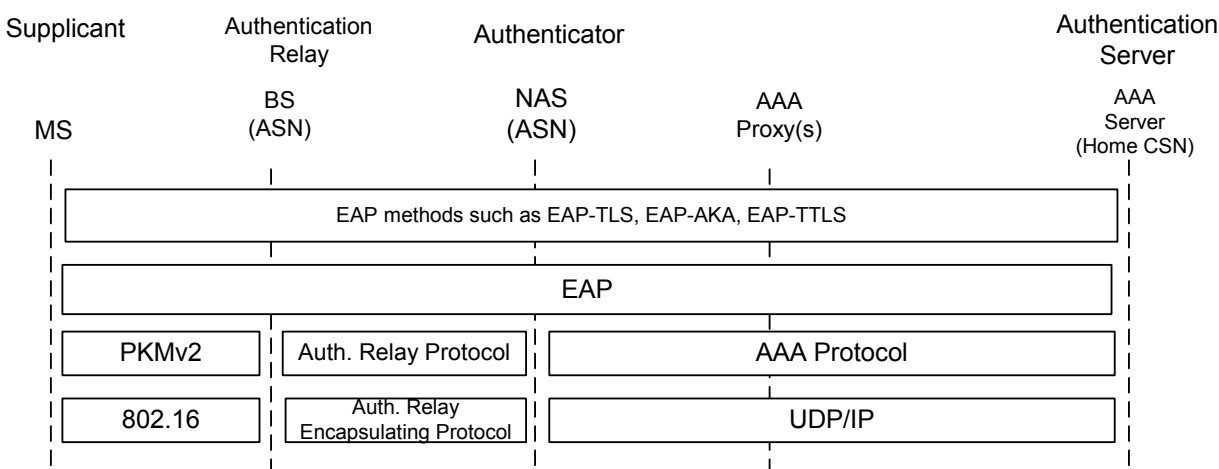
3   **Figure 7-16 - PKMv2 User Authentication Protocols**

4   **7.3.7.2   Device Authentication**

5   EAP must be used for Device Authentication. The RSA-based Device Authentication modes and the no
6   authorization mode specified in 802.16e are not supported. Only EAP-based authentication (single-EAP) and
7   Authenticated EAP-after-EAP (double-EAP) are supported.

8

9   EAP methods used for Device Authentication must generate the MSK and EMSK key.

10   **7.3.7.2.1   NAI (Network Access Identifier)**

11   The network access identifier (NAI) used in WiMAX shall conform to [60]. It is used as identifier within EAP-based
12   user and device network access authentication.

13   In EAP there are two instances where the identity is to be specified. This is when the mobile responds to the EAP-
14   Request Identity message (outer-identity), and the identity specified in the EAP method itself (inner-identity). The
15   outer-identity, as recommended by [81] and section 5.1 of [2], should be used primarily to route the packet and act
16   as a hint helping the EAP Authentication Server select the appropriate EAP method. The outer-identity is used to
17   populate the User-Name attribute of the RADIUS access-request message.

18   The inner-identity is used to identify the user, or authenticated credentials. EAP methods that provide identity
19   hiding will transmit the inner-identity within an encrypted tunnel created by the EAP method.

20   In order to support identity hiding it shall be possible to carry the real identity of the MS in the inner-identity only.
21   For the outer-identity, in this case a pseudonym is used that can be resolved to the real user identity only by the MS
22   itself and the home CSN.

23   Device credentials can be either a Device-Cert or a Device-PSK. The EAP device identifier should be a MAC
24   address or an NAI in the form of MAC_address@NSP_domain, depending on where the Device Authentication
25   terminates.

26   **7.3.7.2.2   Device Authentication Policy**

27   It is assumed that MS and home CSN know the Device Authentication policy applicable for the home CSN, with
28   regard to when the Device Authentication needs to be performed. MS should learn the Home CSN Device
29   Authentication policy as part of the MS provisioning process. The policy may dictate not performing Device
30   Authentication at all, performing Device Authentication only after power-on, or something else. The policy is an
31   operator decision. A typical policy can be to perform both device and user authentication at each power on only.

1 Until the next time the MS powers off, user-only re-authentication may be sufficient to authorize IP access of the
2 MS.

3

4 Upon access to the serving system, the MS must inform the system of its capability to perform the Device
5 Authentication. Based on the local policy of the Visited ASN, the MS may be requested to perform the Device
6 Authentication if it is capable of doing so. Alternatively, based on the local policy, the Visited CSN may grant the
7 access bypassing Device Authentication, or refuse the service to the roaming MS.

8 The serving ASN does not have to know the Device Authentication policy of the Home CSN.

9 7.3.7.2.3   Executing User and Device Authentication

10 If both user and Device Authentication need to be performed separately, Double EAP Mode must be selected. This
11 is typically the case when user and Device Authentication terminate in different AAA servers, e.g. if these are
12 located in different CSNs. These two cases are illustrated in Figures 7-16 and 7-17, respectively. In case of joint
13 authentication of device and user, a single EAP authentication will be performed if both user and Device
14 Authentication terminate in the same CSN. This selection is driven by the CSN as it knows the Device
15 Authentication policy.

16 If the MS negotiated double EAP mode, the ASN must perform Device Authentication. In this case, if Device
17 Authentication terminates in the ASN, a MAC address is used as the MS identifier instead of a fully formed NAI to
18 ensure the authentication is not forwarded to another domain.

19 The credentials for Device Authentication may be of the type Device-Cert, such that the ASN or CSN can locally
20 perform verification based on the availability of an appropriate public key infrastructure. Local authentication
21 reduces the round trip delays by not involving the CSN.

22 If a preshared key is used, then the MS identifier must be an NAI of the form (MAC_address@NSP_domain).

23 If a pre-shared key (PSK) is used, a PSK-based EAP method is used for authenticating the MS. The EAP method
24 must run between the MS and the home CSN. The target CSN is determined from the realm portion of the MS NAI.

25 If the Device Authentication fails, the ASN may deny access. If Device Authentication fails at the CSN, it should
26 notify ASN of Device Authentication failure by sending additional information.

27 Following a successful Device Authentication, the second EAP authentication must be engaged if user
28 authentication is required and Double EAP Mode was selected. The first RADIUS Access-Request message
29 generated in response to EAP/PKMv2 and sent to the home NSP must indicate successful Device Authentication to
30 the AAA server for user authentication and must carry the authenticated MS identifier in Calling-Station-ID
31 attribute. Additionally, a new vendor specific attribute (Authenticated_MS) is needed to convey the message that the
32 identifier is already authenticated. It is generated and added to the AAA exchange by the Authenticator. If the home
33 mandates Device Authentication, and the Authenticated-MS VSA is not included, that means the MS has not
34 complied with the policy. The access should be denied by the home/visited CSN in that case.

1
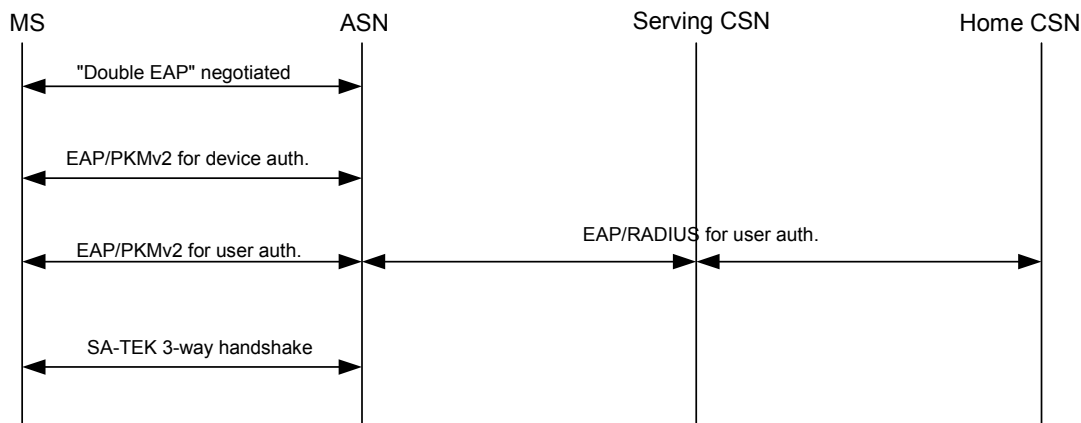
2   **Figure 7-17 - Device Authentication Terminating in ASN, User Authentication in Home CSN**

3
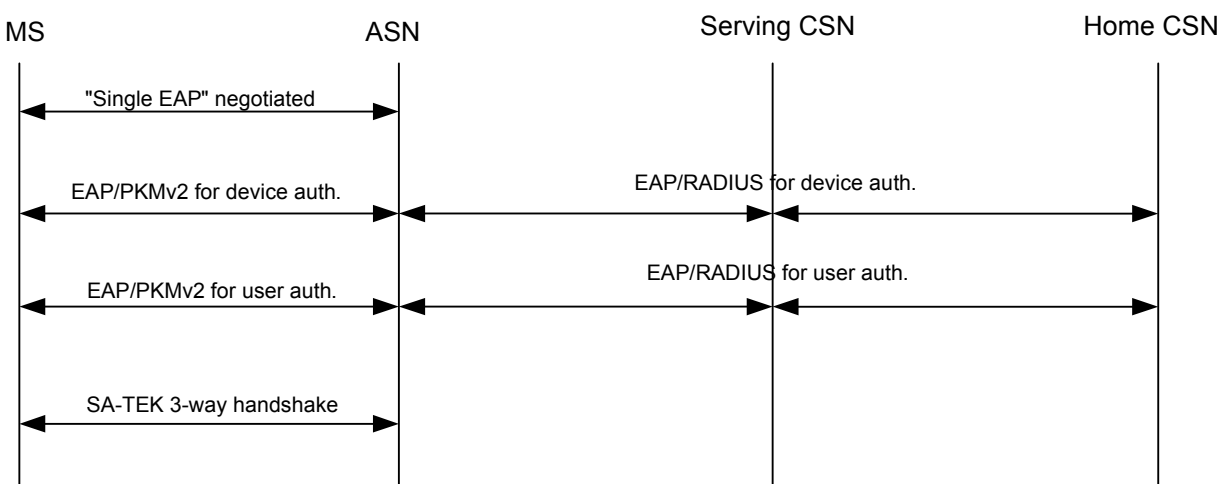
4   **Figure 7-18 - Device and User Authentication Terminating in Home CSN (tunneled EAP)**

5   When both the user and Device Authentication are based on PSK and terminate in the home CSN, the two will be
6   performed jointly as one single EAP authentication. In this case, a combined identity is generated. One PSK-based
7   EAP authentication must be performed using the computed credential. A successful authentication between the MS
8   and home CSN implicitly authenticates both the device and the user. This optional optimization aims at reducing the
9   authentication setup latency. The MS is assumed to be informed of the availability of this CSN feature either during
10   the provisioning process, or throughout the negotiations phase.

11   In some deployments only Device Authentication is required. Device Authentication must terminate in the home
12   CSN in this case.

13   ## 7.3.8   Authentication and Authorization Procedures

14   ### 7.3.8.1   PKMv2 Procedure During Initial Network Entry

15   Figure 7-18 illustrates PKMv2 procedure during initial network entry of the MS
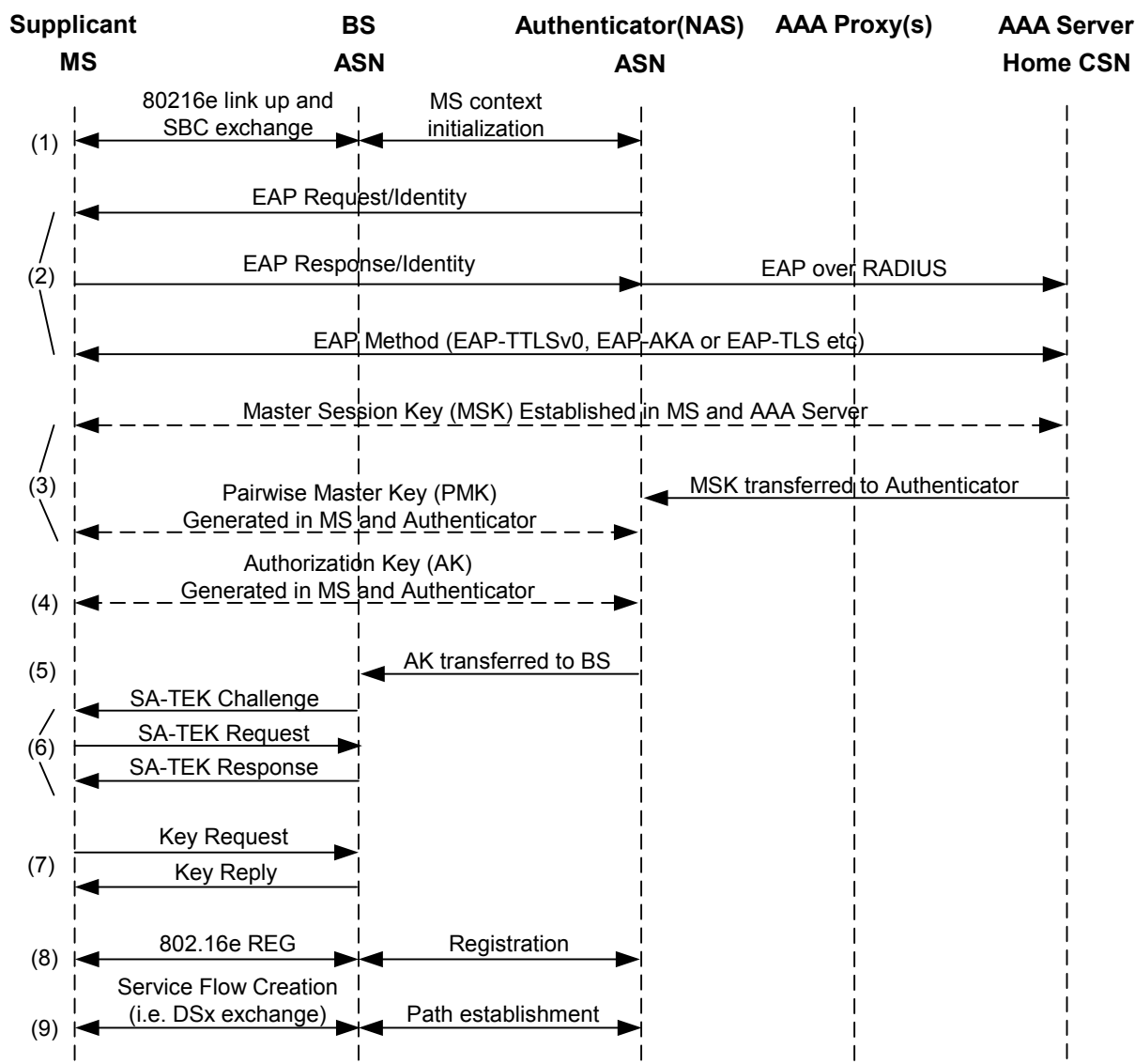
Figure 7-19 - PKMv2 Procedures

Steps for flow setup using PKMv2:

(1) Initiation of network entry according to IEEE std 802.16e

    a) Upon successful completion of ranging, the MS SHALL send the *SBC_Req* message.

    b) The ASN SHALL respond to the MS by sending the *SBC_Rsp*. During this SBC negotiation, the MS and ASN SHALL negotiate the PKM version, PKMv2 security capabilities and authorization policy including requirements and support for Device Authentication.

As a result of the successful establishment of an 802.16 air link between the BS and the MS, a link activation is sent (e.g. over R6) to the Authenticator. This causes the Authenticator to begin the EAP sequence.

(2) EAP Exchange

The authenticator sends an EAP-Identity request to the supplicant i.e. MS. Depending on the Authenticator location (i.e. BS or ASN-GW), the message may be transferred over the Authentication Relay protocol (across

1   the R6 reference interface), is next encapsulated into a MAC management PDU at the BS, and is then
2   transmitted in a EAP-Transfer message [PKM-REQ(PKMv2 EAP-Transfer)].

3   The supplicant receives the PKMv2 EAP-Transfer message, passes its payload to the local EAP method for
4   processing, and then when response is received, transmits it in a PKMV2 EAP-Transfer message [PKM-
5   REQ(PKMv2 EAP-Transfer)]. From now on the authenticator forwards all the responses from the MS to the
6   AAA proxy, which then routes the packets based on the associated NAI realm.

7

8   (3) Shared Master Session Key (MSK) and Extended Master Session Key (EMSK) establishment

9   As part of successful EAP exchange in step 2), a Master Session Key (MSK) and an Extended Master Session
10   key (EMSK) are established at the MS and the Home AAA Server. The Home AAA Server then transfers the
11   generated MSK to the Authenticator (NAS) in the ASN. The MSK is included as a VSA in the RADIUS Accept
12   message, which is sent over a secured path from the AAA Server to the ASN. The EMSK is retained at the
13   Home AAA Server. From the MSK, both the MS and the Authenticator generate a PMK as per IEEE 802.16e
14   specifications. From the EMSK, the MS and the Home AAA Server generate the mobility keys.

15   The authentication part of the authorization flow (and the involvement of the generic EAP layer) is now
16   complete.

17   (4) Authentication Key (AK) generation

18   The Authenticator and the MS generate the AK from the PMK based on the algorithm specified in the IEEE
19   802.16e specification.

20   (5) AK Transfer

21   The Key Distributor entity in the Authenticator delivers the AK and its context to the Key Receiver entity in the
22   Serving BS. The Key Receiver caches the AK and relevant security context related to the MS and is responsible
23   of generating subsequent subordinate IEEE 802.16e- specified keys from the AK and its context.

24   (6) AK Liveliness establishment and SA transfer

25   To mutually prove possession of valid Security Association based on AK, the MS and the BS perform PKMv2
26   three-way handshake procedure.

27   The BS transmits the *PKMv2 SA_TEK_Challenge* message as a first step in the PKMv2 three-way handshake at
28   initial network entry and at reauthentication. It identifies an AK to be used for the Security Association, and
29   includes a unique challenge, i.e. BS Random, that can either be a random number or a counter.

30   The MS responds with the *PKMv2 SA_TEK_Req* message after receipt and successful CMAC verification of an
31   *PKMv2 SA_TEK_Challenge* from the BS. The *PKMv2 SA_TEK_Req* message contains the number, called MS-
32   Random, which can also be either a random number or a counter.

33   The *PKMv2 SA_TEK_Req* proves liveliness of the Security Association in the MS and its possession of the
34   valid AK. Since this message is being generated during initial network entry, it constitutes a request for SA-
35   Descriptors identifying the primary and static SAs, and GSAs the requesting SS is authorized to access, and
36   their particular properties (e.g., type, cryptographic suite).

37   The BS transmits the *PKMv2 SA_TEK_Rsp* message as a third step in the PKMv2 three-way handshake. It
38   constitutes a list of SA-Descriptors identifying the primary and static SAs, the requesting SS is authorized to
39   access and their particular properties (e.g. type, cryptographic suite).

40   After the successful completion of PKMv2 three-way handshake, the MS and the BS shall start using the newly
41   acquired AK for MAC management messages protection (by CMAC) as per IEEE 802.16e specification.

42   (7) Traffic Encryption Key (TEK) generation and transfer

43   For each SA, the MS requests two TEKs from the BS. The TEKs are randomly created by the BS, encrypted
44   using the KEK as the symmetric secret key, and are transferred to the MS. This step is repeated for each SA.

45   (8) IEEE 802.16e Network Registration

After the successful PKMv2 three-way handshake completion (the MS receives *PKMv2 SA_TEK_Rsp* message from the BS), the MS SHALL send REG Request message to the BS providing ASN with the supported registration parameters. The BS SHALL respond with REG Response message. During this REG exchange, the MS and ASN negotiate network registration parameters. The BS may negotiate these parameters with the Authenticator entity in ASN GW (over R6). The completion of REG process is made known to Authenticator/ ASN GW (over R6) and it triggers Service Flow and Data Path establishment process.

(9) Service Flow Creation

The Anchor SFA entity collocated with the Authenticator starts Service Flow and the corresponding Data Path establishment process toward the BS.

The BS uses DSA-REQ/RSP/ACK MAC management messages to create a new service flow and map an SA to it thereby associating the corresponding TEKs with it.

7.3.8.2 PKMv2 Procedure During Hand-off

The PKMv2 procedure during handoff SHALL be optimized according to the following guidelines:

a) When a mobile moves within the same mobility domain, the AK is validated by signing and verifying a frame via the CMAC using the AK which is newly generated from the same PMK as long as the PMK remains valid.

b) Validating the AK is usually combined with the procedure of ranging which include 802.16e RNG-REQ and RNG-RSP with CMAC tuple.

c) Sharing TEK within a same mobility domain is possible when Handover procedure between two base stations can transfer TEK context information. If the TEK is shared among BSs, the set of BSs are considered as same security entities within a same trusted domain

7.4 ASN Security Architecture

The security architecture inside the ASN consists of the following functional entities, namely, *Authenticator*, *Authentication Relay*, *Key Distributor* and *Key Receiver*. Authenticator is defined per the Authenticator in the EAP documentation [52]. Authentication Relay is defined as the functional entity that relays EAP packets without snooping into or modifying the EAP packet via an Authentication Relay Protocol defined in Section 7.4.3 between the Authentication Relay and the Authenticator. Key Distributor is defined as the functional entity that is a key holder for both MSK and PMK resulting from an EAP exchange. The MSK is sent to the Key Distributor from the home AAA server, and the PMK is derived locally from the MSK. Additionally, Key Distributor also derives AK and creates AKID for an <MS, BS> pair and distributes the AK and its context to the Key Receiver in a BS via Context Transfer protocol. Key Receiver is the key holder for AK and is responsible for generation of IEEE 802.16e specified keys from AK.

In profiles A and C, the Authentication Relay and Key Receiver always reside in the BS. The Authenticator and Key Distributor are usually co-located. There are two deployments models: the Integrated deployment model and Standalone deployment model. In the Integrated deployment model, the Authenticator and Key Distributor are collocated with the Authentication Relay and Key Receiver and thus reside in the same BS as shown in Figure 7-20.
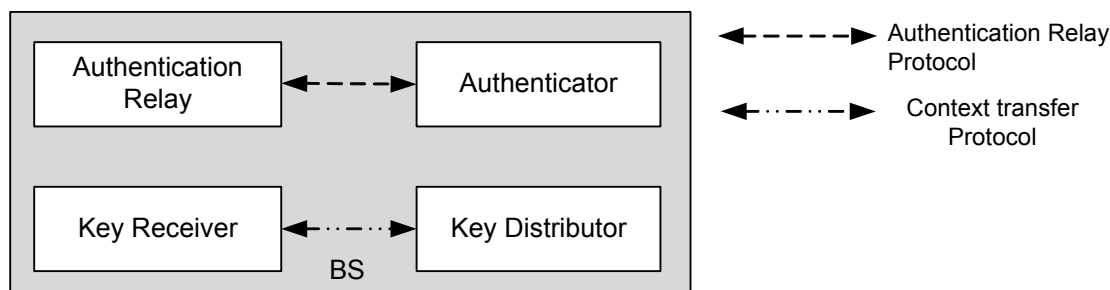
Figure 7-20 - Integrated Deployment Model

1   In the Standalone deployment model, the Authenticator and Key Distributor are collocated together on a physical
2   functional entity other than the BS as shown in Figure 7-21. It is possible to think about an architecture where
3   Authenticator and Key Distributor are not collocated but that model is not considered here.

4
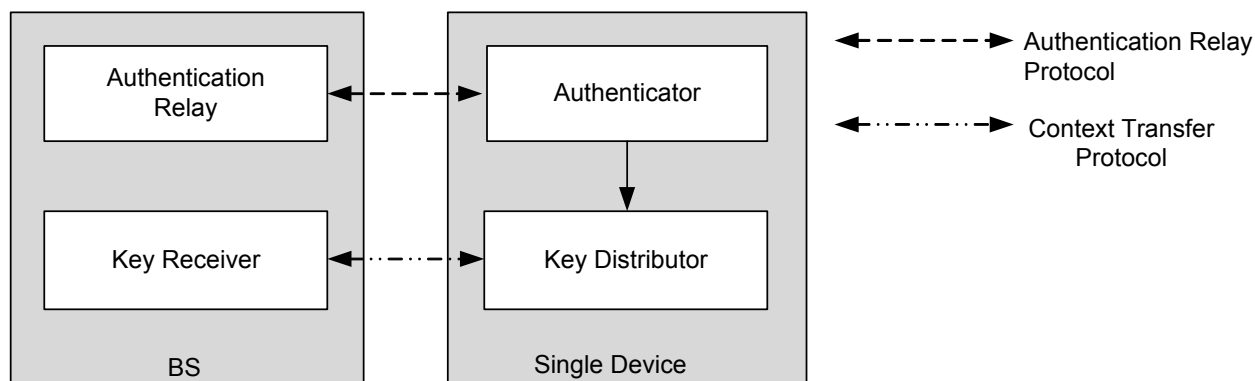
5   **Figure 7-21 - Standalone Deployment Model**

6   In the Integrated deployment model the Authentication Relay and Context Transfer Protocols are internal to the
7   implementation. In the Standalone deployment model, an Authentication Relay Protocol is defined between
8   Authentication Relay and Authenticator for relaying EAP packet as shown in Figure 7-22.

9
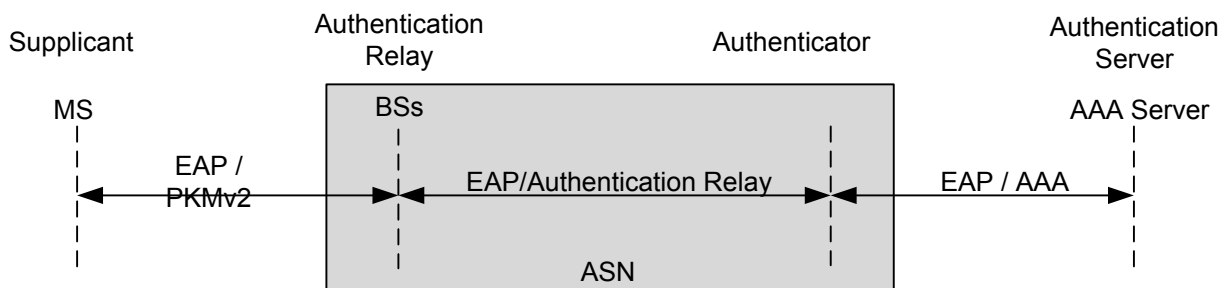
10   **Figure 7-22 - Authentication Relay Inside the ASN**

11   Additionally, for both Integrated and Standalone deployment models, the Context Transfer Protocol is defined to
12   securely transfer the keying material namely AK, and it's context (e.g. CMAC_KEY_COUNT, AK Sequence
13   Number, AKID, AK lifetime, EIK, etc.) from the Key Distributor to the Key Receiver in the target BS to which an
14   MS does a HO as shown in Figure 7-23. Since the Integrated deployment model is a sub-set of the Standalone
15   deployment model, this document just refers to Standalone deployment model.

1
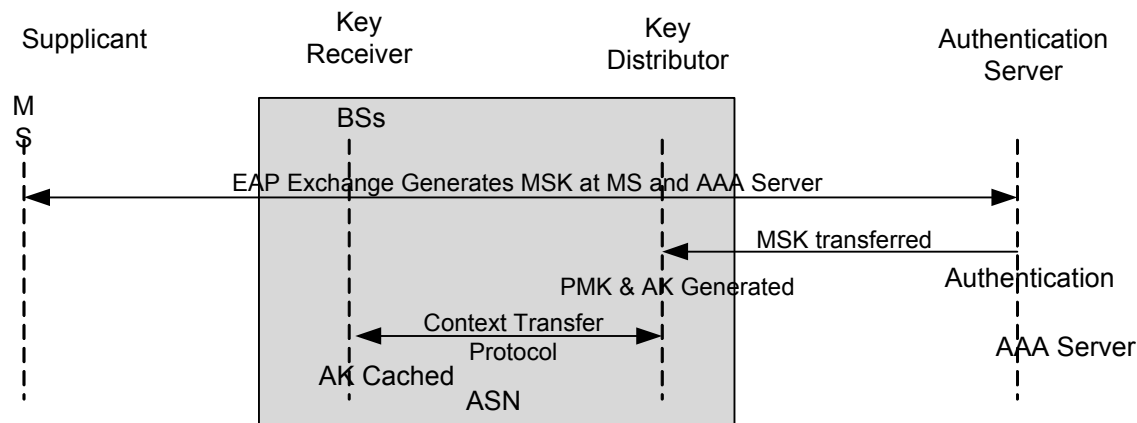
2 **Figure 7-23 - AK Transfer Inside the ASN**

3 ### 7.4.1 Architectural Assumptions

4 The function of authenticator as mentioned in [52] and EAP keying draft, [61], is not split. All authenticator
5 functions are implemented in one place.

6 The authenticator and BSs belong to the same administrative entity. Communications between them is assumed to
7 be secure, e.g., via proper encryption and integrity protection. This implies that the authenticator and BSs share
8 secrets required for secure communications. The mechanisms regarding how these shared secrets are established are
9 outside the scope of this specification. In essence this document assumes that the BSs are like physical ports of an
10 authenticator as per the EAP keying draft. Figure 7-24 shows two variants, i.e., a single or multiple BS/port(s) per
11 Authenticator.

12
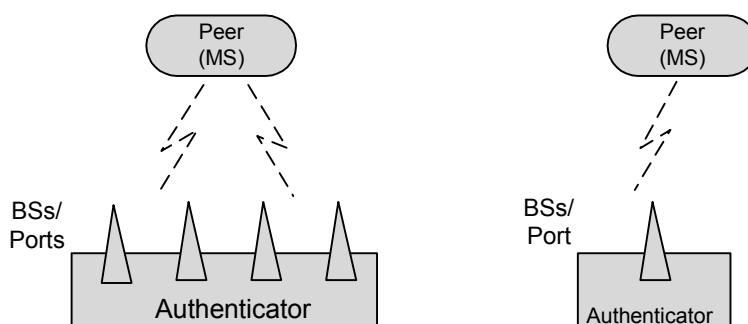
13 **Figure 7-24 - Single Versus Multiple BS per Authenticator**

14 ### 7.4.2 Authenticator Domain and Mobility Domain

15 The architecture defines a concept of *Authenticator Domain*, which consists of one or more of BSs (stand alone or
16 Integrated BS) that are under the control of a single Authenticator. All BSs within a given Authenticator Domain
17 SHALL forward EAP messages to and from the Authenticator of the domain of a given subscriber. Each BS can
18 belong to more than one Authenticator Domain.

19 When an MS enters a network, the BS forwards its EAP packets to the Authenticator of the given Authenticator
20 Domain, which becomes its *Anchor Authenticator* residing within a given trusted domain. The Anchor Authenticator
21 caches the PMK and related authentication information for MS that enter the network via one of the BSs in the
22 domain, and retains this cached information until the MS re-authenticates with a different Authenticator (which then
23 becomes the new Anchor Authenticator for the MS). If the MSK/PMK lifetime is expired (e.g. the MS leaves the
24 network), the cached information SHALL be discarded. Every MS is, at a given time, anchored at exactly one
25 Authenticator located within a NAP. Association between MS and Anchor Authenticator does not have to physically
26 match any association between MS and other ASN functions (e.g. page controller, FA).

1   The architecture also defines a concept of *Mobility Domain*, which consists of a set of BSs for which a single PMK
2   can be used to derive BS-specific AK and its contexts as the MS performs handoffs. A Mobility Domain MAY be
3   equal to a NAP, and maps to one or more Authenticator Domains. However, as the PMK SHALL be generated by
4   the Authenticator, the PMK CANNOT be shared across the Authenticator Domains within the mobility domain.

5   A *Key Distributor* belongs to a Mobility Domain, and there MAY be multiple Key Distributors in a domain, and
6   Figure 7-25 and Figure 7-26 show the relationships between the two domains and the Authentication Relay and
7   Context Transfer protocols in context of integrated and standalone models.

8
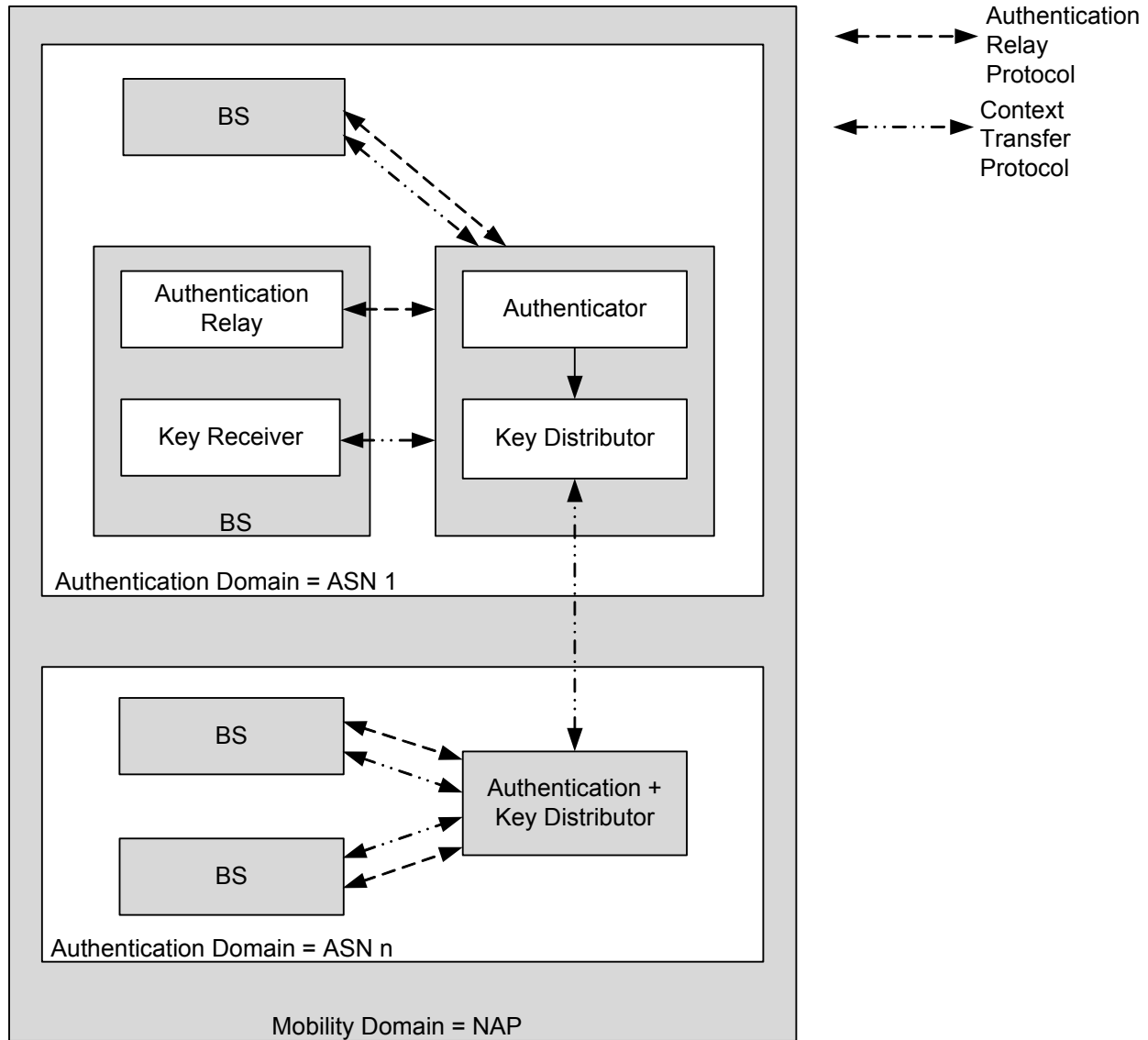
9   **Figure 7-25 - Mobility and Authenticator Domains – Standalone Model**

Unspecified Mechanism

Context Transfer Protocol

1
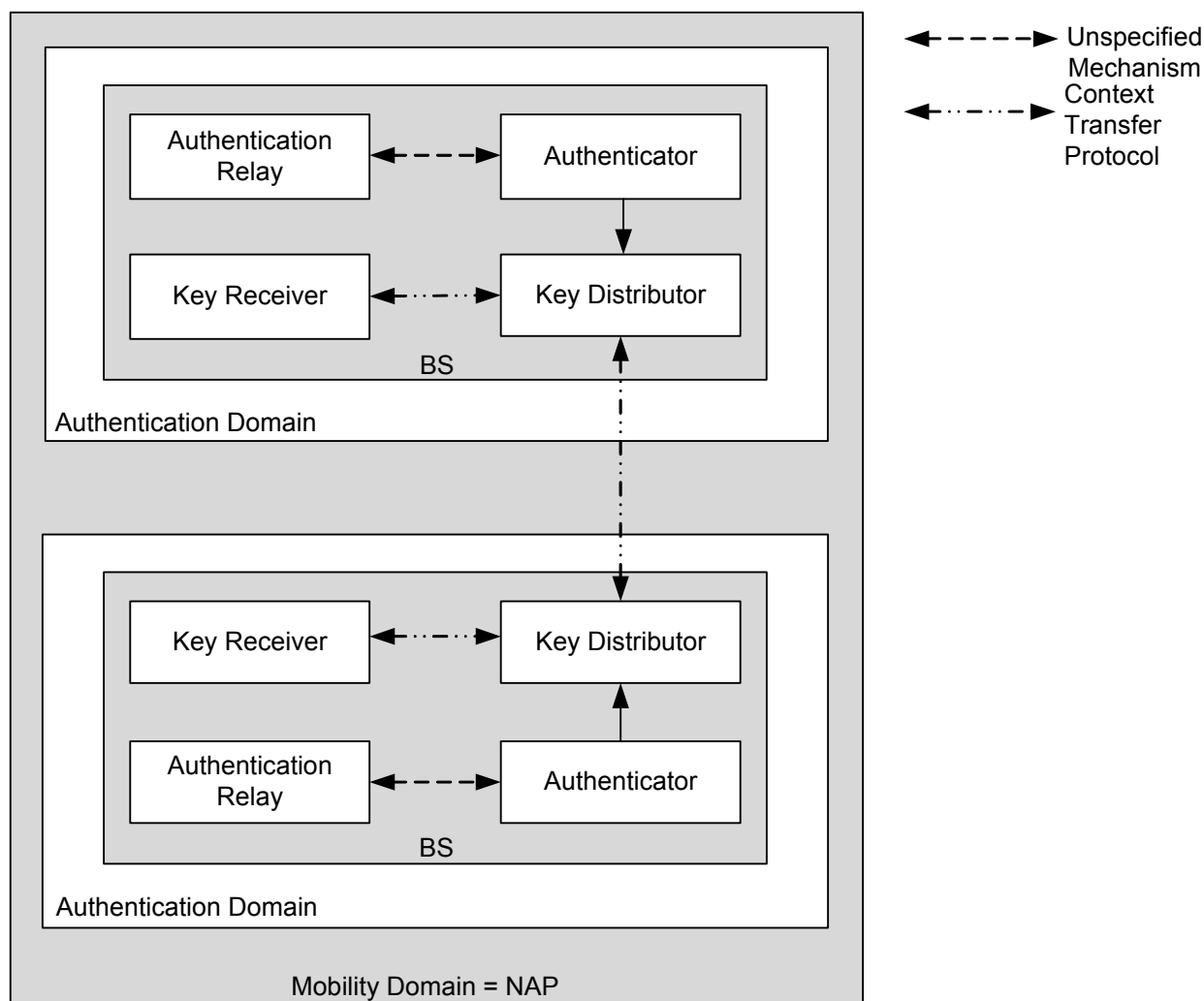
Figure 7-26 - Mobility and Authenticator Domains – Integrated Model

7.4.3 Re-Authentication Procedure

The full re-authentication EAP exchange like the initial authentication EAP exchange is done via the authenticator associated with the current serving BS. Typically, this MAY lead to a change of authenticator, if the current serving BS is associated with a different authenticator than the one which is current acting as the authenticator for the MS.

The re-authentication MAY be initiated by either:

The target authenticator: In this case, the target Authenticator autonomously initiates and executes the full EAP exchange authentication. Once the EAP exchange authentication is successfully completed, the target Authenticator becomes an Anchor Authenticator, and MAY send to the serving Authenticator an optional "RE-AUTH-IND" message including the MS identity. Thus the serving Authenticator can free resources.

Or the serving Authenticator: In this case the serving (current Anchor) Authenticator informs the target Authenticator that the full EAP exchange authentication is required. The re-authentication is initiated by a RE-AUTH-REQ message from the serving to the target Authenticator. Once the EAP exchange authentication is successfully completed, the target Authenticator sends a RE-AUTH-CONF message to the serving Authenticator so that it can free resources.

7.4.4 Authentication Relay Protocol

In the Standalone model a transport protocol is needed to exchange the EAP PDUs between the Authentication Relay and Authenticator as shown in Figure 7-27.

1
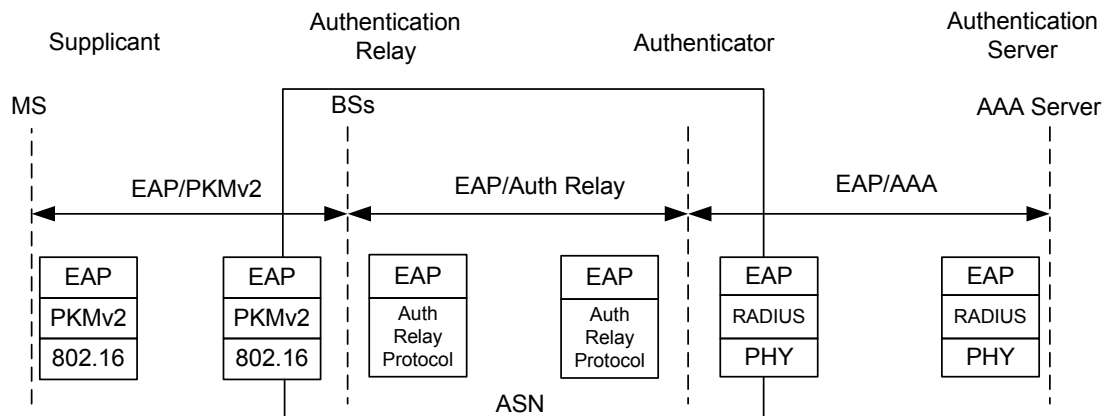
Figure 7-27 - Authentication Relay Protocol

Also, the protocol SHOULD address all the requirements placed by [52] on the EAP lower layer. Authentication Relay Protocol MAY transfer EAP.

7.4.5 Context Transfer Protocol

When the MS handoffs between BSs that belong to the same mobility domain, the key receiver in the target BSs need to be populated with AKs derived from the PMK stored in the Key Distributor if it has not expired. The Key Distributor uses the Context Transfer protocol to populate AK in the Key Receiver in the target BS to which the MS conducts HOs.

The Context Transfer protocol[6] is a two-message exchange between the Key Distributor and the Key Receiver, consisting of an optional Request message and a mandatory Transfer message. The *Context_Req* message requests a new AK from the Key Distributor, and the *Context_Rpt* message either delivers an AK, AKID, AK Lifetime, AK Sequence Number and EIK or indicates a failure. The identity of the Key Distributor is determined based on the MS identifier in the *Context_Req* message. This is depicted below:

Key Receiver → Key Distributor: *Context_Req*

Key Distributor → Key Receiver: *Context_Rpt*

The following figures show example scenarios of how the *Context_Req* and *Context_Rpt* exchange is triggered. The actual instance during a handoff when this transfer is triggered is controlled by ASN mobility management protocol.

---

[6] It is expected that Context Transfer Protocol primitives will be implemented in form of TLVs that will be exchanged as part of intra-ASN and inter-ASN mobility management protocols.

1
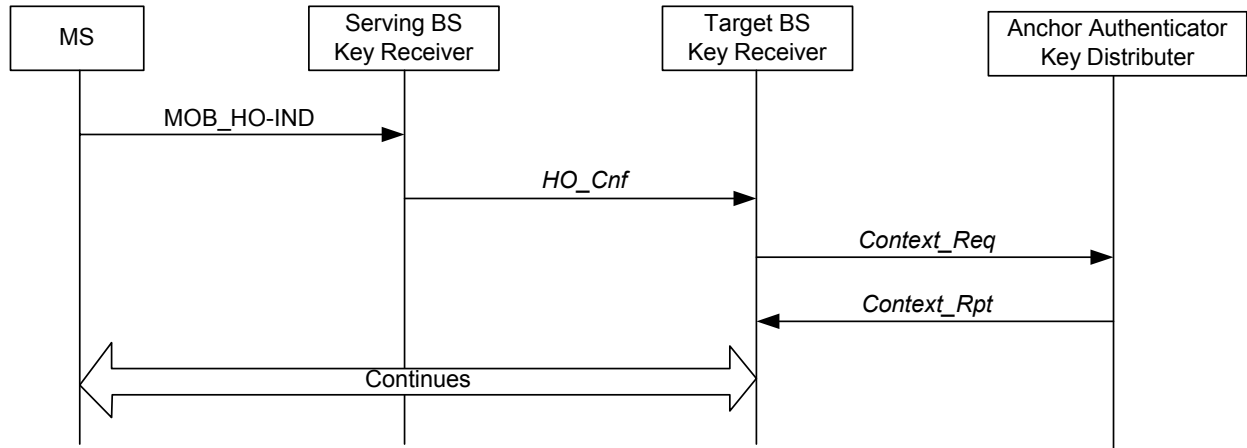
Figure 7-28 - *Context_Rpt* **Triggered by MOB_HO-IND**

2

3
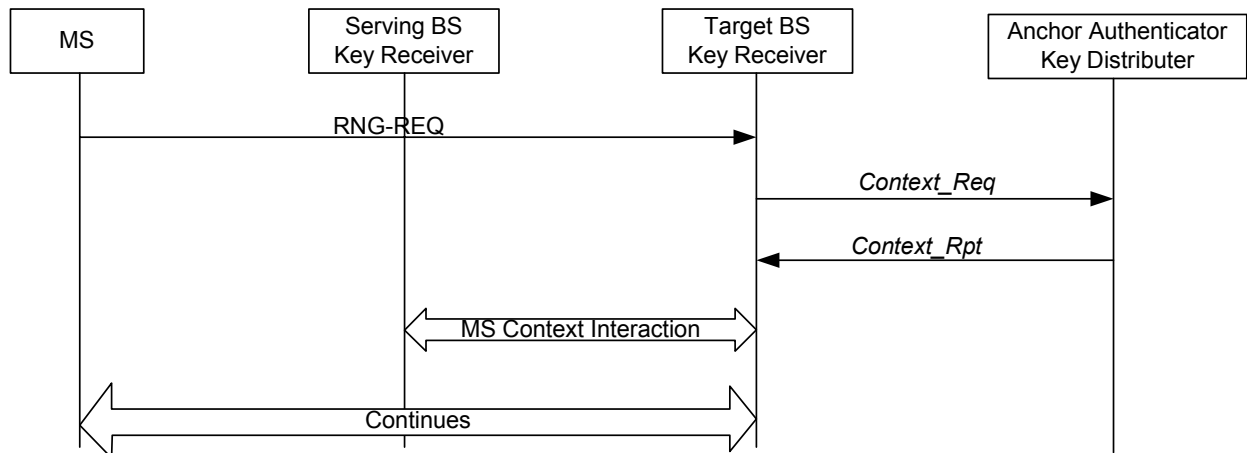
Figure 7-29 - *Context_Rpt* **Triggered by RNG-REQ**

4

1
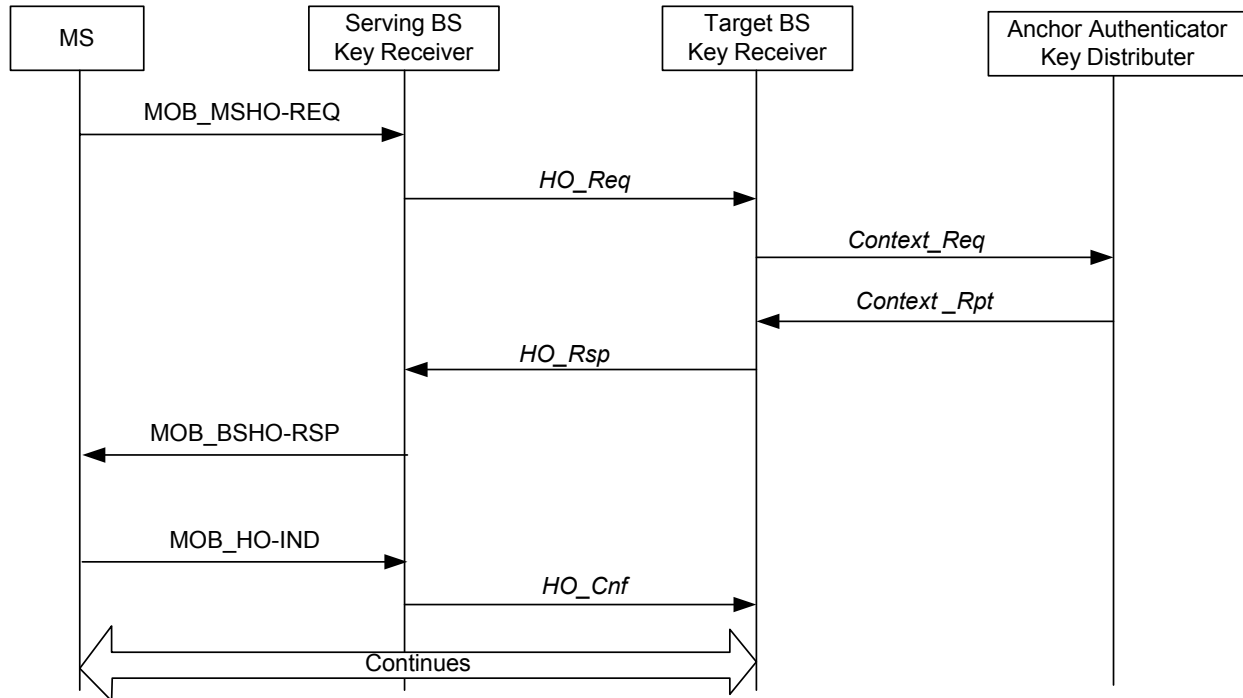
Figure 7-30 - *Context_Rpt* **Triggered by MOB_MSHO-REQ**

3   In both the Integrated model and Standalone model, AK can be transferred to a Key Receiver that is not co-located
4   with the Key Distributor. Therefore, a secure association SHOULD exist between Key Receiver and Key Distributor
5   in order to secure the transfer of AK, etc. AK, AKID, AK Sequence Number and EIK are derived as per 802.16e
6   draft. The BS upon receiving the *Context_Rpt* message, decrypts the AK, AKID, AK Lifetime, AK Sequence
7   Number, CMAC_KEY_COUNT and EIK etc., and stores them locally for future use.

8   Lastly, when MS does a handoff such that serving and target BSs are associated with different Key Distributors,
9   Context Transfer protocol exchanges occur between the Key Distributors as shown in Figure 7-31. Any intermediate
10   Key Distributors just act as relay in such a situation.

11
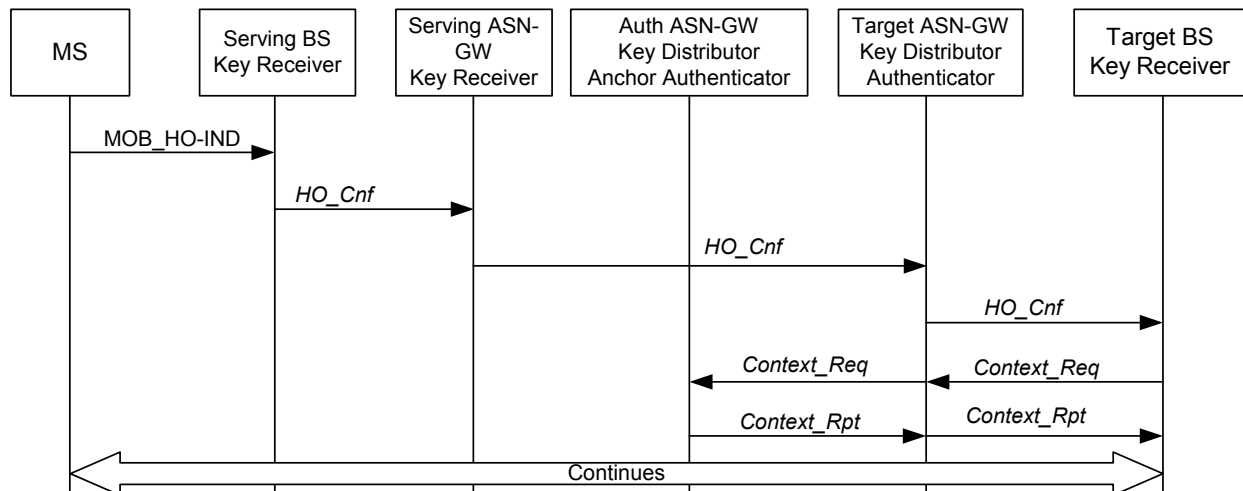
Figure 7-31 - *Context_Rpt* **Triggered by MOB_HO-IND**

13   Considering the Target BS address Anchor Authenticator, it is necessary to exchange Anchor Authenticator ID
14   information during HO preparation between Serving BS and Target BS.

1   ## 7.5   Accounting

2   Accounting in NWG Release 1.0.0 will be based on RADIUS. Both offline (post-paid) and online (prepaid)
3   accounting capabilities are supported. The accounting architecture, protocols and procedures are described in the
4   following sections.

5   ### 7.5.1   Accounting Architecture

6   Accounting architecture is shown in Figure 7-32 below. The figure shows network elements for both offline and
7   online services. The figure also shows the network elements for Hot-lining support and negative volume count for
8   ASN. A description of each entity is provided in the following sections.

9
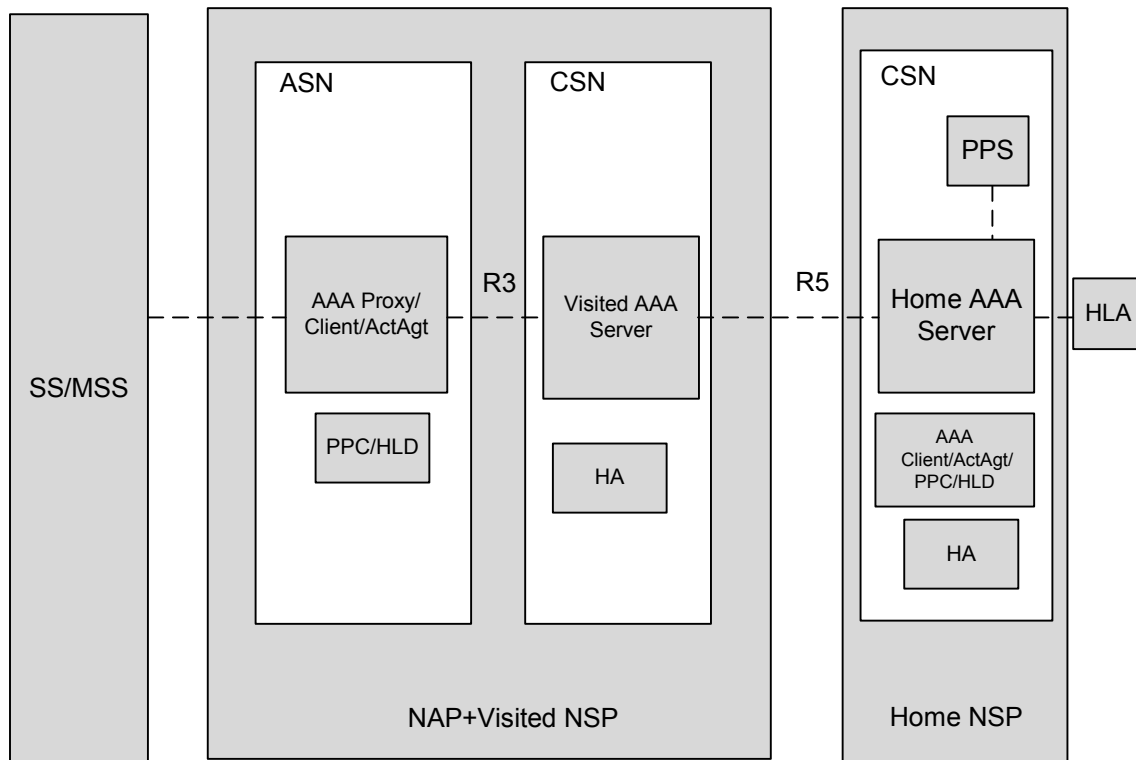
10   **Figure 7-32 - Accounting Architecture**

11   **7.5.1.1   Accounting Primitives**

12   **7.5.1.1.1   Accounting Information Request**

13   This primitive is sent from AAA client to accounting agent to configure accounting agent or request accounting
14   information**.**

15   **7.5.1.1.2   Accounting Information Report**

16   This primitive is sent from accounting agent to AAA client to report accounting information which can be triggered
17   by accounting information request or automatically report to AAA client per configuration.

18   **7.5.1.1.3   Accounting Information Acknowledge**

19   This primitive is sent from AAA client to accounting agent to acknowledge the receiving of accounting report.

1   ## 7.5.2   Accounting Protocols

2   ### 7.5.2.1   Negative Volume Count in ASN

3   The AAA Proxy/Client sends all downlink data to the Account Agent over the interface in the ASN. Any discarded
4   or unsent data between MS and the Account Agent causes inaccurate charging, as the AAA Proxy/Client cannot
5   account for this and subsequently causing overcharging. Negative Volume count records the packet volume of lost
6   packets which can be measured as number of packets, octets, etc.

7

8   The following figure illustrates negative volume count protocols:

9
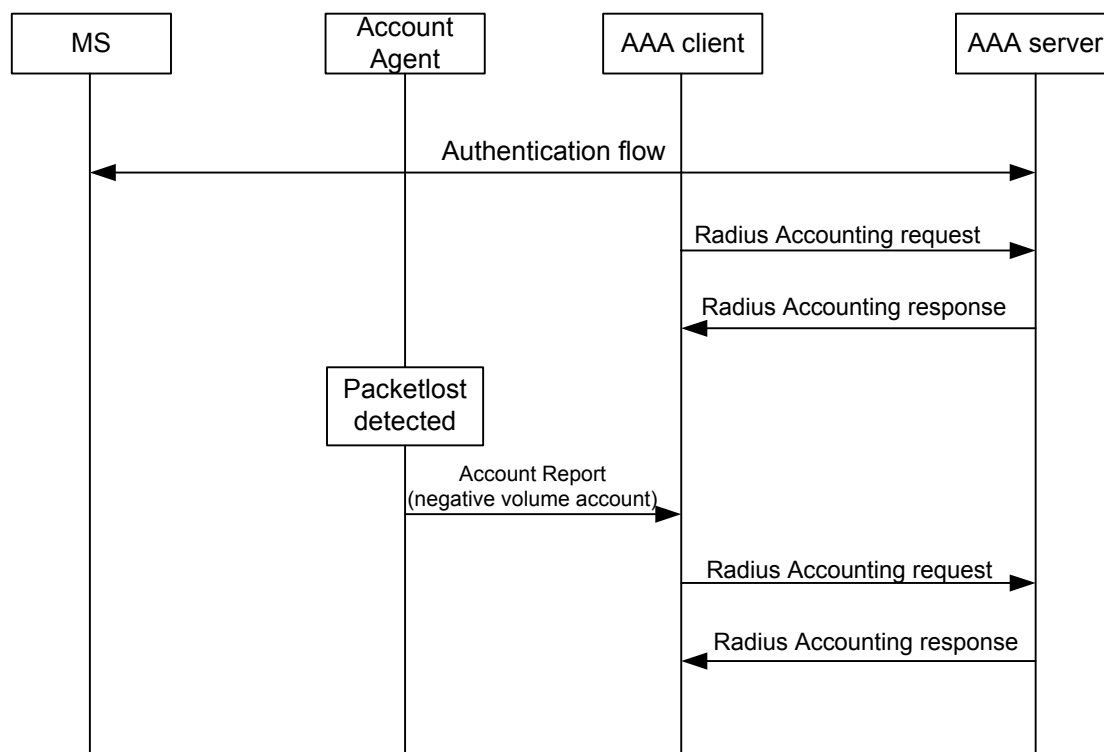
10 **Figure 7-33 - Negative Volume Count**

11 ## 7.5.3   RADIUS Server Requirements

12 The RADIUS Server SHALL follow the guidelines specified in [23], [24], and [36].

13 The Visited and Home RADIUS server SHALL support the attributes as specified in Stage 3 RADIUS Message
14 section 5.4.1.

15 Upon receiving RADIUS Accounting-Request records from the ASN, the Visited RADIUS server SHALL forward
16 the RADIUS Accounting-Request records to the home or broker network.

17 The communication between RADIUS client and RADIUS server or between RADIUS servers SHALL be protected
18 using the secret shared with the next hop RADIUS server using the procedures described in [23].

19 ## 7.5.4   HA Requirements as RADIUS Client

20 If the HA supports the Radius client then the HA SHALL support RADIUS client as specified in [23] and RADIUS
21 Accounting as specified in [24] and [36].

22 The HA SHALL send a RADIUS Access-Request to the Home RADIUS server when it receives an RRQ
23 (Registration Request) containing the authentication extension to request authentication and authorization of the user

1 by the RADIUS infrastructure. The HA SHALL include the RADIUS attributes and VSAs in the Access Request as
2 specified in Stage 3 section 5.4.1.

7.5.5   Offline Accounting

4 This section describes the off-line (post-paid) accounting procedures and the Usage Data Records (UDRs). It also
5 describes the RADIUS standard attributes and VSAs used to support accounting capabilities in the WiMAX
6 network.

7 It is important to note that a lower case letter implies an accounting attribute in an Airlink Record whereas an
8 uppercase letter implies an accounting attribute in a UDR.

9 Packet data accounting parameters are divided into radio specific parameters (e.g., number of bytes/packets dropped
10 at the BS), and IP network specific parameters collected by the Serving ASN. The Serving ASN SHALL merge
11 radio specific parameters called Airlink Records with IP network specific ones to form one or more Usage Data
12 Records (UDR). After merging, the Serving ASN SHALL use RADIUS accounting messages to send UDR
13 information to the home RADIUS Server (via the visited AAA server if the subscriber is roaming). The detailed
14 procedures for creating UDRs are described in the following sections.

7.5.6   Airlink Records

16 The ASN generates the following airlink records:

17 • An Active Start Airlink Record when the MS has connected the associated over-the air service flow.

18 • An Active Stop Airlink Record when the MS has released the associated over-the-air service flow.

7.5.7   ASN Procedures

20 The following events cause the ASN to take accounting action:

21 • R6 Connection Setup Airlink Record received over R6 reference point.

22 • Data service establishment on the ASN-GW for profile A or C or data path establishment for a MS at the
23 ASN for profile B.

24 • Data service termination on the ASN-GW for profile A or C or data path termination for a MS at the ASN
25 for profile B.

26 • Reception of Active Start Airlink Record.

27 • Reception of Active Stop Airlink Record.

28 • Interim-Update record trigger.

29 • Stop record trigger.

30 • Time of day timer expiry.

31 • Hot-lining

32 • Inter-ASN hand-off trigger.

33 • The location information for postpaid (Only location based postpaid accounting is specified in this release.
34 Location based prepaid will be specified in a later release)

35 • The QoS of the service flow or the session is changed.

36 Each individual session SHALL be accounted for independently. All UDR information is stored and transmitted per
37 assigned IPv4 address or IPv6 prefix, or per packet data flow. During the lifetime of the session, UDRs are created,
38 modified, maintained, copied, and released for each individual connection. The Serving ASN SHALL create one
39 UDR per R6 connection ID or other data path ID established for the MS

40 The ASN closes a UDR when any of the following events occur:

41 • An existing service flow is deleted, denied, or failed.

42 • The ASN determines the packet data session has ended.

At an initial R6 connection establishment, a UDR is created and initialized from the R6 connection setup airlink record. When there is a new R6 connection due to a handoff for an existing packet data session, or when there is a new R6 connection for an existing packet data session, a UDR is created by copying data from a previous UDR.

During a inter ASN handoff either two R6 connections, or an R4 and an R6 connection, or two R4 connections with the same SFID and MSID MAY exist momentarily due to the ASN bicasting. Since the MS can connect to only one ASN for a given service flow, the ASN accounting procedures SHALL ensure that double counting between the current and new (copy) never occurs despite the ASN bicasting of data to both service flows.

RADIUS accounting messages are generated from the information in the UDR. The Acct-Multi-Session-Id is used to match different accounting records (Account Session IDs) across R6, R4 or both connections for a single packet data session. One Acct-Multi-Session-Id for all R6 connections is maintained for a packet data session for each NAI and IP pair within the same Visited CSN. The Account Session ID is used to match a single RADIUS Start and Stop pair. A different Account Session ID is used for each R6 connection.

A new R6 connection due to intra-ASN handoff between BSs SHALL result in a new R6 Connection ID and Account Session ID. The MSID and SFID are used to select the proper UDR after an intra-ASN handoff. One R6 Connection ID MAY be associated with multiple simultaneous NAI, IP pairs in the Serving ASN (i.e., multiple packet data sessions).

In profile A and C, airlink records are only associated with an R6 connection ID. The Serving ASN matches the R6 Connection ID in the airlink record to the R6 Connection ID in the appropriate UDR(s). If more than one UDR matches, the actions are applied to all UDRs.

Some events cause certain UDR fields to change in the middle of a session. When this happens, the ASN MAY send a RADIUS Accounting-Request-Stop record to capture accounting data before the event, followed by a RADIUS Accounting-Request-Start record with the new field values. In fact, an ASN MAY send a RADIUS Accounting-Request-Stop and RADIUS Accounting-Request-Start anytime during a single session as long as no accounting data is lost. In these cases, the ASN SHALL send the same Acct-Multi-Session-Id in both the RADIUS Accounting-Request-Start and RADIUS Accounting-Request-Stop records.

The subsequent sections specify the actions to take for each event.

7.5.8   Online Accounting (Prepaid)

This section describes the online (prepaid) accounting procedures in the WiMAX network. The prepaid packet data service allows a user to purchase packet data service in advance based on volume or duration. Account status is stored on a prepaid server (PPS) that is located in the user's home network and accessed via the HAAA server. To provide service to roaming prepaid users, the visited ASN or CSN needs to support the prepaid service and the local and broker AAA servers need to forward the new prepaid accounting attributes transparently to and from the home AAA server. The HAAA server and the prepaid server could be collocated or could be separate entities (see Figure 7-32).

From the ASN perspective, the HAAA and the prepaid server are indistinguishable. Although this document does not make assumptions about the prepaid server – HAAA interface, the call flows MAY show the prepaid server and the HAAA as separate entities.

The prepaid billing solution can provide the following services:

    a)   Simple IP based service metering in real time.

    b)   Undifferentiated Mobile IP services in real time with support for multiple Mobile IP sessions per user. "Undifferentiated" means that all the Mobile IP sessions for a single user will be rated equally.

    c)   Rating measurement based on data volume and/or call duration. Data volume is measured as total octets, uplink octets, downlink octets, total packets, uplink packets or downlink packets and total duration. The rating function can be done either by the prepaid client or prepaid server.

Prepaid service for multiple simultaneous data sessions is also allowed. As the network does not have any a priori knowledge of the user usage behavior, the solution is built on an iterative authorization paradigm. The prepaid server will apportion a fraction of subscriber's balance into a quota, each time an authorization request is made. Multiple sessions from the same user will each obtain their own quota, each session needs to seek reauthorization when the previously allocated quota is depleted thus minimizing any leakage. The granularity and the magnitude of

the quota are implementation details of the prepaid server; therefore, it is beyond the scope of this specification. The limitation with this method is as the number of session increases, the quota for each session will be diluted. The user might need to close some sessions in order to collect all remaining quota that was allocated to his active sessions.

In order to support prepaid packet data service the ASN and/or the CSN SHALL support the prepaid client (PPC) function and the prepaid server (PPS) function MAY be collocated with the Home RADIUS server. In this specification, the prepaid packet data service supports a set of capabilities as described in the next section. Additional capabilities MAY be supported in future revisions of this specification. When the prepaid account of user is depleted, the PPC SHALL stop the online accounting service. If the user also has a postpaid account and is authorized to hand off off-line accounting base on profile or rule, the PPC of the ASN can notify the AAA client of ASN that SHALL create the UDR and send an off-line RADIUS accounting-request to AAA server but the service flow SHOULD not be terminated.

7.5.9 Online Accounting Capabilities

In this revision of the specification, the following prepaid capabilities are supported:

- Volume based prepaid, with quota assigned at a service flow level if the PPC resides in the ASN.

- Volume based prepaid with quota assigned at the packet data session level (IP/NAI) if the PPC is located in the CSN.

- Duration based prepaid, with quota assigned at a service flow level if the PPC resides in the ASN.

- Duration based prepaid, with quota assigned at the packet data session level (IP/NAI) if the PPC is located in the CSN.

- Ability for the Home AAA/PPS to allow/deny/select a PPC based on the Home AAA/PPS policy, user profile, PrePaidAccountingCapability (PPAC) VSA and the Session Termination Capability (STC) VSA of the ASN and/or the CSN.

- The prepaid packet data service is based on the RADIUS protocol.

- Home AAA/PPS ability to manage the prepaid packet data service when the quota allocated to a PPC is consumed or a pre-determined threshold value is reached, through triggers provided to the PPC.

- The capability of the PPC based in the ASN to support VolumeQuota and a tariff switch time interval concurrently per service flow. The capability of the PPC based in the CSN to support VolumeQuota and a tariff switch time interval concurrently per packet data session.

- The capability in the PPC and the Home AAA/PPS to provide tariff switch volume based prepaid packet data service, with tariff switch trigger controlled at the Home AAA/PPS. This capability includes:

- Charged by volume, different tariff for different time of a day.

  o Charged by volume, different tariff for different volume consumed, and the PPS SHALL allocate the quota so that the quota does not overlap the two charging rates.

  o Charge by volume, different tariff for different QoS. When the Qos is changed, the PPC can report the consumed volumes before the change and the PPS SHALL allocate the new quota for new QoS.

Tariff switching with duration based prepaid at the Home AAA/PPS. This capability includes:

- Charged by duration, different tariff for different time of a day.

- Charged by duration, different tariff for different duration consumed, and the PPS SHALL allocate the quota so that the quota does not overlap the two charging rates.

- Charged by duration, different tariff for different QoS.

- Account balance updated by the Home AAA/PPS according to the quota consumed by the user and reported by PPC and the tariff information in the user's profile.

- The prepaid account SHALL be reconciled at the Home AAA/PPS at inter-ASN handoff.

7.5.10 QoS-based Accounting

The QoS-based accounting is charging on service session, not user connection as traditional accounting does. The WiMAX network is capable of support multiple services for one user simultaneously with appropriate QoS level. The accounting on QoS is both feasible and useful.

The accounting function SHOULD be capable of separating one service session from others by characteristics of the service such as TCP/UDP port, protocol type, etc. RADIUS accounting messages, added with the information of service session and QoS level, are generated in AAA client and sent to AAA server.

7.5.11 ASN Requirements for Prepaid

If the ASN supports a PPC, it SHALL also support Dynamic Authorization with RADIUS [48] and Registration Revocation for Mobile IPv4 capabilities [45]. The ASN is referred to as a prepaid capable ASN, and the prepaid capability is based on the following principles:

- The ASN includes in the RADIUS Access-Request message to the Home RADIUS server/PPS, the PPAC VSA and the STC VSA. The values for each VSA are set appropriately and will be specified in the stage 3 specifications.

- Except for quota initialization for the Initial service flow (ISF), which is included in the RADIUS Access-Accept message by the Home RADIUS server/PPS, on-line quota update operation is performed by the prepaid capable ASN using on-line RADIUS Access-Request/Accept messages with Service-Type (6) set to "Authorize Only". The on-line RADIUS Access-Request SHALL contain the PrePaidAccountingQuota (PPAQ) VSA.

- The Home RADIUS Server/PPS initializes a quota for a user at authentication and authorization if it determines that the user is a prepaid user with positive prepaid balance and that the home network policy allows the ASN to provide prepaid service. The initialized quota is sent to the PPC in the RADIUS Access-Accept message associated with the creation of the Initial service flow. The RADIUS Access-Accept message includes the PPAQ and PPAC VSAs.

- The processing of off-line Accounting Request/Response messages proceeds independent of prepaid service.

- RADIUS Accounting (Stop/Start) messages caused by events such as parameter change, time of the day change, intra-ASN handoff do not cause the prepaid counters (such as VolumeQuota used, DurationQuota used etc.) to be re-set to zero.

If the RADIUS Access-Accept message includes the initial quota and contains the Service Profile attribute which indicates that the user is allowed to establish multiple service flows, the prepaid capable ASN MAY immediately initiate an on-line RADIUS Access-Request message to request pre-initialization of quota for any additional service flow that the user MAY establish.

If the user requests establishment of a service flow for which quota pre-initialization is not done, the ASN sends an on-line RADIUS Access-Request message to request initialization of quota.

The PrePaid capable ASN and the Home RADIUS/PPS MAY support tariff switch for volume based PrePaid packet data service.

7.5.12 CSN Requirements for Prepaid

The prepaid capable CSN SHALL support prepaid for packet data sessions identified by IP/NAI.

The prepaid capable home CSN SHALL enforce reverse tunneling for all the authorized volume based prepaid packet data sessions.

The prepaid capable CSN SHALL send a RADIUS Access-Request message to the Home RADIUS/PPS upon receiving the initial RRQ, re-registration and updated (new CoA) RRQ. The RADIUS Access-Request message SHALL include the additional VSAs: PPAC, STC and a Acct-Multi-Session-Id generated by the CSN. For the initial RRQ, the CSN SHALL include in the RADIUS Access-Request the MIP Lifetime VSA containing the RRQ Lifetime Sub-Type with the value corresponding to the lifetime received from the RRQ message. For the re-registration or the updated RRQ (new CoA) for the user, the CSN SHALL include the Session Continue VSA set to TRUE, the Correlation ID VSA with the same Acct-Multi-Session-Id value that is in use and the MIP Lifetime VSA

1   containing both the RRQ Lifetime Sub-Type (lifetime value received in the RRQ) and the Used Lifetime From
2   Existing Session Sub-Type (value of used lifetime of the existing Mobile IP session) if duration based prepaid is
3   being provided for the session.

4   If the RADIUS Access-Accept message from the Home RADIUS/PPS contains the PPAC VSA indicating that
5   prepaid accounting SHOULD be provided for the user, the RADIUS Access-Accept message SHALL include a
6   PPAQ VSA with an initial quota unless the Acct-Multi-Session-Id sent in the RADIUS Access-Request is the same
7   as an existing prepaid session for which there exists an outstanding quota.

8   If a new MIP Lifetime VSA is included in the RADIUS Access-Accept message from the Home RADIUS/PPS, the
9   prepaid capable CSN SHALL include the value in the MIP RRP back to the ASN.

10   If both DurationQuota and TariffSwitchInterval are received for the same prepaid packet data session, the prepaid
11   capable CSN SHALL discard the TariffSwitchInterval and SHALL provide prepaid based on the DurationQuota
12   only.

13   If the PTS VSA is received, it SHALL include the TariffSwitchInterval (TSI) Sub-Type, and MAY include the
14   TimeIntervalafterTariffSwitchUpdate timer (TITSU) Sub-Type. TITSU Sub-Type MAY be included when more
15   than one tariff switch boundary exists, and the user MAY not reach the VolumeThreshold before the next tariff
16   switch boundary is crossed. The prepaid capable CSN SHALL monitor both the Volume and the Duration
17   concurrently to support tariff switching. The detailed accounting procedures for various prepaid services (Volume-,
18   Duration- and Tarrif-Switched-base) are specified in the stage 3 of this specification.

19   7.5.13 Hot-Lining

20   The Hot-lining feature provides a WiMAX operator with the capability to efficiently address issues with users that
21   would otherwise be unauthorized to access packet data services. When a problem occurs such that a user MAY no
22   longer be authorized to use the packet data service, a wireless operator using this feature MAY hot-line the user, and
23   upon the successful resolution of the problem, return the user's packet data services to normal. When a user is hot-
24   lined, their packet data service is redirected to a Hot-line Application (HLA) which notifies the user of the reason(s)
25   that they have been hot-lined and offers them a means to address the concerns meanwhile blocking access to normal
26   packet data services. Reasons for hot-lining a user are: prepaid users whose account has been depleted; or users who
27   have billing issues such as expiration of a credit card; or users who have been suspected of fraudulent use.

28   As a result, hot-lining performs the following four fundamental activities:

29   • Blocking normal packet data usage.

30   • Notifying MS that packet data usage is blocked.

31   • Directing MS to rectify blockage.

32   • Restoring normal operations when the User has rectified issues that triggered the hot-lining of their service.
33   Or,

34   • Terminate service if the user failed to address the issues that triggered the hot-lining of their service.

35   Hot-lining would help provide a consistent user experience for all users, irrespective of which MS application is
36   using the packet service. This includes preventing negative user experience resulting from arbitrarily blocking
37   packet data service without notifying the MS of packet data block and a mechanism to rectify the blockage. Hot-
38   lining would further provide consistency across all applications that utilize the packet data service plus it would
39   lower operating costs.

40   7.5.14 Hot-Lining Capabilities

41   The following section describes the general hot-line capabilities supported for this release:

42   a) Hot-lining is supported for both CMIP and PMIP operations both at the ASN and the CSN.

43   b) A user can be hot-lined at the start of their packet data session or mid-session as described below:

Active-Session Hot-lining:	The user starts a packet data session. In the middle of the session it is hot-lined and after the account is reconciled by some manner, the hot-lining status off the session is removed. The hot-lining is done with RADIUS Change of

	Authorization (COA) message.
New-Session Hot-lining:	The user's session is hot-lined at the time of packet data session establishment. In this scenario the RADIUS Access-Accept message is used to hot-line the session.

1   c)   Similarly, hot-lined status can be removed mid-session or at the start of a new session.

2   d)   There are two methods in which the HAAA indicates that a user is to be hot-lined:

Profile-based Hot-lining	The HAAA sends a hot-line profile identifier in the RADIUS message. The hot-line profile identifier selects a set of rules that are pre-provisioned in the Hot-line MS (HLD) that cause that user's packet data session to be redirected and/or blocked.
Rule-based Hot-lining	The HAAA sends the actual redirection-rules (HTTP or IP) and filter-rules in the RADIUS messages that cause the user's packet data session to be redirected and/or blocked.

3   e)   In order to properly account for the hot-lining state of the user, the user's hot-line state SHOULD be
4   recorded in the accounting stream.

5   The following capabilities are not covered by this specification but are described in so far that they are needed to
6   implement a complete hot-lining solution:

7   a)   The trigger(s) that cause an operator to hot-line a user is not in scope for this specification. These triggers
8   could come from a number of sources such as a billing system, fraud detection system, etc.

9   b)   The means to notify the HAAA that a user is to be hot-lined is not in scope for this specification.

10   c)   The means by which the user is notified that they have been hot-lined is not in scope of this specification.
11   Typically, the user will be notified that they have been hot-lined via their browser or other means.

12   d)   The means by which the user interacts with the system to correct the symptoms that caused them to be hot-
13   lined are not in scope for this specification.

14   e)   The means by which the system notifies the HAAA that user need not be hot-lined, that their packet data
15   session is to be returned to normal is not covered as part of this specification.

16   f)   The details of what happens when the ASN or CSN performs Profile-based Hot-lining are out of scope. It
17   is assumed that the user's traffic is blocked and that the user gets notified.

18   When the packet data session is hot-lined some IP flows will be blocked and some IP flows will be redirected. The
19   intent of the redirection is not to continue the normal operation of the flow but rather to provide information to the
20   Hot-line application so that the Hot-line application can determine how to notify the user of their hot-lined state.

21   ## 7.5.15 Hot-Lining Operation

22   Hot-lining involves the following packet data network entities (Figure 7-34):

23   •   Visited/Home CSN

24   •   ASN

25   •   HAAA

26   •   VAAA

27   The CSN and ASN contain certain MSs that implement the hot-lining rules requested by the HAAA. In this
28   document, any of these MSs that apply the hot-line rules for a user is called the Hot-lining MS (HLD). The role of
29   the VAAA with respect to Hot-lining is to act as proxy and as such will not be discussed further.
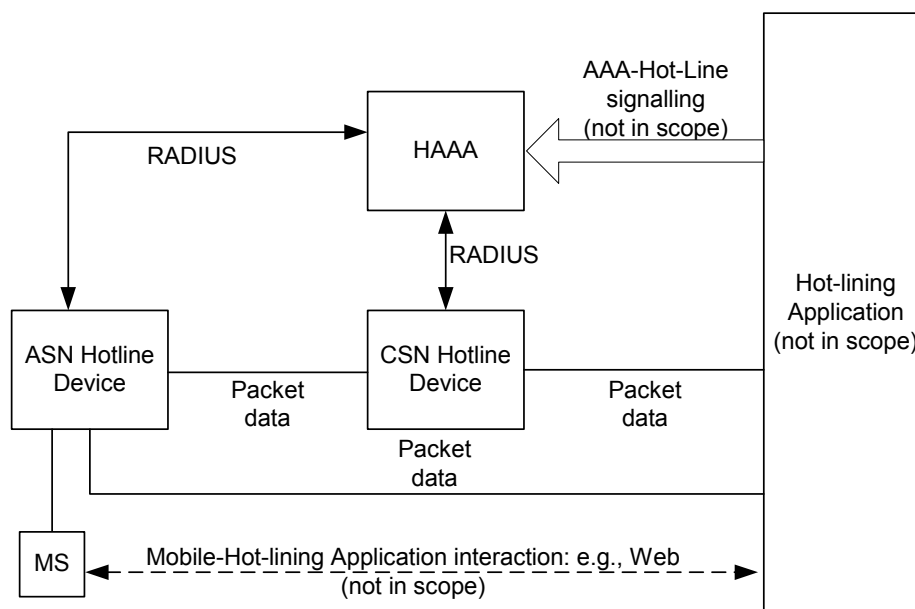
Figure 7-34 - Hot-Lining Operation

Hot-lining also involves the Hot-Line Application (HLA). The Hot-Line Application is a functional entity that performs the following roles:

- Determines when the user SHOULD be hot-lined.

- Initiates the hot-lining signaling with the HAAA.

- Hot-lined flows are redirected to the Hot-Line Application.

- Responsible for initiating notification of the hot-line status to the MS. This could be done via a delivery of an HTML page to the subscribers' browser or via some other means.

- Provides a mechanism for the user to rectify the issue that triggered hot-lining.

- Upon successful resolution of the problem, return the user back to normal operating mode.

- Upon unsuccessful resolution of the problem, terminate the user's packet data session.

The implementation of the Hot-Line Application is not within scope of this document. The interface between the Hot-Line Application and the various entities is out of scope.

The Hot-Line Application can reside over multiple servers in the network. For example, the Hot-Line Application could reside in its entirety on a web server. Or certain parts of Hot-line Application can reside on ASN or CSN as shown in Figure 7-34.

Hot-lining of a user's packet data service starts when the Hot-Line Application determines that the user's service is to be hot-lined. This determination is entirely deployment specific and can be a result of many factors. Details are not in scope for this document.

To initiate Hot-lining of the user, the Hot-Line Application will notify the HAAA that the user is to be hot-lined. The method of notification is out of scope. Upon receiving the notification from the Hot-Line Application, the HAAA records the hot-lining state against the user record.

The HAAA will determine if the user is currently in-service or out-of-service. If the user is in-service the HAAA initiates the Active-Session Hot-Lining procedure, if the user is out-of-service the HAAA initiates the New-Session Hot-Lining procedure.

Hot-lining requires that the Hot-lining MS be able to support Profile-based Hot-lining and or Rule-based Hot-lining. When support for Active Session Hot-lining is not provided the operator could utilize RADIUS Disconnect Message

1 to terminate the user's session or specify a time period after which the session would be terminated by the Hot-lining
2 MS. To participate in Hot-lining an access MS (ASN-GW/FA or HA) SHALL advertise its Hot-lining capabilities
3 using the Hot-line Capability VSA sent in a RADIUS Access-Request message. The HAAA uses the contents of the
4 Hot-line Capability VSA and other local policies to determine which access MS will be the Hot-lining MS for the
5 session.

6 The hot-line signaling for a given packet data session is communicated by the HAAA to the Hot-line MS by sending
7 the Hot-Line Profile Id VSA; or by sending HTTP/IP Redirection Rule VSAs and Filter Rule VSAs.

7.6   QoS

9 The NWG Release 1.0.0 specification defines the following procedures: (1) Pre-provisioned service flow creation,
10 modification, and deletion. (2) Initial Service Flow creation, modification and deletion. (3) QoS policy provisioning
11 between AAA and SFA. Service Flow ID management. As the scope of Release 1.0.0 is limited to pre-provisioned
12 service flows, PF-SFA interactions are not addressed in this section. Figure 7-38, 7-36, 7-37, section 7.6.5.2, are not
13 applicable for Release 1.0.0

7.6.1   Introduction and Scope

15 The scope of the QoS section is focused on the WiMAX radio link connection. QoS specific treatment in the fixed
16 part of the access and core networks are implementation specific and are not described. As a result, this release
17 makes no guarantees concerning end-to-end QoS.

18 The IEEE 802.16 specification defines a QoS framework for the air interface. This consists of the following
19 elements:

20 • Connection-oriented service

21 • Five data delivery services at the air interface, namely, UGS, RT-VR, ERT-VR, NRT-VR and BE

22 • Provisioned QoS parameters for each subscriber

23 • A policy requirement for admitting new service flow requests

24 Under the IEEE 802.16 specification, a subscription could be associated with a number of service flows
25 characterized by QoS parameters. This information is presumed to be provisioned in a subscriber management
26 system (e.g., AAA database), or a policy server. Under the static service model, the subscriber station is not allowed
27 to change the parameters of provisioned service flows or create new service flows dynamically. Under the dynamic
28 service model, an MS or BS MAY create, modify or delete service flows dynamically. In this case, a dynamic
29 service flow request (triggered using mechanisms not specified in IEEE 802.16) is evaluated against the provisioned
30 information to decide whether the request could be authorized. More precisely, the following steps are envisioned in
31 the IEEE 802.16 specification for dynamic service flow creation:

32 a) Permitted service flows and associated QoS parameters are provisioned for each subscriber via the
33   management plane.

34 b) A service flow request initiated by the MS or BS is evaluated against the provisioned information, and the
35   service flow is created if permissible.

36 c) A service flow thus created transitions to an admitted, and finally to an active state either due to BS action
37   (this is possible under both static and dynamic service models). Transition to the admitted state involves the
38   invocation of admission control in the BS and (soft) resource reservation, and transition to the active state
39   involves actual resource assignment for the service flow. The service flow can directly transit from
40   provisioned state to active state without going through admitted state.

41 d) A service flow can also transition in the reverse from an active to an admitted to a provisioned state.

42 e) A dynamically created service flow MAY also be modified or deleted.

43 This specification extends the QoS framework established in the IEEE 802.16 specification to the NWG reference
44 architecture. This specification does not address the provisioning of QoS in the access and core networks. There are
45 many possibilities for enforcing QoS in L2 and L3 networks, and operators MAY require specific L2 and L3
46 interfaces in ASN network elements to use known methods for mapping IP traffic onto these networks.

1 Please note that dynamic service flow creation triggered by the MS or the AF is not planned for this release. One of
2 the impacts is that no PF-SFA interface is defined in this release.

3

4 **7.6.2   QoS Functional Elements**

5 Based on the IEEE 802.16 specification and the Stage 2 architectural reference model, the QoS functional model
6 includes the following elements, as illustrated in Figure 7-35

7
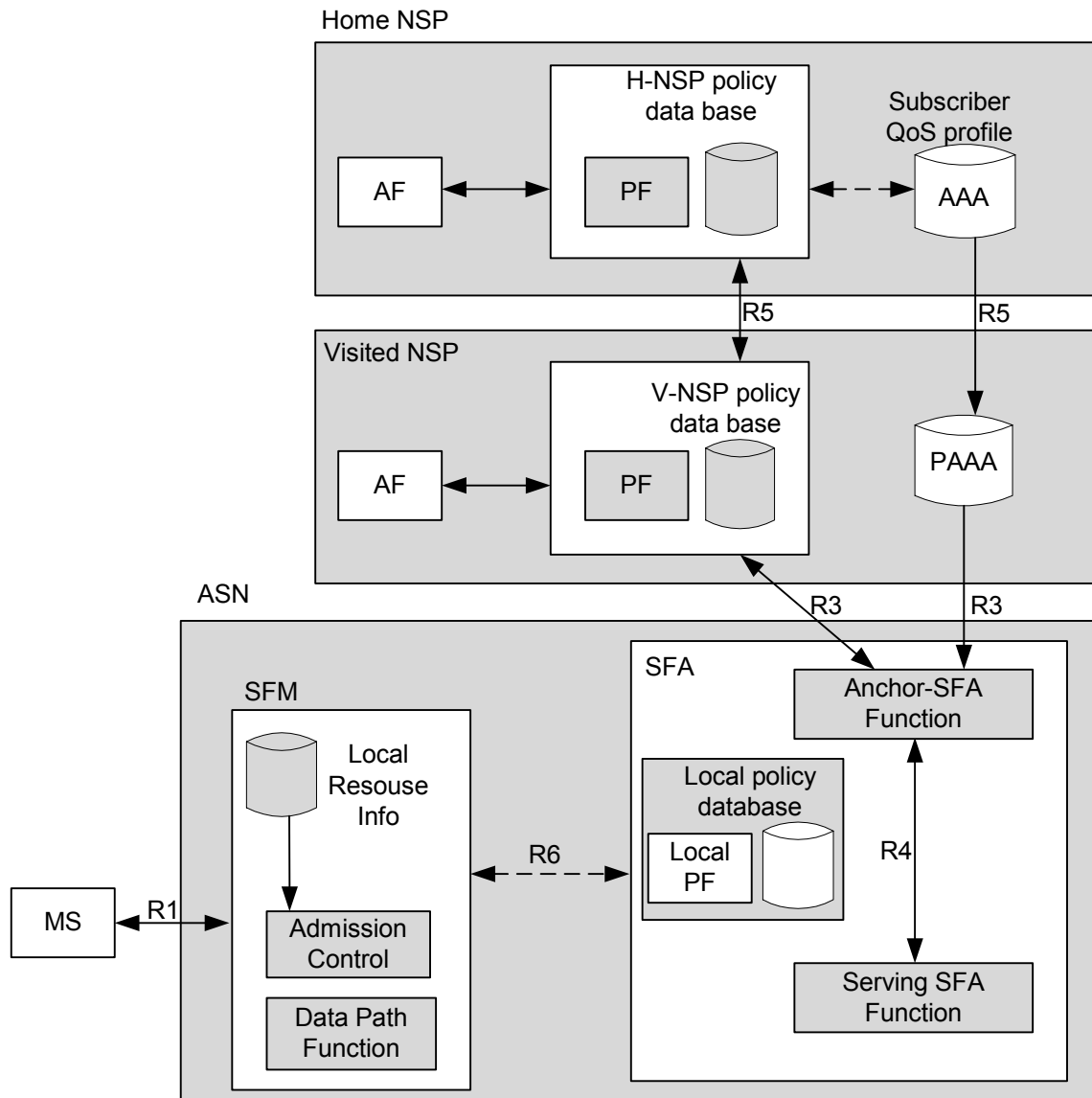
8 **Figure 7-35 - QoS Functional Elements**

9   a)   MS and ASN. The WiMAX network SHALL support ASN-initiated creation of service flows. An MS
10   MAY*,* but is not required to, have this capability (the MS must, however, respond appropriately to ASN-
11   initiated service flow actions).

12   b)   The home policy function (PF) and its associated policy database belong into the home NSP. Maintained
13   information includes H-NSP's general policy rules as well as application dependant policy rules. The AAA
14   MAY, in addition, provision the PF's database with user's QoS profile and associated policies. However,
15   interaction between PF and AAA, represented by the dotted arrow, is out of scope of this specification. The

1   PF is in charge to evaluate service requests against these policies. The MS directly communicates with the
2   AF using application layer control protocols, and the AF MAY issue WiMAX service flow triggers to the
3   PF as a result (in roaming case, the AF could be located at the H-NSP as well as at the V-NSP where the
4   corresponding PF's are triggered).

5   c)   AAA server holds the user's QoS profile and associated policy rules. This information can be used in two
6   different and exclusive ways: They can be downloaded to the SFA at network entry as part of the
7   authentication and authorization procedure. Alternatively they can be provisioned in the PF, where this
8   option is not part of WiMAX Release1.0. In the former case, the SFA evaluates the forthcoming service
9   request against the user profile. In the latter case, it is up to the home PF to do so.

10   d)   A Service Flow Management (SFM) logical entity in the ASN. The SFM entity is responsible for the
11   creation, admission, activation, modification and deletion of 802.16 service flows. It consists of an
12   Admission Control (AC) function, and associated local resource information. The AC is used to decide
13   whether a new service flow can be admitted based on existing radio and other local resource usage. The
14   precise definition of the admission control functions is left to implementations. The SFM entity is always
15   located in the BS.

16   e)   Service Flow Authorization (SFA) logical entities in the ASN. In case the user QoS profile is downloaded
17   from the AAA into the SFA at network entry phase, the SFA is responsible for evaluating any service
18   request against user QoS profile. For a given ASN/NAP there exists an *anchor* SFA assigned to each MS.
19   The anchor SFA does not change for the duration of the Device Authentication session. Optionally, there
20   MAY be one or more additional SFA entities that relay QoS related primitives and apply QoS policy for
21   that MS. The relay SFA that directly communicates with the SFM is called the *serving* SFA (when there are
22   no relays, the anchor SFA is also the serving SFA). The identity of the serving SFA, if different from the
23   anchor, SHALL be known by the anchor SFA at all times. Similarly, the serving SFA SHALL know the
24   identity of the anchor SFA. The anchor and/or serving SFA MAY also perform ASN-level policy
25   enforcement using a local policy database and an associated local policy function (LPF). The LPF can also
26   be used to enforce admission control based on available resources. The implementation of this is local to
27   the SFA and outside the scope of this specification. A serving SFA MAY be in the bearer path towards the
28   SS, but only the signalling interactions for SFA are in the scope of this document.

29   f)   A network management system (not shown) that allows administratively provisioning service flows.

30 In case the QoS profiles and associated policies are downloaded from the AAA to the SFA they SHALL be
31 expressed as depicted in the stage 3 part of the present specification. Based on service provider requirements, the
32 provisioned information MAY include user priority, which is used to enforce relative precedence in terms of access
33 to radio resources so that differentiated service categories (e.g., gold, silver, and bronze) across users can be
34 realized. For example, the user priority MAY be taken into account in situations where the service flow requests
35 across all users exceed the radio resource capacity and therefore a subset of those has to be selected for rejection.

36 The scope of the provisioned QoS profile is assumed to be specific to the MAC connections at the air interface. In
37 other words, this profile does not imply specific QoS treatment in the wireless backhaul of the access and core
38 networks. The latter would depend on the available QoS mechanisms in the fixed networks.

39   7.6.3   Triggers

40 The provisioned QoS profile serves to authorize dynamic requests initiated by the MS (not in scope of this release)
41 or the BS. These dynamic requests (creation, admission, activation as well as modification and deletion of service
42 flows) MAY result from different types of triggers including the ones described in the following subsection.

43   7.6.3.1   Pre-Provisioned Service Flows

44 A set of service flows can be created, admitted, and activated by default after a subscriber station registers with the
45 WiMAX network, before any IP data begins flowing. This is the minimum capability mandated by this
46 specification. This capability is realized by including the description of the service flows to be created and
47 optionally, user priority.

48 After successful MS registration with the WiMAX network, an anchor SFA SHALL be assigned, and its location
49 updated with the associated PF entity, unless the PF is aware of the anchor SFA through other means.

1 If the user's QoS profile has been downloaded from the AAA during the authentication procedure of the network
2 entry, the SFA initiates the creation, admission and activation of the pre-provisioned service flow.

3 If the user's QoS profile has not been downloaded, then it is the PF or the LPF that initiates the creation and
4 activation of pre-provisioned service flow (out of scope of Release 1.0.0.).

5 There MAY be circumstances under which a pre-provisioned service flow cannot be created or activated in the
6 ASN. The action to be taken in this case will be dependent on the policies within the ASN, and the agreements
7 between the NAP and the NSP. The QoS framework SHOULD allow the communication of the result of an attempt
8 to pre-provision a service flow from the ASN to the CSN.

9 ### 7.6.4 Messages

10 #### 7.6.4.1 Message types

11 The following sets of abstract messages are required to convey triggers, initiate service flow actions, request policy
12 decisions, download policy rules, and update MS location:

13   a) Resource-Reservation (RR): *RR_Req* messages could be originated by the anchor SFA. A *RR_Req* message
14   is sent from the anchor SFA to the serving SFA (if different from anchor), and finally, from the serving
15   SFA to the SFM, to request reservation of resources for one or more identified unidirectional traffic flow(s)
16   from/to the same MS. *RR_Rsp* is sent from, the SFM to the serving SFA, from the serving SFA to the
17   anchor SFA (if different) to indicate the result of a resource reservation request
18   Traffic flows listed within a *RR_Req* message could behave dependent or independent. In case of
19   dependent behaviour, the request will only be accepted if all of the listed traffic flows could be reserved
20   successfully. The receipt of the *RR_Rsp* is acknowledged by sending a RR_Ack by the anchor SFA to the
21   serving SFA (if different from anchor SFA) and finally from the serving SFA to the SFM.

22   .

23 #### 7.6.4.2 Trigger Points for Dynamic SFs (not in scope of this release)

24 From the description above, it is clear that the trigger point could be the SFM, or the PF. Specifically, the trigger
25 point is the SFM when the MS generates explicit create, admit, or activate request. Similarly, the PF could get
26 explicit or administrative triggers where in the roaming case the source could be the visited PF as well as the home
27 PF. The admission control function is located in the SFM in all cases.

28 ### 7.6.5 QoS-Related Message Flow Examples

29 In this subsection, the control flows are illustrated for service flow creation and deletion, and updating of the SFA
30 location. In all these examples, it is assumed that there is a security association between communication entities, and
31 suitable retransmission mechanisms are implemented to ensure reliable communication.

32 #### 7.6.5.1 Pre-Provisioned Service Flows

33 This procedure is initiated by the anchor SFA after the completion of MS registration.

34 If the user's QoS profile and associated policies have been downloaded from the AAA, the SFA applies them in
35 order to identify the pre-provisioned service flow that need to be created admitted and activated. The procedure is
36 shown in Figure 7-36.

37

1
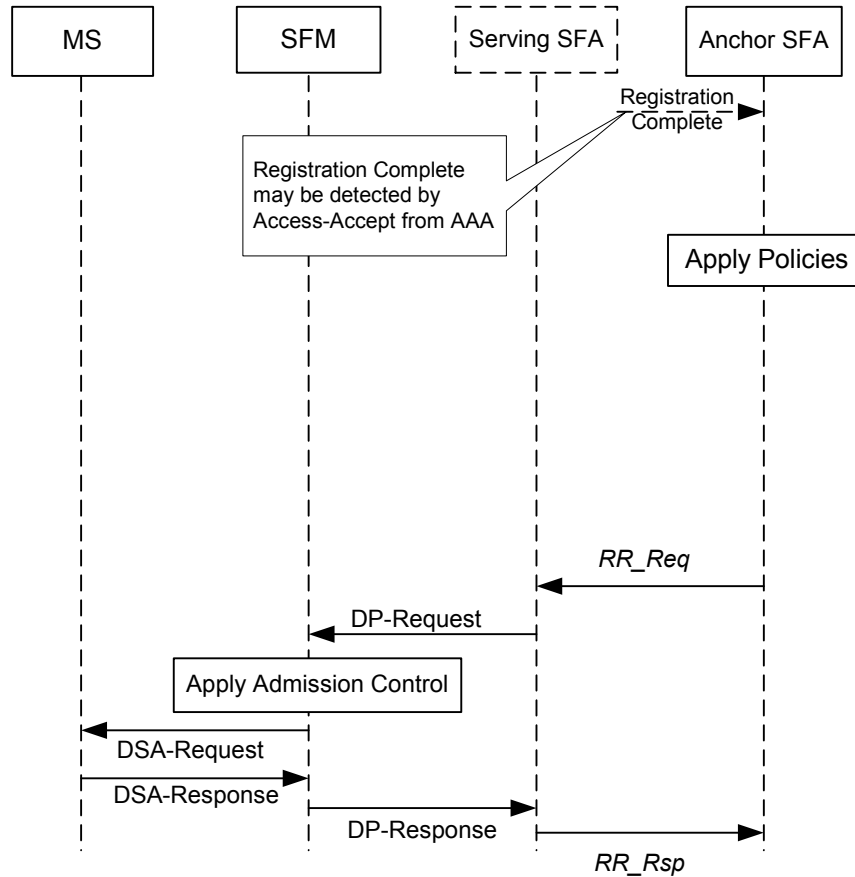
Figure 7-36 - Pre-Provisioned Service Flow Creation

3 If the user's QoS profile has not been downloaded, the PF or LPF (which, in that case, SHOULD hold it) initiates the
4 creation and activation of pre-provisioned service flows, if so configured.

5 The PF applies policies configured for the MS and determines that one or more service flows SHALL be pre-
6 provisioned. It then sends an *RR_Req* message to the anchor SFA to create and activate service flows. The rest of the
7 message sequence is as shown in Figure 7-37 (*DSA_Req* and *DSA_Rsp* messages are defined in IEEE 802.16
8 specifications).

9 In case of roaming, the PF could be split up into a home and visited PF. In this case, the visited PF will act as a relay
10 function where the visited PF could adapt the user profile data according local policies.
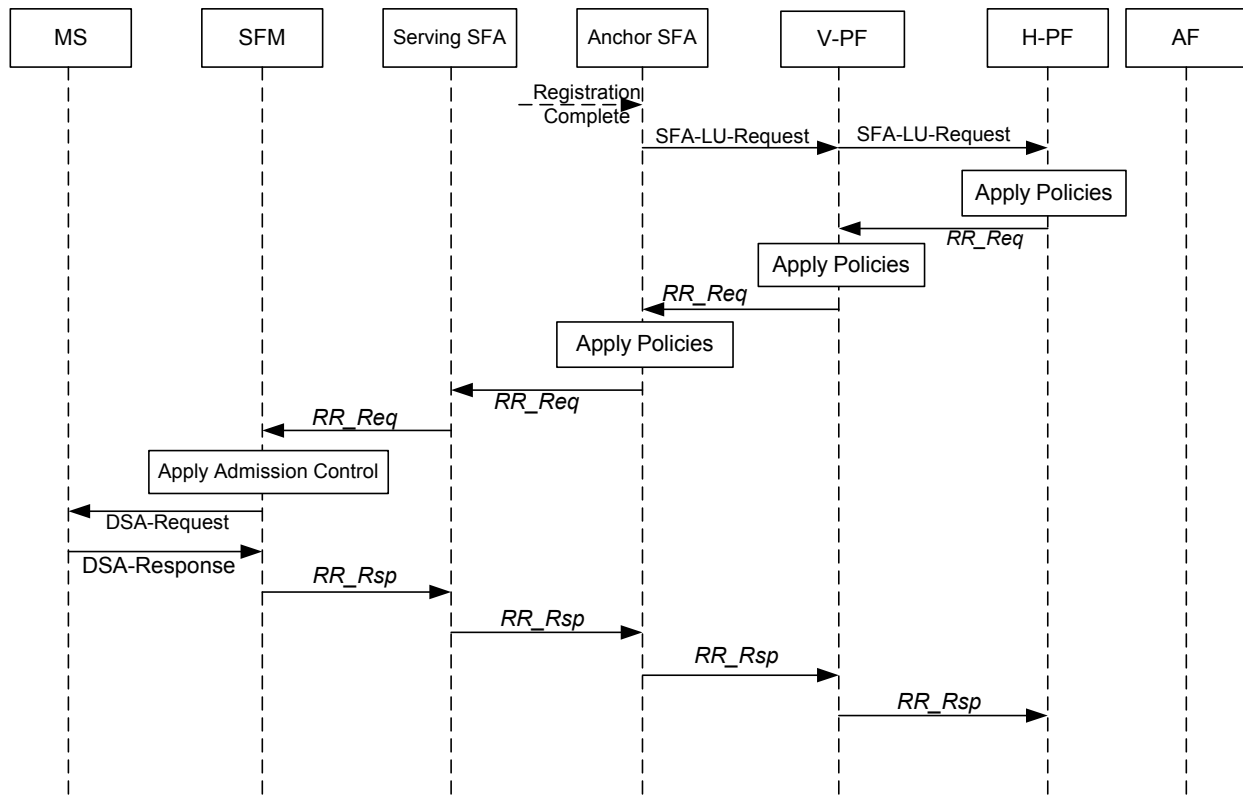
Figure 7-37 - Pre-Provisioned Service Flow Creation

7.6.5.2   AF-Triggered Service Flows

Service Flows could be triggered by an AF at the Home NSP as well as by an AF at the Visited NSP. Figure 7-38 illustrates AF-triggered service flow creation where the AF is located at the Home NSP. This is similar to the previous case, except that the service flow creation is initiated by the AF. User profile related policies are part of the policies applied by the SFA or are part of those applied by the H-PF depending whether the QoS profile and associated policies have been downloaded in the SFA or not (charts are the same in both cases).

In case of roaming, the PF could be split up into a home and visited PF. In this case, the visited PF will act as a relay function where the visited PF could adapt the user profile related policies according to the local policies.

1
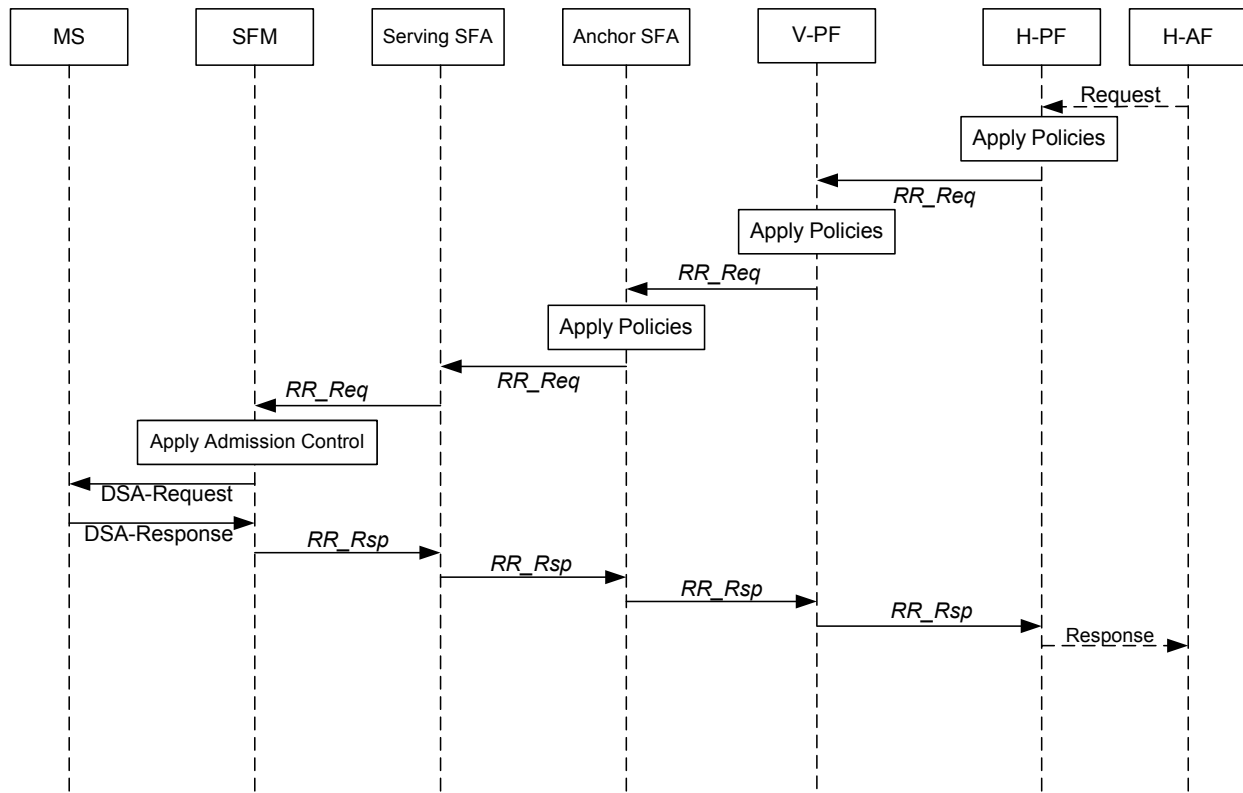
2 **Figure 7-38 - Service Flow Creation triggered by the AF at the Home NSP**

3   In case of roaming, also the AF of the visited network MAY trigger a service flow creation. In such a case, the PF of
4   the visited network SHOULD send the request to the PF of the home network to check against local policies. The
5   flow is similar to the previous case, except that the service flow creation is initiated by the Visited AF and the
6   verification of the request by the PF of the home NSP. User profile related policies are part of the policies applied by
7   the SFA or are part of those applied by the H-PF depending whether the QoS profile and associated policies have
8   been downloaded in the SFA or not (charts are the same in both cases).

Figure 7-39 - Service Flow Creation triggered by the AF at the Visited NSP

7.6.5.3   Updating SFA Location

The anchor SFA remains invariant during the Device Authentication session as the MS moves in the network. The serving SFA, however, might change. The anchor SFA SHALL keep track of the current serving SFA when network-triggered service flows are implemented. For this, the serving SFA SHALL know the identity of the anchor SFA. This information can be achieved by the mobility procedures as the anchor SFA should be collocated with the AAA-client and SHALL be addressed by the Authenticator ID. The serving SFA should be collocated with the FA / AR and SHALL be addressed by the Anchor GW ID as the Serving-SFA triggers the DP-handling on the Anchor-DP function.

7.6.6   IP Differentiated Services

Differentiated services (diffserv) is an IP layer QoS mechanism, whereby IP packets are marked with diffserv code points at the network point of entry and network elements enforce relative priority of packets based on their code points. The diffserv methodology allows network resources to be reserved for classes of traffic, rather than for individual flows, as defined in [18].

In the context of the WiMAX air link, IP diffserv mechanism can be used to enforce priorities for packets within a service flow, or to establish service flows based on diffserv classes for a given subscriber. As an example, a single pre-provisioned service flow for a subscriber can be used to carry multiple types of traffic, with relative precedence established based on diffserv code points. On the other hand, service flows MAY be established dynamically to carry different diffserv traffic classes. An example of this is the establishment of a UGS service flow dynamically to carry a voice call, where the voice traffic is marked with diffserv EF class (described in [20]).

In the first case above, the diffserv code points are used to prioritize and schedule packet transmission within a service flow. The manner in which this is done is a matter of local implementation in the BS and the SS, subject to the prioritization rules of diffserv. In the second case, the diffserv code point is used to classify packets onto separate service flows. This scenario occurs when packets entering the BS or the MS are already marked with diffserv code points by an application or some prior network entity.

1

7.7   ASN Anchored Mobility Management

7.7.1   Scope

ASN Anchored Mobility Management is defined as mobility of an MS not involving a CoA update (i.e. a MIP re-registration). Procedures described for ASN Anchored Mobility Management also apply for mobility in networks not based on MIP. There MAY be scenarios involving "ASN Anchored Mobility Management", followed by subsequent CoA update and CSN Anchored Mobility Management. In this case the initial mobility management procedures up to the CoA update trigger are described here, while the procedures starting with CoA update triggering are in the scope of Section 7.8.

7.7.2   Functional Requirements for ASN Anchored Mobility Management

The functional requirements for ASN Anchored Mobility Management are:

a) The architecture SHALL accommodate three scenarios of operation (as described in [79])

   o Nomadicity (and fixed access)

   o Portability and with Simple Mobility

   o Full Mobility

b) The architecture SHALL consider:

   o Minimizing or eliminating packet loss

   o Minimizing handoff latency

   o Maintaining packet ordering

c) The architecture SHALL comply with the security and trust architecture defined in the IEEE 802.16 specification and IETF EAP RFCs.

d) The architecture SHALL support private addresses allocated by the Home NSP or the Visited NSP, as well as NAP sharing.

e) The architecture SHOULD support Macro-Diversity Handoff (MDHO) and Fast Base Station Selection (FBSS).

f) The architecture SHOULD support MS in various states— Active, Idle, and Sleep.

g) The number of roundtrips of signalling between BS and Intra-ASN mobility anchor point to execute a HO SHALL be minimized

h) The HO control primitives and Data Path enforcement control primitives SHALL be independent of each other such that it allows separation of HO control and Data Path enforcement control.

i) The Data Path enforcement mechanism SHOULD support and be compatible with the NWG QoS architecture.

7.7.2.1   ASN Anchored Mobility Management Consideration

This section mentions ASN Anchored Mobility Management:

a) It SHOULD support multiple deployment scenarios.

b) It SHOULD be agnostic to the ASN Decomposition, and SHOULD work with any defined form of ASN construction and profiles.

c) It SHOULD accommodate HO procedures for Data Path anchoring as well as procedures for re-anchoring.

d) It SHOULD accommodate signalling and data transmission protocols within an ASN or ASNs which are within a NAP administrative domain.

e) Its protocol SHOULD accommodate multiple Data Path types with varying granularities.

1   f)   It SHOULD be independent of RRM procedures.

2   **7.7.2.2   ASN Anchored Mobility Management Functional Decomposition**

3   The ASN Anchored Mobility Management SHALL be defined by the following functions:

4   •   **Data Path (Bearer) Function**: Manages the data path setup and includes procedures for data packet
5   transmission between two functional entities

6   •   **Handoff Function**: Controls overall HO decision operation and signaling procedures related to HO

7   •   **Context Function**: Addresses the exchanges required in order to setup any state or retrieve any state in
8   network elements.

9   Each of these functions is viewed as a peer-to-peer interaction corresponding to the function.

10   **7.7.2.2.1   Generic ASN Anchored Mobility Management Functional Reference**

11
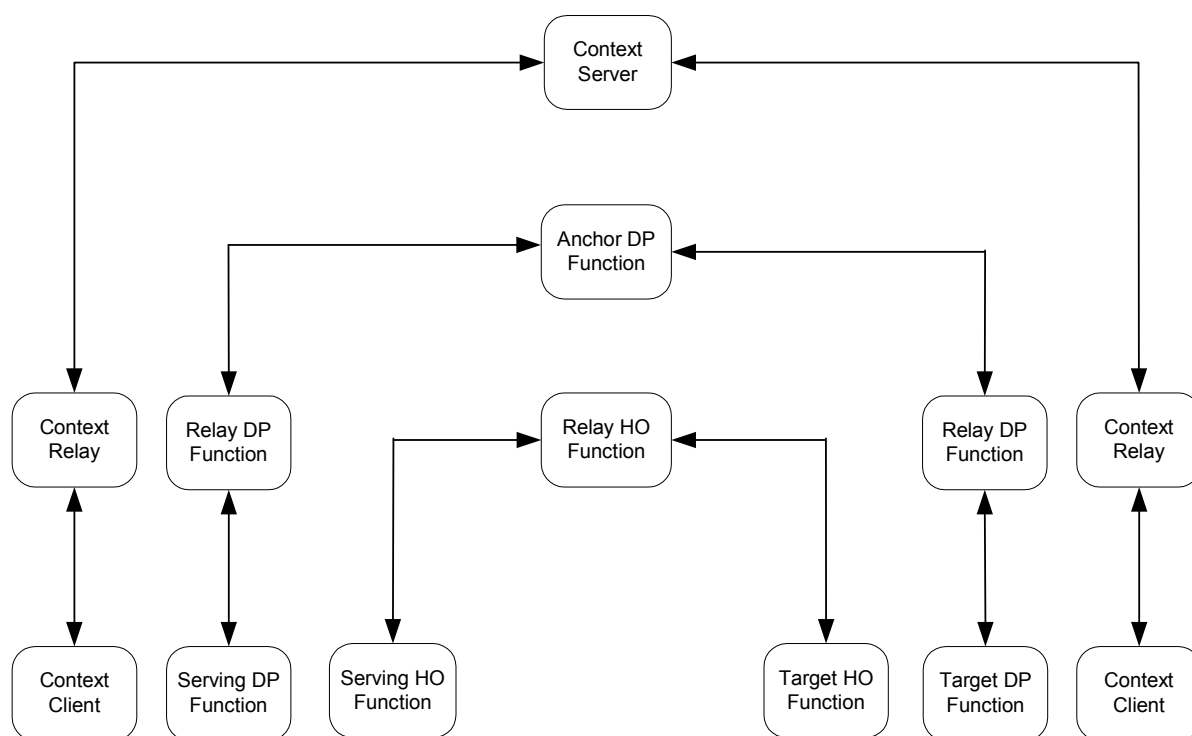
12   **Figure 7-40 - Overall Reference for ASN Mobility Functions**

13   Figure 7-40 depicts the relationship between the functional entities.

14   **7.7.2.2.2   Data Path Function**

15   The Data Path Function manages the setup of the bearer plane between two peers. This MAY include setup of any
16   tunnels and/or additional functionality that MAY be required for handling the bearer plane. The Data Path function
17   is used to setup the bearer plane between Base-Stations or between other entities such as Gateways or between
18   gateways and base-stations. Any additional requirements such as support of multicast or broadcast are also handled
19   by this function. Data Path Function shall support the use of packet sequence number. The Data Path Function is
20   also used to optionally ensure a low latency connection during handovers.

21   Each Data Path function is responsible for instantiating and managing data bearer between it and another Data Path
22   function and for selecting the payload traversing the established data bearer. There are two types of Data Path
23   Functions:

1 **Type 1:** IP or Ethernet packet forwarding with layer-2 or layer-3 transport

2 For Type 1, data path bearer is typically a generic layer 3 tunnels (e.g. IP-in-IP or GRE) a layer-2 network such
3 as Ethernet or MPLS. The payload is an IP datagram or an Ethernet packet. Additional semantics can be
4 applied to the transport header and payload to handle scenarios such as header compression, sequenced
5 delivery. The data bearer can be routed or bridged.

6 **Type 2:** forwarding with Layer-2 or layer-3 transport

7 For Type 2, data path bearer is also typically a generic layer 3 tunnels (e.g. IP-in-IP or GRE) a layer-2 network
8 such as Ethernet or MPLS. The payload is a Layer-2 data packet which is defined as an 802.16e MAC Service
9 Data Unit (SDU) or part of it appended with additional information such as CID of Target BS, Automatic
10 Retransmission Request (ARQ) parameters, etc. In Type 2, layer-2 session state (e.g., ARQ state) is anchored in
11 the Anchor Data Path Function.

12 The Data Path Function can be further classified by its roles in handover and initial entry operation as follows:

13 • **Anchor DP Function**: The DP (Data Path) Function at one end of the data path, which anchors the data
14 path associated with the MS across handovers. This Function SHALL forward the received data packet
15 toward the Serving DP function using either Type 1 or Type 2 Data Path. This Function MAY buffer the
16 data packets from the network and maintain some state information related to bearer for MS during
17 handovers.

18 • **Serving DP Function:** The DP Function at other end of a data path,, at the moment, has the association
19 with the Serving PHY/MAC function and takes charge of transmission of all messages associated with the
20 corresponding MS. This DP Function, associated with a Serving BS, communicates with the Anchor DP
21 Function through Type-1 or Type-2 Data Path, to forward/receive MS data packets.

22 • **Target (New Serving) DP Function:** The DP Function which has been
23 selected as the target for the handover. This DP Function, associated with a Target BS, communicates with
24 the Anchor DP Function to prepare a Data Path to replace the current path after the completion of the
25 handover. Upon successful handoff it will assume the role of Serving DP.

26 • **Relaying DP Function:** The DP Function which mediates information delivery between Serving, Target
27 and Anchor DP Functions.

28 ### 7.7.2.2.2.1 Data Path Considerations
29 Depending upon the level of classification used within Data Path Functions, uplink and downlink subscriber flows
30 between Data Path Functions can be forwarded using different granularities, as an aggregate or as individual flows
31 etc.

32 As shown in Figure 7-41, there are three levels of aggregations that can be used to transfer subscriber flows over a
33 Data Path.

34 • **Case 1**: Per Service Flow per subscriber i.e. finest classification granularity.
35 Each individual Service Flow of a subscriber is given a specific forwarding treatment across the ASN.

36 • **Case 2**: Per subscriber Flows belonging to a single subscriber MAY be transferred as an aggregate across
37 or within ASNs.

38 • **Case 3**: Per Functional Entities, i.e. coarsest classification granularity.
39 Flows belonging to all subscribers of a BS MAY be transferred as an aggregate across or within ASNs.

40 A Data Path is identified via the classification operation based on a set of classification criteria such as MS MAC
41 address.

42 The flow classification of each Type of Data Path Function MAY use different parameters as the classifier. That is,
43 for example, Type-2 Data Path Function SHALL use the information included in the layer-2 packets such as MS
44 MAC address, CID, etc.

45 The protocols considered in the following discussion are GRE, MPLS and 802.1Q VLANs are examples of
46 technologies that can be used to forward subscriber flows across ASN. These technologies provide for a level of

1 keying or tagging between the two end-points. Such a tag or key MAY be used in a classification decision by the
2 Data Path Function.

3
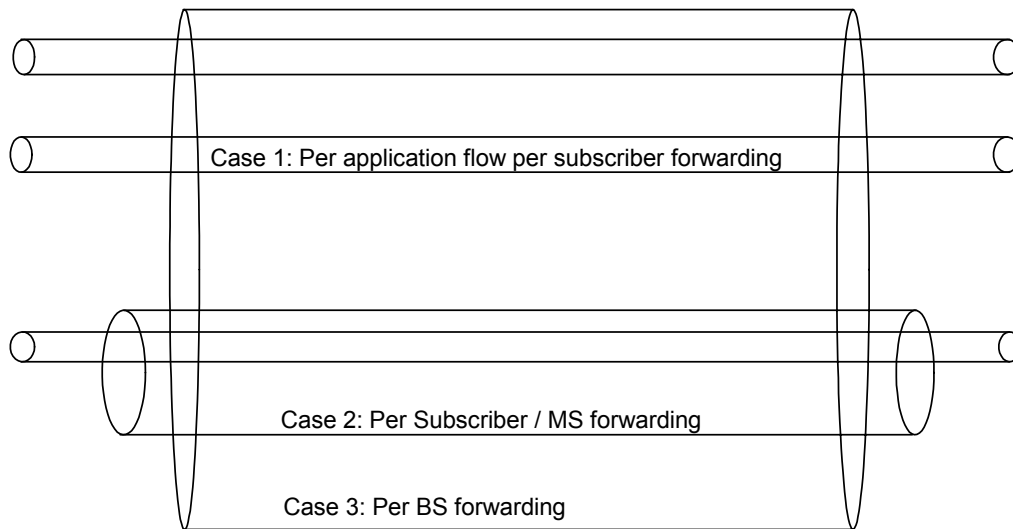
4 **Figure 7-41 - Data Path Granularity**

5 **7.7.2.2.2.2   Type-1 Bearer Operation**

6 Typically, a Type-1 Bearer is used to send IP or Ethernet packets tunneled or tagged using GRE, MPLS or 802.1Q
7 etc. between the data path functional peers. In order to satisfy several requirements such as overlapping addresses as
8 well as layer-2 transparency, a protocol which provides a level of tagging MAY be desirable for use with Type-1
9 Bearer. Such a tagging helps in identification of the MS and/or the specific QoS flows associated with the MS.

10 Type-1 Bearers are used to deliver the payload associated with a user to the respective data path peer function. A
11 Type-1 Bearer can be created per MS or per MS QoS Flow (SFID), or can be shared across multiple MS (aggregate
12 path). When a Type-1 bearer is created per MS or per MS QoS Flow, a directional key or tag MAY be associated
13 with the bearer.

14 When a key or tag is used, the bearer is classified to the appropriate MS or MS QoS Flow (SFID) based on the
15 classifier programmed for the traffic addressed to the specific MS. The traffic received from the MS MAY be
16 mapped on to the data path based on the CID.

17 GRE shall be the tunneling protocol. 'pure' IP packet will be transported by a per-flow GRE tunnel.

18 Figure 7-41 below shows an example of the classification operations for Type-1 Bearer

Data Packet (Towards MS)   Data Packet (From MS)

| Classifiers | | Classify based on CID |

| Identification of specific key and data path tunnel | | Identification of specific key and data path tunnel |

| Transmit packet with correct Data Path Tag towards MS | | Transmit packet with correct Data Path Tag from MS |

1
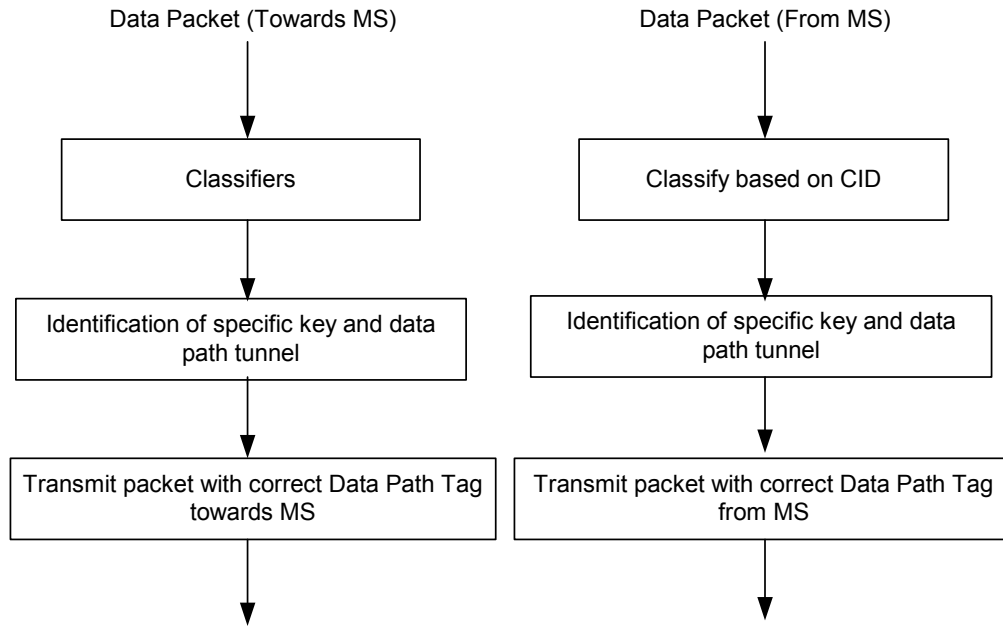
2 **Figure 7-42 - Optional Classification Operations of Type 1 Bearer**

3 **7.7.2.2.2.3   Type 2 Bearer Operation**

4 **7.7.2.2.2.3.1   Data Anchoring: Data Packet or ARQ Block**

5 When employing Type-2 Data Path Function for Intra- and Inter-ASN mobility support, layer-3 data communication
6 path from the core network to the Anchor Data Path Function SHALL NOT be changed by HO and remains the
7 same as what is before the HO. With the Type-2 Data Path Function, switching of path for layer-3 data
8 communication MAY be deferred until a session relocation request from a HO Function becomes outstanding

9 Figure 7-43 below shows a typical mobility model that employs Type-2 Data Path Function.

1
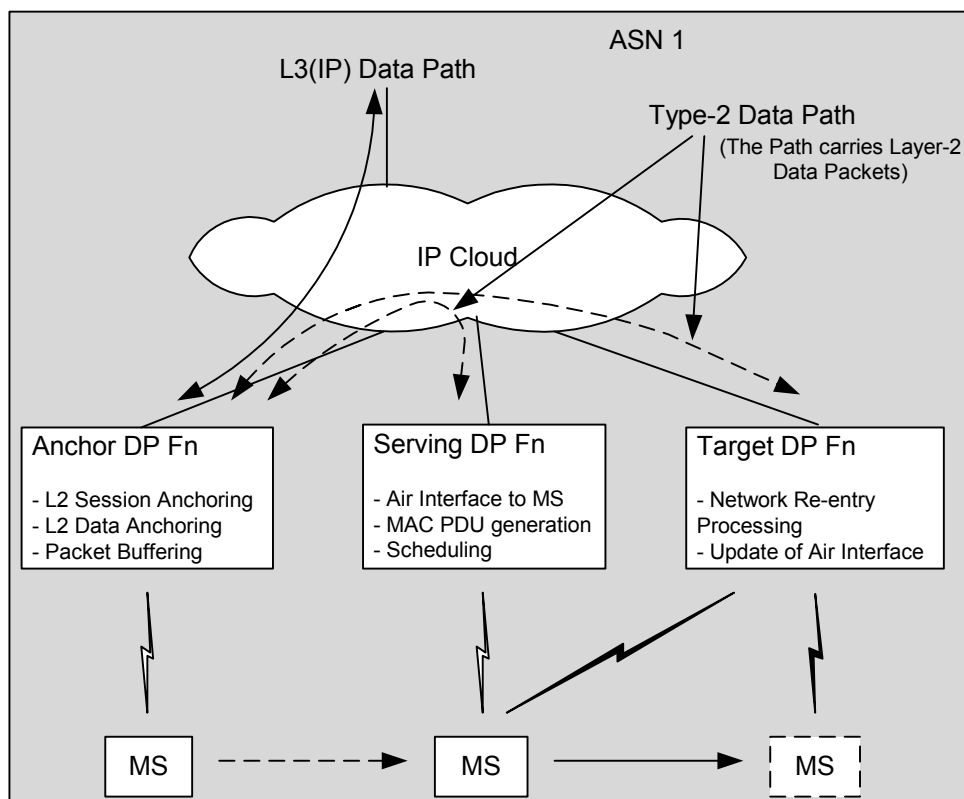
Figure 7-43 - Layer-2 Data Anchoring with Type-2 DP Function

In a mobility model that employs Type-2 Data Path Function, the Anchor Data Path Function MAY be located in the different entity from what has the Foreign Agent function. And, in this model, R3 mobility event MAY be deferred until the Anchor Handover Function triggers the R3 MM.

In Type-2, the Anchor Data Path Function SHALL anchor active Layer-2 sessions including ARQ States, and data paths used to transmit user IP packets to/from core network.

In Type-2, the Anchor Data Path Function SHALL generate Layer 2 Data Packets[7] from the received layer 3 IP packets, and then encapsulate them into the tunnel packets to forward them toward the appropriate destination Functional Entity.

In Type-2, the Serving Data Path Function, residing in the Functional Entity that has 802.16 physical associations with MS now, SHALL take charge of transmissions of all MAC messages to MS.

If MS moves to another cell and a handover is desired, the Target Data Path Function, residing in the Functional Entity that is determined as the target for the handover, SHALL perform backbone communication with Anchor Data Path Function to prepare a Type-2 Data Path to serve the pending MS handover.

7.7.2.2.2.3.2 Bearer Operation

In Type-2, bearer paths SHALL be used to deliver Layer-2 Data Packets between the Anchor Data Path Function and the Serving Data Path Function. A Layer-2 data packet is defined as an 802.16e MAC SDU or part of it which is appended with additional information such as CID of Target BS, ARQ parameters, etc.

Figure 7-42 below illustrates the overall data transmission process over a bearer of Type-2 Data Path Function.

---

[7] Here, the Layer-2 packet does not mean MAC Protocol Data Unit (PDU). It is rather MAC Service Data Unit (SDU) appended with additional information such as CID of Target BS, ARQ parameters, etc.

1
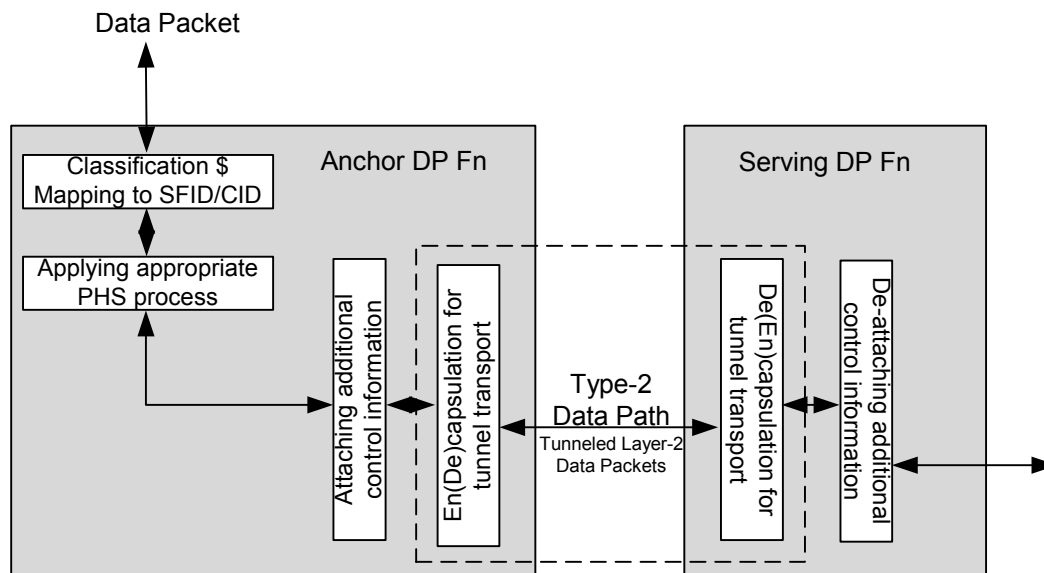
Figure 7-44 - Data Transmission over Type-2 Bearer

3 When an IP packet arrives at the Anchor Data Path Function through a data path, it SHALL be classified by the
4 Anchor Data Path Function and mapped to an appropriate IEEE 802.16 Service Flow and SFID.

5 Then the Anchor Data Path Function MAY apply an appropriate Packet Header Suppression rule per SFID to the
6 packet to make a MAC CS PDU (i.e., MAC SDU), segment the MAC SDU into an appropriate size, if required, and
7 attaches additional control information such as CID, ARQ parameters, etc. to the MAC SDU.

8 The Anchor Data Path Function then encapsulates the output into IP tunnel packet to transmit to Serving Data Path
9 Function through a Type-2 Data Path.

10 The Serving Data Path Function SHALL de-encapsulate the Layer-2 Data Packets and control information, which
11 was attached by the Anchor Data Path Function, from the packet received through the data path bearer.

12 **7.7.2.2.2.3.3 ARQ State Anchoring**

13 In Type-2 Data Path Function, ARQ state is anchored at the Anchor Data Path Function. In this case, ARQ states, as
14 well as the data packets themselves, SHALL be retained at the Anchor Data Path Function in spite of HOs, and data
15 packets need not be retransmitted over the radio link to recover the state mismatch between MS and network or the
16 state reset are caused by the handover process.

17 When the Anchor Data Path Function receives an IP packet for an ARQ-enabled connection from the network, it
18 converts the IP packet into Layer-2 Data Packet(s) or packets, as specified in Section 7.7.2.2.2.3.2. If it converts the
19 IP packet into a set of Layer-2 Data Packets, the size of each converted Layer-2 Data Packet SHALL be a multiple
20 of ARQ block size and the content of each Layer-2 Data Packets SHALL be extracted around the ARQ block size
21 boundaries. That is, only a datagram which consists of n tuples of ARQ block SHALL be transmitted through the
22 Type 2 Data Path. For the ARQ-enabled connection, the Anchor Data Path Function SHALL attach ARQ control
23 information, such as Retransmission State, Starting ARQ BSN, etc., to Layer-2 Data Packets. After all Layer-2 Data
24 Packets which are produced from the same MAC SDU, the Anchor Data Path Function SHALL store the MAC SDU
25 and the related ARQ control information locally for possible retransmission request from MS.

26 The attached information SHALL be used by the Serving Data Path Function to divide a received Layer-2 Data
27 Packet into a set of ARQ Blocks. That is, the Serving Data Path Function divides the received packet into ARQ
28 blocks with the pre-specified ARQ block size, and then assigns an ARQ BSN to each block, with starting from the
29 Starting_ARQ_BSN received from the Anchor Data Path Function through Type-2 Data Path and increasing one for
30 each block.

31 When an ARQ block(s) is requested to be retransmitted by MS or when an ARQ Ack has not been received for an
32 ARQ block(s) within the pre-specified ARQ timeout, then the Anchor Data Path Function SHALL refer to the ARQ

1 state of the connection to support retransmission according to the ARQ BSN information and update the ARQ
2 retransmission state value. The remaining packet transmission process in the Serving Data Path Function will be the
3 same excepting that it is treated as retransmission.

7.7.2.2.3   Handoff Function

5 The following types of handovers are supported by the handoff function.

6 • Mobile initiated handovers at a given serving Base-Station.

7 • Network initiated handovers.

8 • FBSS and MDHO (possibility to support MDHO SHOULD be further discussed)

9 The Handoff Function can be further classified by its roles in handover operation as follows:

10 • **Serving HO Function**: The Handover function which controls overall HO decision operation and signaling
11   procedures related to HO. It signals the Target HO Function, via zero or more Relaying HO Functions, to
12   prepare for handover, and sends the result to MS.

13 • **Relaying HO Function:** This Function relays HO related control messages between Serving and Target
14   HO Functions. A Relay HO Function MAY modify the content of HO messages and impact HO decisions.

15 • **Target HO Function:** The Handover function which has been selected as the target for the handover, or a
16   potential target for the handover.

7.7.2.2.4   Context Function

18 Due to intra-NAP mobility, there is an MS related context in the network and network related context in MS that
19 need to be either transferred and/or updated. Specifically,

20 • MS specific context in the Context Function associated with the Serving/Anchor Handoff function needs to
21   be updated.

22 • MS specific context in the Context Function associated with the Serving Handoff function that needs to be
23   transferred to the Context Function associated with the Target Handoff function. This will also require
24   some of Network specific context in MS to be updated.

25 This specification defines primitives between peer Context Functions that are used to transfer MS specific context
26 between a Context Function acting as Context-Server and a Context function acting as Context-Client.

27 The information transfer regarding a specific MS can be triggered in the following scenarios (not exhaustive).

28 • To populate the context e.g. security context corresponding to a MS at a target Base-Station.

29 • To inform the network regarding the idle mode behaviors of the MS.

30 • To inform the network of initial network entry of a specific MS.

31 The Context Function can be further classified as:

32 • **Context-Server**: The Context function is the repository of the most updated session context information
33   for MS.

34 • **Context-Client**: The Context function which is associated with the functional entity that has the 802.16
35   physical link. It retrieves session context information stored at the Context Server during the handover
36   procedure.

37 • **Relaying Context Function**: The Context Function which relays information delivery between the Context
38   Server and the Context Client.

7.7.2.2.5   SFID and CID Management

40 Per IEEE 802.16 Standard Specification, Service Flow ID (SFID) does not change upon HO across BSs belonging to
41 a single NAP, while Connection ID (CID) is defined as temporary in a particular cell coverage area. SFID SHALL
42 be set just once when a layer 2 service flow is originally established, and SHALL NOT be modified by HOs. On the

1 contrary, CID SHALL be refreshed whenever MS moves into a new cell. SFID identifies a particular Layer 2
2 session while CID specifies a particular logical radio link.

3 SFID SHALL be assigned when a new service flow is set up and SHALL be maintained as the same value at the
4 Anchor Data Path Function in spite of HOs. In normal situation, CID SHALL be assigned by the Serving BS.
5 However, in handover situation, new CID SHALL be allocated by the Target BS during HO procedures.

6 In Type 2 Data Path Function, the new CID SHALL be transmitted from the Target Handoff Function to the Serving
7 Handoff Function through the backbone communication and SHALL be mapped to the corresponding SFID at the
8 Anchor Data Path Function to relocate the Data Path. The CID SHALL never be used to identify a session at the
9 Anchor Data Path Function. It is only used as tag information for Layer-2 Data Packet (tunnel) transmission by the
10 Anchor Data Path Function. That is, when a packet is transmitted from the Anchor Data Path Function to the
11 Serving Data Path Function through Type-2 Data Path, the SFID for the packet will be translated into the
12 corresponding CID at the Serving Data Path Function and be attached as a tag to the packet. Therefore, a connection
13 is identified by SFID in the Anchor Data Path Function and by CID in the Serving Data Path Function.

7.7.2.2.6   Data Integrity Consideration During HO

15 Different class of services imposes different requirements in the quality of the traffic delivered to the MS, which is
16 measured mainly on the basis of data integrity, latency and jitter. The impact of HO in any of these parameters shall
17 be minimized. More concretely, maintaining data integrity during HO implies that the rate of packet loss,
18 duplication or reordering will not be substantially increased as a result of HO, while, at the same time, impact on
19 datapath setup latency /jitter shall be kept to a minimum

20 From QoS point of view, there are 2 types of HO: controlled and uncontrolled. A controlled HO is the one that
21 respects the following conditions:

22 • If the HO is MS initiated, the MS shall communicate to the BS a list of potential targets via msg #1
23   (MOB_MSHO-REQ)

24 • The network SHALL perform target selection based on the list of potential targets provided by the MS
25   (when MS initiated HO). The anchor DPF or serving DPF may start bi-casting or multicasting to all
26   potential targets.

27 • The network SHALL communicate to the MS the list of available targets for HO (MOB_BSHO-RSP or
28   MOB_BSHO-REQ). If the list is void, the network refuses to accept MS HO.

29 • The targets provided by the network to the MS should be a subset of the ones requested by the MS or
30   reported by the MS via MOB_SCN-REP.

31 • The MS SHALL move to one of the targets provided by the network or reject the HO

32 • The MS shall perform HO or reject by sending MOB_HO-IND

33 If any of the above conditions is not respected, the HO is considered as uncontrolled or un-predictive, and QoS is
34 not guaranteed.

35 If the MS leaves the serving BS before receiving MOB-BSHO_RSP but it succeeds to at least send MOB-BSHO-
36 IND with an indication of the target BS, this is considered uncontrolled HO. In the worst case, the MS may suddenly
37 connect in the target BS without any indication given to the target BS: this is considered as un-predictive HO

38 Several Data integrity mechanisms are provided, and the selection of Data integrity mechanism is configuration
39 issue. These mechanisms can be classified in 2 main groups: datapath setup and datapath synchronization
40 alternatives.

7.7.2.2.6.1   Data Path Setup Mechanism (Buffer Transferring vs Bi/Multicasting)

42 Datapath setup mechanisms refer mainly to R6 datapath, but when anchoring (i.e. R4 forwarding or R8 forwarding)
43 the same concepts are applicable. Data integrity mechanisms available for guaranteeing data integrity:

44 • **Buffering:** Traffic of the services for which data integrity is required is buffered in the datapath Originator
45   or in the Terminator. For one direction traffic, DP Originator is the DP function that sends data to another
46   DP   functions, and DP terminator is the DP function that receives data from another DP functions and

delivers data through the air-interface. This buffering might be done only during the HO or for simplicity it might be done within the lifetime of the session. The buffering can be conducted in Datapath Originator or terminator. And the buffering in this section is referred to the buffering mechanisms during HO, the buffering point MAY change during HO base on data integrity mechanism selection.

- **Bi/Multi-casting:** This technique consists on multicasting downstream traffic at the Originator endpoint of the datapath. Bicasting is a particular case: traffic is bicasted to the serving element and to only 1 target. There's no such concept as upstream multicast in the context of data Integrity.

These two mechanisms are not mutually exclusive, in fact bi-casting offers a better result when combined with buffering.

While multicasting requires setting up multiple data paths, this is not the case for buffering. Buffering is considered as a datapath setup mechanism since the sequencing of the datapath switch will be determined by where the buffering is done.

7.7.2.2.6.2   Data Delivery Synchronization Mechanism

In order to synchronize guarantee the data delivery in different data functions which buffered the different data paths (serving and target) used to deliver the data during HO, certain synchronization methods can be used and the data need to be synchronized. This synchronization can be achieved in 3 different ways:

(1) Using Sequence number: A sequence number is attached to each SDU in the ASN datapath. This sequence number SHALL be increased by 1 every time a SDU is forwarded in the datapath. There are two options to obtain SN of last transmitted SDU by serving datapath function during handover. One is reported by serving datapath function, and the other is through SDU SN report by MS as described in IEEE802.16e-2005. The used of the SNs is different depending on the buffering mechanism used for maintain the data integrity, example:

a) Buffering in the datapath Originator: For downlink traffic, the serving datapath function MAY report to the Originator an acknowledgement of the SDUs delivered to the MS while the HO start. So after HO, the target DP function becomes Terminator and continue receive data from the SDU next to the last one acknowledged from originator. See section 7.7.6.1.1 for detail

These acknowledgements are not meant to guarantee reliable delivery in the ASN at all times since there's no retransmission)

b) Buffering in the datapath Terminator: if multi / bi-casting is used, the serving terminator SHALL report to the originator the SN of the first SDU need to multicast to the target(s) DP terminators. When actual HO is started, the target terminator start sending the SDU next to the last one acknowledged SDU to MS. See section 7.7.6.1.2 for detail.

If no multicasting is used, After HO, the DP terminating point is changed from serving to the target DP. The SN of last Ack SDU SN is reported to the target terminator. The datapath Originator MAY report to the Serving Terminator the SN of the last SDU for the Serving Terminator to validate that there's no packet in flight in the datapath. The example procedure is demonstrated in section 7.7.6.1.3.

Data retrieving: Without creating SN for each SDU, the Anchor DPF copy/buffer the data during HO preparation, when a final target BS is identified through HO-IND, the serving BS is asked to push back all of its un-sent/un-acked packets to anchor / target DF. See section 7.7.6.1.4 for detail. For sequential delivery, the method can be used with sequence number enable.

Ack window with Sequence number disable: Data Storage buffers in Anchor DP are released by full or partial ACKs from serving BS without sequence number needed. See section 7.7.6.1.5 for detail. The method can be used with sequence number enable also.

7.7.2.2.6.3   ARQ Synchronization

There are two types Data Path in ASN and how to maintain ARQ state synchronization differs between them.

In Type-1 Data Path, ARQ states SHOULD be synchronized. The details are in 7.7.2.2.6.3.1 and 7.7.2.2.6.3.2.

In Type-2 Data Path, ARQ states MAY also be anchored at the ARQ Anchoring which resides in Anchor Data Path Function. The detail is in 7.7.2.2.2.3.3.

7.7.2.2.6.3.1 ARQ Synchronization for Downlink

For ARQ enable traffic, IEEE 802.16e MAC divides the SDUs onto logical parts called ARQ Blocks. All Blocks are of equal size except from the last one in the SDU (the Block Size is a per Connection parameter). Each Block is assigned a sequence number called Block Sequence Number – BSN. The IEEE 802.16e MAC ARQ works with BSNs.

A typical situation with the transmission buffer in the Serving MAC Function, which MAY occur prior to MS leaving, is shown on the Figure 7-45. The transmission buffer in MAC Function might be represented as sequence of Blocks labeled with BSNs. On the other hand each BSN belongs to the corresponding SDU labeled with SDU SN. The situation on the Figure 7-45 appears as follows:

- All the Blocks belonging to all the SDUs with SNs lower than Y have been transmitted and acknowledged.

- The first SDU with unacknowledged Blocks is labeled with SN = Y and the Block which corresponds to the beginning of that SDU is labeled with BSN = B. And, the Block with BSN = B has been transmitted and acknowledged.

- The Blocks labeled with BSN = B+1 and BSN = B+2 also belong to the SDU labeled with SN = Y. The Block with BSN = B+2 has been transmitted and acknowledged while the Block with BSN = B+1 has been transmitted but not acknowledged.

- The Blocks from BSN = B+3 to BSN = B+6 belong to the SDU with SN = Y+1. The Block with BSN = B+3 has been transmitted but not acknowledged. The Block with BSN = B+4 has been transmitted but and acknowledged. The Blocks with BSN = B+5 and BSN = B+6 have not been transmitted yet.

- No Block belonging to any SDU with SNs higher than Y+1 has been transmitted.

Thus in order to synchronize ARQ States between the Serving and Target MAC Functions the former SHOULD share with the later the information about the ARQ State and downlink SDU /ARQ Blocks buffers (per Service Flow)

The specific details of how the whole ARQ state is synchronized can be found in stage3.

All Blocks of all SDUs with SN greater than Y+1 have not been sent

Blocks That Have Not Been Sent
(BSNs = B+5, B+6)

B+6

B+5

B+4

B+3

SDU SN
= Y+1

Sent But Not Acknowledged
(BSNs = B+1, B+3)

B+2

B+1

SDU SN
= Y

Sent And Acknowledged Blocks
(BSNs = B, B+2, B+4)

B

All Blocks of all SDUs with SN lower than Y have been sent and acknowledged
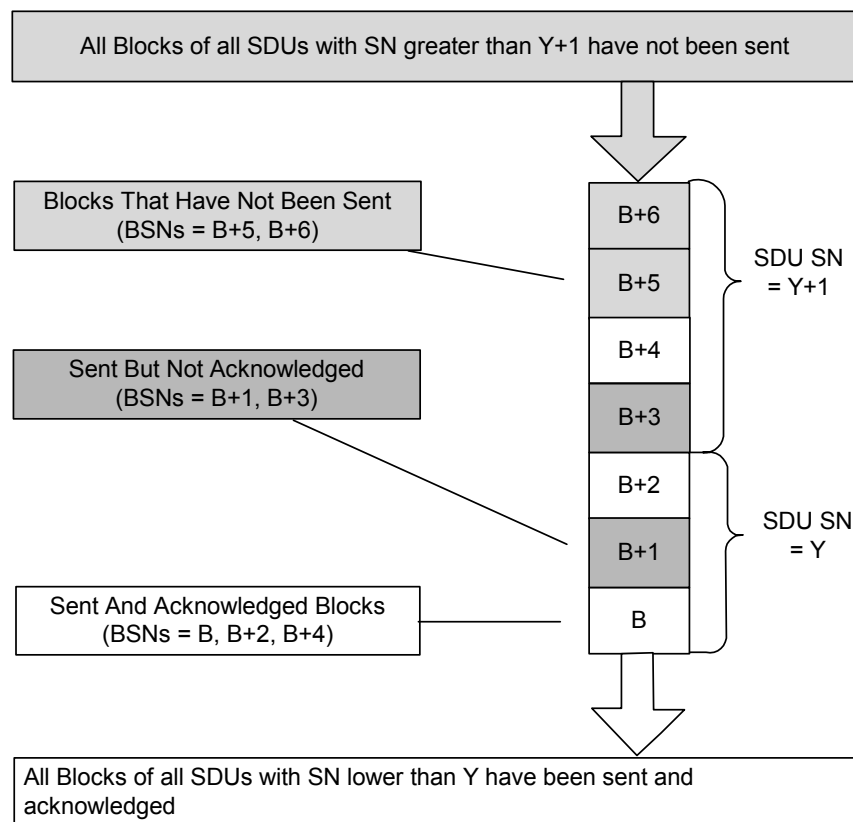
Figure 7-45 - Transmission Buffer in the Serving BS upon MS Leaving

7.7.2.2.6.3.2   ARQ Synchronization for Uplink

A typical situation with the reception buffer in the Serving MAC Function, which MAY occur prior to MS leaving, is shown on the Figure 7-46. The transmission buffer in MAC Function might be represented as sequence of Blocks labeled with BSNs. On the other hand each BSN belongs to the corresponding SDU labeled with SDU SN. The situation on the Figure 7-46 appears as follows:

- All the Blocks belonging to all the SDUs with SNs lower than Z have been received and acknowledged.

- The first SDU with unacknowledged Blocks is labeled with SN = Z and the Block which corresponds to the beginning of that SDU is labeled with BSN = b. And, the Block with BSN = B has been transmitted and acknowledged.

- The Blocks labeled with BSN = b+1 and BSN = b+2 also belong to the SDU labeled with SN = Z. The Block with BSN = b+1 has been received and acknowledged while the Block with BSN = b+2 has been received but not acknowledged.

- The Blocks from BSN = b+3 to BSN = B+6 belong to the SDU with SN = Z+1. The Block with BSN = b+3 and the Block with BSN = b+4 have been received but not acknowledged. The Block with BSN = b+5 and the Block with BSN = b+6 have not been received yet.

- No Block belonging to any SDU with SNs higher than Z+1 has been received.

Thus in order to synchronize ARQ States between the Serving and Target MAC Function the former share with the later the information about the ARQ State and uplink SDU /ARQ Blocks buffers (per Service Flow).

When the Target BS receives the synchronization information discussed above it can proceed in one of three possible ways discussed in 7.7.2.2.6.3.2.1, 7.7.2.2.6.3.2.2 and 7.7.2.2.6.3.2.3.

All Blocks of all SDUs with SN lower than Z have been received and acknowledged

Received And Acknowledged Blocks
Blocks (BSNs = b, b+2, b+4)

b
b+1
b+2

SDU SN
= Z

Received But Not Acknowledged
Blocks (BSNs = b+1, b+3)

b+3
b+4
b+5
b+6

SDU SN
= Z+1

Block That Have Not Been Received
(BSNs = b+5, b+6)

No Block of any SDU with SN greater than Z+1 has not been received

1
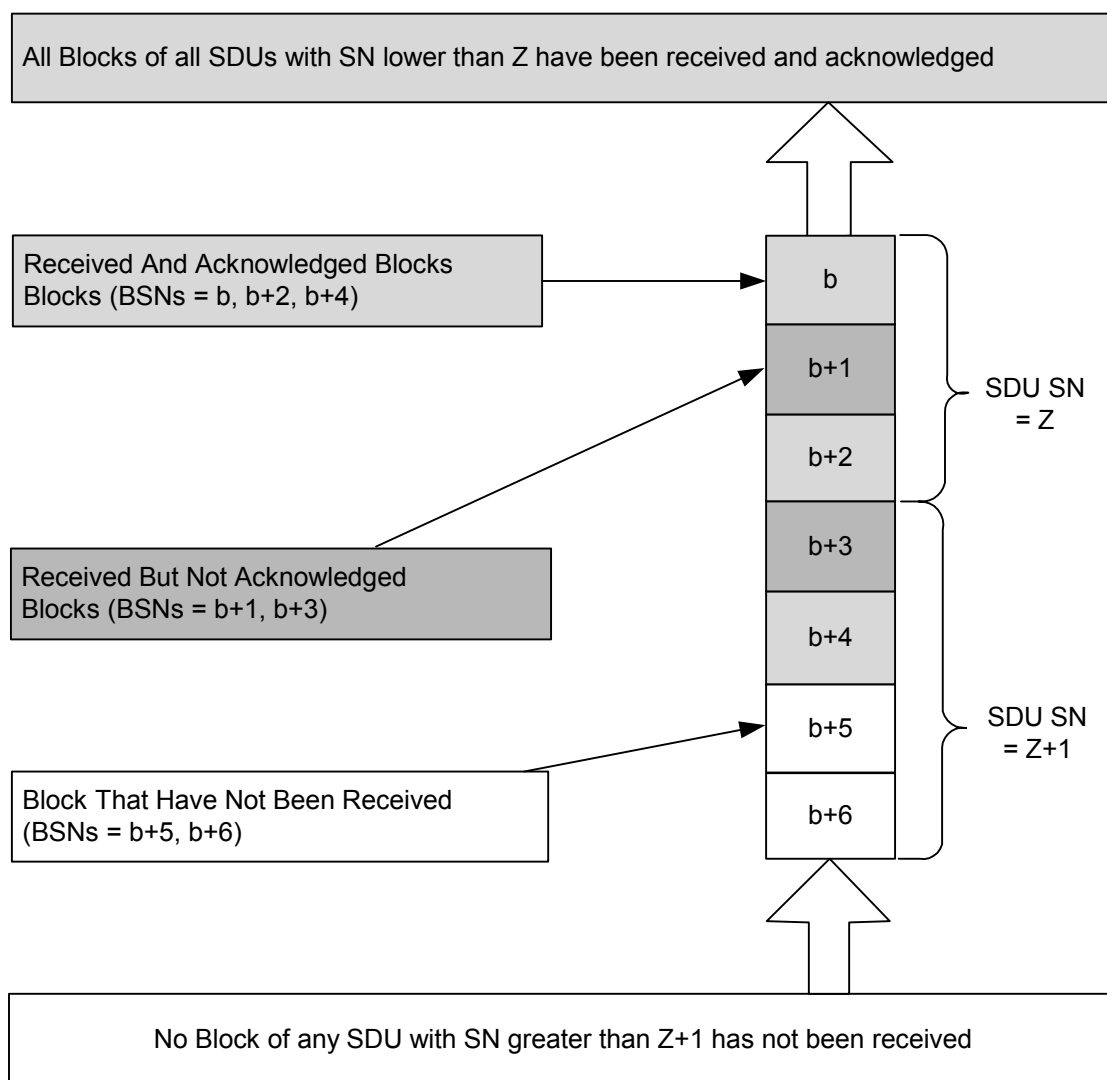
2 **Figure 7-46 - Reception Buffer in the Serving BS upon MS Leaving**

3 **7.7.2.2.6.3.2.1 MS Resending Incomplete SDUs**

4 This approach suggests that the Target MAC Function instructs the MS to reset its ARQ state and start transmitting
5 again from the first Block of the first SDU with unacknowledged Blocks. In the example shown on the Figure 7-46
6 the MS will have to resend Blocks starting with the Block with BSN=b.

7 This approach allows simple implementation but introduces some overhead over the air.

8 **7.7.2.2.6.3.2.2 Re-Assembly in the Anchor DP Function**

9 This approach suggests that the Target DP Function MAY send fragments of the SDUs to the Anchor DP Function
10 thus delegating reassembly of the SDUs to the latter.

11 This approach is more complex for implementation, but allows lower overhead over the air.

12 **7.7.2.2.6.3.2.3 Re-Assembly in the MAC Data Path Function**

13 In this approach, only complete SDUs SHALL travel between the MAC and FA function. Upon HO, the source
14 MAC function SHALL transfer any received blocks to the target MAC function along with the acknowledged/un-
15 acknowledged status. The target MAC function SHALL have the responsibility of completing acknowledgement of

1 non-acknowledged blocks as well as re-assembling received blocks into complete SDUs before transmitting uplink
2 to the FA function.

7.7.3 HO Function

7.7.3.1 HO Function Network Transaction

5 HO Function Transaction is shown in Figure 7-47
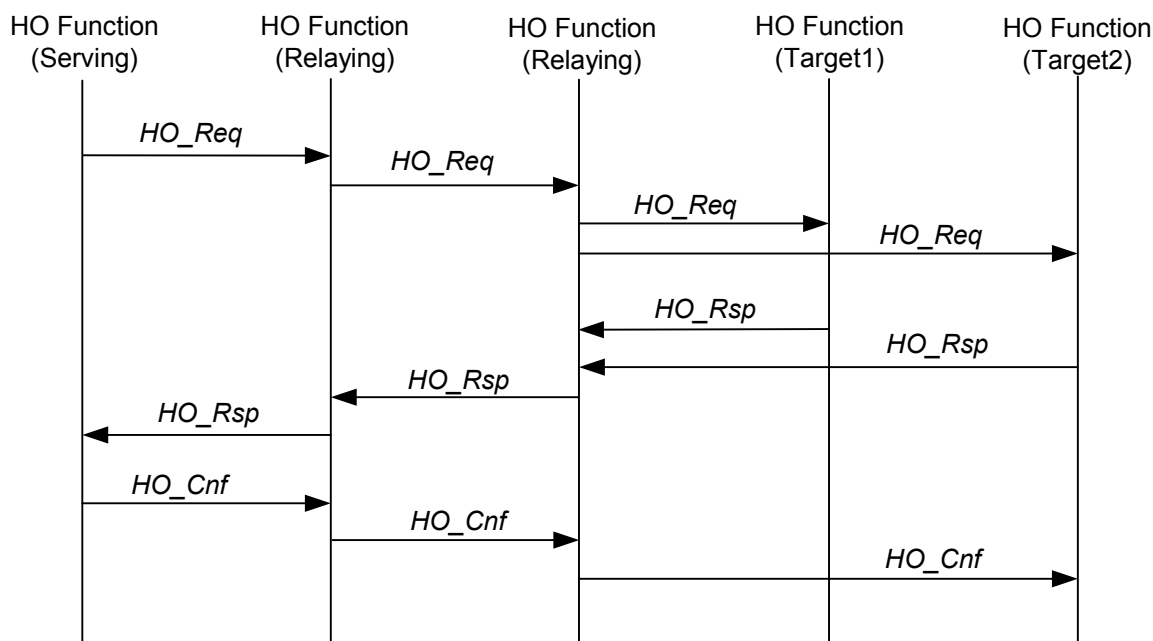
Figure 7-47 - HO Function Network Transaction

8   a) The Serving HO Function initiates an HO Network Transaction by sending *HO_Req*. There can be only one
9   Serving HO Function for any given HO Network Transaction. After receiving HO IND from MS, serving
10   HO Function the Serving HO Function confirms HO to only one Target HO Function by sending *HO_Cnf*.

11 b) The Target HO Function responds to the HO Network Transaction with *HO_Rsp*. There can be one or more
12   Target HO Functions for an HO Network Transaction.

13 c) Serving and Target HO Functions MAY communicate either directly or with assistance of one or more or
14   Relaying HO Functions. If the Serving and Target HO Functions cannot communicate directly for any
15   reason, the Relaying HO Functions take care of delivering the relevant information to the corresponding
16   Target HO Functions. A single HO Primitive (e.g. *HO_Req*) that is sent from the Serving HO Functions
17   MAY contain information relevant for several Target HO Functions. In this case several behavioral policies
18   might be applied, for example:

19   o The Relaying HO Functions sends the relevant information in separate primitives to each Target HO
20   Function via zero or more Relaying HO Function. It is the responsibility of the first Relaying HO
21   Functions directly in communication with Serving HO Function to get responses from the Target HO
22   Functions and compile the information into a single response, and it MAY but doesn't have to collect
23   all the responses. This situation is shown in the Figure 7-47 where one of the Relaying HO Functions
24   splits the original *HO_Req* into two ones and sends them to the Target HO Functions. Then the
25   Relaying HO Function, which has split the original *HO_Req*, waits for *HO_Rsp* from both Target
26   HO Functions and sends back a single *HO_Rsp*, which includes the information received from both
27   Target HO Functions.

28   o The Relaying HO Function sends the relevant information in separate primitives to each Target HO
29   Function, however it relays only the first response and drops the others.

o   The Relaying HO Function behaves like explained in the case) above, however it waits for the responses only for a limited period of time and ignores those that arrived after the time period has expired.

Other policies can be applied as well.

7.7.3.2   HO Function Primitives

7.7.3.2.1   HO_Req

This primitive is used by the Serving HO Function to inform the Target HO Functions about an incoming *HO_Req* from an MS.

HO_Req delivers at least the following Information Elements; other additional information elements MAY be included too:

- **MS ID** which identifies the MS that has requested HO.

- **The list of the Candidate Target BS Ids**.

- **MS/Session Information Content MAY** be attached to the *HO_Req* as well.

- **First requested Bi-cast SDU SN**. This IE is presented if it's lossless HO and synchronization method is sequence number method. It's the Sequence Number of the earliest SDU which hasn't been sent or Acked, and need to be delivered to target DP Function.

7.7.3.2.2   HO_Rsp

The Target HO Function responds to the Serving HO Function with the list of recommended Target BSs.

HO_Rsp is always sent in reply to the *HO_Req*. It delivers the following Information Elements at least:

- MS ID.

- The list of the Recommended Target BS IDs. The list must be a subset of the Candidate Target BS IDs list from the corresponding *HO_Req*. For each target BS in that list, service level prediction information will be included. Ideally the list would contain only one Target BS ID. If the list contains more than one Target BS ID the final selection of the Target BS is up to the MS.

- Info_Support_HO_Optimization Optional information for supporting HO Optimization.

- HO_ID. The optional HO_ID is assigned by Target BS.

- HO Action Time   The optional HO Action time is specified by Target BS for assigning Fast_Ranging_IE time, and notifies MS performing re-entry network procedure. In the case TBS decides not to support it, the value 0 is delivered in this parameter.

- First Bi-cast SDU SN. Identifies the SN of the first SDU after the data path has been changed to deal with mobility. This might be used to indicate to the serving DP which is the first SDU bi-cast to the target. Another use of this field is to indicate to the serving DP which is the last SDU sent before the data path changed. The Serving HO Function should trigger the Serving PHY/MAC function to send MOB_BSHO-RSP after the announced SDU has been delivered to the MS. If the IE is omitted the Serving PHY/MAC function may trigger sending MOB_BSHO-RSP at any moment.

7.7.3.2.3   HO Directive

This primitive is used by the related ASN functions to indicate Serving HO Function to trigger a HO procedure, such as .16e function entity, RRC or NRM Entity. HO Directive MAY deliver following Information Elements:

- **The list of the IDs of the handover MSs** which identifies the MS that has been requested HO.

- **The list of the Candidate neighbor BSs Info** This parameter is optional and indicates the HO MS's Candidate neighbor BSs information, such as neighbor BSID, signal quality, etc.

- **Trigger source** which identifies the HO source, such as RRC, NRM, or 16e function entity.

1 **7.7.3.2.4 HO Directive Response**

2 This primitive is used to reply HO Directive primitive, and indicate that the Serving HO Function have already
3 received the HO Directive primitives from the related function entity, such as RRC or NRM Entity. HO Directive
4 Response delivers following Information Elements:

5 • **Transaction ID**.

6 *7.7.3.2.5 HO_Cnf*

7 This primitive indicates the final HO action such as initiation, cancellation or handover rejection. It is sent from the
8 Serving HO Function to the Target HO Function and conveys at a minimum the following Information Elements:

9 • **Target BS ID**.

10 • **MS ID.**

11 • **Downlink ARQ Sync Info (per Service Flow):** ARQ Context that is necessary to restore communication
12 from the very point it has been interrupted. See discussion in 7.7.2.2.6.3.1.

13 • **Uplink ARQ Sync Info (per Service Flow):** ARQ Context that is necessary to restore communication
14 from the very point it has been interrupted. See discussion in 7.7.2.2.6.3.2.

15 Primitives/Content Elements for data flow integrity and sequence synchronization are TBD

16 **7.7.4 Data Path Function**

17 Data Path ID included in Request message means opposite direction's Data Path, and in Response message means
18 opposite direction's Data Path

19 **7.7.4.1 Data Path Function Network Transaction**

20 Data Path Establishment or Release is initiated from the Anchor or Target Data Path Function and terminated by the
21 Anchor or Serving Data Path Function.

22
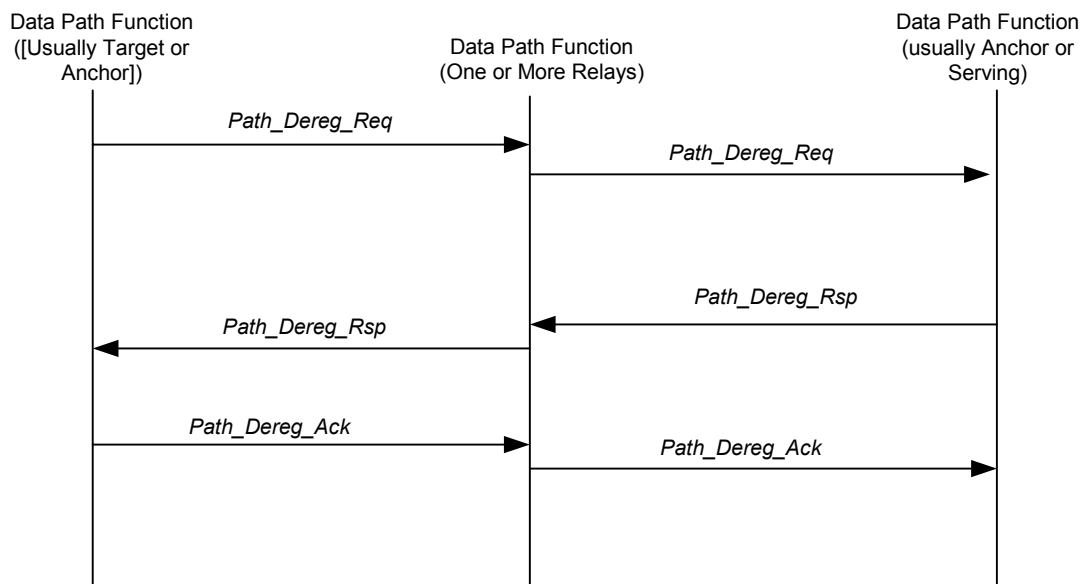
23 **Figure 7-48 - Data Path Function Network Transaction**

24 Data Path Function MAY work in three modes:

25 a) Target/Anchor Mode. The Data Path Function that initiates a Data Path Network Transaction by sending
26 *Path_Prereg_Req* and *Path_Dereg_Req*. There can be only one Data Path Function in Requesting Mode
27 for any given Data Path Network Transaction.

b) Anchor/Serving Mode. The Data Path Function that responds to the Data Path Network Transaction with *Path_Prereg_Rsp* and *Path_Dereg_Rsp*. There can be only one Terminating Data Path Function for a Data Path Network Transaction.

c) Relaying Mode. The Data Path Function that terminates incoming *Path_Prereg_Req* and *Path_Dereg_Req* messages and generates new *Path_Prereg_Req* and *Path_Dereg_Req* messages related to the same Data Path. The same way it works with *Path_Prereg_Rsp* and *Path_Dereg_Rsp* message as shown in Figure 7-48.

7.7.4.2 Data Path Function Primitives

7.7.4.2.1 Information Elements conveyed with Data Path Primitives

- **Operation ID**. Identifies the operation requested. There four operations: Path Registration, Path De-Registration and Path Pre-Registration, Path Modification.

- **Operation Reason**. Identifies the reason behind the request. The reasons MAY include but are not limited to: Handover, Initial Network Entry, Entering or Exiting Idle Mode, MS loss of carrier, etc.

- **Operation Status**. Success/Failure (used only in Responses).

- **Failure Code** (if Failure)

- **MS ID**. A unique Identifier for the MS (e.g. MAC Address). Data Paths are established to convey data that are either destined to / originated at an MS or an entity behind an MS.

- **Data Path Info.** It describes the Data Path in the direction opposite to that in which the primitive is sent. It potentially includes:

  o **Data Path Type** specifies the type of the Data Path (e.g. GRE, MPLS, VLAN, etc.)

  o **Data Path ID** specifies Data Path ID (e.g. LSP identification for MPLS, GRE Key for GRE, LAN ID for VLAN, etc.).

  o **List of Classifiers** that identify what data SHOULD be classified onto the Data Path and allows optional negotiating Data Path IDs on per microflow (IEEE 802.16 Connection) basis.

  o **Multicast Info**. Specifies relation of the Data Path to the IP Multicast Group.

  o **Endpoint Identifier.** Specifies the addressable subscriber-side endpoint for which the Data Path is being established or maintained.

  o **Data Integrity operation flag:** Indication if data integrity is required for this data path.

- **Data Integrity Info:** It describes the data integrity scheme used during the HO. It potentially includes the following IEs:

  o **Data Integrity Buffering Method**: Indication of buffering mechanisms: Anchor Buffering in the Originator, Buffering in the Terminator, or Bi/Multi-Casting.

  o **Data delivery synchronization method**: Indication of buffered data delivery synchronization mechanism: sequence number enable, data retrieve with sequence number disable and Ack window with sequence number disable.

  o **Data integrity operation ID:** Specifies the operation which related to particular data integrity mechanisms. There are 3 operations: DP_SYNC-REQ, DP_SYNC-ACK and DP_SYNC-RSP.

  o **First requested Bi-cast SDU SN**: The Sequence Number of the earliest SDU which hasn't been sent or Acked and need to be delivered to target DP Function.

  o **First Bi-cast SDU SN:** Identifies the SN of the first SDU after the datapath has been changed to deal with mobility. This might be used to indicate to the serving DP which is the first SDU bi-cast to the target. Another use of this field is to indicate to the serving DP which is the last SDU sent before the data path changed.

- o **Last Packet Indication.** The LPI can be used in the target as an indication that all traffic from the serving has been "synchronized" and normal scheduling of traffic arriving from anchor can be resumed

- o **List of lossless session IDs:** Since not all sessions for the MS requires lossless handoff, the list of the lossless session IDs SHALL be included. The session ID is the identifier which can identify a unique service session in the anchor ASN DF.

- o **Data retrieve info:** contains the information for data retrieving, such as number of SDU need to be retrieved.

7.7.4.2.2 Path_Reg_Req

Path_Reg_Req is used to handle a registration of a MS, or a MS Flow in the Data Path Function which receives the *Path_Reg_Req*. The registration request is also used for registering the membership of multicast groups corresponding to the MS. It contains the following information:

- • **Operation ID**. Set to Path Registration.

- • **Operation Reason**. One of the reasons mentioned in 7.7.4.2.1.

- • **MS ID**. As described in 7.7.4.2.1.

- • **Data Path Info.** Describes Data Path for the direction from the Data Path Function that receives *Path_Reg_Req* to the Data Path Function that sends *Path_Reg_Req*. The content of Data Path info is discussed in 7.7.4.2.1.

- • **Anchor DP redirection Indication.** It is used to indicate Anchor DP function relocation when the originating DP function decide to relocate Anchor DP function directly.

- • **Data Integrity Info. As describe in** 7.7.4.2.1. The data integrity Info IEs MAY be includes in this primitives are:

  - o **Data Integrity Buffering Method**: Indication of buffering mechanisms: Anchor Buffering in the Originator, Buffering in the Terminator or, Bi/Multi-Casting.

  - o **Data synchronization method**: Indication of buffered data delivery synchronization mechanism: sequence number enable, data retrieve with sequence number disable and Ack window with sequence number disable.

  - o **First requested Bi-cast SDU SN**. As described in 7.7.4.2.1.

  - o **Data integrity operation ID:** The three following data integrity operation ID can be carried by Path Registration response: DP_SYNC-REQ:

    - – DP_SYNC-REQ: It indicates that the indicated sessions SHOULD be lossless handoff. It is sent to the serving ASN DF (from the anchor target DF to the serving ASN DF when there's direct communication between them otherwise is sent from Anchor DF) to establish the a data path for retrieving data synchronization. The primitive conveys at a minimum the following Information Elements.

    - – The MS ID and List of lossless session IDs are needed while this operation ID is presented.

For supporting IP multicasts, the primitive is used to indicate that a specific MS is part of the multicast group.

Upon receipt of *Path_Reg_Req*, the Data Path Function which receives *Path_Reg_Req* MAY begin recognizing packets destined for the MS and forward them (using the selected Data Path enforcement mechanism) to the Data Path Function which sends the *Path_Reg_Req* (possibly via Relaying Data Path Functions).

7.7.4.2.3 Path_Prereg_Req

Path_Prereg_Req is used during handovers in order to establish a new Data Path for an MS without destroying the old one. The information the primitive delivers is identical to that of *Path_Reg_Req*, except from the Operation ID which SHALL be set to Path Pre-Registration.

1 The Data Path Function that receives *Path_Prereg_Req* expects Registration Request to follow in order to complete
2 new DP establishment.

7.7.4.2.4   Path_Dereg_Req

4 *Path_Dereg_Req* is used to cancel an existing Data Paths for an MS.

5 *Path_Dereg_Req* contains the following information:

6 • **Operation ID**. Set to Path De-Registration.

7 • **Operation Reason**. One of the reasons mentioned in 7.7.4.2.1.

8 • **MS ID**. As described in 7.7.4.2.1.

9 • **Data Path Info.** Describes Data Path for the direction from the Data Path Function that receives
10 *Path_Reg_Req* to the Data Path Function that sends *Path_Reg_Req*. The content of Data Path info is
11 discussed in 7.7.4.2.1. Data Path Info might be omitted in the *Path_Dereg_Req*. It means that all the Data
12 Paths for the specified MS SHOULD be cancelled.

7.7.4.2.5   Path_Modification_Req

14 *Path_Modification_Req* is used to modify attributes of an existing Data Path. It contains the following information:

15 • **Operation ID**. Set to Path Modification.

16 • **Operation Reason**. One of the reasons mentioned in 7.7.4.2.1.

17 • **MS ID**. As described in 7.7.4.2.1.

18 • **Data Path Info.** Describes Data Path for the direction from the Terminating Data Path Function to the
19 Originating one. The content of Data Path info is discussed in 7.7.4.2.1.

20 For supporting IP multicasts, the primitive is used to indicate that a specific MS is part of the multicast group. Upon
21 receipt of *Path_Modification_Req*, the Terminating Data Path Function begins modify QoS Info, Data Path Info
22 indicated in the message to the Originating Data Path Function (possibly via Relaying Data Path Functions).

7.7.4.2.6   Path_Reg_Rsp

24 *Path_Req_Rsp* is sent in reply to the *Path_Reg_Req*. It contains the following information:

25 • **Operation ID**. Set to Path Registration.

26 • **Operation Status**. Success/Failure.

27 • **MS ID**. As described in 7.7.4.2.1.

28 • **Data Path Info**. It describes the Data Path in the direction from the Data Path Function that sends
29 *Path_Reg_Req* to the Data Path Function that receives *Path_Reg_Req*. The content of Data Path info is
30 discussed in 7.7.4.2.1.

31 • **Anchor DP redirection Indication.** It is used to indicate Anchor DP function relocation when the
32 terminating DP function decide to relocate Anchor DP function.

33 • **Data Integrity Info. As describe in** 7.7.4.2.1. The data integrity Info IEs MAY be includes in this
34 primitives are:

35 ○ **Data integrity operation ID:** The following data integrity operation ID can be carried by Path
36 Registration response: DP_SYNC-RSP:

37 – DP_SYNC_RSP: indicates that the Data Path Sync Request message is received and the
38 corresponding produce is being processed. The received downlink packets for the MS in the
39 serving DF, as well as the un-transmitted downlink packets for the MS in the BS, will be
40 returned to. If the requester was the Anchor DF, where all downlink traffic for this MS is
41 buffered in the anchor DF till the final target DF is identified and the data path is established

1 between Anchor DF and target DF. It is sent from the serving DF to the anchor DF requester.
2 The MS ID is need while this operation ID is presented.

3 Upon receipt of Path Registration Response, the Data Path Function that sends *Path_Reg_Req* MAY begins
4 recognizing packets originated from MS and forwards them (using the selected Data Path enforcement mechanism)
5 to the Data Path Function that receives *Path_Reg_Req* MAY (possibly via Relaying Data Path Functions).

6 ### 7.7.4.2.7 Path_Prereg_Rsp

7 *Path_Prereg_Rsp* is sent in reply to the *Path_Prereg_Req*.

8 It contains the following information:

9 - **Operation ID**. Set to Path Pre-Registration.

10 - **Operation Status**. Success/Failure.

11 - **MS ID**. As described in 7.7.4.2.1.

12 - **Data Path Info**. It describes the Data Path in the direction from the Originating Data Path Function to the
13 Terminating one). The content of Data Path info is discussed in 7.7.4.2.1.

14 - **Data Integrity Info. As describe in** 7.7.4.2.1. The data integrity Info IEs MAY be includes in this
15 primitives are:

16 - o **Data Integrity Buffering Method**: Indication of buffering mechanisms: Anchor Buffering in the
17 Originator, Buffering in the Terminator or, Bi/Multi-Casting.

18 - o **Data synchronization method**: Indication of buffered data delivery synchronization mechanism:
19 sequence number enable, data retrieve with sequence number disable and Ack window with sequence
20 number disable.

21 - o **First requested Bi-cast SDU SN** As described in 7.7.4.2.1.

22 ### 7.7.4.2.8 Path_Dereg_Rsp

23 *Path_Dereg_Rsp* is sent in reply to *Path_Dereg_Req*. It contains the following information:

24 - **Operation ID**. Set to Path De-Registration.

25 - **Operation Status**. Success/Failure.

26 - **MS ID**. As described in 7.7.4.2.1.

27 ### 7.7.4.2.9 Path_Modification_Req

28 *Path_Modification_Req* is sent in reply to the Path_*Modification_Req*. It contains the following information:

29 - **Operation ID**. Set to Path Modification.

30 - **Operation Status**. Success/Failure.

31 - **MS ID**. As described in 7.7.4.2.1.

32 - **Data Path Info**. It describes the Data Path in the direction from the Originating Data Path Function to the
33 Terminating one). The content of Data Path info is discussed in 7.7.4.2.1.

34 Upon receipt of *Path_Reg_Rsp*, the Originating Data Path Function begins recognizing packets destined for the MS
35 and forwards them (using the selected Data Path enforcement mechanism) to the Terminating Data Path Function
36 (possibly via Relaying Data Path Functions).

37 ### 7.7.4.2.10 Path_Reg_Ack

38 *Path_Reg_Ack* acknowledges the completion of a Path Registration Transaction. It contains the following
39 information:

40 - **Operation ID**. Set to Path Registration.

1   • **MS ID**. As described in 7.7.4.2.1.

2   • **Data Integrity Info. As describe in** 7.7.4.2.1. The data integrity Info IEs MAY be includes in this
3   primitives are:

4   o **Data integrity operation ID:** The following data integrity operation ID can be carried by
5   *Path_Reg_Ack*: DP_SYNC-ACK:

6   – DP_SYNC-ACK: It indicates that the completion of the retrieve data path establishment. It is
7   sent to the serving DF from the target DF it there's direct communication among them,
8   otherwise it is sent from the anchor DF. The MS ID and Data retrieve IE are need while this
9   operation ID is presented.

10 Upon receipt of *Path_Reg_Ack* which indicates the completion of final data path registration transaction, the Data
11 Path Function which receives *Path_Reg_Req* MAY begin recognizing packets destined for the MS and forwards
12 them (using the selected Data Path enforcement mechanism) to the Data Path Function which sends the
13 *Path_Reg_Req* (possibly via Relaying Data Path Functions) if this action hasn't been started.

7.7.4.2.11 Path_Dereg_Ack

15 *Path_Dereg_Ack* acknowledges the completion of a Path De-Registration Transaction. It contains the following
16 information:

17   • **Operation ID**. Set to Path De-Registration.

18   • **MS ID**. As described in 7.7.4.2.1.

7.7.4.2.12 Path_Prereg_Ack

20 *Path_Prereg_Ack* acknowledges the completion of a Path Pre-Registration Transaction. It contains the following
21 information:

22   • **Operation ID**. Set to Pre-Registration.

23   • **MS ID**. As described in 7.7.4.2.1.

7.7.4.2.13 Path_Modification_Ack

25 *Path_Modification_Ack* acknowledges the completion of a Path Modification Transaction. It contains the following
26 information:

27   • **Operation ID**. Set to Path Modification.

28   • **MS ID**. As described in 7.7.4.2.1.

7.7.4.2.14 Data-ACK

30 If the delivery scheme of data integrity uses Ack window, This primitive is sent from serving Data function to
31 Anchor DF to indicate the sequence number of the SDU which has been Acked.

7.7.4.3 Simultaneous Data Path Establishment by Both Peers

33

34 The peer Data Path Functions may instigate Data Path Establishment for the same MS simultaneously as shown on
35 the Figure 7-49.

36

Data Path
Function 1

Data Path
Function 2

Path_Prereg_Req
[DP Info = X]

Path_Prereg_Req
[DP Info = Y]

Path_Prereg_Rsp
[DP Info = X]

Path_Prereg_Rsp
[DP Info = Y]

Path_Prereg_Ack

Path_Prereg_Ack

1
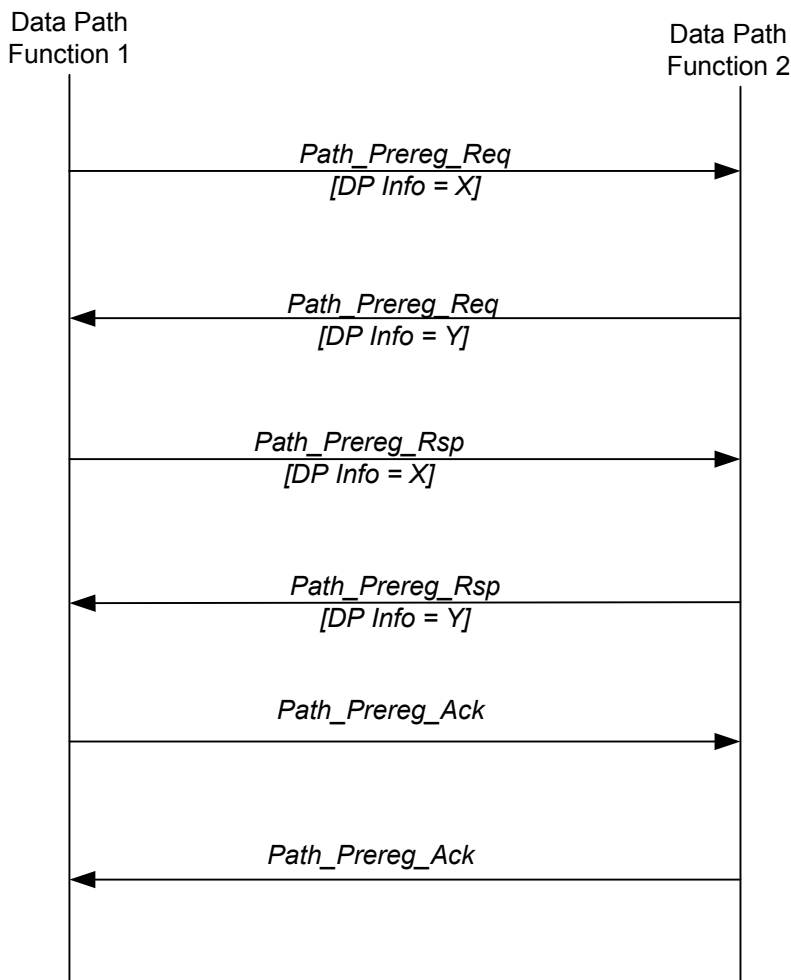
2 **Figure 7-49 - Both Peers Establish Data Path Simultaneously**

3 When such condition take place both peers follow the following rule:

4

5 ▪ Both *Path_Prereg_Req* and *Path_Prereg_Rsp* that are sent in the same direction and refer to the same Data
6 Path should convey the same Data Path Info.
7

8 This rule utilizes the fact that, in accordance with the definition in 7.7.4.2.1, each peer independently specifies Data
9 Path Info for its respective reception direction and this is why such a collision does not really create a race condition.

10

11 In the situation shown on the Figure 7-49, it is enough if only one of the Data Path Establishment transactions
12 succeeds.

13 **7.7.4.4   Target Centric Pre-Registration and Registration during HO**

14 Target Centric refers to an approach according to which the Target DP Function instigates both Pre-Registration and
15 Registration Transactions during HO.

16 Path Pre-Registration Transaction (*Path_Prereg_Req* and *Path_Prereg_Rsp* and *Path_Prereg_Ack*) is invoked in
17 order to establish a Data Path for an MS between the Anchor DP Function and Target DP Function without
18 destroying the Data Path between the Anchor DP Function and Serving DP Function for the same MS.

1 It is allowed to pre-register simultaneous Data Paths between the same Anchor DP Function and multiple Target DP
2 Functions.

3 Pre-establishing Data Paths between the Anchor DP Function and Target DP Functions does not affect forwarding
4 data along the Data Path between the Anchor DP Function and Serving DP Function.

5 By default when a Data Path between the Anchor DP Function and a Target DP Function is established the data are
6 not forwarded along this Data Path. However other traffic handling options might be negotiated during Path. The
7 data may be forwarded along the pre-established Data Path between the Anchor DP Function and a Target DP
8 Function simultaneously with data forwarding along the Data Path between the Anchor DP Function and the Serving
9 DP Function. Alternatively the data may be buffered for the pre-established Data Path between the Anchor DP
10 Function and a Target DP Function in order to be delivered later upon request. These traffic delivery options are part
11 of the Data Integrity framework.

12 Path Registration Transaction is invoked when a new Serving Data Path between Anchor DP Function and the DP
13 Function which is a Target DP Function upon beginning of the Transaction and which becomes the new Serving DP
14 Function upon completion of the Transaction. It should not happen earlier than MS arrives to the Target BS/ASN
15 (with which the Target DP Function is associated)

16 At the moment the Anchor DP Function receives *Path_Reg_Req* from a Target DP Function (which is about to
17 become the new Serving DP Function) it should stop forwarding data along the Data Path to the old Serving DP
18 Function. Shortly after that the Anchor DP Function shall De-Register the Data Path to the old Serving DP Function.
19 The Serving DP Function may also instigate Path De-Registration if it learns from HO Function that the MS has
20 completed HO in the Target BS/ASN.

21 Path Pre-Registration Transaction may be executed prior to Path Registration Transaction (for the same data path). If
22 Path Pre-Registration Transaction has been completed prior to starting Path Registration Transaction then the
23 purpose of the Path Registration Transaction is only to trigger "data path switch". In this case *Path_Reg_Req* and
24 *Path_Reg_Rsp* do not have to convey any Informational Elements except from MS ID and, optionally, Data Path ID.
25 The rest of the parameters that are relevant to the data path have to be exchanged during the preceding Path Pre-
26 Registration Transaction. Furthermore in this case Path Registration Transaction is completed with two-way
27 handshake – *Path_Reg_Req* and *Path_Reg_Rsp* exchange without *Path_Reg_Ack*.

28 As it has been mentioned above, by default the Anchor DP Function does not forward data to a Target DP Function
29 along the corresponding pre-established Data Path (unless a different traffic forwarding option was negotiated upon
30 the Data Path Pre-Registration) In this case the Anchor DP Function may start forwarding data to the Target DP
31 Function immediately after it receives *Path_Reg_Req*. The Target DP Function may start forwarding data to the
32 Anchor DP Function immediately after it receives *Path_Reg_Rsp*.

33 Figure 7-50 shows the typical sequence for Pre-Registration, Registration and De-Registration Transactions as they
34 likely to occur during HO.
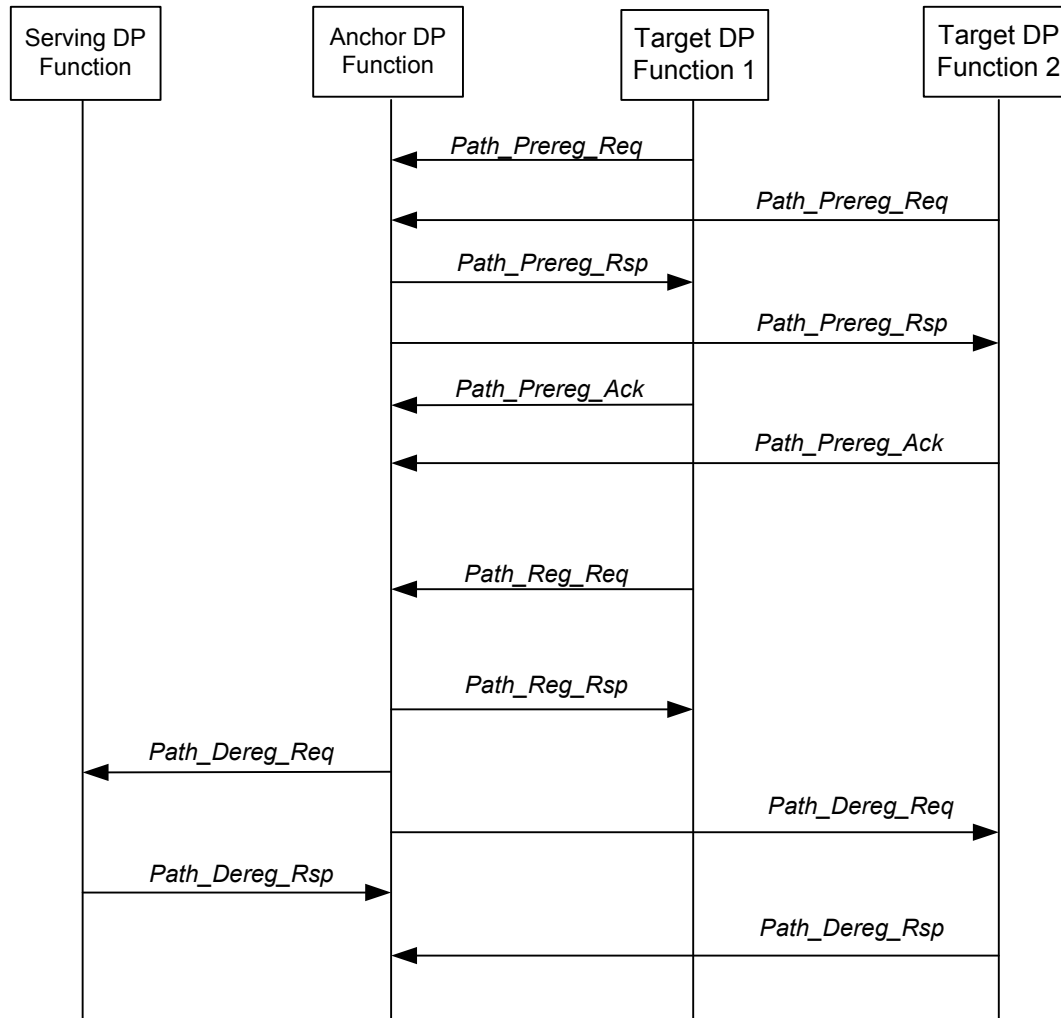
Figure 7-50 - Target Centric DP Control Transactions (with Pre-Registration) during HO

3 If Path Registration Transaction starts without any preceding Path Pre-Registration Transaction, then Registration
4 Request and Response shall convey all Informational Elements that contain parameters relevant for the data path to
5 be established. In this case *Path_Reg_Ack* shall be sent in response to *Path_Reg_Rsp*. Still, the Anchor DP Function
6 may start forwarding data to the Target DP Function immediately after it receives *Path_Reg_Req*. The Target DP
7 Function may start forwarding data to the Anchor DP Function immediately after it receives *Path_Reg_Rsp*.

8 Shortly after completing Path Registration Transaction, Anchor DP Function should De-Register the Data Path to
9 the old Serving DP Function. Figure 7-51 shows the transactions involved. The Serving DP Function may also
10 instigate Path De-Registration if it learns from HO Function that the MS has completed HO in the Target BS/ASN.
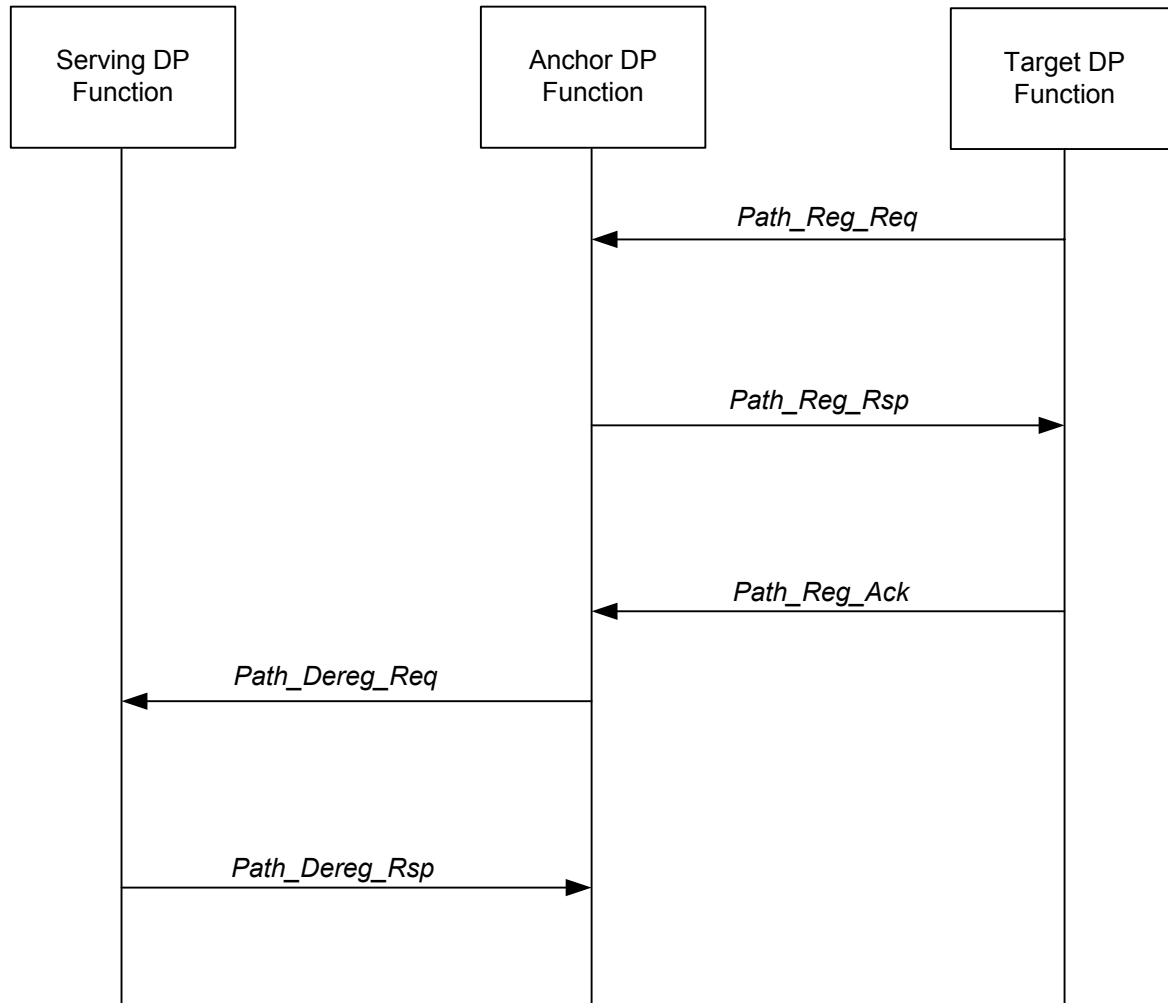
Figure 7-51 - Target Centric DP Control Transactions (without Pre-Registration) during HO

7.7.4.5 Anchor Centric Pre-Registration and Registration during HO

Anchor Centric refers to an approach according to which the Anchor DP Function instigates Pre-Registration Transaction. Registration Transaction however is still instigated by the Target HO Function because the Transaction should not start earlier than MS registers with the Target BS (with which the Target DP Function is associated)

The message processing rules are identical to the rules discussed for the Target Centric approach. Figure 7 52 shows the typical sequence for Pre-Registration, Registration and De-Registration Transactions as they likely to occur during HO.

1
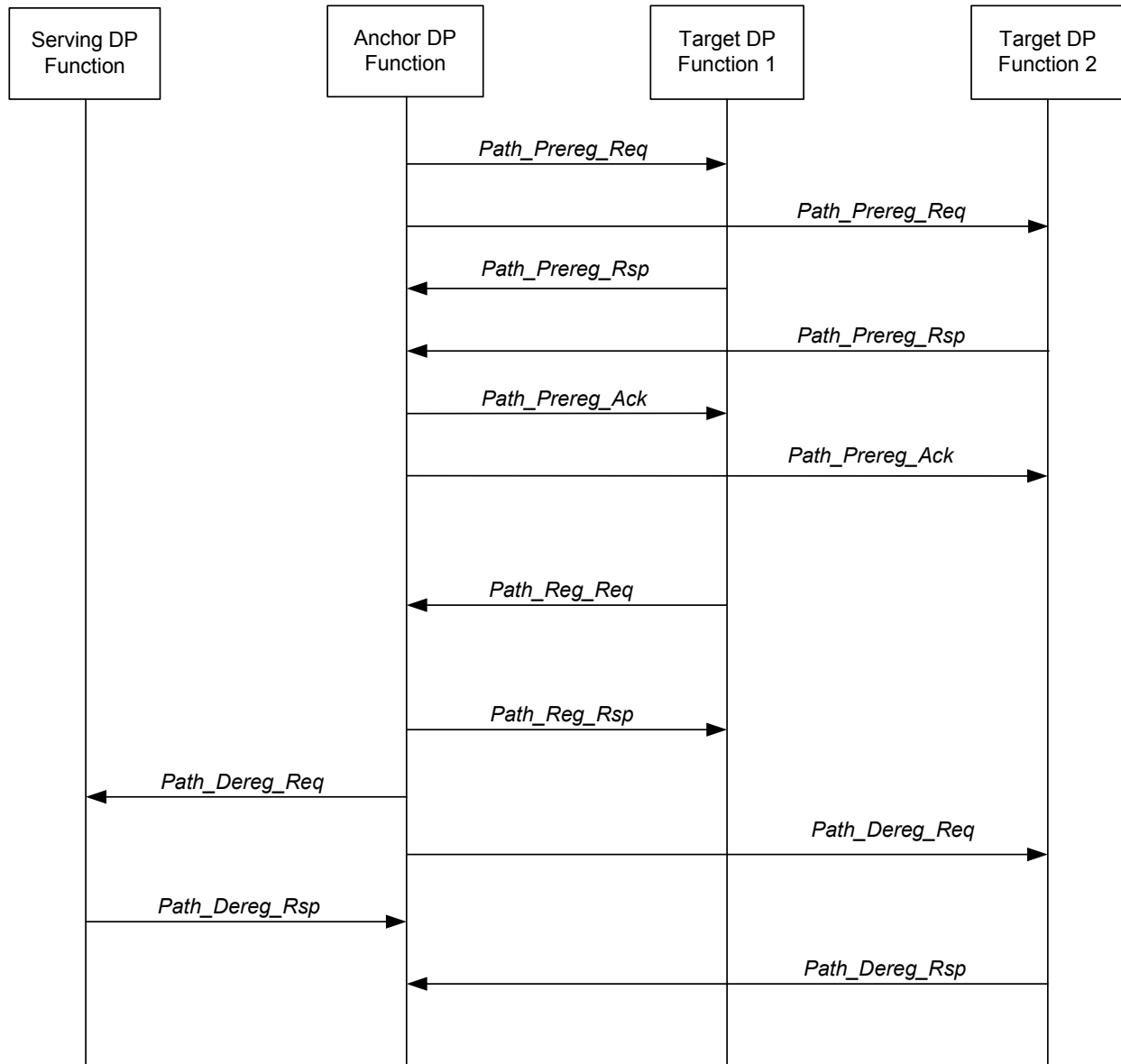
2 **Figure 7-52 - Typical Anchor Centric DP Control Transactions during HO**

3 ### 7.7.5 Context Delivery Function

4 Context Client MAY request from the Context Server the Session/MS Context (or parts of it).

5 The Session Info Context MAY include any or all of the following:

6 • MS NAI

7 • MS MAC Address

8 • Anchor ASN GW (profile A&C) or Anchor ASN (profile B) associated with the MS

9 • List of Service Flow IDs with associated:

10   o SF Classifiers

11   o SF QoS

12   o CID (associated with the SFID)

1   o   Data Path tagging (ID) Information

2   o   Etc.

3   •   R3 related information

4   o   Home Agent IP address

5   o   CoA

6   o   DHCP Server

7   o   AAA Server

8   o   R3 status Details

9   •   Security Information

10   o   Security information related to PKMv2 (e.g. SAs and its contexts including TEK, lifetime and PN
11   etc.)

12   o   Security information related to Proxy MIP (if used)

13 **7.7.5.1   Context Delivery Primitives**

14 ***7.7.5.1.1 Context_Req***

15 This primitive is used by a network entity to request the session information of a given MS from another network
16 entity.

17 *Context_Req* contains type identifiers of the requested Informational Elements belonging to an MS's session context.

18 The *Context_Req* MAY be used multiple times to derive the set of information required from multiple entities. For
19 example, the security information MAY be delivered via an authenticator.

20 ***7.7.5.1.2 Context_Rpt***

21 *Context_Rpt* might be sent unsolicited or in response to the *Context_Req*.

22 The entity that received the *Context_Req* SHALL respond with the *Context_Rpt* and include in the response the
23 Informational Elements that have been specified in the *Context_Req*.

24 The Context Server MAY lack some information requested by the Context Client. Thus the Report does not have to
25 contain all the Informational Elements requested with the *Context_Req*. If the Context Server lacks any requested
26 information it SHALL send an empty Report.

27 The *Context_Rpt* MAY be unsolicited attached to the HO Control primitives.

28 **7.7.6   Cooperation between the Functions**

29 The Functions described in the sections above trigger each other's operations by issuing internal triggers to one
30 another. With those triggers the information delivered with primitives of one Function might be used in the
31 operations of another Function.

32 The triggers are out of scope of Stage 2 and are mentioned only to facilitate explanation of the Inter-Function
33 Cooperation. This Cooperation would depend on the actual placement of the Functions. Thus, only examples of
34 Inter-Function Cooperation are given here.

35 Figure 7-53 and Figure 7-54 shows possible Inter-Function Cooperation in an ASN.

1
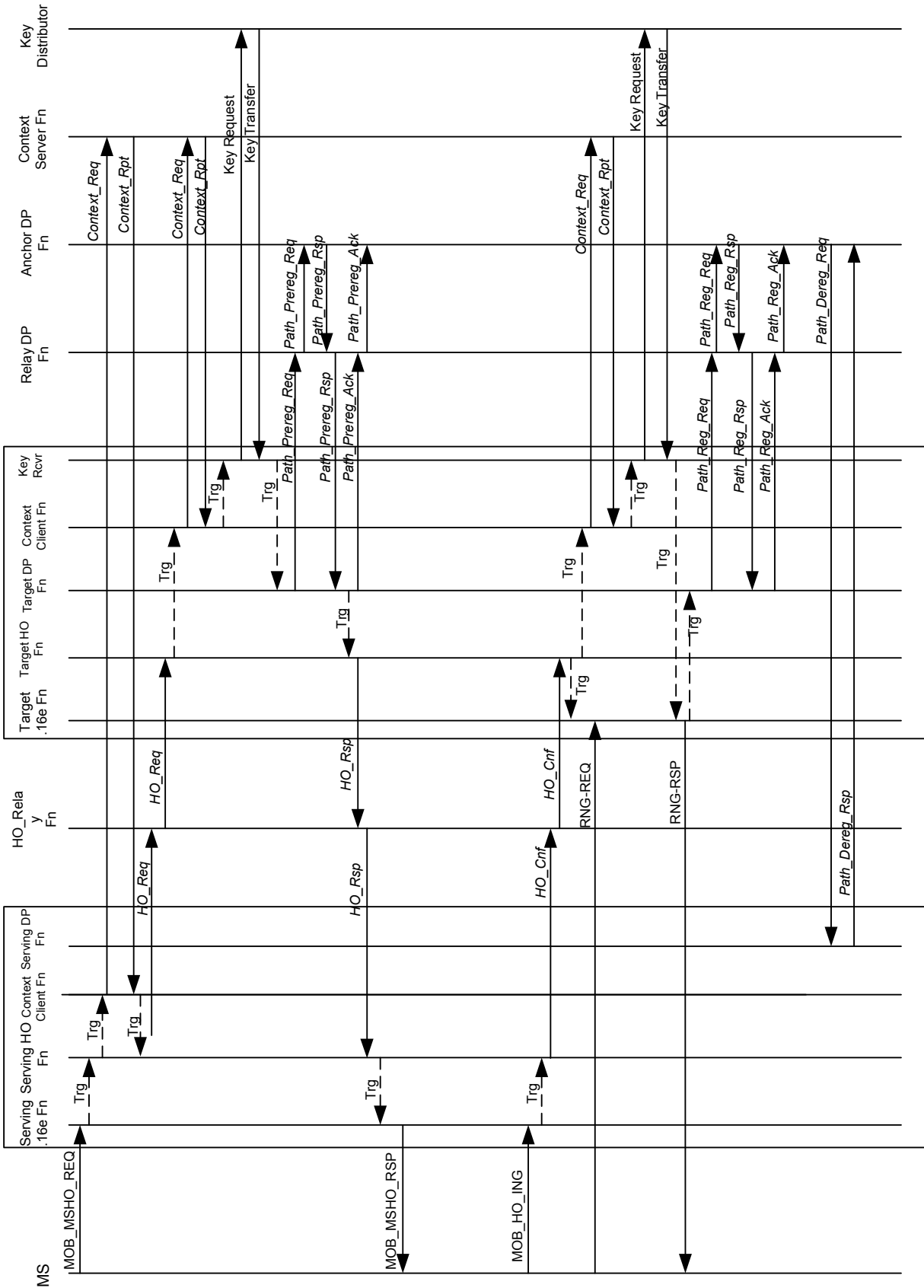
1 **Figure 7-53 - Cooperation between the Functions (Example)**

2
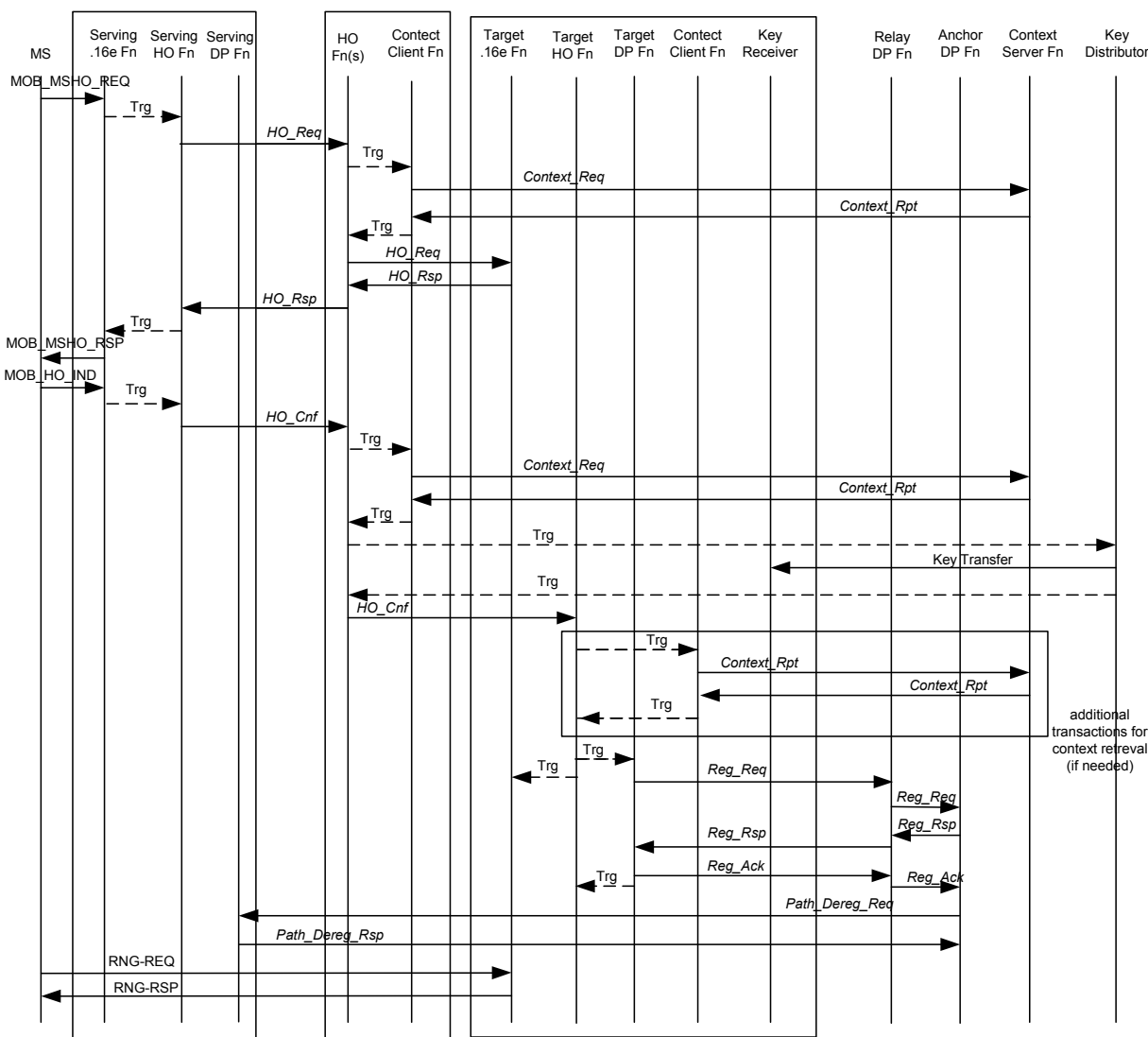
3 **Figure 7-54 - Cooperation between the Functions (Example2)**

4 Figure 7-53 and Figure 7-54 show example scenarios of Mobile Initiated HO:

5 The MS sends MOB_MSHO-REQ to the Serving .16e Function, which in turn triggers the Serving HO Function to
6 send *HO_Req* to the Target HO Function(s) via the Relay HO Function(s).

7 The Context retrieval transaction MAY be performed at different points in the HO procedure by different Functional
8 Entity, in different implementations. The three typical points are: before transmitting *HO_Req* to Target HO
9 Function, after receiving *HO_Req* by Target HO Function, and before transmitting *HO_Cnf* to Target HO Function.

10 In a option, prior to sending the *HO_Req* to the Target HO Function(s), the Serving HO Function (as in the example
11 1) or the Relay HO Function (as in the example 2) MAY trigger its associated Serving Context Client to request
12 required MS Context (via *Context_Req* and *Context_Rpt* Transaction) which is to be delivered to the Target HO
13 Function with *HO_Req*. It is also possible that a part of the MS Context is delivered here and the other parts are
14 delivered later in time (e.g. when transmitting *HO_Cnf*).

15 When *HO_Req* arrives to the Target HO Function the latter MAY trigger the associated Context Client Function to
16 send *Context_Req* in order to retrieve the necessary MS Context, if the received *HO_Req* does not have such

Context information (as in the example 1). In this case, the Security Context (e.g. AK, PN associated with AK, etc.) MAY also be retrieved using the Key Distribution Protocol. The MS Context and Key Delivery transactions are optional at this stage. Alternatively these transactions MAY be conducted later when the Serving HO Function or one of Relay HO Functions transmits the *HO_Cnf* to the Target HO Function.

If all necessary MS Context is available in the Target BS(s), then the Data Path Function MAY Pre-Register with the Anchor DP Function via the Relay DP Function(s). This step is optional and is needed only if the Data Path between the Anchor DP Function and the Target DP Function has to be established prior to removing the Data Path between the Anchor DP Function and the Serving DP Function (e.g. for bi-casting). When the optional Pre-Registration is completed the Target DP Function triggers the Target HO Function.

Then the Target HO Function sends *HO_Rsp* to the Serving HO Function.

Upon receiving the *HO_Rsp* the Serving HO function triggers the .16e Function to respond to the MS with MOB_BSHO-RSP.

When the MS is about to leave the Serving .16e Function it sends MOB_HO-IND. The Serving .16e Function in turn triggers the Serving HO Function to send *HO_Cnf* to the Target HO Function via the Relay HO Function(s). Optionally the MS Context and Key Delivery Transactions might be conducted here, and the context and key information are to be delivered to the Target HO Function with *HO_Cnf*.

When *HO_Cnf* arrives to the Target HO Function the latter triggers the Target .16e Function to stand by for MS Network Re-Entry.

And the Target HO Function triggers the Target DP function to Register Data Path with the Anchor DP Function via the Relay DP Function(s), if it receives *HO_Cnf* with MS context and a Data Path has not been made yet. (If needed, the Target HO Function MAY trigger the Context Client to make an additional Context retrieval transaction, before it triggers Target DP Function)

When Registration is completed the Data Path between the Anchor DP Function and the Old Serving DP Function is removed and only the Data Path between the Anchor DP Function and the Target (New Serving) DP Function remains.

1   **7.7.6.1   Data Integrity HO Mechanism**

2   **7.7.6.1.1   Anchor DF Buffering with Sequence Number**

3
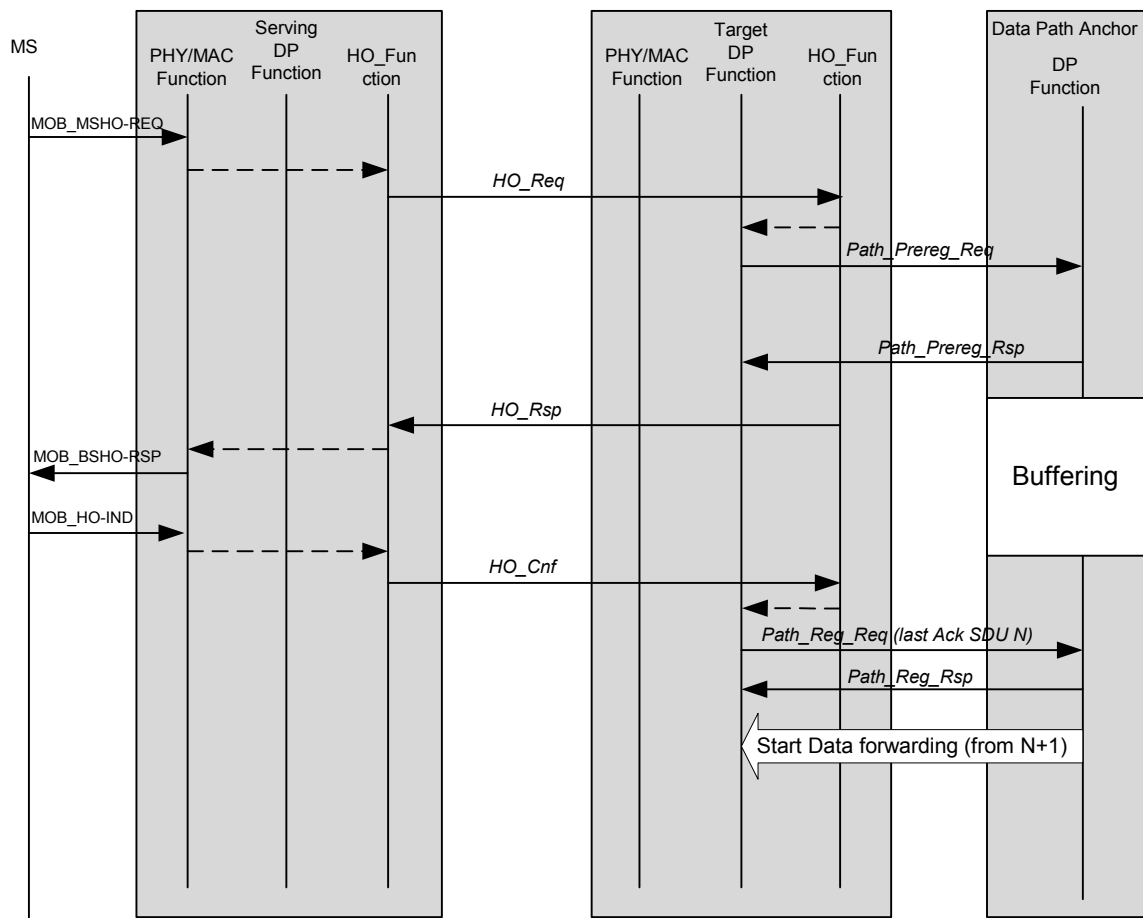
4   **Figure 7-55 - Anchor Data Path Function Buffering with SDU Sequence Numbering**

1   **7.7.6.1.2   Anchor DF Bi/Multi-casting with Sequence Number**
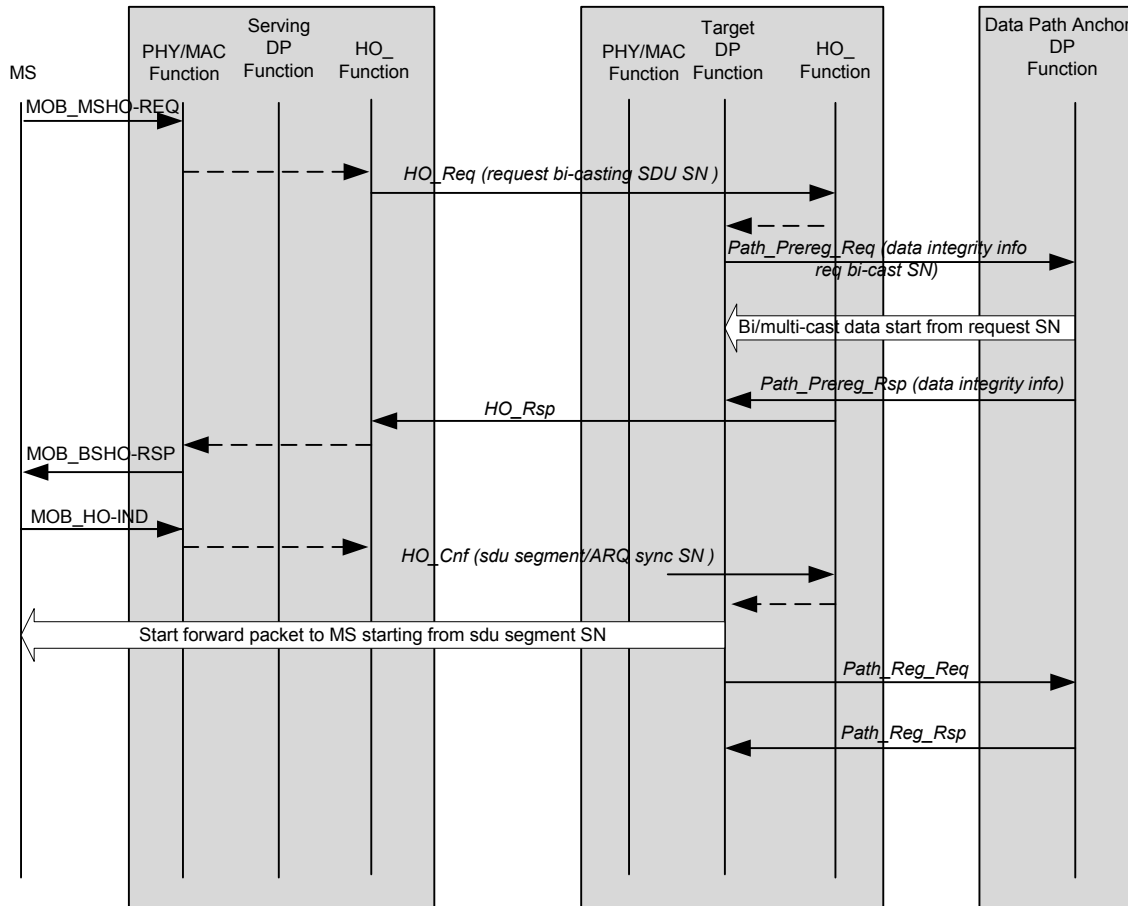
2

3   **Figure 7-56 - Anchor Data Path Function Bi-Cast with SDU Sequence Numbering[8]**

---

[8] The Target DP Function may be required to buffer the DL packets, once the Anchor DP Function starts bi-casting the traffic

1   **7.7.6.1.3   Serving & Target Data Path Function Buffer Transferring**
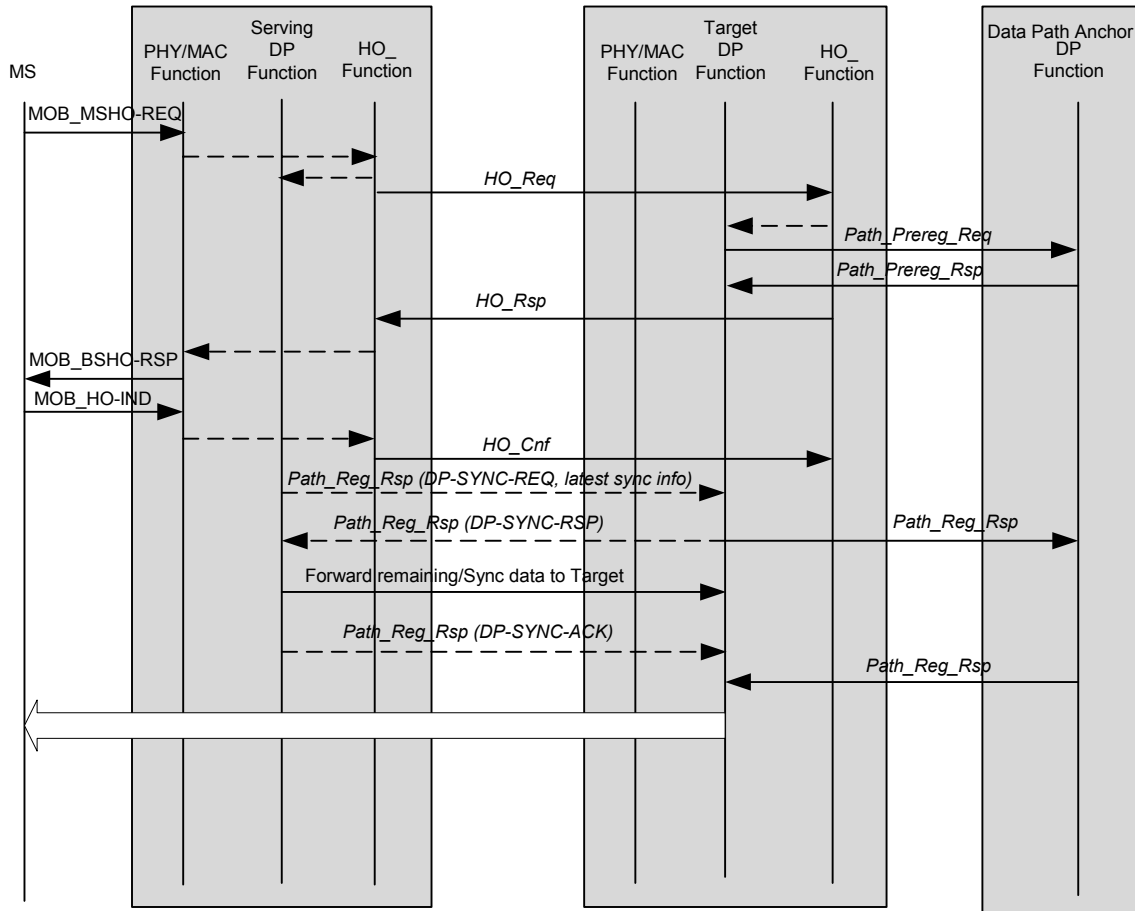
2

3   **Figure 7-57 - Serving Data Path Function Bi-cast to Target[9]**

---

[9] The Target DP Function may be required to buffer the DL packets, once the Anchor DP Function starts bi-casting the traffic

1   **7.7.6.1.4   Anchor & Target Data Path Function Buffer Transferring**
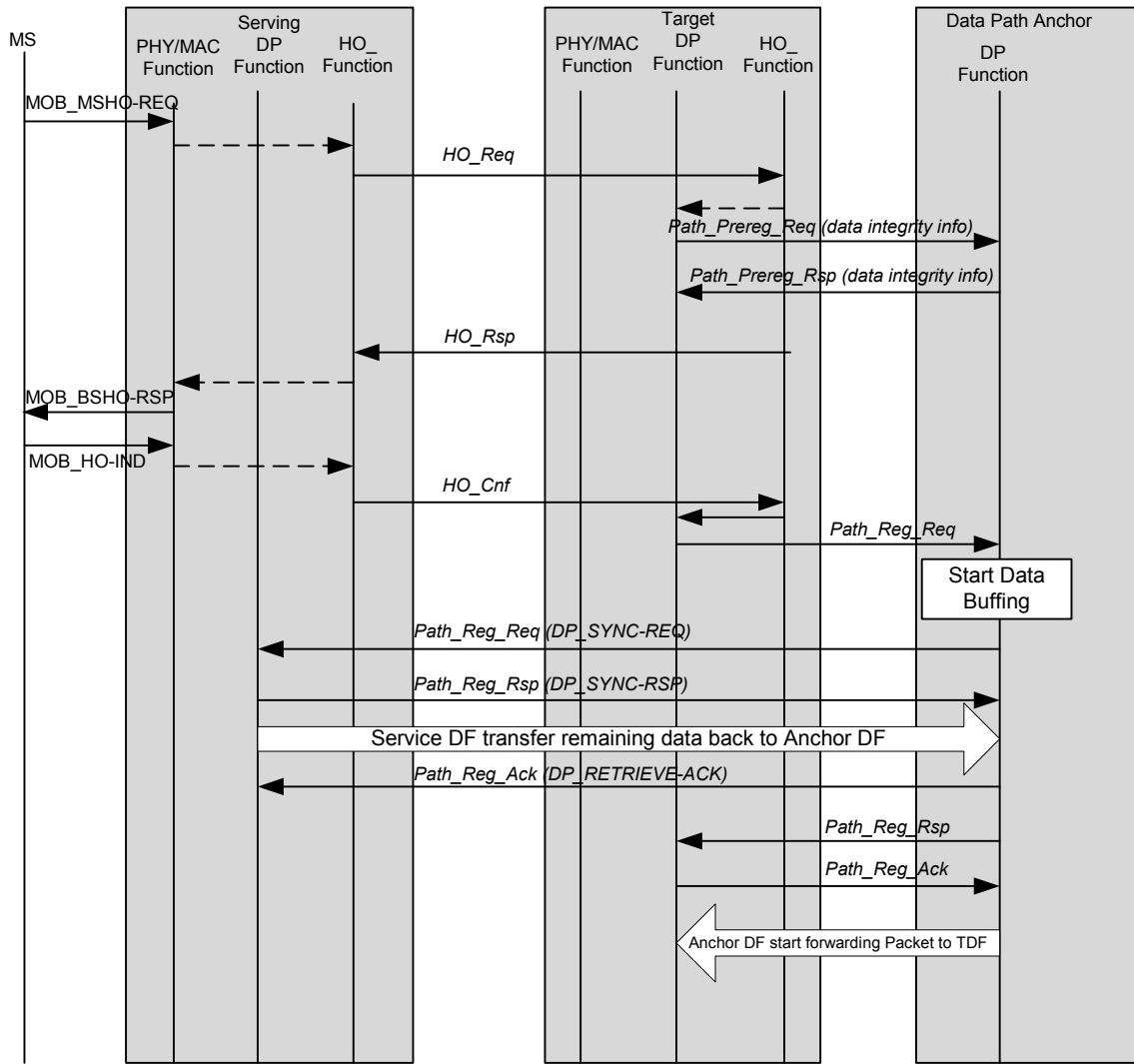
2

3   **Figure 7-58 - Data Retrieval into Anchored Buffer and Data Forwarding to Target**

1 **7.7.6.1.5   Buffering with Ack Window**

2
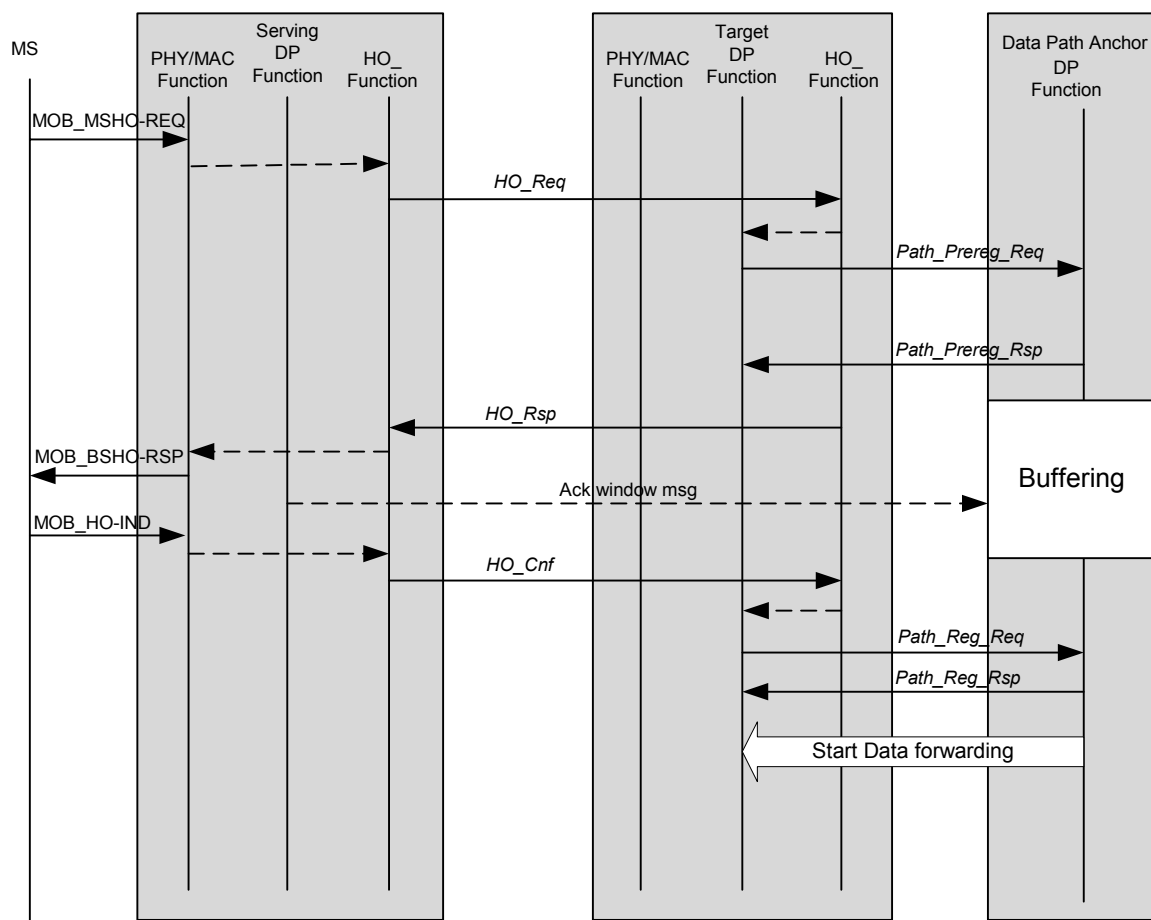
3   **Figure 7-59 - Data Path Anchor Buffering with Sliding Window Forwarding**

4 **7.8   CSN Anchored Mobility Management**

5 **7.8.1   Scope and Requirements for CSN Anchored Mobility (MIPv4) Management**

6 **7.8.1.1   Scope**

7 This section describes mobile IP based macro mobility between the ASN and CSN across the R3 reference point. In
8 the case of IPv4, this implies re-anchoring of the current FA to a new FA and the consequent binding updates (or
9 MIP re-registration) to update the upstream and downstream data forwarding paths. The procedures described in this
10 section complement the procedures outlined in Section 7.7 (where ASN—anchored mobility management
11 procedures are discussed without changes to the anchor FA in the case of IPv4).

12 The WiMAX mobility solution consists of two mobility levels:

13   • ASN-anchored mobility or micro mobility is when the MS moves between Data Path Functions while
14   maintaining the same anchor FA sitting at the northbound edge of the ASN network. The data flow
15   between CSN and Data Path Functions pivots at the anchor FA. CSN is unaware of any mobility that
16   occurs between ASN Data Plane Functions. This scenario is covered in Section 7.7.

1   • CSN Anchored Mobility Management or macro mobility is when the MS changes to a new anchor FA.
2   The new FA and CSN exchange signaling messages to establish data forwarding path.[10]. This chapter
3   describes the solution for this type of mobility.

4   The following additional considerations apply for R3 mobility management:.

5   • CSN Anchored Mobility Management SHALL be established between ASN and CSN that are in the same
6   or different administrative domains.

7   • The mobility management MAY extend to handovers across ASNs in the same administrative domain. (See
8   Figure 7-60)

9   • Inter-technology handovers are outside the scope of Release 1.0.0.

10 The CSN Anchored Mobility Management procedures MAY not be synchronized with the event of MS changing its
11 point of attachment to the ASN. In other words, the procedures MAY be delayed relative to the completion of link
12 layer handover by the MS.

13 Figure 7-60 illustrates the CSN Anchored Mobility Management scope for IPv4 based mobile IP. In an intra NAP
14 R3 mobility case, a MS is mobile between FAs within a single NAP domain. As shown, the R3 mobility event
15 results in a handover between two FAs, thereby relocating the ASN R3 reference anchor point in the NAP.

16 Note that Inter-NAP R3 mobility is not supported in Release1.

17
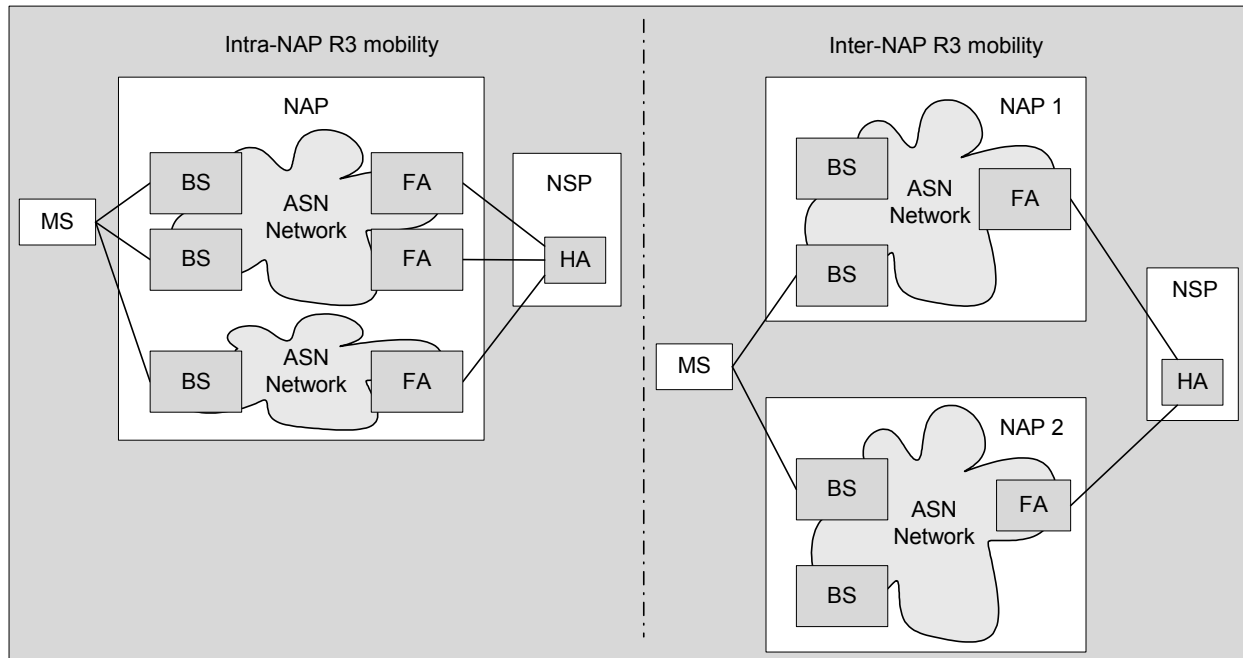
18 **Figure 7-60 - R3 Mobility Scope**

19 **7.8.1.2   Functional Requirements**

20 The following functional requirements have been identified for CSN Anchored Mobility Management:

21 • CSN Anchored Mobility Management for IPv4 SHALL be based on [43] and related RFCs. Proxy-MIP
22   differs from client-based MIP in that the ASN network performs the role of the Mobile Node (MN).

---

[10] The scope of this version of the document only covers the inter/intra-ASN handover (R3 mobility) between FAs belonging to the same NAP.

1   •   R3 mobility SHALL NOT automatically terminate or otherwise interfere with idle/sleep mode of operation
2   of the MS. CSN Anchored Mobility Management SHALL accommodate the scenario in which MS
3   remains in idle/sleep state until it is ready to send upstream traffic or is notified of downstream traffic from
4   the network and relinquishes the idle/sleep state.

5   •   Reverse tunneling between ASN and CSN SHALL be supported.

6   •   In all non-roaming scenarios, the HA SHALL be located in the CSN of Home-NSP. For roaming scenarios,
7   the HA MAY be located in the CSN of either the Home-NSP or Visited-NSP depending on:

8   o   Roaming agreement between Home-NSP and Visited-NSP.

9   o   User subscription profile and policy in Home-NSP

10   •   CSN Anchored Mobility Management within a single NAP administrative domain SHALL introduce
11   minimal latency and packet loss.

12   •   Make-before-break operation (when coupled with ASN-anchored mobility procedures described in Section
13   7.7) SHOULD be possible within the same NAP administrative domain. To accomplish this, the previous
14   anchor SHOULD be capable of maintaining continuous data flow while signaling to establish the data path
15   to a new anchor FA.

16   •   It SHALL be possible to generate triggers to re-anchor at any time independent of ASN-anchored mobility.

17   •   From a MIP point of view an MS SHALL always operate as if in a foreign network.

18   •   Both the CMIP and PMIP mobility schemes are mandatory.

19   •   Efficient use of wireless link. Extra overhead over the air-interface to accomplish CSN Anchored Mobility
20   Management SHALL be minimized.

21 **7.8.1.2.1   PMIP-Specific Functional Requirements**

22   •   PMIP procedures SHALL NOT require additional signaling over the air or additional data headers to
23   complete CSN Anchored Mobility Management.

24   •   MS SHALL be unaware of CSN Anchored Mobility Management activities.

25   •   Use of DHCP by the MS for IP address assignment and host configuration SHALL be supported.

26 **7.8.1.2.2   CMIPv4-Specific Functional Requirements**

27   •   MIP [43] specified procedures SHALL be used on MS for IP address assignment and host configuration.

28 **7.8.1.3   R3 Mobility Security Requirements**

29 **7.8.1.3.1   Intra-domain Security**

30   •   When FA and HA are in the same administrative domain a trust relationship (via established FA-HA
31   security association) is assumed between the FA and HA. The set of the FA-HA security associations is an
32   implementation and/or operational issue that are outside the scope of this specification.

33 **7.8.1.3.2   Inter-domain Security**

34   •   FA and HA, which are in different administrative domains, need to set up a trust relationship for mobility
35   signaling.

36   •   Mobility service authorization for MS is needed to set-up data forwarding.

37   •   Signaling between ASN and CSN SHOULD be secure:

38   o   For PMIP, the H-AAA will derive the PMIP MN-HA key for a particular MS to the ASN during
39   network access authentication process. The PMIP MN-HA key is unique for each MS; key sharing
40   between MS SHALL NOT be allowed.

1   o Mobility service key is used to set up forwarding path via dynamically established tunnels between
2   FA and HA.

3   o User Data encryption is out of the scope of this document.

4   o The choice of authentication methods SHALL comply with [43]. For example, HMAC_SHA1 can
5   be applied to protect the signaling for now. More importantly, authentication mechanism SHALL be
6   extensible to support future cryptography.

7 7.8.1.4   CSN anchored mobility (R3 Mobility)

8 This section describes requirements and procedures for Mobile IPv4 based R3 mobility management.

9 Mobile IP (MIP, RFC 3344 and related RFCs for IPv4) is adopted as the mobility management protocol for all
10 applicable usage/deployment scenarios requiring seamless inter-subnet/inter-prefix layer-3 handovers. Within the
11 Mobile IP framework, an MIP client maintains a persistent Home IP address when handing off between different
12 FAs. The R3 Mobility solution has four functional components— a MIP client, an Foreign Agent (FA) located in the
13 access network, a Home Agent (HA) typically located in the user's home network (but MAY be dynamically
14 assigned/requested from a visited operator's network) and a AAA server.

15 For CSN Anchored Mobility Management two variants of the MIP protocols are supported:

16 • Client MIP (CMIP): CMIP is an IETF compliant MIP solution based on a Mobile IP enabled MS. CSN
17   Anchored Mobility Management will cover CMIP based mobility schemes for IPv4 and IPv6.

18 • Proxy MIP (PMIP): Proxy MIP is an embodiment of the standard Mobile IP framework in which an MN is
19   transparently instanced in the access network on behalf of a client that is not MIP-aware or MIP-capable.

20 7.8.1.5   CSN Anchored Mobility Management triggers

21 The following types of event can trigger the procedure:

22 • *MS mobility:* The MS hands off to a new Base Station under a new FA.

23 • *Wake-up from idle mode*: The MS wakes up from the idle mode at a different ASN than the one under
24   which it entered the idle mode.

25 • *Resource optimization:* The network decides for resource optimization purposes to transfer the R3 endpoint
26   for the MS from the serving FA to a new FA, independently of any MS movement.

27 7.8.1.6   MIP Extensions

28 The following standards SHALL be used for Mobile IPv4 operations with any limitations or extensions described in

29 this document:

30 - Mobility support for IPv4 [43]

31 - Reverse Tunneling [29]

32 - NAI Extension [22]

33 - Registration Revocation [45]

34

35 The following standards MAY be used for Mobile IPv4 operations with any limitations or extensions described in
36 this document:

37 - Foreign Agent Challenge [28]

38 - Mobile IP Vendor/Organization Specific Extensions [33]

1 **7.8.1.7   Addressing Support**

2 **7.8.1.7.1   Private HoA Address Support**

3 It is possible that two different MS served by the same FA have the same, overlapping private address because they
4 belong to two different private networks.

5 **7.8.1.7.2   Dynamic Home Agent Assignment**

6 In roaming cases the Home Agent can be assigned by either the Home NSP or the Visited NSP. It's the home
7 operator that will decide based on the roaming agreement with the visited operator and/or the end-user's
8 subscription profile which network is responsible for assigning the MIP Home Agent.

9 If a Home Agent is assigned in the visited network the MIP authentication will take place between the visited HA
10 and the Home AAA server. Security exchanges are transparent to the visited AAA proxy.

11 If the HA is to be assigned by the Home CSN both the Home Agent address and optionally the DHCP server address
12 or HoA address are appended to the AAA reply by the Home-AAA server.

13 For Home Agents in the Visited CSN the AAA proxy can append the Home Agent address and the optional DHCP
14 server address or HoA address to the AAA exchange between the home AAA server and the authenticator.

15 For static agreements between two operator domains (e.g. HA always in the visited network) the AAA proxy can be
16 configured to add a HA address based on the Home-AAA server domain.

17 For more dynamic Home Agent location algorithms (e.g. based on subscription profile) the AAA proxy decision to
18 append the HA address will depend on the presence of the HA address container in the AAA reply from the home
19 AAA.

20 Although not considered very scalable the address of a HA in the visited network can be provided by the home AAA
21 server based on pre-configured information.

22 The Home Agent can be provided in the form of an IP address or a FQDN (Fully Qualified Domain name).

23 **7.8.1.7.3   Dynamic HA: PMIP Considerations**

24 The PMIP security information is always exchanged between the Home AAA server and the authenticator.

25 The PMIP client will insert the HA address retrieved during the access authentication step in the MIP Registration
26 Request.

27 **7.8.1.7.4   Dynamic HA: CMIP Considerations**

28 The network SHALL support dynamic HA allocation algorithm. When the FA receives an Registration Request
29 from the MS with an HA IP address value of 0.0.0.0, the HA will be assigned based on the AAA HA attribute
30 downloaded during the access authentication step and its HoA address returned in the Home Address field of the
31 RRP.

32 **7.8.1.7.5   MIP Addressing**

33 The FA SHALL support [22] NAI extension.

34 If the HA address provided by the CMIP client is different from the HA address downloaded during access
35 authentication the FA MAY decide (depending on operator policies) to forward the Registration Request to the
36 dynamically assigned HA unicast address. The HA MAY accept the Registration Request contrary to [43] or MAY
37 reject it with an error code of 136 in accordance to [43]. The HA SHALL put its own IP address in the Registration
38 Reply. The FA SHALL use a publicly routable and visible address as the CoA address.

39 **7.8.1.8   Proxy MIP R3 Mobility Management**

40 Proxy-MIP R3 mobility is based on MIP signaling between MIP client, FA and the Home Agent. In the proxy-MIP
41 approach the MIP client resides within the ASN network and performs R3 mobility management on behalf of the
42 MS. Co-location between the proxy-MIP instance and the Authenticator functional entity in the ASN is assumed;

1   i.e. any communication between these two entities is beyond the scope of this document. The R3 mobility FA is
2   located at the northbound boundary of the ASN. The Home agent is located in a CSN network.

3   Proxy-MIP does not put additional requirements on the MS in order to support R3 mobility and is fully network
4   controlled.

5   To distinguish between a PMIP instance managing the R3 mobility for a single user and the functional entity
6   combining all these logical instances a new definition is introduced:

7   1.   **PMIP Mobility Manager**: Functional entity managing multiple PMIP clients

8   2.   **PMIP client**: Logical entity managing R3 Mobility for a single user/MS

9   In other words a 'PMIP Mobility Manager' = Σ 'PMIP clients'

10   Any R3 mobility session or PMIP client is uniquely identified by the user's NAI. The NAI used for R3 Mobility can
11   be the same as the one used for access authentication.

12
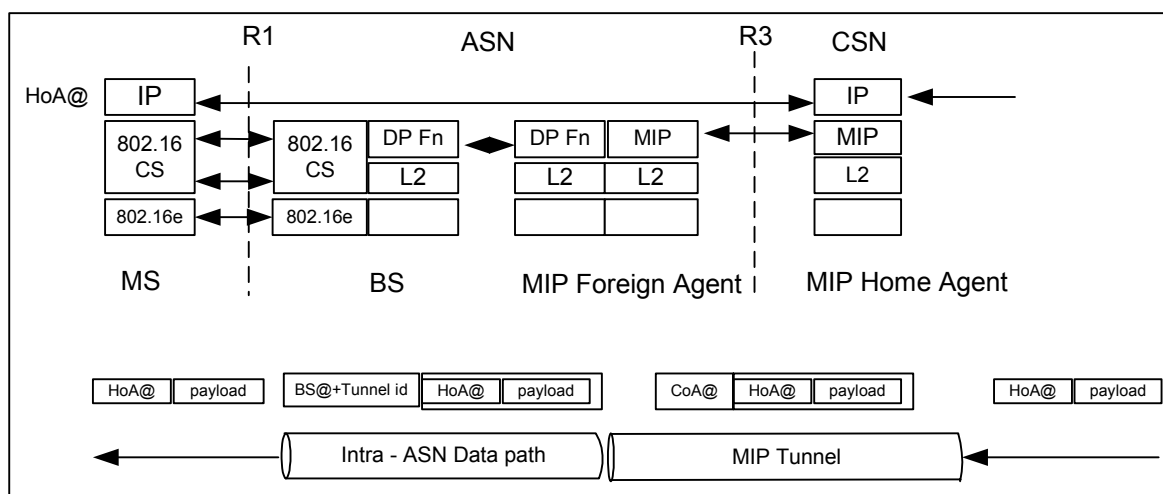
13   **Figure 7-61 - Proxy MIP Data Plane (Example)**

14
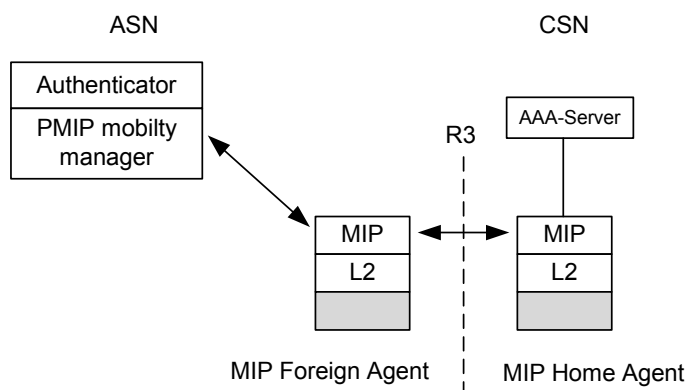
15   **Figure 7-62 - Proxy MIP Control Plane**

16   In the proxy MIP solution, the IP network aspects of the CSN Anchored Mobility Management handovers are
17   transparent to the MS. The MIP registration to set up or update the MS's forwarding path on the HA is performed by
18   the proxy-MIP client on behalf of the MS. The MIP related information required to perform MIP registrations to the
19   HA are retrieved via the AAA messages exchanged during the authentication phase. This information consists of
20   Home Agent address, and the security information to generate the MN-HA authentication extension and either the
21   DHCP server address or HoA address.

7.8.1.8.1 Proxy-MIP FA Considerations

Additionally, in applicable ASN configurations the alternative PMIP redirection procedure as described in Section 7.8.1.8.7 MAY be used.

As illustrated in Figure 7-62 the Foreign Agent behavior for proxy-MIP differs slightly from RFC3344 in that the destination IP addresses for the control and data plane are different.

In the IETF MIP model the MIP client resides on the host and is the termination point for both the MIP signaling and user traffic. In PMIP approach user data is sent to the MS over the corresponding R6 or R4 data path, MIP signaling needs to be directed to a PMIP client within the PMIP mobility manager.

To achieve this goal, odd-numbered MN-HA SPI is used as an indication of PMIP usage.

Messages originated by the PMIP mobility manager will set the IP packet source address to the address of the PMIP mobility manager.

MIP Registration Reply will be returned to the PMIP mobility manager instead of the MS by FA. The PMIP mobility manager address is not directly linked to an MS's R3 mobility session and can be changed at any time independently of an ongoing R3 mobility session.

7.8.1.8.2 DHCP server/proxy consideration

There are two DHCP server/proxy deployments options for CSN anchored mobility in Release 1.0.0:

2) DHCP proxy: There is DHCP proxy in the ASN acting as DHCP server to manage DHCP exchange with MS. There is no DHCP messages cross R3.

3) DHCP relay: There is DHCP relay in the ASN to forward the DHCP messages between the DHCP server in the CSN and MS. There are DHCP message cross R3.

7.8.1.8.3 Proxy-MIP Connection Setup Phase

After successful access level authentication the R3 mobility connection setup takes place.

During R3 mobility connection-setup following actions are performed:

- Location of the Home-Agent is determined based on inter operator policies.
- MS PoA assignment
- MS IP host configuration
- MIP registration
- R3 mobility authentication between MN and HA

The following signaling flow describes the connection setup phase for the Proxy-MIP solution using DHCP Relay option.
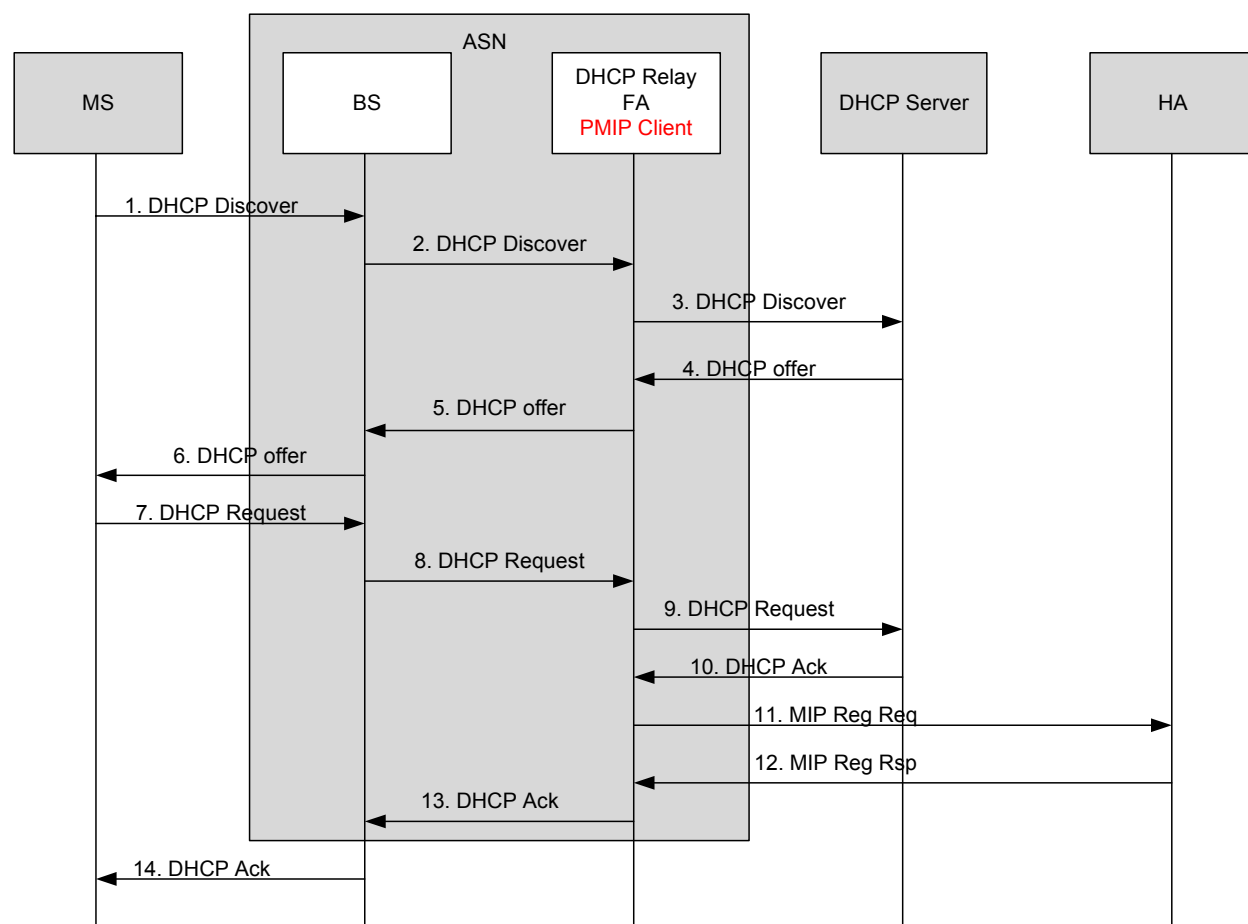
Figure 7-63 - Connection Setup in the Proxy MIP Solution (HA in H-NSP)

The following steps are written based on R3 is already secured, if R3 is not secured the DHCP Relay shall add the authentication sub-option as explained in RFC 4030 to have data integrity and replay protection for relayed DHCP messages.

STEP 1:

The MS sends a **DHCP Discover** as a broadcast message. The DHCP message is sent on the MS's Initial service flow setup over R1 interface to the BS.

STEP 2:

The **DHCP Discover** message is forwarded from BS to DHCP Relay present in ASN through the data path established for the ISF (Initial Service Flow) traffic.

STEP 3:

The DHCP Relay in ASN will intercept and change the destination IP address from broadcast to unicast and configure the giaddr field in the DHCP payload and sends the **DHCP Discover** message to the DHCP server of the MS based on configuration information. The configuration information in the most generic case will be downloaded via AAA but it may also be statically provisioned

If the Datapth is per MS or per SF, the MS context can be found based on the Datapath and not on the MAC address.
If the Datapath is per BS the MS context can be found based on the MAC address or MS NAI

1

2 **STEP 4:**

3 DHCP servers receiving the **DHCP Discover** request reply by sending a **DHCP Offer** message including an offered
4 IP address.

5

6 **STEP 5**:

7 The DHCP Relay in ASN forwards the DHCP replies to the MS. The **DHCP Offer** message is sent from ASN GW
8 to BS through the Data Path.

9 The destination IP address of the **DHCP Offer** message sent to MS is a unicast one. Normally DHCP servers or
10 relay agents attempt to deliver the **DHCP Offer** to a MS directly using unicast delivery. Unfortunately some MS's
11 implementations are unable to receive such unicast IP datagram until they know their own IP addresses. To work
12 around with this kind of MS's broadcast address MAY be used in **DHCP Offer** message. ASN need to check the
13 BROADCAST (B) flag in the **DHCP Offer** message. If this flag is set, ASN need to use broadcast address to send
14 **DHCP Offer** message, otherwise unicast address, but the delivery will be over a unicast CID.

15

16 **STEP 6:**

17 BS sends **DHCP Offer** message to the MS on the MS's Initial Service Flow.

18

19 **STEP 7:**

20 MS receives **DHCP Offer** message, and sends a **DHCP Request** to the selected DHCP server as a broadcast
21 message confirming its choice of the DHCP Server.

22

23 **STEP 8:**

24 **DHCP Request** message is sent from BS to DHCP relay in ASN through the Data Path established.

25

26 **STEP 9:**

27 The DHCP Relay in ASN will relay the **DHCP Request** to the DHCP server.

28

29 **STEP 10:**

30 The selected DHCP server receives the **DHCP Request** and replies with a **DHCP Ack** containing the configuration
31 information requested by the MS.

32

33 **STEP 11:**

34 The DHCP Relay in the ASN triggers a newly instantiated PMIP client to initiate the Mobile IP Registration
35 procedure (not shown in Figure 7-63). The PMIP client uses the HoA information and constructs a Mobile IP
36 Registration Request message. This message contains HoA and CoA for this MS. The source address for this R3
37 message is CoA, and the destination address is HA address.

38

39 **STEP 12:**

40 The HA responds with the Mobile IP Registration Response message. The source address for this R3 message is
41 HA, and the destination address is CoA.

1

2 **STEP 13:**

3 After the establishment of MIP tunnel the PMIP client triggers DHCP Relay to send the **DHCP Ack** to the BS.

4

5 **STEP 14:**

6 BS sends **DHCP Ack** message to the MS on the MS's provisioned Initial Service Flow.

7 If MS doesn't receive a **DHCP Ack**, or **DHCP Nak** message when timeout, it will retransmit **DHCP Request**. If
8 neither **DHCP Ack** nor **DHCP Nak** received when the maximum retransmission reached, MS shall restart the IP
9 initialization process.

10 ### 7.8.1.8.3.1   Backend IP Address Assignment Options

11 In the proxy-MIP solution a DHCP request is sent to the ASN network to retrieve the HoA address and IP host
12 configuration parameters.

13 Between the ASN and CSN network following options are available:

14 - *DHCP relay*: The DHCP relay in the ASN manages the DHCP exchange with the DHCP server in the
15   CSN. The DHCP server address is retrieved during access authentication.

16 - *AAA based HoA assignment*: IP host information and HoA address can be retrieved from the CSN as part of
17   the access authentication AAA exchange. In this case the ASN will host a DHCP proxy and return the
18   complete IP configuration to the MS.

19 - *MIP*: MIP exchange can be used by the PMIP client to retrieve the MS HoA address. For the MS host
20   configuration the PMIP client SHALL use normal Vendor/Organization Specific extensions [33] in the
21   MIP registration request. In that case, Mobile IP registration exchanges are triggered by DHCP proxy after
22   DHCP discovery is received, DHCP proxy will not send DHCP offer until MIP registration is complete.
23   After getting HoA from HA through the MIP registration progress, the PMIP client sends the HoA to the
24   DHCP proxy which will act as a server in the forthcoming DHCP exchanges.

25 In the AAA scheme the IP address of the MS is available in the ASN network prior to the IP connection or radio
26 connection establishment. In case of network-initiated connections, this information can be used to configure the SF
27 classifiers directly with the correct IP address information, avoiding address spoofing or bootstrapping procedures.

28 ### 7.8.1.8.4   Proxy-MIP Session Renewal

29 To update session state in the network and allow context release in case of SS/MS or network failure both the MIP
30 context and the DHCP session state have to be renewed.

31 In a proxy MIP approach the MIP context renewal is handled completely by the network. As MIP re-registrations do
32 not generate overhead over the air interface or interfere with SS/MSs going into sleep mode small refresh timer
33 values can be chosen.

34 DHCP renewals are initiated by the MS.

1   **7.8.1.8.4.1   DHCP Relay**

2
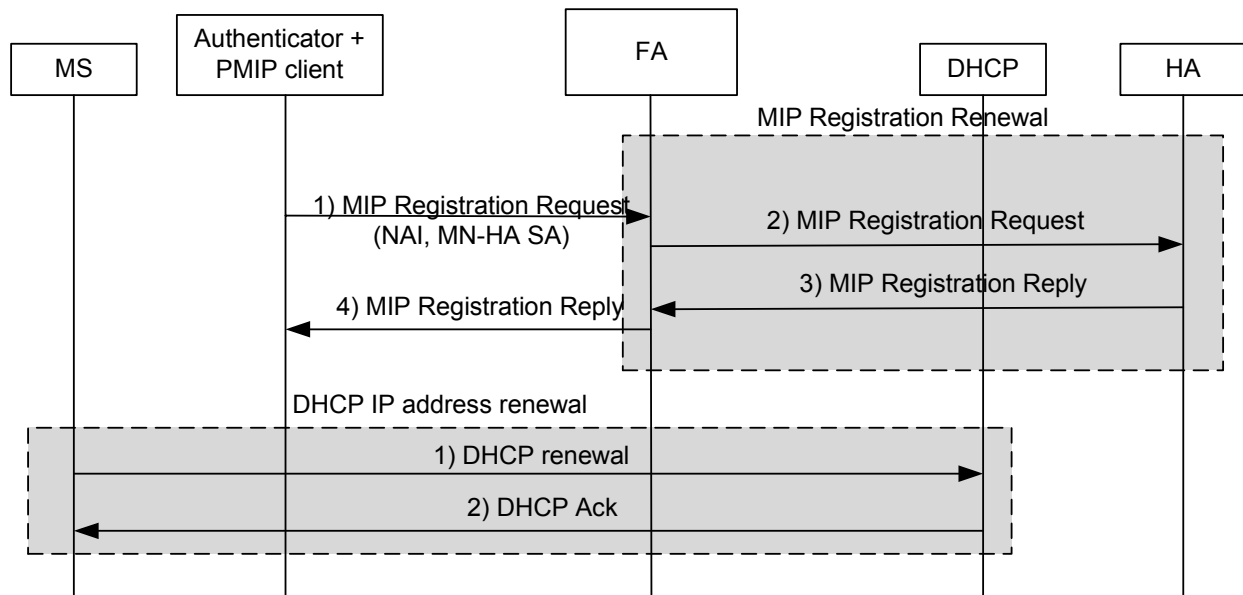
3   **Figure 7-64 - Proxy-MIP, MIP Re-registration + IP Address Renewal**

4   **MIP session renewal:**

5   In conformance with the [43] regular MIP registration messages are sent by the PMIP-client to FA to be forwarded
6   to the Home-Agent.

7   Upon receiving the MIP registration message the Home-Agent will reset the MIP session timer.

8   Authentication of the source of the MIP registration messages is based on the keys exchanged during access
9   authentication and do not require re-synchronization with the user's authentication server.

10   **DHCP session renewal:**

11   Through DHCP renewal the MS is able to maintain its HoA address.

12   DHCP renewal messages are initiated by the mobile, using the siaddr field from the initial DHCP ack message
13   during the initial address allocation as the IP address of the DHCP server. The ASN can either act as DHCP relay or
14   DHCP proxy as described in section 7.8.1.8.3.1.

15   In scenarios where AAA or MIP is used on R3/R5 to assign the HoA address the ASN will host the DHCP server.

16   **7.8.1.8.5   Proxy-MIP CSN Anchored Mobility Management Handovers**
17   The following signaling flow describes the CSN Anchored Mobility Management based on MS mobility event. In
18   the Proxy MIP approach handovers are initiated by the Proxy-MIP client.

1 **7.8.1.8.5.1 CSN Anchored Mobility Management Triggered by MS Mobility**

2
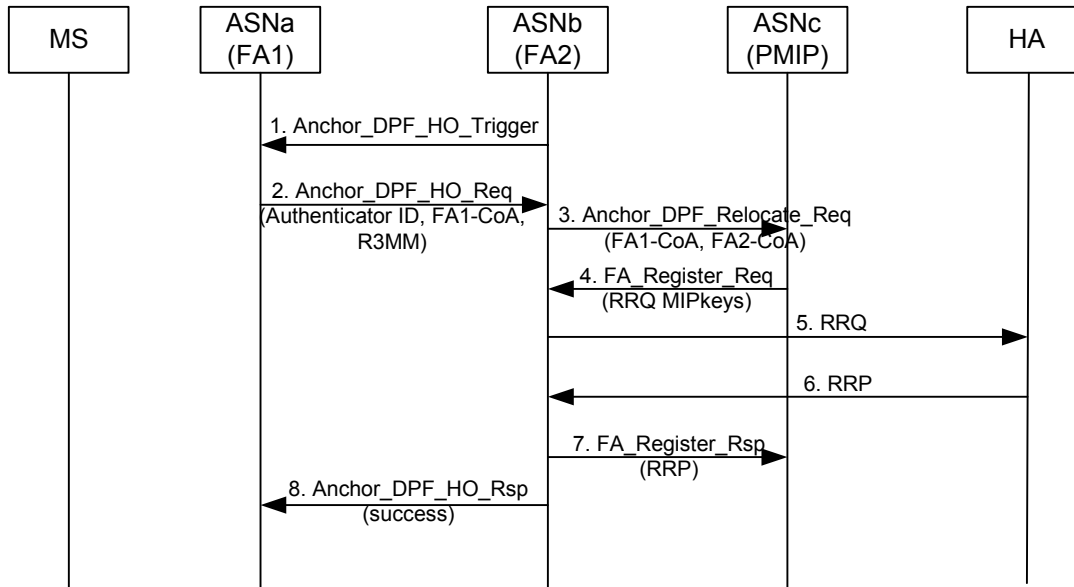
3 **Figure 7-65 - MS Mobility Event Triggering a Network Initiated R3 Re-anchoring (PMIP)**

4 **STEP 1**

5 If the target ASNb initiates the FA relocation negotiation, it sends a *Anchor_DPF_HO_Trigger* message to the
6 anchor DPF in ASNa. If ASNa agrees with the FA relocation, it proceeds to Step2.

7 If the source ASNa initiates the FA relocation procedure, the call flow starts from Step2.

8 **STEP 2**

9 ASNa sends a AnchorDPF_*HO_Req* message to the DPF in ASNb. The message contains Authenticator ID, the
10 current FA-CoA address and the DHCP context information for the MS.

11 **STEP 3**

12 Target ASN for FA relocation sends an *Anchor_DPF_Relocate_Req* message to the PMIP Client. This message
13 relays some information about target ASN that is necessary in order to construct and send the MIP RRQ message in
14 step4. The message contains CoA for the target FA, and target FA address if it is different than the CoA. In addition
15 to target FA-CoA, current FA-CoA is included in the message.

16 **STEP 4**

17 The PMIP Client verifies that the current FA-CoA indeed matches the FA on its record, and starts the MIP
18 registration with the target FA by sending *FA_Register_Req* message. This message contains a fully formed RRQ
19 according to RFC3344, with CoA field in the RRQ set to the CoA of the Target FA which is received in
20 *Anchor_DPF_Relocate_Req* message in step3. The source address of the RRQ is that of the MS and the destination
21 address the CoA or the FA if FA address is different from CoA. In addition, *FA_Register_Req* message contains the
22 FA-HA MIP key if this key is used. This message is sent to the Target ASN, whose address was identified as the
23 source address of the *Anchor_DPF_Relocate_Req* message in step3.

24 **STEP 5**

25 The target FA relays the RRQ to the HA.

26 **STEP 6**

27 The HA responds with the RRP.

28 **STEP 7**

1 The target ASN relays the MIP RRP encapsulated in an *FA_Register_Rsp* message to the PMIP Client. The PMIP
2 Client updates the FA in its record.

3 **STEP 8**

4 The target ASN also replies to the source ASNa with a Anchor_DPF_*HO_Rsp* message indicating a successful FA
5 relocation. The source ASNa can then remove the mobility binding, DHCP context information and the R4 data path
6 towards the ASNb.

7 **7.8.1.8.6   Proxy-MIP Session Termination**

8 In case of MS session termination the corresponding R3 mobility session has to be released.

9 An MS can either gracefully terminate its ongoing IP connection (e.g. by sending a DHCP release) or a session
10 termination can be caused by an error condition.

11 Typical error conditions could be, MS out of coverage, low battery, system error, etc.

12 Criteria for initiating a R3 session release are not covered in this section.

13 The proxy MIP client will receive a session release trigger from an ASN functional entity, or the MIP Revocation
14 from HA.

15 The R3 Mobility session is released by sending a MIP registration with a lifetime of zero.

16
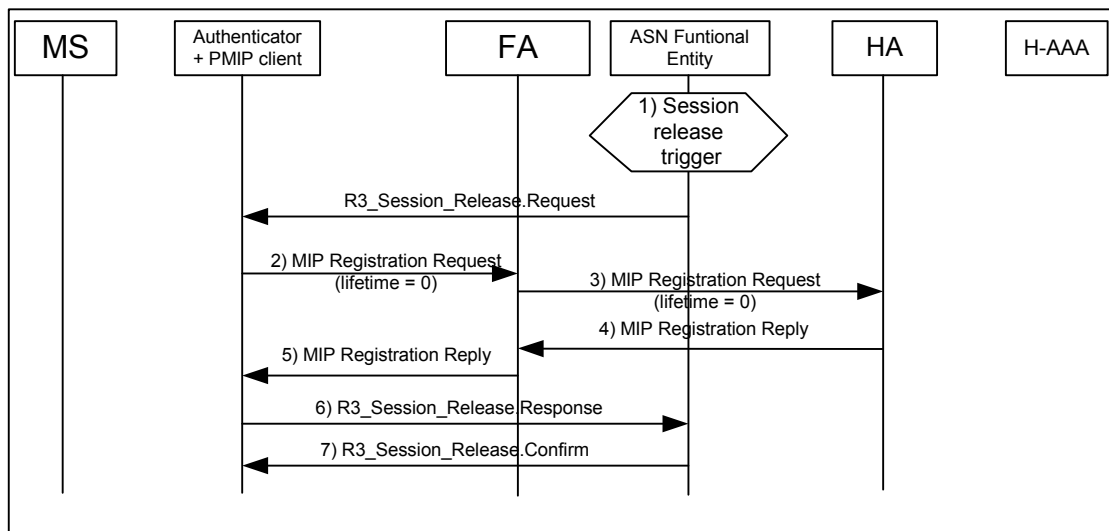
17 **Figure 7-66 - R3 Session Release**

18 For charging and accounting purposes the HA MAY optionally send an AAA Accounting message to the MS's H-
19 AAA server.

20 Note that R6 or R4 session termination is not covered by the signaling flow illustrated in Figure 7-66.

21 After receiving the R3_Session_Release.Request message from the ASN Functional Entity, the PMIP client SHALL
22 release the tunnel associated with the MS. In addition, the PMIP client SHALL notify the ASN functional entity to
23 update the MS session context.

24 If there are more than one session identifiers contained in the R3_Session_Release.Request message, the PMIP
25 client SHALL repeat the same steps for each session contained in the R3_Session_Release.Request.

26 **7.8.1.9   Client MIP R3 Mobility Management**

27 This section describes requirements and procedures for the CMIP R3 mobility management.

1   Figure 7-67 provides an example of an MS with multiple wireless and wired access options. The depicted stack can
2   support handoff across different access technologies. In the following discussion we only address R3 mobility for
3   IEEE 802.16 access links. For release one, Inter-technology handovers are outside the scope of R3 mobility.

4
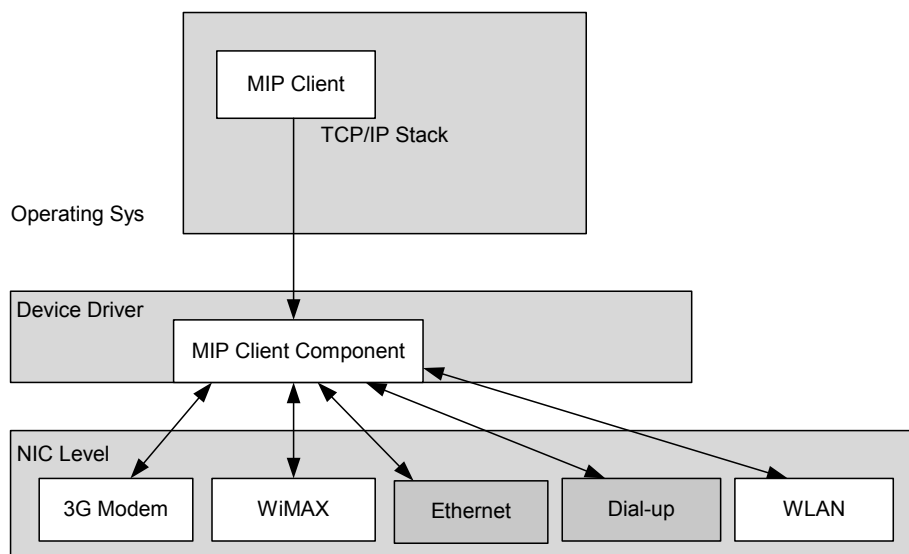
5   **Figure 7-67 - MS with Mobile IP Stack and Multiple Access Options**

6   At the time of the initial MIP session establishment, when new R6 tunnel is established between the Data Path
7   Function at the ASN-GW and the Data Path Function in the new target BS, the MIP client receives a mobility
8   trigger in the form of new MIP advertisement from the FA.

9   The FA is located at the boundary of the ASN and the CSN and terminates the R3 Reference Point within the ASN.
10   The MIP client is a single entity that supports R3 mobility for a single user and is located above the 802.16 drivers
11   and can be an integral part of the OS stack. Such client typically includes multiple components (modules) that MAY
12   span various stack elements as shown above.

13
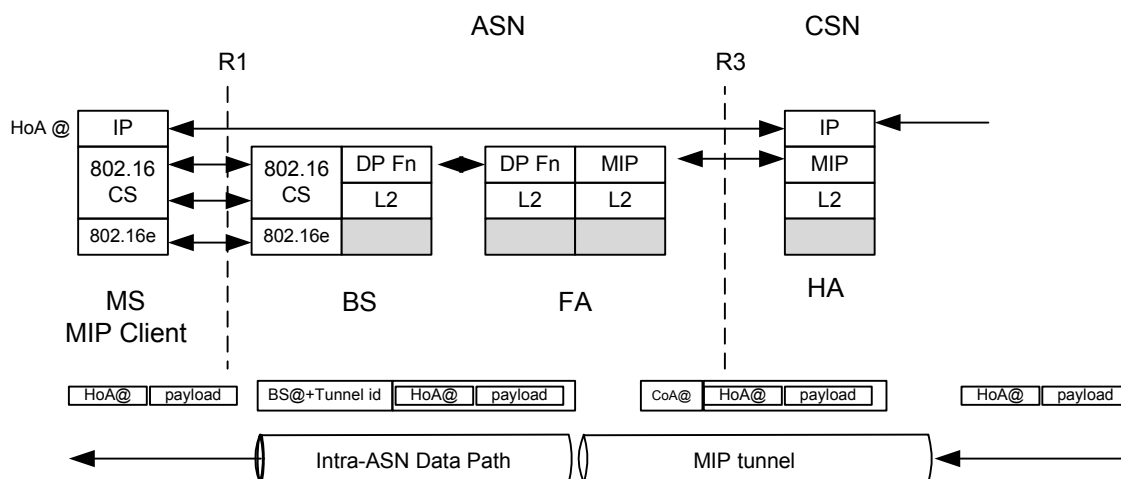
14   **Figure 7-68 - Mobile IP Data Plane (Example)**

MIP			MIP	MIP	MIP
UDP			UDP		UDP
IP			IP	IP	IP
CS	CS	L2 / Intra-ASN Data Path	L2 / Intra-ASN Data Path	L2	L2
802.16 MAC	802.16 MAC				
802.16 PHY	802.16 PHY	PHY	PHY	PHY	PHY
MS	BS		FA		CSN/HA
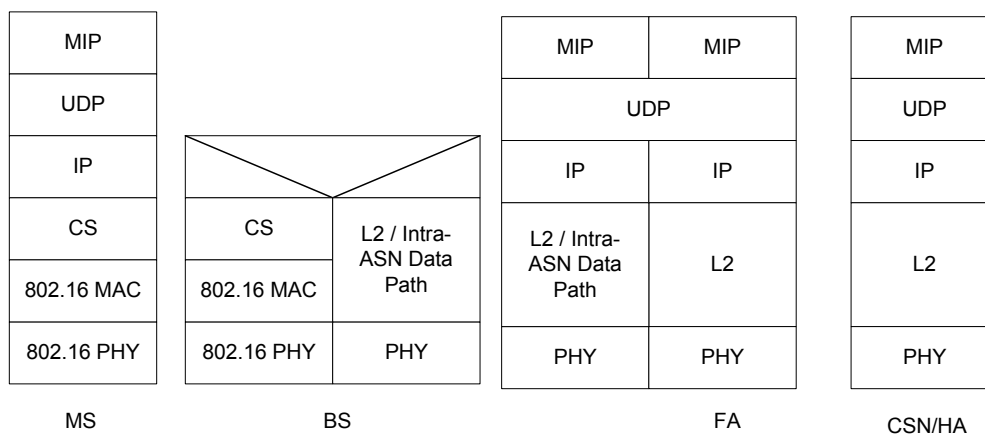
Figure 7-69 - Mobile IP Control Plane

The MIP client in the MS participates in the message exchanges required to perform inter-ASN and inter-NAP mobility. The MIP client supports dynamic address assignment and dynamic HA allocation. To support unambiguous detection of the MS' capabilities and determination of use of CMIP versus PMIP for Ipv4, the use of co-located CoA mode with CMIPv4 (when used only with the WiMAX interface), SHALL NOT be supported in this specification. When the MIP client is involved in inter-technology handoffs, the use of Collocated CoAs (CCoA) is allowed in association with access interfaces different than IEEE 802.16.

7.8.1.9.1   Client-MIP Connection Setup Phase

Upon successful access level authentication, the MS obtains the AAA-Key/MSK and EMSK. When HA address is not assigned, the MS can obtain the HA address as part of the Mobile IP registration messages exchange.

The following signaling flow describes the connection setup phase:
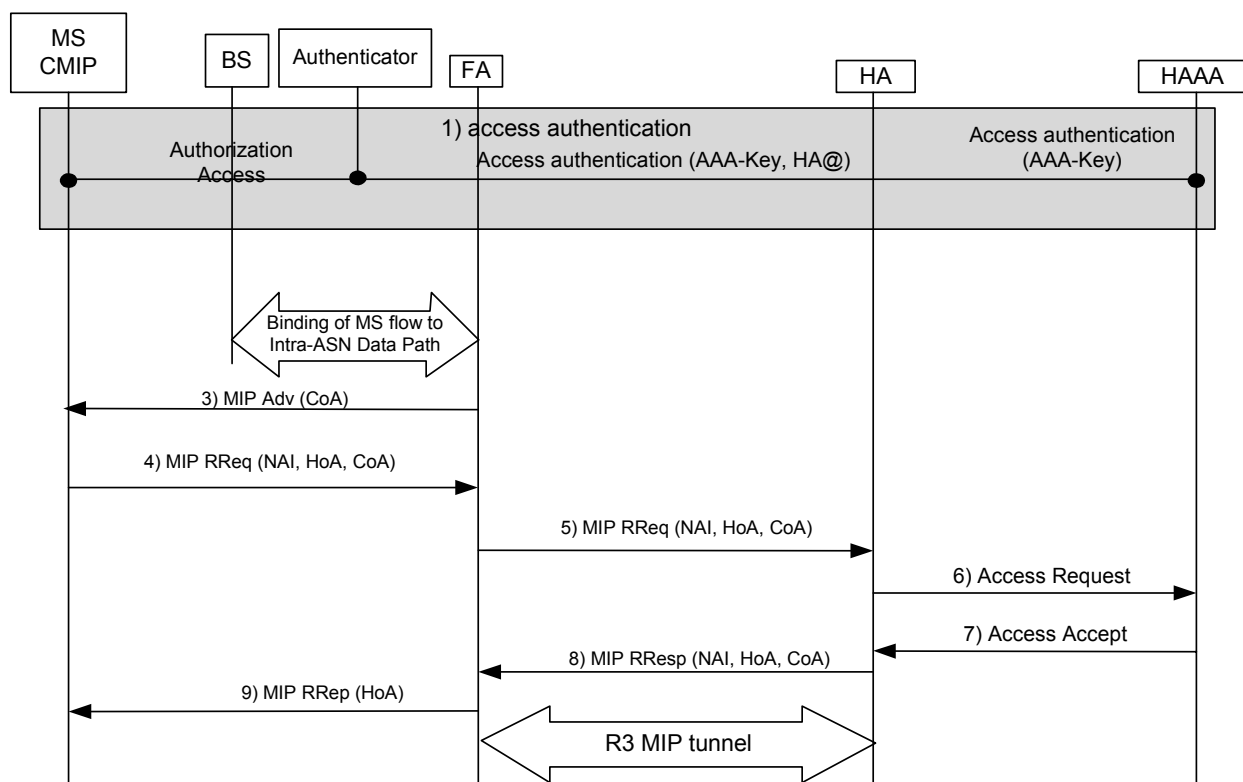
Figure 7-70 - Connection Setup

Step 1) Access Authentication: During access level authentication the AAA authentication key is retrieved from the AAA access authentication message exchanged with the MS home AAA server.

Step 2) A trigger is generated when binding of MS or MS flow with intra-ASN Data Path is established.

Step 3) When new intra-ASN Data Path is established configurable number of advertisements is sent to the MS.

Step 4-5) The MIP registration is performed by the client and forward to the HA. MS using Mobile IP connectivity will not issue DHCP requests and will only use MIP signaling to obtain its home address.

Step 6) HA sends RADIUS Access-Request message to Home AAA.

Step 7) Upon receipt of a RADIUS Access-Request message from a HA containing the MN-HA attribute, the RADIUS server SHALL send a RADIUS Access-Accept message containing the MN-HA shared key encrypted. If registration request included dynamic HA assignment and IP host configuration the HA address and the IP configuration will be respectively returned by the AAA as well.

Step 8) The HA forwards the Registration Reply to the FA.

Step 9) MIP Registration Reply is forwarded to the MS containing the MS home address.

IP Host configuration: The MS MAY use extensions defined in draft-bharatia-mip4-gen-ext-01.txt in the MIP Registration Reply to obtain its IP host configuration.

7.8.1.9.2 Client MIP Session Renewal

To update session state in the network and allow a context release in case of SS/MS or network failure the MIP context SHALL be renewed. The client sends Mobile IP re-registration messages to the FA according to [43]. Upon receiving the re-registration request the HA will reset the MIP session timer. Authentication is based on the prior keys obtained during initial authentication and as such do not require a synchronization with the user authentication server. The following depicts the message flow. If MN-FA is used, the challenge used by the MS for re-registration SHOULD be the one last sent by the prior MIP registration/re-registration response. On re-registration, the FA

1 MAY communicate user FAC authentication information to the Home AAA Server. The frequency of this re-
2 authentication and re-authorization is configurable.

3
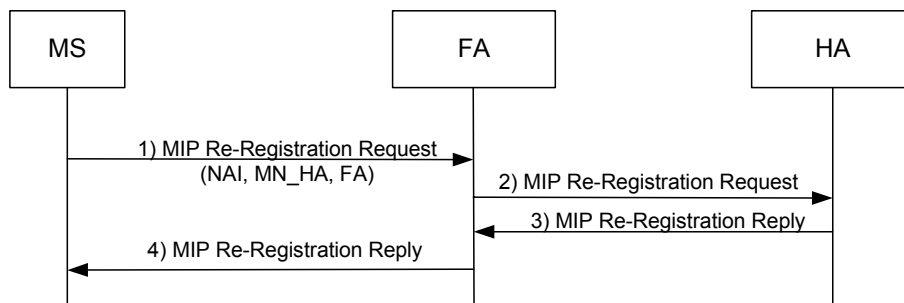
4 **Figure 7-71 - Session Renewal, MIP Re-Registration**

5 7.8.1.9.3 Client MIP CSN Anchored Mobility Management

6 As previously mentioned, MIP R3 mobility handovers are always network initiated. Even when the mobile initiates
7 the handover to a new BS and FA, the R3 mobility is a result of a network event that strives to minimize impact on
8 real time traffic when migration R3 from anchored to target FA. The R3 mobility trigger is typically a delayed event
9 to the FA re-anchoring procedure described in 7.8.1.10.

10 7.8.1.9.4 Foreign Agent Advertisement

11 When a new MS or a service flow within MS is initially bound to an intra-ASN Data Path, the FA begins the
12 transmission of configurable number of Agent Advertisements to the MS. Once the configurable number of Agent
13 Advertisement is sent, the FA will not send more Advertisement. Only when the MS sends Agent Solicitation
14 message the FA will respond with an Agent Advertisement. When the first MIP Registration Request is received by
15 the FA, it SHALL cease sending Agent Advertisements even if the number sent is less than the configurable number
16 of Agent Advertisements.

17 In order to minimize Agent Advertisement sent over the air, the FA SHOULD not send unsolicited Agent
18 Advertisements to the MS to refresh the advertisement lifetime. The MS MAY send Agent Solicitation when the FA
19 advertisement lifetime expires or about to expire. The advertisement lifetime is a configurable value and can be set
20 to the maximum value of 9000 seconds (the maximum ICMP advertisement lifetime).

21 7.8.1.9.5 Client-MIP Session Termination

22 In case an MS active IP session has to be terminated, both the MAC state as well as intra-ASN Data Paths between
23 the FA and the HA has to be gracefully removed.

24 The four termination scenarios are as follows:

25 (1) An MS initiated graceful termination: a session is gracefully terminated by sending a MIP Registration Request
26 message with lifetime = 0. This termination is triggered either by the user or MS being in an error conditions
27 such as low battery power, etc.

28 (2) ASN initiated graceful termination: The conditions for ASN initiated termination MAY be some error
29 conditions with respect to the MS such as the MS being identified as a rogue MS with security violations,
30 planned maintenance, etc. This scenario is depicted in Figure 7-73. A session is gracefully terminated by
31 sending an R3_Session_Release.Request message from an ASN Functional entity like the intra-ASN Handover
32 function. After receiving the R3_Session_Release.Request message from an ASN Functional entity, the FA
33 SHALL trigger registration revocation procedure with HA to terminate binding as per RFC 3543.

1
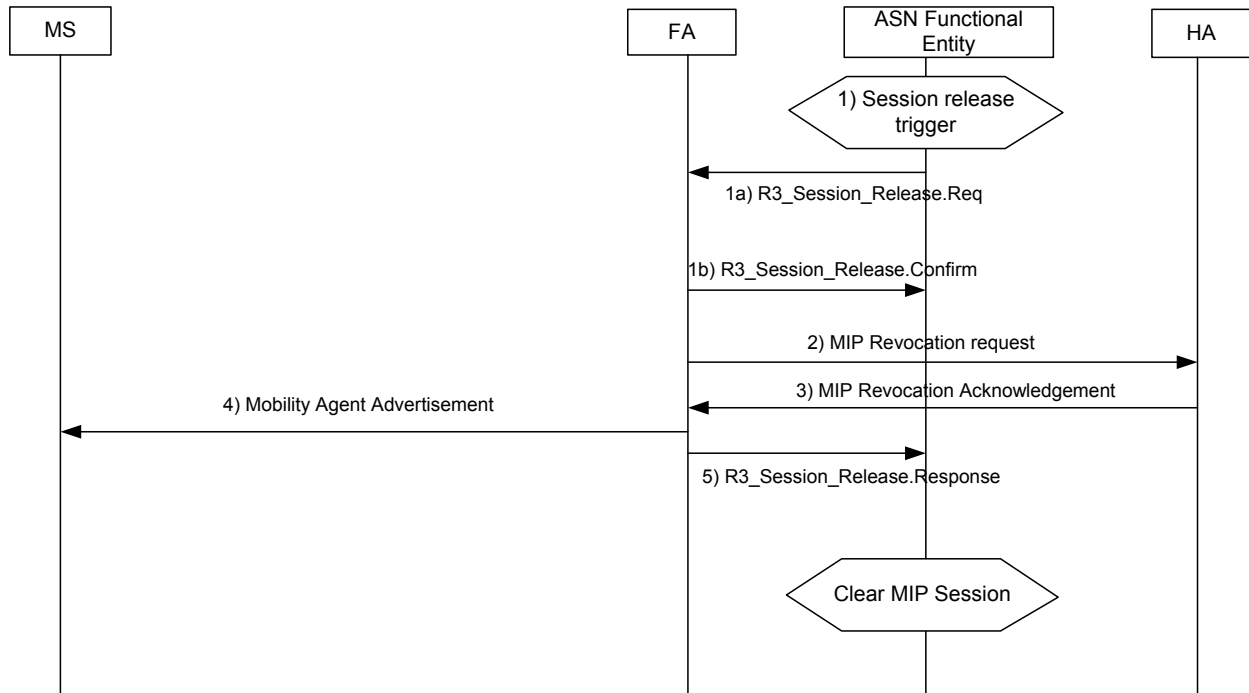
Figure 7-72 - ASN Initiated Graceful Termination

4) HA initiated graceful termination: This scenario is depicted in Figure 7-74. A session is gracefully terminated when HA triggers registration revocation with FA as per RFC 3543. FA sends the R3_Session_Release.Request to ASN Functional to notify termination of mobility binding. MS may be informed depending on if the I bit is set in Revocation message.
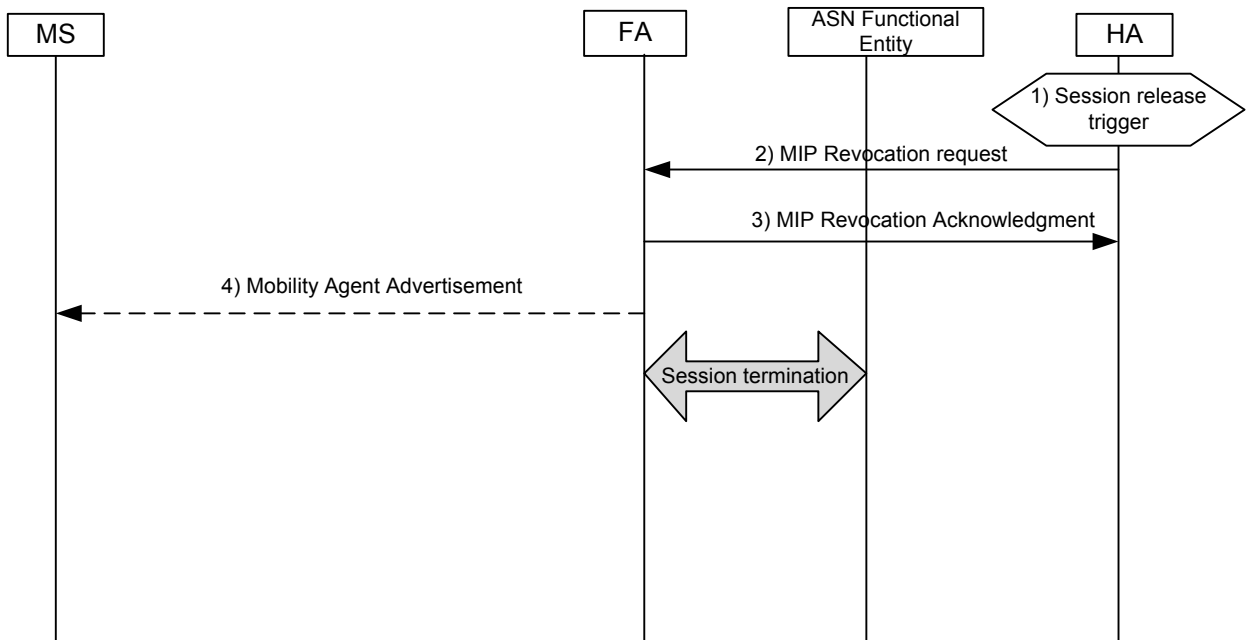
Figure 7-73 - HA Initiated Graceful Termination

1   5)   MS loss of carrier unconventionally termination: the scenario when the BS detects the MS is loss of carrier
2   unconventionally, the BS SHALL inform ASN Function Entity by sending an *Path_Dereg_Req* with
3   operation reason as "MS loss of carrier". Then, if the SFA and Data Path Function of ASN Function Entity
4   make a decision to release R3 and the related R6 or R4 resource, it SHALL inform the FA to release the
5   HA to unbind the PoA address of the MS by sending Path_Dereg_Req, thus the session is terminated. This
6   scenario is depicted in Figure 7-75. At the same time, in this scenario, ASN Function entity can release
7   ASN resource for the MS, such as intra-ASN data path etc.

8
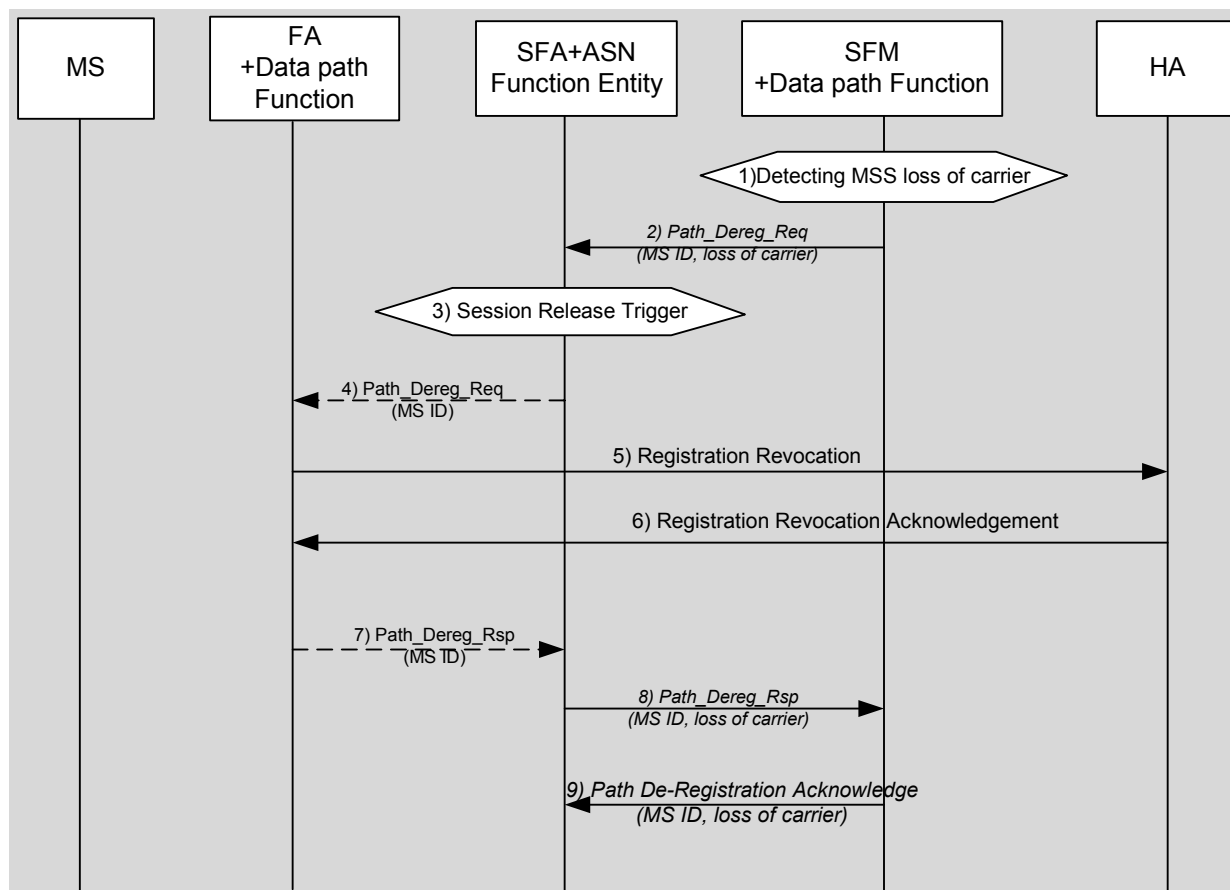
9   **Figure 7-74 - MS Loss of Carrier Unconventionally Termination**

10   **7.8.1.10 CSN Anchored Mobility Management to ASN-Anchored Mobility Management**
11   **Relationship**

12   This section describes a possible link between ASN-anchored mobility and CSN Anchored Mobility Management
13   and is meant as informational. Actual implementations can differ from the option described below.

14   Figure 7-75 illustrates the two major handover types described above from both an architecture and functional
15   perspective. The top of the Figure shows ASN1 anchoring R3 and forwarding bearer traffic to ASN2 over R4
16   (labeled before) followed by an R3 relocation message that relocates R3 bearer traffic from ASN1 to ASN2 (labeled
17   after). The bottom part shows a combined CSN -anchored mobility handover events where R3 is relocated from
18   ASN1 to ASN2 without a prior ASN anchoring. Combined CSN/ASN-anchored mobility handovers is normally
19   triggered by an MS mobility event like running into coverage of a new Base Station, although these handover can
20   also be a result of a resource optimization decision. The dotted line represent the initial state before a handover, the
21   solid line depicts the data path after a combined R3/R6 handover.

1   The top part of Figure 7-75 illustrates a typical RRM based handover that results in both an ASN Anchored Mobility
2   where traffic is forward from ASN1 to ASN2 followed by a CSN-anchored mobility handover where R3 is relocated
3   from ASN1 to ASN2.

4   In case of an RRM based handovers the R3 handover request is never sent directly from the RRM controller to the
5   mobility manager but will be passed through the ASN Handover Function. This approach facilitates synchronization
6   between the different ASN functional elements. Additionally it makes the R3 mobility transparent to the RRM
7   management.

8
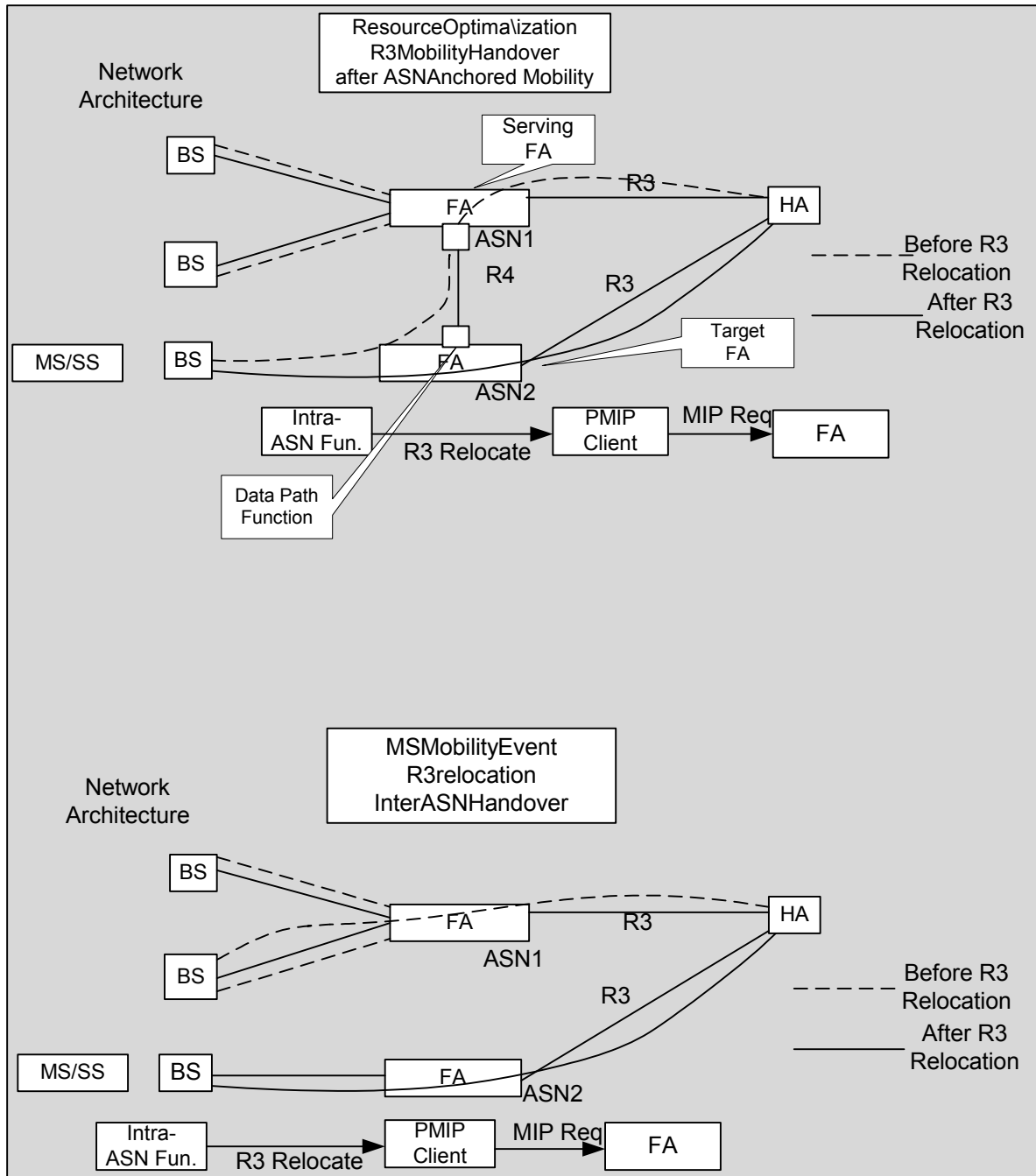
9   **Figure 7-75 - R3MM to Intra-ASN Mobility Relationship**

1　From ASN-anchored mobility management perspective, there are two scenarios exist where an R3 handover can be
2　initiated. The first scenario is during an ASN-anchored mobility handover event, e.g. upon receiving an HO-
3　indication message at the ASN Functional entity. The second scenario (which is preferred) is to initiate an R3
4　handover after the ASN-anchored mobility handover has been successfully executed, e.g. when the ASN Functional
5　Entity receives a '*Anchor_DPF_Relocate_Req*'. Triggering an R3 handover after the ASN-anchored mobility
6　handover has been fully processed avoids scenarios where an R3 handover needs to be cancelled and the old
7　connection is reestablished due to unsuccessful ASN-anchored mobility.

8　Applying ASN data forwarding prior and during the time it takes to complete an R3 handover minimizes packet loss
9　and handover interruption time. After the new R3 path has been established the PMIP mobility manager will notify
10　the ASN Functional Entity by sending an '*Anchor_DPF_Relocate_Rsp*' message.

11　The *Anchor_DPF_Relocate_Rsp* message can be used by the ASN Functional Entity to terminate inter-ASN data
12　forwarding between the old and new ASN.

13　**7.8.1.11　CSN Anchored Mobility Management Trigger Primitives**

14　Table 7-2 lists the messages involved in R3 mobility. Note that these messages MAY be exchanged between
15　functional entities within a single ASN, or between functional entities in different ASNs.

16　**Table 7-2 - R3MM Mobility Management Primitives "for information only, the binding facts are**
17　**defined in the Stage3 Spec"**

Primitives	From => To	Message Content	Applicability CMIP/PMIP
HoA_Address	DHCP Proxy => PMIP Client	MSID, HoA @, Transaction ID	PMIP
HoA.Address.Ack	PMIP Client => DHCP Proxy	MSID, Status, [error code], Transaction ID, Status	PMIP
DHCP_Gating.Release	PMIP Client => DHCP Proxy	MSID, Transaction ID	PMIP
R3_Session_Release.Request	ASN-Fn => PMIP Client ASN-Fn => FA	MSID, list of (status (Successful, Failed), [Error Code]) attributes, Transaction ID	PMIP CMIP
R3_Session_Release.Response	PMIP Client => ASN-Fn FA => ASN-Fn	MSID, list of (MIP session ID, status (Successful, Failed), [Error Code]) attributes, Transaction ID	PMIP CMIP
R3_Mobility_Context	DHCP Proxy => ASN-Fn FA => ASN-Fn	MSID, R3 Mobility Mode, Transaction ID	PMIP CMIP
R3_Mobility_Context.Ack	ASN-Fn => DHCP Proxy ASN-Fn => FA	MSID, Transaction ID, Status (Successful, Failed), [Error Code]	PMIP CMIP
Anchor_DPF_Relocate_Req	ASN-Fn => PMIP Client ASN-Fn => Target FA	MSID, Target FA, Transaction ID	PMIP CMIP
R3_Relocate. Confirm	PMIP Client => ASN-Fn FA => ASN-Fn	MSID, Transaction ID	PMIP CMIP
Anchor_DPF_Relocate_Rsp	PMIP Client => ASN-Fn	MSID, Transaction ID	PMIP

Primitives	From => To	Message Content	Applicability CMIP/PMIP
	Target FA => ASN-Fn		CMIP

7.8.1.11.1 HoA_Address

The HoA_Address message provides the HoA address retrieved from the CSN to the PMIP client.

As described in the session setup paragraph the HoA address can be provided during the access authentication as part of the AAA exchange or can be retrieved for a DHCP server in the CSN network.

- **MSID**: identifies the MS for which an R3 handover is requested.

- **HoA Address**: Home address of the MS.

- **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together with the MS uniquely identifies a request

7.8.1.11.2 HoA_Address.Ack

A HoA_Address.Ack is send by the PMIP Client upon successfully receiving the HoA_Address message.

- **MS ID:** identifies the MS for which an R3 handover is requested.

- **Transaction ID:** Correlates the replies with the correct request. To match Replies with Requests the Transaction ID in the reply SHALL match the Transaction ID in the Request

- **Status:** Indicates whether or not the HoA_Address message was successful received.

  o In case of failure an additional error code identifying the reason of failure can be added (e.g., unknown MS ID).

7.8.1.11.3 R3_Session_Release.Request

An R3_Session_Release.Request will terminate the R3 MIP session for a specific MS.

- **MS ID**: identifies the MS for which an R3 handover is requested.

- **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together with the MS uniquely identifies a request.

7.8.1.11.4 R3_Session_Release.Response

The R3_Session_Release.Response message indicates either a successful or failed R3 handover event in response of an R3_Release.Request.

- **MS ID:** identifies the MS for which an R3 handover is requested.

- List of (Status (Successful, Failed), [Error Code]) attributes: Optionally list the MIP session to be released event result.

- **Status:** Indicates whether or not the R3 handover was successful.

  o In case of failure an additional error code identifying the reason of failure can be added.

- **Transaction ID**: Correlates the replies with the correct request. To match Replies with Requests the Transaction ID in the response SHALL match the Transaction ID in the Request

7.8.1.11.5 R3_Mobility_Context

The R3_Mobility_Context is used to inform the ASN Functional Entity whether the MS is in Proxy-MIP or CMIP mode. Additionally some R3 context information can be added. This information is used by the ASN Function Entities to determine the correct moment in time to trigger an R3 handover request plus the correct destination of the message (e.g. FA or PMIP mobility manager).

1   •   **MSID**: identifies the MS for which an R3 handover is requested.

2   •   **R3 Mobility Mode**: Indicates the R3 mobility the MS is using. The field can take two values, either
3   CMIPv4, CMIPv6 or PMIPv4.

4   •   **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together
5   with the MSID uniquely identifies a request.

6 **7.8.1.11.6 R3_Mobility_Context.Ack**

7 An R3_Mobility_Context.Ack is send by the ASN Functional Entity upon successfully receiving the
8 R3_Mobility_Context message.

9   •   **MSID**: identifies the MS for which an R3 handover is requested.

10   •   **Transaction ID**: Correlates the replies with the correct request. To match Replies with Requests the
11   Transaction ID in the response SHALL match the Transaction ID in the Request

12   •   **Status**: Indicates whether or not the R3_Mobility_Context message was successful received.
13   In case of failure an additional error code identifying the reason of failure can be added (e.g. unknown
14   MSID).

15 *7.8.1.11.7 Anchor_DPF_Relocate_Req*

16 R3 *Anchor_DPF_Relocate_Req*s are used to trigger an R3 handover. R3 *Anchor_DPF_Relocate_Req*s can be
17 triggered by the resource management function or other network entities.—Upon receiving an R3
18 *Anchor_DPF_Relocate_Req*, the ASN Functional Entity will send a R3_Relocation.Request to the ASN Functional
19 Entity and start R3 handover procedure.

20   •   **MSID**: identifies the MS for which an R3 relocate is requested. The MSID is based on the MS's NAI. In
21   PMIP the MS identifies a specific PMIP client in the PMIP client.

22   •   **Target FA**: Identifies the new R3 anchor point for the MS. In MIP terminology the Target FA address
23   corresponds to the FA's CoA address.

24   •   **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together
25   with the MSID uniquely identifies a request.

26 **7.8.1.11.8 R3_Relocate.Confirm**

27 R3_Relocate Confirm is used to acknowledge successful receipt of the R3 *Anchor_DPF_Relocate_Req* message.
28 The confirmation does not give any feedback on the actual processing or state of the R3 relocation.

29   •   **MSID**: identifies the MS for which an R3 relocate is requested. The MSID is based on the MS's NAI. In
30   PMIP the MS identifies a specific PMIP client in the PMIP client.

31   •   **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together
32   with the MSID uniquely identifies a request.

33 *7.8.1.11.9 Anchor_DPF_Relocate_Rsp*

34 The R3 *Anchor_DPF_Relocate_Rsp* message indicates either a successful or failed R3 relocate event in response of
35 an R3 *Anchor_DPF_Relocate_Req*.

36   •   **MSID**: identifies the MS for which an R3 relocate is requested. The MSID is based on the MS's NAI. In
37   PMIP the MS identifies a specific PMIP client in the PMIP mobility manager.

38   •   **Target FA**: Identifies the new R3 anchor point for the MS. In MIP terminology the Target FA address
39   corresponds to the FA's CoA address.

40   •   **Transaction ID**: Random generated number to correlate request and response. The Transaction ID together
41   with the MSID uniquely identifies a request.

1 **7.8.1.12 Proxy-MIP and Client MIP Coexistence**

2 R3 mobility can be provided based on two mechanisms:

3 • Client MIP solution based on a MIP client in the MS.

4 • Proxy MIP solution based on MIP client in the network.

5 Both solutions are based on a different network and SS/MS behavior and therefore require special consideration to
6 support both on the same network. Which R3 mobility scheme is used depends on a number of factors like SS/MS
7 type, MIP client availability, inter-technology handovers support, type of operator, roaming considerations, etc.

8 In order to be able to accommodate for any type of SS/MS and inbound roamer a network SHOULD ideally be able
9 to support both the CMIP and PMIP R3 mobility schemes.

10 With both PMIP and CMIP being mandatory from network point of view several scenarios can be identified, the
11 table below gives a short overview of the different possibilities. Table 7-3 only covers R3 mobility, fallback options
12 to nomadic access based on network capabilities or operator policies are not covered.

13 **Table 7-3 - R3MM coexistence scenarios**

MS support	Network Support	Decision
MIP	CMIP	CMIP
Simple-IP	PMIP	PMIP
MIP	CMIP + PMIP	CMIP
Simple IP	CMIP + PMIP	PMIP
MIP	PMIP	Not Applicable
Simple-IP	CMIP	Not Applicable

14 The Coexistence solution focuses on the following points:

15 • **MS capability discovery**. A MS can be categorized as either a simple IP SS/MS or a MIP enabled MS. A
16 simple IP SS/MS can be any IP SS/MS using DHCP for IP address assignment.

17 • **Supported network mobility schemes discovery**. Based on some of the arguments listed above an
18 operator might decide to only support PMIP or CMIP or both schemes.

19 • **R3 mobility scheme selection**. Once both the SS/MS and network capabilities are known the correct R3
20 mobility scheme needs to be activated.

21 **7.8.1.13 Coexistence for Networks Supporting Both CMIP and PMIP**

22 This specific coexistence scenario deals with networks that are able to support both simple IP SS/MSs as well as
23 Mobile-IP enabled MSs.

24 Which scheme the network applies will depend on the SS/MS capabilities and can additionally be imposed by the
25 Home-NSP based on the knowledge of both the SS/MS capabilities and NAP mobility support.

26 If the Home NSP is unable to determine the SS/MS capabilities or the network supported R3 mobility schemes the
27 home AAA-server will provide both the necessary PMIP and CMIP information to the ASN during the Access
28 Authentication phase.

29 Prior to an intra-ASN data path establishment the network is unaware of the MS capabilities, so immediately after
30 the data path between ASN-located FA and MS is established, the FA entity will send an FA advertisement to the
31 SS/MS over this newly established data path. If the SS/MS is MIP enabled it will perform a MIP registration using
32 the CoA advertised in the FA advertisement.

1 The MIP registration originated from the MS will force the network into CMIP mode.

2 A MS without MIP functionality (simple IP SS/MS) will discard the FA advertisement and send a DHCP request to
3 get an IP address. The DHCP request will trigger the PMIP Mobility Manager – HoA_Address message – to setup
4 an R3 session on behalf of the MS.

5 So for networks supporting both CMIP and PMIP the selection is straightforward and driven by the SS/MS.
6 Network capability discovery is based on MIP agent advertisement messages send just after connection setup. The
7 mobility scheme selection is determined by the ASN, based on the type of message received from the SS/MS and
8 can be either a DHCP request or a MIP registration request.

9 To avoid situations where due to loss of the FA advertisement message or unexpected delays a MIP client would go
10 into collocated CoA mode the MIP client needs to be configured such that collocated CoA mode is prevented for the
11 WiMAX interface. In collocated CoA mode, the MIP client will send a DHCP request to retrieve the co-located care
12 of address, this message will be wrongly interpreted by the network as a request to establish a PMIP session.

13 After initial R3 session setup the ASN network stores the current R3 Mobility mode the SS/MS is in.

14 The R3 mobility mode needs to be stored at the ASN Functional Entity. Based on this information the ASN
15 Functional entity can determine the right moment and destination to send an R3 *Relocation_Req* to. Knowledge of
16 the R3 mobility mode will also prevent unnecessary air-overhead by suppressing FA advertisements after every
17 handover in case of PMIP users.

18 For MIP enabled SS/MSs the R3 mobility trigger will be send directly to the FA, for PMIP user the R3 mobility
19 trigger will be sent to the PMIP mobility manager.

20 **7.8.1.14 R3 Mobility Session Authentication and Authorization**

21 **7.8.1.14.1 Proxy-MIP Security**
22 The following section describes the elements of the PMIP security framework and their interaction to dynamically
23 establish a PMIP key to enable a Proxy Mobile IP client and Home Agent (HA) exchange authenticated registration
24 requests and response messages.
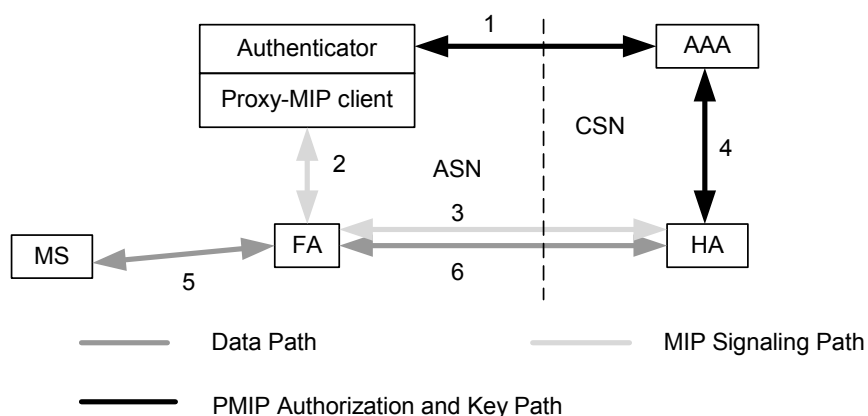
26 **Figure 7-76 - PMIP Functional Elements**

27 Figure 7-76 shows the function elements related to PMIP. During network entry the mobile node (MS) authenticates
28 to the AAA via an authenticator, using an EAP authentication process. At the end of the exchange, if the
29 authentication is successful, the AAA server sends an EAP success and a notification of authorization for PMIP
30 process to the authenticator. At this point the Authenticator obtains the PMIP Key. The AAA server SHALL send
31 the SPI, lifetime and any other PMIP related information (such as HoA, HA IP address, and so on, if desired) along
32 with the authorization notification for PMIP. The lifetime of this key SHALL be the same as that of the MSK that is
33 generated as a result of successful authenticator. The Authenticator SHALL share the PMIP key and related
34 information with the Proxy-MIP client. The Proxy Mobile Node (PMN) MAY use this key for the lifetime of the

1 key, i.e. additional registration requests MAY be generated using the same Proxy-MIP Client when the lifetime of
2 the registration expires or when the MS moves to a new subnet requiring a new registration.

3
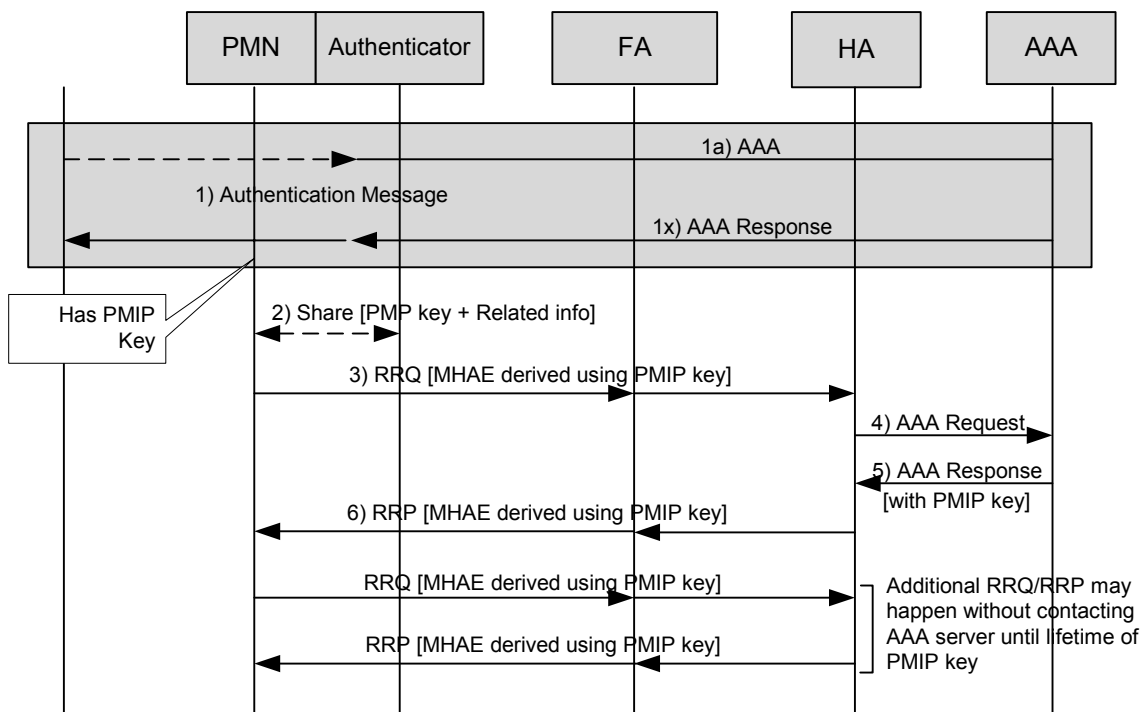
4 **Figure 7-77 - PMIP Key Generation and Transfer – Message Sequence**

5   a) During network entry the mobile node (MS) authenticates to the AAA via the authenticator, using an EAP
6   authentication process. This MAY take multiple steps and at the end of successful authentication the
7   authenticator obtains the PMIP Key. Note that the PMIP key that is obtained by the authenticator is in
8   addition to the MSK that is provided by the AAA server as a result of EAP.

9   b) The PMN function obtains the key and related information from the authenticator function.

10 c) When the PMN generates a registration request (Registration Request) it uses the PMIP key to create the
11   Mobile-Home Authentication Extension (MHAE) to authenticate the registration request to the HA. The
12   PMN MAY include the NAI extension in the Registration Request

13 d) When a HA receives a registration request, if it does not have the SPI/keys corresponding to the MN, it
14   queries the AAA server via an AAA Request.

15 e) The AAA server validates the request and sends an AAA Response with the MN-HA key (PMIP key)
16   corresponding to the Proxy-MIP Client that is identified in the Request. After receiving the PMIP key, the
17   HA validates the MHAE in Registration Request, and processes the Registration Request and generates a
18   registration response with a valid authentication extension using the same MN-HA key.

19 Further exchanges of Registration Request and Registration Reply can happen without contacting the AAA server
20 until the expiration of the MN-HA key.

21 **7.8.1.14.2 Client-MIP Security**

22 **7.8.1.14.2.1 Client MIP Authentication**

23 For Mobile Ipv4 authentication MN-HA and FA-HA authentication are mandatory, MN-FA authentication is
24 optional. MN-HA and MN-FA keys are derived from EAP EMSK

7.8.1.14.2.2 AAA Support

7.8.1.14.2.2.1 RADIUS Support

If using MN-FA challenge extension according to [28], the FA SHALL act as a RADIUS client in accordance with [23]. Upon initial MS access, the FA SHALL communicate user MN-FA Challenge extension information to a RADIUS Server, via the broker RADIUS servers if required, in a RADIUS Access-Request message. Upon receipt of the Registration Request from the MS, and if the SPI in the MN-AAA Authentication Extension is set to CHAP-SPI, the FA SHALL create a RADIUS Access-Request message.

If the SPI in the MN-AAA Authentication Extension is set to CHAP-SPI as per [28], the FA SHALL use MD5 when computing the CHAP challenge. If the authentication succeeds, the RADIUS server SHALL send a RADIUS Access-Accept message to the FA. If the authentication fails, the RADIUS server SHALL send a RADIUS Access-Reject message to the FA.

7.8.2 R3 Mobility Management with CMIPv6

This subsection describes requirements and procedures for Mobile IP operation with Ipv6 (CMIPv6) [53]. Within the Mobile IP framework, an MS with Mobile IP stack maintains a persistent IP address when handing off between different subnets. Mobile Ipv6 provides the user IP routing service to a NSP's network.

CMIPv6 is different from CMIPv4 ([43]) in many ways. The most obvious differences are the lack of a foreign agent (FA) in CMIPv6, and the support for route optimization (RO) in CMIPv6. Instead of a FA, CMIPv6 uses a co-located care-of-address (CoA) that is in the mobile node, which is then communicated with the HA using a binding update message. The CoA can be derived by the mobile node using several methods; the most common methods are stateless autoconfiguration [16] and stateful configuration using DHCPv6 [42]. Route optimization is another advantage that CMIPv6 has over CMIPv4. It will allow the correspondent node to communicate directly to the mobile node without having to transverse the home network. The mobile node registers its bindings with the correspondent node and then the correspondent node will check its binding cache and can route traffic directly to the mobile node. If the correspondent node cannot support the binding cache, then it will simply route the IP packets to the mobile node's home address and the HA will forward to the CoA.

CMIPv6) is adopted as the preferred mobility management protocol for all applicable usage/deployment scenarios requiring seamless inter-subnet/inter-prefix layer-3 handovers for Ipv6 based SS/MSs. The R3 Mobility solution has four functional components— a MIP client, a Home Agent (HA) typically located in the user's home network (but MAY be dynamically assigned/requested from a visited operator's network), a correspondent node, and a AAA server.

A WiMAX mobile node cannot be connected to its MIPv6 home network. In other words, the MN never directly connects to its Home Link. To ensure macro mobility between ASNs a subnet cannot span multiple ASNs. To work within these restrictions several assumptions need to be made and enforced. They are as follows.

- Each ASN SHOULD be a unique subnet to the Visited CSN

- A MS SHOULD have no more then one (1) MIP "home" network.

- The MIP "Home" network SHALL belong to a CSN domain.

7.8.2.1 CMIPv6 Specific Functional Requirements

- Efficient use of wireless link. Extra overhead over the air-interface to accomplish R3 mobility SHALL be minimized.

- IP address assignment and host configuration SHALL be performed per Section 7.2.2.2 of this document.

- The MIP client SHOULD be located above all physical adaptors and can be integrated into the OS stack.

- To support DAD on the MS's CoA, the ASN-GW which acts as access router SHALL perform proxy DAD function, that maintain all the assigned CoA information and responses to Neighbor Solicitation from MS for DAD,

1 **7.8.2.2   Network Initiated Mobility**

2 R3 Mobility handover procedure is always initiated by the network. The following types of event can trigger the
3 procedure:

4 *1) MS mobility:* The MS hands off to a new Base Station under a new Access Router.

5 *2) Wake-up from idle mode*: The MS wakes up from the idle mode under a different Access Router than the one
6 under which it entered the idle mode.

7 *3) Resource optimization:* The network decides for resource optimization purposes to transfer the R3 endpoint for
8 the MS from the serving Access Router to a new Access Router, independently of any MS movement.

9 **7.8.2.3   CMIPv6 Extensions**

10 The MIPv6 Client SHALL include the NAI Option [59], in all CMIPv6 message.

11 **7.8.2.4   Mobile IPv6 Operations**

12 The following standards SHALL be used for Mobile Ipv6 operation with any limitations or extensions described in
13 this document:

14 • Mobility Support in Ipv6 [RFC 3775]

15 • Mobile Node Identifier Option for Mobile IPv6 [RFC 4285]

16 • Authentication Protocol for Mobile IPv6 [RFC 4283]

17 • draft-ietf-mip6-ikev2-ipsec-08.txt

18 • draft-ietf-mip6-hiopt-02.txt

19 **7.8.2.4.1   Dynamic Home Agent assignment**

20 In roaming cases the Home Agent can be assigned by either the Home NSP or the Visited NSP. It's the home
21 operator that will decide based on the roaming agreement with the visited operator and/or the end-user's
22 subscription profile which network is responsible for assigning the MIPv6 Home Agent.

23 If a Home Agent is assigned in the visited network the MIPv6 authentication will take place between the visited HA
24 and the Home AAA server. The visited AAA proxy is not involved in the MIPv6 security part.

25 If the HA is to be assigned by the Home CSN both the Home Agent address is appended to the AAA reply by the
26 Home-AAA server. For Home Agents in the Visited CSN the AAA proxy can append the Home Agent address to
27 the AAA exchange between the home AAA server and the authenticator.

28 For static agreements between two operator domains (e.g. HA always in the visited network) the AAA proxy can be
29 configured to add a HA address based on the Home-AAA server domain.

30 For more dynamic Home Agent location algorithms (e.g. based on subscription profile) the AAA proxy decision to
31 append to HA address will depend on the presence of the HA address container in the AAA reply from the home
32 AAA.

33 Although not considered very scalable the address of a HA in the visited network can be provided by the home AAA
34 server based on pre-configured information.

35 The Home Agent information can be provided in the form of an IP address or a FQDN. The Home Agent
36 information received from the AAA system is conveyed to the MS via DHCPv6.

37 **7.8.2.5   CMIPv6 R3 Mobility Management**

38 This section describes requirements and procedures for the MIPv6 R3 mobility management.

39 At the time of the initial MIPv6 session establishment, when a new intra ASN Data Path tunnel is established
40 between the Access Router and the new target BS, the MIPv6 client receives new mobile router advertisement
41 messages as defined in section 7.5 of [53] to trigger the MS to perform a new CCoA update and binding update to
42 the HA

1
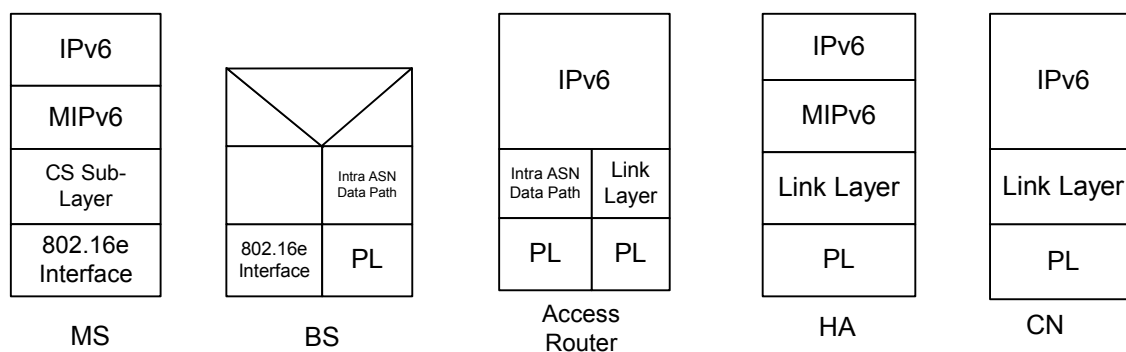
2 **Figure 7-78 - CMIPv6 Data Plane with Tunneling**

3
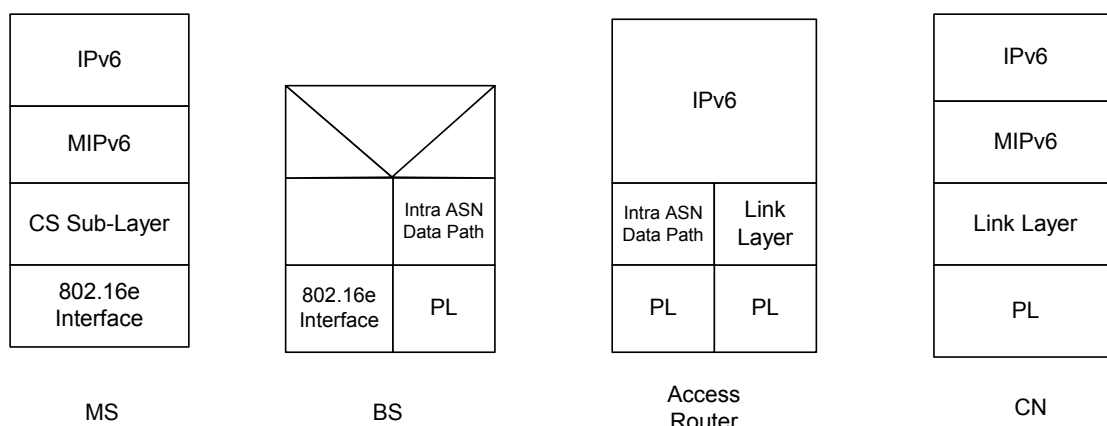
4 **Figure 7-79 - CMIPv6 Data Plane with RO**

5
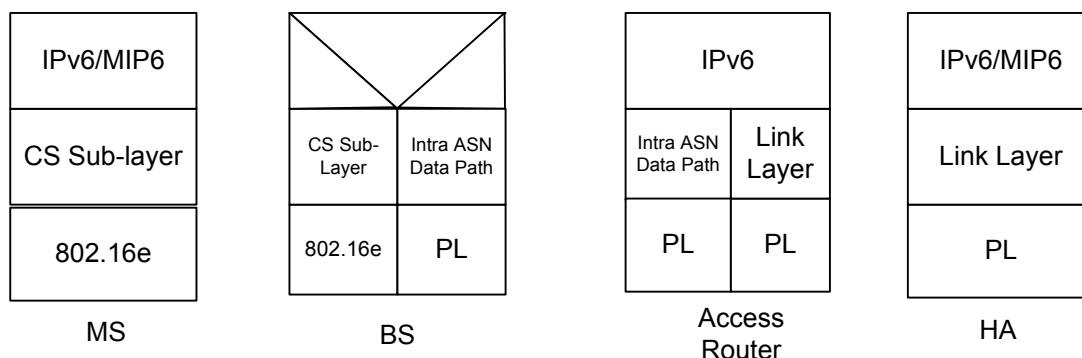
6 **Figure 7-80 - CMIPv6 Control Plane**

7 The MIPv6 client in the MS participates in the message exchanges required to perform anchor CSN mobility. The
8 MIPv6 client supports dynamic address assignment and dynamic HA allocation.

9 **7.8.2.5.1   CMIPv6 Connection Setup and Authentication Phase**

10 In order for the MS to authenticate and authorize with the home network, the MS includes the mobility options
11 carrying the authentication protocol [58]. This type of authentication and authorization allows the MS to perform
12 Home Registration without IPsec. The HA can authenticate and authorize the MS based on other identity credentials
13 that are included in the BU such as the MN-HA authentication mobility option or the MN-AAA authentication
14 mobility options [59].

1   For an initial home registration, the MN uses the MN-AAA authentication mobility option.

2   Upon successful access level authentication, the MS obtains the AAA-Key/MSK and possibly the HA address
3   allocated to the user. When HA address is not assigned, the MS can obtain the HA address as part of the Mobile IP
4   registration messages exchange.

5   The following signaling flow describes the connection setup phase:
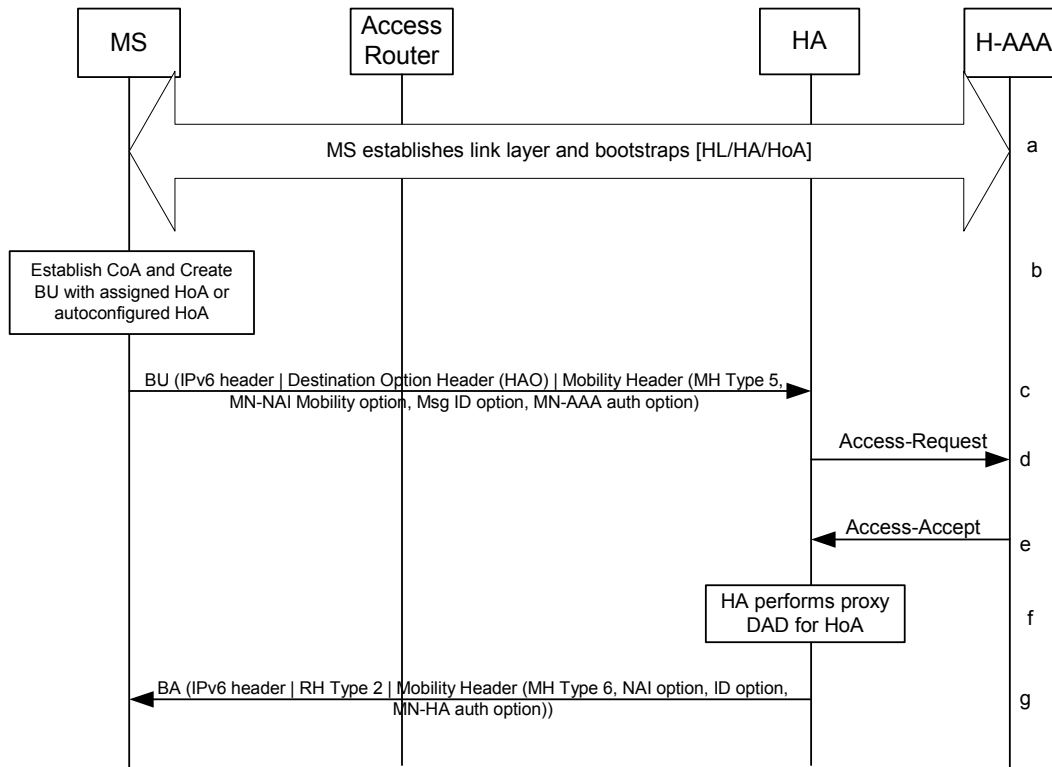
7   **Figure 7-81 - CMIPv6 Connection Setup**

8   a)   The MS performs Link Layer establishment. Optionally, the MS acquires bootstrap information from the
9   Home AAA server (via the Access Router). The MS uses stateless DHCPv6 [51] to obtain the bootstrap
10   information.

11   b)   If the MS is assigned a new HoA in step a, the MS begins to use it. If no HoA was assigned in step a, the
12   MN generates (auto-configure) an Ipv6 global unicast address. It MAY be based on Home Link Prefix
13   information if it was received in step a. MS generates a CoA address based on subnet-id received in router
14   advertisement messages

15   c)   At this step the MS sends a Binding Update (Mobility Header type 5) to the selected Home Agent. The MS
16   sets L to 1 if the MS wants the HA to defend (through proxy DAD) its link-local and global addresses
17   created with the same IID. The fields in this BU are set as per [53], [58], and [59]. In the BU, the MS
18   includes the MN-AAA authentication mobility option.

19   d)   The HA extracts the NAI, authenticator etc. from the BU and sends a AAA Access Request message to the
20   Home AAA server. This step always occurs for the initial registration regardless of whether the MS is
21   using an auto-configured HoA.

22   3.   The Home AAA server authenticates and authorizes the user and sends back an AAA Access-
23   Accept to the HA indicating successful authentication and authorization. At this step the Home
24   AAA server also distributes the MN-HA Key to the HA for subsequent MN-HA processing.

1 e) At this step the HA performs replay check with the ID field in the received BU. The HA MAY optionally
2   performs proxy Duplicate Address Detection (DAD) on the MS's home address (global) using proxy
3   Neighbor Solicitation as specified in [15].

4 f) Assuming that proxy DAD is successful, the HA sends back a Binding Acknowledgment (Mobility Header
5   type 6) to the MS. In this BA message the HA includes a Type 2 Routing Header (RH) destined to the
6   MS's home address, the MN-HA authentication mobility option, MN-NAI mobility option and the ID
7   mobility option. The MN-HA authenticator is calculated based on the Integrity Key that was derived in the
8   Home RADIUS server and sent to the HA at step e).

9 ### 7.8.2.5.2 CMIPv6 Session Renewal

10 To update session state in the network and allow a context release in case of SS/MS or network failure the MIPv6
11 context SHALL be renewed. The client sends Mobile Ipv6 binding update messages to the HA according to [53].
12 Upon receiving the binding update the HA will reset the MIPv6 session timer. Authentication is based on the prior
13 keys obtained during initial authentication and as such do not require a synchronization with the user authentication
14 server. The following depicts the message flow.
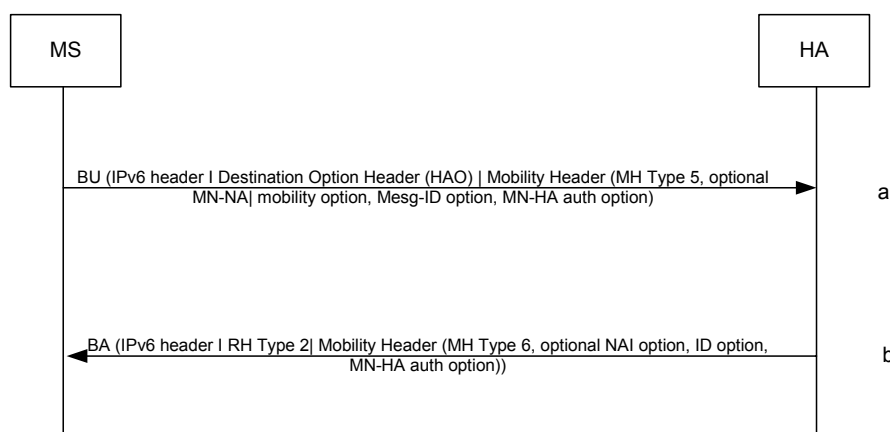
16 **Figure 7-82 - CMIPv6 Session Renewal, MIP Re-Registration**

17 a) The MS sends a BU to the HA. The BU includes ID and the MN-HA authentication mobility options. The
18   BU MAY also include the MN-NAI mobility option. The MN-HA authenticator is computed with the
19   CMIPv6-MN-HA key.

20 b) The HA authenticates the BU by verifying the MN-HA authenticator using the stored MN-HA Key. The
21   HA performs replay check. If both authentication and replay check succeeds, the HA sends a BA back to
22   the MS. The BA contains the MN-HA authentication mobility option. The BA contains the MN-NAI
23   mobility option.

24 Replay protection is provided using the Mobility message identification option as specified in [58]. Timestamp
25 based replay protection is used in this document for the both MN-AAA and MN-HA authentication mobility
26 options.

27 ### 7.8.2.5.3 MIPv6 Inter Access Router Handovers

28 As previously mentioned, CMIPv6 R3 mobility handovers are always network initiated. Even when the mobile
29 initiates the handover to a new BS and Access Router, the R3 mobility is a result of a network event that strives to
30 minimize impact on real time traffic when migration R3 from anchored to serving Access Router.

31 ### 7.8.2.5.3.1 Inter Access Router Handover

32 The following flow diagram describes the inter Access Router handover.
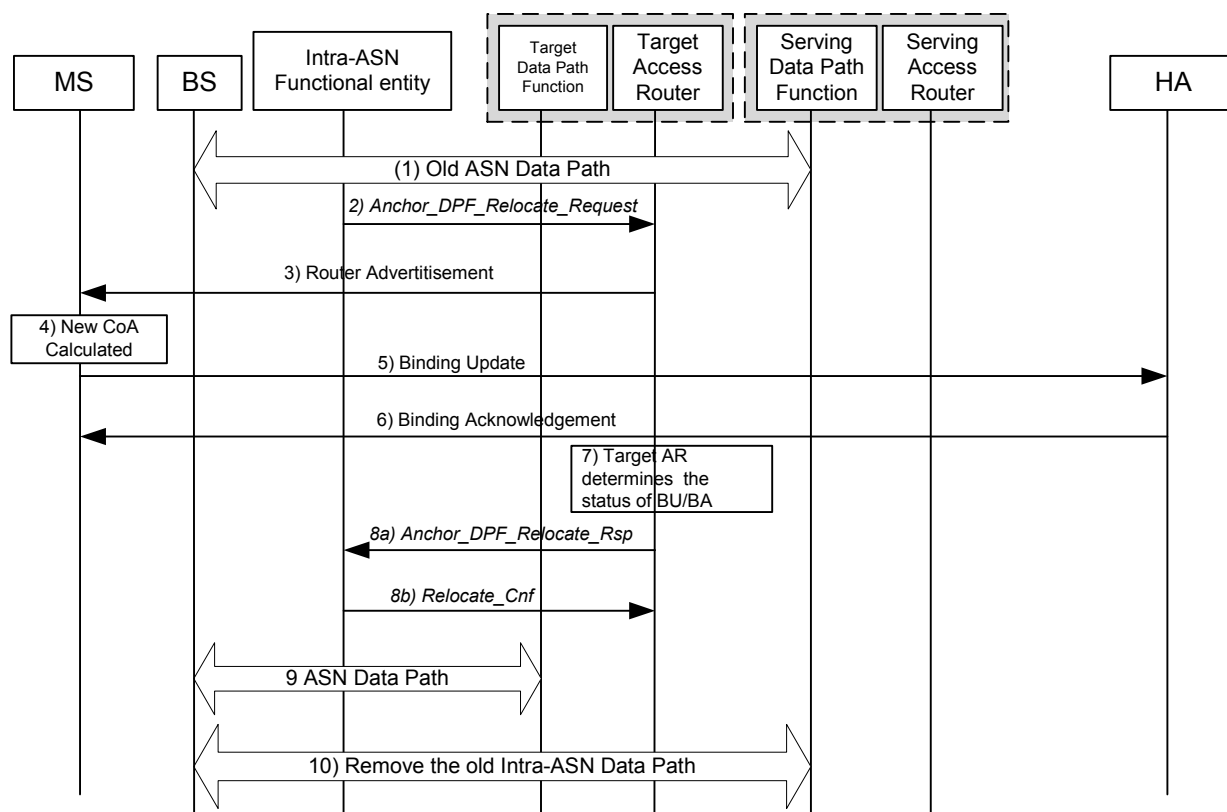
Figure 7-83 - CMIPv6 Mobility Event Triggering a Network Initiated R3 Re-Anchoring (CMIPv6)

1-2) *Old Access Router:* Arrows 1 represent the old intra-ASN data path prior to handover.

2) *Inter/Intra-ASN mobility trigger*: R3 handovers is initiated by an ASN Functional Entity.

After successful R3 Handover the Intra-ASN Functional entity is notified by an R3 *Anchor_DPF_Relocate_Rsp*. This message is acknowledged by sending the R3 relocation.Confirm. This completes the establishment of the new MIP context.

3) Upon receiving R3 mobility relocation trigger, target Access Router sends router advertisement to MS.

5-6) *MIP context update*: New binding with the HA is created

7) The Target AR determines the state of the MIPv6 registration process by parsing the BU/BA in a passive mode

8) *Inter-ASN context update*: After successful R3 Handover the Intra-ASN Functional entity is notified by an R3 *Relocation_Rsp*. In case of an unsuccessful handover the Intra-ASN Functional Entity is also informed so that the old states can be restored.

9) *Establishment of new Intra-ASN tunnel*: Together with an R3 re-anchoring also new intra-ASN Data Paths need to be established.

10) Upon successful R3 relocation the old ASN Data Path between serving and target Access Routers can be released

7.8.2.5.4   Router Advertisements
The router advertisements are sent as per IPv6 address configuration procedures.

7.8.2.5.5   MIPv6 Session Termination
In the case where a MS's IPv6 session has to be terminated, the MIP6 binding state between the MS and the HA has to be gracefully removed.

1   The two termination scenarios are:

2   • An MS initiated graceful termination: a session is gracefully terminated by sending a MIPv6 binding
3   update message with lifetime = 0. This termination is triggered either by the user or MS being in an error
4   conditions such as low battery power, etc.

5   • Network initiated graceful termination: a session is gracefully terminated by sending an
6   R3_Session_Release.Request message from the ASN-Functional Entity to the Serving Access Router. The
7   AR can in turn send a RA to the MS with Router Lifetime set to 0. This will force the MS to terminate it's
8   IPv6 session with the AR. This should also prompt the MS to send a binding update with the lifetime=0 to
9   the HA. For transport of the BU/BA, the AT needs to keep the IPv6 session alive until the MS is able to
10   de-regiester successfully with the HA. This will require the AR to inspect the BU/BA in a passive mode so
11   that it can determine when to remove the IPv6 session state with the MS and initiate R6 teardown. The
12   conditions for network initiated termination MAY be some error conditions with respect to the MS such as
13   the MS being identified as a rogue MS with security violations, planned maintenance, etc. This scenario is
14   depicted in Figure 7-84.

15
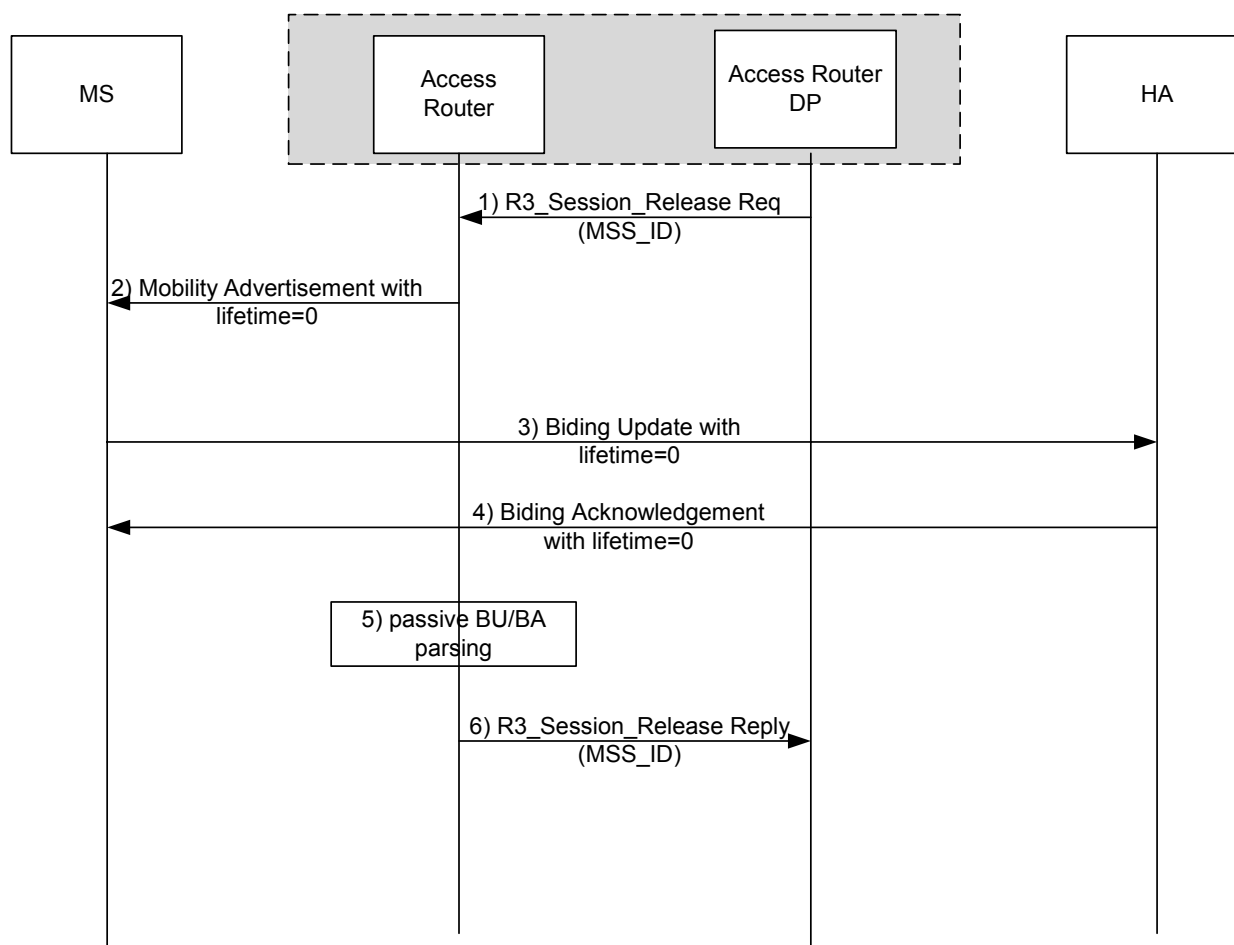
16   **Figure 7-84 - CMIPv6 Network Initiated Graceful Termination**

17 **7.8.2.5.6   Dynamic Home Agent Assignment via CMIPv6 Bootstrap**

18 The Home AAA server allocates the Home Agent and the Home Link Prefix to an MS during access authentication
19 using MIP6 Home Agent VSA and MIP6 Home Link Prefix VSA. The MS obtains the assigned HA information
20 using stateless DHCPv6 procedures as described in Figure 7-85.

1
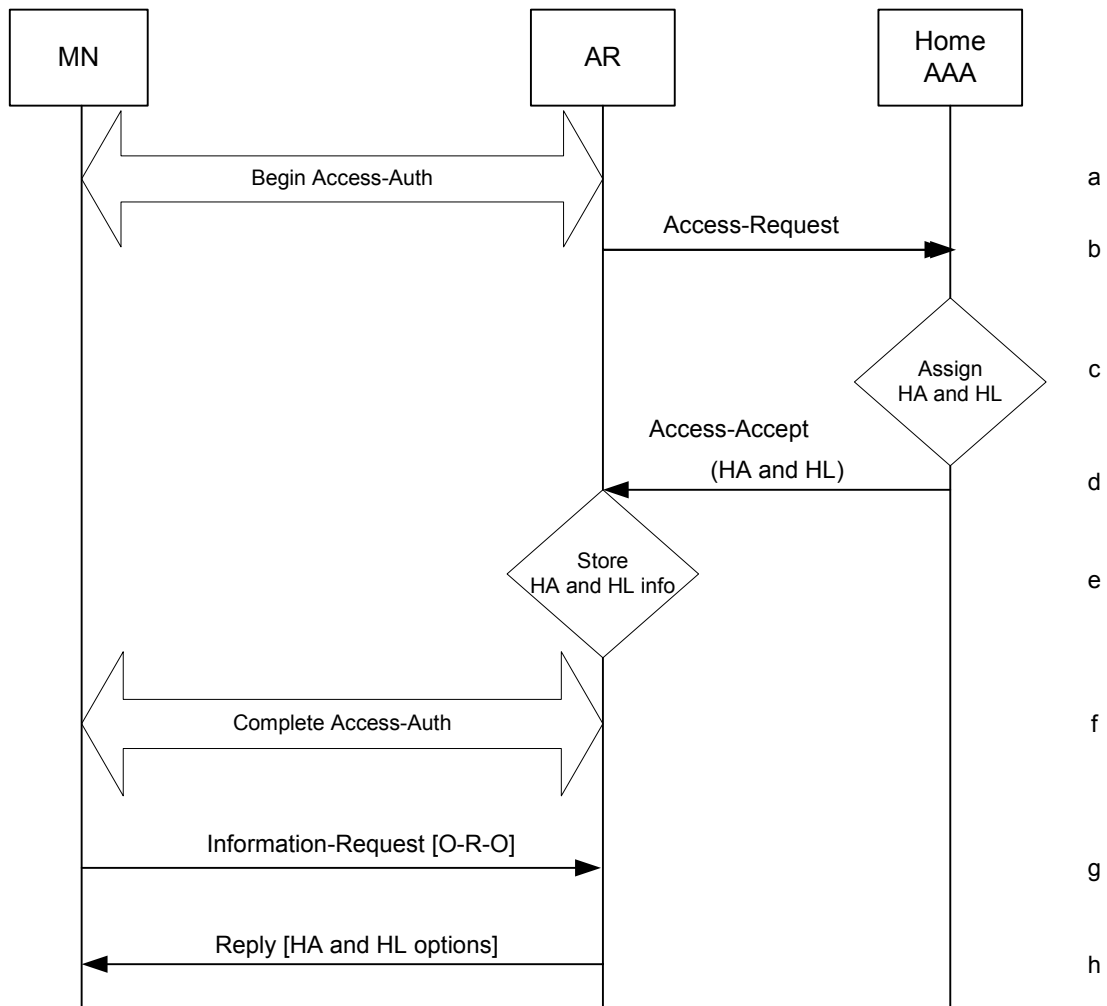
Figure 7-85 - Flow Diagram for Dynamic Home Agent Assignment

3 a) The MS begins the Access Authentication procedure.

4 b) The AR sends Access-Request to the Home AAA server.

5 c) The Home AAA server verifies the user's profile and detects that the user is a MIP6 subscriber. The Home
6   AAA server assigns an HA and a Home Link Prefix for the MS.

7 d) The Home AAA server includes a Home Agent address in the MIP6 Home Agent VSA. The Home AAA
8   server also includes a Home Link Prefix in the MIP6 Home Link Prefix VSA.

9 e) The AR receives the HA and HL information VSAs from the Home AAA server and stores them.

10 f) The Access Authentication procedure completes at this step.

11 g) The MS requests MIP6 bootstrap information using the DHCPv6 Information-request message [51] sent to
12   the AR. The MS uses the opcodes in the O-R-O for MIP6. The Opcodes are defined in draft-jang-mip6-
13   hiopt-00.txt.

14 h) The ASN looks up the appropriate record based on the Client Identifier and replies back to the MS [51]
15   with the options that were requested, attaching the HA information in a DHCP WiMAX Vendor Option
16   with a Vendor-Specific Option-Code=1. It also attaches the HL information in a DHCPv6 opcode as
17   defined in draft-jang-mip6-hiopt-00.txt.

1 **7.8.2.5.7   Dynamic Home Link Prefix Discovery via CMIPv6 Bootstrap**

2 The Home Link Prefix information is delivered the AR during the authentication setup phase. The Home RADIUS
3 server selects the Home Link Prefix and includes it in a MIP6 Home Link Prefix VSA in the Access-Accept
4 message. The Home Link Prefix information is delivered to the MS when the MS sends a DHCPv6 Information-
5 Request message.

6
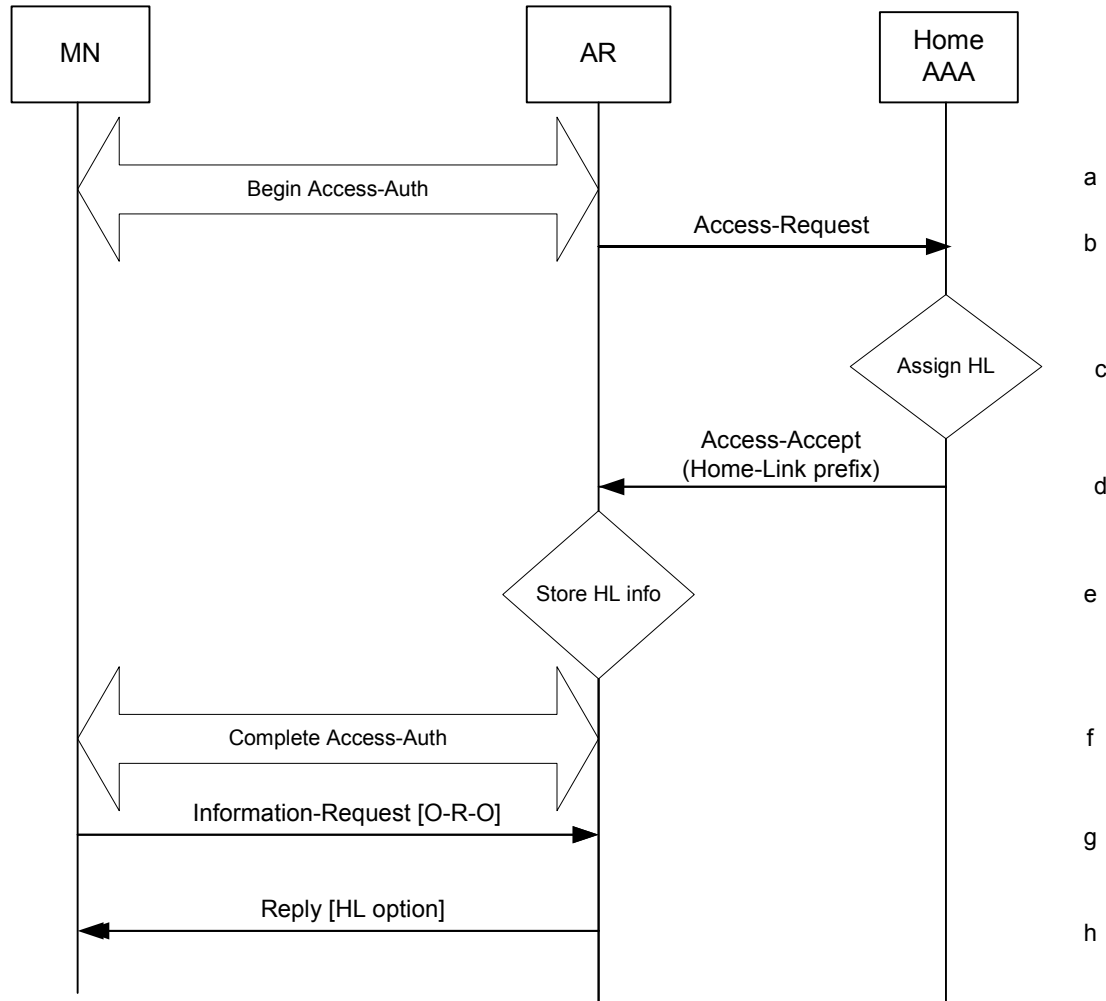
7 **Figure 7-86 - Bootstrap of Home Link Prefix**

8   a)   The MS begins the Access Authentication procedure.

9   b)   The AR sends Access-Request to the Home AAA server.

10   c)   The Home AAA server detects that the user is a MIP6 subscriber by verifying with the user's AAA profile.

11   d)   The Home AAA server assigns a HL prefix for the MS.

12   e)   The Home AAA server includes the assigned Home Link Prefix in an AAA MIP6-Home Link Prefix VSA.

13   f)   The AR receives the HL information from the Home AAA server. The AR stores the HL information. The
14   Access Authentication procedure completes at this step.

15   g)   The MS requests the MIP6 bootstrap information using the DHCPv6 Information-request message [51] sent
16   to the AR. The MS uses the opcodes in the O-R-O for MIP6. The Opcodes are defined in draft-jang-mip6-
17   hiopt-00.txt.

1   h)   The AR looks up the appropriate record based on the Client Identifier and replies back to the MS [51] with
2   the options that were requested and attaches the HL information in a DHCP option as specified in draft-ietf-
3   mip6-hiopt-00.txt

4   With the assigned Home Link Prefix, the MS performs dynamic Home Agent Address discovery by using the
5   procedure defined in [53] Section 5.3. The MS also auto-configures a Home Address with the assigned Home Link
6   Prefix.

7   **7.8.2.5.8   Dynamic Home Address Configuration**

8   The MS is allowed to perform stateless auto-configuration of its Home Address based on the Home Link Prefix.
9   Alternatively, the MS MAY be assigned a Home Address by DHCPv6 [42]. In either case, the Binding Cache Entry
10   (BCE) Lifetime is limited by the home-link prefix lifetime at the HA. This is controlled by the HA via the lifetime
11   field in the Binding Acknowledgement message sent to the MS. The MS can request an extension to the HoA/BCE
12   lifetime by sending a Binding Update to the Home Agent.

13   Once the BCE expires, the MS SHALL NOT use the HoA from the expired session. The MS SHALL initiate the
14   bootstrapping procedure when starting a new MIP6 session if the MS does not have the registration information (i.e.,
15   HL Prefix, HoA, HA) provisioned.

16   If the Binding Refresh Advice mobility option is present in the BA message [53], the Refresh Interval field in the
17   option SHALL be set to a value less than the lifetime value being returned in the Binding Acknowledgement. This
18   indicates that the mobile node SHOULD attempt to refresh its home registration at the indicated shorter interval.
19   The HA SHALL still retain the registration for the BCE lifetime period, even if the mobile node does not refresh its
20   registration within the refresh period. However, if the mobile node does not refresh the binding by sending a new
21   BU to the HA before the BCE lifetime expires, the HA SHALL delete the BCE.

22   **7.8.2.5.9   Home Address Assignment by DHCPv6**

23   **7.8.2.5.10 Home Address Auto-Configuration by the Mobile Station**

24
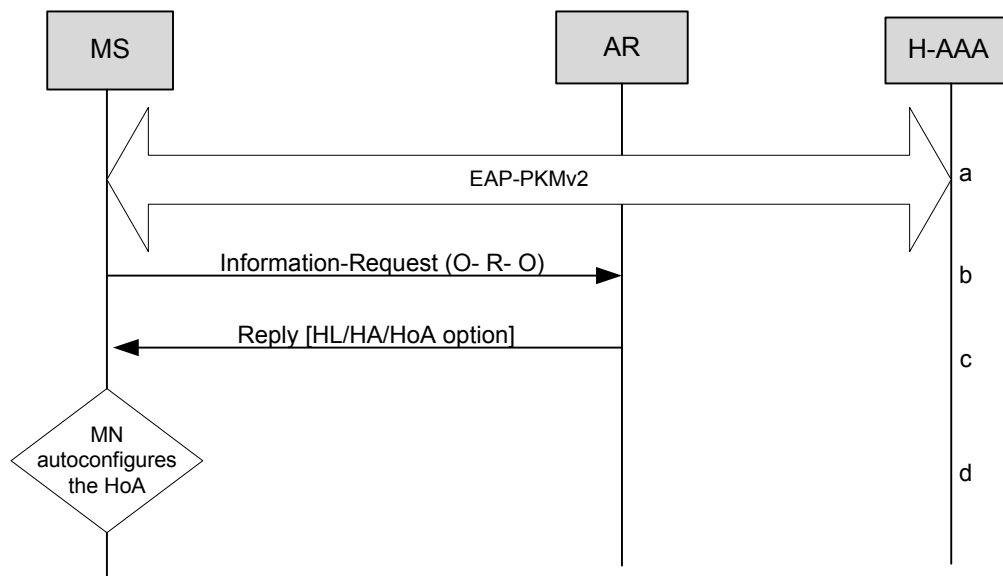
25   **Figure 7-87 - Home Address Auto-Configuration**

26   a)   The MS performs Device Authentication using EAP-PKMv2.

27   b)   The MS requests the MIP6 bootstrap information using the DHCPv6 Information-request message [51] sent
28   to the AR The MS uses the opcodes in the O-R-O for MIP6. The Opcodes are defined in draft-jang-mip6-
29   hiopt-00.txt.

1   c)   The AR looks up the appropriate record based on the Client Identifier and replies back to the MS [51] with
2   the MIP6 bootstrap options.

3   d)   Upon receiving the MIP6 bootstrap information from the AR, the mobile station checks whether a HoA is
4   included or not. If HoA is not included, the MN uses the Home Link Prefix. The MN auto-configures the
5   Home Address in a stateless manner as described in [16].

7.8.2.6   Home Agent Requirements to Support Dynamic Home Agent Assignment

7   The HA SHALL support Dynamic Home Agent Address Discovery as defined in [53].

8   The HA SHALL process Binding Updates that contain Mobility message authentication options (MN-HA or MN-
9   AAA), Mobility message Identification (ID) option and MN-NAI mobility option.

7.8.2.7   Home Agent Requirements to Support Dynamic Home Address Configuration

11   The Home Agent SHALL support Home Addresses that are either assigned by the Home AAA server or auto-
12   configured by the Mobile Station as long as the use of the Home Address by the user (NAI) is authorized by the
13   Home AAA server and the proxy Duplicate Address Detection procedure on the Home Link passes. In the case
14   where the MS uses an auto-configured HoA, no authorization check against the HoA is performed by the Home
15   AAA server. The HA does not include the HoA information in the AAA Access Request message.

16   Upon receiving a Binding Update containing Mobility Message Authentication Mobility Options (MN-HA or MN-
17   AAA), Mobility Message Mobility Message replay protection option, MN-NAI mobility option and a Home
18   Address Option (HAO) with a unicast Ipv6 address in the Home Address field, the HA SHALL process the Binding
19   Update. The HA SHALL perform proxy Duplicate Address Detection for the requested Home Address as per RFC
20   3775. The lifetime in the Binding Acknowledgement is controlled by local configuration at the Home Agent or it is
21   set to the valid-lifetime remaining for the home-link prefix ([15], Section 4.6.2).

7.8.2.8   Multiple Registrations

23   The HA SHALL support multiple home registrations with the same NAI but different Home Addresses. The
24   Binding Cache Entry (BCE) in the HA SHALL be indexed with the NAI and the Home Address of the MS at a
25   minimum. The HA SHALL rely on the Home AAA server to authorize a user to perform multiple simultaneous
26   home registrations on the same home link.

27   The MS is allowed to send more than one Binding Update for home registration with different HoA and with same
28   or different CoA. Whether these home registrations will be allowed or disallowed depends on the Home Network
29   provider's policy. If multiple registrations are not authorized, the HA will receive an AAA Access-Reject message
30   for subsequent home registration authorization.

7.8.2.9   Home Registration Support

32   The HA SHALL support the Authentication Protocol [58] and IPsec/IKEv2 [ref draft-ietf-mip6-ikev2-ipsec-06.txt]
33   based Home Registration.

34   The following sub-sections describe the detailed HA requirement.

7.8.2.10   Authentication Protocol Based Home Registration Support

36   The HA SHALL support Mobile Ipv6 authentication protocol as defined in [58] and the MN-NAI mobility option as
37   defined in [59]. Upon receiving the BU, the HA SHALL perform authentication of the BU based on the Mobility
38   authentication option contained in the BU and the MN-NAI mobility option.

7.8.2.11   Authentication with MN-AAA Authentication Mobility Option

40   The authentication protocol operation is as per RFC 4285. The MS and the HA uses CMIPv6 specific keys that are
41   derived and distributed by the HAAA server.

7.8.2.12   Authentication with MN-HA Authentication Mobility Option

43   The authentication protocol operation for MN-HA Mobility Option processing is as per RFC 4285.

1 ### 7.8.2.13 IPsec/IKEv2 based CMIPv6

2 The MS can perform IPsec/IKEv2 based Mobile IPv6 home registration. The detailed procedure for this type of
3 Mobile IPv6 access is described in draft-ietf-mip6-ikev2-ipsec-06.txt.

4 ### 7.8.2.14 Return Routability Support for Route Optimization

5 The Home Agent SHALL support Return Routability (RR) for Route Optimization as specified in [53] with the
6 exception that IPsec is not used to protect (ESP encrypted) the RR messages when auth protocol is in use. These
7 messages MAY be protected on a hop-by-hop basis through the operator's network. When IPsec/IKEv2 is used, the
8 messages (HoT/HoTi) can be protected using ESP to meet the RR requirement

9

10 ## 7.9 Radio Resource Management

11 ### 7.9.1 Functional Requirements

12 The functional requirements for Radio Resource Management are:

13 a) RRM specification SHALL be based on a generic architecture that enables efficient radio resource
14 utilization in a WiMAX network.

15 b) Generic architecture implies that while RRM implementations MAY assist several other WiMAX network
16 functions that impact available radio resources at any given time (QoS, Service Flow Admission Control,
17 mobility management, network management, etc.), the RRM functionality itself MAY be specified
18 independent of any such functions that RRM assists as long as inter-vendor interoperability is not affected.

19 c) RRM specification SHALL define mechanisms and procedures to share radio resource related information
20 between ASN network entities (e.g. BS or ASN-GW). Examples of such information include wireless link
21 capability or available spare capacity in a BS.

22 d) RRM procedures SHALL allow for different BSs to communicate, in a standardized manner, with each
23 other or with a centralized RRM entity residing in the same or a different ASN to exchange information
24 related to measurement and management of radio resources.

25 e) Each BS SHALL perform radio resource measurement locally between itself and the population of MS
26 served by it, as per IEEE 802.16 specifications. Procedures for such measurements SHALL remain out of
27 the scope of NWG specifications, even though such measurements MAY be used as a basis for radio
28 resource allocation and reconfiguration decisions by ASN network entities (e.g. BS or ASN-GW).

29 f) It SHALL be possible to deploy RRM in an ASN using Base Stations that have no direct communication
30 between them.

31 g) It SHALL be possible to deploy RRM in an ASN using Base Stations that support direct communication
32 between them.

33 h) It SHALL be possible to deploy RRM in an ASN using Base Stations with RRM function as well as a
34 centralized RRM entity that does not reside in the BS, and that collects and updates radio resource
35 indicators from several BSs in a standardized way. These indicators SHOULD be sufficient to provide the
36 required information for making such decisions as choice of Target BS, admission or rejection of Service
37 Flows, etc. The frequency of such collections MAY be dependent on a vendor/operator's specific
38 requirements. The content of such collections, however, SHALL be specified.

39 i) The architecture SHALL NOT require a BS to dynamically collect Radio Resource indicators from other
40 BSs. However, the architecture SHALL allow a BS to learn about neighboring BSs using

41 o Static configuration data (e.g., existence of neighboring BSs)

42 o Another RRM entity in the ASN that is aware of dynamic load situation of neighboring BSs

43 RRM procedures MAY provide decision support for one or more of the following WiMAX network functions.
44 However, RRM specification SHALL NOT be tied to any one of the following functions as long as inter-vendor
45 interoperability is not affected:

a) MS Admission Control and Connection Admission Control— i.e., ascertaining a priori that required radio resources are available at a potential target BS before handover.

b) Service Flow Admission Control— i.e., creation or modification of existing/additional service flows for an existing MS in the network. Selection of values for Admitted and Active QoS parameter sets for Service Flows.

c) Load Control—manages situation where system load exceeds the threshold and some counter-measures have to be taken to get the system back to feasible load.

d) Handover preparation and Control—for improvement/maintenance of overall performance indicators (for example, RRM MAY assist in system load balancing by facilitating selection of the most suitable BS during a handover.)

e) RRM procedures SHALL only specify the interfaces (i.e., protocols and procedures) between functional RRM entities residing in BS or outside BS (e.g., a centralized RRM entity in ASN-GW or elsewhere). Any interfaces between these RRM entities and other control entities in ASN (e.g., QoS, session management, etc.), while feasible, SHALL be outside the scope of RRM specification.

In some ASN function split profiles, an RRM entity and the said other control entities that MAY benefit from RRM data are collocated in the same logical component (e.g. BS or ASN-GW), so the information exchange between them is internal communication.

a) RRM communication procedures SHALL be interoperable and compliant with IEEE standards.

b) RRM communication procedures SHALL provide for interoperability between BS, ASN-GW, or other ASN network elements from different vendors.

There MAY be a need for an additional function in the ASN which takes care of network resources measurement and might be labeled Network Resource Measurement and Sampling (NRMS). It SHOULD monitor the transport channel resources, collecting measurements about R6 reference point resources, R4 reference point resources and R3 reference point resources. The NRMS might be located in the ASN-GW or in a BS, depending on ASN Profile. This function is not considered part of RRM, however a close cooperation of RRA, RRC and NRMS will be recommended.

7.9.2   Functional Decomposition

7.9.2.1   Functional Entities

RRM is composed of RRA and RRC from signaling transaction perspective as follows:

a) **Radio Resource Agent (RRA)—** This functional entity resides in BS and each BS shall have an RRA. It maintains a database of collected radio resource indicators. An RRA is responsible for assisting local Radio Resource Management (RRM) as well as communicating to the RRC, if present, including for example:

   o Collection/Measurement of radio resource indicators from the BS.

   o Collection/Measurement of radio resource indicators from the population of MS registered to the BS, using MAC management procedures as per IEEE 802.16 specifications and other measurement reporting for upper layers (e.g. derived bit error rate, MAC PDU error rate).

   o Communicating RRM control information over the air interface to MS, as per IEEE 802.16 specifications. An example of such RRM control information is set of neighbor BSs and their parameters.

   o Signaling procedure exchange with RRC for radio resource management function.

   o Controlling the radio resources of the respective BS, based on the measurements performed and measurement reports received by the BS and based on information received from the RRC functional entity if available. This local resource control includes power control, supervising the MAC and PHY functions, modifying the contents of the MOB_NBR-ADV broadcast message (by help of information from RRC or from management system), assisting the local Service Flow Management (SFM) function and policy management for Service Flow admission control, making determinations

1   and conducting actions based on radio resource policy, assisting the local HO functions for initiating
2   HO etc.

3   b) **Radio Resource Controller (RRC)** — This optional functional entity MAY reside in BS (one per BS), in
4   ASN-GW, or, as a standalone server in an ASN. The RRC MAY be collocated with RRA in the BS, or
5   separate. In the former case, the interface between RRC and RRA is out of the scope of this specification.
6   Such RRC MAY also communicate with RRCs in neighboring BSs which may be in the same or different
7   ASN. In the latter case, RRC MAY reside in the ASN-GW (or as a standalone server) communicating to
8   RRAs across R6 reference point. When RRCs are present in ASN, each RRA shall be associated with
9   exactly one RRC. On the other hand an RRC may be associated with zero, one or more RRAs in the same
10   ASN. An RRC is responsible for:

11   o   Collection of radio resource indicators from associated RRA(s): When RRA is collocated with RRC
12   in the same BS, the interface between RRA and RRC is outside the scope of this specification. When
13   RRA(s) and RRC are separated across R6 reference point, the collection of radio resource indicators
14   SHALL be as per primitives and information reporting procedures defined in this specification.

15   o   Communication between/across RRCs: An RRC MAY communicate with other RRCs across NWG-
16   specified interfaces.

17 c) **RRC Relay** — This functional entity MAY reside in ASN-GW for the purpose of relaying RRM messages.
18   RRC Relay cannot terminate RRM messages but it only relays these to the final destination RRC

19 When RRC is collocated with the BS, RRCs in different BSs SHALL communicate through the RRC Relays located
20 in the ASN-GWs when there is no R8 interface. If the R8 is exist, RRCs in different BSs may communicate through
21 the R8 interface.
22 When RRC resides in ASN as a standalone server or in ASN-GW, RRCs MAY communicate across R4 reference
23 point.

24 Standardized RRM procedures are required between RRA and RRC, and between RRCs across NWG-specified
25 interfaces. These procedures are classified into two types:

26 •   **Information Reporting Procedures** for delivery of BS radio resource indicators from RRA to RRC, and
27   between RRCs.

28 •   **Decision Support Procedures** from RRC to RRA for communicating suggestions or hints of aggregated
29   RRM status (e.g., in neighboring BSs) for various purposes.

7.9.2.2   RRM Generic Reference Models

31 RRM reference model MAY take one of the following two forms as follows:

32 Generic Reference Model #1 is shown in Figure 7-88.

33
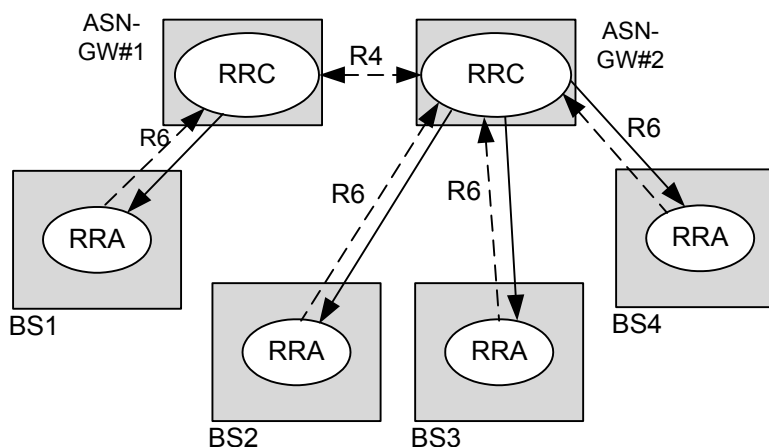
Figure 7-88 - RRAs Resident in BS and RRC Resident in ASN

1   The above reference model is based on RRA in each BS and RRC resident outside BS in the ASN. RRAs and RRC
2   interact across R6 reference point, using two types of procedures visible at NWG-specified open interfaces—
3   information reporting procedures (dashed lines) and decision support procedures (solid lines). RRCs MAY
4   communicate with each other using R4 reference point.

5   Generic Reference Model #2 is shown in Figure 7-89.

6
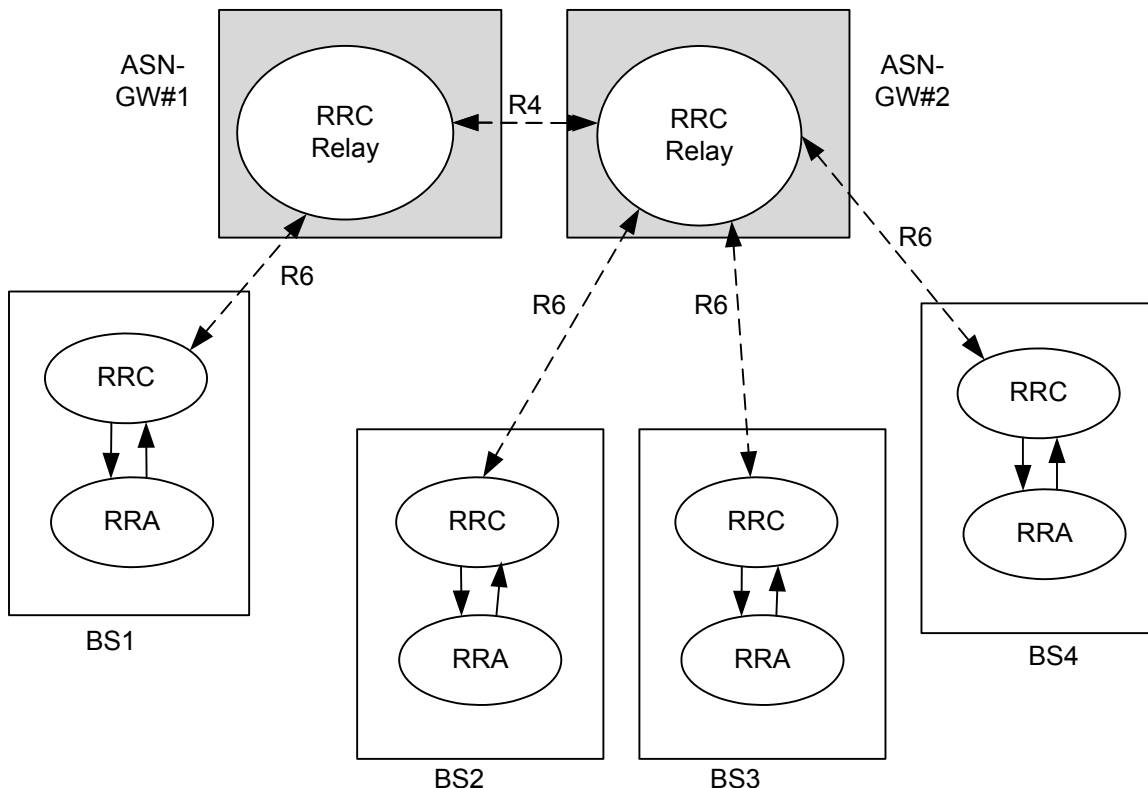
7   **Figure 7-89 - RRA and RRC Collocated in BS**

8   The above reference model is based on collocated RRA and RRC in each BS. The interface between RRA and RRC
9   is outside the scope of this specification. We introduce the "RRC Relay" in the ASN to enable the RRC-RRC
10   communication within and between ASNs over the standard reference interfaces. RRC Relay resides in the ASN
11   GW and acts as a relay for the RRM messages.

12   Note: this reference model is based on the assumption that there is no R8 reference point, which may be used for
13   direct communication between BSes.

14   The above two generic reference models can be mapped to the ASN reference model and ASN entities.

15   **7.9.3   Primitives**

16   RRM primitives MAY be used either to report radio resource indicators (i.e., from RRA to RRC, or, between RRCs)
17   or, to communicate decision support information (i.e., from RRC to RRA). The former type of primitive is called
18   information reporting primitive and the latter is called decision support primitive.

19   The following information reporting procedures SHALL be supported:

20   a) **Per-BS Spare Capacity Reporting procedure** — These reports are indexed by BS ID and indicate the
21   radio resources available at the BS (BS-ID refers to a sector with a single frequency assignment), e.g. as a
22   hint for Base Station selection during network entry or handover. Such reporting MAY be solicited or
23   unsolicited. Such reports SHALL be sent from RRA to RRC as well as between RRCs such that all
24   interested RRCs MAY have available information on current spare capacity of the BS for which they are
25   responsible, or, of neighboring BSs. – Note that this report does not refer to the service requirements of a

1　　　　　　specific MS and hence is not a replacement of the "*HO_Req* and *HO_Rsp*" specified for the Intra-ASN
2　　　　　　Handover preparation phase.

3　　　　b)　**Per MS PHY Service Level Reporting procedure** — These reports are indexed by MS. Such reporting is
4　　　　　　always solicited by RRC. Such reports SHALL be sent from RRA to RRC to update the per-MS databases
5　　　　　　in the RRC. These reports SHALL be generated for MS registered with the BS that is associated with the
6　　　　　　RRC. (See section 7.9.4.3 - Per-MS PHY Measurement Solicitation and Report)

7　　The following decision support procedures SHALL be supported:

8　　　　c)　**Neighbor BS radio resource status update** — These reports are delivered from RRC to RRA to propose a
9　　　　　　change of the broadcasted advertising message. (See section 7.9.4.4 - Neighbor BS Radio Resource Status
10　　　　　Update)

11　　Corresponding to these information reporting and decision support procedures, the corresponding RRM primitives
12　　are listed in Table 7-4.

13　　　　　　　　　　　　　　　　　**Table 7-4 - Primitives for RRM**

Name	Source	Destination	Purpose	Reporting or Decision support
RRM *PHY_Parameters_Req*	RRC	RRA	Request for *PHY_Parameters_Rpt*, per MS.	Request reports from RRA
RRM *PHY_Parameters_Rpt*	RRA	RRC	Assessment of link level quality per MS.	Reporting from RRA to RRC
RRM *Spare_Capacity_Req*	RRC	RRA/RRC	Request for *Spare_Capacity_Rpt* per BS.	Request reports from RRA; Request reports from RRC
RRM-Spare-capacity-report	RRA/RRC	RRC	Available Radio Resource report per BS.	Reporting from RRA to RRC; Reporting between RRCs
RRM-Neighbor-BS radio resource status update	RRC	RRA	Update the broadcasted Neighbor BS list	Decision support
RRM-Radio-configuration-request	RRC	RRA/RRC	Request for *Spare_Capacity_Rpt* per BS.	Request reports from RRA; Request reports from RRC
RRM-Radio-configuration-report	RRA/RRC	RRC	Available Radio Resource report per BS.	Reporting from RRA to RRC; Reporting between RRCs

14

15　　Note: The final set of RRM procedures is defined in the Stage-3 Specification.

7.9.4　Procedures

17　　This subsection describes the protocol primitives at a functional level.

18　　　　•　Request for per-BS *Spare_Capacity_Rpt*

19　　　　•　Per-BS *Spare_Capacity_Rpt*

1   •   Request for per-MS PHY measurement report

2   •   Per-MS PHY measurement report

3   •   Neighbor BS radio resource status update

4   Note: The final set of RRM procedures is defined in the Stage-3 Specification.

7.9.4.1   Request for *Spare_Capacity_Rpt*

6   This primitive can be applied by an RRC to request a Per-BS *Spare_Capacity_Rpt* from an RRA or from another
7   RRC.

8   An RRC SHALL send this request whenever to query spare capacity in a BS.

9   The RRC MAY send this request periodically or at any time. The RRC MAY also send this request based on a
10   network event trigger.

11
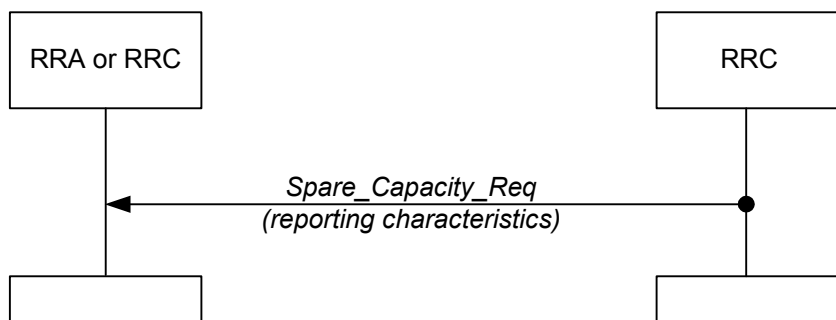
12   **Figure 7-90 - Request for *Spare_Capacity_Rpt*, per BS**

13   Reporting characteristics: Indicates whether report SHOULD be sent periodically, or event-driven etc. The detailed
14   list of events is given in the Stage-3 Specification:

7.9.4.2   Per-BS *Spare_Capacity_Rpt*

16   RRA (RRC) SHALL send the following type of report to RRC:

17   *Spare_Capacity_Rpt* which includes the "Available Radio Resource" indicator (percentage of reported average
18   available sub-channels and symbols resources per frame. The average is over a configurable interval with a default
19   value of 200 frames).

20

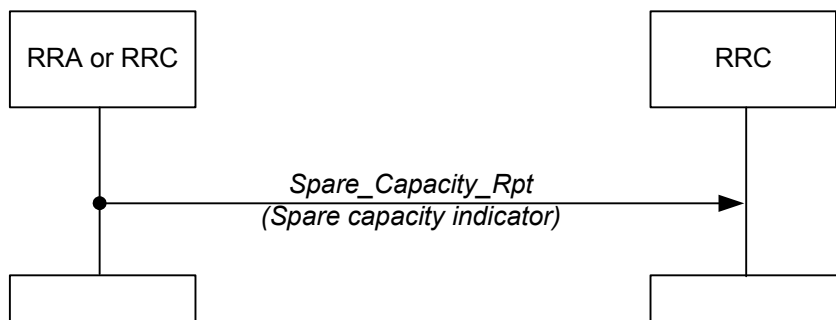21   **Figure 7-91 - *Spare_Capacity_Rpt*, per BS (Unsolicited or Solicited)**

22   The report MAY be sent periodically or event-driven. The detailed list of events is given in the Stage-3
23   Specification.

24   A tabular representation of the Spare Capacity Reporting primitive reporting the "Available Radio Resource"
25   indicator is given in the Stage-3 Specification.

1 **DL (UL) Available Radio Resource:**

2 Available Radio Resource indicator SHALL indicate the average percentage of available physical radio resources
3 for DL (or UL, respectively) where averaging SHALL take place over a configurable time interval with a default
4 value of 200 frame. Available physical radio resources SHALL be defined as the set of subchannels and symbols
5 within a radio frame, which are not used by any non-best-effort service flow class.

6 ### 7.9.4.2.1 Usage Scenarios

7 The "Available radio resource" measurements provided by the RRAs to RRC MAY be used by RRC for load
8 balancing: A potential strategy of RRC MAY be to interact with the HO controller with the objective to have
9 approximately equal load, as expressed by the "available resource indicator", in all BSs controlled by RRC – subject
10 to the availability of suitably radio path conditions between a MS and the potential HO target BSs.

11 The "available radio resource" indicator SHALL be determined by the BSs as specified above.

12 Possible ways of RRM interaction with the HO decisions have been described in NWG Stage-2 specification;
13 Section 7.7 - ASN Anchored Mobility Management and 7.8 - CSN Anchored Mobility Management. In Network
14 Initiated Handoff as well as in MS Initiated Handoff, the ASN uses Handover Request primitive to communicate
15 with a number of candidate BSs for permission to handoff a MS or MS'. The candidate BS list MAY be
16 recommended or modified by the external module such as RRC.

17 ### 7.9.4.3   Per-MS PHY Measurement Solicitation and Report

18 This primitive can be applied by an RRA to report to an RRC, or by an RRC to report to another RRC.

19 RRC MAY use this primitive exchange once it has received a *HO_Req* from Serving BS to learn (or recollect a
20 more updated set of parameters) regarding the MS PHY service levels for the Serving BS and each candidate BS. In
21 addition, RRC MAY check the latest "Spare capacity report" whether capacity is available for adding the MS, and
22 RRC will return the updated list of candidate BSs to Serving BS.

23
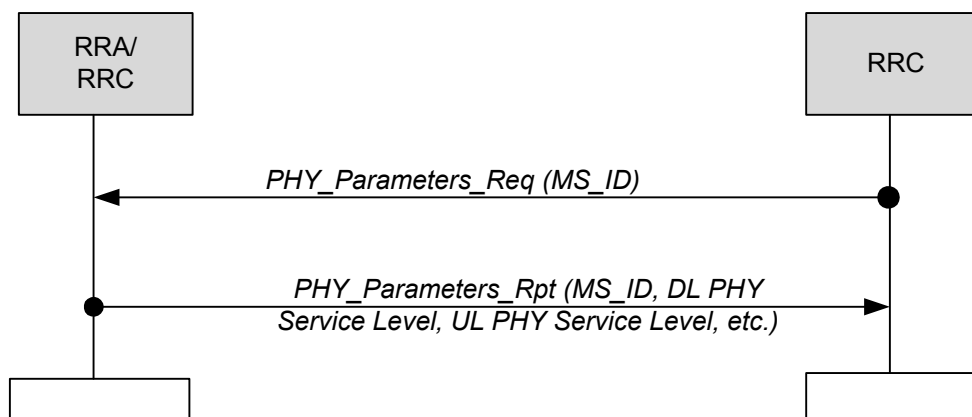
24 **Figure 7-92 - PHY Report (Solicited)**

25 As per this primitive exchange, the BS SHALL send the following types of reports to RRC:

26 **PHY reports** for DL & UL per MS. These reports include the set of parameters described in Section 8.4.11 of [1].
27 Additionally, these reports include the PHY feedback parameters (on a per-MS basis). All parameters are encoded in
28 TLVs.

29 DL parameters are measured by MS and reported by BS to RRC. UL parameters are measured and reported by BS to
30 RRC. Same parameters MAY be reported from one RRC to another.

31 A tabular representation of the PHY Report primitive is given in the Stage-3 Specification

32 In case the RRC is collocated with Target HO Function, it MAY be possible to include these measurement reports
33 into the Handover-Request messages or *HO_Rsp* messages sent from BS to the HO Control. This is FFS.

1 In order to meet a Stage-1 Requirement for channel quality monitoring, this message might be augmented to include
2 measurements related to QoS parameters, e.g. "burst error rate". – To be checked during work at Stage-3.

3 7.9.4.4 Neighbor BS Radio Resource Status Update

4 This procedure can be used by RRC to inform a Serving BS about the list of Neighbor BSs which are potential HO
5 Target Base Stations for any MS being served by the SBS, including information about their radio resource status. It
6 is important consideration for the serving RRC to synchronize the radio resource information that are received from
7 the RRAs of the neighbor BSs as well as from other RRCs to provide the accurate and up-to-date information to the
8 RRA of the Serving BS in order to allow the MS to make appropriate HO decision. The policy on the information
9 processing at the RRC and the frequency of the status update is outside the scope of this specification.

10 RRA (in SBS) MAY use this hint from RRC as a basis for updating the Neighbor BS Advertisement: SBS would
11 ask the MS to trigger the scanning of the respective neighbor BSs, by means of MOB_NBR_ADV.

12
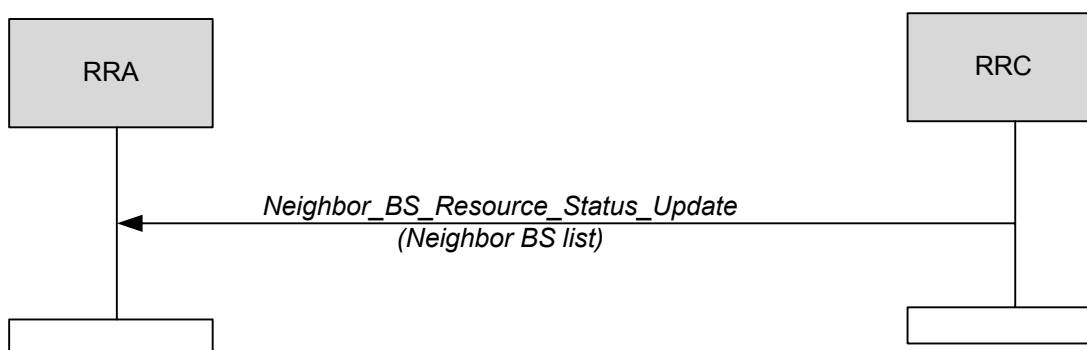
13 **Figure 7-93 - Neighbor BS Radio Resource Status Update Procedure**

14 A tabular representation of the RRM-Neighbor-BS-Radio-Resource-Status-Update primitive is given in the Stage-3
15 Specification. The primitive has been suitably adopted from MOB_NBR-ADV message format, as defined in [2]
16 and amended by [80].

17 7.9.5 Power Management and Interference Control

18 In Release 1.0.0, power management and interference control is primarily a task performed by each BS. In addition
19 there is an RRM primitive "RRM *PHY_Parameters_Rpt*", see above, for interference measurement report from
20 RRA to RRC to allow RRC to get involved in interference control.

21 Power management during idle mode and sleep mode is handled elsewhere in the Stage-2 document.

22 Potential enhancements of power management and interference control, as well as of RRM in general, are for further
23 study.

24 **Future enhancements of RRM** MAY include adding RRM primitives for the following applications that in Release
25 1.0.0 are considered to be solved locally by the BS Site, or to be left to BS configuration or Network Management:

26 • Reconfiguration of sub-channel space to be used in a BS (sector).

27 • Reconfiguration of maximum transmit power of a BS

28 • Reconfiguration of burst selection rules.

29 • Reconfiguration of radio resource allocation and scheduling policies in a BS.

30 • Reconfiguration of UL/DL switching point for TDD

31 • Reconfiguration of broadcast information (e.g. supported burst profiles)

32 • Forwarding of DCD and UCD information between neighboring base stations

7.10 Paging and Idle-mode MS Operation

7.10.1 Functional requirements

The following functional requirements SHALL be supported in the WiMAX network:

a) Paging features should be supported in Nomadicity and Portability usage models whereas they are mandatory for Full Mobility usage scenario (see Stage 1 document). These features shall be compliant with IEEE 802.16e.

b) Paging Groups, as defined in IEEE 802.16e, shall comprise a set of Base Stations. An access network (i.e., NAP) may be provisioned to consist of one or more Paging Groups. A NAP may comprise one or more Paging Controllers. Each Idle MS in the NAP is assigned a single Paging Controller, called Anchor PC.

c) An MS in idle mode must be accessible in the network during Paging Intervals for Paging and Location Updates. This covers cases where the MS:

(1) stays in the coverage area of same BS in the access network or

(2) moves to the coverage area of a new BS (in the same or different Paging Group) in the access network.

7.10.2 Functional Decomposition

The Paging operation shall comprise the following functional entities:

Paging Controller (PC) — Paging controller is a functional entity that administers the activity of idle mode MS in the network. It is identified by PC ID (6 bytes) in IEEE 802.16e, which could map to the address of a functional entity in NWG. The PC MAY be either co-located with BS or separated from BS across R6 reference point. There are two types of PCs:

o   Anchor PC: For each idle mode MS, there shall be a single Anchor PC that contains the updated location information of the MS.

o   Relay PC: There may also be one or more other PCs in the network (called Relay PC) that participate in relaying Paging and Location Management messages between PA and the Anchor PC

Paging Agent (PA) – Paging Agent is a functional entity that handles the interaction between PC and IEEE 802.16e specified Paging related functionality implemented in the Base Station. A Paging Agent is co-located with BS. The interaction between PA and Base Station is out of scope of NWG. When the PA is located across R6 reference point from the PC, its interaction with PC is within the scope of NWG specification. However, when PC is also co-located with BS, the interaction between the co-located PA and PC is outside the scope of NWG.

Paging Group (PG), defined in IEEE 802.16e, may be interpreted as comprising one or more Paging Agents. A Paging Group resides entirely within a NAP boundary. Paging Groups are managed by the network management system and provisioned per the access network operator's provisioning requirements. Paging Group management and its provisioning requirements are not in scope of this document.

Location Register (LR) — An LR is a distributed database with each instance corresponding to an Anchor PC. Location registers contain information about Idle mode MSs. The information for each MS includes, but is not limited to:

a) Contains MS Paging Information for each MS that has registered with the network earlier but currently in Idle mode.

Current paging group ID (PGID)

PAGING_CYCLE

PAGING_OFFSET

Last reported BSID

Last reported Relay PCID

1   b)   MS Service Flow Information comprising

2   (1) Idle Mode retention information for each MS in idle-mode

3   (2) Service Flow Information for each MS

4   An instance of a Location Register is associated with every Anchor PC. Specifying communication between LR and
5   PC is outside the scope of this specification.

6

8   The following points are noteworthy regarding this reference model:
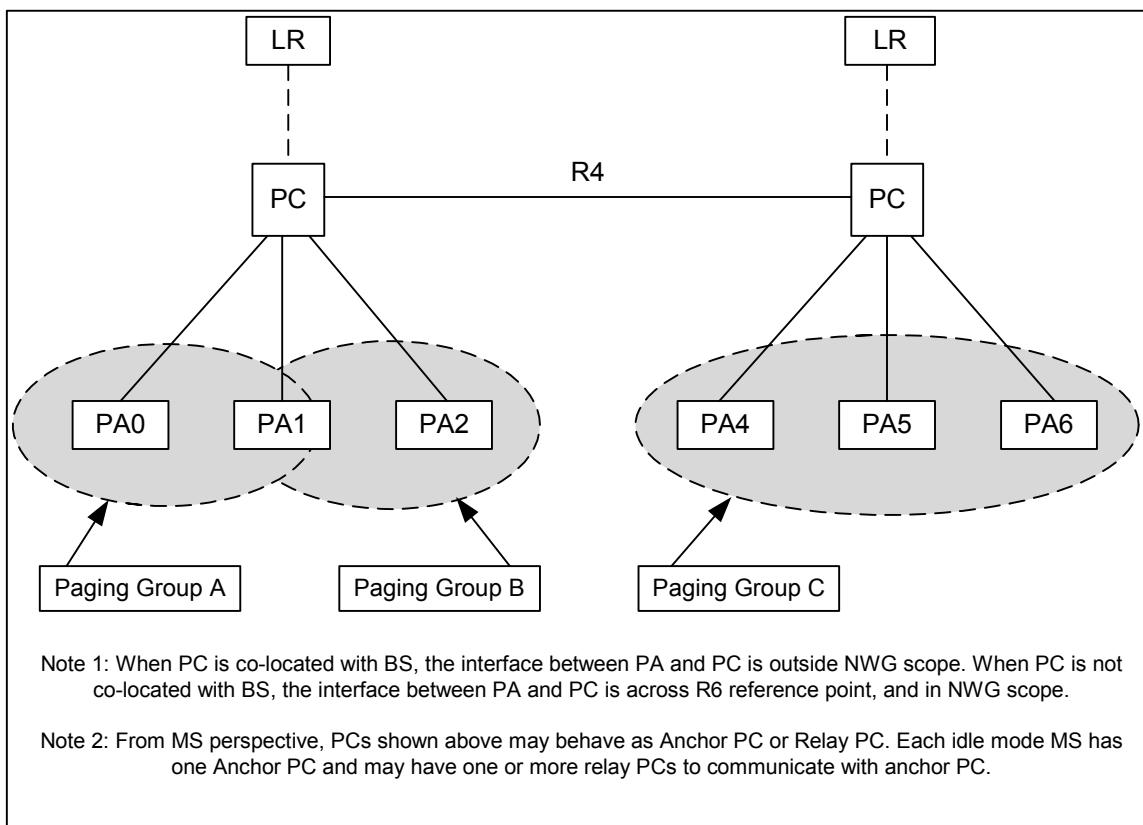
9   a)   There MAY be multiple PGs inside an operator's (i.e., NAP) network domain.   To keep Paging
10   functionality optimally implemented (i.e., prevent Paging Groups from becoming too large), multiple
11   Paging Groups shall be allowed in the network. Figure 7-94 specifies Paging Groups in reference to
12   WiMAX network reference model. A BS (and its corresponding, co-located PA) may be part of more than
13   one Paging Group.

14   b)   IEEE 802.16e standard specifies PC to be co-located with either BS or a separate entity in the network.
15   This specification describes Paging related control protocol and messages between PA and PC. For the
16   former deployment scenario (where PC is co-located with BS), the messages between these co-located
17   entities (PA and PC) are not exposed over an NWG specified reference point, and therefore not a
18   consideration for interoperability. For the latter deployment scenario (where PC is not co-located with BS),
19   Paging control protocol (messages) are exchanged over R6 reference point between PA and PC. In both
20   deployment scenarios, Paging Control messages between PCs are exchanged across R4 reference point.

21   The Location Register (LR) comprises a location database in the network. This database, accessible
22   by/through PC, tracks the current Paging Group (identified by Paging Group Id, PGID) of each idle-mode
23   MS in the network. It also stores the context information required for Paging. In the event of MS movement
24   across Paging Groups, location update occurs across PCs via R6 and/or R4 interfaces and information is
25   updated in the LR that is associated with the Anchor PC assigned for the MS.

1   When MS enters IDLE mode, the LR entry for this MS is created. The LR will be updated with MS idle-
2   mode retain information. For this idle-mode MS, its Anchor PC shall be either static or may change until
3   MS becomes active and performs a full network entry.

4   As MS travels in IDLE mode and crosses the boundary of it current PG, it is enforced to perform Location
5   Update. Location Update messaging between PA and Anchor PC occurs over R6 and in some cases over
6   R4 reference interfaces. R4 reference interface is involved when PA has no direct connectivity with Anchor
7   PC over R6 and, therefore, needs to reach it via intermediate routing nodes (i.e. Relay PCs).

8   NOTE 1- For CMIP/PMIP based services, MS movements while in idle mode may not result in FA change (wakeup,
9   MIP registration etc.)

10 NOTE 2- For Simple IP based services, when an idle mode MS location update results in full network entry (e.g.,
11 unsecured location update, re-authentication), the MS PoA IP address refresh may be performed.

7.10.3 Paging and Idle-Mode MS Operation Procedures

13 This section describes the protocols and procedures as per the above reference model.

14 The following is a generic case that depicts an MS about to enter IDLE mode as it is served by Foreign Agent (FA)
15 and Authenticator in the network.

16
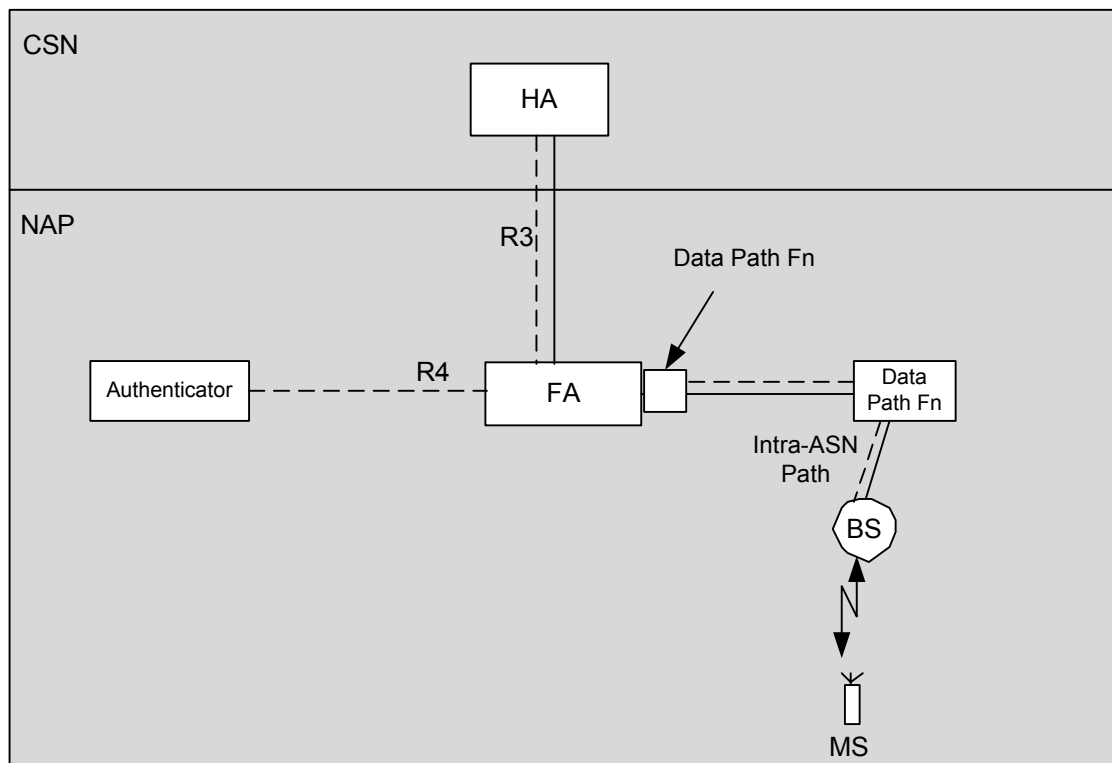
Figure 7-95 - Generic Depiction of Functional Entities Prior to MS Entering Idle Mode

18 When the MS enters Idle mode a PC entry for the MS is created (instantiated) and the bearer tunnels for data
19 forwarding between Anchor Data Path Function, and BS are removed. If Anchor DPF and FA are collocated, all
20 bearer tunnels between FA and BS are removed. Note that the ability to send R4 and R6 signaling is not impacted by
21 the removal of the bearer tunnels. As idle mode MS moves in the network, the FA itself could be migrated as well
22 but that is left as an implementation option.

1
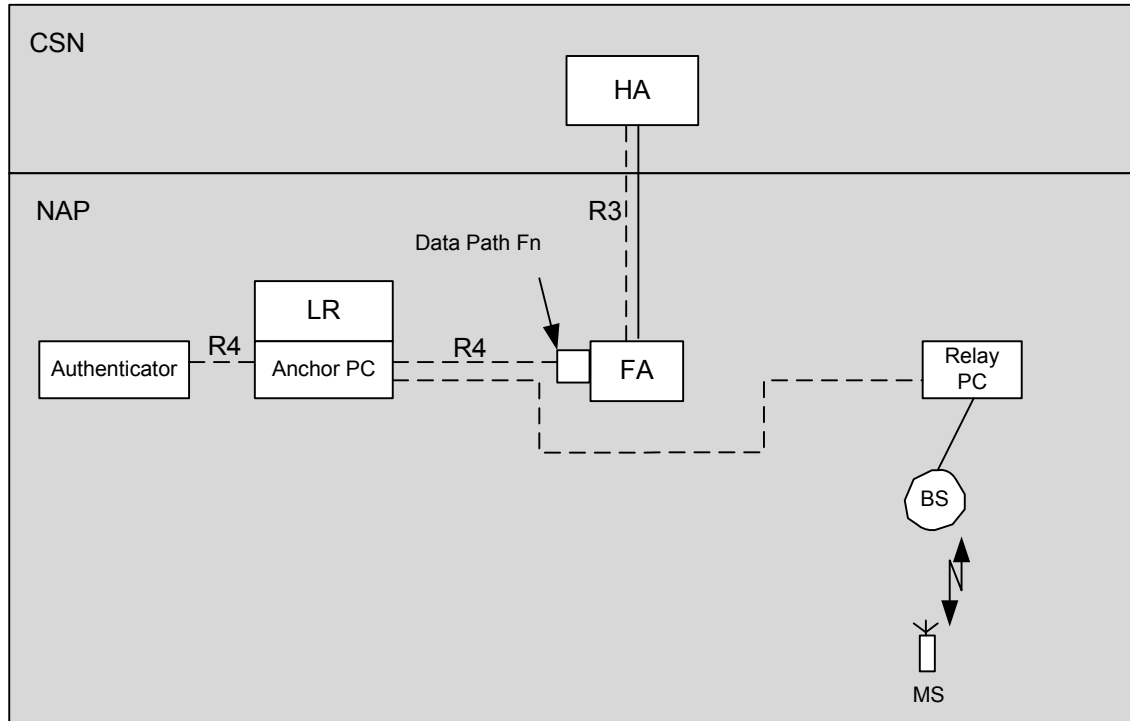
2 **Figure 7-96 - Generic Depiction of Functional Entities after MS Enters Idle Mode**

3 **7.10.3.1 Backbone Primitives for Paging and Idle Mode**

4 Paging and Idle Mode Primitives are divided into the following two groups:

5 (1) Primitives for signaling paging control and location management

6 (2) Primitives for signaling LR updates

7 summarizes the backbone primitives, which may be communicated between PA and PC.

8 **Table 7-5 - Primitives for Paging Control and Location Management "for information only, the**
9 **binding facts are defined in the Stage3 Spec"**

Primitives	From → To
Paging_Announce	Anchor PC →Relay PC(s) (in PG) → PAs in PG
Location Update Request	PA → Relay PC(s) → Anchor PC
LU_Rsp	Anchor PC → Relay PC(s) → PA
Delete_MS_Entry_Req	Data Path Fn → PC
LU_Cnf	PA -> Relay PC(s) -> Anchor PC
Initiate_Paging_Req	Data Path Fn → Anchor PC

Primitives	From → To
Initiate_Paging_Rsp	Anchor PC → Data Path Fn
IM_Exit_State_Change_Req	Data Path Fn → Anchor PC
IM_Exit_State_Change_Rsp	Anchor PC → Data Path Fn
IM_Entry_State_Change_Req	Relay PC → Anchor PC
IM_Entry_State_Change_Rsp	Anchor PC → Relay PC
R4 *Delete_MS_Entry_Req*	ADPF→ APC/LR, BS/DPF→DPF/Relay PC, DPF/Relay PC→ APC/LR
R4 Anchor PC Indication	Anchor DPF/FA → Anchor PC / LR
R4 Anchor PC Ack	Anchor PC / LR → Anchor DPF/FA
R4 PC Relocation Indication	Current Anchor PC ASN → Anchor DP / FA ASN
R4 PC Relocation Ack	Anchor DP / FA ASN → Current Anchor PC ASN

1 The following backbone HO primitives (Table 7-6) can also be utilized in the paging 1 and location management for
2 idle mode MS.

3 **Table 7-6 - Reuse of HO Primitives for Paging Operation**

Primitives	From → To
Context_Req	PA → Anchor PC
Context_Rpt	Anchor PC → PA
Path_Reg_Req	BS/DPF → DPF/Relay PC
Path_Reg_Rsp	DPF/Relay PC → BS/DPF
Path_Reg_Ack	BS/DPF → DPF/Relay PC
Path_Dereg_Req	BS → Serving ASN
Path_Dereg_Rsp	Serving ASN → BS

Path_Dereg_Ack	BS → Serving ASN
CMAC Update	Serving ASN → Authenticator
CMAC Update Ack	Authenticator → Serving ASN

1   **7.10.3.2 Procedures for Paging the MS and MS Exiting IDLE mode**

2   *Paging_Announce* occurs under several scenarios which include:

3   a)   Data arriving for the MS at the Anchor DPF

4   b)   Location update forced by the network for this MS

5   c)   MS re-entry into the network as forced by the network

6   d)   Cancel *Paging_Announce* once the MS has exited IDLE state.

7   In scenario a), when Data arrives at the anchor DPF (which may be collocated with the FA as in Figure 7-97) for the
8   MS, thus triggering a *Paging_Announce*, the Paging context information (including PGID, Relay PCID, BSID, etc.)
9   would be retrieved from LR associated with Anchor PC for the MS. The anchor PC may issue one or more
10 *Paging_Announce* messages based on whatever knowledge it has of the topology of the paging group for the MS. If
11 the anchor PC has no knowledge of the topology of the PG, it should send the Paging Announce message to an
12 appropriate Relay PC, which can then relay the message to BSs in a Paging Region comprising BSs and zero or
13 more relay PCs. Figure 7-97 illustrates the procedure for MS Paging upon receipt of downlink data for the MS.
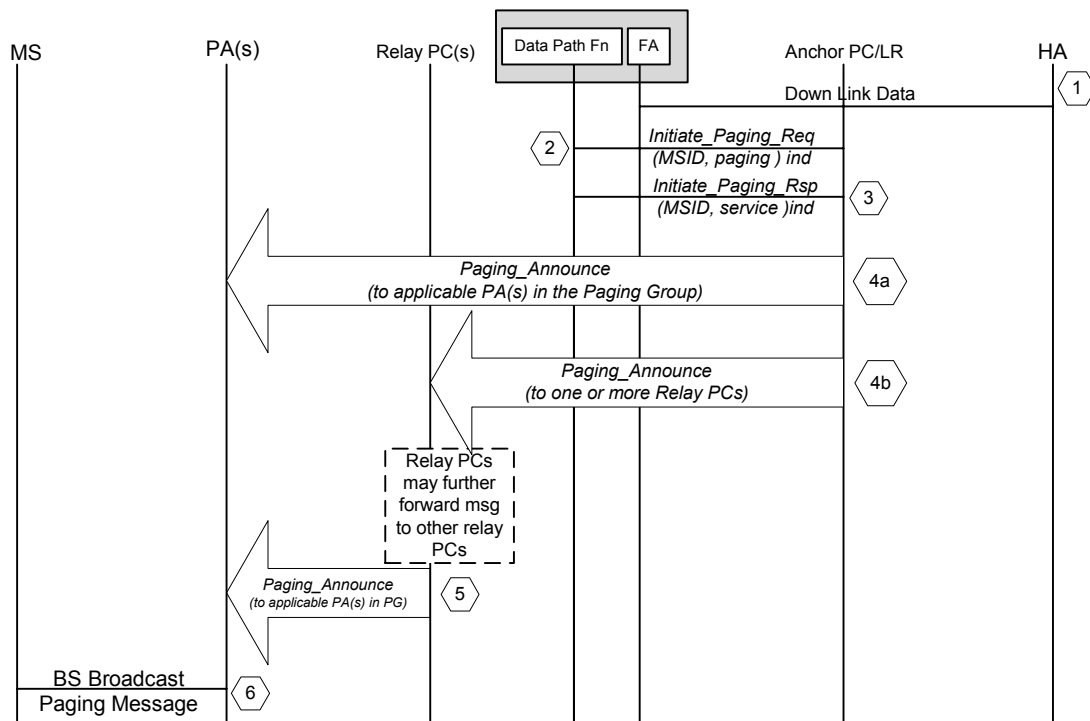

15   **Figure 7-97 - Paging Generated for MS by Incoming Packets for MS in Idle Mode**

16   Paging flow**:**

17   (1) HA sends downlink data to MS over MIPv4 tunnel to Data Path function associated with FA. In the event that
18   there is no FA (e.g.: MIPv6), the incoming data will be buffered at the anchor DPF (not shown in the figure).

1   (2) The Anchor Data Path Function recognizes that MS is in Idle mode. Receiving downlink data triggers sending
2   *Initiate_Paging_Req* to Anchor PC to initiate Paging. (anchor Data Path function keeps track of MS's Anchor
3   PC). *Initiate_Paging_Req* contains: MSID, indication that MS is a paging candidate.

4   (3) Anchor PC sends *Initiate_Paging_Rsp* to Data Path function. This message may be utilized to indicate that the
5   MS is authorized for service. For such a case, *Initiate_Paging_Rsp* contains: MSID, and service authorization
6   indicator.

7   (4) Anchor PC retrieves the MS paging info (comprising PGID, paging cycle, paging offset, a relay PCID, or a set
8   of BSIDs including last reported one) and constructs *Paging_Announce* message. The Anchor PC may issue one
9   or more *Paging_Announce* messages based on its knowledge of topology of the Paging region. Figure 7-96
10   depicts two alternative methods (step 4a and 4b, respectively) for generating *Paging_Announce* messages:

11   a) Anchor PC may be topologically aware of Paging region to be Paged (e.g. PG). For example, it may be
12   aware of BSs in region. In this case, the Anchor PC may issue *Paging_Announce* messages to one or
13   more BSs and/or relay PCs in this region, or,

14   b) The Anchor PC may be topologically unaware of the Paging region except that it is aware of one or
15   more Relay PCs that can forward the *Paging_Announce* message appropriately to the Paging region. In
16   this case, the Anchor PC may issue *Paging_Announce* message to this relay PC (or relay PCs) that
17   would in turn forward it to the Paging region.

18   Messages 4a) and 4b) can also be used to cancel *Paging_Announce*. This can happen in the events such as:
19   the MS is successfully paged by one of the BSs or PC wants to stop paging, etc.

20   Relay PCs receiving Paging Request for the specific PG forward it to the relevant BSs or other relay PCs associated
21   with the PGID received in Paging Request.

22   BSs send BS Broadcast Paging Message requesting that MS exit Idle mode. If not receiving response from MS, BS
23   has to resend BS_Broadcast_Paging Message as specified in IEEE 802.16e specification.

24   Other paging scenarios described above would follow steps 4a-6 as in the above figure.

25   Note: The above flow does not illustrate termination of Paging Broadcast by BS.

1   The following depicts an example of the message flow for MS exiting IDLE mode procedure:

2
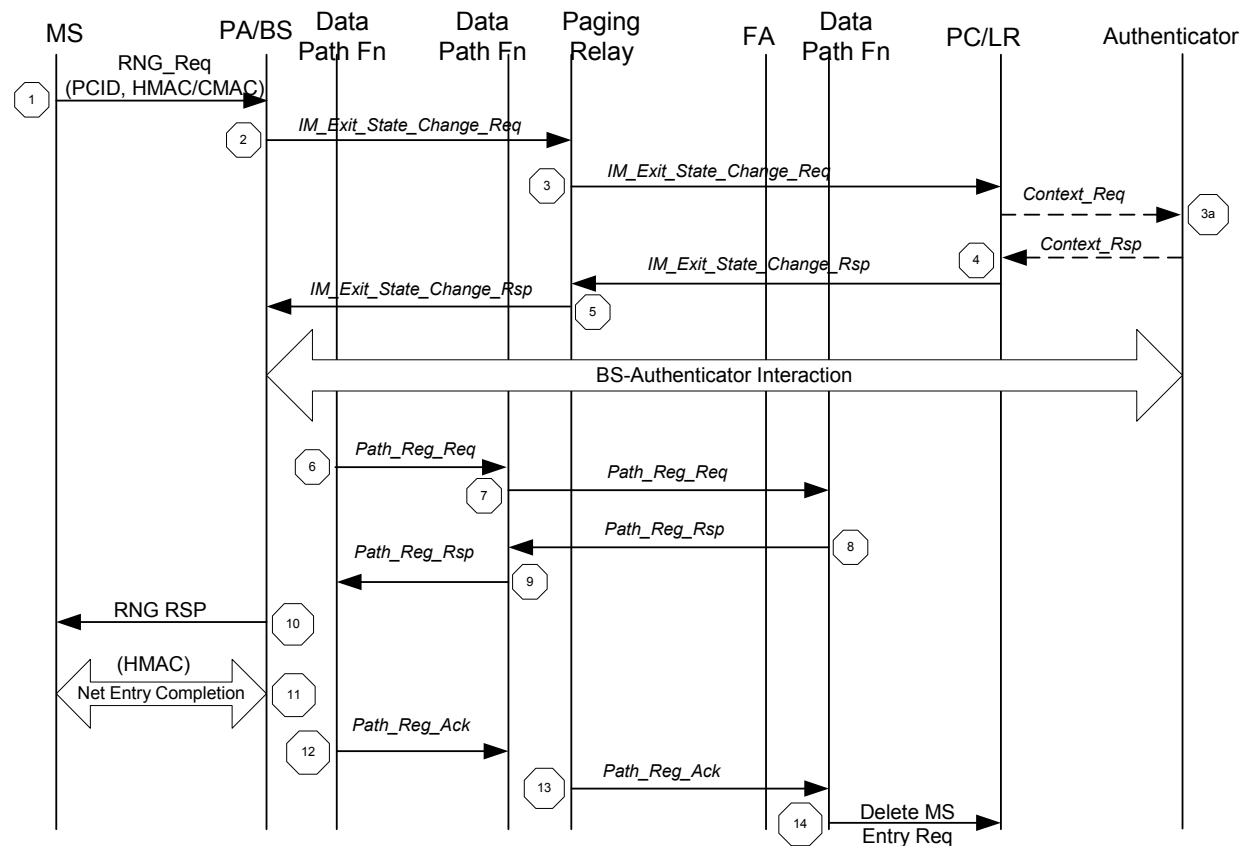
3   **Figure 7-98 - MS Exiting Idle Mode**

4   Flow description:

5   1) MS initiates exit from IDLE mode procedure (e.g., as a result of Paging) and sends RNG_REQ as described in
6   IEEE 802.16 specification. Ranging Purpose Indication must be set to one (1) and PC ID TLV must be present,
7   thus indicating that the MS intends to Re-Entry from Idle Mode.

8   2) BS receives RNG_REQ message from MS. Correspondingly, PA sends IM-Exit-State-Change Request to
9   Paging Relay (when PA is not directly connected to Anchor PC, as shown). IM-Exit-State-Change Request
10   contains the following information from the RNG_REQ: MS ID (MAC Address), BSID, PC ID (PCID). If the
11   BS has the Authenticator ID and CMAC/HMAC digest already when the BS receives RNG-REQ message from
12   MS, the BS_Authenticator interaction procedure of verifying RNG-REQ can be started simultaneously.

13 3) Paging Relay receives *IM_Exit_State_Change_Req* from BS and sends it to Anchor PC. Paging Relay recognizes
14   the PC according to the received PCID field. *IM_Exit_State_Change_Req* contains the following information:
15   MS ID (MAC Address), BSID;

16 4a) When receiving the *IM_Exit_State_Change_Req*, the Anchor PC/LR proceeds to request the security context
17   from the Anchor Authenticator and receives it in a *Context_Rpt* message. If the PC and Authenticator are co-
18   located this step is not required. It also initiates the cancel Paging Procedure at this point.

19 4b) Anchor PC receives the *IM_Exit_State_Change_Req*, and sends *IM_Exit_State_Change_Rsp* to the Paging
20   Relay. *IM_Exit_State_Change_Rsp* contains the following information: MSID, ID of Anchor DPF,
21   Authenticator ID, MS Idle Mode Retain Information, (SFIDs, CIDs, QoS context, etc.);

22 5) Paging Relay forwards the *IM_Exit_State_Change_Rsp* to the BS; The AK is fetched from the appropriate
23   authenticator in order to verify the RNG-REQ.

1　6) The Data Path function in BS starts data path establishment – it sends *Path_Reg_Req* to the Data Path Function
2　　across R6. *Path_Reg_Req* contains the following information: MSID, Data Path Fn Id (e.g., IP Address),
3　　Service Flow info (SFIDs, QoS context, etc.) It also initiates the cancel Paging Procedure at this point.

4　7) The Data Path Function across R4 continues data path establishment to the anchor Data Path function (which
5　　could be collocated with FA as shown in the figure) - sends *Path_Reg_Req* to anchor Data Path Function.
6　　*Path_Reg_Req* contains the following information: MSID, Service Flow info (SFIDs, QoS context, etc.)

7　8) The anchor Data Path Function confirms data path establishment - sends Data Path Establishment across R4.
8　　*Path_Reg_Rsp* contains: MSID, Service Flow info (SFIDs, Tunnel parameters, QoS context, etc.)

9　9) The Data Path functions cross R6 confirms data path establishment toward SBS— sends Data Path
10　　Establishment Response to the Data Path Function in SBS. *Path_Reg_Rsp* contains: MSID, Service Flow info
11　　(SFIDs, QoS context, etc.)

12　10)　BS sends RNG_RSP to the MS formatted according to IEEE 802.16e specification. This RNG_RSP SHOULD
13　　deliver information necessary to resume service in accordance with Idle Mode Retain Information.

14　11)　The MS completes Network Re-Entry from the Idle Mode as described in IEEE 802.16e specification.

15　12)　Upon the MS Network Re-Entry completion the BS sends *Path_Reg_Ack* to the Data Path function across R6
16　　confirming data path establishment completion. *Path_Reg_Ack* message contains: MSID

17　13)　The Data Path function across R4 sends *Path_Reg_Ack* to the anchor Data Path function. *Path_Reg_Ack*
18　　contains: MSID.

19　14)　The anchor Data Path function sends a Delete MS entry message to PC/LR in order to delete the idle mode
20　　entry associated with the MS in the PC.

21　**7.10.3.3　MS Performing Location Update, Secure Location Update**

22　MS performs Location Update procedure when it meets the LU conditions as specified in IEEE 802.16e
23　specification. The MS shall use one of two processes for Location Update: Secure Location Update or Unsecure
24　Location Update. Un-Secure Location Update process is performed when MS and BS do not share valid security
25　context means that BS is not able to receive a valid AK (e.g., MS crossed Mobility Domain boundaries or PMK
26　expired).

27　Un-Secure Location Update results in MS network re-entry and re-authentication. It is performed in the same way as
28　a regular MS network entry process.

29　The Secure Location Update procedure:
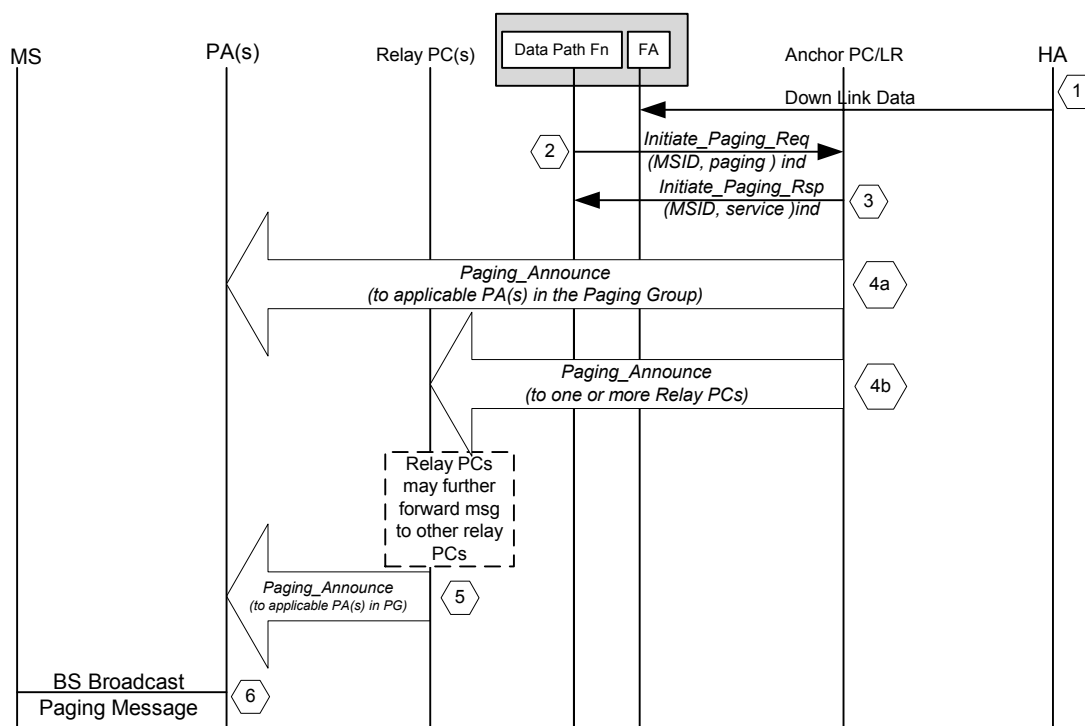
Figure 7-99 - Secure Location Update

1) MS initiates Location Update, or the Location Update is forced by network if the conditions described in IEEE 802.16e specification are met and as a result, the MS sends RNG_REQ. Ranging Purpose Indication must be set as described in IEEE 802.16e specification indicating that the MS intends to update its location. PC ID (which points to PC acting as MS's Anchor PC) must also be present.

2) PA sends *LU_Req* to the Paging Relay (as shown in the figure). It contains information like PCID, BSID.

3) Paging Relay sends *LU_Req* to Anchor PC. It contains: MSID, BSID and recommended paging parameters (PGID, Paging cycle, Paging Offset) etc.

4) When PC/LR receives a *LU_Req* message and the security information is not retained in the LR, it will request the security information from the Authenticator. If the PC and the Authenticator are co-located this step is not required.

5) If the *LU_Req* is accepted by Anchor PC and the Paging operation is still continuing, at this step .Paging_Annouce to 'Stop Page' may also be sent to the Paging groups defined for the MS. Anchor PC either accepts the recommended paging parameters or assigns new PGID and the paging parameters and sends *LU_Rsp* message to Paging relay. *LU_Rsp* includes: MSID, BSID, PGID and paging parameters, Anchor Authenticator ID, PCID etc.

6) Paging Relay forwards *LU_Rsp* to PA.

7) BS (where PA resides) determines whether it has a valid AK for the MSID from the indicated Anchor Authenticator. If it does not, the BS sends *Context_Req* (not shown in the diagram) to the Anchor Authenticator. *Context_Rpt* (not shown) provides the AK sequence number, as well as the AK for the BS-MS secure association (as specified in 7.20.2 "Context Transfer Protocol"

8) BS (where PA resides) uses AK to verify the integrity of the RNG-REQ received from MS. If the MS's RNG_REQ is successfully verified, the BS responds to the MS with RNG_RSP with HMAC/CMAC. If the RNG-REQ could not be verified (such as when the Anchor Authenticator could not provide an AK), the BS begins the "Un-secure Location Update" sequence by initiating re-authentication;;

9) In the case where RNG_REQ was verified, PA sends *LU_Cnf* to Paging Relay (incl. BSID, success indication). It indicates location update from MS has been authenticated and the process is successfully completed.

10) Paging Relay forwards LU_Cnf to Anchor PC. Anchor PC receives LU_Cnf and finally updates MS location in the LR. In the event that the Location Update was triggered by paging the MS, the PC/LR initiates the cancel paging procedure (as described above). It may send the Paging Announce message to stop the paging operation within the paging groups.

11) If PC relocation has occurred during the LU procedure, the PC will send Context Response Ack   message with the LU result to the Authenticator.

.

7.10.3.4 Paging Operation and R3 Mobility Management

Migration of foreign agent while the MS is in idle mode (e.g., when idle mode MS moves) shall be considered an implementation option. Such FA migration requires that MS come out of idle mode to complete MIP registration procedure.

The alternative is to not migrate FA while MS remains in idle mode. For such a scenario, the following points are noteworthy:

1) For the registration lifetime for L3 connectivity (e.g., MIP registration lifetime or DHCP lease time), the idle mode MS shall retain its IP address without IP address renegotiation. Registration lifetime will be set to max by the MS when Idle mode is entered.

2) While MS moves across PG boundaries, it performs LU as per procedures above, without resulting in any FA migration. During this time, R3 shall be maintained between Home Agent and the FA. If Anchor DPF and FA are not collocated, the bearer tunnel between the FA and Anchor DPF is also maintained.

3) Upon packet arrival at HA destined for MS, and their delivery over R3 to Data Path function associated with FA, packets shall be buffered in ASN until MS paging procedures are completed.

4) The Anchor PC sends *Paging_Announce* over R4 using either topologically aware or topologically unaware procedures. Paging Relays receiving *Paging_Announce* from PC forward it over R6 interface to all the BSs (or Paging Relay(s)) associated with the PGID in the Paging Request.) via single step or multi-step procedures (see stage 3 [xx] for details).

5) MS performs a full network entry.

6) MS may re-register with its old Home IP address. Tunnel establishment (over R6 and R4) is performed between Data Path functions in SBS, intermediate Data Path Functions, and the Data Path function associated with FA in a way similar to HO process.

7) Packets are transferred from Data Path associated with FA to other Data Path Functions in the path over R4.

8) R3 traffic anchor point (i.e., Data Path function associated with FA) and FA may migrate from the current Anchor point to another Anchor point   or may optionally stay as they are.

9) When MS goes out of Idle Mode, the PC/ LR entry corresponding to this MS is deleted.

10) When MS goes into Idle Mode, serving FA could migrate to the same ASN as the anchor authenticator or as the anchor PC. This is left as an implementation option, as Idle but stationary MS will not benefit from such migration.

11) As the MS has no way to determine a-priori whether it shares a valid security context with the BS,, the MS will always include a HMAC/CMAC tuple in the RNG-REQ. The BS and the anchor authenticator will either validate the HMAC/CMAC or reject the *LU_Req*.
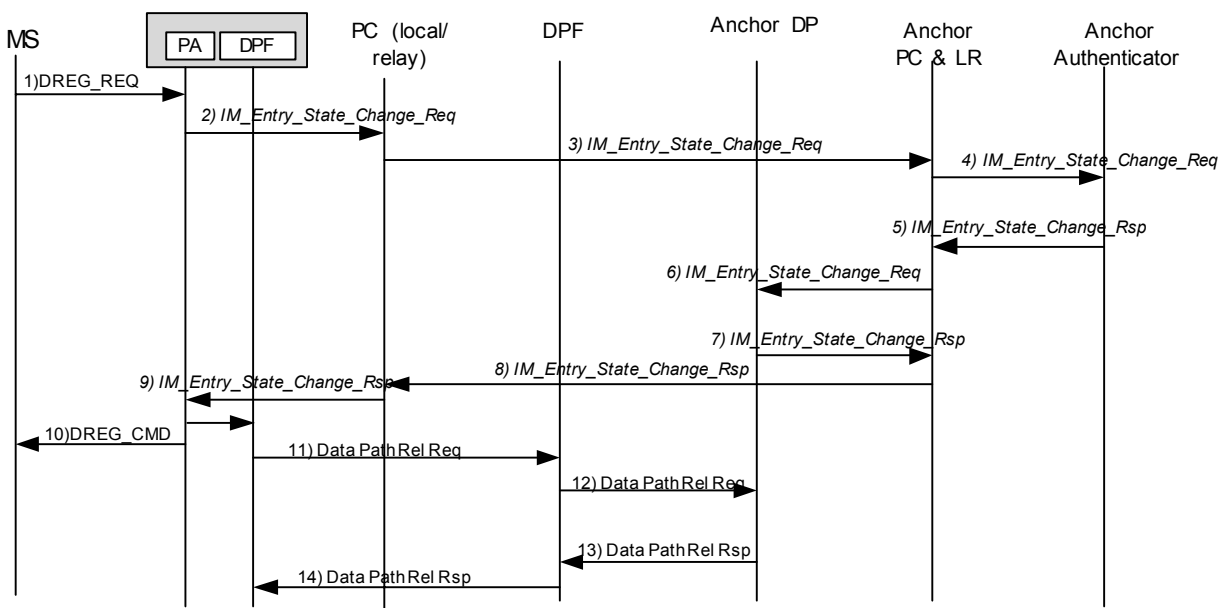
1 **7.10.3.5 MS entering IDLE mode**

2

3   **Figure 7-100 - MS Entering Idle Mode**

4   Dashed arrows are internal to network elements and out of scope.

5   MS enters Idle mode when there is no data to exchange between the MS and the network. MS Idle mode entry could
6   be initiated by either the MS or the BS.

7   1)   If MS decides to initiate entry into Idle Mode, then it sends DREG_REQ formatted as described in IEEE
8   802.16e. The De-Registration Request Code is set to 0x01 indicating that the MS intends entering Idle Mode.

9   2)   Regardless of who (MS or BS) initiated the entry into idle mode, the PA in the serving BS sends
10   *IM_Entry_State_Change_Req* message to its local Paging Controller (who oversees paging at this base station).
11   The *IM_Entry_State_Change_Req* contains the following information: MSID, BSID, PG_ID, Idle Mode Retain
12   Information, etc

13   3)   Upon receipt of *IM_Entry_State_Change_Req* from the PA, the local PC assigns an Anchor PC for this mobile,
14   and puts this information as a recommendation into the message. The chosen anchor PC could be the local
15   Paging Controller itself or a different PC based on implementation considerations such as network policy, MS
16   profile or Relay PC loading conditions. Further, the local PC sends the *IM_Entry_State_Change_Req* message
17   to the recommended Anchor PC, the *IM_Entry_State_Change_Req* message contains the following information:
18   Recommended PC_ID, PG_ID, Paging_CYCLE, Paging_OFFSET, some MS contexts(including Anchor
19   Authenticator ID, Anchor DPF ID etc.

20   4~5）The Anchor PC contacts the Anchor Authenticator to verify that the MS is allowed to enter Idle mode, and
21   may transfer some security context to Anchor Authenticator to retain, such as PKM contexts. Anchor
22   Authenticator records the Anchor PC ID into MS context and reply *IM_Entry_State_Change_Rsp* to Anchor PC
23   including Idle mode authorization indication;

24   6~7) These steps represent the handshake between the Anchor PC and Anchor DPF of the MS entering Idle mode.
25   Anchor PC/LR sends *IM_Entry_State_Change_Req* message to the Anchor DPF/FA to indicate the MS entering
26   Idle Mode. The Anchor DPF updates the information of this MS including the Anchor PC ID of this MS, and
27   then the Anchor DPF responds back with *IM_Entry_State_Change_Rsp* to Anchor PC/LR.

28   8)   If confirmed, Anchor PC either accepts the recommended paging parameters and PGID or newly assigns these
29   parameters and updates Location Register with current information including the DPF ID, and sends
30   *IM_Entry_State_Change_Rsp* back to the Local PC. The *IM_Entry_State_Change_Rsp* contains: MSID, actual
31   paging parameters (selected PGID, Paging CYCLE, Paging OFFSET), PCID (The ID of the GW Acting as

1   Anchored PC formatted as specified in IEEE 802.16e to be delivered to the MS with DREG_CMD as "PC ID")

2   and IDLE mode authorization indication

3   9) The Local PC forwards the *IM_Entry_State_Change_Rsp* message to PA;

4   10) The PA sends DREG_CMD to the MS either in response to its DREG_REQ or as an unsolicited response (BS

5   initiated entry into idle mode), as specified in IEEE 802.16e containing "PC ID" field in the DREG_CMD

6   which points to the assigned Anchor PC for the MS, the assigned Paging CYCLE, and the assigned Paging

7   OFFSET

8   11～14） After receiving DREG_REQ message from MS and the expiration of the Management Resource Holding

9   Timer, the DPF associated with PA located in BS initiates the related R6, R4 data path release procedure.

10 Note: The procedure illustrated in Figure 7-100 and described here is the general procedure of accomplishing entry

11 into idle mode. Depending on the implementation and choice of ASN profile, the procedure can be optimized by

12 changing the sequence and flow of messages. The implementation would still be compliant to the specification as

13 long as the messages and functional behaviors are not changed. Implementation details and optimizations are out of

14 Stage 2 document scope, therefore a general case that is profile agnostic is described in this document.

7.11 Data Path

16 Section 7.7.2.2.2 introduces Type 1 Data Paths for carrying either IP or Ethernet packets between peers within an

17 ASN or between ASNs. User payload packets are transferred over Type 1 Data Paths between ASNs (R4) or

18 between the BS and the ASN-GW of an ASN exposing an interoperable R6 reference point. The functions to set up

19 and manage such data paths are described in Section 7.7.2.2.2.2.

20 This section provides additional information about the encapsulation of user payload packets within Type 1 Data

21 Paths. Detailed message formats and tag values are given in Stage 3. For routed transport architecture an IP-in-IP

22 type of tunnel protocol has to be applied. GRE is taken as an example in this section to show the required functions

23 of the tunnel protocol.

24 For transport of user payload packets over R1, the [1] specification amended by [2] supports various types of

25 convergence sub-layers to address different types of service deployment scenarios. Different convergence sub-layers

26 are provided for Ethernet as well as for IP providing particular classification and encapsulation functionalities.

27 Several different convergence sub-layers can coexist within the same ASN, e.g. IPv4-CS can coexist in the same

28 ASN with IPv4oETH-CS. Handover of MS from an Ethernet based CS to a plain IP based CS within the same ASN

29 or when moving from one ASN to another ASN is not supported.

7.11.1 IP Convergence Sub-layer

31 The IP convergence sub-layers are defined in [2] in Section 5.2.6. When one of the IP CS is employed, IP datagrams

32 are carried directly in the payload of 802.16 PDUs. Classifiers for IP CS connections can make use of fields in the IP

33 header as well as source and destination port numbers of transport protocol fields. Packet header suppression is an

34 optional method operating with existing convergences sub-layers.

7.11.2 Services Provided over IP Convergence Sub-layer

7.11.2.1 IP Connectivity for a Single Host MS

37 A single IP address is assigned to the MS deploying separate CIDs for up- and downlink.

38 Multiple CID assignments are possible to provide multiple service flows under the same IP address.

7.11.2.2 IP Connectivity for Multiple Hosts Behind the MS

40 This service is out of scope for Release 1.0.0

7.11.3 IP Convergence Sub-layer Transport Architecture

42 Figure 7-101 shows the generic protocol layering for the control plane as well as the data path applying IP-CS on

43 R1, R6 (when exposed), R3 and R5. GRE is provided as example of an IP-in-IP tunnel protocol.
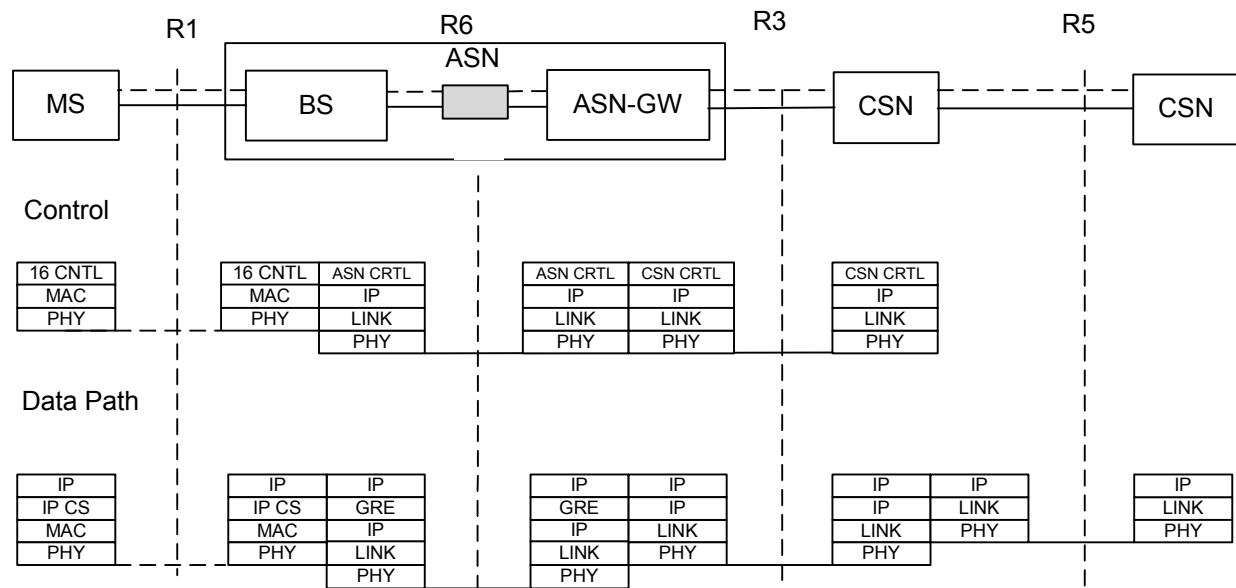
Figure 7-101 - Protocol Layer Architecture for IP-CS

7.11.4 IP Packet Forwarding Over the Air

In case of IP-CS the MS SHALL encapsulate IP datagrams from the IP host layer into 802.16 MAC frames for upstream over the R1 reference point. The BS (on ASN side) SHALL encapsulate IP datagrams received from the ASN-GW IP router via R6 into 802.16-MAC frames for downstream over R1. All IP datagrams are transferred over R1 according to the applied classifier for the particular CID.

7.11.5 Ethernet Convergence Sub-layer

The Ethernet convergence sub-layers are defined in [2] in Section 5.2.4. When one of the Ethernet CS is employed, IEEE802.3 frames carrying the IP datagrams are encapsulated in the payload of 802.16 PDUs. Classifiers for Ethernet CS connections can make use of fields in the 802.3 header as well as higher layer protocol fields (according to the specific Ethernet CS type). Packet header suppression (PHS) is an optional method operating with existing convergences sub-layers. PHS can serve to replace the entire 802.3 header and eventually even higher layer header fields with a one-byte PHS-Index. The BS MAY implement subnet-wide forwarding of subscriber broadcasts so as to complete LAN emulation functionality. This broadcast functionality MAY include filtering, filters MAY be implemented at the MS (using classifiers with the "Drop action" or with a filter above the MAC layer) so as to restrict inappropriate traffic (e.g. Printer announcements) from the uplink; or the BS MAY respond to ARP requests rather than propagating them.

7.11.6 Services Provided Over ETH CS

7.11.6.1 IP Connectivity for a Single Host MS

In this scenario, the MS implements a single "virtual LAN" endpoint that can be attached beneath a standard host IP stack on the client MS. Use of the 802.3/Ethernet CS (with optional PHS) provides various benefits, such as:

- Support for transport of downlink-direction unicast data packets that lack IP addresses (e.g. DHCPOFFER as described in [11]; Mobile IP signaling messages in scenarios described in [43] which carry destination IP address of 0.0.0.0)

- Seamless and reduced-latency support of client-based Mobile IP handovers: after an MS enters a new FA domain, the MAC-address-based classifiers associated with its active connections will still be valid (as they are independent of the care-of address) - so there is no need for the 3-way DSC handshake that is mandated by [1] to modify the classifiers.

- Ability to operate with a private Ipv4 address space (i.e. Even if multiple connectivity providers use the same private IP addresses, packets will be forwarded to the correct MSs).

1   •   Support for multiple access routers and load-balancing: the access router at the headend (which might be
2   located at the end of a L3 tunnel) MAY send ICMP-redirect to instruct the MS to communicate via a
3   different L3 gateway.

4   •   Independence of layer 2 data connectivity from IP endpoint configuration mechanisms: A fully functioning
5   ASN can be deployed using static layer-2 configuration only. The ASN can then work easily with AAA-
6   based IP parameter assignment or stateless autoconfiguration mechanisms (in addition to the more typical
7   DHCP or Mobile IP – and need not know which is in use.

8   •   Facilitation of bridging-based ASN architecture: Use of the 802.3/Ethernet CS enables the BS application
9   to perform transparent bridging or ARP-based bridging (i.e. [6], which ensures all packets traverse the
10   gateway for accounting purposes). A bridging-based ASN enables a simple mechanism for intra-ASN
11   datapath updates via gratuitous broadcasts

12   7.11.6.2 IP Connectivity for Multiple Hosts Behind a MS

13   This topic is for further study and deferred beyond Release 1.0.0

14   7.11.6.3 WiMAX Access to DSL Infrastructure

15 This is typically a fixed/nomadic usage scenario, in which a user host (typically a PC or network equipment hosting
16 IP based applications) behind the MS has an Ethernet connection to an IEEE 802.16 MS, which provides broadband
17 access from a service provider with a DSL infrastructure. There is an Ethernet connection from the SS to the BS
18 using the Ethernet CS. There is an Ethernet connection over the ASN from the BS to the BRAS (Broadband Remote
19 Access Server). PPPoE is used on top of the mobile WiMAX access network to provide a user connection that is
20 similar to the existing DSL deployment.

21   7.11.6.4 Ethernet Service to Enterprise Customer Locations

22 This is typically a fixed/nomadic usage scenario. An enterprise location has a MS with an Ethernet interface that
23 could support one or many user hosts in the local network through a switch. There is an Ethernet connection from
24 the SS to the BS using the Ethernet CS. An Ethernet connection from the ASN to the core network edge point could
25 be provided over IP. The network service to the enterprise customer is an Ethernet service from the core network all
26 the way to the enterprise MS. This could be an extension of a MetroEthernet connection based on IEEE 802.1Q
27 VLANs to manage the service. The MS location could be a branch of a main network that benefits from being
28 connected at the Ethernet layer. If the local network is controlled by the enterprise, the hosts can be assumed to be
29 trusted to use proper QoS signaling such as IEEE 802.1Q VLAN tags or DSCP markings.

30   7.11.6.5 IEEE802.1Q VLAN Network Service

31 IEEE802.1Q support can be viewed in the following two ways:

32   •   The VLAN ID and the priority bits are transported across the WiMAX link with no alteration (IEEE802.1Q
33   VLAN transport). This assumes the MS part of the VLAN transport network architecture and the hosts
34   behind the MS are trusted to use the correct VLAN Id and Priority.

35   •   The VLAN ID and the Priority are translated or stacked or inserted/removed when transitioning the
36   WiMAX link (IEEE802.1Q VLAN translation). This allows the network connected to the MS to have its
37   own set of VLAN IDs and Priorities, which can be independent of the VLAN transport network
38   architecture. The translation of these VLAN IDs and priorities will allow the CSN to switch relatives to its
39   provisioned VLAN IDs. This also allows for networks connected to the MS that have no tagging capability
40   to be able to be switch to the customer specific VLAN (in the case of a wholesaler model) in the core
41   network.

42 IEEE802.1Q VLAN Network Service is deferred into Release 1.0.0.5.

43   7.11.7 ETH-CS Transport Architecture

44 Figure 7-102 shows the generic protocol layering for the control plane as well as the data path applying ETH-CS on
45 R1, R6 (when exposed), R3 and R5. GRE is provided as example of an IP-in-IP tunnel protocol.
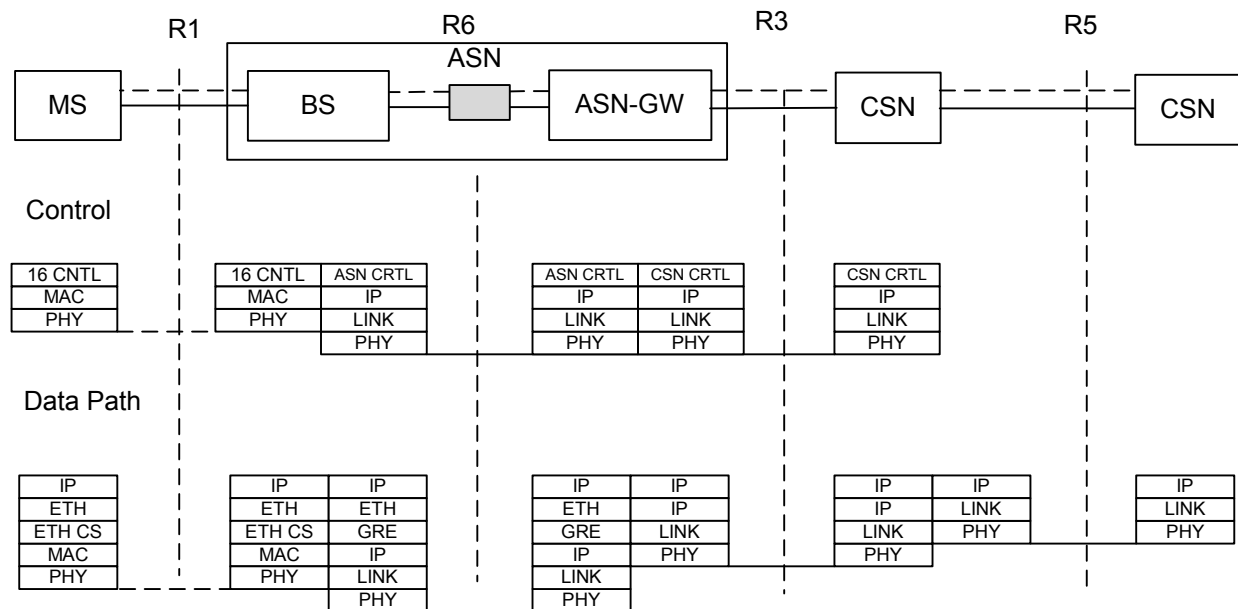
1

2 **Figure 7-102 - Protocol Layer Architecture for ETH-CS**

3 ### 7.11.8 ETH CS Packet Transmission Format over R1

4 IEEE802.16 MAC frames are protected by a MAC layer FCS. The FCS trailer of Ethernet packets does not provide
5 a higher level of protection and will be suppressed for the transmission over the air. This reduces the packet
6 overhead by 4 bytes. The Ethernet FCS is re-generated at the receiving side out of the transmitted data and appended
7 to the packet.

Ethernet frame format

DA	SA	Length/Type	Data	FCS

Transmission of Ethernet over R1

DA	SA	Length/Type	Data

IEEE 802.1Q frame format

DA	SA	0x8100	Tag Control Information	Length/Type	Data	FCS

Transmission of IEEE 802.1Q over R1

DA	SA	0x8100	Tag Control Information	Length/Type	Data

8

9 **Figure 7-103 - FCS Suppression Over R1**

10 ### 7.11.9 Ethernet Packet Filtering Over the Air

11 To reserve resources over the R1 reference point, Ethernet broadcast packets are filtered. The filter MAY be
12 implemented at the MS (using classifiers with the "Drop action" or with a filter above the MAC layer) so as to
13 restrict inappropriate traffic (e.g. Printer announcements) from the uplink; or the ASN MAY respond to ARP
14 requests rather than propagating them. Both Ingress Broadcast Filtering and Egress Broadcast Filtering SHALL
15 have the ability of being enabled or disabled. A summary of the filter operation is described below. Details of
16 operation are given in Stage 3.

1 ### 7.11.9.1 Ingress Filter MS

2 The MS Ingress Filter is responsible for filtering and discarding unwanted packet from going over the air. Filtering
3 can be enforced at the MAC or the IP layer. Packet from a host SHALL be discarded if that packet's source MAC
4 address cannot be found in the current MS authenticated managed MAC list. The authenticated MAC list is
5 composed from the authentication methods defined this document (DHCP Response MAC/IP). In the case of
6 Address Resolution Protocol messages, the MS Ingress Filter SHALL permit all to pass to be solved by the BS. The
7 Ingress Filter SHALL permit all DHCP messages to pass to the BS for further processing. Upon receiving any
8 packet from the MS that is identified as an IP datagram, the Ingress Filter SHALL discard the datagram if the source
9 IP address cannot be found in the current MS Authenticated MAC List.

10 ### 7.11.9.2 Egress Proxy ARP/Filter

11 The ASN SHALL have the ability to enable or disable all ARP Ingress Proxy Agent and/or ARP Egress Proxy
12 Agent functionality defined herein. The functionality of these agents is to manage broadcast traffic going over the
13 R1 reference point. ARP Egress Proxy Agent SHALL unicast an ARP Response back to that trusted source on
14 behalf of the MS and unicast the APR request to the MS, provided that the target MAC address matches an entry in
15 the Authenticated MAC List. The ARP Egress Proxy Agent SHALL issue a gratuitous ARP for any new addition
16 to the Authenticated MAC ID.

17 ## 7.11.10 Tunneling within the ASN

18 ### 7.11.10.1 IP-in-IP Tunnel Protocol GRE

19 If GRE is used as the tunneling mechanism between the ASN-GW and the BS (over R6) and between ASN-GW and
20 ASN-GW (over R4), then the Tunneling Info Extension SHOULD be set to GRE. The value for the GRE Key is
21 negotiated between the ASN-GW and the BS or between ASN-GW and ASN-GW. The GRE Payload Protocol
22 Types are assigned according to [3] for IP and Transparent Ethernet Bridging.

23 The encapsulation format for GRE appears in Figure 7-104.

24

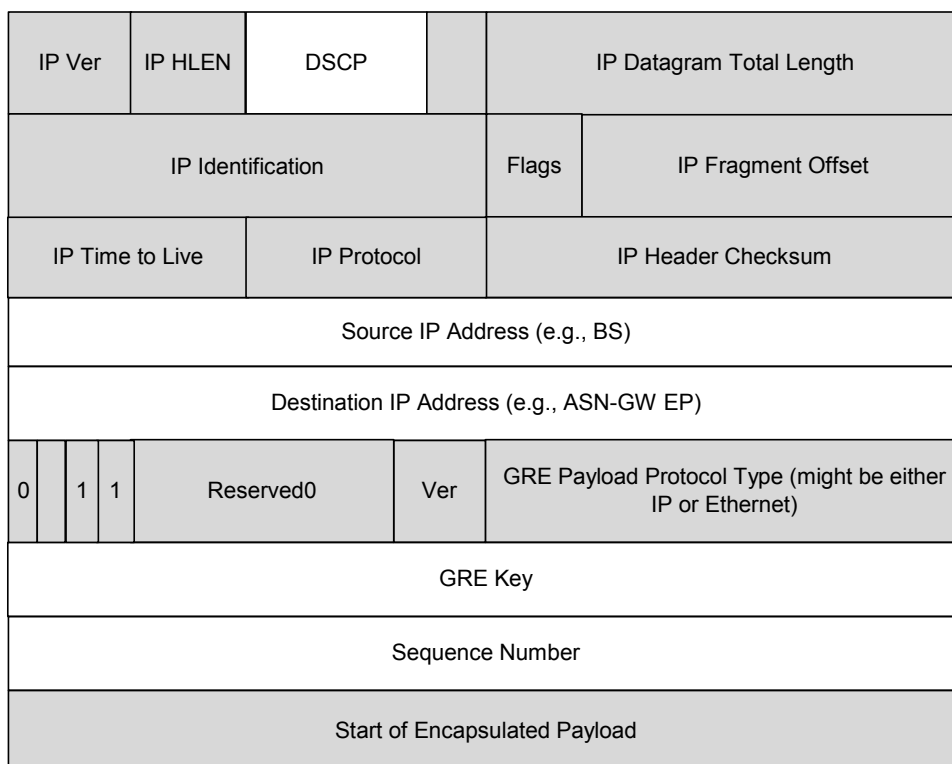| IP Ver	IP HLEN	DSCP		IP Datagram Total Length			
IP Identification				Flags	IP Fragment Offset		
IP Time to Live		IP Protocol		IP Header Checksum			
Source IP Address (e.g., BS)							
Destination IP Address (e.g., ASN-GW EP)							
0		1	1	Reserved0	Ver	GRE Payload Protocol Type (might be either IP or Ethernet)	
GRE Key							
Sequence Number							
Start of Encapsulated Payload							

25 **Figure 7-104 - GRE Encapsulation**

1 • DSCP in the Encapsulation IP Header specifies the QoS Class. Note that it MAY differ from the DSCP in
2   the Encapsulated Payload.

3 • Source and Destination IP Addresses specify the tunnel end points.

4 • The meaning of the GRE Key value is defined by the node that allocates the Key value.

5 • The Sequence Number might be used for synchronization of Data Delivery during HO.

6 Figure 7-105 shows an example of IP Data Path with GRE Encapsulation within the ASN.
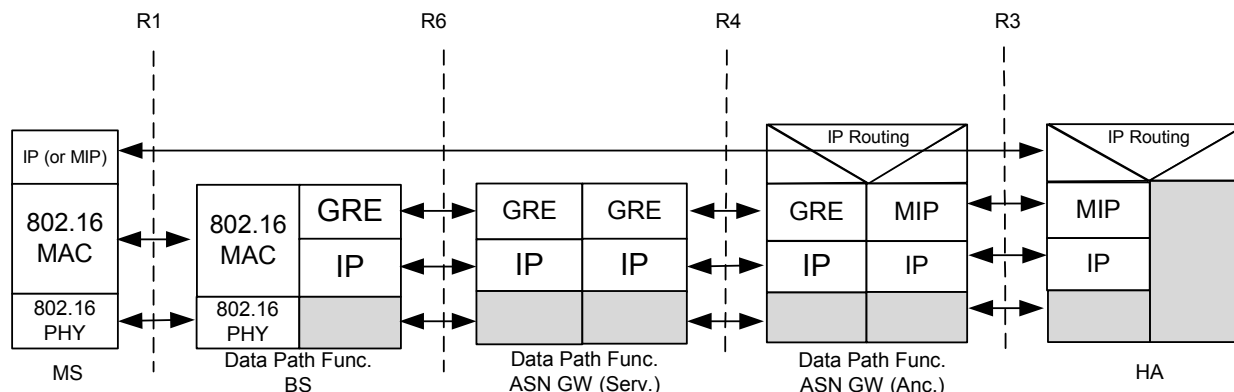
7

Figure 7-105 - GRE Encapsulation for IP CS

9 The same IP CS Data Path can be used either for Proxy MIP or for Client MIP.

10 The BS maps the IEEE 802.16 Connections (CID) on the R6 GRE Tunnels for both downstream and upstream
11 traffic. There is 1 to 1 correspondence between the IEEE 802.16 Connections and the GRE Keys (in case per Service
12 Flow granularity on R6/R4) or 1 to n correspondence (in case per MS granularity on R6/R4). The BS does not need
13 to implement any IP routing functionality. This mechanism is applied either for unicast or for multicast traffic.

14 The ASN-GW terminates the R6 Tunnels from BS. Various encapsulation techniques (e.g. GRE, MPLS, etc.) might
15 be used for R6 Tunnels and the granularity of the tunnel IDs might also vary (e.g. the Tunnel IDs might be assigned
16 per Connection, per MS, per IP Realm, etc.). The R6 Data Path Function protocol supports encapsulation type and
17 Tunnel ID granularity negotiations.

18 • In case of "per SF granularity" Anchored ASN-GW (Data Path Function) SHALL classifying the
19   downstream traffic.

20 • In case of "per MS granularity" BS (Data Path Function) SHALL classifying the downstream traffic.

21 MS SHALL always classify the upstream traffic.

7.12 VoIP Services

23 While existing mechanisms specified in the QoS framework and accounting and charging framework could be used
24 by the CSN operator to support VoIP, fulfillment of all quantitative requirements, regulatory requirements and
25 requirements mentioned in Section 7.12 for VoIP are outside the scope of Release 1.0.0.

7.12.1 Emergency Service

27 Emergency Service is considered as a non-subscription based service, provided by the network operator (NSP) or
28 third party IP service providers (ASP). This service does not require explicit authentication and authorization of the
29 Caller. Decision on the access authentication for using emergency service and analysis of the security threats are
30 FFS.

31 Figure 7-106 depicts the high-level view of the emergency service architecture.
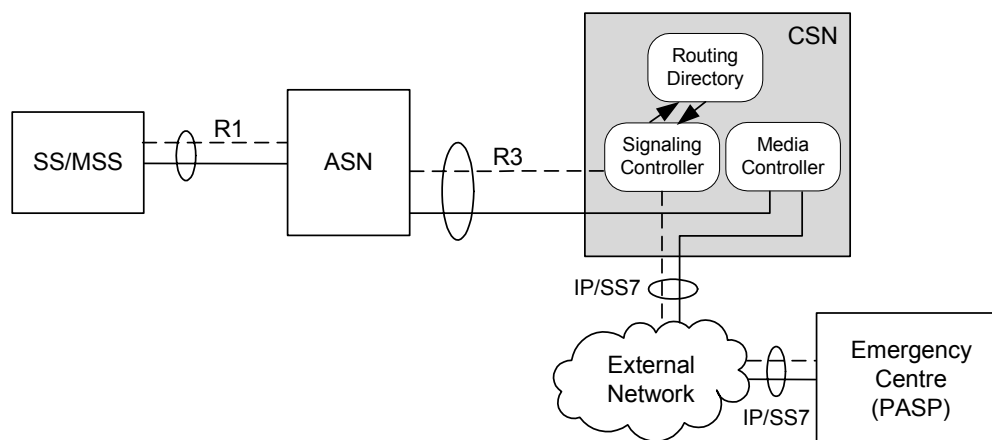
Figure 7-106 - High-Level View of Emergency Service Architecture

There are four basic steps involved for supporting emergency service. They are as follows:

a) *Detection of emergency request:* Detection of the emergency request MAY be done by the MS or by the network entities within CSN based on certain criteria outside the scope of Release 1.0.0.

b) *Location information:* Caller location plays a central role in routing emergency calls. The location information MAY be communicated from MS, BS, ASN entities, or by some other means. The exact procedure on communicating location information as required by emergency services regulatory requirements is outside of the scope of Release 1.0.0.

c) *Finding the location of nearest PSAP (Public Safety Answering Point):* For practical reasons, each PSAP generally handles only calls for certain geographic area. Also, for time sensitive request like emergency service, it is better to handle request locally. Upon contacting PSAP, it forwards emergency calls to the emergency control center for the purpose of dispatching police, fire and rescue services. The address of the PSAP is based on the Caller's location information. The support is provided by the CSN through a functional entity labelled as "Routing Directory." This step is assumed to be supported by CSN in Release 1.0.0.

d) *Routing call to PSAP:* Once the location of the Caller and the address of PSAP are identified, the request is routed to the PSAP. This step is also assumed to be supported by CSN in Release 1.0.0.

Prioritization of the access and network resources is typically required in order to support emergency service in a reliable manner. The selection of an appropriate QoS for prioritization required by emergency service is based on the QoS framework discussed in this document. While the CSN operator could use an existing QoS signaling method specified in the framework, explicit prioritization support for emergency service support is outside the scope of Release 1.0.0.

8. ASN Profile Introduction

A profile maps ASN functions into BS and ASN-GW so that protocols and messages over the exposed reference point are identified. The following text describes the three profiles of an ASN based on the current Stage 2 specifications. These three profiles show three possible implementations of the ASN and do not necessarily mandate a vendor to support all three. If a vendor chooses to implement any given profile, then that vendor's implementation SHALL conform to the chosen profile as specified in this text. The depiction of a function on either the ASN GW or the BS in the figures below does not imply that the function exists in all manifestations of this profile. Instead, it indicates that if the function existed in a manifestation it would reside on the entity shown. For example, PMIP Client MAY not always be present in all manifestations of Profile A. However, if it is used, it SHALL reside on the ASN GW. Note that the intent of an ASN profile is to describe intra-ASN reference points for intra-ASN interoperability within the context of that profile. An ASN of any profile SHALL be interoperable with an ASN of any other profile through the inter-ASN reference points R4. Thus, the inter-ASN interoperability through reference points R4 is independent of any particular ASN profile.

Identification of the ASN profiles was done for the specific goal of providing a bound framework for interoperability among entities inside an ASN. Specifically, interoperability in relation to the protocols, primitives and messages associated with the reference points R6 and R4 is addressed. In this section, R6 is normative only for the profiles where it is exposed.

8.1 Profile A

ASN functions are mapped into ASN-GW and BS as shown in Figure 8-1. Some of the key attributes of Profile A are:

- HO Control is in the ASN GW

- RRC is in ASN GW that allows RRM among multiple BSs

- ASN Anchored mobility among BSs SHALL be achieved by utilizing R6 and R4 physical connections.
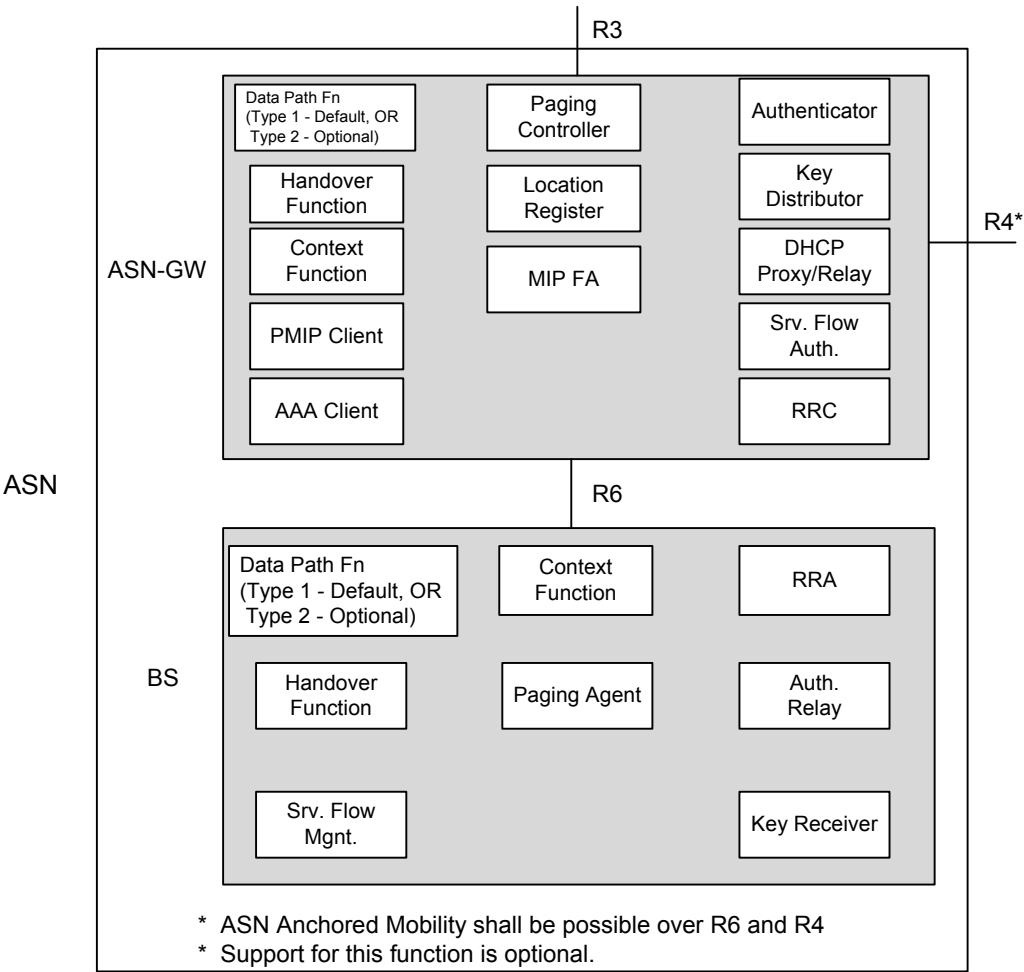
* ASN Anchored Mobility shall be possible over R6 and R4
* Support for this function is optional.

1

Figure 8-1 - Functional View of ASN Profile A

3   Table 8-1 illustrates the reference points over which intra-profile intra-ASN interoperability is achieved in
4   accordance with Profile A.

5   **Table 8-1 - Profile A Interoperability Reference Points**

Function Categories	Function	ASN Entity Name	Exposed Protocols, Primitives, API	Associated RP
Security	Authenticator	ASN GW	Auth Relay Primitives	R6
	Auth Relay	BS	Auth Relay Primitives	R6
	Key Distributor	ASN GW	AK Transfer Primitives	R6
	Key Receiver	BS	AK Transfer Primitives	R6

Function Categories	Function	ASN Entity Name	Exposed Protocols, Primitives, API	Associated RP
IntraASN Mobility	Data Path Fn (Type 1 or 2)	ASN GW & BS	Data Path Control Primitives	R6
	Handover Fn	ASN GW & BS	HO Control Primitives	R6
	Context Server & Client	ASN GW & BS		R6
L3 Mobility	MIP FA	ASN GW	Client MIP	R6
	MIP AR	ASN-GW	Client MIP	R6
Radio Resource Management	RRC	ASN GW	RRM Primitives	R6
	RRA	BS	RRM Primitives	R6
Paging	Paging Agent	BS	Paging & Idle Mode Primitives	R6
	Paging Controller	ASN GW	Paging & Idle Mode Primitives	R6
QoS	SFA	ASN GW	BS	R6
	SFM	BS		

8.2   Profile B

Profile B ASNs are characterized by unexposed intra-ASN interfaces and hence intra-ASN interoperability is not specified. However, Profile B ASNs shall be capable of interoperating with other ASNs of any profile type via R3 and R4 reference points. Inter-ASN anchored mobility SHALL be possible via R4.

Mapping of ASN functions is not specified for Profile B ASNs and as such there can be several different realizations of a Profile B implementation. These include, for example, implementations where all the ASN functions are located within a single physical device such as an Integrated BS network entity (IBS), and ones where ASN functionality is distributed over multiple network nodes. Specification of entities, interfaces, and protocols within a Profile B ASN are vendor specific implementation and outside the scope of this document.

R3

BS	FA	Location Register
Authenticator/AAAClient	PMIP Client	Paging Controller
Key Distributor		Paging Agent
		Context Fn
Key Receiver	SFA · RRC	
	SFM · RRA	Data Path Fn
DHCP Proxy/Relay		Handoff Fn

R4*
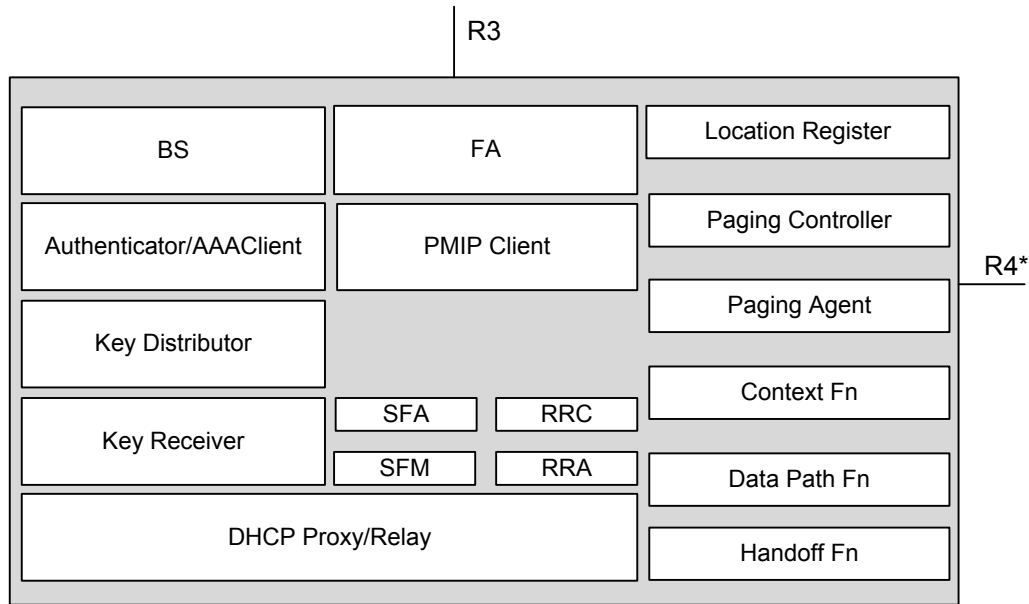
Notes:
1. No assumption made on physical co-location of functions within an ASN.
2. Allows centralized, distributed or hybrid implementations. Intra ASN interfaces are not exposed in this profile..

1

2 **Figure 8-2 - Functional View of Profile B**

3 ## 8.3   Profile C

4 According to Profile C, ASN functions are mapped into ASN-GW and BS as shown in Figure 8-3. Key attributes of
5 Profile C are:

6 •   HO Control is in the Base Station.

7 •   RRC is in the BS that would allow RRM within the BS. An "RRC Relay" is in the ASN GW, to relay the
8   RRM messages sent from BS to BS via R6.

9 •   As in Profile A, ASN Anchored mobility among BSs SHALL be achieved by utilizing R6 and R4 physical
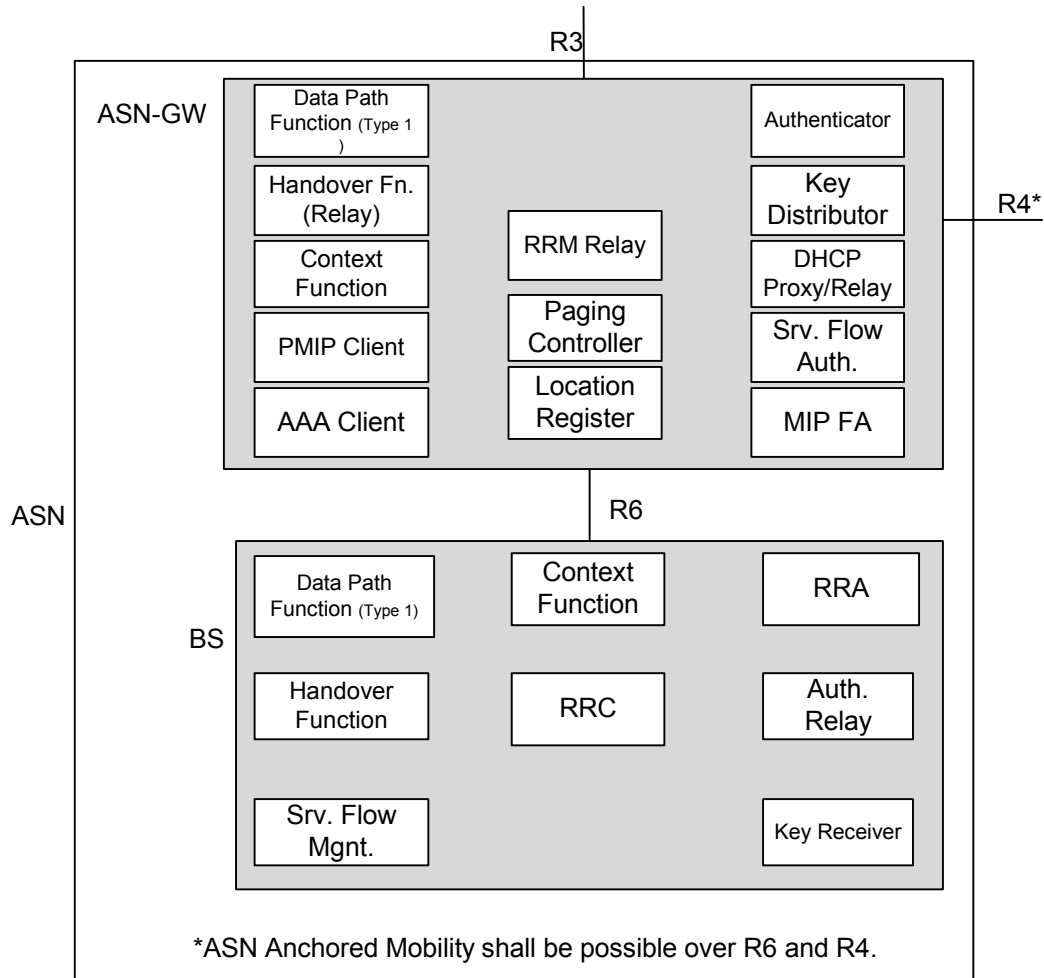10   connections.

1

Figure 8-3 - Functional View of ASN Profile C

Table 8-2 illustrates the reference points over which intra-profile intra-ASN interoperability is achieved in accordance with Profile C.

Table 8-2 - Profile C Interoperability Reference Points

Function Categories	Function	ASN Entity Name	Exposed Protocols, Primitives, API	Associated RP
Security	Authenticator	ASN GW	Auth Relay Primitives	R6
	Auth Relay	BS	Auth Relay Primitives	R6
	Key Distributor	ASN GW	AK Transfer Primitives	R6
	Key Receiver	BS	AK Transfer Primitives	R6

Function Categories	Function	ASN Entity Name	Exposed Protocols, Primitives, API	Associated RP
IntraASN Mobility	Data Path Function (Type 1)	ASN GW & BS	Data Path Control Primitives	R6
	Handover Fn	ASN GW & BS	HO Control Primitives	R6
	Context Server & Client	ASN GW & BS		R6
L3 Mobility	MIP FA	ASN GW	Client MIP	R6
	MIP AR	ASN-GW	Client MIP	R6
Radio Resource Management	RRC	BS	RRM Primitives	R6
	RRA	BS	None (BS internal)	-
	RRC Relay	ASN GW	RRM Primitives	R6
Paging	Paging Agent	BS	Paging & Idle Mode Primitives	R6
	Paging Controller	ASN GW	Paging & Idle Mode Primitives	R6
QoS	SFA	ASN GW	QoS Primitives	R6
	SFM	BS		

1