WiMAX Forum Network Architecture

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

[Part 3 – Informative Annex]

Release 1.1.0

July 11, 2007

WiMAX Forum Proprietary

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

1 **TABLE OF CONTENTS**

39

1 **TABLE OF FIGURES**

16

1   **LIST OF TABLES**

8

A. WiMAX NWG Reference Architecture Deployment Scenarios

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

This annex illustrates the motivations behind functional partitioning in WiMAX NWG reference architecture by depicting.

- Business relationships between WiMAX subscriber, NAP and NSPs
- Decomposition of NAP into physical elements and sharing of NAP by multiple NSPs
- A few end-to-end WiMAX deployment scenarios by NAPs and NSPs.

A.1   Business Relationships Between WiMAX Subscriber, NAP, and NSPs

Figure A-1 illustrates the contractual interrelationships between WiMAX subscriber, NAP, and NSPs.
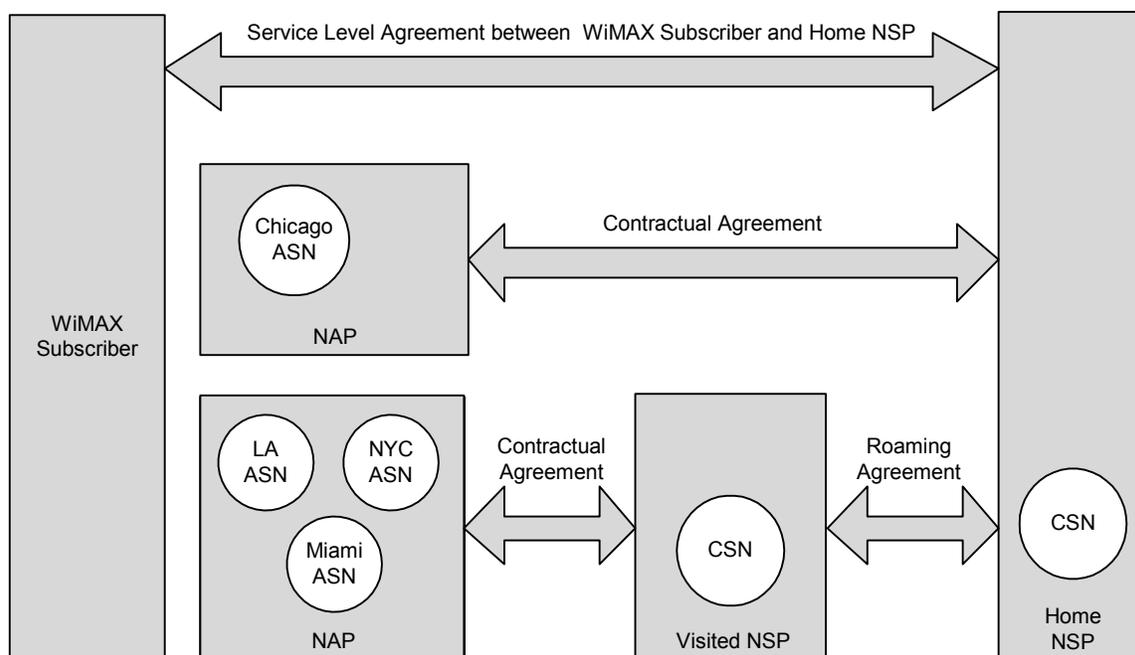
Figure A-1 - Business Relationship Between WiMAX Subscriber, NAP, and NSPs

As Figure A-1 illustrates, there are three basic types of business agreements between various business entities in WiMAX network:

   a.   **Service Level Agreement between WiMAX Subscriber and Home NSP.** This agreement allows the WiMAX subscriber to have access to a suite of WiMAX services and enable accurately billing for these services by the Home NSP.

   b.   **Contractual Agreement between NSP and NAP.** This agreement authorizes an NSP to use a given NAP's coverage area (or a part of it).

   c.   **Roaming Agreement between NSPs.** This agreement establishes roaming agreements between NSPs.

A.2   NAP Decomposition and NAP Sharing

Figure A-2 illustrates how a NAP may be decomposed in a given deployment.
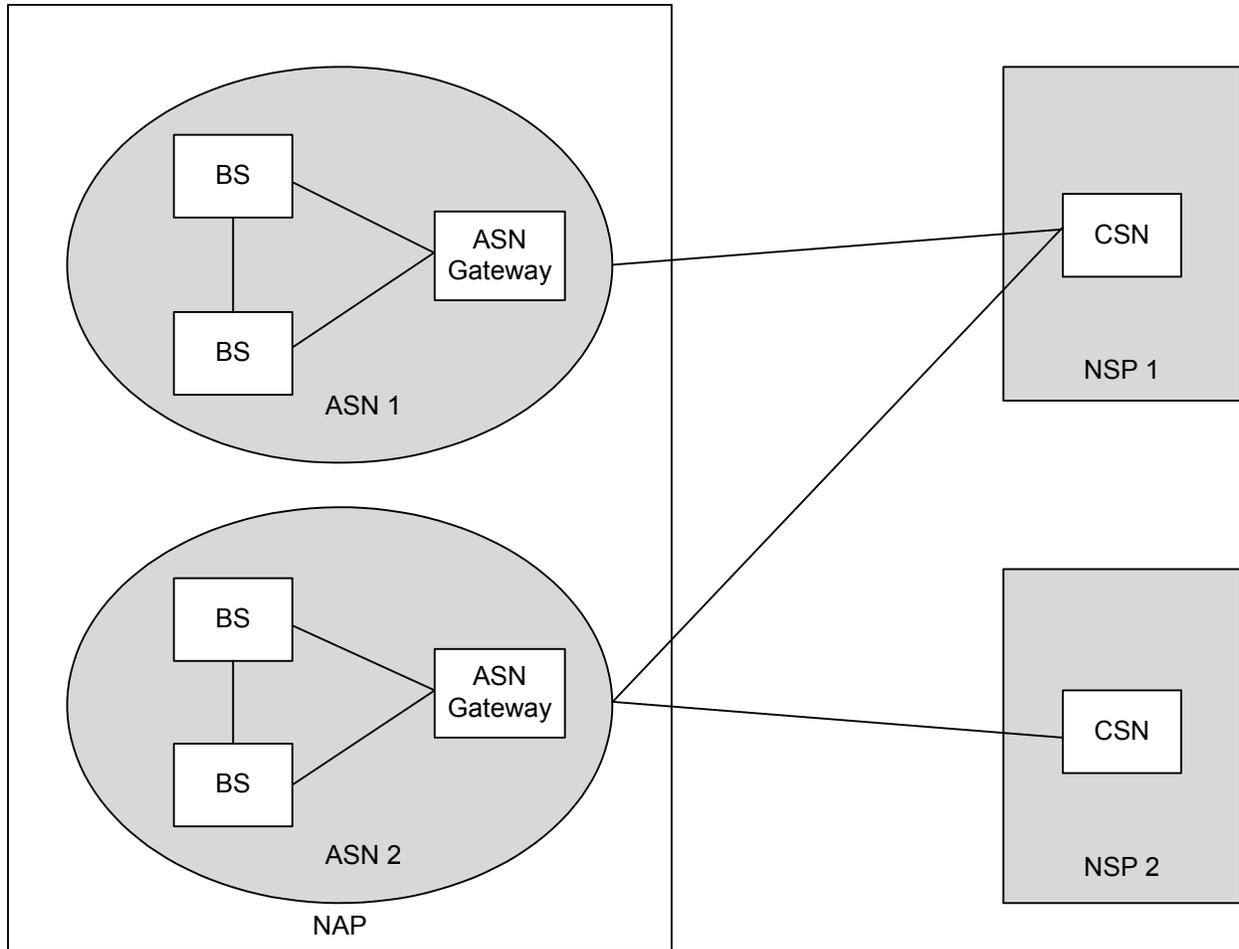
1

Figure A-2 - Decomposition and NAP Sharing by Multiple NSPs

3 Following salient features of NAP decomposition and NAP sharing are worth noting:

4 • A NAP may deploy one or more ASNs in a single or diverse geographic area. (NOTE— An NSP may use
5   multiple NAPs).

6 • An ASN in profiles A& C comprises Base Stations (BS) (or BS clusters) and ASN Gateway(s). In profile
7   B, ASN-GW may not be included.

8 • An ASN Gateway provides connectivity to one or more CSNs over a WiMAX NWG defined interface.
9   Such CSNs may belong to same or different types of NSPs. For example, , NSP1 may be a WiMAX
10 Greenfield NSP whereas NSP 2 may be an incumbent 3G operator (e.g., CDMA operator) that is also an
11 NSP (i.e., providing WiMAX services).

A.3   Deployment Scenarios

13 This section depicts seven deployment scenarios that illustrate interrelationships between NAP, NSP, ASN, and
14 CSN. Following deployment scenarios are depicted in following subsection:

1 **A.3.1   NAP Sharing by Multiple NSPs**
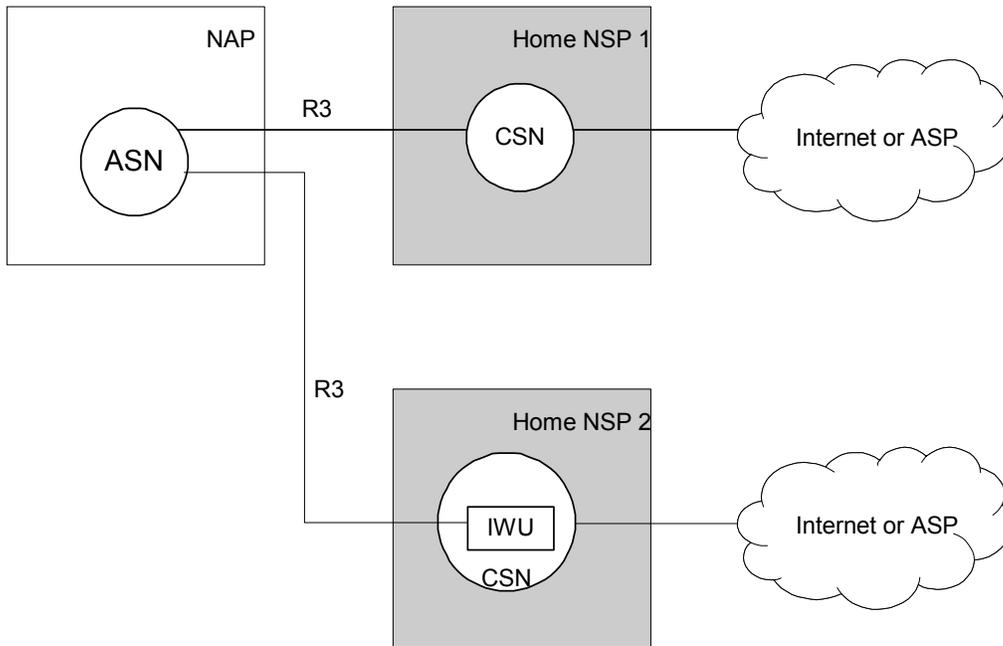
2   H-NSP1 and HNSP2 may be different types of NSPs. For example, in the above figure, H-NSP1 may
        be a Greenfield WiMAX operator whereas H-NSP2 may be an incumbent 3GPP2 operator.

3   **Figure A-3 - NAP Sharing by Multiple NSPs**

4 **A.3.2   Single NSP Providing Access Through Multiple NAPs**

5
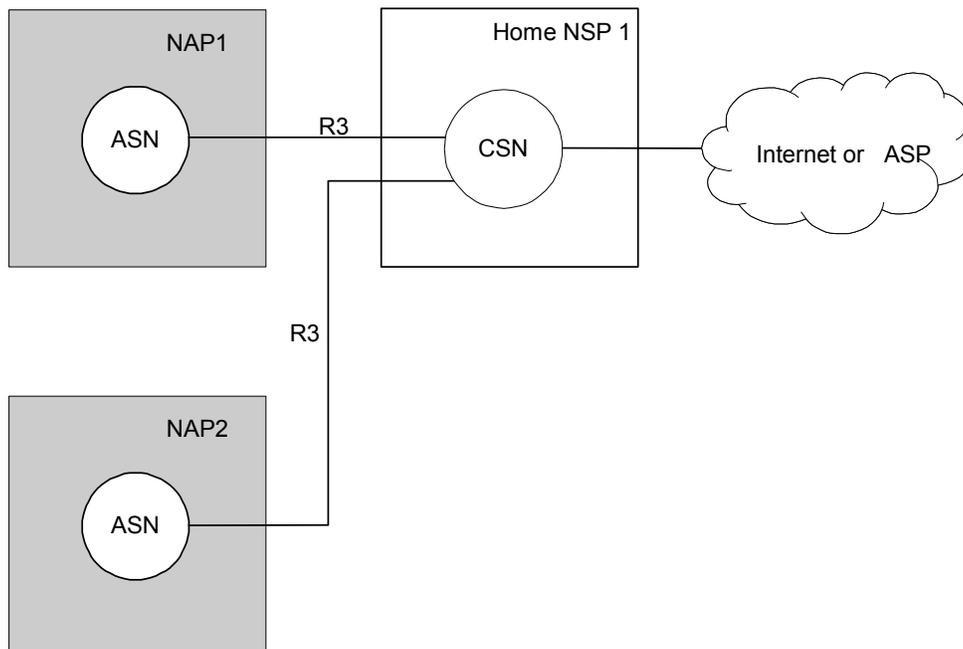
6   **Figure A-4 - Single NSP Providing Access Through Multiple NAPs**

1   **A.3.3   Greenfield WiMAX NAP+NSP**
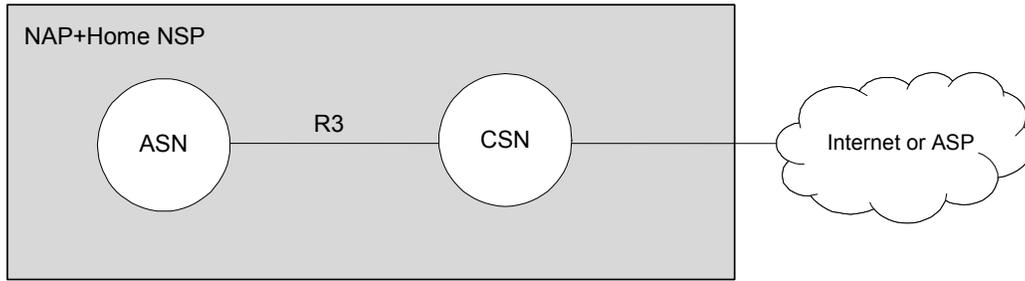
2

3   **Figure A-5 - Greenfield WiMAX NAP + NSP**

4   **A.3.4   Greenfield WiMAX NAP+NSP with NAP Sharing**
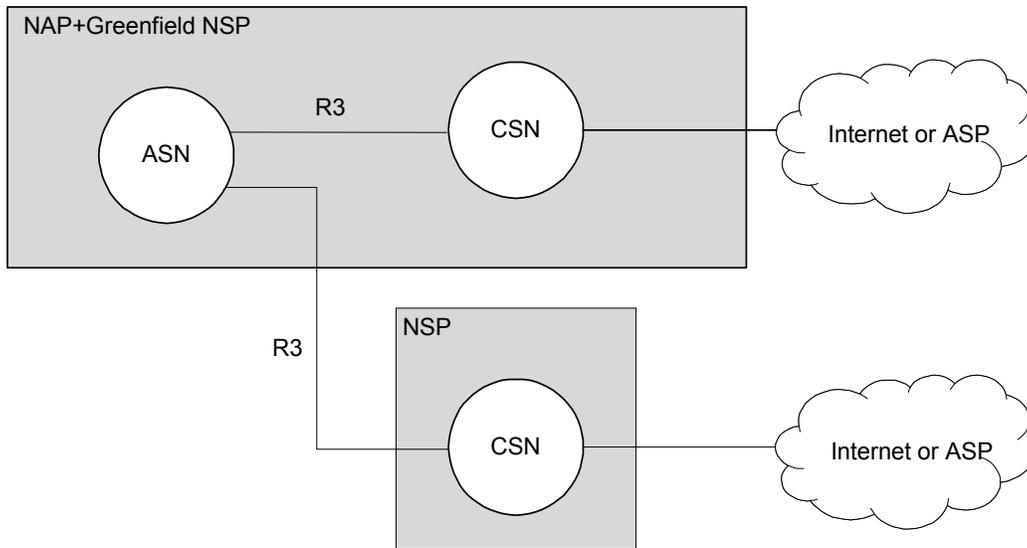
5

6   **Figure A-6 - Greenfield WiMAX NAP+NSP with NAP Sharing**

1   **A.3.5   Greenfield WiMAX NAP+NSP Providing Roaming**
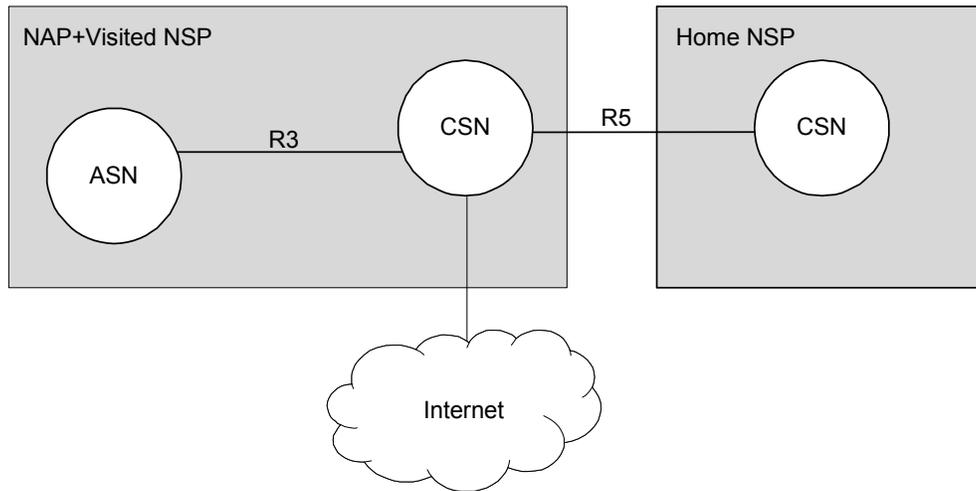
2

3   **Figure A-7 - Greenfield WiMAX NAP+NSP Providing Roaming**

4   **A.3.6   Visited NSP Providing WiMAX Services**
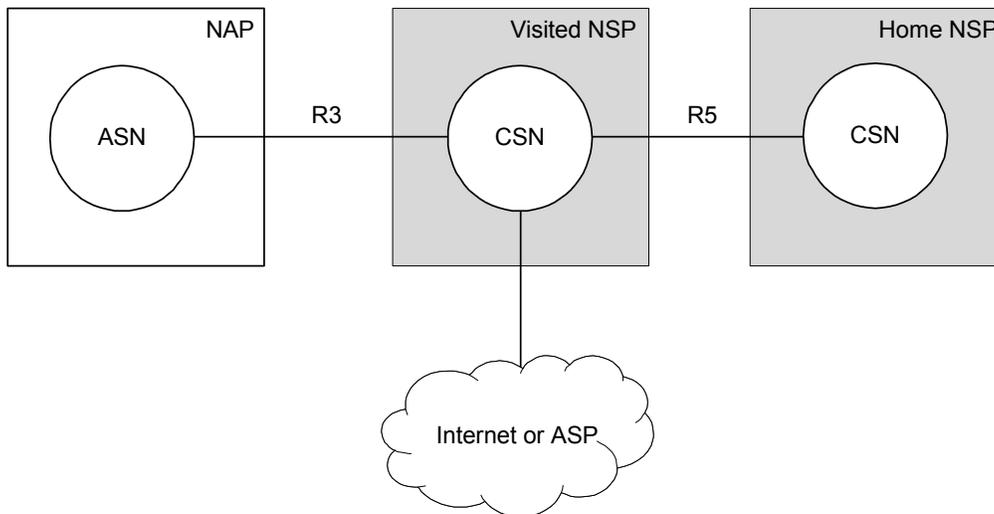
5

6   **Figure A-8 - Visited NSP Providing WiMAX Services**

1   **A.3.7   Home NSP Providing WiMAX Services**

2
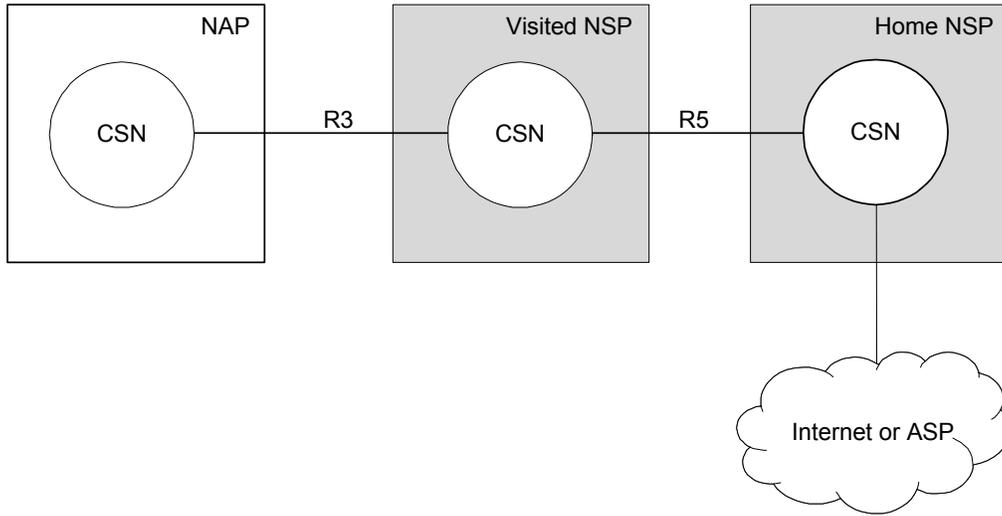
3   **Figure A-9 - Home NSP Providing WiMAX Services**

4

B. MS Movement with FA change, no PC change

If PMIP is used for a given mobile, when the mobile performs a location update procedure, the foreign agent that receives data for the mobile may be migrated using PMIP without having the mobile itself send any MIP registration request. Note that migration of the FA is optional. When the foreign agent is migrated to a new FA, it may be necessary to notify a Data Path Function associated with the new FA to monitor for data arriving for the mobile in idle mode. The Data Path Function can be provided with the identity of the Anchor PC, so that when data arrives for the mobile in idle mode, the Data Path function can trigger the Anchor PC to initiate paging for the mobile in the appropriate paging group.

The following figure illustrates the case of migration of the FA by triggering PMIP procedures when the Anchor PC remains the same (i.e. the mobile's context information is not relocated to a new PC but remains at the same Anchor PC where it was prior to the location update). The following steps describe the steps shown in the illustration.

    a. Mobile sends a RNG_REQ to a serving base station to perform location update.

    b. The serving BS sends a LU Req to its Relaying PC, which contacts the Anchor PC based on the PC_ID provided by the mobile. (Note that in some cases the Anchor PC may be the same as the Relaying PC associated with the Serving BS). It also asks for the mobile's context information, so as to determine the identity of the KDF/Authenticator from where the AK for the mobile can be obtained.

    c. The Anchor PC acknowledges the location update using LU_Rsp and provides the mobile's context information to the Relaying PC, which provides it to the BS. However, in this case the Anchor PC retains the mobile's context (i.e. remains the anchor PC), and the mobile will be provided with the PC_ID of the same Anchor PC while confirming the location update.

    d. In order to verify the HMAC/CMAC-tuple on the RNG_REQ, the S-BS' associated Key Receiver fetches the AK from the KDF associated with the authenticator where the mobile had last authenticated, using the KDF/Authenticator ID provided in the mobile context information.

    e. LU_Confirm is sent from the S-BS (through the Relaying PC) to the Anchor PC to confirm the validation of the RNG_REQ.

    f. The appropriate functional entity determines that the Data Path Function associated with the mobile's new location (shown as "Data Path Fn-New") is different from the mobile's previous Data Path Function. The logic for making this determination is unspecified and may be dependent on the physical configuration.

    g. The appropriate functional entity (e.g. Anchor PC) sends a message called "Data Path Monitor Notification" to the Data Path Fn-New indicating that if new data arrives for this mobile in idle mode, the Data Path Function should contact the Anchor PC to initiate paging for the mobile.

    h. The appropriate functional entity determines that the FA associated with the mobile's new location (shown as "FA-new") should be different from the mobile's previous anchor FA. The logic for making this determination is unspecified and may be dependent on the physical configuration. The PMIP client entity is triggered to initiate a Proxy MIP registration request.

    i. The Proxy MIP registration procedure is executed to switch the R3 tunnel from the HA to point to the new FA.

    j. An RNG_RSP message is sent to the mobile confirming the location update and providing the PC_ID of the Anchor-PC. Note that this step may occur any time after the RNG_REQ is validated by the SBS.

Note that in the above, the exact timing of steps f through g, and h through I, may be interchanged depending on physical configuration.

1

Figure B-1

2
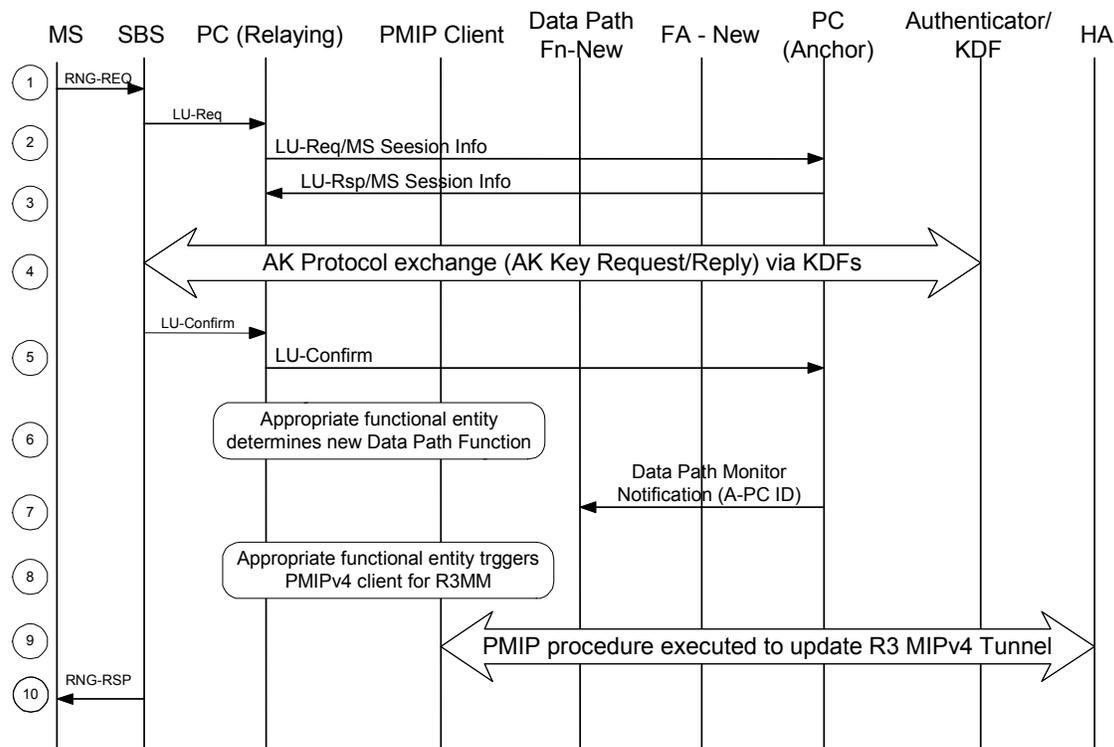
3 The following figure illustrates the case of migration of the FA by triggering PMIP when the mobile context is
4 relocated to a new PC from the Anchor PC prior to the location update. Note that relocation of the mobile context to
5 a new PC is optional. If this option is exercised, it results in the new PC taking on the role of the Anchor PC for that
6 mobile. In the following illustration, this occurs along with an FA migration using PMIP.

7 a. Mobile sends a RNG_REQ to a serving base station to perform location update.

8 b. The serving BS sends a LU Req to its Relaying PC, which contacts the (old) Anchor PC based on the
9   PC_ID provided by the mobile (assuming here that the Relaying PC is different from the (old) Anchor PC).
10   It also asks for the mobile's context information, so as to determine the identity of the KDF/Authenticator
11   from where the AK for the mobile can be obtained.

12 c. The (old) Anchor PC acknowledges the location update using LU_Rsp and provides the mobile's context
13   information to the Relaying PC, which provides it to the BS. In this case, the Relaying PC will become the
14   new Anchor PC for this mobile, and the mobile will be given a PC_ID corresponding to the new Anchor
15   PC when confirming the location update.

16 d. In order to verify the HMAC/CMAC-tuple on the RNG_REQ, the S-BS' associated Key Receiver fetches
17   the AK from the KDF associated with the authenticator where the mobile had last authenticated, using the
18   KDF/Authenticator ID provided in the mobile context information.LU_

19 e. Confirm is sent from the Relaying PC (which is now the new Anchor PC for that mobile) to the (old)
20   Anchor PC. This confirms the validation of the RNG_REQ and the relocation of the Anchor PC, and the
21   old Anchor PC can now delete the mobile's information from its LR.

22 f. The appropriate functional entity determines that the Data Path Function associated with the mobile's new
23   location (shown as "Data Path Fn-New") is different from the mobile's previous Data Path Function. The
24   logic for making this determination is unspecified and may be dependent on the physical configuration.

25 g. The appropriate functional entity (e.g. new Anchor PC) sends a message called "Data Path Monitor
26   Notification" to the Data Path Fn-New indicating that if new data arrives for this mobile in idle mode, the
27   Data Path Function should contact the new Anchor PC to initiate paging for the mobile.

1   h.   The appropriate functional entity determines that the FA associated with the mobile's new location (shown
2   as "FA-new") should be different from the mobile's previous anchor FA. The logic for making this
3   determination is unspecified and may be dependent on the physical configuration. The PMIP client entity is
4   triggered to initiate a Proxy MIP registration request.

5   i.   The Proxy MIP registration procedure is executed to switch the R3 tunnel from the HA to point to the new
6   FA.

7   j.   An RNG_RSP message is sent to the mobile confirming the location update and providing the PC_ID of
8   the new Anchor-PC. Note that this message may be sent any time after the RNG_REQ has been validated.

9   Note that in the above, the exact timing of steps f through g, and h through I, may be interchanged depending on
10 physical configuration.

11
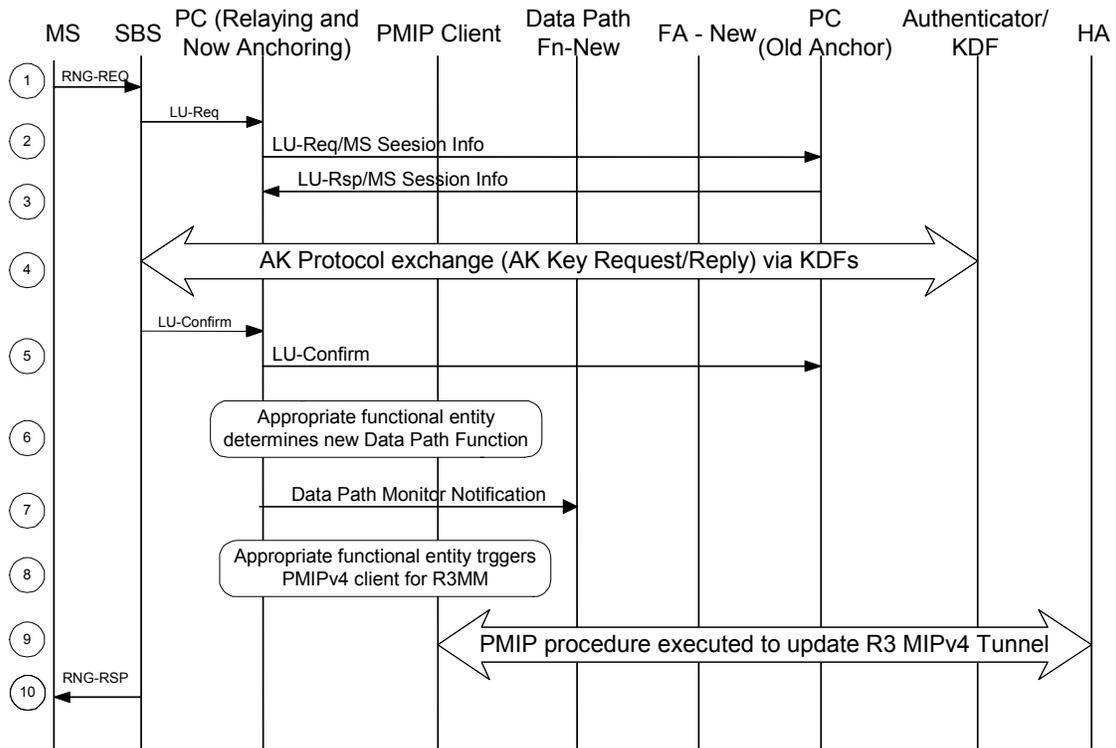
12   **Figure B-2**

1 # C. ASN-GW Selection Protocol

2 This document covers two cases:

3 • Initial ASN-GW selection for Base Station and ASN-GW communications

4 • Per Session ASN-GW selection

5 ## C.1 Initial ASN-GW Selection by Base Station

6
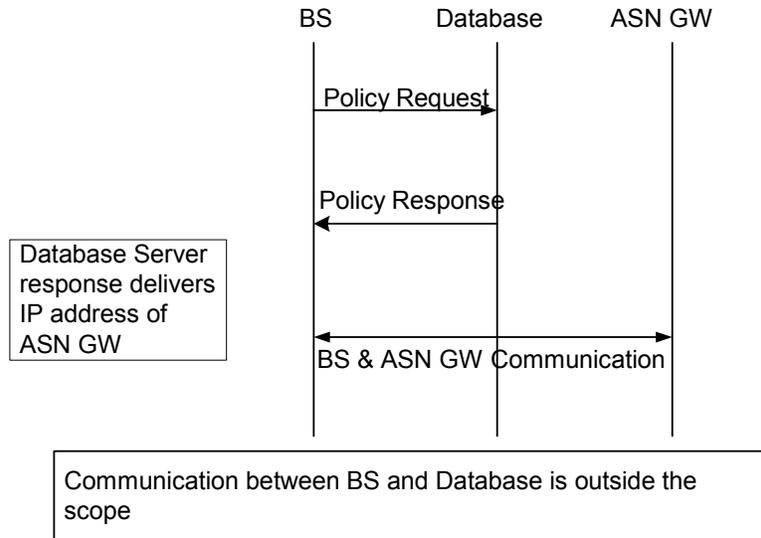
7 **Figure C-1 - Initial ASN-GW Selection by Base Station**

8 On Base Station startup or initial configuration Base Station contacts DB to get information about serving ASN-
9 GW. The response includes the ASN-GW IP address.

10 The triggers for sending the Policy Request may include but are not restricted to the following:

11 • Initial Base Station startup

12 • Base Station reload

13 ## C.2 Per Session Selection of Physical Entities of Logical ASN-GW

14 It may not be scalable to contact policy server/database for each and every session. Base station always contacts
15 known ASN-GW which may be determined by the previous procedure. Once the data path registration request is
16 received by ASNGW1, it may forward to ASN-GW2. The data path registration response is returned by ASN-GW1
17 (or ASN-GW2) and will include the ASN-GW IP address for the specific session. It may also return IP addresses of
18 different physical entities of the logical ASN-GW if they exists. The ASN-GW IP address may be the same as the
19 initial ASN-GW address or different one. The actual algorithm of determining the specific ASN-GW address
20 returned in the response is out of scope of this document.

21 Multiple IP addresses of different functional entities of an ASN-GW can also be delivered to the Base Station.

1
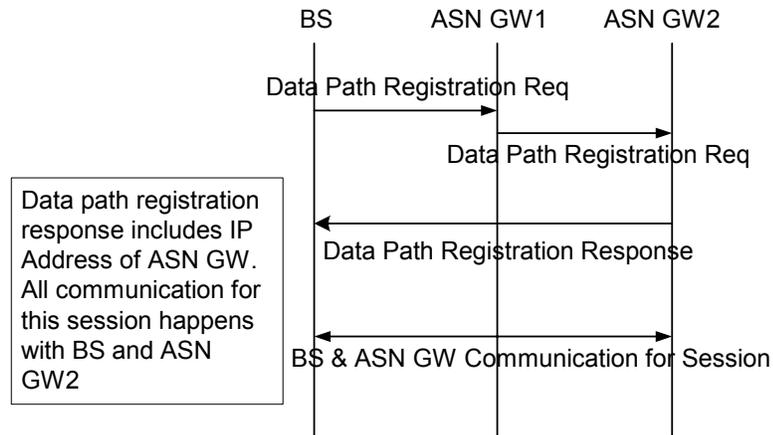
2 **Figure C-2 - Per Session ASN-GW Selection**

3 One example of the selection procedure is shown above. The Data Path Registration Request is sent to the initial
4 ASN-GW, ASN-GW1 that the BS has initial communication with. This request may be forwarded to another ASN-
5 GW2. ASN-GW2 will reply back with Data Path registration response and all communication for the session after
6 this point will happen between BS and ASN-GW2.

7 ## C.2.1 Security Considerations

8 It is assumed that the Security Association between the Base Stations and ASN Gateways are pre-provisioned (e.g.,
9 there could be pre-established IPsec tunnels between each BS and ASN-GW). Thus the security context is not part
10 of the ASN-GW Selection.

11

1 # D. 'RRM': Spare Capacity Report per QoS Profiles

2 ## D.1   Introduction to Type 1 and Type 2 Spare Capacity Report

3 This annex describes Spare Capacity report per-BS, per QoS Profile and per Physical Service Level (PSL), Type 1
4 and Type 2.

5 **Spare capacity report** Type 1 and 2 are indexed by QoS profile ID and PHY service level, see details below. This
6 type of Spare capacity report contains "Spare Capacity Indicator" (SCI) values, indicating the number of MS of the
7 given type that may be added to the BS without degradation. It is calculated by the BS itself, using vendor
8 proprietary algorithm, on the base of detailed knowledge of scheduling algorithm and real time load situation.

9 • Type 1 is the report for several combinations of DL and UL PSL values within a predefined two-
10 dimensional range

11 • Type 2 is for exactly one pair of DL and UL PSL values.

12 The reporting format for spare capacity reports of **Type 1** and **Type 2** is specified in Section 9.10.2.

13 **Type 1** shall not be supported in Release-1 and is for further releases.

14 **Type 2** shall be used in a modified form as part of the Handover Preparation phase, as decided in the "Motion on
15 RRM": "Type-2 (Spare Capacity report for a single QoS Profile and a single PHY service level PSL) for a specific
16 MS during **HO Pre-Notification response**, and QoS Profile and PSL should be in the HO Pre-Notification request".
17 The required modification is:

18 • It shall be embedded in the HO Pre-Notification request and response messages, i.e. these are no longer
19 RRM primitives; and

20 • The MS Identity must be added: The report is no longer for an anonymous, potential MS but for a specific
21 MS with already known QoS Profile and PSL value.

22 Since this Type 2 report will be part of a HO Primitives, rather than RRM primitive, it does not belong to section
23 7.10 (RRM) but should be considered for section 7.x "Intra-ASN Mobility".

24 ## D.1.1   Format of Spare Capacity Records, Type 1 and 2

25 A spare capacity record is used to carry information on many potential options of BS-MS communication rates. It
26 may be exchanged in one of two formats – Type 1 and Type 2 - as specified in Tables below.

27 Table D-1 describes aggregate spare capacity report from RRA to RRC:

28 **Table D-1 - Spare Capacity Report, Type 1**

QoS profile descriptor	SCI = Spare capacity indicator for DL PSL = 1 UL PSL = 1	SCI = Spare capacity indicator for DL PSL = 1 UL PSL = 2	…	SCI = Spare capacity indicator for DL PSL = N UL PSL = N
4 bytes	2 bytes	2 bytes	…	2 bytes

29 Value SCI = 0 means "no information available".

30 Value SCI > 0 means that the BS is able to accommodate (SCI – 32) MS with QoS requirements specified by QoS
31 profile descriptor and specific DL/UL PSL.

32 The result belongs to the range [-31 .., 65504]. Value SCI < 32 means that the BS suffers from degradation, which
33 will be relaxed if (32 – SCI) MS with corresponding PSL values leave the BS.

1 Table D-2 describes an optional alternative format of spare capacity report from BS. This format shall be used when
2 RRC queries a specific BS on its ability to accommodate a new service flow characterized by a QoS profile
3 descriptor. For such cases, the BS may decide report the spare capacity for that QoS profile, for a specific set of DL
4 PSL and UL PSL values. Alternatively, the BS may report the spare capacity for all sets of DL PSL and UL PSL
5 values using Type 1 report format.

6

7 **Table D-2 - Spare Capacity Report, Type 2**

QoS profile descriptor	DL PSL	UL PSL	SCI = Spare Capacity Indicator
4 bytes	1 byte	1 byte	2 bytes

8 Value SCI = 0 means "no information available".

9 Value SCI > 0 means that the BS is able to accommodate (SCI – 32) MS with QoS requirements specified by QoS
10 profile descriptor.

11 The result belongs to the range [-31 to 65504]. Value SCI < 32 means that the BS suffers from degradation, which
12 will be relaxed if (32 – SCI) MS with corresponding PSL values leave the BS.

13 D.1.2 Format of QoS Profile Descriptor

14 The QoS profile descriptor contains information on service flows authorized for MS. The descriptor has the
15 following format: {**DescrType, NRTSInd, RTSInd1, RTSInd2**} where **DescrType** identifies the format of
16 descriptor. This field is a function of the number of different services assigned to MS.

17 Value **DescrType = 0** corresponds to the case when there are **at most *three* services** per mobile terminal including
18 at most two real time (RT) services. Each **RT service** is carried by MAC connection (or **pair of connections, for**
19 **DL and UL**). All **non-real time services** are carried by a single pair of **DL and UL MAC connection** with certain
20 QoS properties.

21 Other DescrType values are reserved for future extensions

22 **NRTSInd** is an index associated with certain set of parameters for non-real time service (see examples in Table
23 D-3).

24 **Table D-3 - NRT Services Encoding (example)**

NRTSInd	Direction	QoS Parameters
…	…	…
18	DL	NRT-VR Max rate =512, reserved rate = 128
	UL	NRT-VR Max rate =128, reserved rate = 64
19	DL	NRT-VR Max rate =1024, reserved rate = 256
	UL	NRT-VR Max rate =128, reserved rate = 64

25 **RTSInd1/2** are indexes associated with certain set of parameters for two real-time services (see examples in Table
26 D-4).

1   **Table D-4 - RT Services Encoding (example)**

RTSInd	Activity	Direction	QoS Parameters	Notes
…	…	…	…	
120	Non-active	DL	RT-VR Nominal rate =384, reserved rate = 256, max latency = 100 ms	Video conferencing
		UL	RT-VR Nominal rate =384, reserved rate = 256, max latency = 100 ms	
121	Active	DL	RT-VR Nominal rate =384, reserved rate = 256, max latency = 100 ms	Video conferencing
		UL	RT-VR Nominal rate =384, reserved rate = 256, max latency = 100 ms	
122	Non-active	DL+UL	UGS packet length = 120, period = 60ms	VoIP call
		DL+UL	UGS packet length = 120, period = 60ms	
123	Active	DL+UL	UGS packet length = 120, period = 60ms	VoIP call
		DL+UL	UGS packet length = 120, period = 60ms	
…	…	…	…	

2   All indexes are one byte length. Index 0 means no service specified.

3   Meaning of indexes and their correspondence to QoS parameters is configured, per ASN or NAP. This encoding
4   may differentiate between active and non-active RT services. For example, RT services LSB may be allocated for
5   activity flag. So if the service is for VoIP, LSB will be set for calls, which are currently active (and therefore need an
6   immediate capacity allocation after HO).

7   **Note:** The need for the ''Activity'' indicator in the Spare Capacity indicator for RT Services should be reviewed. –
8   The report might be restricted to active services only. This is FFS.

9   ### D.1.3 Dynamic Configuration of Supported Service Types between RRM Entities (BS
10   ###   and RRC)

11   In order to provide scalability of new service deployments (i.e., new QoS profiles) without impacting changes in
12   RRM procedures across several operators offering services, the supported Service Types to be used in RRM Spare
13   Capacity reports whenever these are indexed by QoS Profiles are learnt dynamically between BS and RRC.
14   Following considerations apply for dynamic learning of supported QoS profiles:

15   BSs may dynamically learn supported profiles from RRC.

16

17   Learning of the profiles may be done via the R6 protocol during initialization.

18   Each profile is identified for a unique profile ID, which could be used to index further RRM measurements.

1 A primitive to retrieve profiles on R6 is sent from the BS to RRC, and as a response, the BS receives all the profiles
2 to be used.

3 A Service is defined as a pair of DL and UL QoS description and is formatted as (Service Indicator ServInd, Type of
4 Service, and parameters associated with profile)

5 Example of a **Non Real time Service** is as follows:

6 **Table D-5**

ServInd	Type	DL Max Rate	DL Reserved Rate	UL Max Rate	UL Reserved Rate
1	NRT	1024	512	512	256

7 Example of a **Real-Time Service** is as follows:

8 **Table D-6**

ServInd	Type	DL Nominal rate	DL Reserved Rate	DL Max Latency	UL Nominal rate	UL Reserved Rate	UL Max Latency
2	RT	384	256	100	384	256	100

9

10 Forwarding of Ethernet encapsulated IP frames (ETH-CS w/ IP)

11 **D.2   Alternative RRM reference model**

12 Generic Reference Model #2b is characterized by:

13 - RRA and RRC collocated in the BSs;

14 - R8 is used for RRC to RRC communication.

15 This is shown in Figure D-1.
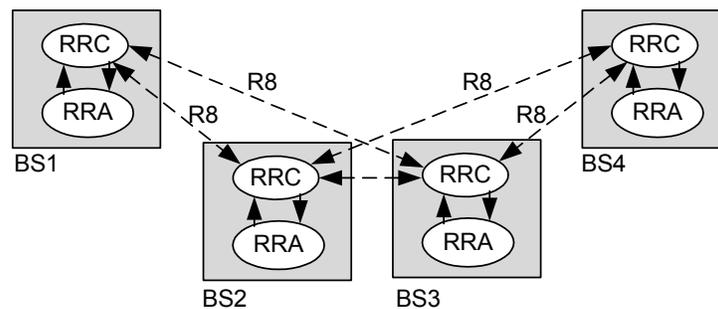
16

17 **Figure D-1 - RRA and RRC Collocated in BS**

18 The above reference model is based on collocated RRA and RRC in each BS. The interface between RRA and RRC
19 is outside the scope of this specification. It MAY be noted that in this reference model, only the information
20 reporting procedures (dashed lines) are standardized at the NWG-specified R8 reference point, while the decision
21 support procedures (bold lines) between RRA and RRC in each BS are proprietary and not standardized. The R6
22 reference point is not shown because R6 primitives are not used to exchange RRM information in this reference
23 model.

1

1 E. Ethernet Operational Behavior

2 The sections below cover operational behavior of Ethernet

3 E.1 Packet Forwarding

4 The System shall classify any and all hosts connected to a MS as an un-trusted source connected to an un-trusted
5 port.

6 The System shall classify any and all hosts connected to the BS via its Ethernet interface as trusted sources
7 connected to trusted ports.

8 The System shall support basic packet forwarding.

9 The System shall support an Authenticated ID List.

10 When receiving a packet from an un-trusted port that is not singled out by requirements stated herein, the System
11 shall forward that packet to a trusted port provided the source MAC address is found in the Authenticated ID List.

12 When receiving a packet from a trusted port that is not singled out by requirements stated herein, the System shall
13 forward that packet to a specific un-trusted ports identified by the destination MAC address provided that this
14 destination MAC address is found in the Authenticated ID List.

15 E.2 Authenticated ID List

16 The System shall provide a persistent data storage for the current *MS Authenticated ID List* that is stored in each
17 specific MS.

18 The System shall synchronize the *BS Authenticated ID List* with the *MS Authenticated List* any time the MS
19 registers with the BS.

20 The System shall synchronize the *BS Authenticated ID List* for the current BS of a MS when the *system provisioning*
21 *element Authenticated ID List* is updated for that MS. The Authenticated ID list may be provisioned via PKMv2
22 EAP authentication, in which case the mechanism for synchronization is described below:

23 In particular in the case of ETH CS with IP:

24 The System shall support dynamic additions/deletions to/from the *BS Authenticated ID List* from the *DHCP*
25 *Authenticating Agent* that is performing *DHCP ACK Snooping.*

26 The System shall synchronize the *MS Authenticated ID List* as a subset from the *BS Authenticated ID List* any time
27 an entry is added to or removed from the *BS Authenticated ID List* as a result of either the *Authenticating DHCP*
28 *Agent* or the system provisioning element *Authenticated ID List* synchronization.

29 In the case where the Authenticated ID list is provisioned via PKMv2 EAP authentication:

30 When the MS successfully authenticates to the network (using whatever identities and credentials are required by
31 the operator), the AAA server sends to the BS (via the AAA protocol) indication of authentication success as well as
32 the provisioned classifier and service flow parameters.

33 The prioritized classifier list shall specify classifiers and associated service flow information for the packets
34 originating at MAC address or addresses that are permitted origin addresses for this authenticated user.

35 The prioritized classifier list shall specify "drop" for non-authentication packets originating at any other MAC
36 address.

37 If dynamic authentication is supported for additional MS devices (e.g. via 802.1x), then upon successful MS
38 authentication a management element at the provider shall dynamically provision appropriate classifier and service
39 flow parameters for frames bearing the source MAC address of the newly authenticated MS.

40 In particular, in the case of ETH CS with VLAN Tags..

41 VLAN tag associations shall be provisioned per MS.

1   Host generated VLAN tags shall be authenticated using the MS provisioned tag and VLAN feature.

2   VLAN Ethernet frames as well as plain Ethernet frames shall be forwarded as defined herein to the trusted network
3   after authentication; otherwise the VLAN tagged frames shall be silently ignored.

E.3   Packet Filtering

5   The System shall support *Broadcast Filtering*.

6   The System shall have the ability to enable or disable all *Ingress Broadcast Filter* and *Egress Broadcast Filter*
7   functionality defined herein.

8   If disabled, the *Ingress Broadcast Filter* and *Egress Broadcast Filter* shall pass all packets destined for the MAC
9   broadcast or any MAC multicast address.

10   Upon receiving any packet destined for the MAC broadcast or any MAC multicast address, the *Broadcast Ingress*
11   *Filter* shall silently discard the packet.

12   Upon receiving any packet destined for the MAC broadcast or any MAC multicast address, the *Broadcast Egress*
13   *Filter* shall silently discard the packet.

14   The System shall support *Basic Ingress Filtering*.

15   The System shall have the ability to enable or disable all *Ingress Filter* functionality defined herein.

16   If disabled, the *Ingress Filter* shall pass all packets.

17   The *Ingress Filter* shall silently discard any packet received for which the packet's destination MAC address can be
18   found in the *MS Authenticated ID List*.

19   Upon receiving any packet from the MS, the *Ingress Filter* shall discard the packet if the source MAC address
20   cannot be found in the current *MS Authenticated ID List*.

21   In particular in the case of ETH CS w/ IP:

22   The *Ingress Filter* shall permit all Address Resolution Protocol messages to pass to the *ARP Ingress Proxy Agent*.

23   The Ingress Filter shall permit all DHCP messages to pass to the Authenticating and Tagging DHCP Agents.

24   Upon receiving any packet from the MS that can be identified as an IP datagram, the *Ingress Filter* shall discard the
25   datagram if the source IP address cannot be found in the current *MS Authenticated ID List*.

E.4   Forwarding of Plain Ethernet Frames (ETH-CS)

27   The MS may support *Standard Learned Bridging* between its airlink and any physical or logical MS side interfaces

28   The BS shall support *Standard Learned Bridging* between its airlink and its backhaul links

29   When performing *Standard Learned Bridging*, the BS or MS shall learn all source MAC addresses originating from
30   a given un-trusted MS port up to MAXMSIP individual learned addresses. Subsequently, any packets destined for
31   one of those learned address should be forwarded directly to that un-trusted port. The accumulation of all learned
32   MAC to port associations constitutes the *MS Learned Bridge Table* as managed by the MS. The accumulation of all
33   learned MAC to port associations constitutes the *BS Learned Bridge Table* as managed by the BS.

34   When performing *Standard Learned Bridging*, the BS or MS shall silently discard all packets received from an un-
35   trusted port, e.g. MS, for which the packet's destination MAC address is also an entry for that port in the *MS*
36   *Learned Bridge Table*.

37   When performing *Standard Learned Bridging*, the BS or MS shall automatically unlearn a MAC to un-trusted port
38   relationship after BRIDGETIMEOUT seconds have expired without any traffic from that MAC address.

39   When performing *Standard Learned Bridging*, the BS or MS shall forward all packets received from any un-trusted
40   port to a trusted port provided the destination MAC address does not match a currently learned relationship to an un-
41   trusted port. This implies that peer-to-peer communication is not available when performing *Standard Learned*
42   *Bridging*.

1 When performing *Standard Learned Bridging*, the BS or MS shall flood any packet received from a trusted port
2 destined for a MAC broadcast or multicast address to all un-trusted ports.

3 When performing *Standard Learned Bridging*, the BS or MS shall forward all packets received from a trusted port
4 to an un-trusted port that is identified by the destination MAC address. If a learned port corresponding to the
5 destination MAC address does not exist, the packet must be silently discarded. The IP TOS field shall be inspected
6 and may be used as an authenticated QoS trigger.

E.5 Forwarding of Ethernet-encapsulated IP Frames (ETH-CS w/ IP)

8 The System shall support port and host classification.

E.6 Proxy Address Resolution Protocol (Proxy-ARP)

10 The System shall support Proxy-ARP.

11 The System shall have the ability to enable or disable all *ARP Ingress Proxy Agent* and/or *ARP Egress Proxy Agent*
12 functionality defined herein.

13 If disabled, the *ARP Ingress Proxy Agent* or *ARP Egress Proxy Agent* shall pass all ARP packets without
14 discrimination or modification using *Standard Learned Bridging*.

15 Upon receiving an ARP Request from a trusted source, the *ARP Egress Proxy Agent* shall unicast an ARP Response
16 back to that trusted source, provided that the target address matches an entry in the *Authenticated ID List*. If the
17 match is found, the *ARP Egress Proxy Agent* shall also forward the original ARP Request to the specific MS
18 identified by the match. Otherwise, the *ARP Egress Proxy Agent* shall silently discard the Request.

19 Upon receiving an ARP Response message from a trusted source, the *ARP Egress Proxy Agent* shall forward the
20 response to the MS specifically addressed by the destination MAC address, provided that this address can be found
21 in the *Authenticated ID List*. Otherwise, the *ARP Egress Proxy Agent* shall silently discard the Response.

22 Upon receiving an ARP Request from an un-trusted source, the *ARP Ingress Proxy Agent* shall unicast an ARP
23 Response back to that trusted source provided that the target address matches an entry in the *Authenticated ID List*.
24 If the match is found, the *ARP Ingress Proxy Agent* shall also forward the original ARP Request to the specific MS
25 identified by the match. Otherwise, the *ARP Ingress Proxy Agent* shall flood the Request to all trusted ports.

26 Upon receiving an ARP Response message from an un-trusted source, the *ARP Ingress Proxy Agent* shall silently
27 discard the Response.

28 The *ARP Ingress Proxy Agent* shall silently discard any received self-ARP Requests. Those are requests for a target
29 IP address, that when queried in the *Authenticated ID List* results in a response MAC equal to the Request's source
30 MAC address.

31 The ARP Egress Proxy Agent shall issue a gratuitous ARP for any new addition to the Authenticated ID List
32 resulting from DHCP ACK Snooping, MS Authenticated ID List merging, or provisioning system Authenticated ID
33 List synchronization. An unsolicited broadcast ARP Response constitutes a gratuitous ARP.

E.7 Forwarding of VLAN-tagged Ethernet Frames (VLAN ETH-CS)

35 Filtering and forwarding of plain Ethernet shall apply to IEEE 802.1pq VLAN tagged frames.

E.7.1 IEEE 802.1Q VLAN Transport

37 Filtering and forwarding of plain Ethernet shall apply to VLAN tagged frames.

38 Authenticated host generated VLAN Ethernet frames as well as plain Ethernet frames shall be forwarded to the
39 trusted network.

40 Unauthenticated VLAN Ethernet frames shall be discarded.

E.7.2 BS VLAN Proxy

42 The BS shall act as a VLAN proxy and add VLAN tags to ingress traffic and remove egress traffic.

1   The BS shall transmit only the untagged Ethernet frames over the air.

2   The BS shall make VLAN tag associations based on BS provisioned policies.

E.7.3   BS VLAN Translation and Stacking

4   VLAN IDsVLAN IDsVLAN IDsThe BS shall make VLAN tag translation or stacking associations based on BS
5   provisioned policies. The BS shall translate MS private VLAN IDs and Priorities to the CSN core VLAN IDs and
6   priorities, or the BS shall stack MS private VLAN IDs and Priorities inside the CSN core VLAN IDs and priorities.

E.7.4   BS VLAN Classification

8   The VLAN priority tag IEEE 802.1p shall be inspected and may be used as an authenticated QoS trigger.

E.8   Dynamic Host Configuration Protocol Agent— Address Authentication

10 The System shall support DHCP Agent Address Snooping.

11 The System shall have the ability to enable or disable all *Authenticating DHCP Agent* functionality defined herein.

12 If disabled, the *Authenticating DHCP Agent* shall forward all DHCP messages without discrimination or
13 modification using *Standard Learned Bridge Forwarding*.

14 The *Authenticating DHCP Agent* shall add an entry in the *Authenticated ID List* upon detection of a DHCP ACK
15 from the server on a trusted port. This is called *DHCP ACK Snooping*. The duration of the lease, LEASE, the
16 moment of lease, LEASEMOMENT, and the corresponding MS shall also be recorded in the *Authenticated ID List*.

17 The *Authenticating DHCP Agent* shall silently discard all DHCP DISCOVERY, INFORM, REQUEST, and
18 DECLINE messages received on a trusted port.

19 The *Authenticating DHCP Agent* shall silently discard all DHCP OFFER, ACK, NACK, and FORCERENEW
20 messages received on an untrusted port.

21 When forwarding DHCP OFFER, ACK, NACK, FORCERENEW to untrusted MS ports, the Authenticating *DHCP*
22 *Agent* shall correlate the target hardware address (not destination MAC), transaction identifier, and agent remote
23 identifier (if present) with a previously DHCP DISCOVERY, INFORM, REQUEST, or DECLINE. If a correlation
24 is made, only the MS identified from the first message shall be used to forward the subject message, even if destined
25 for a broadcast MAC. Otherwise, the message shall be silently discarded.

26 When maintaining state for target hardware address, transaction identifier, and agent remote identifier received from
27 a DHCP DISCOVERY, INFORM, REQUEST, or DECLINE that is meant to correlate with a returning DHCP
28 OFFER, ACK, NACK, or FORCERENEW, the *Authenticating DHCP Agent* shall expire the state and reclaim
29 resources if the response is not received within T4 seconds.

30 When adding an entry to the *Authenticated ID List*, the *Authenticating DHCP Agent* shall start a timer for that entry
31 which is set to expire at a point not to exceed the original lease duration (LEASE) from the original lease moment
32 (LEASEMOMENT). This includes List augmentation from *DHCP ACK Snooping*, *MS Authenticated ID List*
33 merging, and *provisioning system Authenticated ID List* synchronization.

34 The *Authenticating DHCP Agent* shall remove an entry from the *Authenticated ID List* when forwarding a DHCP
35 NACK to an untrusted port.

36 The *Authenticating DHCP Agent* shall remove an entry from the *Authenticated ID List* when forwarding a DHCP
37 DECLINE message issued from an untrusted port.

38 NOTE—The resulting DHCP ACK must still be forwarded even after the entry is removed from the List.

39 The *Authenticating DHCP Agent* shall remove an entry from the *Authenticated ID List* upon detection of a timer
40 expiration.

41 The *Authenticating DHCP Agent* shall remove all entries from the *Authenticated ID List* corresponding to a
42 particular MS when a Registration Cancellation is received.

1 The *Authenticating DHCP Agent* shall remove an old entry from the *Authenticated ID List* upon detection of an
2 existing IP address in the List before adding a new entry. The old entry is only discarded if it has a finite LEASE
3 period. Otherwise, the new entry is discarded.

4 The *Authenticating DHCP Agent* shall discard the least-recently-leased entry, e.g., the one with the oldest
5 LEASEMOMENT, in the *Authenticated ID List* that uses the same MS if an attempt to added a new entry to the List
6 is made which results in more than MAXMSIP entries for that MS.

7 ## E.8.1   Dynamic Host Configuration Protocol Optional Information Tagging

8 The System shall support DHCP Information Option Tagging.

9 The System shall have the ability to enable or disable all *Tagging DHCP Agent* functionality defined herein.

10 If disabled, the *Tagging DHCP Agent* shall forward all DHCP messages without discrimination or modification
11 using *Standard Learned Bridge Forwarding*.

12 The *Tagging DHCP Agent* shall append (or tag) an Information Option to all DHCP DISCOVERY, INFORM,
13 REQUEST, and DECLINE messages received from an untrusted port. The modified message must be then
14 forwarded/flooded to all trusted ports.

15 Any DHCP DISCOVERY, INFORM, REQUEST, or DECLINE message received by the *Tagging DHCP Agent* that
16 already contains an Information Option shall be silently discarded.

17 The *Tagging DHCP Agent* shall remove (or detag) any Information Options from all DHCP OFFER, ACK, NACK,
18 and FORCERENEW messages received from a trusted port. The modified message must be then forwarded to the
19 untrusted MS port.

20 NOTE—The subject message is not required to have the Information Option.

21 When tagging a DHCP message, the *Tagging DHCP Agent* shall add the Agent Circuit ID sub-option (1), specifying
22 the BS ID as the circuit ID.

23 When tagging a DHCP message, the *Tagging DHCP Agent* shall add the Agent Remote ID sub-option (2),
24 specifying the MS ID as the circuit ID.

25

F. Technical Annex: Support of real time services

As Release 1.0.0 provides only pre-provisioned QoS-Service Flows, Service Flows for real time service could not be activated dynamically. This limitation requires specific arrangements to support real time services also in Release 1.0.0.

As QoS resources are reserved for the whole duration while a subscriber is attached to the network, it is recommended to only activate QoS-services which allow sharing of radio resources dependent on the current traffic. The use of UGS (Unsolicited Grant Service) is not recommended because it will lock radio resources also in case if there is no traffic.

To provide 100% service guarantee it is recommended that the amount of bandwidth of real time services for the maximum of attached users per BS do not exceed the maximum bandwidth provided by the BS.

$$BW_{RT} * Subs_{Max} < BW_{Max}$$

BW_{RT} ...Bandwidth of real time service

$Subs_{Max}$ ... Maximum number of subscribers attached to a BS

BW_{Max} ... Maximum bandwidth provided by the BS

An illustrative example:

A guaranteed best effort together with the amount of active real time services should not exceed the BS capabilities. The unassured bandwidth of best effort traffic could exceed the capability of a BS.

Key:
R   Reserved Best Effort
G   Guaranteed Best Effort
S   Subscribed Real Effort
B   BS Capability
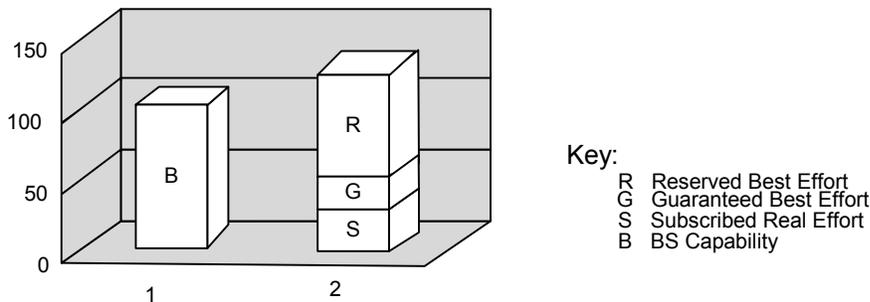
The number of maximum subscribers with real time service could be increased dependent on the distribution of active and inactive subscribers attached to a network and the usage of the real time service. E.g. a usage frequency of 50% for a service (which means, that an attached subscriber uses the service actively 50% of the time) will double the number of subscribers possible to be attached to a BS.

$$Subs_{Max} < BW_{Max}$$

Such extension of supported users may reduce the service guarantee.

An illustrative example:

All the registered subscribers are composed by users with and without a subscription for real time services. Furthermore, subscribers with a subscription can be reduced by them which haven't them activated.

Key:
A Active realtime services
I Inactive realtime services
U Users without realtime services
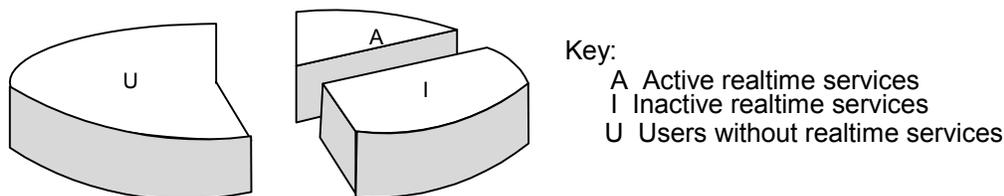
1   This will reduce the BS capability to guaranteed bandwidth and the traffic expected by subscribers with activated
2   real time traffic.

3