

3GPP2 X.S0054-300-0
Version 1.0
Date: December 19, 2007



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

QoS Support for Converged Access Network Specification

COPYRIGHT

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

This page is left blank intentionally.

QoS Support for Converged Access Network Specification

CONTENTS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

1	Introduction.....	1
	1.1 Scope.....	1
2	References.....	2
	2.1 Normative References.....	2
	2.2 Informative References.....	2
3	QoS Architecture.....	4
4	Subscriber QoS Profile.....	6
	4.1 Subscriber QoS Profile Attributes.....	6
	4.1.1 Maximum Authorized Aggregate Bandwidth.....	6
	4.1.2 Authorized FlowProfileIDs for the User	6
	4.1.3 Inter-User Priority.....	6
	4.1.4 Allowed Differentiated Service Markings.....	7
	4.2 AGW Requirements.....	7
	4.2.1 RADIUS	8
	4.2.2 Diameter	9
	4.3 AAA Requirements.....	9
	4.3.1 RADIUS	9
	4.3.2 Diameter	10
5	Backhaul QoS Management.....	11
	5.1 AGW Requirements.....	11
	5.2 eBS Behavior	11
6	Diffserv Support for CMIP/PMIP Traffic	12
	6.1 AGW Requirements.....	12
	6.2 HA Requirements	12
	6.3 AT Requirements.....	12

LIST OF FIGURES

<i>Figure 1</i>	QoS Architecture in CAN System	5
-----------------	--------------------------------------	---

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

LIST OF TABLES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

<i>Table 1</i>	Additional RADIUS Attributes between SRNC and AGW for Subscriber QoS Profile	8
<i>Table 2</i>	Additional RADIUS Attributes between AGW and AAA for Subscriber QoS Profile	8
<i>Table 3</i>	Additional Diameter AVPs between SRNC and AGW for Subscriber QoS Profile.....	9
<i>Table 4</i>	Additional Diameter AVPs between AGW and AAA for Subscriber QoS Profile	9

REVISION HISTORY

Revision	Date	Remarks
0	December 2007	Initial release

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

FOREWORD

(This foreword is not part of this Standard.)

This document was prepared by 3GPP2 TSG-X.

This document is a new specification.

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

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

X.S0054-300-X version n.0

where:

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

This document uses the following conventions:

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

This page is left blank intentionally.

1 Introduction

This document defines the stage-3 requirements for QoS support in the Converged Access Network (CAN).

1.1 Scope

This document is part of a multi-part document consisting of multiple parts that together describes Ultra Mobile Broadband^{TM1} Wireless IP Network operation.

The scope of this document covers support for over-the-air, backhaul and IP Quality of Service for Converged Access Networks.

¹ Ultra Mobile BroadbandTM and (UMBTM) are trade and service marks owned by the CDMA Development Group (CDG).

2 References

2.1 Normative References

This section provides references to other specifications and standards that are necessary to implement this document.

- [1] 3GPP2: C.S0084-0 v2.0, "Ultra Mobile Broadband (UMB) Air Interface", September 2007.
- [2] 3GPP2: A.S0020-0 v1.0, "Interoperability Specification (IOS) for Ultra Mobile Broadband (UMB) Radio Access Network Interfaces", November 2007.
- [3] 3GPP2: X.S0054-100-0 v1.0, "Basic IP Service for Converged Access Network Specification", December 2007.
- [4] 3GPP2: C.R1001-F, "Administration of Parameter Value Assignments for cdma2000 Spread Spectrum Standards", January 2007.
- [5] 3GPP2: X.S0054-910-0 v1.0, "CAN Data Dictionary", December 2007.
- [6] IETF: RFC2474, Nichols, et.al., "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", December 1998.
- [7] IETF: RFC2597, Heinanen, et.al., "Assured Forwarding PHB Group", June 1999.
- [8] IETF: RFC2598, Jacobson, et.al., "An Expedited Forwarding PHB", June 1999.
- [9] IETF: RFC2983, Black, "Differentiated Services and Tunnels", October 2000.
- [10] IETF: RFC2475, Blake, et.al., "An Architecture for Differentiated Services", December 1998.

2.2 Informative References

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

- <1> 3GPP2: X.S0054-000-0 v1.0, "CAN Wireless IP Network Overview and List of Parts", December 2007.
- <2> 3GPP2: X.S0054-102-0 v1.0, "Multiple Authentication and Legacy Authentication Support for CAN", December 2007.
- <3> 3GPP2: X.S0054-110-0 v1.0, "MIP4 Specification in Converged Access Network Specification", December 2007.
- <4> 3GPP2: X.S0054-210-0 v1.0, "CMIP based Inter-AGW Handoff", December 2007.
- <5> 3GPP2: X.S0054-220-0 v1.0, "Network PMIP Support", December 2007.
- <6> 3GPP2: X.S0054-300-0 v1.0, "QoS Support for Converged Access Network Specification", December 2007.

<7> 3GPP2: X.S0054-400-0 v1.0, "Converged Access Network Accounting Specification", December 2007.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

3 QoS Architecture

CAN system allows QoS differentiated IP services (such as VoIP and other data services) to be defined and specified independently within the confines of the UMB air interface (see 0). The UMB air interface supports multiple IP flows per AT. An IP flow is a series of packets that share a specific instantiation of IETF protocol layers. For example, an RTP flow may consist of the packets of an RTP/UDP/IP protocol instantiation, all of which share the same source and destination IP addresses and UDP port numbers. One or more IP flows can be mapped onto a single reservation identified by ReservationLabel and direction. One or more reservations are mapped to an over the air stream (see 0).

As specified in [2] and [3], the eBS exchanges data with the AGW via a RAN PMIP4 GRE tunnel. The eBS and AGW establish a per-AT GRE tunnel to transport data packets between the AT and the AGW. This per-AT GRE tunnel supports all IP sessions for the AT. If the AGW supports multiple RAN PMIP4 bindings per AT, the AGW may have a per-AT GRE tunnel with multiple eBSs [3], each tunnel using the same GRE key for the same AT.

Figure 1 illustrates the QoS architecture in CAN system. It is a graphical illustration of the relationship between IP flows, GRE Tunnel, and over-the-air reservations.

On the forward link, the AGW copies the DSCP contained in the inner IP header to the DSCP field of the outer IP header with consideration for DSCP marking specified by local policy. Upon receiving IP packets from an AGW, the eBS uses the packet filters received from the AT to map forward traffic to the corresponding over the air streams which may have different over the air QoS treatment.

On the reverse link, the eBS either copies the DSCP contained in the inner IP header to the DSCP field of the outer IP header, assigns a DSCP value in the outer IP header based on over-the-air QoS (e.g., QoS FlowProfileID) and local backhaul policy (see [2]). The AGW may modify the DSCP markings of the IP packet header based on the subscriber QoS profile and local policy.

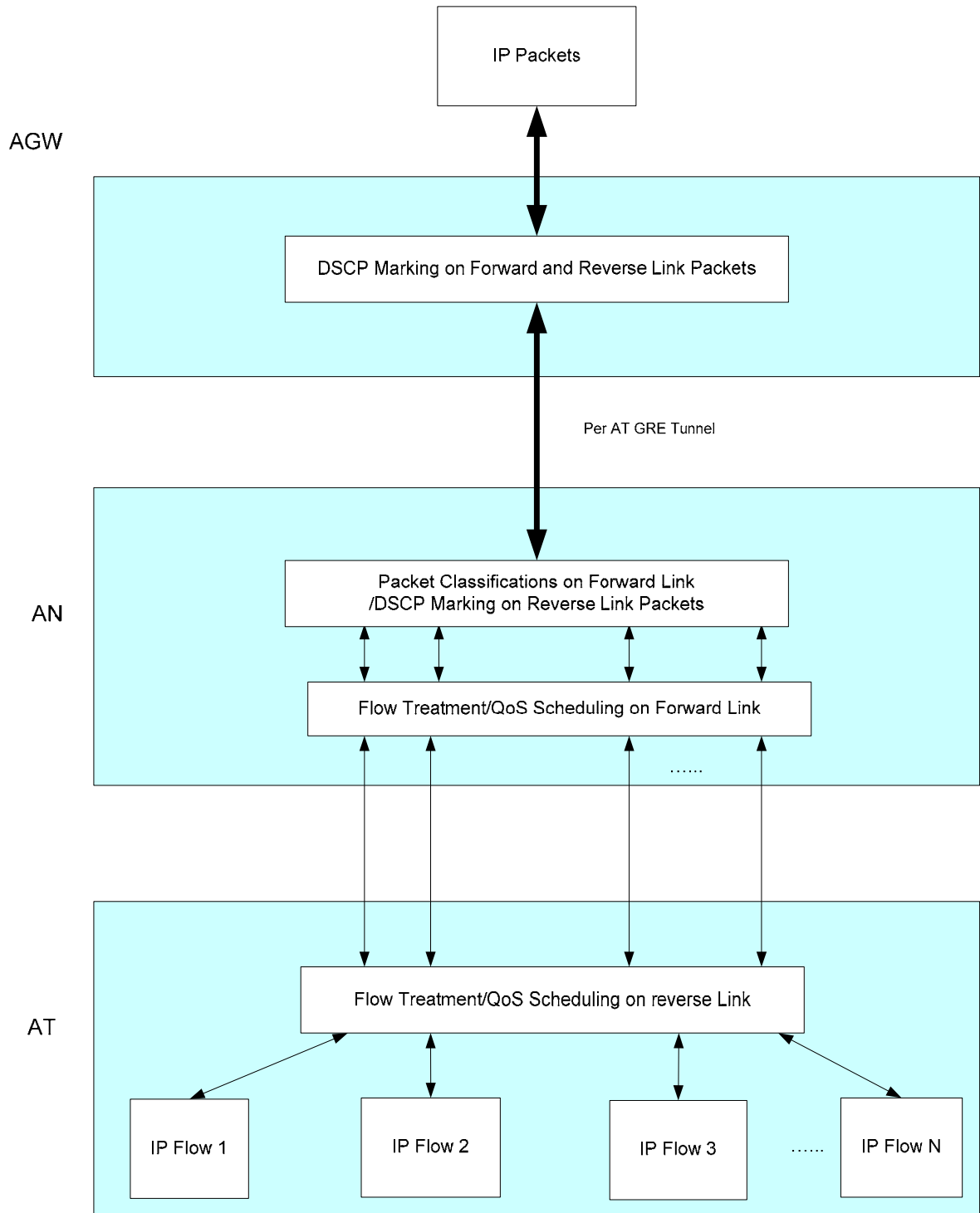


Figure 1 QoS Architecture in CAN System

4 Subscriber QoS Profile

4.1 Subscriber QoS Profile Attributes

The Subscriber (AT's) QoS Profile consists of the following 3GPP2 attributes (see [5]):

- Maximum-Authorized-Aggregate-Bandwidth,
- Authorized-FlowProfileIDs-for-the-user,
- Inter-User-Priority,
- Allowed-Differentiated-Services-Marking.

Passing of verbose authorized QoS parameters is not supported in this release.

4.1.1 Maximum Authorized Aggregate Bandwidth

A QoS Profile may contain Maximum Authorized Aggregate Bandwidth for the user. If the AGW receives the Maximum-Authorized-Aggregate-Bandwidth attribute used for both best effort and QoS traffic from the HAAA, the AGW shall send the attribute to the SRNC as part of the EAP Access Authentication and Authorization procedures (see [3]). The SRNC provides the Maximum-Authorized-Aggregate-Bandwidth attribute to the eBS (see [2]). The eBS uses this parameter for radio resource management.

4.1.2 Authorized FlowProfileIDs for the User

The Authorized-Flow-Profile-IDs-for-the-User attribute includes the authorized list of FlowProfileIDs for forward link and reverse link flows. The authorized list of FlowProfileIDs may be different in the forward and reverse links. Also, a FlowProfileID on the authorized list can be specified as applicable to both forward and reverse links. QoS parameters requested by the AT may contain a prioritized list of FlowProfileIDs for the forward link and reverse link (see 0). If the AGW receives the Authorized-Flow-Profile-IDs-for-the-User attribute from the HAAA, the AGW shall send the attribute to the SRNC as part of the EAP Access Authentication and Authorization procedures (see [3]). The SRNC provides the Authorized FlowProfileIDs to the eBS (see [2]). The eBS enforces the set of authorized profiles by not granting FlowProfileIDs that do not appear in the Authorized FlowProfileID list. The FlowProfileIDs are specified in [4].

4.1.3 Inter User Priority

A QoS Profile may contain an Inter-User priority value for the user. If the AGW receives the Inter-User-Priority attribute from the HAAA, the AGW shall send the attribute to the SRNC as part of EAP Access Authentication and Authorization procedures (see [3]). The SRNC provides the Inter-User-Priority attribute used for both best effort and QoS traffic to the eBS (see [2]). The eBS uses the Inter-User priority value for admission control, resource management and QoS scheduling.

4.1.4 Allowed Differentiated Service Markings

A QoS Profile may contain the Allowed-Differentiated-Services-Marking attribute. If the AGW receives the Allowed-Differentiated-Services-Marking attribute from the HAAA, the AGW shall store it and use it for DSCP markings.

In accordance with differentiated services standards [6], the AT may mark packets in the reverse direction. The AGW, however, may limit the differentiated services markings that the AT applies to packets based on the Subscriber QoS Profile received from the HAAA or based on its local policy. The AGW may provide a fixed marking for CMIP4 based reverse tunneled traffic and Network PMIP4 based tunneled traffic based on the Subscriber QoS profile received from the HAAA or based on its local policy.

The supported Differentiated Services Code Points (DSCPs) shall be based on the following RFCs:

- RFC2474 defines Class selectors as code points, whose lower three bits (3, 4, and 5) are all zero. Therefore, there are eight such classes. Default Forwarding (often called Best Effort) is a class selector with class equal to 0.
- RFC2597 defines Assured Forwarding (AF) classes.
- RFC2598 defines Expedited Forwarding (EF) Classes.

When the AT marks an IP packet with a DSCP, the AGW shall ensure that only an allowed DSCP is used as authorized by the HAAA in the users Subscriber QoS Profile. If the HAAA does not include the Subscriber QoS Profile for the user, the AGW shall offer default QoS settings to the user's packets if provisioned by the service provider.

The Allowed-Differentiated-Services-Marking attribute indicates the type of marking the user may apply to a packet. The attribute contains three subtypes. The subtype 1 contains three bits, the 'A', 'E', and 'O' bits. When the 'A' bit is set, the user may mark packets with any AF class. When the 'E' bit is set, the user may mark packets with EF class. When the 'O' bit is set, the user may mark packets with experimental/local use classes. The subtype 2 contains Max Class field which specifies the maximum class for which a user may mark a packet. For example, if the Max Class is set to Selector Class 3, all selector classes up to and including Selection Class 3 are allowed. If the Max Class is set to AF12, AF12 and AF13 marking are allowed. When all three subtype 1 bits are not set, and when the Max Class is set to zero, the user may only send packets marked best effort. The subtype 3 of the Allowed-Differentiated-Services-Marking attribute contains a reverse tunnel marking ('RT Marking', see [5], which is the DSCP marking level the AGW applies to CMIP4 reverse tunneled packets and/or Network PMIP4 reverse tunneled packets when those packets are not marked [9].

When reverse direction traffic arrives at the AGW, the AGW shall match the source address of such packets to a source address that is associated with an authenticated NAI. The AGW shall apply a DSCP to the packet based on the subscriber QoS profile if available and otherwise based on local policy.

4.2 AGW Requirements

If the AGW receives the Subscriber QoS Profile from the HAAA, the AGW shall provide QoS attributes as specified in Table 1 (RADIUS) or Table 3 (Diameter) to the SRNC for QoS request authorization and traffic policing purposes.

The formats of all the attributes in from Table 1 to Table 4 are specified in CAN AAA dictionary [5].

The AGW shall only use a subscriber QoS profile per AT associated with network access authentication NAI [3].

4.2.1 RADIUS

Table 1 Additional RADIUS Attributes between SRNC and AGW for Subscriber QoS Profile

Attribute Name	Type	Access-Request	Access-Accept	Access-Challenge	Access-Reject
Authorized Flow Profile IDs for the User	26/131	0	0-1	0	0
Maximum-Authorized Aggregate-Bandwidth	26/190	0	0-1	0	0
Inter-User-Priority	26/191	0	0-1	0	0

0 This attribute shall not be present.

0+ Zero or more instances of this attribute may be present.

0-1 Zero or one instance of this attribute may be present.

1 Exactly one instance of this attribute shall be present.

1+ One or more instances of these attributes shall be present.

Table 2 Additional RADIUS Attributes between AGW and AAA for Subscriber QoS Profile

Attribute Name	Type	Access-Request	Access-Accept	Access-Challenge	Access-Reject
Allowed Differentiated Services Marking	26/73	0	0-1	0	0
Authorized Flow Profile IDs for the User	26/131	0	0-1	0	0
Maximum-Authorized-Aggregate-Bandwidth	26/190	0	0-1	0	0
Inter-User-Priority	26/191	0	0-1	0	0

0 This attribute shall not be present.

0+ Zero or more instances of this attribute may be present.

0-1 Zero or one instance of this attribute may be present.

1 Exactly one instance of this attribute shall be present.

1+ One or more instances of these attributes shall be present.

4.2.2 Diameter

Table 3 Additional Diameter AVPs between SRNC and AGW for Subscriber QoS Profile

AVP Name	AVP Code	Diameter-EAP-Request	Diameter-EAP-Answer
Maximum-Authorized-Aggregate-Bandwidth	5535/25	0	0-1
Authorized-Flow-Profile-IDs-for-the-User	5535/26	0	0-1
Inter-User-Priority	5535/27	0	0-1

0 This attribute shall not be present.

0+ Zero or more instances of this AVP may be present.

0-1 Zero or one instance of this AVP may be present.

1 Exactly one instance of this AVP shall be present.

1+ One or more of these AVPs shall be present.

Table 4 Additional Diameter AVPs between AGW and AAA for Subscriber QoS Profile

AVP Name	AVP Code	Diameter-EAP-Request	Diameter-EAP-Answer
Maximum-Authorized-Aggregate-Bandwidth	5535/25	0	0-1
Authorized-Flow-Profile-IDs-for-the-User	5535/26	0	0-1
Inter-User-Priority	5535/27	0	0-1
Allowed-Differentiated-Services-Marking	5535/28	0	0-1

0 This attribute shall not be present.

0+ Zero or more instances of this AVP may be present.

0-1 Zero or one instance of this AVP may be present.

1 Exactly one instance of this AVP shall be present.

1+ One or more of these AVPs shall be present.

4.3 AAA Requirements

4.3.1 RADIUS

During the AT' access authentication and authorization with the HAAA [3] server, if the AT is successfully authenticated, the HAAA server may return the user's Subscriber QoS Profile information as specified in Table 2.

4.3.2 Diameter

During the AT's access authentication and authorization with the HAAA [3] server, if the AT is successfully authenticated, the HAAA server may return the user's Subscriber QoS Profile information as specified in Table 4.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

5 Backhaul QoS Management

The QoS treatment given to packets on the backhaul between the eBS and AGW is based on the IETF DS architecture [10].

5.1 AGW Requirements

On the forward link, the AGW may copy the DSCP value of the inner IP header to the DSCP field of the outer IP header. The AGW may remark the DSCP field of the outer IP header based on local policy. The AGW shall not modify the IP header of the inner IP packets.

On the reverse link, when the AGW receives packet from the eBS, the AGW shall match the source address of that packet to a source address that is associated with an authenticated NAI. The AGW may remark the packet based on the Allowed Differentiated Service Marking attribute and local policy.

5.2 eBS Behavior

For the forward link, upon receiving IP packets from the AGW, the eBS uses the packet filters received from the AT to map forward traffic to the corresponding over the air streams which may have different over the air QoS treatment. See 0 for the detailed requirements.

For the reverse link, upon receiving IP packets from an AT, the eBS copies the DSCP contained in the inner IP header to the DSCP field of the outer IP header, or marks the DSCP of the outer most IP header based on over-the-air granted QoS (e.g., QoS FlowProfileID), QoS Profile (Inter-User Priority), and local policy.

6 Diffserv Support for CMIP/PMIP Traffic

6.1 AGW Requirements

The Allowed-Differentiated-Services-Marking attribute contains a reverse tunnel marking ('RT Marking', see [5]), which is the marking level the AGW shall apply to reverse tunneled packets when those packets are not marked [9]. If CMIP4 reverse tunneling or Network PMIP4 is enabled, the AGW may copy the DSCP value of the inner IP header to the DSCP field of the outer IP header or the AGW may re-mark the DSCP value of the outer IP header based on RT Marking field in the Allowed-Differentiated-Services-Marking attribute received from the HAAA server or based on its local policy.

6.2 HA Requirements

For each received packet bound to the AT in CMIP4 FA mode or Network PMIP4 forward traffic, the HA shall either copy the DSCP value of the inner IP header to the DSCP field of outer IP header or re-mark the DSCP value of the outer IP header for the HA-FA tunnel based on local policy.

For each received packet bound to the AT in CMIP6 forward traffic, the HA shall either copy the DSCP value of the inner IP header to the DSCP field of the outer IP header or re-mark the DSCP value of the outer IP header for the HA-AT tunnel based on local policy.

6.3 AT Requirements

For CMIP6 reverse link traffic, the AT shall copy the DSCP marking of the inner IP header to the DSCP field of the outer IP header.