

Attachment 4-2-13

WiMAX Forum[®] Network Architecture

System Requirements, Network Protocols and Architecture for Multi-cast Broad-cast Services

Dynamic Service Flow Based (MCBCS - DSx)

WMF-T33-112-R015v01

Note: This Document is reproduced without any modification with the consent of the WiMAX Forum®, which owns the copyright in them.



WiMAX Forum[®] Network Architecture

System Requirements, Network Protocols and Architecture
for Multi-cast Broad-cast Services

Dynamic Service Flow Based (MCBCS – DSx)

WMF-T33-112-R015v01

WiMAX Forum[®] Approved
(2009-11-21)

WiMAX Forum Proprietary

Copyright © 2007-2009 WiMAX Forum. All Rights Reserved.

Copyright Notice, Use Restrictions, Disclaimer, and Limitation of Liability.

Copyright 2007-2009 WiMAX Forum. All rights reserved.

The WiMAX Forum® owns the copyright in this document and reserves all rights herein. This document is available for download from the WiMAX Forum and may be duplicated for internal use, provided that all copies contain all proprietary notices and disclaimers included herein. Except for the foregoing, this document may not be duplicated, in whole or in part, or distributed without the express written authorization of the WiMAX Forum.

Use of this document is subject to the disclaimers and limitations described below. Use of this document constitutes acceptance of the following terms and conditions:

THIS DOCUMENT IS PROVIDED “AS IS” AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST EXTENT PERMITTED BY LAW, THE WiMAX FORUM DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE WiMAX FORUM DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND DISCLAIMS ANY WARRANTIES TO THE CONTRARY.

Any products or services provided using technology described in or implemented in connection with this document may be subject to various regulatory controls under the laws and regulations of various governments worldwide. The user is solely responsible for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such regulations within the applicable jurisdiction.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE APPLICABILITY OR NON-APPLICABILITY OF ANY SUCH LAWS OR REGULATIONS OR THE SUITABILITY OR NON-SUITABILITY OF ANY SUCH PRODUCT OR SERVICE FOR USE IN ANY JURISDICTION.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF THE WiMAX FORUM OR ANY THIRD PARTY.

The WiMAX Forum has not investigated or made an independent determination regarding title or noninfringement of any technologies that may be incorporated, described or referenced in this document. Use of this document or implementation of any technologies described or referenced herein may therefore infringe undisclosed third-party patent rights or other intellectual property rights. The user is solely responsible for making all assessments relating to title and noninfringement of any technology, standard, or specification referenced in this document and for obtaining appropriate authorization to use such technologies, technologies, standards, and specifications, including through the payment of any required license fees.

NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES OF TITLE OR NONINFRINGEMENT WITH RESPECT TO ANY TECHNOLOGIES, STANDARDS OR SPECIFICATIONS REFERENCED OR INCORPORATED INTO THIS DOCUMENT.

IN NO EVENT SHALL THE WiMAX FORUM OR ANY MEMBER BE LIABLE TO THE USER OR TO A THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY’S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS DOCUMENT, THE USER WAIVES ANY SUCH CLAIM AGAINST THE WiMAX FORUM AND ITS MEMBERS RELATING TO THE USE OF THIS DOCUMENT.

The WiMAX Forum reserves the right to modify or amend this document without notice and in its sole discretion. The user is solely responsible for determining whether this document has been superseded by a later version or a different document.

“WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum Certified,” the WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks of the WiMAX Forum. Third-party trademarks contained in this document are the property of their respective owners.

TABLE OF CONTENTS

1	REVISION HISTORY.....	1
2	DOCUMENT SCOPE.....	2
3	MCBCS NETWORK REFERENCE MODEL.....	6
3.1	Overview of MCBCS Network Reference Model	6
3.2	MCBCS Specific Reference Points	10
4	MCBCS NORMATIVE PROCEDURES.....	12
4.1	MCBCS Controller/Server Discovery	12
4.1.1	General Procedure	12
4.1.2	Co-existence of Service Pre-configuration and Dynamic Discovery of the MCBCS Controller/Server to Support NAP sharing.....	16
4.1.3	AAA server procedure	16
4.1.4	Anchor Authenticator procedure	16
4.1.5	DHCP Server procedure	17
4.1.6	DHCP Relay Procedure	17
4.1.7	DHCP Proxy Procedure.....	17
4.1.8	MS Procedures	17
4.1.9	DHCP option.....	18
4.1.10	Error Handling.....	18
4.1.10.1	No information of MCBCS Controller/Server in the Access Accept message	18
4.1.10.2	Timers consideration for DHCP Proxy in the ASN and DHCP Relay	18
4.1.10.3	Handling Error Condition	18
4.1.11	RADIUS Related Messages and Attributes.....	19
4.2	End-to-end MCBCS Service Establishment	19
4.3	MCBCS Service initialization Procedure between MBS Proxy and MCBCS Controller/Server	22
4.3.1	MCBCS Service Intialization with Static Configuration	22
4.3.2	MCBCS Service initialization after the First MS Network Entry	22
4.3.2.1	MCBCS Service Initialization for Pre-provisioned Service Triggered by the very first MS's Initial Network Entry	23
4.3.2.2	MCBCS Service Initialization Triggered by the first Dynamic MCBCS Service Subscription after MS Attachment to the network.....	25
4.3.3	MCBCS Security Association Establishment between MBS Proxy and MCBCS Controller/Server	27
4.3.4	Error Handle Procedures.....	27
4.3.4.1	Timer MAX Retries	27
4.3.4.2	Timer Expiry.....	28
4.3.5	Message Primitive	29
4.3.6	Radius Message between the ASN and the CSN to Support MCBCS Service Initialization and Establishment.....	30
4.4	Service Provisioning Procedures	30
4.4.1	MS-side Service Provisioning.....	32
4.4.1.1	Service Annoucement/Service Guide Delivery	32
4.4.1.1.1	Service Annoucement.....	32
4.4.1.2	Service Subscription	32
4.4.1.3	Joining Service.....	33
4.4.1.3.1	Network Initiated Join	33
4.4.1.3.1.1	Network Initiated Join with Pre-provisioned MCBCS Services.....	33
4.4.1.3.1.2	Network initiated join with dynamic MCBCS subscription	38
4.4.1.3.1.3	MS Initiated Join	40
4.4.1.4	Leaving Service	42

MCBCS-DSx

1	4.4.1.4.1 MS initiated leaving service	43
2	4.4.1.4.2 Network initiated leaving service	46
3	4.4.2 Network-side Service Provisioning	48
4	4.4.2.1 Session Start	48
5	4.4.2.2 Session Stop	49
6	4.4.3 Timers and Timing Considerations	50
7	4.4.4 Service Provisioning Error Conditions	50
8	4.4.4.1 Timer Expiry	50
9	4.4.5 RADIUS Message between the ASN and the CSN to Support MS MCBCS Service Provisioning	51
10	4.5 MCBCS Data Path	51
11	4.5.1 Protocol Stack	52
12	4.5.1.1 Type-1 Protocol Stack	52
13	4.5.1.1.1 IP Transport over R3	53
14	4.5.1.1.2 IP Transport over R1/R4/R6	53
15	4.5.1.2 Type-3 Data Path Protocol Stack	54
16	4.5.1.2.1 IP Transport over R3	54
17	4.5.1.2.2 IP Transport over R1/R4/R6	54
18	4.5.1.3 GRE Encapsulation	55
19	4.5.2 MCBCS Datapath Service Mapping	56
20	4.5.2.1 MCBCS Datapath Reference Model	56
21	4.5.3 MCBCS Data Path Creation	58
22	4.5.3.1 Pre-configured Data Path	58
23	4.5.3.2 Dynamic Data Path Creation	58
24	4.5.4 Data Path Modification	62
25	4.5.5 Data Path Deletion	64
26	4.5.6 Error Handle Procedures	67
27	4.5.6.1 Timer MAX Retries	67
28	4.5.6.2 Timer Expiry	68
29	4.5.7 RADIUS Related Message and Attributions	68
30	4.5.7.1 RADIUS Message between the ASN NAS and CSN for the MCBCS Session Management	68
31	4.6 Mobility Management	68
32	4.6.1 MCBCS Service Continuity Handover Support for Multi-BS MBS	68
33	4.6.2 Intra MBS Zone	70
34	4.6.3 Inter MBS Zone	70
35	4.6.3.1 Fully Controlled HO for Inter-MBS Zones Mobility	70
36	4.6.3.1.1 HO Preparation Phase	70
37	4.6.3.1.1.1 R4 Message Definitions for HO Preparation Phase	71
38	4.6.3.1.1.2 MS Initiated HO Preparation Phase	72
39	4.6.3.1.1.3 Network Initiated HO Preparation Phase	73
40	4.6.3.1.1.4 HO Preparation Phase Error Conditions	74
41	4.6.3.1.2 HO Action Phase	74
42	4.6.3.1.2.1 R4 Message Definitions for HO Action Phase	74
43	4.6.3.1.2.2 Handover Action Scenario: Serving ASN Sends R4 HO_Cnf to Target ASN	75
44	4.6.3.2 Uncontrolled (Unpredictive) HO with Context Retrieval	77
45	4.6.3.2.1 R4 Message Definitions for Uncontrolled (Unpredictive) HO with Context Retrieval	77
46	4.6.3.2.2 Successful Uncontrolled Handover	78
47	4.6.4 Coexisting unicast service and MBS service	80
48	4.7 MCBCS Power Saving Support	80
49	4.7.1 Power Saving Support for MCBCS during the Intra and Inter MBS Zones Transitions	80
50	4.7.2 Location Update	81
51	10.6.1.1 Successful Location Update due to MBS Update triggered by inter-MBS Zone transition	81
52	4.7.2.1 Location Update Error Procedures	83
53	4.7.2.1.1 MBS Zone Update Failure	83
54	4.7.2.1.2 Message Primitive	83
55	4.7.3 MS MBS Idle Mode Exit	87
56	4.7.3.1 Idle Mode Exit - Serving ASN Has no MS Context	87

MCBCS-DSx

1	4.7.3.2	Idle Mode Exit Error Conditions	90
2	4.7.3.2.1	MBS Zone Update Failure.....	90
3	4.7.3.2.2	Message Primitive	90
4	4.7.4	MS MBS Idle Mode Entry.....	91
5	4.8	Security.....	92
6	4.9	MCBCS QoS	92
7	4.9.1	MCBCS QoS Support for Broadcast/Multicast Transport.....	92
8	4.9.1.1	MCBCS QoS Management Functional Descriptions.....	92
9	4.9.1.2	MCBCS QoS Support for Multicast Distribution Tree.....	94
10	4.9.1.3	MCBCS QoS Support Strategy over WiMAX ASN.....	94
11	4.10	MCBCS Charging and Accounting	95
12	4.10.1	MCBCS Charging/Accounting Support Reference Model.....	95
13	4.10.2	MCBCS Accounting Record Generation Principles.....	96
14	4.10.3	MCBCS Offline Accounting Support	98
15	4.10.3.1	Basic Principles.....	98
16	4.10.3.2	MCBCS Broadcast Services	99
17	4.10.3.3	MCBCS Multicast Services	99
18	4.10.4	MCBCS Online Accounting Support	99
19	4.10.5	UDR Generation.....	99
20	4.10.5.1	UDRs Related to MCBCS user.....	99
21	4.10.5.2	UDRs Related to MCBCS Content Provider	99
22	4.10.6	MCBCS UDR Collection Scenarios.....	99
23	4.10.6.1	MCBCS UDR for user - Timely Based Accounting Triggered by MS Join/Leave	99
24	4.10.6.2	Volume Based Accounting	101
25	4.11	End-to-end Transport Mechanism for Content Delivery	102
26	4.11.1	Data Transportation between CSN and ASN.....	102
27	4.11.2	Data Transportation within the MCBCS Transmission Zone inside the ASN	104
28	4.11.2.1	Unicast based Transport Multicast Distribution Tree Establishment.....	104
29	4.11.2.2	Multicast Distribution using Unicast-based Transport.....	106
30	4.11.2.3	Multicast Distribution using Multicast-based Transport.....	107
31	4.11.2.3.1	Multicast-based Transport Within the multicast-capable ASN	107
32	4.11.3	Multicast-based Transport Multicast Distribution Tree Establishment.	109
33	4.12	MCBCS Network Resource Management	110
34	4.12.1	MBS Data Synchronization	110
35	4.12.1.1	Intra-MBS Zone Data Synchronization	110
36	4.12.1.2	Inter-MBS Zones Data Synchronization.....	111
37	4.12.1.3	MBS Data Synchronization Functions.....	111
38	4.12.1.4	MCBCS Synchronization Functions implementation models	113
39	4.12.1.5	Implementation models coexistence considerations	115
40	4.12.2	Synchronization methodology.....	116
41	4.12.2.1	MBS Sync Rules Design Considerations.....	117
42	4.12.3	MCBCS Data Synchronization Support.....	117
43	4.12.3.1	MBS Sync Rule delivery	117
44	4.12.3.1.1	Synchronization Rules announcement.....	117
45	4.12.3.1.2	Synchronization Rule recovery	122
46	4.12.3.1.3	MBS Data Path recovery procedure	123
47	4.12.3.2	Timers and Timing Considerations.....	126
48	4.12.3.2.1	MBS sync rule and data recovery error handling	126
49	4.12.3.3	MBS Data flow level of synchronization across MBS Zones.....	126
50	4.12.3.4	MBS payload synchronization.....	127
51	4.12.3.5	MBS Sync Rule synchronization	129
52	4.12.4	Overlapping MBS Zones.....	130
53	5	MESSAGE AND PARAMETER DEFINITIONS.....	133
54	5.1	Message Definitions and Construction Rules.....	133

MCBCS-DSx

1	5.1.1	MBS Join Request.....	133
2	5.1.2	MBS Join Response	133
3	5.1.3	MBS Leave Request	133
4	5.1.4	MBS Leave Response.....	133
5	5.1.5	MBS Service Counter Request.....	134
6	5.1.6	MBS Service Counter Response	134
7	5.1.7	MBS Sync Rule Announcement.....	134
8	5.1.8	MBS Sync Rule Request.....	134
9	5.1.9	MBS_Data_Recovery_Request.....	135
10	5.1.10	MBS_Data_Recovery_Response.....	135
11	5.2	TLV Encoding	135
12	5.2.1	MBS Proxy and MCBCS Controller/Server Service Association SPI.....	135
13	5.2.2	MCBCS Controller/Server IPv4	135
14	5.2.3	MCBCS Controller/Server IPv6	136
15	5.2.4	MCBCS Controller/Server FQDN.....	136
16	5.2.5	MCBCS Service Info.....	136
17	5.2.6	MCBCS Transmission Zone ID	137
18	5.2.7	R3 Multicast IP Address.....	137
19	5.2.8	MCID.....	137
20	5.2.9	MBS Zone ID	137
21	5.2.10	Volume Required.....	138
22	5.2.11	Current Volume Counter	138
23	5.2.12	MBS Zone Update Indicator.....	138
24	5.2.13	SF Info (Refer to 5.3.2.185 in NWG Release v1.3.0)	138
25	5.2.14	CID/MCID (Refer to 5.3.2.29 in NWG Release v1.3.0).....	140
26	5.2.15	MCBCS Service Continuity Indicator.....	140
27	5.2.16	QoS Paramters (Refer to 5.3.2.141 in NWG Release v1.3.0)	140
28	5.2.17	Sync Rule GPS timestamp.....	141
29	5.2.18	OFDMA frame offset	141
30	5.2.19	MAC PDU Size.....	141
31	5.2.20	MBS_Data_Info.....	142
32	5.2.21	GRE sequence number start	142
33	5.2.22	GRE sequence number end.....	142
34	5.2.23	MBS data packet size.....	142
35	5.2.24	MBS_DATA_IE_Context.....	143
36	5.2.25	MBS_MAP_IE_Context.....	143
37	5.2.26	MBS Burst Frame Offset.....	144
38	5.2.27	Next MBS MAP change indication	144
39	5.2.28	Next MBS No. OFDMA Symbols	145
40	5.2.29	Next MBS No. OFDMA Subchannels	145
41	5.2.30	MBS DIUC	145
42	5.2.31	OFDMA symbol offsets DATA IE	145
43	5.2.32	Subchannel offset DATA IE	146
44	5.2.33	Boosting.....	146
45	5.2.34	No. OFDMA Symbols	146
46	5.2.35	No. OFDMA Subchannels	146
47	5.2.36	No. Subchannels	146
48	5.2.37	Repetition Coding indication.....	147
49	5.2.38	Next MBS Burst Frame offset	147
50	5.2.39	Next OFDMA Symbol offset	147
51	5.2.40	MBS Permutation Zone Defined.....	147
52	5.2.41	OFDMA symbol offset MAP IE	148
53	5.2.42	Subchannel offset MAP IE.....	148
54	5.2.43	Permutation	148
55	5.2.44	DL_PermBase	148
56	5.2.45	PRBS_ID	148

MCBCS-DSx

1	5.2.46	MBS MAP message allocation included indication.....	149
2	5.2.47	Downlink Burst Profile.....	149
3	5.2.48	MBS Burst.....	149
4	5.2.49	Next Sync Rule expected TOA	150
5	5.2.50	MBS Burst Scheduling Cycle.....	150
6	5.2.51	MBS MAC Burst SN.....	150
7	5.2.52	MAX MAC PDU Size.....	150
8	5.2.53	MBS SDU packet size.....	150
9	5.2.54	Requested packet.....	151
10	5.2.55	Packet SN	151
11	5.2.56	Packet size	151
12	5.2.57	MBS Distribution DPF ID.....	152
13	5.3	RADIUS Messages and Attributes	152
14	5.3.1	WiMAX RADIUS Message Definitions	152
15	5.3.1.1	Radius Message between the NAS and AAA for the support of Dynamic Discovery of MCBCS Controller/Server	152
16	5.3.1.1.1	WiMAX Radius VSA Definition for MCBCS Controller/Server Discovery	153
17	5.3.1.1.1.1	MCBCS-Controller-Server-IPv4	153
18	5.3.1.1.1.2	MCBCS-Controller-Server-IPv6	153
19	5.3.1.1.1.3	MCBCS-Controller-Server-FQDN.....	154
20	5.3.1.1.1.4	MCBCS-Service-Association-SPI.....	155
21	5.3.1.2	Radius Message between the ASN and the CSN to Support MCBCS Service Initialization and Establishment as well as MS MCBCS service provisioning	155
22	5.3.1.3	RADIUS MCBCS service attributes which are required to support the MCBCS session management messaging exchanged between the MBS Proxy and MCBCS Controller/Server	157
23	5.3.1.3.1	WiMAX Radius VSA Definition for MCBCS Session Management and Service Profile	158
24	5.3.1.3.1.1	MCBCS-Program-Descriptor	158
25	5.3.1.3.1.2	Packet-Flow Descriptor [Refer to 5.4.2.28 in NWG Release v1.3.0].....	159
26	5.3.1.3.1.3	QoS-Descriptor [Refer to 5.4.2.29 in NWG Release v1.3.0].....	161
27	5.3.1.4	Radius Related messages for MCBCS Accounting	163
28	5.3.1.4.1	Status and Type	163
29	5.3.1.4.2	Record Correlators.....	164
30	5.3.1.4.3	User Identification	165
31	5.3.1.4.4	Time	166
32	5.3.1.4.5	L3 Counters	166
33	5.3.1.4.6	Granted-QoS.....	167
34	5.3.1.4.7	Flow Specification.....	168
35	5.3.1.4.8	RADIUS VSA Definition for MCBCS Accounting Support	168
36	5.3.1.4.8.1	MCBCS service Type.....	168
37	5.3.1.4.8.2	Transport Type	169
41	ANNEX A: IEEE 802.16 MCBCS SYNCHRONIZATION SUPPORT (INFORMATIVE).....		170
42	ANNEX B – SYNCHRONIZATION AMONG THE MULTIPLE MBS DISTRIBUTION DPFS (INFORMATIVE)		173
44	ANNEX C – IEEE 802.16 SERVICE CONTINUITY SUPPORT CAPABILITIES		174
45			

List of Figures

FIGURE 3-1 : MCBCS NETWORK REFERENCE MODEL	6
FIGURE 4-1 : DYNAMIC MCBCS CONTROLLER/SERVER DISCOVERY VIA DHCP PROXY	12
FIGURE 4-2 : DYNAMIC MCBCS CONTROLLER/SERVER DISCOVERY VIA DHCP PROXY WITH DHCP- INFORM/INFORMATION-REQUEST	13
FIGURE 4-3 : DYNAMIC MCBCS CONTROLLER/SERVER DISCOVERY VIA DHCP RELAY	14
FIGURE 4-4 : DYNAMIC MCBCS CONTROLLER/SERVER DISCOVERY VIA DHCP RELAY WITH DHCP- INFORM/INFORMATION	16
FIGURE 4-5 : MCBCS SERVICE INITIALIZATION ESTABLISHMENT SCENARIO TRIGGERED BY THE FIRST MS ENTERING THE NETWORK	19
FIGURE 4-6 : MCBCS SERVICE INITIALIZATION ESTABLISHMENT SCENARIO TRIGGERED BY THE SESSION START	21
FIGURE 4-7: PRE-PROVISIONED MCBCS NETWORK INITIALIZATION PROCEDURES WITH THE VERY FIRST MS INE TO TRIGGER	24
FIGURE 4-8 : DYNAMIC MS SERVICE SUBSCRIPTION OR REGISTRATION TO TRIGGER THE MCBCS NETWORK INITIALIZATION PROCEDURES	25
FIGURE 4-9 : MCBCS SERVICE STATE TRANSITION – MS SIDE	30
FIGURE 4-10 : MCBCS SERVICE STATE TRANSITION – NETWORK SIDE	31
FIGURE 4-11 : NETWORK INITIATED JOIN PROCEDURE WITH PRE-PROVISIONED MCBCS SERVICE	34
FIGURE 4-12 : NETWORK INITIATED JOIN WITH DYNAMIC MCBCS SUBSCRIPTION	39
FIGURE 4-13 : MS INITIATED JOIN PROCEDURE	41
FIGURE 4-14 : MS INITIATED LEAVING SERVICE	43
FIGURE 4-15 : NETWORK INITIATED LEAVING SERVICE	47
FIGURE 4-16 : SESSION START PROCEDURE	48
FIGURE 4-17 : SESSION STOP PROCEDURE	49
FIGURE 4-18 : PROTOCOL STACK FOR TYPE-1 MCBCS DATA PLANE	53
FIGURE 4-19 : EXAMPLE OF TYPE-1 MCBCS DATA TRANSFER	54
FIGURE 4-20 : PROTOCOL STACK FOR TYPE-3 MCBCS DATA PLANE	54
FIGURE 4-21 : TYPE-3 DATA PATH PACKET PROCESSING	55
FIGURE 4-22 : EXAMPLE OF TYPE-3 MCBCS DATA TRANSFER	55
FIGURE 4-23 : MCBCS SERVICE DATA PATH MAPPING	56
FIGURE 4-24 : MCBCS DATA PLANE OBJECT MODEL	57
FIGURE 4-25 : MBS DATAPATH CREATION TRIGGERED BY THE ANCHOR SFA	59
FIGURE 4-26 : MBS DATAPATH CREATION TRIGGERED BY MCBCS CONTROLLER	62
FIGURE 4-27 : MBS DATA PATH MODIFICATION	63
FIGURE 4-28 : MBS DATA PATH DEREGISTRATION	65
FIGURE 4-29: DATA PATH DELETION TRIGGERED BY THE LAST MS EXIT	66
FIGURE 4-30 : SUCCESSFUL HO PREPARATION PHASE	72
FIGURE 4-31: SUCCESSFUL HO PREPARATION PHASE FOR NETWORK-INITIATED HO	73
FIGURE 4-32 : SUCCESSFUL HO ACTION PHASE	76
FIGURE 4-33 : UNCONTROLLED (UNPREDICTIVE) HO	79
FIGURE 4-34 : LOCATION UPDATE PROCEDURE DUE TO THE TRIGGER OF MBS UPDATE FOR INTER MBS ZONE TRANSITION CASE	82
FIGURE 4-35 : IDLE MODE EXIT PROCEDURE FOR INTER MBS ZONE CASE	88
FIGURE 4-36 : MCBCS QOS MANAGEMENT FUNCTIONAL MODEL	93
FIGURE 4-37 : NRM FOR MCBCS ACCOUNTING RECORDS GENERATION	96
FIGURE 4-38 : MCBC SERVICE IDENTIFIERS FORACCOUNTING SUPPORT	97
FIGURE 4-39 : MCBCS UDR FOR USER TIMELY BASED ACCOUNTING TRIGGERED BY MS JOINT/LEAVE	100
FIGURE 4-40 : MCBCS VOLUME BASED ACCOUNTING	101
FIGURE 4-41 : DATA TRANSPORT OVER R3	103
FIGURE 4-42: EXAMPLE OF MULTICAST DISTRIBUTION WITH UNICAST BASED TRANSPORT TRIGGERED BY SESSION START	104

MCBCS-DSx

1	FIGURE 4-43 : EXAMPLE OF MULTICAST DISTRIBUTION WITH UNICAST BASED TRANSPORT	
2	TRIGGERED BY THE FIRST MS	105
3	FIGURE 4-44 : UNICAST-BASED MULTICAST-DISTRIBUTION REFERENCE MODEL	106
4	FIGURE 4-45 : MULTICAST-BASED TRANSPORT MECHANISM FOR MULTICAST DISTRIBUTION	
5	SUPPORT FOR THE MCBCS CONTENT DELIVERY	107
6	FIGURE 4-46 : MULTICAST GROUP MEMBERSHIP MANAGEMENT	108
7	FIGURE 4-47 : MULTICAST-BASED TRANSPORT MULTICAST DISTRIBUTION DATA PATH	
8	ESTABLISHMENT	109
9	FIGURE 4-48 : MBS DATA SYNCHRONIZATION GENERIC REFERENCE MODEL	112
10	FIGURE 4-49 : MODEL A IMPLEMENTATION OF MCBCS SYNC FUNCTIONS	114
11	FIGURE 4-50 : MODEL B IMPLEMENTATION OF MCBCS SYNC FUNCTIONS	114
12	FIGURE 4-51 : MODEL C IMPLEMENTATION OF MCBCS SYNC FUNCTIONS	115
13	FIGURE 4-52 : MBS DATA SYNCHRONIZATION METHODOLOGY	116
14	FIGURE 4-53 : MBS SYNC RULE ANNOUNCEMENT BY MBS SYNCHRONIZATION CONTROLLER	118
15	FIGURE 4-54 : MBS SYNC RULE ENFORCEMENT TIME AND MBS BURST SCHEDULING	118
16	FIGURE 4-55 : MBS SYNC RULE RECOVERY	123
17	FIGURE 4-56 : MBS DATA RECOVERY OVER THE MBS DATA PATH	124
18	FIGURE 4-57 : MBS PAYLOAD SYNCHRONIZATION ACROSS MBS ZONES – OPTION 1	128
19	FIGURE 4-58 : MBS PAYLOAD SYNCHRONIZATION ACROSS MBS ZONES – OPTION 2	128
20	FIGURE 4-59 : MBS SYNC RULE SYNCHRONIZATION ACROSS MBS ZONES – OPTION 1	130
21	FIGURE 4-60 : MBS SYNC RULE SYNCHRONIZATION ACROSS MBS ZONES – OPTION 2	130
22	FIGURE 4-61 : EXAMPLE OF OVERLAPPING MBS ZONE AREAS	131
23	FIGURE 4-62 : EXAMPLE OF MBS ZONES COLOURING GRAPH	131

26 LIST OF TABLES

27	TABLE 2-1: PHASE-1 SCOPE FOR MCBCS DEVELOPMENT	3
28	TABLE 3-1 : MCBCS REFERENCE POINT IMPACT SUMMARY	10
29	TABLE 4-1: MAX RETRIES TIMER VALUES	27
30	TABLE 4-2 : ACTIONS AFTER TIMER MAX RETRY	28
31	TABLE 4-3 : MBS_JOIN_REQ MESSAGE	29
32	TABLE 4-4 : MBS_JOIN_RSP MESSAGE	29
33	TABLE 4-5 : MBS_JOIN_REQ MESSAGE FROM ANCHOR SFA TO MBS PROXY	35
34	TABLE 4-6 : MBS_JOIN_RSP MESSAGE FROM MBS PROXY TO ANCHOR SFA	35
35	TABLE 4-7 : RR-REQ MESSAGE FOR MCBCS SERVICE FROM ANCHOR SFA TO SFM	36
36	TABLE 4-8 : RR-RSP MESSAGE FOR MBS SERVICE FROM SERVING SFA TO ANCHOR SFA	37
37	TABLE 4-9 : MBS_JOIN_REQ MESSAGE FROM SERVING SFA TO ANCHOR SFA	41
38	TABLE 4-10 MBS_JOIN_RSP MESSAGE FROM ANCHOR SFA TO SERVING SFA	42
39	TABLE 4-11 : MBS_LEAVE_REQ MESSAGE FROM SERVING SFA TO ANCHOR SFA	43
40	TABLE 4-12 : MBS_LEAVE_RSP FROM ANHOR SFA TO SERVING SFA	44
41	TABLE 4-13 : MBS_LEAVE_REQ FROM ANCHOR SFA TO MBS PROXY	44
42	TABLE 4-14 : MBS_LEAVE_RSP FROM MBS PROXY TO ANCHOR SFA	44
43	TABLE 4-15 : RR-REQ MESSAGE: DELETION OF SF	45
44	TABLE 4-16 : RR-RSP MESSAGE: DELETION OF SF	46
45	TABLE 4-17 : TIMER VALUES FOR SERVICE PROVISIONING PROCEDURE	50
46	TABLE 4-18 : TIMER MAX RETRY CONDITIONS	51
47	TABLE 4-19 : PATH REGISTER REQUEST MESSAGE	59
48	TABLE 4-20 : PATH REGISTER RESPONSE MESSAGE	60
49	TABLE 4-21 : PATH MODIFICATION REQUEST MESSAGE	63
50	TABLE 4-22 : PATH MODIFICATION RESPONSE MESSAGE	64
51	TABLE 4-23 : PATH DE-REGISTRATION REQUEST MESSAGE	65
52	TABLE 4-24 : PATH DE-REGISTRATION RESPONSE MESSAGE	66
53	TABLE 4-25 : NETWORK EXIT TIMER VALUES	67

MCBCS-DSx

1	TABLE 4-26 : ACTIONS AFTER TIMER MAX RETRY	68
2	TABLE 4-27: HO REQ	71
3	TABLE 4-28 : HO CNF (HO CONFIRM TYPE IS CONFIRM OR UNCONFIRM)	74
4	TABLE 4-29 : CONTEXT RPT (FROM THE SERVING ASN TO THE TARGET ASN).....	77
5	TABLE 4-30 : LU_REQ PRIMITIVE STRUCTURE	84
6	TABLE 4-31 : LU_RSP PRIMITIVE STRUCTURE	84
7	TABLE 4-32 : LU_CNF PRIMITIVE STRUCTURE.....	86
8	TABLE 4-33 : IM_EXIT_STATE_CHANGE_RSP.....	90
9	TABLE 4-34 : IM_ENTRY_STATE_CHANGE_REQ.....	91
10	TABLE 4-35 : CHARGING/ACCOUNTING REQUIREMENTS FOR SERVICE DELIVERY	97
11	TABLE 4-36 : APPLICABILITY OF ACCOUNTING MEASUREMENT.....	98
12	TABLE 4-37 : MBS_SYNC_RULE_ANNOUNCEMENT FROM MBS SYNC CONTROLLER TO MBS SYNC	
13	EXECUTOR	119
14	TABLE 4-38 : MBS_SYNC_RULE_REQUEST FROM MBS SYNC EXECUTOR TO MBS SYNC	
15	CONTROLLER	123
16	TABLE 4-39 : MBS_DATA_RECOVERY_REQUEST	125
17	TABLE 4-40 : MBS_DATA_RECOVERY_RESPONSE	125
18	TABLE 4-41 : TIMER VALUES FOR SYNC RULE DELIVERY AND RECOVERY PROCEDURE.....	126
19	TABLE 4-42 : ACTION ON THE RECOVERY FAILURE	126
20	TABLE 5-1 : MCBCS CONTROLLER/SERVER ATTRIBUTES IN FINAL RADIUS ACCESS-ACCEPT FROM	
21	AAA TO ASN.....	152
22	TABLE 5-2 : RADIUS ACCESS MESSAGES FOR MCBCS BETWEEN MBS PROXY AND MCBCS	
23	CONTROLLER/SERVER.....	155
24	TABLE 5-3 : RADIUS ACCESS MESSAGES FOR MCBCS BETWEEN ASN AND AAA.....	155
25	TABLE 5-4 : RADIUS COA MESSAGE FOR MCBCS FROM AAA TO ASN NAS.....	156
26	TABLE 5-5 : COA MESSAGE (FOR SESSION START/STOP)	157
27	TABLE 5-6 : COA ACK (SESSION START/STOP RSP MESSAGE)	158
28	TABLE 5-7 : STATUS AND TYPE FOR RADIUS ACCOUNTING START/STOP/INTERIM MESSAGES	163
29	TABLE 5-8 : RECORD CORRELATORS FOR RADIUS ACCOUNTING START/STOP/INTERIM MESSAGES	
30	164
31	TABLE 5-9 : USER IDENTIFICATION FOR RADIUS ACCOUNTING START/STOP/INTERIM MESSAGES	
32	165
33	TABLE 5-10 : TIME FOR RADIUS ACCOUNTING START/STOP/INTERIM MESSAGES.....	166
34	TABLE 5-11 : L3 COUNTERS FOR RADIUS ACCOUNTING START/STOP/INTERIM MESSAGES	166
35	TABLE 5-12 : GRANTED-QOS FOR RADIUS ACCOUNTING START/STOP/INTERIM MESSAGES	167
36	TABLE 5-13 : FLOW SPECIFICATION FOR RADIUS ACCOUNTING START/STOP/INTERIM MESSAGES	
37	168

Annex A - Table- 1: MBS Sync Rule information for MBS bearer processing operations

1 Revision History

November 6, 2009	Initial version of Release 1.5.
---------------------	---------------------------------

2 Document Scope

This section describes the phase-1 development of Multicast and Broadcast (MCBCS) services for the WiMAX network which is fully compliant to IEEE 802.16-Rev2 [3] specification and more importantly, it is fully compliant to the WiMAX Forum TWG Rel-1.0 and the upcoming TWG Rel-1.5 system profiles.

This document refers to the service requirements that are provided by SPWG to specify over the system requirements and stage 2 specifications to support the MCBCS services in WiMAX network. The following summarized the agreed partitioning of the phase-1 and phase-2 development for the support of MCBCS in the WiMAX network.

1

Table 2-1: Phase-1 Scope for MCBCS Development

SPWG Req#	Requirements	Phase1	Phase2
R-[333]	In WiMAX networks, MCBCS feature specifications MAY maximize reuse of existing MCBCS frameworks defined by other standard organizations such as 3GPP Ref[60], 3GPP2 Ref [93] and Ref[85] and OMA Ref [115], in order to maximize reuse of existing broadcast/multicast technologies and opportunities for shared network resources. <i>Informative Note:</i> Full compatibility with 3GPP and 3GPP2 network solutions may be achieved but is not required.	X	
R-[334]	WiMAX networks with MCBCS capability SHOULD be consistent with OMA defined BCAST architecture model Ref [115], interfaces and protocols to deliver multicast/broadcast services.		X
R-[335]	WiMAX networks with MCBCS SHALL provide radio resource sharing between broadcast, multicast and unicast transmissions.	X	
R-[336]	The WiMAX network SHALL provide open interfaces between functional entities that support MCBCS	X	
R-[337]	Upon subscription to a MCBCS program, the WiMAX network SHOULD utilize standardized mechanism from 3GPP, 3GPP2, or OMA, such as 3GPP Ref[60], 3GPP2 Ref [93] and Ref[85] and OMA Ref [115], to allow user to set user preference.	X	
R-[338]	The WiMAX Network SHALL provide user with means of controlling, e.g. receiving and rejecting, his or her subscribed MCBCS program while at home or roaming. NOTE: The MCBCS roaming support is part of Phase-2		X
R-[339]	The WiMAX network MAY store the MCBCS user service preferences and use them in content delivery and charging considerations .	X	
R-[340]	The WiMAX network MAY collect MCBCS statistical data such as lost frames, assigned resources, achieved bit-rates, etc.	X	
R-[341]	The WiMAX network SHALL provide procedures and signaling to trigger the collection of MCBCS statistics from select MSs based on operator policy.	X	
R-[342]	The WiMAX network SHALL be capable of delivering the collected MCBCS statistics to OAM&P functional elements.	X	
R-[362]	In a WiMAX network that supports power saving modes, the MS SHALL receive MCBCS programs in the power saving modes at the negotiated QoS level.	X	
R-[343]	The MCBCS transmission zone for each MCBCS program SHALL be independently defined.	X	
R-[434]	The WiMAX Network SHALL allow every BS to simultaneously transmit broadcast, multicast, and unicast data on the same radio.	X	
R-[477]	The AP SHALL have the ability to independently configure the MCBCS Transmission Zones for each MCBCS program.	X	
R-[478]	The SP SHALL be able to determine and to provide to AP the service areas where a specific MCBCS program is to be offered. The service area refers to specific geographic or regulatory defined regions	X	
R-[346]	One MCBCS transmission zone MAY span multiple cells/sectors of the same WiMAX network.	X	
R-[472]	The Transmission Zones for the same MCBCS program MAY overlap, so that one BS MAY belong to multiple MCBCS Transmission Zones.	X	

MCBCS-DSx

R-[346]	One MCBCS transmission zone MAY span multiple cells/sectors of the same WiMAX network.	X	
R-[472]	The Transmission Zones for the same MCBCS program MAY overlap, so that one BS MAY belong to multiple MCBCS Transmission Zones. NOTE: This requirement will further be clarified until IEEE settles with the definition of the MBS Zone.	NA	NA
R-[347]	It SHOULD be possible to use RF boundaries such as sectors, cells, clusters, to define the MCBCS transmission zones..	X	
R-[349]	Each BS in the MCBCS transmission zone, when offering Multicast Services, MAY independently decide to use over the air unicast or multicast transmission for distribution of the MCBCS program based on the number of users served by the BS, on the QoS associated with the MCBCS flows, or other configurable radio resource management policies. NOTE: Dynamic switching support between unicast and multicast transport for MCBCS is deferred to phase-2. Sprint, Nokia and NSN object with such decision.		X
R-[350]	Delivery verification: the WiMAX network SHALL provide secure mechanisms to request for and capture content delivery confirmation for MCBCS messages requiring delivery confirmation by the MS.		X
R-[351]	When MCBCS delivery verification is supported, the WiMAX network SHOULD schedule the uplink transmission of the verification messages in order to minimize their impact on the normal network operation and services.		X
R-[352]	The WiMAX network MAY synchronously simulcast the same MCBCS program from multiple BSs to facilitate macro-space diversity combining of the signals received by the MS. The WiMAX network SHALL support Multi-BS access type defined in the IEEE 802.16e-2005 standard Ref[9].	X	
R-[353]	The WiMAX network MAY support independent scheduling of MCBCS transmissions by individual base stations, i.e. for the case of single BS MCBCS..	X	
R-[354]	All media types for MCBCS SHALL be supported independently of the specific data types and formats used for media encoding, including but not limited to: • Text, including embedded hypertext • Still Images • Video • Speech • Mono/Stereo Audio	X	
R-[355]	The WiMAX network SHALL provide the means for discovery and initial acquisition of Service Information	X	
R-[491]	The WiMAX network SHALL provide the Service Information including Program/Content general information, Program/Content access information, and Program/Content acquisition information	X	
R-[356]	The WiMAX network SHALL be able to provide the necessary QoS for real-time applications such as audio and video	X	
R-[357]	The MCBCS capability SHALL enable multiple priority levels for MCBCS flows, so that if contention for resources arises, a higher-priority MCBCS flow SHALL have precedence over lower-priority flows..		X
R-[358]	The WiMAX MS MAY be involved in multiple concurrent active MCBCS and unicast sessions.	X	
R-[359]	The WiMAX network SHALL support MS or Network initiated activation of additional MCBCS and unicast sessions while delivering the MCBCS and/or unicast program.	X	

	NOTE: MS initiated is deferred to Phase-2.	
R-[360]	The MS SHALL be able to receive incoming call/service notification while receiving MCBCS programs.	X
R-[361]	When a MS fails to successfully receive parts of a MCBCS content, the MS MAY selectively request for and receive the missing parts	X
R-[363]	The WiMAX network MAY support multiple concurrent MCBCS transmissions of independent programs over dissimilar transmission zones, e.g. MCBCS Transmission zones configured for and associated with <i>transmission of local, regional or national MCBCS Programs all in the same network. For example a network consisting of 200BS's may define 50 local, 5 regional and 1 National Zones.</i>	X
R-[364]	Roaming MCBCS users SHOULD receive MCBCS content from home network MCBCS service delivery and from serving network MCBCS service delivery based on policy and business agreements.	X
R-[365]	The WiMAX network SHALL be able to authenticate MCBCS users, to provide service protection.	X
R-[366]	The WiMAX network SHALL authorize MCBCS users on designated subscribed MCBCS programs.	X
R-[367]	The WiMAX network SHALL support both static multicast group and dynamic multicast group. Any member of the group SHOULD be able to check the integrity and authenticate the source of each packet in multicast or broadcast data streams. NOTE: Dynamic multicast is phase-2 work item	X
R-[368]	MCBCS authentication MAY be different between broadcast and multicast operation.	X
R-[369]	The WiMAX network SHALL support application-level encryption of MCBCS content.	X
R-[370]	The WiMAX network SHALL support secure delivery of MCBCS content and service related information to the subscribed users.	X
R-[371]	The WiMAX network SHOULD control MCBCS content distribution as per OMA Digital Rights Management Ref [116]. NOTE: Need to consult with security group for advice regarding the content security support with this mechanism when the application layer encryption is already supported.	TBD
R-[372]	Accounting records SHALL include the following information: <ul style="list-style-type: none"> • Delivered content and service class • Geographic Service Area • Time and date of start and end of content delivery • Delivery confirmation if applicable • User information • The accounting record MAY also include some information on radio resources utilized to offer the MCBCS service to the user 	X

3 MCBCS Network Reference Model

3.1 Overview of MCBCS Network Reference Model

This section describes the system functional components that are required to support MCBCS over a WiMAX network.

MCBCS shall leverage the airlink features at both the MAC and PHY layers, defined in the IEEE 802.16Rev2 specification, to establish and to release the transport of the MCBCS content(s). The WiMAX MCBCS system is composed of ASN and CSN WiMAX- specific procedures and signaling.

Application level procedures and signaling between the MBS client in the MS and the MCBCS Controller/Server in CSN is out of scope for the WiMAX MCBCS specification. This allows for flexibility when accommodating all broadcast application level solution such as OMA BCAST.

Note that not all the functional elements, that are described in the following NRM, are within the development scope of this specification. The presence of all the functional elements in the NRM is for the purpose of a complete description of the end-to-end MCBCS system architecture. When appropriate, the clarification will be provided in the corresponding functional description.

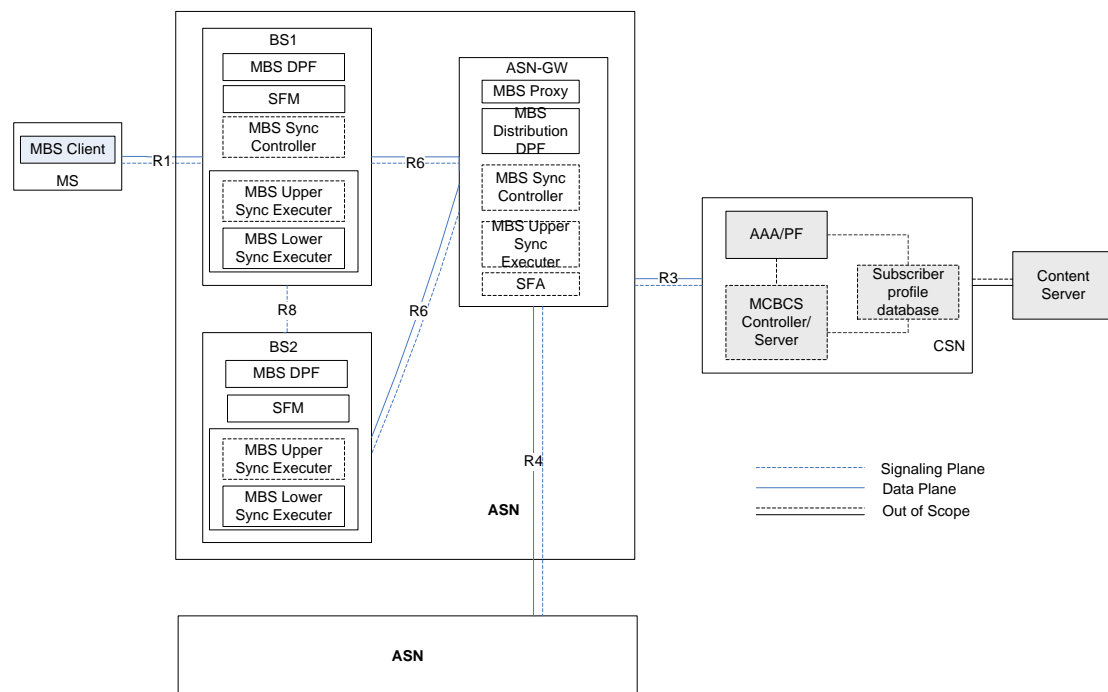


Figure 3-1 : MCBCS Network Reference Model

- MCBCS Content Server:

The MCBCS Content Server provides the content for MCBCS services, like multimedia flows, data files, etc. The content provider can be the NSP or can be a third party such as commercial broadcast network servers/video head, outside the WiMAX network. The interface between the MCBCS Controller/Server function and the Content

Server is out of scope of this specification. There may be one or more MCBCS Content/Servers. The development of the MCBCS Content Server is not within the scope of this specification.

MCBCS Functions in the CSN

- MCBCS Controller/Server:

The MCBCS Controller/Server is an optional network entity that hosts all the MCBCS specific functional components in the CSN. It may perform the following functions:

- IP multicast group management
- MCBCS program management
- MCBCS service announcement management, including MCBCS service guide manipulation and distribution.
- MCBCS MS and network session management
- Data encryption support
- Application layer key management
- Security association below application layer, e.g. SRTP, IPSec

The design of the “optional” MCBCS Controller/Server is based on the assumption that the bearer plane establishment, as well as the service association between the ASN and CSN, is statically configured by default; however, it can also be dynamically established based on some form of event trigger within the ASN associated with the given MCBCS service, and that the given MCBCS service is permanent.

Not all CSN functions for WiMAX MCBCS are specified here in this specification. When applicable, references to other specifications will be provided for corresponding functions.

For the phase-1 implementation, if the MCBCS Controller/Server is supported at the CSN, the dynamic signaling communication between the ASN and CSN over the R3 interface shall be supported. Optionally, the configuration information exchange between the MCBCS Controller/Server and the ASN MBS Proxy/MBS Distribution DPF can also be statically configured.

- AAA/Policy Function (PF)

- This entity is responsible for MCBCS authentications, authorizations, and accounting. It accesses the Subscriber Profile Repository to obtain relevant information. This entity is also responsible for providing the MS access authorization for the access of a particular MCBCS service over the corresponding WiMAX access network.

The AAA and PF are not required to be co-located. The MS WiMAX access authorization is also used to authorize access to the MCBCS services that can be supported by the AAA. The interaction with the PF for MCBCS support is FFS.

- Subscriber Profile Database:

- Stores and manages subscriber profiles.
- The interface between the subscriber profile database, the AAA, and the MCBCS Controller/Server is out of scope of this specification. The subscriber profile database may be the same as the one used for unicast services.

MCBCS Entities and Functions in the NAP

• MBS Proxy:

MBS Proxy is a control plane function for the whole MBS zone, located in the ASN-GW to support MCBCS service. In some cases, for a given MCBCS service, the span of control of the MBS Proxy can be spread across one or more MBS zones. MBS Proxy is collocated with the MBS Distribution DPF. However, for a given MBS zone, there shall be no more than one MBS Proxy. The MBS Proxy may responsible for the following functions:

- Interact with the ASN and CSN MCBCS-functions to support MCBCS network session management. .
- Assign the MCBCS access parameters such as MCID's, MBS Zone ID's, etc. for a given MBS Zone
- MBS service policy enforcement for multicast transport (e.g. QoS, accounting, MCBCS Transmission Zone to MBS Zone mappings, etc.) to enable the MCBCS service over the WiMAX system.
- Interface with the MBS Distribution DPF to trigger MBS DP establishment, maintenance, and release within a MBS zone

• Anchor SFA:

Anchor Service Flow Authorization (SFA) is a logical entity in the ASN, which is located in the ASN-GW/ASN. In addition to the functions that the SFA supports for the existing unicast service flow, when MCBCS service is enabled for a given MS, the following functions are added to the anchor SFA:

- The anchor SFA is responsible for managing the MCBCS service request for a given MS according to its corresponding user's service profile if the user's service profile is downloaded to the anchor SFA.
- Assign service flow ID for a given MCBCS service flow for the MS once the MCBCS service is authorized by the AAA/PF for the MS
- May interact with MBS Proxy to support the MCBCS service flow establishment, modification and release

The SFA may not be collocated with the MBS Distribution DPF.

• MBS Distribution DPF:

The MBS Distribution DPF function is a bearer plane entity in the NAP, which is located at the ASN-GW for the MBS bearer control management and data distribution for one or more MBS Zones. The main functions of the MBS Distribution DPF are:

- MBS bearer control management including the datapath (DP) establishment, maintenance, and release.
- MBS bearer traffic classification and data distribution
- GRE key and sequencing number management and distribution.
- Support the MCBCS accounting agent functions for the MCBCS accounting support
- Forward the MBS packets received over the R3 interface from the MCBCS Controller/Server to the MBS data sync functions in order to support downlink frame level coordination or macro diversity
- Primary MBS Distribution DPF is unique per MBS zone.
 - Act as an IGMP client. Send IGMP report message to the last MR between the ASN and the CSN to join IP multicast group tree.
 - Interact with MBS sync function to support downlink frame offset synchronization for inter MBS Zones and, frame level synchronization or macro diversity for intra MBS Zone
 - To manage more than one zone if synchronization is required between zones
- Serving MBS Distribution DPF:

MCBCS-DSx

- Forward IP multicast packets received from the primary MBS Distribution DPF if unicast transport multicast distribution tree is used
- Potentially act as the Secondary Distribution MBS DPF in a MBS zone to receive data from Primary MBS Distribution DPF and further deliver content in its zone if synchronization between zones is supported.

- MBS DPF

- The MBS DPF includes the collection of MBS bearer control management specific functions of ASN which are located at the BS.

- SFM

SFM is a service flow management logical entity in the ASN and is located at the BS. In addition to the normal functions that the SFA supports for unicast service flow, when MCBCS service is enabled for a given MS, the SFM is responsible for:

- the creation, modification or deletion of service flow for a given IP multicast address and the associated airlink service parameters assignment for an MS using the IEEE 802.16Rev2 based DSx airlink signaling .

- MBS Sync function

The MBS Sync Function is designed to coordinate the MCBCS content downlink transmission over a single frequency or multi-frequency WiMAX networks in one or more MBS zones. The MBS Synchronizing function consists of two sub functions:

MBS Sync Controller Function

- A centralized control entity that is responsible for interacting with the MBS Distribution DPF in order to specify the synchronization rules, including time stamp to support the downlink frame level coordination or macro diversity.
- Delivers the MBS sync rules including time stamp to the MBS Sync Executer.
- An MBS Sync Controller may support more than one MBS Zones, however an MBS zone shall not be served by more than one MBS Sync Controllers.

NOTE: The support of the MBS Sync Controller Function at the ASN-GW/ASN is required and mandatory. However, it is optional to support the MBS Sync Controller Function at a selected BS that is a member of a given MBS Zone.

MBS Sync Executer Function

- MBS Sync Executer is responsible for executing the MBS synchronization rules that are instructed by MBS Sync Controller in support of data synchronization.

It is further divided into two sub functions:

MBS Upper Sync Executer

- MBS Upper Sync Executer is responsible for constructing the MAC PDU and package them into a MAC burst based on the sync rule received from the MBS Sync controller.

MBS Lower Sync Executer

- MBS Lower Sync Executer is responsible for constructing the final PHY burst which is corresponding to the MCID(s) in the given MBS permutation zone that is corresponding to an MBS Zone based on the sync rules that it received from MBS Sync Controller

MCBCS-DSx

- Delivers the mapping information of the MCID's to the corresponding MBS zone ID's, etc.
- Broadcast the MBS_MAP_IE, MBS_MAP and MBS_DATA_IE including the MBS zone ID and MCID.

- MBS Client

The MBS Client represents functionality required by the MS to support the MCBCS service delivery. The MBS client implements the following functions:

- The PHY and MAC layers protocol specification with all the related MBS functionalities shall be compliant with IEEE P802.16-Rev2 [3].
- IP multicast capable IPv4 and IPv6 stack
- Application layer – Application client at the application layer may be responsible among other things for the following functions:
 - Service discovery/announcement
 - Service subscription/registration
 - Application layer security (if required)
 - Optional statistic collection support
 - Reconstruction of the MCBCS program content

The above layers may be tightly coupled implying a requirement for a specific “integrated MBS client”, otherwise for a loosely coupled layers the clients may be simpler. In the latter case, an MBS Application Client at the application layer is assumed to be an off-the-shelf product and its functionality is out of the scope for this specification.

3.2 MCBCS Specific Reference Points

This section describes all the related WiMAX NRM reference points that are related to the MCBCS system solution.

Table 3-1 : MCBCS Reference Point Impact Summary

Reference point	Functions
R1	✓ IEEE 802.16-Rev2 [3] support
R2	✓ Support of Subscription ✓ Service Guide Distribution (optional, see note-1 below) ✓ Key delivery ✓ Support of Notification ✓ Support of Reception Report
R3	✓ MCBCS Session Management ✓ Multicast support ✓ QoS management

MCBCS-DSx

R4/R6	<ul style="list-style-type: none">✓ Datapath control and bearer plane management✓ Multicast support✓ Transfer synch. Information, data
R8	<ul style="list-style-type: none">✓ Transfer synch. Information

- 1
- 2
- 3 **Note:**
- 4 1) The service guide can be downloaded to the user over R2; however, the service guide can also be delivered via
- 5 other means such as SMS, or via other terminal device that can obtain the service guide offline.
- 6

4 MCBCS Normative Procedures

4.1 MCBCS Controller/Server Discovery

MCBCS Controller/Server Discovery is an optional feature to enable dynamic MCBCS Controller/Server assignment to the MS to register with the MCBCS service.

4.1.1 General Procedure

MS can locate the MCBCS Controller/Server via two main mechanisms. One is via the pre-configuration at the MS regarding the addressing information (e.g. IP address or URL) of the MCBCS Controller/Server. An alternative is to have the MS to discover MCBCS Controller/Server dynamically.

In the pre-configuration approach, MCBCS Controller/Server IP address or URL are pre-installed in the MS (e.g. via OTA), the type of configuration method is out of scope of this specification.

For the dynamic MCBCS Controller/Server discovery approach, regardless the MS has been pre-configured with the addressing information of the MCBCS Controller/Server, the MS may decide to locate another possible MCBCS Controller/Server for the current serving ASN via the support of DHCP, SMS, website, etc to obtain MCBCS Controller's /Server's IP address(es) and/or domain name(s).

The following figures describe the dynamic MCBCS Controller/Server Discovery approach via the support of DHCP Proxy and DHCP Relay for both IPv4 and IPv6.

It is mandatory to support the pre-configured information of the MCBCS Controller/Server at the MS; and it is optionally to enable the dynamic MCBCS Controller/Server discovery via the support of DHCP or DNS.

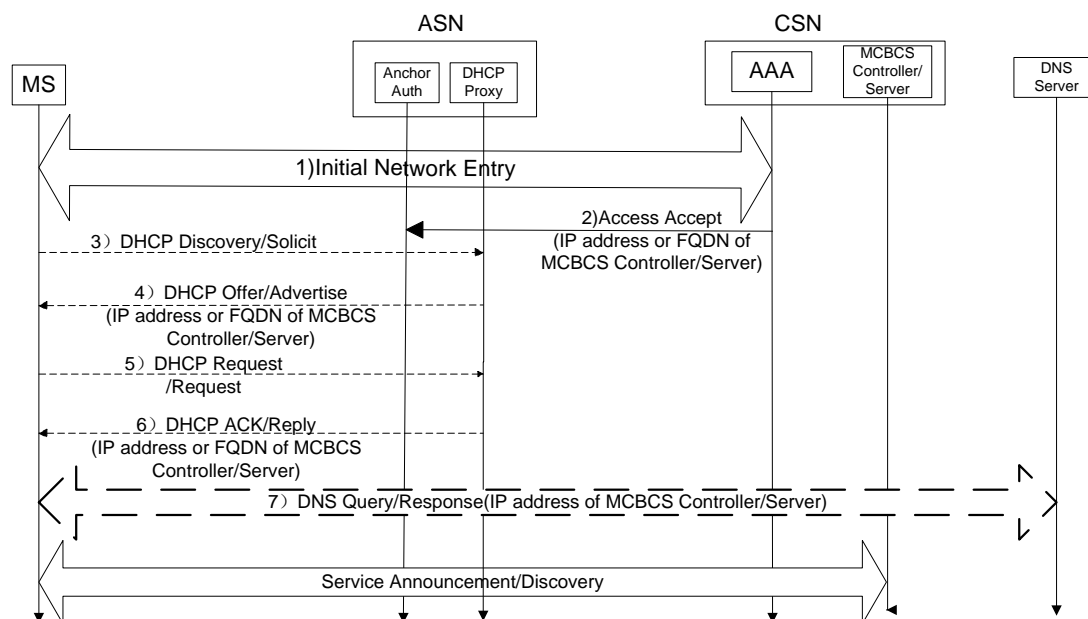


Figure 4-1 : Dynamic MCBCS Controller/Server Discovery via DHCP Proxy

Step 1

MS performs the initial network entry.

Step 2

MCBCS-DSx

AAA returns the IP address(es) or FQDN(s) of MCBCS Controller/Server (s) via Access-Accept message during the initial network entry process. The anchor Authenticator of the MS will then forward the IP addressing information of the assigned MCBCS Controller/Server(s) to the DHCP Proxy at the serving ASN to prepare for the future DHCP inquiry from the MS.

Step 3

MS may send either DHCP Discovery message in the case of IPv4, or SOLICIT message in the case of IPv6 towards DHCP Proxy in ASN to obtain the contact information of MCBCS Controller/Server(s).

Step 4

The DHCP Proxy will then respond to the MS with IPv4/IPv6 address(es) or FQDN(s) of MCBCS Controller/Server(s) in the DHCP OFFER/ADVERTISE message (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6).

Step 5

MS may send either DHCP Request message in the case of IPv4, or REQUEST message in the case of IPv6 towards DHCP Proxy in ASN to confirm the contact information of MCBCS Controller/Server(s).

Step 6

The DHCP Proxy will then respond to the MS with the DHCP-ACK/REPLY message, maybe including IPv4 /IPv6 address(es) or FQDN(s) of MCBCS Controller/Server(s).

Step 7

If the FQDN(s) is returned from DHCP Proxy, the MS may then perform one or more DNS queries (for the FQDN returned in DHCP-Ack/REPLY) to retrieve the IPv4/IPv6 address(es) of the MCBCS Controller/Server (s).

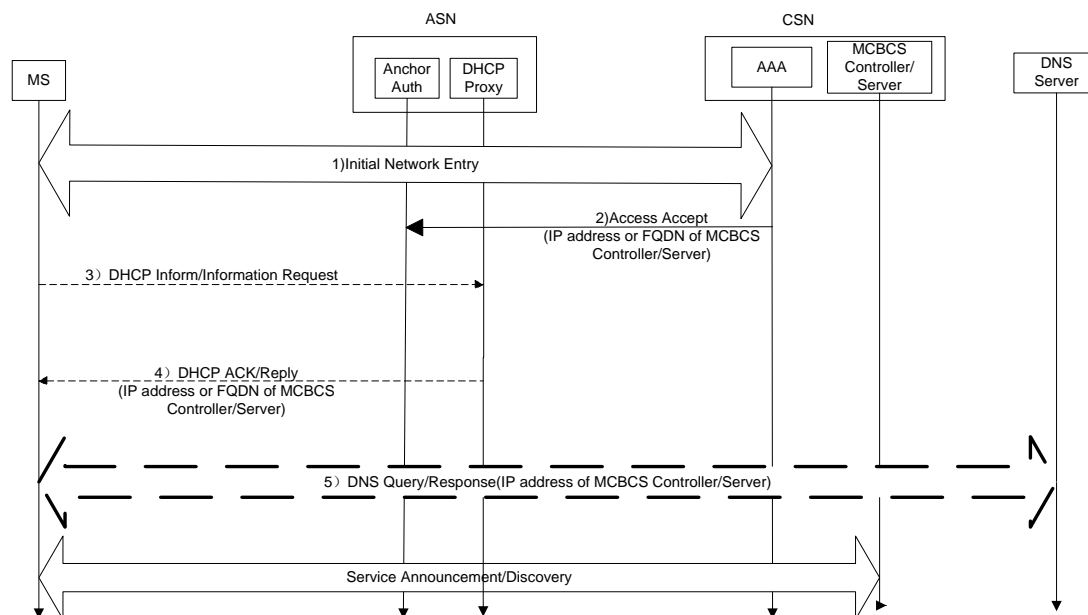


Figure 4-2 : Dynamic MCBCS Controller/Server Discovery via DHCP Proxy with DHCP-Inform/Information-Request

Step 1

MS performs the initial network entry.

Step 2

AAA returns the IP address(es) or FQDN(s) of MCBCS Controller/Server(s) via Access-Accept message during the initial network entry process. The anchor Authenticator of the MS will then forward the contact information of the assigned MCBCS Controller/Server(s) to the DHCP Proxy at the serving ASN to prepare for the future DHCP inquiry from the MS.

Step 3

MS may send either DHCP-Inform message in the case of IPv4, or Information-Request message in the case of IPv6 towards DHCP Proxy in ASN to obtain the contact information of MCBCS Controller/Server.

Step 4

The DHCP Proxy will then responds to the MS with the DHCP-ACK/REPLY message, maybe including IPv4 /IPv6 address(es) or FQDN(s) of MCBCS Controller/Server(s).

Step 5

If the FQDN(s) is returned from DHCP Proxy, the MS may then perform one or more DNS queries (for the FQDN returned in DHCP-Ack/REPLY) to retrieve the IPv4/IPv6 address(es) of the MCBCS Controller/Server (s)

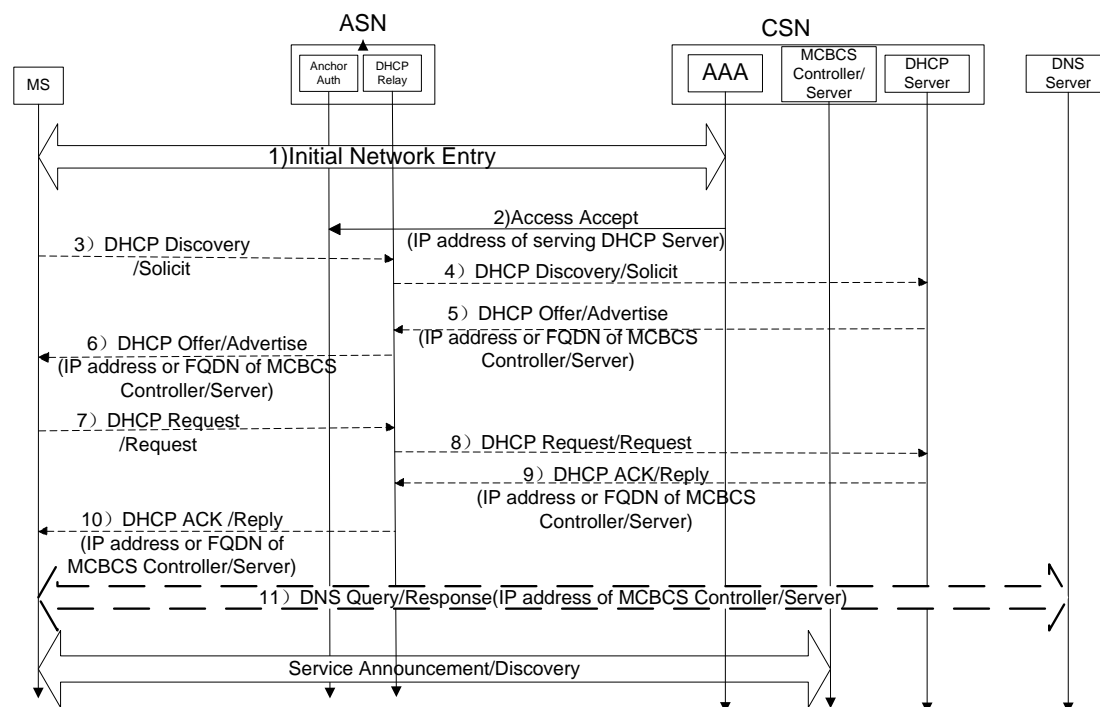


Figure 4-3 : Dynamic MCBCS Controller/Server Discovery via DHCP Relay

Step 1

MS performs the initial network entry procedure.

Step 2

MCBCS-DSx

AAA returns the IP address of Serving DHCP Server via Access-Accept message after the successful initial network entry process. The anchor Authenticator of the MS will then install the DHCP Server address to the DHCP Relay at the serving ASN to prepare for the future DHCP inquiry from the MS.

Step 3-4

MS sends either DHCP-Discovery message in the case of IPv4, or the SOLICIT message in the case of IPv6 towards ASN. The DHCP Relay intercepts the MS's DHCP request and forwards this corresponding DHCP message to the Serving DHCP Server based on the DHCP Server's IP address that was received in Step-1 to inquire about the contact information of MCBCS Controller/Server(s).

Step 5-6

The Serving DHCP Server will respond to the MS via the DHCP Relay with IPv4/IPv6 address(es) or FQDN(s) of the MCBCS Controller/Server(s) in the DHCP OFFER/ADVERTISE message (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6).

Step 7-8

MS sends either DHCP-Request message in the case of IPv4, or the REQUEST message in the case of IPv6 towards ASN. The DHCP Relay intercepts the MS's DHCP request and forwards this corresponding DHCP message to the Serving DHCP Server based on the DHCP Server's IP address that was received in Step-1 to confirm the addressing information of MCBCS controller (s).

Step 9-10

The Serving DHCP Server will respond to the MS via the DHCP Relay with DHCP-ACK/REPLY message, maybe including IPv4/IPv6 address(es) or FQDN(s) of the MCBCS Controller/Server(s).

Step 11

If the FQDN(s) are received from DHCP Server, the MS performs one or more DNS queries (for the FQDN returned in DHCP-Ack/REPLY) to retrieve the IPv4/IPv6 address(es) of the MCBCS Controller/Server(s).

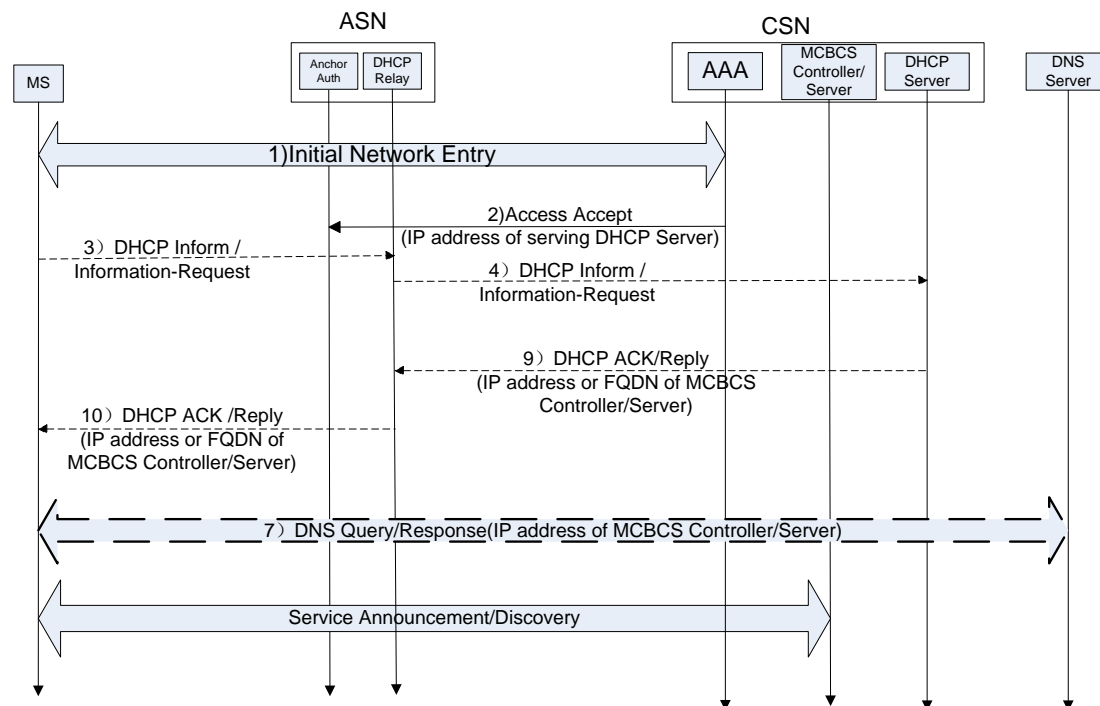


Figure 4-4 : Dynamic MCBCS Controller/Server Discovery via DHCP Relay with DHCP-Inform/Information

Step 1

MS performs the initial network entry procedure.

Step 2

AAA returns the IP address of Serving DHCP Server via Access Accept message after the successful initial network entry process. The anchor Authenticator of the MS will then install the DHCP Server address to the DHCP Relay at the serving ASN to prepare for the future DHCP inquiry from the MS.

Step 3-4

MS sends either DHCP Inform message in the case of IPv4, or the Information-Request message in the case of IPv6 towards ASN. The DHCP Relay intercepts the MS's DHCP request and forwards this corresponding DHCP message to the Serving DHCP Server based on the DHCP Server's IP address that was received in Step-2 to inquire about the addressing information of MCBCS Controller/Server(s). (MS will use the same Options as explained for DHCP Proxy Case for obtaining IPv4 /IPv6 address(es) or FQDN(s) of MCBCS Controller/Server(s))

Step5-6

The Serving DHCP Server will respond to the MS via the DHCP Relay with DHCP ACK/REPLY message, maybe including IPv4/IPv6 address(es) or FQDN(s) of the MCBCS Controller/Server(s).

Step-7

If the FQDN(s) are received from DHCP Server, the MS performs one or more DNS queries (for the FQDN returned in DHCP Ack/REPLY) to retrieve the IPv4/IPv6 address(es) of the MCBCS Controller/Server(s).

4.1.2 Co-existence of Service Pre-configuration and Dynamic Discovery of the MCBCS Controller/Server to Support NAP sharing

Within the same ASN, if the NAP is shared between different NSPs, different MCBCS Controller/Server discovery mechanisms can be supported. Dynamic MCBCS Controller/Server discovery method can co-exist with other configuration schemes such as OTA, for configuring MCBCS Controller/Server information locally in the MS.

Regardless the MS obtain the MCBCS Controller/Server IP address(es) via either pre-configuration or dynamic discovery, the same MCBCS information acquisition procedure applies for the MS to inquire MCBCS programming information from the MCBCS Controller/Server.

4.1.3 AAA server procedure

During the MS initial network entry phase, upon receiving Access Request message which may include the IP address or FQDN of the local MCBCS Controller/Server that can serve the MS for the MCBCS service, and if the MS is successfully authenticated, AAA server SHALL respond to the Anchor Authenticator with Access Accept which may include IP address or FQDN of MCBCS Controller/Server in the case when the DHCP Proxy is enabled for the MS, or may include IP address of Serving DHCP Server in the case when the DHCP Relay is enabled for the MS; . Otherwise, if the MS is failed to be authenticated, AAA server SHALL respond with Access Reject with no information relating to the MCBCS Controller/Server.

4.1.4 Anchor Authenticator procedure

Upon receiving Access Accept, if the IP address or FQDN of the local MCBCS Controller/Server is present, Anchor Authenticator SHALL pass on this IP address or FQDN to the appropriate DHCP Proxy or pass on the DHCP

MCBCS-DSx

server address to the appropriate DHCP relay at the serving ASN to prepare for the future DHCP inquiry from the MS.

4.1.5 DHCP Server procedure

If a DHCP Discovery message or a Solicit message is received from the MS in the case of IPv4 or IPv6, respectively, via the DHCP relay, the DHCP Server may respond to the MS with the appropriate IP address (Option 89 in case of DHCPv4 and Option 34 in case of DHCPv6) or FQDN of MCBCS Controller/Server (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6) in the DHCP Offer for IPv4 or the DHCP Advertise message for IPv6.

If a DHCP Request message, is received from the MS in the case of IPv4 or IPv6 via the DHCP Relay, the DHCP Server SHALL confirm this IP address (Option 89 in case of DHCPv4 and Option 34 in case of DHCPv6) or FQDN of MCBCS Controller/Server (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6) and respond to the MS with the DHCP ACK or the DHCP Reply message to include the IPv4 or the IPv6 address of MCBCS Controller/Server respectively; or alternatively, to include the FQDN of the MCBCS Controller/Server. .

If a DHCP inform message, or a DHCP Information message is received from the MS in the case of IPv4 or IPv6, respectively, via the DHCP Relay, the DHCP Server should respond to the MS with IP address (Option 89 in case of DHCPv4 and Option 34 in case of DHCPv6) or FQDN of MCBCS Controller/Server (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6) in the DHCP ACK or the DHCP Reply message.

4.1.6 DHCP Relay Procedure

No change to standard DHCP Relay behavior.

4.1.7 DHCP Proxy Procedure

Upon receiving the IP address or FQDN of the assigned MCBCS Controller/Server from Anchor Authenticator, DHCP Proxy should then maintain this information for the corresponding MS to prepare for the future DHCP inquiry from the MS.

If a DHCP Discovery message, or a Solicit message is received from the MS in the case of IPv4 or IPv6, respectively, the DHCP Proxy SHALL respond to the MS with IP address (Option 89 in case of DHCPv4 and Option 34 in case of DHCPv6) or FQDN of MCBCS Controller/Server (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6) in the DHCP Offer for IPv4 or the DHCP Advertise message for IPv6.

If a DHCP Request message is received from the MS in the case of IPv4 or IPv6, the DHCP Proxy SHALL confirm this IP address or FQDN of MCBCS Controller and respond to the MS with the DHCP ACK or the DHCP Reply message to include the IPv4 or the IPv6 address of MCBCS Controller/Server, respectively; or alternately, to include the FQDN of the MCBCS Controller/Server.

If a DHCP inform message, or Information message is received from the MS in the case of IPv4 or IPv6, respectively, the DHCP proxy may respond to the MS with IP address (Option 89 in case of DHCPv4 and Option 34 in case of DHCPv6) or FQDN of MCBCS Controller/Server (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6) in the DHCP ACK or the DHCP Reply message, respectively.

4.1.8 MS Procedures

MS may send either DHCP Discovery message, or Solicit message to the DHCP Proxy or the DHCP Relay to ASN, in the case of IPv4 or IPv6, respectively, to obtain the IP address (Option 89 in case of DHCPv4 and Option 34 in case of DHCPv6) or FQDN of MCBCS Controller/Server (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6).

Upon receiving DHCP Offer or the DHCP Advertise message from the DHCP Proxy or the DHCP Relay, which may include the IP address (Option 89 in case of DHCPv4 and Option 34 in case of DHCPv6) or FQDN of MCBCS

MCBCS-DSx

Controller/Server (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6), the MS should send the DHCP Request message, or the DHCP Request message to the DHCP Proxy or the DHCP Relay in ASN, in the case of IPv4 or IPv6, respectively, to confirm this IP address (Option 89 in case of DHCPv4 and Option 34 in case of DHCPv6) or FQDN of MCBCS Controller/Server (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6).

Alternatively, MS may send either DHCP Inform message, or the Information message to the DHCP Proxy or the DHCP Relay in ASN, in the case of IPv4 or IPv6, respectively, to obtain the IP address (Option 89 in case of DHCPv4 and Option 34 in case of DHCPv6) or FQDN of MCBCS Controller/Server (Option 88 in case of DHCPv4 and Option 33 in case of DHCPv6).

Upon receiving the DHCP ACK or the DHCP Reply message from the DHCP Proxy or the DHCP Relay, the MS may perform one or more DNS queries to retrieve the IPv4 or the IPv6 address of MCBCS Controller/Server if the FQDN is returned.

4.1.9 DHCP option

For DHCPv4, the MS MAY request either or both of the MCBCS Controller/Server Domain Name List and the IPv4 Address options in the Parameter Request List option (code 55) as defined in RFC2132.

For DHCPv6, the MS MAY request either or both of the MCBCS Controller/Server Domain Name List and the IPv6 Address options in the Options Request Option (ORO) as described in RFC3315.

If the MS receives both the MCBCS Controller/Server Domain Name List and IPv6 or IPv4 Address options, it SHOULD use the Domain Name List option. In this case, the MS SHOULD NOT use the MCBCS Controller/Server IPv6 or IPv4 Address option unless the server in the MCBCS Controller/Server Domain Name List cannot be resolved or reached.

For more details of the DHCP options as specified in this section SHALL be referred to RFC 4280. Any reference of “BCMCS” in RFC 4280 is to be substituted by “MCBCS” as they are referring to the same concept.

4.1.10 Error Handling

If the MCBCS Controller/Server discovery procedure encounters any unresolvable/non-recoverable errors, both network and MS will terminate the procedure with appropriate error handling. The details of the error handling implementation are beyond the scope of this specification.

4.1.10.1 No information of MCBCS Controller/Server in the Access Accept message

If no information of MCBCS Controller/Server is returned in the Access Accept message after the MS has been successfully authenticated, the MS SHALL either use a pre-configured information, if available, or otherwise assume that MCBCS services are not available.

4.1.10.2 Timers consideration for DHCP Proxy in the ASN and DHCP Relay

All the timers shall be set and cleared according to RFC 2131 (DHCP), RFC 3315 (DHCPv6) specifications.

4.1.10.3 Handling Error Condition

Error handling as specified in RFC 2131 (DHCP), RFC 3315 (DHCPv6) specifications shall be supported..

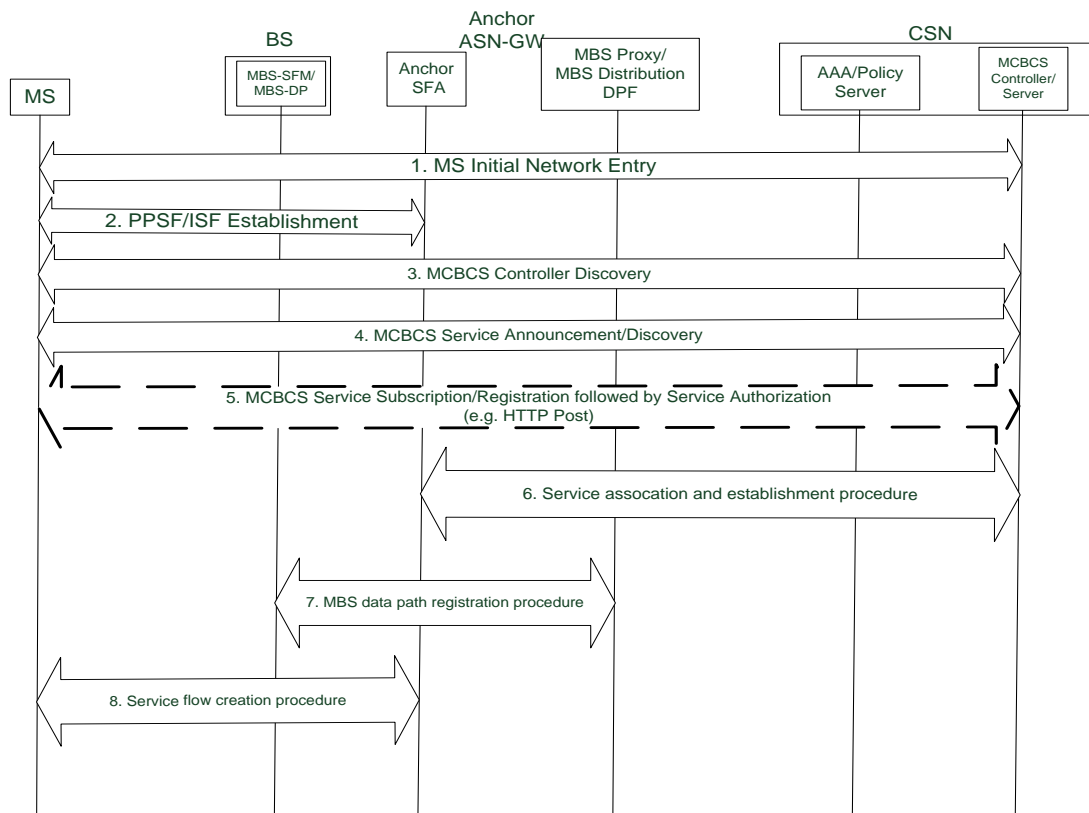
4.1.11 RADIUS Related Messages and Attributes

The additional Radius attributes exchanged between the ASN NAS and the AAA to support the dynamic MCBCS Controller/Server discovery are described in section 5.3.1.1.

4.2 End-to-end MCBCS Service Establishment

This section describes the network perspective system initialization and establishment for enabling the MCBCS broadcast and static multicast service and depicts two examples of service initialization and establishment scenarios.

The Figure 4-5 is to describe the system behaviors when some of network events, e.g. the very first initial network entry of the MS, who is entitled for receiving the given MCBCS service, is used to trigger the network initialization and establishment of the MCBCS service over the WiMAX network. Likewise, the very last network exit of the MS, who is entitled for receiving the given MCBCS service, may be used to trigger the network termination of the MCBCS service over the WiMAX.



Note: MBS Proxy and MBS Distribution DPF are always collocated within the same ASN-GW

Figure 4-5 : MCBCS Service Initialization Establishment scenario triggered by the first MS entering the network

Step-1

MS performs an initial network entry.

Step-2

PPSF/ISF is established according the NWG R1.0 specification.

Step-3

MCBCS-DSx

MS performs a MCBCS controller discovery. If the MS has a local configuration regarding the addressing information (e.g. IP address or URL) of the MCBCS Controller/Server, this step is not performed.

Step-4

MS gets the MCBCS service information through MCBCS Service announcement. Refer to the section 4.4.1 for a detailed description. If the MS already gets the service information through other means, this step is not performed.

Step-5

MS subscribed to the MCBCS program with the serving NSP. If MS has the existing service registration and also the subscription with the serving NSP prior to the MS attachment to the WiMAX access network, this step is not performed

Step-6

ASN performs the service initialization and establishment with the corresponding MCBCS Controller(s)/Server(s) and bearer infrastructure to support the upcoming MBS data. Refer the section 4.3 for the detailed description.

Step-7

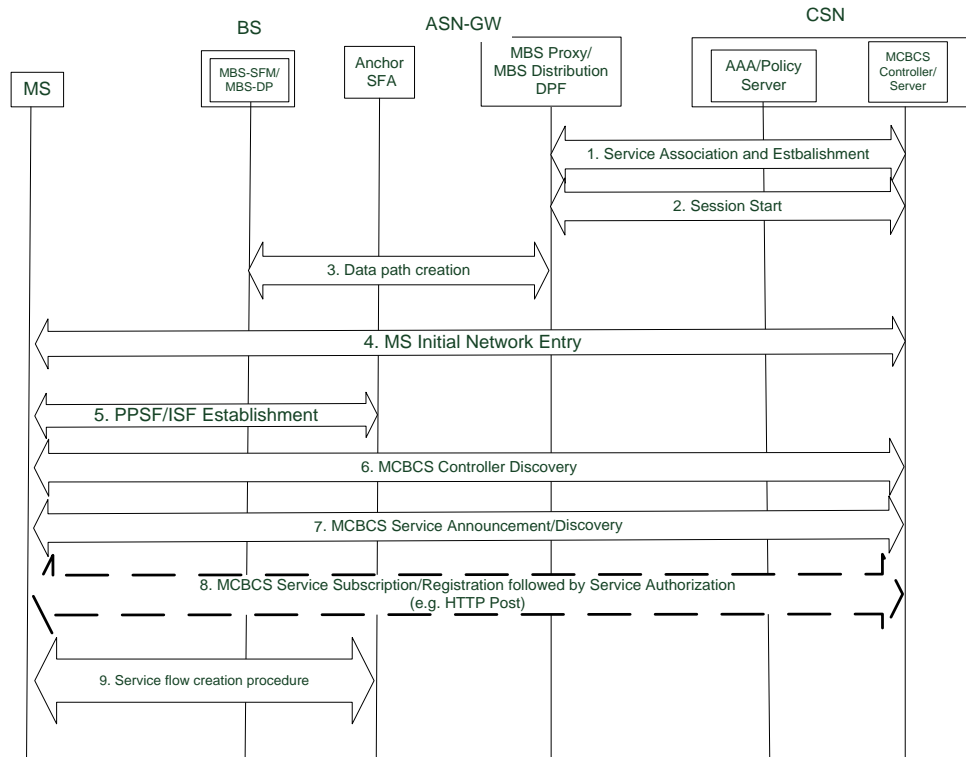
The MBS Proxy will trigger the corresponding MBS distribution DPF to establish the multicast data path. MBS Distribution DPF establishes the multicast data path to all BSs in the same MBS zone or MCBCS Transmission Zone. Refer to the section 4.5 for the detailed description.

Step-8

Anchor SFA initiates a service flow creation procedure. Refer the Section 4.4 service provisioning section for the detailed description.

Once the association between MBS Proxy and MCBCS Controller/Server and multicast distribution tree are established, all subsequent INEs for the MSs with the pre-provisioned MCBCS service will not trigger any MBS Proxy service association with the MCBCS Controller/Server, nor MBS multicast distribution tree establishment. In other words, all subsequent INEs for the MSs do not have Step 6) and 7).

The following section describes another example for MCBCS service scenario based on service initialization with the session start. The Session Start may occur independent to the existence of MS.



Note: MBS Proxy and MBS Distribution DPF are always collocated within the same ASN-GW

Figure 4-6 : MCBCS Service Initialization Establishment scenario triggered by the Session Start

Step-1

ASN performs the service initialization with the corresponding MCBCS Controller(s)/Server(s) and bearer infrastructure to support the upcoming MBS data.

Step-2

MCBCS controller starts an MCBCS service session by sending a session start message. Refer to section 4.4.2.1 for more details.

Step-3

The MBS Proxy will trigger the corresponding MBS distribution DPF to establish the multicast data path. MBS Distribution DPF establishes the multicast data path to all BSs in the same MBS zone or MCBCS Transmission Zone. Refer to the section 4.5 for the detailed description.

Step-4

MS performs an initial network entry.

Step-5

PPSF/ISF is established according the NWG R1.0 specification.

Step-6

MS performs a MCBCS controller discovery. If the MS has a local configuration regarding the addressing information (e.g. IP address or URL) of the MCBCS Controller/Server, this step is not performed. For a detailed description, refer the section 4.1.

Step-7

MCBCS-DSx

MS gets the MCBCS service information through MCBCS Service announcement. Refer the section 4.4.1.1 for a detailed description.

Step-8

MS subscribed to the MCBCS program with the serving NSP. If MS has the existing service registration and also the subscription with the serving NSP prior to the MS attachment to the WiMAX access network, this step is not performed.

Step-9

Anchor SFA initiates a service flow creation procedure. Refer the Section 4.4 service provisioning section for the detailed description.

4.3 MCBCS Service initialization Procedure between MBS Proxy and MCBCS Controller/Server

The one approach for the MCBCS System initialization and establishment for broadcast and static multicast services between the MBS Proxy and the MCBCS Controller/Server is to statically configure the service association between the functional entities at the ASN (e.g. MBS Proxy, MBS Distribution DPF etc.) and at the CSN (e.g. MCBCS Controller/Server), see section 4.3.1 for more details.

Another approach is to allow the ASN and CSN to dynamically establish the service association and connectivity based on some form of event triggers and the network policy that are previously agreed between the ASN and CSN, see section 4.3.2 for more details.

One form of the event trigger is based on the very first MS's network entry which is entitled for the given MCBCS service at the serving ASN. In the case of this kind of event trigger, the control flow sequences are different dependent on the two following service configuration scenarios for the given MCBCS service:

- MCBCS service is a "pre-provisioned" MCBCS service – i.e. pre-configured the given MCBCS service prior to the MS attachment to the WiMAX network
- MCBCS service is based on the "dynamic subscription" – i.e. via the on-line subscription to the given MCBCS service after the MS attachment to the WiMAX network

4.3.1 MCBCS Service Initialization with Static Configuration

The association between MBS Proxy and the MCBCS Controller/Server can be statically pre-configured. It is mandatory to support the pre-configuration for these two entities; however, the configuration management design is out of scope of this specification.

4.3.2 MCBCS Service initialization after the First MS Network Entry

In term of the network event trigger, one approach is to have the MCBCS Service Initialization to be triggered by during the network entry of the first MS whose service profile indicates the MS's entitlement for receiving one or more MCBCS services from one or more MCBCS controller(s), however, the current ASN has not established the service association with the corresponding MCBCS Controller(s)/Server(s) as well as the MBS data path to support the upcoming MBS programming.

The MCBCS service initialization and service association triggered by the first MS network entry can apply to two different service configuration scenarios:.

- MCBCS service is a pre-provisioned MCBCS service
- MCBCS service is based on the dynamic subscription.

MCBCS-DSx

1 The pre-provisioned MCBCS service implies that the given MCBCS service has been assigned to the MS (e.g. via
2 offline subscription or free subscription) by the serving NSP prior to the MS attachment to the WiMAX access
3 network.

4 The dynamic subscribed MCBCS service implies the given MCBCS service is assigned to the MS (e.g. via on-line
5 subscription) by the serving NSP after the MS has attached to the WiMAX access network.

6 For Pre-Provisioned MCBCS service, once the MS is authenticated and authorized by the serving NSP the anchor
7 authenticator will receive the MS's service profile. The MS's service profile should include the contact information
8 (e.g. IP address or FQDN) related to pre-assigned MCBCS controller that the serving NSP authorizes for the MS to
9 receive the MCBCS services over the anchor authenticator.

10 The MS's service profile for the given MCBCS service may include the associated MCBCS Controller(s) contact
11 information (i.e. IP address(es) or FQDN(s)), the required QoS parameters, IP multicast address, MBS programming
12 channel as well as the charging and accounting policy etc..

13 More details on the service association establishment for pre-provisioned MCBCS service are described in section
14 4.3.2.1.

15 For the dynamic MCBCS service, according to the definition, the MS initiates the MCBCS service subscription with
16 the MCBCS controller/server after the MS has already attached to the serving ASN.

17 Once the MS initiates the service subscription for a given MCBCS service with a given MCBCS controller/server,
18 the MCBCS controller/server will then communicate with the corresponding home AAA server of the MS based on
19 the MS MCBCS service registration information to validate the MS's access authorization with the given ASN. The
20 home AAA Server will then push down the MS's service policy that is corresponding to the MS's registered
21 MCBCS service to the anchor ASN. In such case, the MS's service profile will include the associated MCBCS
22 Controller(s)/Server(s) contact information, required QoS parameters, IP multicast address, MBS programming
23 channel as well as the charging and accounting policy etc. related to the given MCBCS service for the MS.

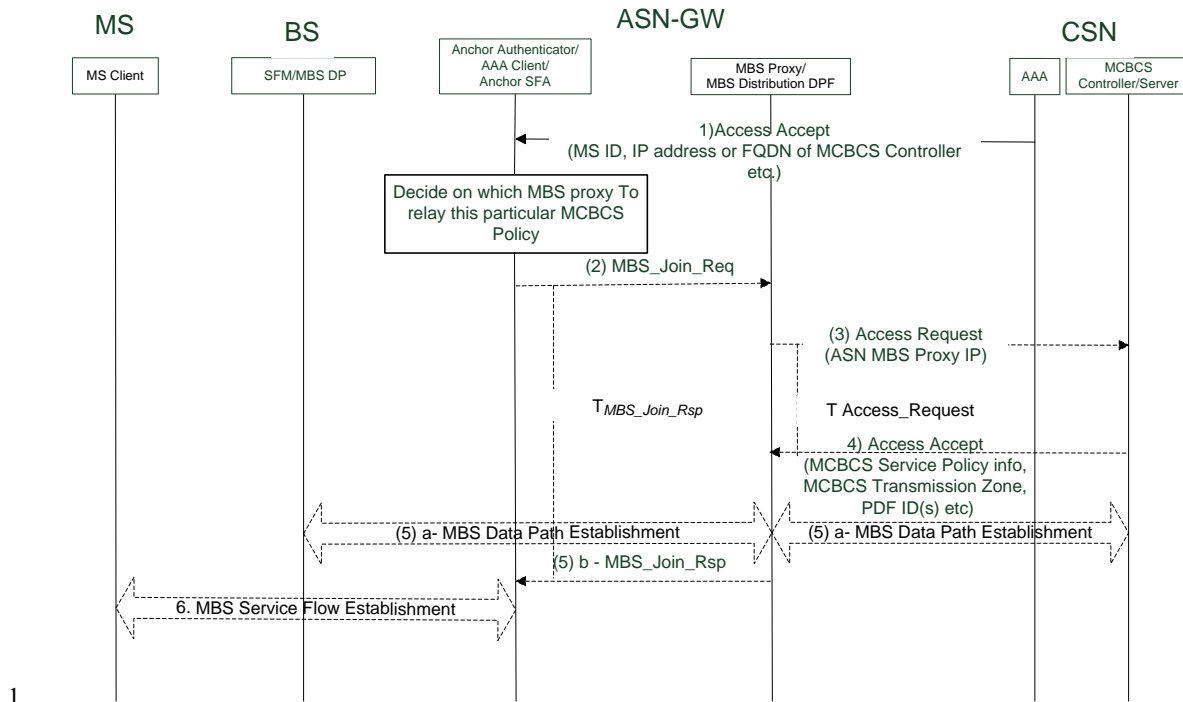
24 The anchor authenticator will then leverage the MCBCS information obtained from the MS's service profile
25 provided by the home AAA server to identify the serving MCBCS Controller(s)/Server(s) of the MS. If the required
26 MCBCS service association has not been established between the MBS Proxy and the corresponding MCBCS
27 Controller/Server, once the anchor authenticator receives the MS's service profile from the AAA server, the anchor
28 SFA of the MS will consult with the responsible MBS Proxy at the anchor ASN who will then trigger the peer-to-
29 peer service association establishment between the MBS Proxy and the corresponding MCBCS Controller/Server.
30 The method of how the anchor SFA of the MS to determine of which the MBS Proxy is responsible for the
31 corresponding MCBCS Controller/Server is a local implementation design decision and is outside the scope of this
32 specification.

33 More detail on Dynamic MCBCS Service trigger for MCBCS Service initialization is described in the section
34 4.3.2.2.

35 Once the peer-to-peer association between a MBS Proxy and a given MCBCS Controller/Server is established, any
36 subsequent MS network entry or service subscription for the same MCBCS service will not trigger the service
37 initialization procedure.

40 **4.3.2.1 MCBCS Service Initialization for Pre-provisioned Service Triggered by the very first MS's Initial** 41 **Network Entry**

42 The following figure describes the scenario of how the very first MS's initial network entry could trigger the Pre-
43 Provisioned MCBCS service initialization procedures.



1
2 Note: MBS Proxy and MBS Distribution DPF are always collocated within the same ASN-GW

3 **Figure 4-7: Pre-Provisioned MCBCS network initialization procedures with the very first MS INE to**
4 **trigger**

5 **Step-1**

6 AAA server pushes down MCBCS Controller/Server information, (i.e. IP address or FQDN of MCBCS Controller
7 as well the MCBCS Service Association Security Parameter Index (SPI)) and MCBCS service profile in Access
8 Accept message towards Authenticator in ASN-GW after the successful MS Initial Network Entry process. The
9 MCBCS service profile contains the MCBCS program (i.e. MCBCS Transmission Zone ID, MCBCS Program ID)
10 and the MCBCS service parameter information (i.e. Packet Flow Descriptor and QoS Descriptor)

11 **Step-2**

12 Upon receiving those parameters, the Authenticator will then pass on all the MCBCS related information provided
13 by AAA server to anchor SFA to process. The anchor SFA recognizes there is a pre-provisioned MCBCS service for
14 the MS from the service profile, based on the pre-configured mapping of the MCBCS Transmission Zone to the
15 local MBS Zone, the anchor SFA identifies the appropriate MBS Proxy that is responsible for the given MBS Zone
16 which is responsible for communicating with the corresponding MCBCS Controller/Server as specified in the
17 MCBCS Controller/Server information.

18 The anchor SFA will send *MBS_Join_Req* message that includes the target MCBCS Controller/Server information
19 as well as the MCBCS service profile information to the corresponding MBS Proxy. The anchor SFA will consult
20 with the MBS Proxy to determine the type of the MCBCS airlink transport (i.e. unicast service flow or multicast
21 service flow) to be established for the MS to receive the MCBCS service. The anchor SFA will set the timer
22 $T_{MBS_Join_Rsp}$ to wait for the *MBS_Join_Rsp* from the MBS Proxy.

23 **Step-3**

24 When the MBS Proxy receives the *MBS_Join_Req* message from the anchor SFA, if there is no existing service
25 association between the MBS Proxy with the corresponding MCBCS Controller/Server, the MBS Proxy will then
26 refer to the given MCBCS service association SPI and the MCBCS Transmission Zone ID from the pre-configured
27 MCBCS security association table to extract the shared security key prior to sending the *Access Request* message to
28 the target MCBCS Controller to trigger the MCBCS service association between them for a given MCBCS program.

MCBCS-DSx

1 MBS Proxy sets the timer $T_{Access_Request}$ to wait for the service association response from the target MCBCS
2 Controller/Server.

3 **Step-4**

4 Once the MCBCS service association is established between the MBS Proxy and the MCBCS Controller/Server, the
5 MCBCS Controller/Server may push down all the MCBCS service profiles that are corresponding to each MCBCS
6 service (e.g. MCBCS Program Descriptor, Packet-Flow Descriptor, Qos Descriptor) in the *Access Accept* message to
7 the MBS Proxy who will then cancel the timer $T_{Access_Request}$

8 **Step-5 a, b**

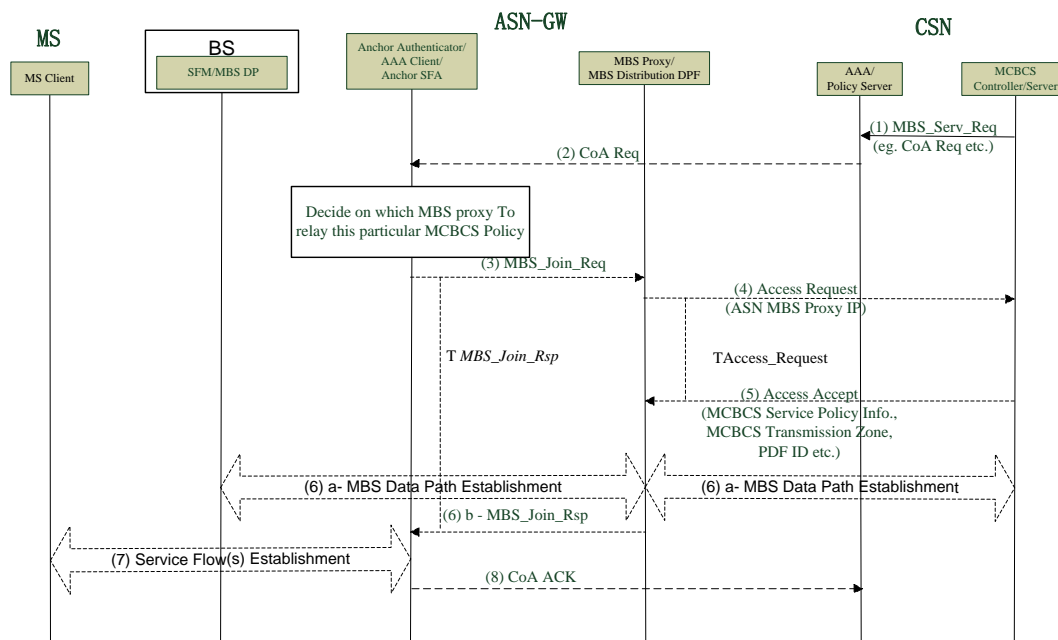
9 MBS Proxy triggers the MBS Distribution DPF to join the CSN Multicast Distribution Tree; in addition, MBS
10 Proxy initiates MBS data path establishment to all BSs which are belonged to the same MBS Zone or same MCBCS
11 Transmission Zone. Once the MBS data path establishment is completed, the MBS Proxy sends the *MBS Join_Rsp*
12 message to the Anchor SFA with the information of the MBS service flow type (i.e. unicast or multicast service flow)
13 and the corresponding SF Info (e.g. MCID(s)) and optionally, the revised MCBCS service profile to trigger the
14 service flow establishment for the given MCBCS service towards the target MS. The Anchor SFA will then cancel
15 the timer $T_{MBS_Join_Rsp}$.

16 **Step-6**

17 The Anchor SFA initiates the service flow for the given MCBCS service establishment RR_Req towards the target
18 MS according to the MBS service flow type that was instructed by the MBS Proxy as described in Step-5.

20 4.3.2.2 MCBCS Service Initialization Triggered by the first Dynamic MCBCS Service Subscription after 21 MS Attachment to the network

22 The following figure describes the scenario of how the first dynamic MS service subscription or registration with
23 MCBCS Controller/Server could trigger the MCBCS service initialization procedures.



24
25 *Note: MBS Proxy and MBS Distribution DPF are always collocated within the same ASN-GW*

26 **Figure 4-8 : dynamic MS service subscription or registration to trigger the MCBCS network**
27 **initialization procedures**

MCBCS-DSx

The service initialization procedure in Figure 4-8 is triggered by the first dynamic service subscription for a MCBCS program with the NSP after the MS attachments to the network.

Step1-2

After the MS signs up with the MCBCS Controller/Server for a given MCBCS service, the MCBCS controller/Server will initiate request to the AAA server of the MS to validate the access privilege to this given MCBCS service for the MS over the serving ASN. If authorized, the AAA server will push down MCBCS Controller/Server information (i.e. IP address or FQDN of MCBCS Controller as well as the MCBCS Server association Security Parameters Index (SPI)) and MCBCS Server Profile in CoA Request message towards Anchor Authenticator in ASN-GW. The MCBCS service profile contains the MCBCS program (i.e. MCBCS Transmission Zone ID, MCBCS Program ID) and the MCBCS service parameter information (i.e. Packet Flow Descriptor and QoS Descriptor)

The anchor Authenticator will then pass on all the MCBCS related information provided by AAA server to the anchor SFA of the MS to process.

Note: The interface between the MCBCS Controller/Server and the AAA server is outside the scope of the phase-1 MCBCS.

Step-3

The anchor SFA recognizes there is a MCBCS service for the MS from the service profile, based on the pre-configured mapping of the MCBCS Transmission Zone to the local MBS Zone, the anchor SFA identifies the appropriate MBS Proxy that is responsible for the given MBS Zone which is responsible for communicating with the corresponding MCBCS Controller/Server as specified in the MCBCS Controller/Server information.

The anchor SFA will send *MBS_Join_Req* message that includes the target MCBCS Controller/Server information to the corresponding MBS Proxy as well as the MCBCS service profile information. The anchor SFA also consults with the MBS Proxy to determine the type of the MCBCS airlink transport (i.e. unicast service flow or multicast service flow) to be established for the MS to receive the MCBCS service. The anchor SFA will set the timer T_{MBS_Join_Rsp} to wait for the MBS_Join_Rsp from the MBS Proxy.

NOTE: The unicast service flow support is deferred to the future release.

Step-4

When the MBS Proxy receives the *MBS_Join_Req* message from the anchor SFA, if there is no existing association between the MBS Proxy with the corresponding MCBCS Controller/Server, the MBS Proxy will then refer to the given MCBCS service association SPI and MCBCS Transmission Zone ID from the pre-configured MCBCS security association table to extract the shared key prior to sending the *Access_Request* message to the target MCBCS Controller to trigger the MCBCS service association between them for a given MCBCS Program. The MBS Proxy sets the timer T_{Access_Request} to wait for the service association response from the target MCBCS Controller/Server.

Step-5

Once the MCBCS service association is established between the MBS Proxy and the MCBCS Controller/Server, the MCBCS Controller/Server may push down all the MCBCS service profiles that are corresponding to each MCBCS service (e.g. MCBCS Program Descriptor, Packet-Flow Descriptor, Qos Descriptor) in the *Access_Accept* message to the MBS Proxy who will then stops the timer T_{Access_Request}.

Step-6 a, b

The MBS Proxy triggers the MBS Distribution DPF to join the CSN Multicast Distribution Tree; in addition, the MBS Proxy initiates the MBS data path establishment towards the BSs which are belonged to the same MBS Zone

MCBCS-DSx

or MCBCS Transmission Zone. Once the MBS data path is established, the MBS Proxy sends the *MBS_Join_Rsp* message to the Anchor SFA with the information of the MBS service flow type (i.e. unicast or multicast) and the corresponding SF Info (e.g. MCID(s)) and optionally, the revised MCBCS service profile to trigger the service flow establishment for the given MCBCS service towards the target MS. The Anchor SFA will then cancel the timer T

NOTE: The unicast service flow support is deferred to the future release.

Step-7

After the successful bearer infrastructure establishment, the anchor SFA will then initiate the service flow for the given MCBCS service establishment request towards the target MS according to the MBS service flow type and the corresponding SF Info.

Step-8

After successful service flow establishment, the Anchor Authenticator of the MS will then send CoA ACK message back to the AAA server; otherwise, CoA NAK should be sent to the AAA server in CSN.

4.3.3 MCBCS Security Association Establishment between MBS Proxy and MCBCS Controller/Server

The communication between the MBS Proxy and MCBCS Controller/Server is protected by a pre-configured shared security key. The same SPI between the given MBS Proxy and the given MCBCS Controller is shared by all MSs who receive the same MCBCS service. The method of the pre-configuration is outside the scope of this specification.

After the successful MS network entry or the dynamic service subscription, the MCBCS service association SPI will be returned to the Anchor Authenticator of the MS who will then pass onto the anchor SFA. Once the anchor SFA identifies the target MBS Proxy, the anchor SFA will then forward the SPI to the target MBS Proxy. The target MBS Proxy will then refer to the pre-configured MCBCS security association table which is indexed by the MCBCS service association SPI and the MCBCS Controller information (e.g. IP address and/or FQDN) to obtain the pre-configured shared security key to support the secured service association establishment.

4.3.4 Error Handle Procedures

4.3.4.1 Timer MAX Retries

This Timer, $T_{MBS_Join_Rsp}$, is started by ASN associated with the Anchor SFA after transmission of *MBS_Join_Req* message to the MCBCS Proxy and stopped upon reception of *MBS_Join_Rsp* message.

This Timer, $T_{Access_Request}$, is started by ASN associated with the MCBCS Proxy after transmission of *Access Request* message to the MCBCS Controller and stopped upon reception of *Access Accept* message.

Table 4-1: Max Retries Timer Values

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
$T_{MBS_Join_Rsp}$	TBD		TBD
$T_{Access_Request}$	TBD		TBD

4.3.4.2 Timer Expiry

Table 4-2 shows the details of the corresponding action(s) associated with timer expiry. Upon each timer expiry, if maximum retries has not exceeded, the related message is retransmitted and timer is restarted. Otherwise corresponding action(s) should be performed as indicated in Table 4-2.

Table 4-2 : Actions after Timer Max Retry

Timer	Entity where Timer Started	Action(s)
$T_{MBS_Join_Rsp}$	Anchor SFA at the anchor ASN-GW.	Establish the unicast service flow – by default.
$T_{Access_Request}$	MBS Proxy at the ASN-GW	The MBS proxy reports failure and no MCBCS service will be enabled within the MCBCS Transmission Zone.

4.3.5 Message Primitive

Table 4-3 : MBS_Join_Req message

IE	Description	M/O	Notes
SF Info (one or more)		O	Service flow description
>SFID		O	Service flow Identifier
>MBS Zone ID	5.2.9	O	The identifier of MBS Zone.
>MCBCS Transmission Zone ID	5.2.6	O	The identifier of MCBCS Transmission Zone.
>PDFID		O	The PDFID is used together with the MCBCS Transmission Zone ID to unique identify the given MCBCS service flow for a given MCBCS service
>QoS parameter	5.2.16	O	This TLV indicates the MBS service QoS parameter and policy
> MCBCS Service Association SPI	5.2.1	CM	Index a MCBCS Proxy secured service association index with the MCBCS Controller
>MCBCS Controller/Server IPv4	5.2.2	O	IPv4 address of the MCBCS Controller for the given MCBCS service. This TLV is used for MBS proxy to associate with controller in case it is not preconfigured. This TLV SHALL be used if MCBCS controller ID is included.
>MCBCS Controller/Server IPv6	5.2.3	O	IPv4 address of the MCBCS Controller for the given MCBCS service. This TLV is used for MBS proxy to associate with controller in case it is not preconfigured. This TLV SHALL be used if MCBCS controller ID is included.
>MCBCS Controller/Server FQDN	5.2.4	O	Fully qualified domain name of the MCBCS Controller for the given MCBCS service. This TLV is used for MBS proxy to associate with controller in case it is not preconfigured. This TLV SHALL be used if MCBCS controller ID is included.

Table 4-4 : MBS_Join_Rsp message

IE	Description	M/O	Notes
Failure Indication		O	
SF Info (one or more)		M	Service flow description
>MCID	5.2.8	M	
>MBS Zone ID	5.2.9	O	The identifier of MBS Zone.
>MCBCS Transmission Zone ID	5.2.6	O	The identifier of MCBCS Transmission Zone.
>PDFID		O	

IE	Description	M/O	Notes
>QoS Parameters	5.2.16	O	all Parameters pertaining to a specific QoS Description.
>R3 Multicast IP Address	5.2.7	O	

4.3.6 Radius Message between the ASN and the CSN to Support MCBCS Service Initialization and Establishment

New RADIUS MCBCS service attributes are added to support the MCBCS service initialization and establishment messaging which are exchanged between the AAA and the Anchor Authenticator located in the ASN as well as between the MBS Proxy and MCBCS Controller/Server. The details shall be referred to 5.3.1.

4.4 Service Provisioning Procedures

MCBCS service provisioning is referring the system procedures on how the MCBCS application layer interfaces with the WiMAX network to support MCBCS services. Some of the procedures are happening at the application layer, therefore, not all the procedure described in this section is within the scope of this specification.

The overview of on each state of the MCBCS service provisioning operation required to be participated by an MS and by the WiMAX network in order to support the MCBCS service delivery is illustrated in the two figures below.

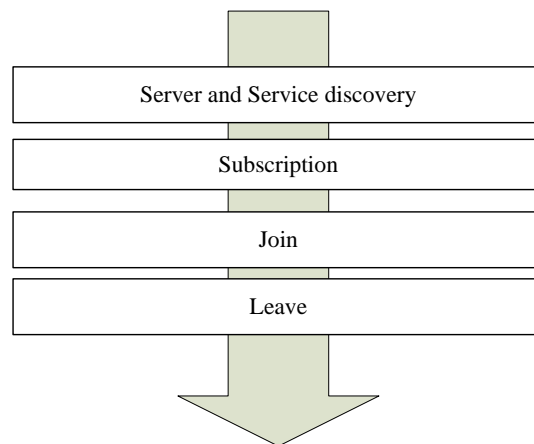


Figure 4-9 : MCBCS Service State Transition – MS Side

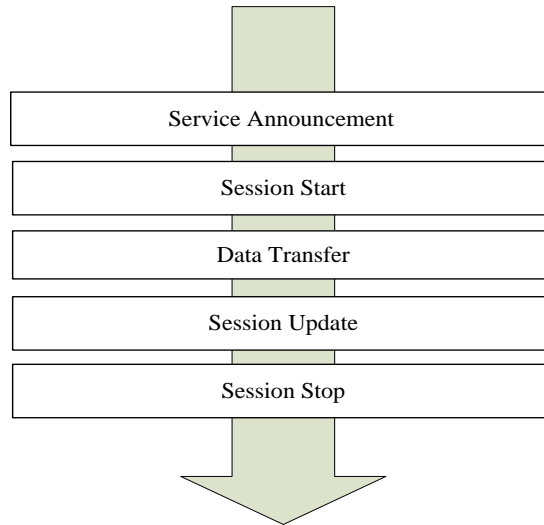


Figure 4-10 : MCBCS Service State Transition – Network Side

Figure 4-9 is an example of the MCBCS Service State Transition for a given MS who is participated in MCBCS service provisioning procedures.

Figure 4-10 is an example of the MCBCS Service State Transition for the network which is participated in the MCBS service provisioning procedures.

MS side activities are performed by each individual user. The MS side activity is performed regardless the number of MSs is participating in the given MCBCS service. The network side service state transition may be independent of the MS side.

The phases of subscription, joining and leaving are operated individually per user. The other phases are performed on a per service basis, i.e. for all users who are participating in the same service. The sequence of phases may be repeated,

Subscription is the first step that user establishes the relationship with the service provider which has the record on the user profile. Dependent on the type of MCBCS service offered by the operator, the subscription may not be required for a free service or emergency service. Subscription can be set up online and offline.

Service Announcement allows users to request or to be informed about the availability of MCBCS services. It has no dependency whether the MS subscribes the MCBCS services or not. User can obtain the service guide online or offline.

The protocol design for the subscription and service announcement is out-of-scope of the WiMAX NWG implementation.

Joining is a procedure when MS is interested in certain set of channels. MS can use multicast IP address(es) from the service guide that was got previously from the MCBCS server/controller; and the MS sends a joining message to ASN to indicate for which the MCBCS service that the MS wants to join. Joining step may not be required for a broadcast service. ,

Leaving is the process that indicates a subscriber leaves a multicast group, i.e. the user is no longer interested in receiving a MCBCS service. If accounting and statistic collection are not required, the leaving is an optional procedure.

Session Start is initiated when the MCBCS controller/server is ready to send data. This is an operation to reserve bearer resources in the network to receive the incoming MCBCS data transmission from the content server. The resource reservation is necessary to prevent resource conflict in the case of overlapping MCBCS transmission zones for different MCBCS services. If the service is a permanent MCBCS service without ending, i.e. the service should

MCBCS-DSx

have been set up when the network is in service, the parameters are pre-configured, and therefore, session start may not be needed. More descriptions on the MCBCS Session Start procedure can be referred to section 4.4.2.1.

Data Transfer is the phase when MCBCS data are transferred to the MSs.

Session update is an optional step which allows the MCBCS controller/server to modify the service QoS and/or the service priority.

Session Stop is triggered when the MCBCS controller/server determines that there will be no more data to send for an extended long period of time which worth's to de-allocate the bearer resource for the given MCBCS session. More descriptions on the MCBCS Session Stop procedure can be referred to section 4.4.2.2.

4.4.1 MS-side Service Provisioning

4.4.1.1 Service Announcement/Service Guide Delivery

4.4.1.1.1 Service Announcement

Service Announcement is to allow users to request or to be informed about availability of an MCBCS service. The operation has no dependency on the MS's subscription for the MCBCS services. Service announcement can be made known in several ways. It MAY be broadcasted to MS. It is also possible for MS to request the control information by unicast.

During the Service Announcement, the network will announce if the Service Subscription is required by the user in order to receive the MCBCS service.

MCBCS Transmission Zone ID and the Packet Data Flow ID (PDFID) are the index for MCBCS service. All MCBCS services with commercial agreements with the attached NAP are included in this service announcement. Service announcement may include MCBCS Transmission zone ID, Service Name, Packet Data Flow ID, contents descriptions, schedule informations (start/end time), etc. The Start time indicates the starting schedule of the MCBCS service area indicates the geographic information of where the MCBCS service is offered.

4.4.1.2 Service Subscription

Subscription is the first step that user establishes the business relationship with the MCBCS service provider to construct the user service profile. Dependent on the operator service offering, for some free services and or emergency services, subscription may not be needed. Subscription can be set up online and offline. For the online case, the request for subscription is sent by MS to MCBCS controller/server at CSN, MS signature, and MCBCS program ID, MCBCS transmission zone ID and multicast IP address may be included. When MCBCS controller/server received this subscription request, MCBCS controller/server will first rely on the NAP's authentication server to authenticate the MS based on the MS signature. If the authentication succeeds, the subscribed MCBCS services will be added to MS's service profile. MCBCS controller/server grants the MS with the requested MCBCS service in the subscription response,

The action in subscription request can be subscribed and un-subscribed. After leaving the MCBCS service, MS can send an un-subscribed request. It is also required to be authenticated. If the authentication is successful, the association between MS and MCBCS service can be released and subscription response indicating the result is sent back.

Subscription, in general, is not needed for the free broadcast services. Non-free broadcast service is considered as the Static Multicast service in the context of this specification. In the case when subscription is needed, both user authentication and authorization are performed in this procedure. The subscription is required for Multicast services.

However, during the service subscription process, the service authorization may take place. The service authorization process is especially important in the case of the free broadcast service because the service authorization during the joining procedure is not required. The subscriber MUST be authorized by the NSP in advance to receive the MCBCS service. In the case of the broadcast service, the service authorization process for

MCBCS-DSx

the MS to access a given MCBCS service can be piggy back with the MS access authentication procedures as described earlier for the pre-provisioning MCBCS service in section 4.3.

4.4.1.3 Joining Service

During service announcement, MBS service information is downloaded to MS. MS collects the favorite MBS services information including a service description (e.g. movie channel, TV channel, etc), IP multicast address and start time.

According to MS's preference, MS can join the favorite IP multicast group at any time. If MS wants to join the IP multicast group, it will pick up IP multicast address from the reserved MCBCS service information and send a joining request message to indicate for which the multicast group that the MS is desired to join. When the network receives the joining request message from MS, it performs the service authorization for the MS. This process is referred as the MS-initiated Join.

On the other hand, based on user profiles or operator policy, network can also invite MS to join an MBS service. But the final decision that receiving this traffic or not is determined by MS. In this case, MS does not need to trigger an explicit join message. This process is referred as the Network-initiated Join.

During the joining procedure, MS shall get the airlink access parameters such as MCID(s) and MBS Zone ID for the associated IP multicast address from ASN to identify the requested MBS downlink traffic over the airlink.

After the joining, the MS's airlink operation will follow the airlink management message (i.e. MBS-MAP message) to receive the MBS traffic according to the MCID(s) and MBS Zone ID in MBS-MAP message that is corresponding to the MBS service information that MS has joint.

For the broadcast service, as it is considered as the pre-provisioned MCBCS service, the joining service procedure is always initiated by Network.

In the case when the data path deletion trigger is enabled when the very last MS leaves the MCBCS service, or when the volume based accounting is required, the anchor SFA shall send MBS_Join_Request /MBS_Leave_Request message to the MBS Proxy. It is optional for the MBS_Join_Request/MBS_Leave_Request to be support, when such option is enabled, the centralized MBS Proxy shall update the MS count.

4.4.1.3.1 Network Initiated Join

Based on user profile or operator policy, network can invite MS to join an MBS service. For a broadcast service, the joining procedure can be triggered by Network.

Two different scenarios are considered for the Network initiated join procedures: Network initiated join for pre-provisioned MCBCS service, and Network initiated join for dynamic subscribed MCBCS service.

In the case of the network initiated join with pre-provisioned MCBCS service, the MS has the MCBCS service subscription with the NSP prior to the MS attachment to the WiMAX access network, hence, the MBS service would have been pre-provisioned for the MS. But, in the case of the network initiated join with dynamic subscribed MCBCS service, the MS subscribes to the MCBCS service after the MS attachment to the WiMAX access network. Once the MS subscribes to the MCBCS service, the user's service profile will then be updated to contain the MCBCS service related information.

4.4.1.3.1.1 Network Initiated Join with Pre-provisioned MCBCS Services

Based on user profile or operator policy, the AAA can trigger the join procedure as shown in 4.4.1.3.1, the MS anchor ASN will receive the MS's service profile, which includes the MCBCS controller/server information as well as the program information, accounting information for the service that MS has already subscribed. The anchor SFA will then send a MBS join request to the MBS Proxy.

MCBCS-DSx

Note that, during the network entry phase, the anchor DPF, anchor SFA, serving SFA, serving MBS DPF are collocated.

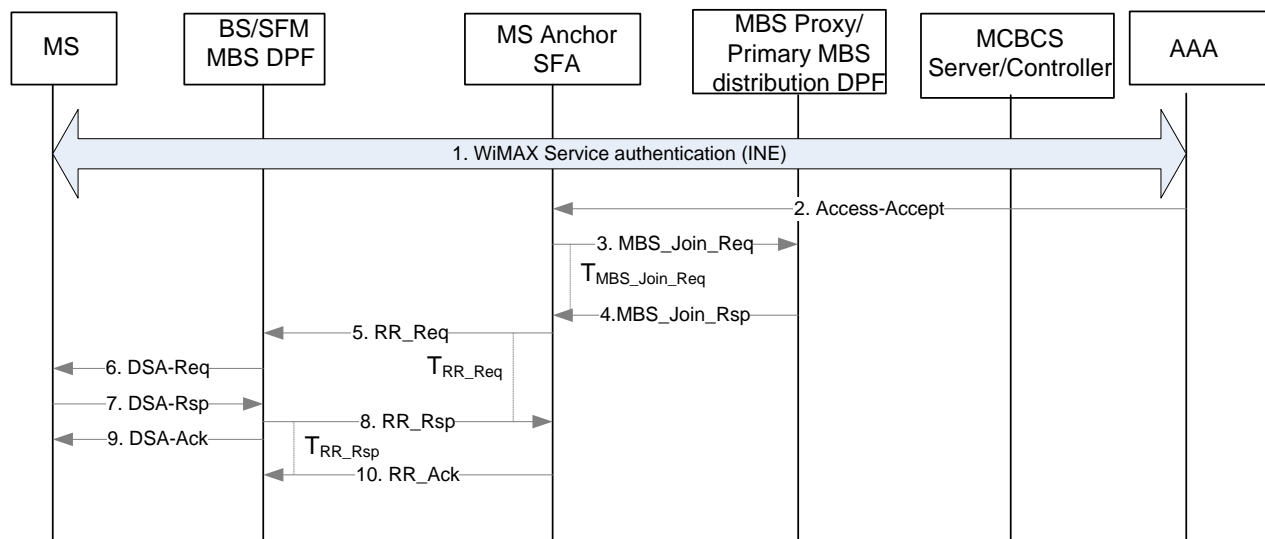


Figure 4-11 : Network initiated Join procedure with pre-provisioned MCBCS service

STEP 1~2:

MS performs an initial network entry. MS gets MBS service profile information through an offline or service announcement procedure. Also, MS may already have the pre-configured service information.

During this step, the user's MCBCS service profile is downloaded from the AAA to Anchor ASN after the completion of a successful initial network entry, AAA sends an Access Accept message to the anchor SFA

STEP 3:

Upon anchor SFA received the authorization successfully from the AAA, the anchor SFA sends a MBS_Join_Req message to the MBS proxy to get MBS Zone ID and MCID(s), and request the airlink service flow type (i.e. unicast or multicast) to receive the MBS data. The MBS_Join_Req message includes the QoS parameters and classification rules which Anchor SFA receives from AAA.

Table 4-5 : MBS_Join_Req message from Anchor SFA to MBS proxy

IE	Description	M/O	Notes
SF Info (one or more)		O	Service flow description
>SFID		O	Service flow Identifier
>MBS Zone ID	5.2.9	O	The identifier of MBS Zone.
>MCBCS Transmission Zone ID	5.2.6	M	The identifier of MCBCS Transmission Zone.
>PDFID		M	The PDFID is used together with the MCBCS Transmission Zone ID to unique identify the given MCBCS service flow for a given MCBCS service
>QoS parameter	5.2.16	O	This TLV indicates the MBS service QoS parameter and policy
> MCBCS Service Association SPI	5.2.1	CM	Index a MCBCS Proxy secured service association index with the MCBCS Controller
>MCBCS Controller/Server IPv4	5.2.2.	O	IPv4 address of the MCBCS Controller for the given MCBCS service. This TLV is used for MBS proxy to associate with controller in case it is not preconfigured. This TLV SHALL be used if MCBCS controller ID is included.
>MCBCS Controller/Server IPv6	5.2.3	O	IPv4 address of the MCBCS Controller for the given MCBCS service. This TLV is used for MBS proxy to associate with controller in case it is not preconfigured. This TLV SHALL be used if MCBCS controller ID is included.
>MCBCS Controller/Server FQDN	5.2.4	O	Fully qualified domain name of the MCBCS Controller for the given MCBCS service. This TLV is used for MBS proxy to associate with controller in case it is not preconfigured. This TLV SHALL be used if MCBCS controller ID is included.

STEP 4:

MBS proxy replies an MBS_Join_Rsp message to the anchor SFA. MBS proxy should include the MBS service parameters for the MBS service flow including the MBS service flow type, MBS Zone ID and MCID(s) in it. If the established flow has different active QoS parameters, classification rules, then MBS proxy should include the new QoS parameters, classification rules, etc.

Table 4-6 : MBS_Join_Rsp message from MBS proxy to Anchor SFA

IE	Description	M/O	Notes
Failure Indication		O	

IE	Description	M/O	Notes
SF Info (one or more)	5.2.13	M	Service flow description
>MCID	5.2.8	M	
>MBS Zone ID	5.2.9	O	The identifier of MBS Zone.
>MCBCS Transmission Zone ID	5.2.6	M	The identifier of MCBCS Transmission Zone.
>PDFID		M	
>QoS Parameters	5.2.16	O	Shall be included if the existing flow has a different active QoS parameters.
>R3 Multicast IP Address	5.2.7	O	
>Current Volume Counter	5.2.11	O	For volume based accounting if it is required

STEP 5:

Upon receiving the MBS_Join_Rsp message from the anchor SFA, the anchor SFA assigns a SFID and sends a RR-req message to the SFM. The RR-Req message includes the additional TLVs for MBS service flow such as a MCBCS transmission zone ID, MCID, MBS zone ID, R3 Multicast IP address, PDF ID.

Note: For the phase-1 MCBCS, only the multicast service flow is supported. The support of the unicast service flow and switching between unicast and multicast is FFS.

Table 4-7 : RR-Req message for MCBCS service from Anchor SFA to SFM

IE	Reference	M/O	Notes
MS Info		M	
SF Info	5.2.13	M	
>Reservation Action		M	SHALL be set to “Create, Admit, Activate or Modify”. For pre-provisioned service flows, Create, Admit and Activate refer to the same service flow state.
>SFID		M	SFID as defined on R1.
>Correlation ID		O	This TLV SHALL be included for packet data flow based accounting.
>Direction		M	Specifies the direction of the reservation.
>CS Type		O	Specifies Service Flow Convergence Sublayer to be used. If omitted, IPv4 CS is assumed as a default value.
>Packet Classification Rule/ Media Flow Description		M	See Release 1.3 for details
>QoS Parameters		M	See Release 1.3 for details
>PHS Rule		O	

IE	Reference	M/O	Notes
>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS packet flow and this TLV is common to every MS for that packet flow
>MCBCS Transmission zone ID	5.2.6	M	
> R3 Multicast IP Address	5.2.7	M	
> MCID	5.2.8	M	
> MBS Zone ID	5.2.9	M	
BS Info		O	
>BS ID		CM	This TLV SHALL be included if BS Info is included in the transmitted message.

STEP 6:

After receiving the MBS RR_req message from the Anchor SFA, the SFM in BS initiates the DSx procedure with the MS to set up the airlink connection with the MS. This procedure must signal the associated IP multicast address (i.e. by packet classification rule parameters) to MS to enable mapping between airlink connections and the MCBCS service contents.

STEP 7

MS sends a DSA-RSP message to the BS according to the IEEE 802.16-Rev2 specification [3].

STEP 8

The SFM sends a RR-Rsp message to the anchor SFA with joining succeed TLV.

Table 4-8 : RR-Rsp message for MBS service from Serving SFA to Anchor SFA

IE	Reference	M/O	Notes
Failure Indication		M	
MS Info		M	
SF Info	5.2.13	M	
>Reservation Action		M	SHALL be set to “Create, Admit, Activate or Modify”. For pre-provisioned service flows, Create, Admit and Activate refer to the same service flow state.
>SFID		M	SFID as defined on R1.

IE	Reference	M/O	Notes
>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS packet flow and this TLV is common to every MS for that packet flow
>MCBCS Transmission zone ID	5.2.6	M	
> R3 Multicast IP Address	5.2.7	M	
>MCID	5.2.8	M	
> MBS Zone ID	5.2.9	M	
BS Info		O	
>BS ID		CM	This TLV SHALL be included if BS Info is included in the transmitted message.

1

2 **STEP 9**

3 The SFM sends a DSA-ACK message to the MS according to the IEEE 802.16-Rev2 specification [3].

4 **STEP 10**

5 The Anchor SFA sends a RR_Ack message to the SFM.

6

7 **4.4.1.3.1.2 Network initiated join with dynamic MCBCS subscription**

8 After the MS attachment to the WiMAX network, the MS may subscribe the MCBCS service with the MCBCS
9 Controller/Server. The MCBCS Controller/Server communicates with the AAA based on the MS's context
10 information, once the MS is authenticated and is authorized to access the MCBCS service, the user's service profile
11 is updated based on the new MCBCS subscription. And the AAA sends the information or policy to the anchor SFA.

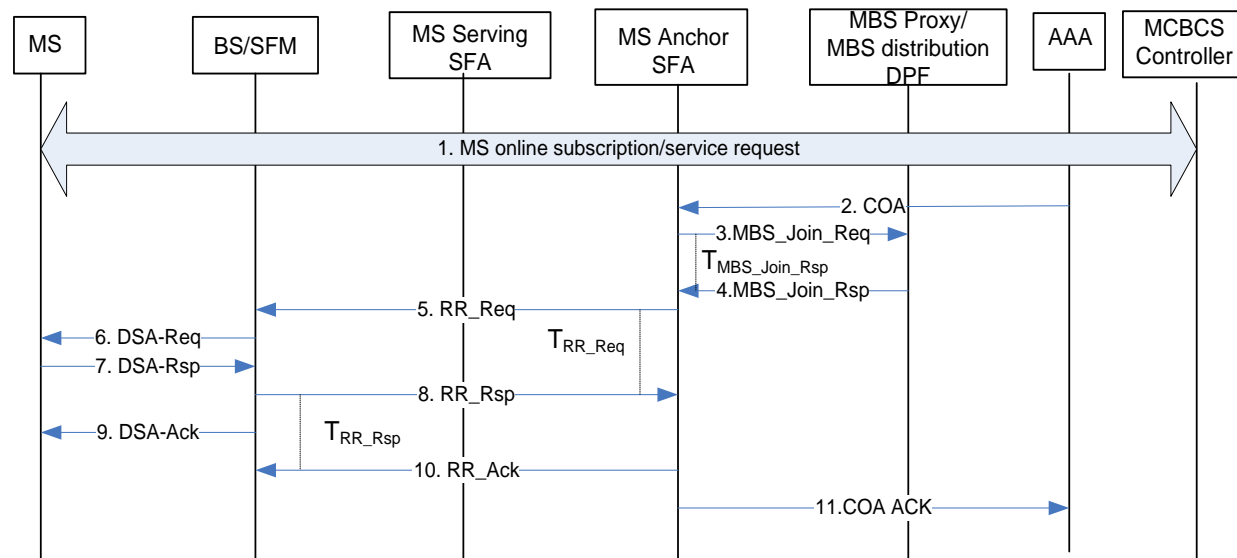


Figure 4-12 : Network initiated join with dynamic MCBCS subscription

Note: For this scenario, the MBS data path to all the BSs within the MBS Zone or MCBCS Transmission Zone is assumed to be established prior to the Join procedure.

STEP 1

After the MS attachment to the WiMAX network, the MS subscribed an MCBCS service with the MCBCS Controller/Server. During MCBCS service subscription process, MCBCS Controller/Server contacts AAA of the MS for the MCBCS service authorization. Once the MS is authorized, the AAA updates user's service profile based on the MS's subscription.

STEP 2

The AAA sends the Change of Authorization (CoA) request message to the MS's anchor Authenticator. The CoA request message includes the updated user's service profile information that contains the given MCBCS service description.

STEP 3

The anchor Authenticator relays the MCBCS service profile information to the anchor SFA. Based on the local implementation design, the anchor SFA refers to the information in the MBS service profile that has received to identify the appropriate target MBS Proxy, and sends a MBS_Join_Req message to the MBS proxy to get MCID and request the service flow type (i.e. unicast or multicast service flow) to receive the MBS data. The MBS_Join_Req message includes the QoS parameters and classification rules which Anchor SFA receives from AAA. The composition of this MBS_Join_Request message is presented in Table 4-5.

Note: For the phase-1 MCBCS, only the multicast service flow is supported. The support of the unicast service flow and switching between the unicast and multicast service is FFS. STEP 4

MBS proxy responds with a MBS_Join_Rsp message to the anchor SFA. MBS proxy should include the service flow type for the MBS data in it. In addition, MBS proxy should include the MBS zone ID and MCID for the flow. If the already established flow has a different active QoS parameters, classification rules, than MBS proxy should include the new QoS parameters, classification rules, etc. The composition of this MBS_Join_Rsp message is presented in Table 4-6.

STEP 5

Upon receiving the MBS_Join_Rsp message from the anchor SFA, the anchor SFA assigns a SFID and sends a RR-Req message to SFM. If the service flow type which MBS proxy notifies is a unicast, the anchor SFA triggers a unicast service flow creation procedure for the MBS data. But, if it is a multicast, the anchor SFA triggers the multicast service flow creation procedure. The RR-Req message includes the additional TLVs for MBS service flow such as a Data Type, MBS Distribution DPF ID, MBS zone ID, MCID. The composition of this RR-REQ message for MBS is presented in Table 4-7.

Note: For the phase-1 MCBCS, only the multicast service flow is supported. The support of the unicast service flow and switching between the unicast and multicast service is FFS.

STEP 6

The SFM in BS performs the DSA procedure with the MS. This procedure must signal IP multicast address to MS to enable mapping between L2 connections and MBS contents.

STEP 7

MS sends a DSA-RSP message to the SFM in BS based on IEEE 802.16 specification [3].

STEP 8

The SFM sends a RR-Rsp message with the result to the Anchor SFA. The composition of the RR-Rsp message for MBS is presented in Table 4-8.

STEP 9

The SFM sends a DSA-Ack message to the Anchor SFA.

STEP 10

The Anchor SFA sends a RR_Ack message to the Anchor SFA.

STEP 11

The Anchor SFA informs the Anchor Authenticator of the MS to send a COA-Ack message to the AAA.

4.4.1.3.1.3 MS Initiated Join

MS initiated Joining happens when MS already subscribed the service sometime before the MS attachment to the ASN (i.e. the user's service profile has the record), but MS is only interested in joining the MCBCS service after the MS attachment to the ASN.

If MS wants to join an IP multicast group, it shall be in the active mode. MS already knows an MBS service information including multicast IP address via the service announcement procedure. To trigger the MS initiated joining for the MBS service, MS selects the MBS content which it wants to play.

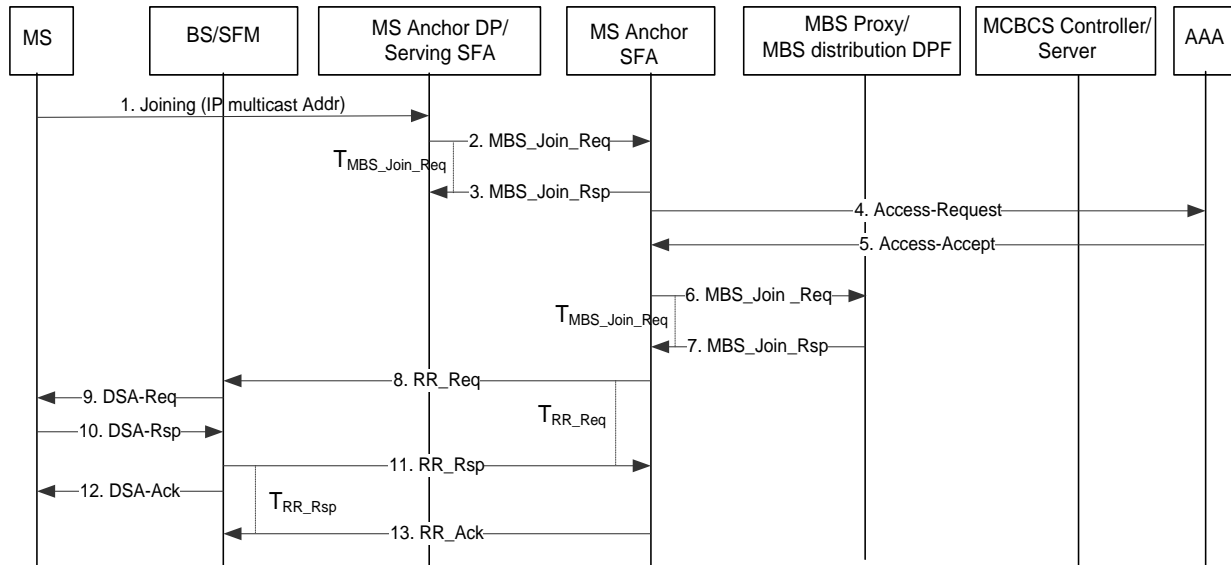


Figure 4-13 : MS initiated Join Procedure

Subscription is an application level procedure between MBS client in MS and MCBCS Controller/Server in the CSN. The details of this procedure are out of scope of this specification; however, the design of this specification is intended to be flexible for accommodating any available application e.g. OMA BCAST [18].

STEP 1:

By referring to the service guide that was received earlier, MS selects the MCBCS service and sends a Join message to the anchor ASN. It can include one or more multicast IP addresses of MBS Contents. An IGMP or MLD can be used for the joining message. However, the decision on the choice of the IP layer signaling to support the MS joining is out of scope of this specification.

STEP 2:

Upon receiving the Joining message, Anchor DPF triggers the Serving SFA to send a MBS_Join_Req message to the MS anchor SFA including the MS NAI and also the corresponding multicast IP address that MS wishes to join.

Table 4-9 : MBS_Join_Req message from Serving SFA to Anchor SFA

IE	Reference	M/O	Notes
MCBCS Service info	5.2.5	M	
>R3 Multicast IP address	5.2.7	M	
MS Info		M	
> MS ID		M	

STEP 3:

MS anchor SFA sends MBS Join_Rsp message to the serving SFA

Table 4-10 MBS_Join_Rsp message from Anchor SFA to Serving SFA

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
MCBCS Service info	5.2.5	M	
> R3 Multicast IP Address	5.2.7	O	

STEP 4, 5:

The Anchor SFA initiates an authentication/authorization procedure with the AAA and/or MCBCS controller/server.

STEP 6:

Upon anchor SFA received authorization successfully from the AAA, the anchor SFA will send an MBS join request message to the MBS proxy to get a MBS Zone ID, the MCID(s) and request the MBS service flow type (i.e. unicast or multicast) to receive the MBS data.

STEP 7:

MBS proxy sends an MBS join response message to the anchor SFA. MBS proxy should include the service parameters for the MBS service flow including the MBS service including the MBS service flow type, MBS Zone ID and the MCID(s) in it.

STEP 8:

Upon receiving the authorization successful message, the anchor SFA sends an MBS RR_request message to the SFM in BS to trigger the DSx procedure.

STEP 9:

The SFM in BS starts the DSx procedure towards the MS. This procedure must signal IP multicast address selected in step1 to MS to enable mapping between airlink connections and requests in step one IGMP join

STEP 10, 11, 12:

Once the successful DSx response is replied from the MS, the SFM in BS sends an MBS RR_response message to the Anchor SFA to indicate that joining procedure is succeed, and also confirms to the MS for the reception of the DSx response.

4.4.1.4 Leaving Service

The leaving service procedure is a signaling procedure between the MS and the network. The procedure removes the MCBCS service related parameters from the MS contexts in ASN and from the MCBCS controller/server for a particular MCBCS service. The MBS leave procedure can be initiated by MS or by the MCBCS controller/server for a MCBCS service. When user doesn't want to receive a MBS data, MS can initiate the leaving service procedure. Also, when MCBCS controller/server decides to terminate the MCBCS service for one or more MSs who prescribe to the same MCBCS service, it will initiate the leaving service procedure. MCBCS controller/server can stop MCBCS service when it does not have a MBS data to transmit or by any other reasons (e.g. MCBCS controller/server management, etc).

The leaving procedure may be optional if the accounting and statistic collection are not required.

4.4.1.4.1 MS initiated leaving service

When MS doesn't want to receive a MBS data, it can initiate the leaving service procedure.

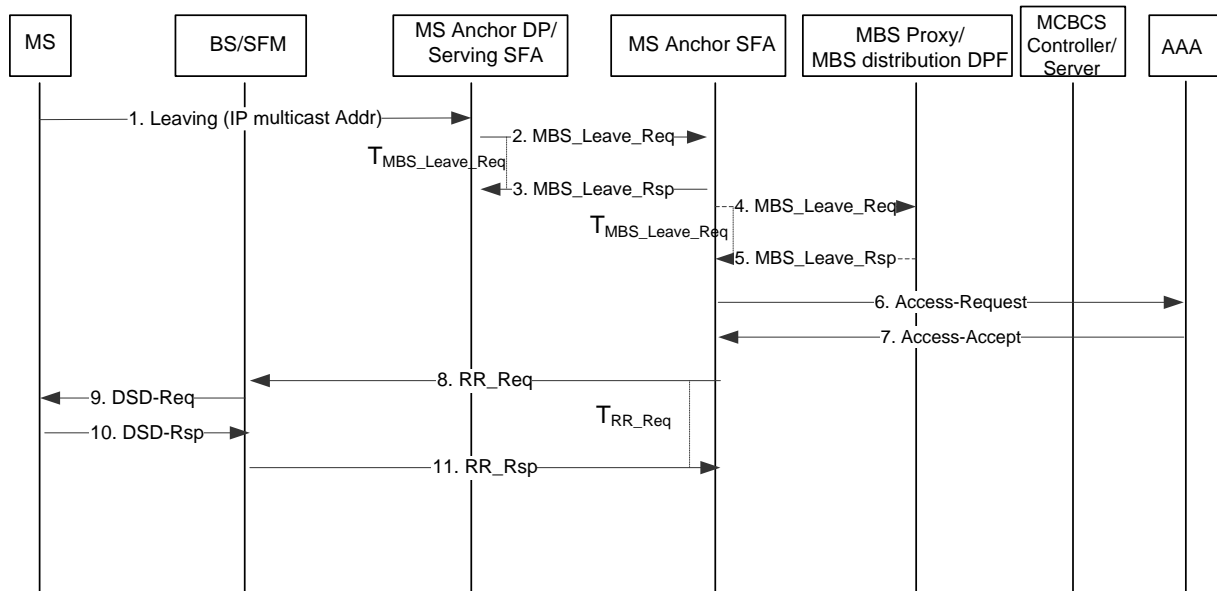


Figure 4-14 : MS initiated leaving service

STEP 1:

MS sends a MBS leaving message to indicate that it is not interested in the contents anymore and wants to leave, the leaving message includes the IP multicast address of MBS contents.

STEP 2:

Upon receiving the leaving message, Anchor DPF triggers the Serving SFA to send an MBS_Leave_Req message to the MS's anchor SFA including the MS NAI and also the multicast IP addresses that the MS wishes to leave.

Table 4-11 : MBS_Leave_Req message from Serving SFA to Anchor SFA

IE	Reference	M/O	Notes
MS Info		M	
> MS ID		M	
MCBCS Service Info	5.2.5	M	
> R3 Multicast IP address(s)	5.2.7	M	If the leaving message includes multiple multicast IP addresses, multiple IP addresses are included.
BS Info		O	

> BS ID		O	Serving BS ID
---------	--	---	---------------

STEP 3:

Anchor SFA sends an MBS_Leave_Rsp message to the Serving SFA.

Table 4-12 : MBS_Leave_Rsp from Anchor SFA to Serving SFA

IE	Reference	M/O	Notes
MCBCS Service Info	5.2.5	M	
> R3 Multicast IP address(s)	5.2.7	M	Multicast IP addresses included in MBS_Leave_Req message.
Failure Indication		O	

STEP 4:

The Anchor SFA sends an MBS_Leave_Req message to the MBS proxy to indicate its leaving if the volume based accounting is required or if the data path deletion trigger is enabled due to the very last MS exit.

Table 4-13 : MBS_Leave_Req from Anchor SFA to MBS proxy

IE	Reference	M/O	Notes
MCBCS Service Info	5.2.5		
> R3 Multicast IP address(s)	5.2.7	M	If the leaving message includes multiple multicast IP addresses, multiple IP addresses are included.
> Volume Required			For volume based accounting if it is required

STEP 5:

Upon receiving a MBS_Leave_Req message, the MBS Proxy will response back a MBS_Leave_Response message which includes the Current Volume Counter if the volume based accounting is required.

Table 4-14 : MBS_Leave_Rsp from MBS proxy to Anchor SFA

IE	Reference	M/O	Notes
MCBCS Service Info	5.2.5	M	
> R3 Multicast IP address(s)	5.2.7	M	Multicast IP addresses included in MBS_Leave_Req message.

> Current Volume Counter	5.2.11		For volume based accounting if it is required
Failure Indication		O	

STEP 6:

The Anchor SFA initiates the authentication/authorization procedure with the AAA and/or MCBCS controller by sending an Access-Request message.

STEP 7:

Upon receiving the authorization successfully from the AAA, AAA responds by sending an Access-Accept message.

STEP 8:

If the authorization is successful, the anchor SFA sends a RR-Req message to the SFM.

Table 4-15 : RR-Req message: Deletion of SF

IE	Reference	M/O	
BS Info		O	
>BS ID		CM	This TLV SHALL be included if BS Info is included in the transmitted message.
MS Info		M	
SF Info	5.2.13		
>Reservation Action		M	SHALL be set to "Delete".
>SFID		M	SFID as defined on R1.
>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS packet flow and this TLV is common to every MS for that packet flow
>MCBCS Transmission zone ID	5.2.6	M	
> R3 Multicast IP Address	5.2.7	M	
> MCID	5.2.8	M	
> MBS Zone ID	5.2.9	M	

STEP 9, 10:

The SFM in BS sends a DSD-Req message to the MS. This procedure must signal IP multicast address selected in step1 to MS to enable a mapping between airlink connections and requests in IGMP leave message.

STEP 11:

Once the DSD procedure is successful, the SFM in BS sends a MBS RR_Rsp message to the Anchor SFA to confirm the successful deletion of the service flow for the given MCBCS service towards the corresponding MS.

Table 4-16 : RR-Rsp message: Deletion of SF

IE	Reference	M/O	Notes
Failure Indication		M	
MS Info		M	
> SF Info	5.2.13	M	
>>Reservation Action		M	SHALL be set to "Create, Admit, Activate or Modify". For pre-provisioned service flows, Create, Admit and Activate refer to the same service flow state.
>>SFID		M	SFID as defined on R1.
>>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS packet flow and this TLV is common to every MS for that packet flow
>>MCBCS Transmission zone ID	5.2.6	M	
>> R3 Multicast IP Address	5.2.7	M	
>> MCID	5.2.8	M	
>> MBS Zone ID	5.2.9	M	

4.4.1.4.2 Network initiated leaving service

MCBCS controller/server can initiate the leaving service procedure when it terminates MCBCS service or it does not have any MCBCS data to deliver MCBCS controller/server can perform a leave procedure without session stop procedure to notify the corresponding MS(s) that the MCBCS session will be stopped. The network initiated leaving service can be targeted to all MBS receivers or a particular MS.

The network initiated leaving service is an optional procedure.

When MCBCS controller/server does not have any MCBCS data to deliver, it may initiate a Session stop as described in section 4.4.2.2 instead of the network initiated leaving service procedure in section 4.4.1.4.2

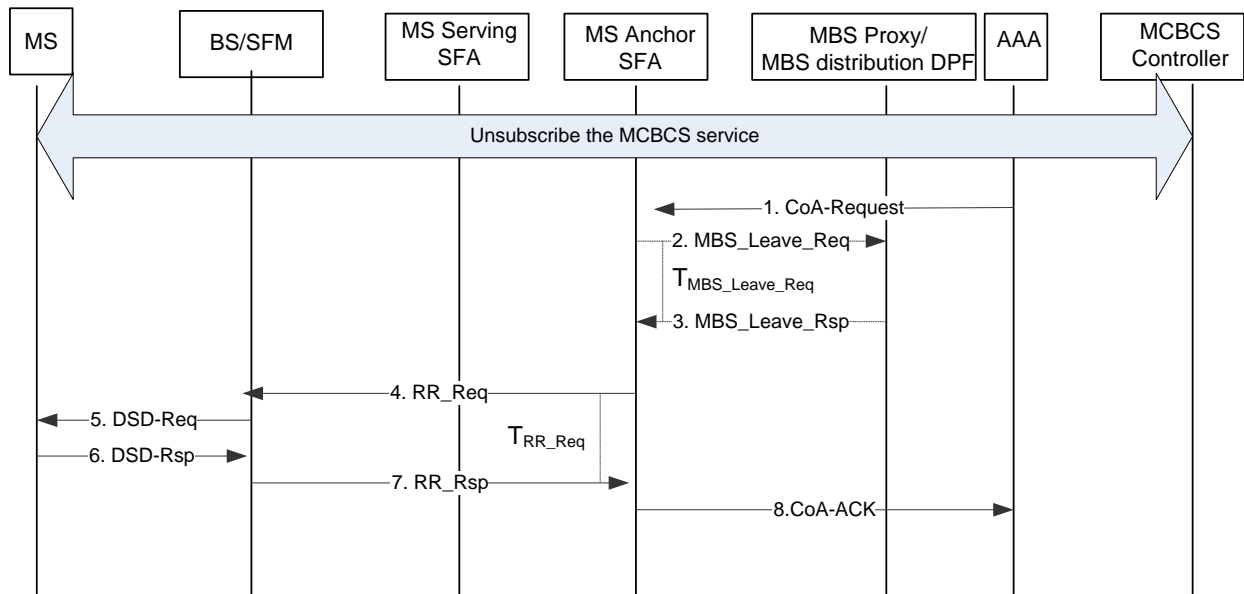


Figure 4-15 : Network initiated leaving service

STEP 1:

MS unsubscribes a MCBCS service. During the unsubscription, MCBCS controller contacts AAA. AAA changes a user profile based on the unsubscription. AAA sends a CoA Request message to the MS's anchor SFA to update the change of user profile.

STEP 2:

Upon receiving the change of user profile, the anchor SFA will send an MBS_leave_req message to the MBS proxy as described in Table 4-11.

STEP 3

MBS proxy sends an MBS_leave_Rsp message to the anchor SFA. The composition of MBS_Leave_Rsp message is presented in Table 4-12.

STEP 4:

Upon receiving the CoA message, Anchor SFA sends a RR-Req message to the BS to indicate a service flow release.

STEP 5:

The SFM in BS performs the DSD_REQ procedure towards the corresponding MS according to IEEE 802.16-Rev2 procedure [3].

STEP 6:

MS sends a DSD-RSP message to the SFM in BS.

STEP 7

Upon successful of DSD_REQ procedure, the SFM in BS sends MBS RR_Rsp message to the Anchor SFA to confirm the successful deletion of the MBS service flow.

STEP 8:

Anchor SFA sends a CoA response message to the AAA to confirm the MBS leaving procedure is successful.

4.4.2 Network-side Service Provisioning

4.4.2.1 Session Start

In the case when the MCBCS service association between the MBS Proxy and MCBCS controller/server is pre-configured, the MCBCS service initialization and establishment at the ASN can be triggered directly by the MCBCS controller/server via the event of Session Start.

Session Start occurs independently of activation of the service by the user – i.e. a given user may activate the service before or after Session Start.

The MCBCS controller/server initiates the MBS Session Start procedure when it is ready to send a data. The Session Start from MCBCS controller/server may also be used to trigger a bearer resource establishment for MCBCS data transfer to deliver the MBS content information when there is no existing MCBCS data path. In the case of type 3 data path (see section 4.5.1.2 for more details) is used, the Session Start procedure may be used to modify the existing data path to add new service flow.

The MCBCS data from MCBCS controller/server can be delivered to the MBS distribution DPF within an MBS zone by an unicast transport or by multicast transport..

After sending the Session Start Request message, the MCBCS controller/server should wait for configurable period of time before sending MBS data. This delay should be long enough to avoid buffering the MBS data in the affected functional entities along the datapath (e.g. MBS Distribution DPF) other than the MCBCS controller/server, i.e. the delay should allow the network to perform all procedure required to enable MBS data transfer before the MCBCS controller/server sends the MBS data.

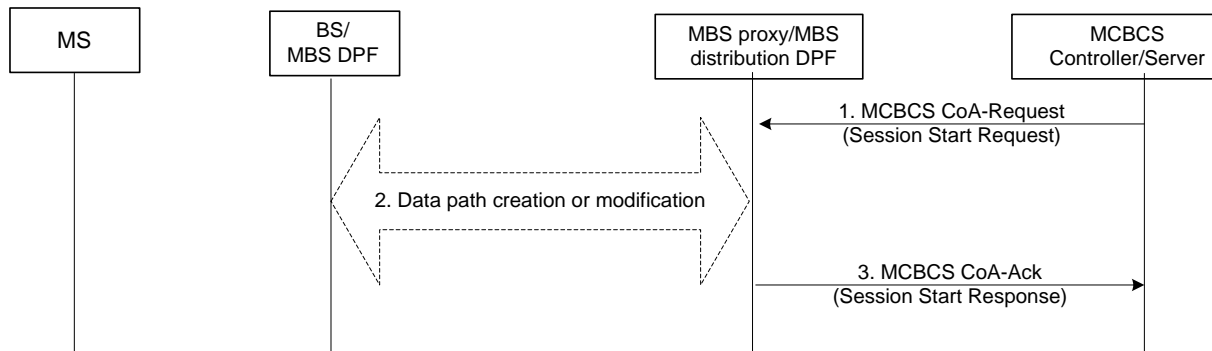


Figure 4-16 : Session Start Procedure

STEP 1:

When the MCBCS controller/server is ready to send a MBS data, it should initiate a session start request message. The session start request message includes a MCBCS content information (Multicast IP Address, MCBCS Transmission zone ID, PDFID(s), MCBCS Program ID, MCBCS Content ID, QoS parameters, estimated session duration, service priority etc)

STEP 2:

Upon receiving a session start request message from MCBCS controller/server, the MBS Proxy will trigger MBS distribution DPF for the MBS data path establishment with the MBS DPF if the data path has not been established yet, and/or to trigger the MBS data path modification to change of QoS if the QoS is different than what it has used

MCBCS-DSx

to set up the data path earlier via some other form of trigger (e.g. via the very first MS join). If the data path is already exist and using type 3 data path, the MBS Proxy may leverage the session start to trigger the data path modification to add new MCBCS service flow to that data path. The detailed data path procedure should refer to the data path section (see section 4.5). This message includes MCID, MBS zone ID, Classification rule, etc.

STEP 3:

Upon receiving the completion of the MBS data path operation from MBS proxy, MBS proxy sends the CoA response message to MCBCS controller/server.

4.4.2.2 Session Stop

Session Stop occurs independently of the termination of the service by the user – i.e. a given user may deactivate the service before or after Session Stop.

The MCBCS Controller/Server initiates the MBS Session Stop procedure when the MCBCS service is over or there is no more MCBCS service data expected to be transmitted for a sufficiently long period of time and therefore, it justifies the release of bearer plane resources in the network. The MCBCS Controller/Server will signal AAA to initiate the network leaving procedure for MS to trigger the DSD procedure as specified in IEEE 802.16-Rev2[3] if timely and volume based accounting is required.

The interface between MCBCS Controller/Server and AAA is out of scope of this specification.

From data path perspective, once the MCBCS Controller/Server receives the notification from AAA for the confirmation of the termination of the given MCBCS service flow(s) from all the affected MSs, it will signal a session stop message to MBS Proxy to delete the context for the given MCBCS service flow for the associated data path. Subsequently, the MBS Distribution DPF will trigger the data path deregistration procedure with MBS DPFs in the corresponding BSs.

The details of data path procedure shall be referred to the data path section 4.5.

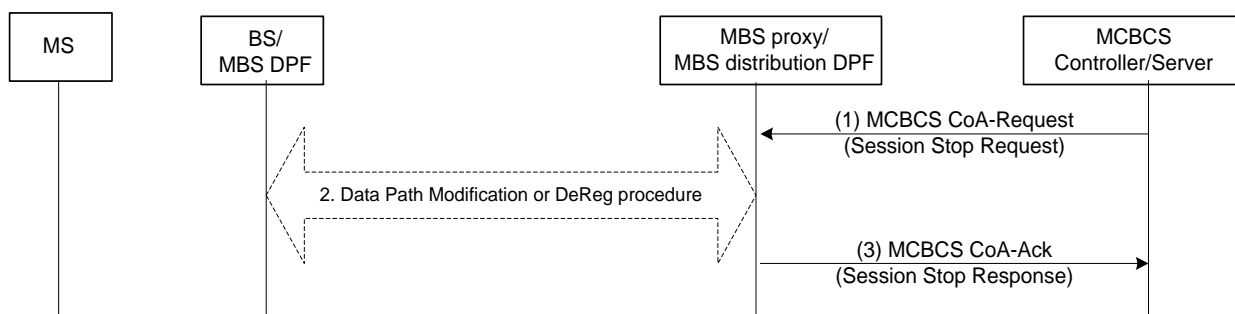


Figure 4-17 : Session Stop Procedure

STEP 1:

The MCBCS Controller/Server sends a Session Stop Request message to the MBS Proxy. The Session Stop Request message includes multicast IP address, etc.

STEP 2:

If it is the last MCBCS service flow on that data path, the MBS Proxy will trigger data path de-registration procedure to delete both the service flow context and the data path. For type 3 data path, if it is not the last MCBCS service flow on the data path, the MBS proxy will trigger data path modification procedure to delete the MCBCS service flow context. The details of data path procedure should refer to section 4.5.

STEP 3:

Once the MCBCS data path procedure is completed, MBS Proxy sends Session Stop Response message to MCBCS Controller/Server.

4.4.3 Timers and Timing Considerations

This section describes the set of timers involved in the service provisioning procedure. The service provisioning procedure employs four timers :

- T_{RR_Req} : is started by an Anchor-SFA upon sending a *RR_Req* message. It is stopped upon receiving a corresponding *RR_Rsp*.
- T_{RR_Rsp} : is started by the Serving SFA when it sends a *RR_Rsp* message and is stopped upon receiving a corresponding *RR_Ack* message.
- $T_{MBS_Join_Req}$: is started when the Anchor SFA sends a *MBS_Join_Req* message and is stopped upon receiving a corresponding *MBS_Join_Rsp* message.
- $T_{MBS_Leave_Req}$: is started by the Anchor SFA when *MBS_Leave_Req* message is sent to the MBS proxy. It is stopped upon receiving a corresponding *MBS_Leave_Rsp* message.

Table 4-17 specifies the maximum value of timers and also indicates the range of the recommended duration of these timers.

Table 4-17 : Timer Values for service provisioning procedure

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
T_{RR_Req}			TBD
T_{RR_Rsp}			TBD
$T_{MBS_Join_Req}$			TBD
$T_{MBS_Leave_Req}$			TBD

4.4.4 Service Provisioning Error Conditions

This section describes error conditions associated with the MBS service flow management procedure.

4.4.4.1 Timer Expiry

The following table shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer expiry, if the maximum retries has not been exceeded, the timer should be restarted. Otherwise, the corresponding action(s) should be performed as indicated in Table 4-18.

Table 4-18 : Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
T_{RR_Req}	Anchor SFA	In case of network initiated joining after dynamic MCBCS subscription, COA-NACK is transmitted from the MBS proxy to the AAA. In other cases, no action is required.
T_{RR_Rsp}	SFM	The requested or deleted resources should be released. The deletion of the SFs on the MS should be triggered as described in NWG R1.0 stage 3 step 2 to 5.
$T_{MBS_Join_Req}$	Serving SFA/Anchor SFA	No action is required.
$T_{MBS_Leave_Req}$	Serving SFA/Anchor SFA	TBD

4.4.5 RADIUS Message between the ASN and the CSN to Support MS MCBCS Service Provisioning

New RADIUS MCBCS service attributes are added to support the MS MCBCS service provisioning messaging which are exchanged between the AAA and the Anchor Authenticator located in the ASN as well as between the MBS Proxy and MCBCS Controller/Server. The details shall be referred to 5.3.1.

4.5 MCBCS Data Path

The MCBCS Data Path Function manages the MBS bearer plane establishment and supports the packet processing between the CSN and the ASN as well as within the ASN to support the MCBCS content downlink transmission for the MCBCS services. The MCBCS Data Path function leverages the GRE tunneling mechanism to transport the MCBCS traffic within the ASN. The packet sequence numbering, part of the GRE tunneling mechanism, is also used for the MBS Data Synchronization operation (see section 4.12 for more details).

Two types of MCBCS Data Paths are supported for the MCBCS transport:

Type 1: Type 1 data path bearer as documented in [5] which is a typical generic layer 3 tunnel. The encapsulated payload is an IP datagram and the tunneling mechanism is based on GRE including the use of the sequence number. It is mandatory to support the Type 1 Data Path for MCBCS transport.

Type 3: A new Type 3 data path bearer is introduced and is also based on a generic layer 3 tunneling. The encapsulated payload is one or more MAC Bursts that is part of a given MBS permutation zone as defined in [3] and is generated by the MCBCS Sync upper executer. Similar to Type 1, the tunneling mechanism is based on the GRE mechanism including the use of the sequence number.

The MCBCS Data Path Function is further classified into two roles to support the MCBCS services:

- **MBS Distribution Data Path Function (DPF):**

The MBS Distribution DPF is a bearer plane functional entity in the ASN that supports the MBS bearer plane management and the MBS data distribution. It receives the downlink transmission of a MCBCS content, sent from the CSN, classifies the incoming SDUs into the appropriate MCBCS Service Flow (e.g. 6-tuple classification) and applies the corresponding WiMAX Convergence Sublayer rules (e.g. Packet Header Suppression). After classification and CS processing, the MBS traffic is delivered to the Sync Controller and the Sync Executer functional entities. In the general case, the Primary MBS Distribution DPF is unique per each MBS Zone, but the same MBS Distribution DPF may serve more than a single MBS Zone.

MCBCS-DSx

For type 1 data path, there may be multiple MBS DPs within the MBS Zone for different MBS contents – i.e. different MBS contents/Service Flows may be transported by different MBS DPs. In order to enable the coordination of processing and distribution of the data content across the BSs belonged to the same MBS Zone or the same MCBCS Transmission Zone over the MBS DPs, certain coordination within the Multicast Routing infrastructure is required. For phase-1 MCBCS, only a single MBS Distribution DPF is expected to manage one or more MBS Zones. Inter-communication of multiple MBS Distribution DPFs across multiple MBS Zones is FFS.

MBS Distribution DPF is always located in the ASN GW/ASN and uses WiMAX R6/ R4 Data Path tunnels (GRE) to deliver MBS traffic to the BSs. For Type 1 data path, each GRE Key tags data that belongs to different MBS contents (MBS Service Flows) and the BS(s) map the GRE Keys to the proper MCIDs (in a way similar to unicast traffic).

For Type 3 data path, where the MBS Upper Sync Executor is collocated with the MBS Distribution DPF, the GRE Key tags data that belongs to the MBS Region including one or more MBS Service Flows. Depending on the functional elements composition (whether the Upper Sync Executor is collocated with MBS Distribution DPF or not), different types of MBS traffic payloads can be used over the R6/R4 data path.

The MBS data path payload is identified by the payload type that describes the packaging format of the MBS data sent to a BS. The actual data path transport mechanism can be either unicast or multicast.

- **MBS DPF**

The MBS DPF includes the collection of MCBCS specific bearer processing functions which are located at the BS and is responsible for receiving packets sent by the MBS Distribution DPF located at the ASN-GW. For type 1 data path, it de-encapsulates the packets, maps the GRE key to the corresponding MCID and forwards them to the Upper Sync Executer. The Upper Synch Executer is located at the BS and constructs the MAC bursts. For type 3 data path, the received payload packet at the MBS Upper Sync Executer (located at the GW) is already pre-processed into the MAC burst, i.e., the mapping of one or more MCIDs to a given MBS Burst has already been done at the ASN-GW.

The data path for the MCBCS is established between the MCBCS Controller/Server and the ASN-GW, and between the ASN-GW and BSs, where each segment may have a different transport strategy. For example, between the MCBCS Controller/Server and the ASN-GW, either unicast or multicast transport can be used; and between the ASN-GW and the BSs (belonging to the same MBS Zone), either unicast or multicast-distribution tree or multicast-based multicast-distribution tree can be implemented. The direction of the data path is downlink only and the data path isn't dedicated to each user but rather shared by all users pre-scribed to the same MCBCS service.

4.5.1 Protocol Stack

4.5.1.1 Type-1 Protocol Stack

The following figure describes the protocol stack for the MCBCS Data Plane.

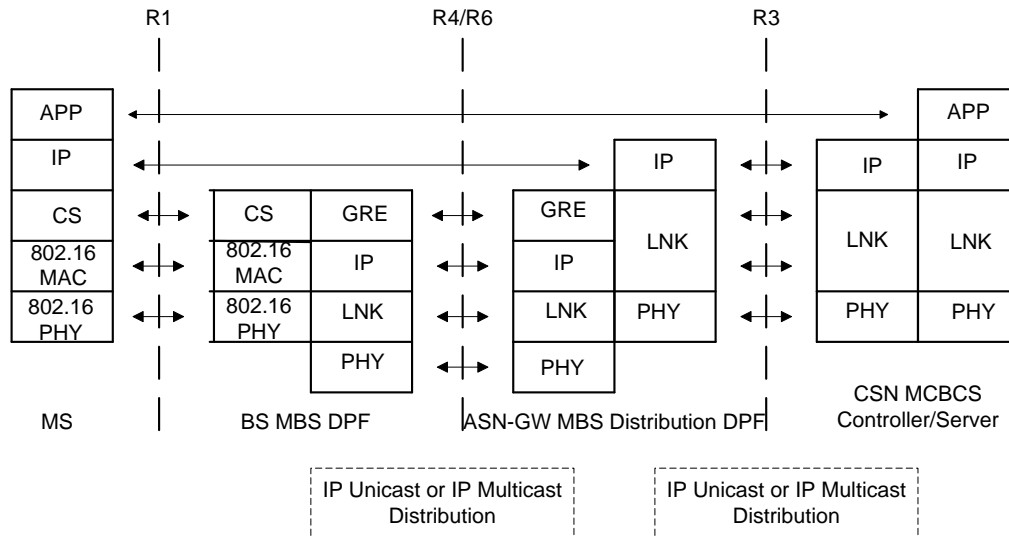


Figure 4-18 : Protocol Stack for Type-1 MCBCS Data Plane

Phase-1 MCBCS specification focuses on the IP-CS based transport. The use of the Eth-CS based transport is FFS.

4.5.1.1.1 IP Transport over R3

The MCBCS Controller/Server sends the content packets based on the delivery rate of the content. The MCBCS Controller/Server may encrypt the content before delivery. For MCBCS Rel-1.5, a content packet is transferred from the MCBCS Controller/Server to the MBS Distribution DPF without any encapsulation over R3. Hence, the NAP shall engineer the WiMAX network with no duplication of the destination IP address.. The destination IP address of the R3 bearer packet is a multicast IP address assigned to the content which is the same multicast IP that is part of the MCBCS service profile for the MS. The mapping between the unicast/multicast IP address with or without the IP port# to the MCBCS content is one-to-one.

In order to receive the R3 bearer packets using IP multicast, the MBS Distribution DPF sends an IGMP Join message to the multicast router located between the ASN and the CSN during the R3 MBS data path setup procedure.

4.5.1.1.2 IP Transport over R1/R4/R6

The MBS Distribution DPF identifies the contents by the destination unicast/multicast IP address and port# of the received R3 packet. For model-B and model-C MBS Sync Function architecture (see section 4.12 for more details), the MBS Distribution DPF takes the type-1 packet processing approach and encapsulates the MBS content into a GRE packet as is, before it is forwarded to the corresponding BSs over the R4/R6 interface for further PHY PDU processing.

The following figure provides a high level view of the type 1 MBS data path processing:

MCBCS-DSx

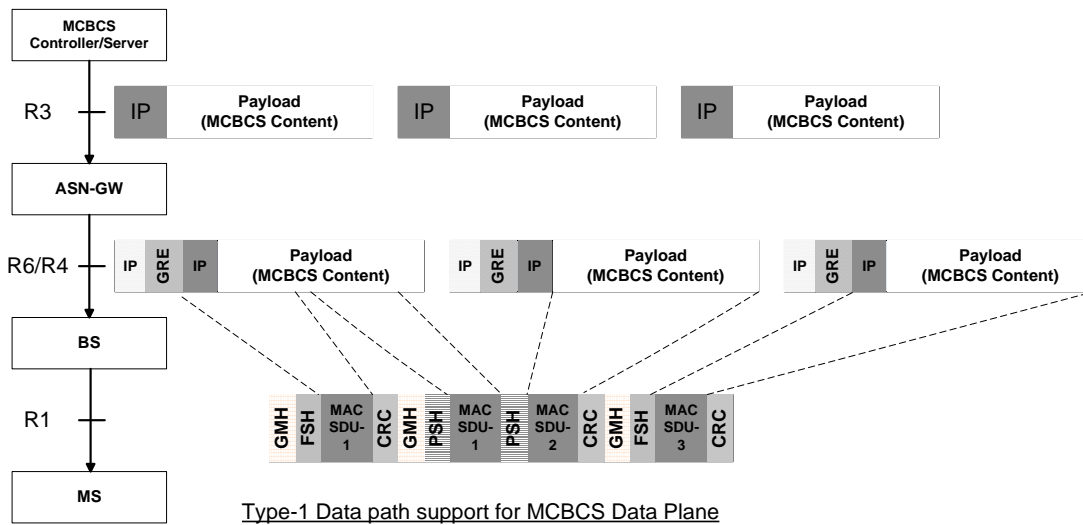


Figure 4-19 : Example of Type-1 MCBCS Data Transfer

4.5.1.2 Type-3 Data Path Protocol Stack

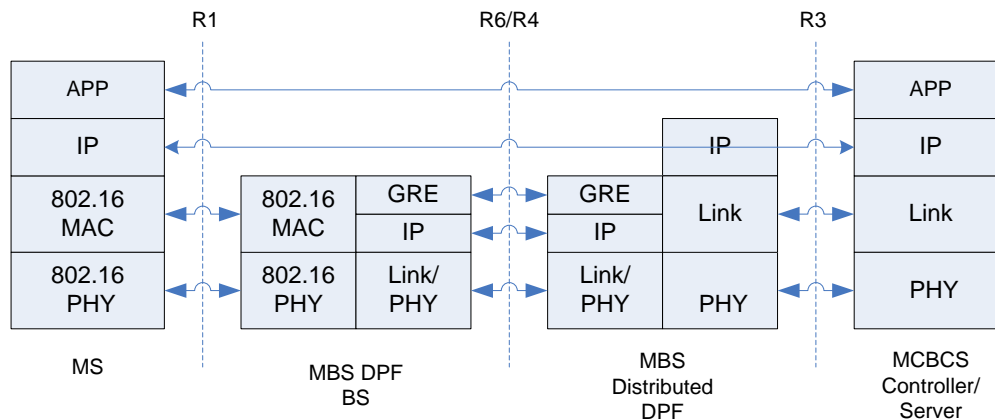


Figure 4-20 : Protocol Stack for Type-3 MCBCS Data Plane

4.5.1.2.1 IP Transport over R3

Same as IP Transport over R3 for Type 1 data path. See section 4.5.1.1

4.5.1.2.2 IP Transport over R1/R4/R6

For model-A MBS Sync Function architecture (see section 4.12 for more details), the upper sync executor and the sync controller are collocated with the MBS Distribution DPF. The Primary MBS Distribution DPF classifies the receives R3 bearer packets and forwards them to the sync controller to generate the rules and from there to the upper sync executor in order to generate the MAC burst that contains one or more MAC PDUs, including the GMH and CRC that are based on the rules from sync controller. The mapping between the MCID and the content is done at the

MCBCS-DSx

sync function. The output generated by the upper sync executor is forwarded to the MBS Distribution DPF. The MBS Distribution DPF encapsulates the packet payload using the GRE header, assigns a sequence number and forwards them to the corresponding BSs over the R4/R6 interface. Once the BS receives the GRE packet, it de-encapsulates the GRE packet, extracts the packet payload and forwards the de-capsulated packet to the lower sync executor at the BS for further PHY PDU processing. The following figures describe the data transmission for a Type 3 Bearer from the functional and packet point of view.

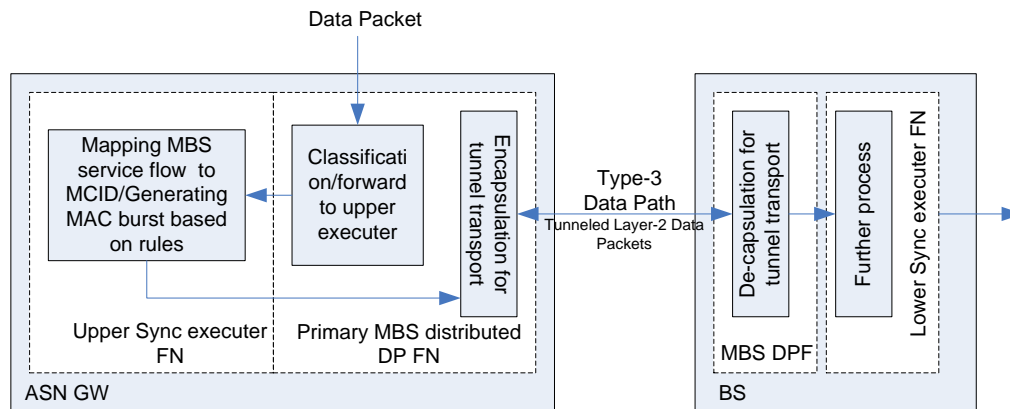


Figure 4-21 : Type-3 Data Path Packet Processing

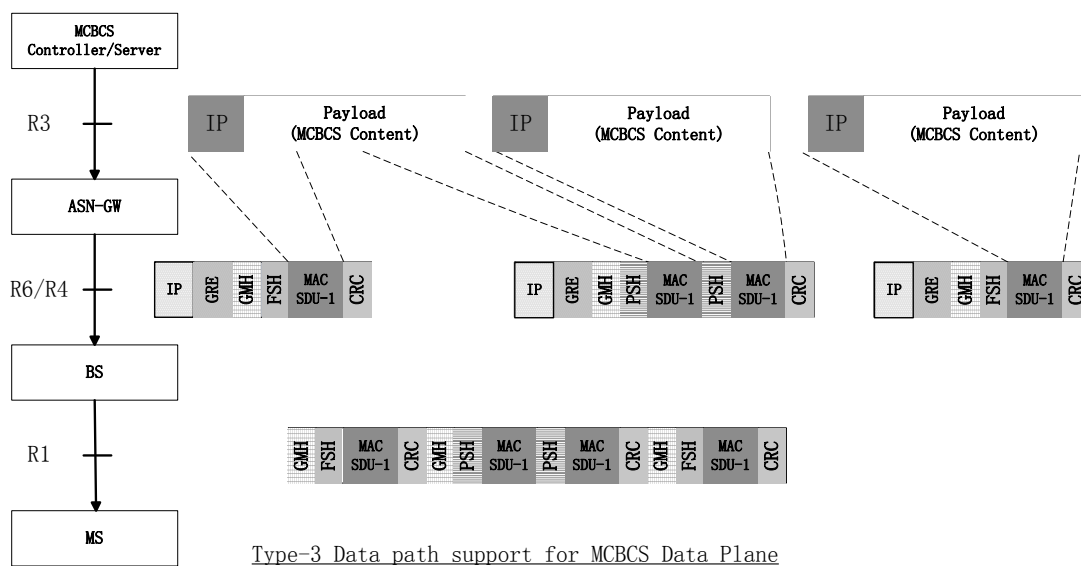


Figure 4-22 : Example of Type-3 MCBCS Data Transfer

4.5.1.3 GRE Encapsulation

The MBS Distribution DPF shall encapsulate the packet with a GRE header and transport it either using multicast or unicast. The GRE protocol is specified by RFC 2784 and extended by 2890. RFC 2890 provides two optional extensions, Key option and Sequence number option. Both options shall be used for transport. The key field depends on the transport mechanism inside the MBS zone. If it is a unicast transport, the BS can uniquely assigns a GRE key,

MCBCS-DSx

however if it is a multicast transport, the GRE key is assigned by the MBS Distribution DPF at the ASN-GW. For the GRE protocol type, the type-3 protocol type shall be 0xFFFFF.

4.5.2 MCBCS Datapath Service Mapping

This section describes how the MCBCS service contents is mapped to the serving MBS DPF.

4.5.2.1 MCBCS Datapath Reference Model

The contents provider creates various media flows and sends them to the MCBCS Controller/Server. The MCBCS Controller/server can combine one or more media flows into a single MCBCS Content based on its policy. The details are out of scope of this document.

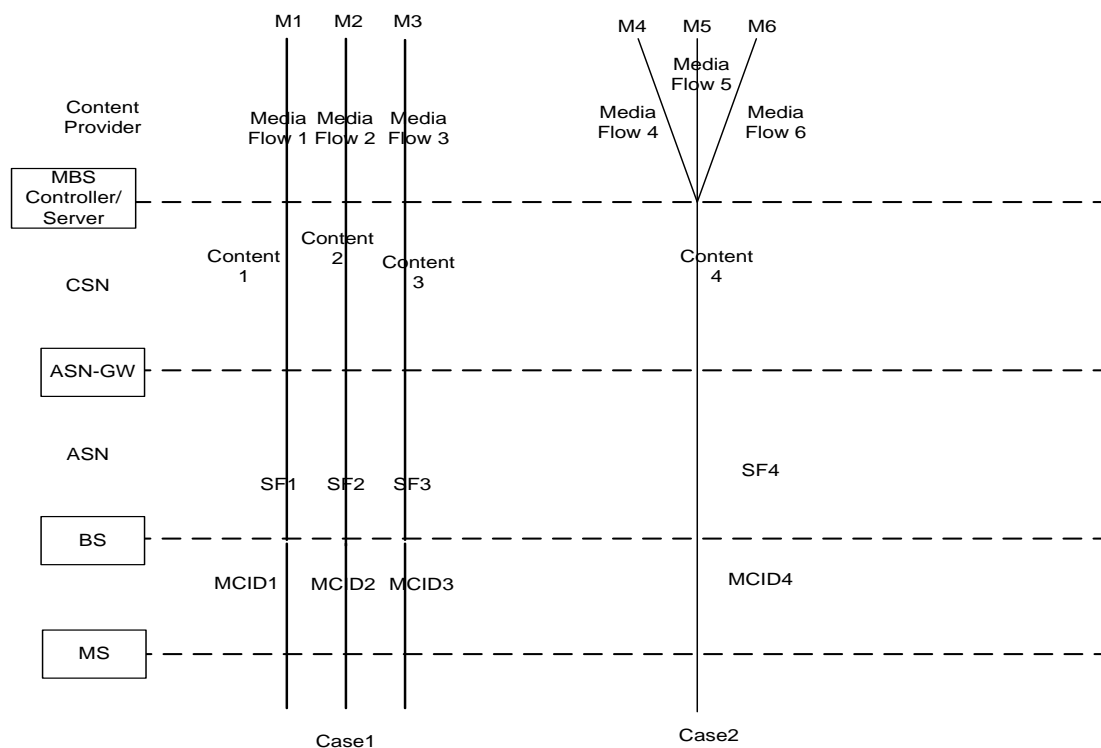


Figure 4-23 : MCBCS Service Data path mapping

MCBCS service data can be mapped as shown in Figure 4-23 in each network entity.

- Case 1: Content provider conveys a media flow to the MCBCS Controller/Server. The ASN maps the MBS content to the service flow and maps the service flow to the MCID.
- Case 2: Content provider conveys media flows to the MCBCS controller/server in the CSN which combines the multiple media flows into a single MCBCS content. The ASN maps the MCBCS content to a service flow with a MCID. Media flow distinguishing is done at the application layer which is out of scope for this specification.

The MCBCS program package is a logical concept from a user point of view and it is identified by a program ID. A MCBCS Program package can contain one or more contents - e.g. CNN, NBC, file transfer. It is a service package that the subscriber subscribes to. The MCBCS Service Flow is a logical view for data transportation and is identified by a PDFID together with the Transmission zone ID that is mapped to a single MCID.

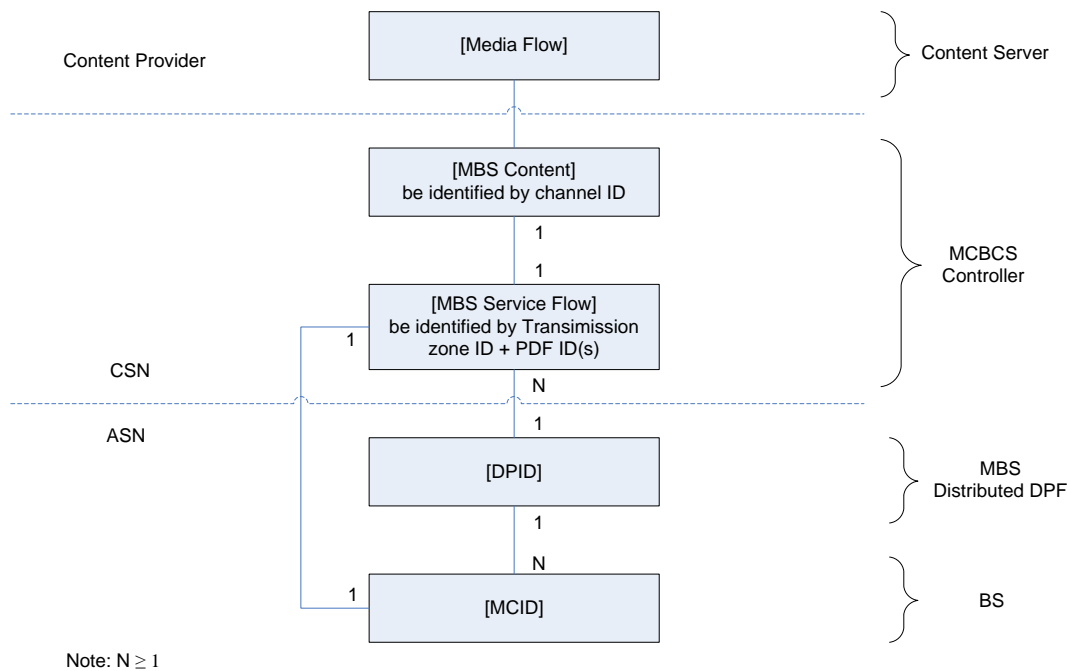


Figure 4-24 : MCBCS Data Plane Object Model

Several relationships are described:

- The relationship between Media Flow and MBS content is based on operator's policy or agreement among the involved operators. This is out of scope for this document.
- The relationship between the MBS content and the MBS service flow is identified by a PDFID and the transmission zone ID mapping is 1:1.
- The relationship between MCBCS service flow and MCID(s) is a 1:1 mapping.
- The relationship between MCBCS service flow and DPID is 1:1 mandatory and optionally N:1. Whether the data path conveys more than 1 MCBCS services flow in an ASN depends on the NAP policy. If the MBS region contains multiple MCIDs, it may use one data path to convey the relationship.
- Since the relationship between the MCBCS service flow and the MCID is 1:1 and one data path may convey more than 1 MCBCS service flows depending on the NAP or other policies, the relationship between the DPID and the MCID is 1:N.

After a successful joining of the MCBCS services, the MS gets content ID, MCID, multicast IP address, and MBS zone ID, etc, and at that point the MS is ready to receive MBS traffic. At the very first step, the MS locates every DL-MAP, decodes it and searches for the MBS-MAP-IE. Once the MS gets an MBS-MAP-IE, it verifies the associated MBS Zone ID. If it matched, the MS then locates the MBS_MAP message according to the physical resource specified in the MBS-MAP-IE as well as in the MBS-DATA-IE. For an MBS-DATA-IE, the MS verifies the multicast CID listed in the MBS-DATA-IE with the allocated multicast CID. The schedule and the incoming downlink MBS traffic can be found in the physical resources specified in that MBS-DATA-IE.

Some mechanisms are provided by the IEEE 802.16-Rev2 specification [3] to ease MBS data reception. For example, the "Next MBS MAP Change Indication" indicates whether the physical resources for the next MBS_MAP message are changed. The "Next MBS No OFDMA Symbols" and the "Next MBS No OFDMA Sub channels" indication help to specify the exact physical location of the scheduled radio resource for the upcoming downlink transmission of the MBS data.

4.5.3 MCBCS Data Path Creation

A MCBCS data path is used to deliver a given MCBCS service in a given MBS zone for all the MSs. The data path is shared by every MSs which are interested in the same MCBCS service or content. The MCBCS data path creation can be pre-configured or it can be triggered by a network event related to a given MCBCS service depending on the network policy such as the trigger by the very first MS joint and/or by the Session Start.

4.5.3.1 Pre-configured Data Path

For static broadcast or some usage scenarios, the association between the MBS Proxy and the MCBCS Controller has already been established. The data path in the MBS zone would have been set up with or without any MS participating in the given MCBCS service, and could already be set up before the service is started. The QoS is also pre-configured. Although the mechanism for the pre-configuration of the necessary data path parameters is out of scope, the GRE key and DPF Identifier pre-configuration SHALL nevertheless be specified.

4.5.3.2 Dynamic Data Path Creation

Dynamic data path creation implies that the data path is not pre-established, but could be triggered by the MCBCS related network events (i.e. triggered by the first MS Join or triggered by a Session Start signaling). In case it is triggered by the first MS Join for the MCBCS service, the MBS Proxy may get the service flow QoS parameters from the Anchor SFA, or it may use the default QoS pre-configuration values, or it may get the service flow QoS parameters from the MCBCS Controller/Server.

The association between the MBS Proxy and the MCBCS Controller/Server can be pre-configured. The method of the pre-configuration between these two entities is out of scope of this specification. In case when the association of the MBS Proxy and the MCBCS Controller/Server is triggered by a network event, the MBS Proxy obtains the MCBCS Controller/Server contact information and possibly also the MCBCS service policy related information from the Anchor SFA. The MBS Proxy then sends a MBS service request message to the MCBCS Controller/Server including the service identification information (e.g. multicast IP address and MCBCS Transmission Zone) indicating it is interested in receiving the given MCBCS service or content as identified. This mechanism can also be used by the MBS Proxy to get service policies from the MCBCS Controller/Server.

Based on the local policy (e.g. triggered by the very first MS joint to receive the service profile for a given MCBCS service from the MCBCS Controller/Server) the MBS Proxy refers to the service parameters that are provided by the AAA server, or provided by the MCBCS Controller/Server, to trigger the establishment of a multicast distribution tree service infrastructure via the support of the corresponding MBS Distribution DPF.

- Establishing the local ASN MCBCS service control and content distribution tree according to the coverage area of the given MCBCS Transmission Zone that is specified in the MCBCS service profile.

Dependening on the ASN local configuration policy and the service policy between the NAP and the serving NSP, and if service continuity is required across the MBS Zones, the anchor MBS Proxy maps the MCBCS Transmission Zone, for a given MCBCS service, into a single or more MBS Zones. If the service continuity is not required, the MBS Zones which support the same MCBCS service, can be managed by one or more MBS Proxies. However, such service mapping decision is an implementation decision that is outside the scope of this specification.

- Never-the-less, if a different MBS Proxy is assigned for another MBS Zone, a different MBS Distribution DPF shall be assigned as well. If that event happens, MBS Proxy triggers the corresponding MBS distribution DPF establishing the R3-binding with the multicast content distribution at the service CSN (e.g. IGMP Join).

Trigger from the Anchor SFA:

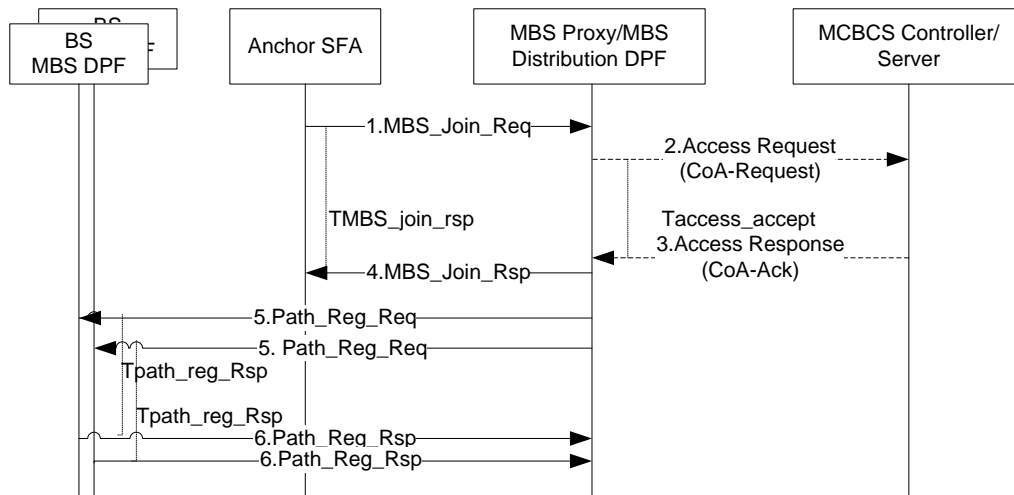


Figure 4-25 : MBS Datapath Creation Triggered by the Anchor SFA

STEP 1:

After the Anchor SFA gets the authorization successful message, the Anchor SFA sends a MBS Join Request message with the service multicast IP address, the optional MCBCS Service Policy, as well as the MCBCS Controller/Server address to the MBS Proxy which is associated with the MCBCS Controller/Server.

STEP 2

If the MBS Proxy would like to get service information from the MCBCS Controller/Server based on the operator policy, the MBS Proxy sends a MCBCS Service Request message (i.e. CoA-Request) to the MCBCS Controller/Server, otherwise, step 2, 3 are omitted.

STEP 3

Upon receiving the Access Request message, the MCBCS Controller/Server sends a MCBCS Access Response (i.e. CoA-Ack) message.

STEP 4

The MBS Proxy then sends a MBS Join Response message to the Anchor SFA with assigned MCID and may include possible QoS attributes which the data path is using.

STEP 5

Based on the network policy, the MBS Proxy triggers the MBS Distribution DPF to create the data path. The MBS Distribution DPF sends a Path_Reg_Req message to every MBS DPFs of all BSs that belong to the same MBS Zone to establish the content distribute tree.

Table 4-19 : Path Register Request Message

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
>SF Info		M	

IE	Reference	M/O	Notes
>>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS service flow and this TLV is common to every MS for that packet flow
>>MCBCS Transmission zone ID	5.2.6	O	
>>MCID	5.2.8	O	MCID as defined on R1
>>MBS zone ID	5.2.9	M	MBS zone ID as defined on R1
>>Reservation Action	5.3.2.151	O	SHALL be set to “Create, Admit & Activate”
>>QoS	5.3.2.141	O	Indicates the QoS parameters of the particular MCBCS service.
>>DP Info	5.3.2.45	M	
>>>DP ID	5.3.2.44	O	
>>>MBS Distribution DPF ID	5.2.57	M	Identifier of primary distributed DPF in that MBS zone
>>>DP Type		M	Identify type 1 or type 3 data path
>>>Transport Type		O	Describes the data plane is unicast transport or multicast transport inside of MBS zone
>>>Transport Mcast IP address		CM	This TLV shall be included if dataTransport type is multicast transport
>>>DP Recovery Mechanism		O	Mechanism to recovery data packet
>Sync Info		O	
>>Sync controller ID		O	
>>Sync rule Mcast IP		O	This TLV shall be included if the control plane is unicast transport or multicast transport inside of MBS zone
>>Sync Rule Recovery Mechanism		O	Mechanism to recovery sync rules
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

STEP 6

After setting up the data path, each MBS DPF at each BS replies with a Path_Reg_Rsp message back to the MBS Distribution DPF.

Table 4-20 : Path Register Response Message

IE	Reference	M/O	Notes
Failure Indicator	5.3.2.69	O	
Registration Type	5.3.2.145	M	
>SF Info		M	
>>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS service flow and this TLV is common to every MS for that packet flow
>>MCBCS Transmission zone ID	5.2.6	M	
>>MCID	5.2.8	O	MCID as defined on R1
>>MBS zone ID	5.2.9	M	MBS zone ID as defined on R1
>>Reservation Result	5.3.2.152	O	
>>QoS	5.3.2.141	O	Indicates the QoS parameters of the particular MCBCS service.
>>DP Info	5.3.2.45	M	
>>>DP ID	5.3.2.44	O	
>>>MBS Distribution DPF ID	5.2.57	M	Identifier of primary distributed DPF in that MBS zone
>>>DP Type		M	Identify type 1 or type 3 data path
>>>Transport Type		O	Describes the data plane is unicast transport or multicast transport inside of MBS zone
>>>Transport Mcast IP address		O	This TLV shall be included if dataTransport type is multicast transport
>>>DP Recovery Mechanism		O	Mechanism to recovery data packet
>Sync Info		O	
>>Sync controller ID		O	
>>Sync rule Mcast IP		O	This TLV shall be included if the control plane is unicast transport or multicast transport inside of MBS zone
>>Sync Rule Recovery Mechanism		O	Mechanism to recovery sync rules
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

1

2 **Trigger from MCBCS Controller/Server:**

MCBCS-DSx

The MCBCS data path establishment may also be triggered by a session start signaling message from MCBCS Controller if the data path has not been pre-established and the MCBCS Controller has data ready to send. The following figure describes the procedure for session start trigger.

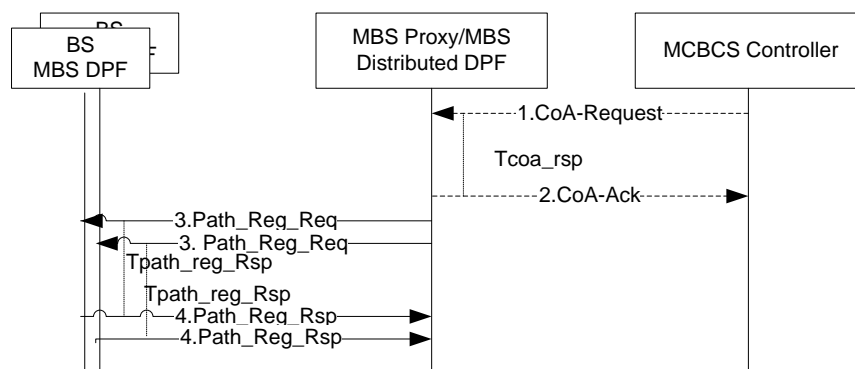


Figure 4-26 : MBS Datapath Creation Triggered by MCBCS Controller

STEP 1

The MCBCS Controller sends a CoA message to indicate a Session Start along with the MCBCS service information to the MBS Proxy. The MBS Proxy Addresses can be pre-configured in the MCBCS Controller. The MCBCS Controller can get some MBS Proxy Addresses by the association procedure also.

STEP 2

Upon receiving a CoA-Request message from the MCBCS Controller, the MBS Proxy sends a CoA-Ack message to the MCBCS Controller and also triggers the MBS Distribution DPF to set up the data path.

STEP 3

If no data path exists, the MBS Distribution DPF sends a Path_Reg_Req message to the MBS DPF at each BS to establish a data path.

Please refer to Table 4-19 for the details of Path_Reg_Req message.

STEP 4

After the data path setup the MBS DPF at each BS sends a Path_Reg_Rsp message back to the MBS Distribution DPF.

Please refer to Table 4-20 for the detail of Path_Reg_Rsp message.

4.5.4 Data Path Modification

MCBCS data path can be modified if new MBS service flow is added/deleted onto the data path, or new settings are required such as new QoS.

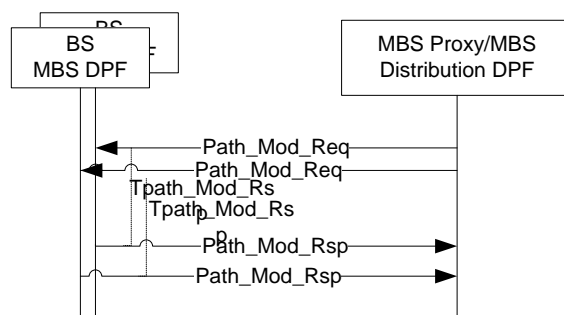


Figure 4-27 : MBS Data Path Modification

STEP 1

The MBS Proxy triggers the MBS Distribution DPF to modify the data path. The MBS Distribution DPF sends a Path_Mod_Req message to every MBS DPFs in all the BSs that belongs to the same MBS Zone to modify some of the parameters in MBS distribute tree. If it is for the deletion of a MBS service flow on the data path, the Path_Mod_Req message shall mark the Reservation Action TLV with “delete” to indicate that a PDF is deleted.

Table 4-21 : Path Modification Request Message

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
BS Info		M	
>BS ID	5.3.2.25	M	
>SF Info		M	
>>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS service flow and this TLV is common to every MS for that packet flow
>>MCBCS Transmission zone ID	5.2.6	M	
>>MCID	5.2.8	O	MCID as defined on R1
>>Reservation Action	5.3.2.151	O	SHALL be set to “Create, Admit & Activate”
>>QoS	5.3.2.141	O	Indicates the QoS parameters of the particular MCBCS service.
>>DP Info	5.3.2.45	M	
>>>DP ID	5.3.2.44	M	Data path Identifier
>>>MBS Distribution DPF ID	5.2.57	M	Identifier of primary distributed DPF in that MBS zone
>>>Transport Type		O	Describes the data plane is unicast transport or multicast transport inside of MBS zone

IE	Reference	M/O	Notes
>>>Transport Mcast IP address		O	This TLV shall be included if dataTransport type is multicast transport

STEP 2

Upon receiving the Path_Mod_Req message, The MBS_DPF at the BS sends a Path_Mod_Rsp message to the MBS Distributed DPF

Table 4-22 : Path Modification Response Message

IE	Reference	M/O	Notes
Failure Indicator	5.3.2.69	O	
Registration Type	5.3.2.145	M	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	
>SF Info		M	The service flow for MCBCS which is the same to every MS in that MBS zone
>>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS service flow and this TLV is common to every MS for that packet flow
>>MCBCS Transmission zone ID	5.2.6	M	
>>DP Info	5.3.2.45	M	
>>>DP ID	5.3.2.44	M	
>>>MBS Distribution DPF ID	5.2.57	M	Identifier of primary distributed DPF in that MBS zone
>>Reservation Result	5.3.2.152	O	

4.5.5 Data Path Deletion

MCBCS data path can be deleted if all the packet flows are deleted on that data path. The deletion of service flow and/or data path results in the removal of the service flow context.

Session stop signaling message from the MCBCS controller is one of the triggers for the removal of a service flow context and the data path.

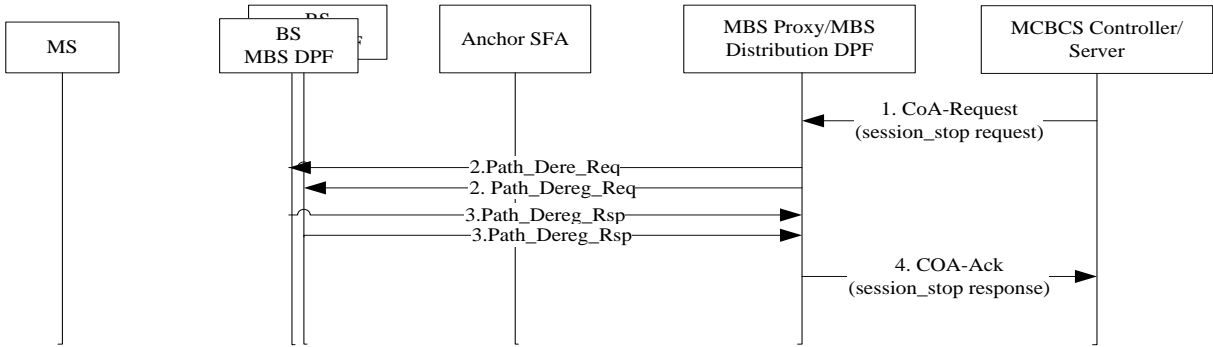


Figure 4-28 : MBS Data Path Deregistration

STEP 1

The MCBCS Controller/Server sends a CoA-Request message to the MBS Proxy to indicate that a particular packet flow is stopped.

STEP 2

If there is only one packet flow on that data path, the MBS Proxy triggers the MBS Distribution DPF deletes the data path by sending MBS De-registration Request Message..

Table 4-23 : Path De-registration Request Message

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	
>SF Info		M	The service flow for MCBCS which is the same to every MS in that MBS zone
>>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS service flow and this TLV is common to every MS for that packet flow
>>MBS Transmission zone ID	5.2.6	M	
>>DP Info	5.3.2.45	M	
>>>DP ID	5.3.2.44	M	
>>>MBS Distribution DPF ID	5.2.57	M	Identifier of primary distributed DPF in that MBS zone

STEP 3

Upon receiving the Path_Dereg_Req message, The MBS_DPF at the BS sends a Path_Dereg_Rsp message correspondingly to the MBS Distribution DPF

Table 4-24 : Path De-registration Response Message

IE	Reference	M/O	Notes
Failure Indicator	5.3.2.69	O	
Registration Type	5.3.2.145	M	
BS Info	5.3.2.26		
>BS ID	5.3.2.25	M	
>SF Info	5.3.2.185	M	The service flow for MCBCS which is the same to every MS in that MBS zone
>>PDF ID		M	This TLV along with transmission zone ID indicates the particular MCBCS channel, This TLV is unique in Transmission zone to identify the particular MCBCS service flow and this TLV is common to every MS for that packet flow
>>MBS Transmission zone ID	5.2.6	M	
>>DP Info	5.3.2.45	M	
>>>DP ID	5.3.2.44	M	
>>>MBS Distribution DPF ID	5.2.57	M	Identifier of primary distributed DPF in that MBS zone

STEP 4

Upon receiving Path_Dereg_Rsp message, the MBS proxy sends a CoA-Ack message to MCBCS Controller/Server to indicate that the deletion is successful

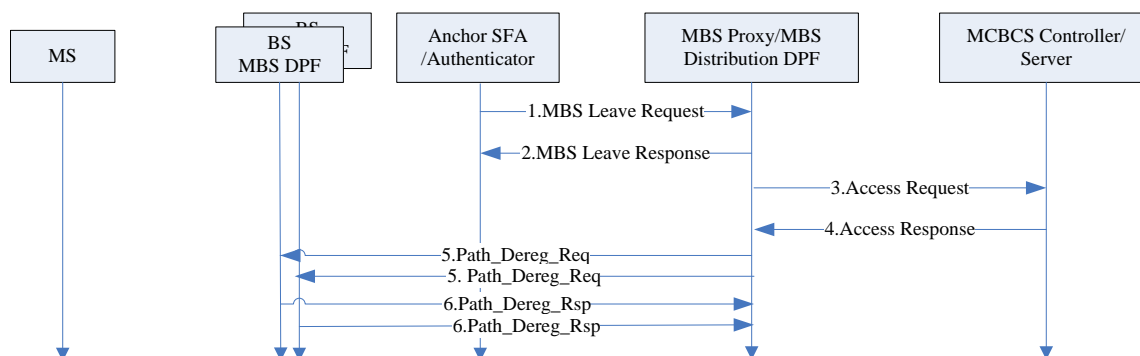


Figure 4-29: Data path deletion triggered by the last MS exit

MCBCS-DSx

Data path deletion may also be triggered by the very last MS exit if the MBS Proxy is a centralized MBS Proxy for the serving access network . The procedure is as follows:

STEP 1

The Anchor SFA which collocates with the Anchor Authenticator sends a MBS Leave Request message to the MBS Proxy to indicate that the MS is going to leave the MCBCS service.

STEP 2

Upon receiving the MBS Leave Request, the MBS Proxy sends a MBS Leave Response message to the Anchor SFA and updates the count of the MSs which are associated with the corresponding MCBCS session.

STEP 3

If the MBS Proxy recognizes that it is the very last MS who subscribes to the MCBCS service are leaving the given MCBCS service, it sends Access Request message to the MCBCS Controller/Server to initiate the termination of the MCBCS service which may trigger the termination of the association between the MBS Proxy and the MCBCS Controller/Server dependent on the operator policy

STEP 4

The MCBCS Controller/Server sends Access Response to the MBS Proxy to confirm the termination the service. If the termination of the association between the MBS Proxy and the MCBCS Controller/Server is required, the MCBCS Controller/Server will also include such request in the response.

STEP 5

If there are no other MCBCS services associated with the corresponding data path, the MBS Proxy will trigger the MBS Distribution DPF to delete the corresponding data path by sending path De-registration Request Message to all BSs which are belonged to the same MBS Zone.

STEP 6

The MBS_DPF at the BS sends a Path_Dereg_Rsp message accordingly to the MBS Distribution DPF

4.5.6 Error Handle Procedures**4.5.6.1 Timer MAX Retries**

This Timer, $T_{MBS_Join_Rsp}$, is started by ASN associated with the Anchor SFA after transmission of *MBS_Join_Req* message to the MCBCS Proxy and is stopped upon reception of *MBS_Join_Rsp* message.

Table 4-25 : Network Exit Timer Values

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
$T_{MBS_Join_Rsp}$	TBD		TBD
$T_{path_reg_Rsp}$	TBD		TBD
$T_{path_mod_Rsp}$	TBD		TBD
$T_{path_Dereg_Rsp}$	TBD		TBD
T_{DM_Ack}	TBD		TBD

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
T_{CoA_Ack}	TBD		TBD
T_{access_accept}	TBD		TBD

4.5.6.2 Timer Expiry

Table 4-26 shows the details of the corresponding action(s) associated with timer expiry. Upon each timer expiry, if maximum retries has not exceeded, the related message is retransmitted and timer is restarted. Otherwise corresponding action(s) should be performed as indicated in Table 4-26.

Table 4-26 : Actions after Timer Max Retry

Timer	Entity where Timer Started	Action(s)
$T_{MBS_Join_Rsp}$	Anchor SFA.	Establish the unicast service flow – by unicast as default.
$T_{path_reg_Rsp}$	MBS distributed DPF	Data path will not be set and establish the unicast service flow by default.
$T_{path_mod_Rsp}$	MBS distributed DPF	Data path will not be modified
$T_{path_Dereg_Rsp}$	MBS distributed DPF	Data path will not be tearing down

4.5.7 RADIUS Related Message and Attributions

4.5.7.1 RADIUS Message between the ASN NAS and CSN for the MCBCS Session Management

The details of the RADIUS MCBCS service attributes, which are required to support the MCBCS session management messaging exchanged between the MBS Proxy and MCBCS Controller/Server are provided in section 5.3.1.

4.6 Mobility Management

4.6.1 MCBCS Service Continuity Handover Support for Multi-BS MBS

According to the IEEE 802.16-Rev2 specification [3], the MS can continue to maintain the reception of the MCBCS DL transmission within the MBS Zone. The Network should maintain the on-going MCBCS program content DL transmission regardless of the MS mode of operation (i.e. active, sleep mode or idle mode); or the MBS type: broadcast or Multicast. This implies that within the MBS Zone, the MCID(s) and MBS Zone ID remain the same.

Once the MS is attached to the ASN and registered with one or more MBS services, all the MCBCS related context information (e.g. MCID(s), MBS Zone ID(s), MCBCS Transmission Zone ID, MBS PDFID(s), Anchor MBS Proxy/MBS Distribution DPF, MCBCS service policy, etc.) together with the other MS context is preserved and accessible by the serving HO function.

MCBCS-DSx

It is the responsibility of the MBS Sync Controller to schedule the MCBCS DL transmission. Therefore, when the MBS Sync Controller is provided by the MBS Distribution DPF with the incoming MCBCS programming contents, the MCBCS Sync Controller combines its prior knowledge of the available resource, configuration of the MBS permutation zone and the QoS requirements of the given MCBCS program with the latest information of the incoming MCBCS programming contents to schedule the MCBCS DL transmission. The Sync Controller also programs the MBS_MAP_IE, MBS_MAP message and MBS_DATA_IE accordingly to support the service continuity as specified in [3].

It is the MS's responsibility to examine and to refer to the MCBCS DL transmission schedule advertised via the MBS_MAP_IE, MBS_MAP message and MBS_DATA_IE as specified in [3] to receive the MCBCS programming contents and to follow the DL MCBCS transmission schedule accordingly.

To support the up-coming and on-going MCBCS operation within the ASN, the MBS Sync Controller continues to update the DCD, the MBS_MAP_IE in the DL_MAP and possibly the MBS_MAP message to advertise the MBS service and the MCBCS DL transmission. In particular, the MBS Sync Controller leverages the MBS_MAP_IE, MBS_MAP message and MBS_DATA_IE to schedule the on-going and up-coming DL transmissions within and across the MBS Zones for the MS so that it can leverage such information to determine the next data reception interval. For more information regarding the MBS Zone transition for service continuity can be referred to section 9.12.1 for more detail.

As described in [3], the design of the MBS_MAP_IE, MBS_MAP message and the MBS_DATA_IE supports 2-level of granularity for the daisy chaining:

- Inter MBS-MAP messages
- Inter MBS bursts

The programming of the MBS_DATA_IE should be agnostic to the MS that can be operating at the active, sleep or idle mode while traversing within the same MBS zone.

Within the MBS Zone, dependent whether it is macro diversity or frame-level coordination enabled within the MBS Zone, the MCBCS programming contents may not necessarily be contained in the MBS permutation zone at the exact location of the DL subframe. The MCBCS programming contents is always scheduled at the same downlink subframe for all BSs belonged to the same MBS Zone for both cases. As long as the MCID(s) and MBS Zone ID remain the same, the MS can retrieve the expected MCBCS programming contents through the support of the MBS_MAP_IE, MBS_MAP message and MBS_DATA_IE as described above. For more details on the definitions and operation of the micro diversity and frame-level coordination refer to [3].

For the inter-MBS Zone transition within the MCBCS Transmission Zone, there are two options to choose from dependent the type of MBS services:

Option-1: maintaining frame-offset coordination to maximize service continuity

Option-2: basic zone switching without any synchronization

When the MS recognizes that it has crossed the MBS Zone boundary and that the Target BS is no longer part of the serving MBS Zone, the MS initiates the handover procedure in order to obtain the corresponding new target MBS Zone related parameters in order to resume MCBCS downlink reception.

The inter-MBS Zone handover support is only expected if the same MCBCS service is spanning multiple MBS zones that belong to the same MCBCS Transmission Zone and the support for service continuity is required. In addition, through either the pre-configuration or the service establishment operation (e.g. MBS data path establishment), the MBS zone neighbors are also provided to the BS for each MBS Zone that the BS supports. MBS Zone neighbors are the immediate neighboring zones to the current serving MBS Zone for a MCBCS service that is current serving the MS. More detailed concept of the MBS Zone neighbor as supported by [3] can be found in Annex-C.

For the intra or inter MBS Zones handover support, there are several basic scenarios to consider: MS-initiated controlled handover, BS-initiated Controlled handover and Un-controlled handover.

The following sections provided more details regarding the MCBCS handover mobility support for intra-MBS Zone, and inter-MBS Zone of which the operation can be MS-initiated and BS-initiated.

4.6.2 Intra MBS Zone

While the MS is in the active mode and the MS has joint the MBS service, regardless where there is an on-going MCBCS downlink transmission or not, the MS continues to monitor the MOB_NBR_ADV to determine whether the target preferred BS belongs to the same MBS Zone. Prior to the handover preparation phase, if the Target BS supports the same MBS Zone ID as the current serving/anchor BS, the MS recognizes that it is still within the same MBS zone. If there is on-going MCBCS downlink transmission, the MS should refer to part of or all the information in the DCD, DL_MAP, MBS_MAP_IE, MBS_MAP message as well as the MBS_DATA_IE to receive the MCBCS downlink transmission. Within the same MBS Zone, the MS can continue to receive the MCBCS programming contents without registering with other BS within that MBS Zone.

The existing handover procedures for the unicast service flow is not impacted by the intra-MBS Zone transition, with the understanding that, all the MBS related service parameters (e.g. MBS Proxy / anchor MBS Distribution DPF IDMCBCS Transmission Zone ID, DPFID(s), MBS Zone ID, MCID(s), etc.) are also part of the MS's context that are required to be passed from the serving BS to the Target BS(s).

4.6.3 Inter MBS Zone

4.6.3.1 Fully Controlled HO for Inter-MBS Zones Mobility

While the MS is in the active mode and the MS has joined the MBS service, regardless there is on-going DL MCBCS transmission or not, the MS continues to monitor the MOB_NBR-ADV to determine whether the target preferred BS belongs the same MBS Zone or not. Prior to handover preparation phase, if the potential Target BS supports a different MBS Zone as the current Serving BS, MS recognizes that it is approaching the boundary of the serving MBS Zone. According to the [3], the MS is required to trigger the handover procedure to retrieve the new target MBS Zone parameters to resume the MCBCS downlink transmission.

4.6.3.1.1 HO Preparation Phase

When the MS recognizes the potential Target BSs in the Target ASNs don't belong to the same serving MBS Zone, it SHALL initiate the MOB_MSHO-REQ to the Serving ASN. Once the MOB_MSHO-REQ message is received, and if the network policy of the MCBCS Service Continuity Indicator is set to "1" (i.e. enabled), the Serving ASN SHALL initiate a handover to one or more selected Target ASNs that supports the same MCBCS service in the MBS Zone neighborhood of the current serving MBS Zone of the MS. The selected candidate Target ASNs may be the entire or the subset of the candidate Target ASNs which are provided by the MS. The serving ASN sends an R4 *HO_Req* message to the selected Target ASN over the R4 interface.

If the MCBCS Service Continuity Indicator is set, however, none of the candidate Target ASNs of the Target BSs provided by the MS serves the same MCBCS service, the Serving ASN may reject the HO request from MS and trigger the Network Initiated HO procedure towards the alternate Target ASN that is part of the MBS Zone neighbor of the serving MBS Zone of the MS. See Network Initiated HO in section 4.6.3.1.1.3 for more details.

If the MCBCS Service Continuity Indicator is not set, then the selection of the candidate Target ASNs will not be based on the consideration of the MBS Zone neighbors. Consequently, the MCBCS service continuity is not warrant after the handover operation.

The rest of the HO procedure during the HO preparation phase stays the same as they are described in section 4.7.2.1 in [5].

4.6.3.1.1.1 R4 Message Definitions for HO Preparation Phase

This section describes the R4 message definitions for the HO Preparation Phase.

Table 4-27: HO REQ

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	
Registration Type	5.3.2.145	O	This SHALL be included when Data Path Pre-reg is piggybacked.
MS Info	5.3.2.103	M	
>NSP ID	5.3.2.368	O	NSP identifier. Used to help distinguish the R4 and R6 tunnels for a specific NSP.
>Anchor ASN GW ID	5.3.2.10	O	Identifies the node that hosts the Anchor DP Function in the Anchor ASN. Included if the originator of <i>HO_Req</i> does not host the Anchor DP Function for the MS.
>Authenticator ID	5.3.2.19	O	Identifies the node that hosts Authenticator and Key Distributor Function. Included if the security context is not included in the message; included if the originator of the <i>HO_Req</i> does not host the Authenticator and Key Distributor Function for the MS.
>SF Info (one or more)	5.2.13	O ¹	
>> SF ID		CM	The identifier of service flow
>> MCID	5.2.8	CM	The multicast CID, refer to [3]
>> MCBCS Transmission Zone ID	5.2.6	CM ²	The identifier of MCBCS Transmission Zone
>> MBS Zone ID	5.2.9	CM	The identifier of MBS Zone, refer to [3]
>> PDFID		CM ²	The identifier of packet data flow;
>> MCBCS Service Continuity Indicator	5.2.15	CM	The flag indicate service continuity is required or not
>Anchor MM Context	5.3.2.11	O	The TLV MAY be included in order to optimize FA Relocation to the Target ASN after HO. If included, notifies the Target ASN that FA relocation to the Target ASN will be initiated after HO. The Target ASN MAY use it to decide whether or not to accept the HO.
Note: the other TLVs is same as with Table 4-64 in NWG Stage-3 Version 1.3.0			

Notes:

- Here SF Info is for MBS service flow only; SF Info of unicast service flow is same with Table 4-64 in [5]
- PDFID shall be together with MCBCS Transmission Zone to uniquely identify a service flow of MBS.

4.6.3.1.1.2 MS Initiated HO Preparation Phase

Section 4.7.2.1 in [5] needs to be update to show a MS Initiated HO Preparation scenario for supporting MCBCS mobility management as well. However, most of the HO procedures are still applied.

The changes to the existing procedures as specified in figure 4-57 in section 4.7.2.1.2 in [5] is given below.

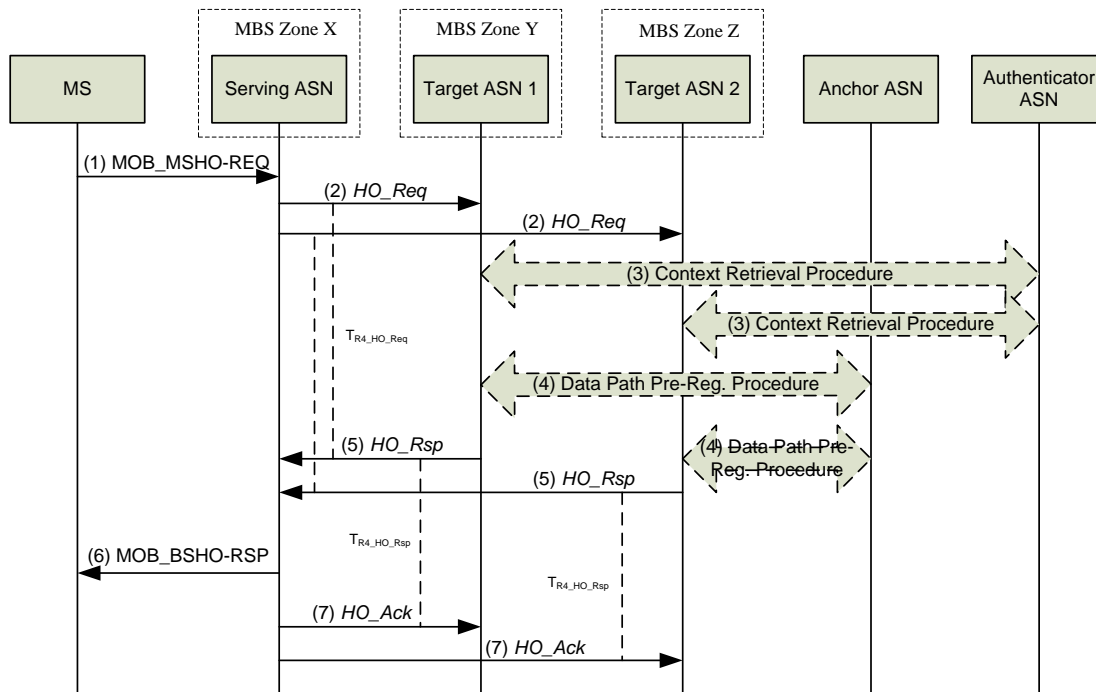


Figure 4-30 : Successful HO Preparation Phase

STEP 1

Prior to the handover preparation phase, the MS examines the MBS Zone ID(s) of Target BS(s) in the Target ASNs via the MOB_NBR_ADV message previously obtained from the current serving/anchor BS. If the Target BS does not support the same serving MBS Zone, the MS recognizes that it is approaching a different MBS Zone, and it triggers the handover procedure by issuing the MOB_MSHO_REQ message towards the Serving ASN. The MS lists potential Target BS(s) in the Target ASNs that meet the HO trigger criteria (e.g. relative CINR or RSSI threshold, etc.).

STEP 2

Once the MOB-MSHO_REQ message is received, and if the network policy of the MCBCS Service Continuity Indicator is set to "1" (i.e. enabled) for the given MCBCS service, the Serving ASN selects only the Target ASNs that supports the same MCBCS service. The selected candidate Target ASNs may be the entire or the subset of the candidate Target ASNs which are provided by the MS. The Serving ASN sends an R4 HO_Req message to each Target ASN over the R4 interface and starts timer T_{R4_HO_Request} for each message. The message includes an Authenticator ID TLV that points to the Authenticator/Key Distributor function at the Authenticator ASN and the Anchor ASN GW ID of the Anchor Data Path function at the Anchor ASN.

In addition, the SF Info of MBS service as part of the MS context is forwarded to the Target ASN. Note that, the MS's context regarding the SF Info of MBS service could be transfer by R4 HO_Req during HO Preparation phase or by R4 HO_Cnf during HO Action phase.

STEP 3 ~ STEP 7

No changes.

4.6.3.1.1.3 Network Initiated HO Preparation Phase

Inter-ASN message transactions associated with the Network Initiated HO Preparation Phase are identical to the transactions associated with the MS Initiated HO Preparation Phase. The difference is in the air interface transactions. Handover is triggered by the internal logic in the Serving ASN without receiving any handover related messages initiated by the MS. With the exception that, when the Network Initiated HO is triggered by the MS crossing the serving MBS Zone, and if the MBS Service Continuity Indicator is set to “1” (i.e. enabled), the Serving ASN should select the neighbor Target ASN which serve the same MBS service for the given MS. The Network Initiated HO Preparation Phase ends with sending MOB_BSHO-REQ to the MS.

If the MS rejects the Target ASN(s) offered by the Serving ASN, the same procedures as described in Figure 4-71 in section 4.7.2.4 in [5] apply.

Section 4.7.2.1 in [5] is modified to show the Network Initiated HO Preparation scenario for supporting inter-MBS Zone handover procedures, which is identical to the Scenario discussed in section 9.6.3.1.1.2 from the networking point of view.

The changes to the existing procedures as specified in Figure 4-60 in section 4.7.2.1.5 in [5] is given below.

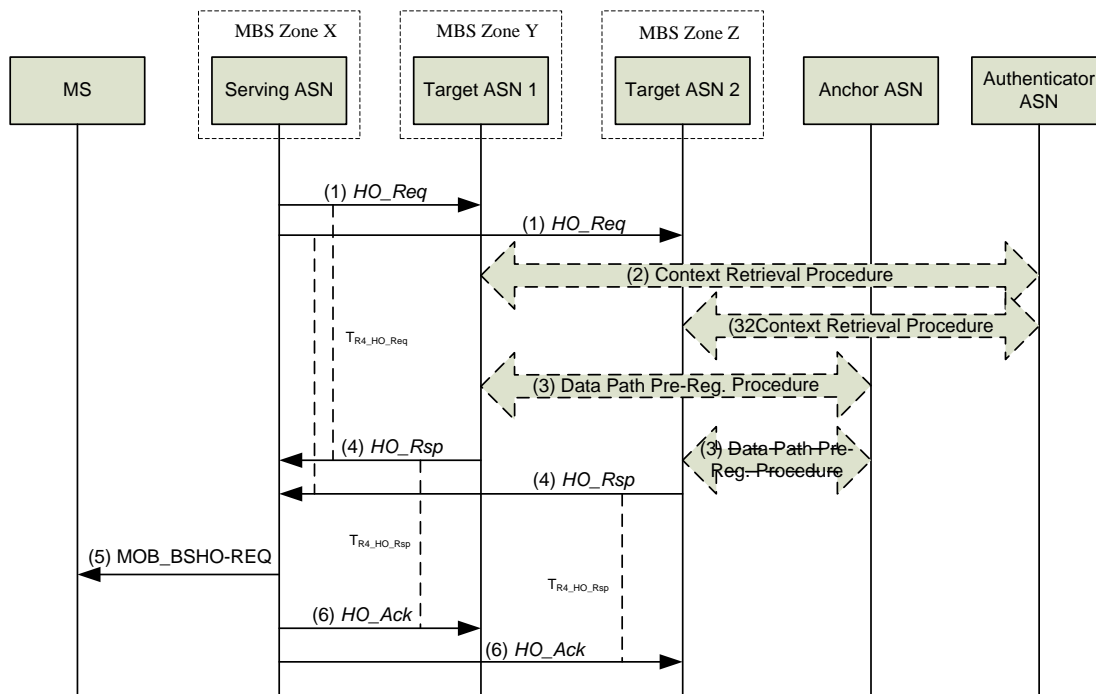


Figure 4-31: Successful HO Preparation Phase for Network-initiated HO

STEP 1

If the network policy of the MCBCS Service Continuity Indicator is set to “1” (i.e. enabled) and the MS is crossing the serving MBS Zone, the Serving ASN SHALL initiate a handover to the neighbor Target ASNs which support the

same MCBCS service in the neighbor MBS Zone. The Serving ASN sends an R4 *HO_Req* messages to each Target ASN over the R4 interface and starts timer $T_{R4_HO_Req}$ for each message. The message includes an Authenticator ID TLV that points to the Authenticator/Key Distributor function at the Authenticator ASN and the Anchor ASN GW ID TLV of the Anchor DP function at the Anchor ASN.

In addition, the MS's context regarding the SF Info of MBS service is forwarded to the Target ASN. Note that, the MS's context regarding the SF Info of MBS service could be transfer by R4 *HO_Req* during HO Preparation phase or by R4 *HO_Cnf* during HO Action phase.

STEP 2 ~ STEP 6

No changes.

4.6.3.1.1.4 HO Preparation Phase Error Conditions

This section describes error conditions associated with the HO Preparation Phase.

An additional error handling case is required comparing to section 4.7.2.1.8 in [3], which is described as the following.

4.6.3.1.1.4.1 No Target ASN support the same MCBCS service

In the case of MS Initiated handover, upon receipt of the *MOB_MSHO-REQ* message, if the MCBCS Service Continuity Indicator is set to "1" (i.e. enabled) and the none of potential Target ASNs that are provided by the MS is able to support the same MCBCS service, the Serving ASN MAY initiate the R4 *HO_Req* message to a different Target ASN. If the Serving ASN does not re-send the R4 *HO_Req* message, or if all subsequent Target ASNs cannot support the same MCBCS service, the Serving ASN SHALL send a *MOB_BSHO_RSP* with mode = 0b111 to the MS.

4.6.3.1.2 HO Action Phase

In general, the same procedure as described in section 4.7.2 in [5] applies, with the additional procedure to the successful HO operation to indicate that when the MS receives the *RNG-RSP* with the updated MBS Zone parameters, the MS can then resume the MCBCS programming contents reception by referring to the DCD, *DL_MAP*, *MBS_MAP_IE*, *MBS_MAP* message and the *MBS_DATA_IE* based on the procedures as described in [3].

4.6.3.1.2.1 R4 Message Definitions for HO Action Phase

This section describes the R4 message definitions for the HO Action Phase.

Table 4-28 : HO Cnf (HO Confirm Type is Confirm or Unconfirm)

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	
HO Confirm Type	5.3.2.76	M	
MS Info	5.3.2.103	M	

IE	Reference	M/O	Notes
>Authenticator ID	5.3.2.19	O	MAY be included if it is not sent during the HO Preparation phase.
>Anchor ASN GW ID	5.3.2.10	O	MAY be included if it is not sent during the HO Preparation phase.
>SF Info (one or more)	5.2.13	O ¹	
>> SF ID		CM	The identifier of service flow
>> MCID	5.2.8	CM	The multicast CID ,refer to [3]
>> MCBCS Transmission Zone ID	5.2.6	CM ²	The identifier of MCBCS Transmission Zone
>> MBS Zone ID	5.2.9	CM	The identifier of MBS Zone, refer to [3]
>> PDFID		CM ²	The identifier of packet data flow;
>> MCBCS Service Continuity Indicator	5.2.15	CM	The flag indicate service continuity is required or not
>Anchor MM Context	5.3.2.11	O	The TLV MAY be included, for Unconfirmed Type and to Targets that were not sent HO_Req during the Preparation phase, in order to optimize FA Relocation to the Target ASN after HO. If included, notifies the Target ASN that FA relocation to the Target ASN will be initiated after successful HO. The Target ASN MAY use it to decide whether or not to accept the HO.
Note: the other TLVs is same as with Table 4-74 in NWG Stage-3 Version 1.3.0			

Notes:

- Here SF Info is for MBS service flow only; SF Info of unicast service flow is same with Table 4-74 in [5]
- PDFID shall be together with MCBCS Transmission Zone to uniquely identify a service flow of MBS.

4.6.3.1.2.2 Handover Action Scenario: Serving ASN Sends R4 HO_Cnf to Target ASN

Section 4.7.2 in [5] needs to be update to show a Handover Action Phase scenario for supporting MCBCS mobility management.

The changes to the existing procedures as specified in Figure 4-63 in section 4.7.2.2.2 in [5] is given below.

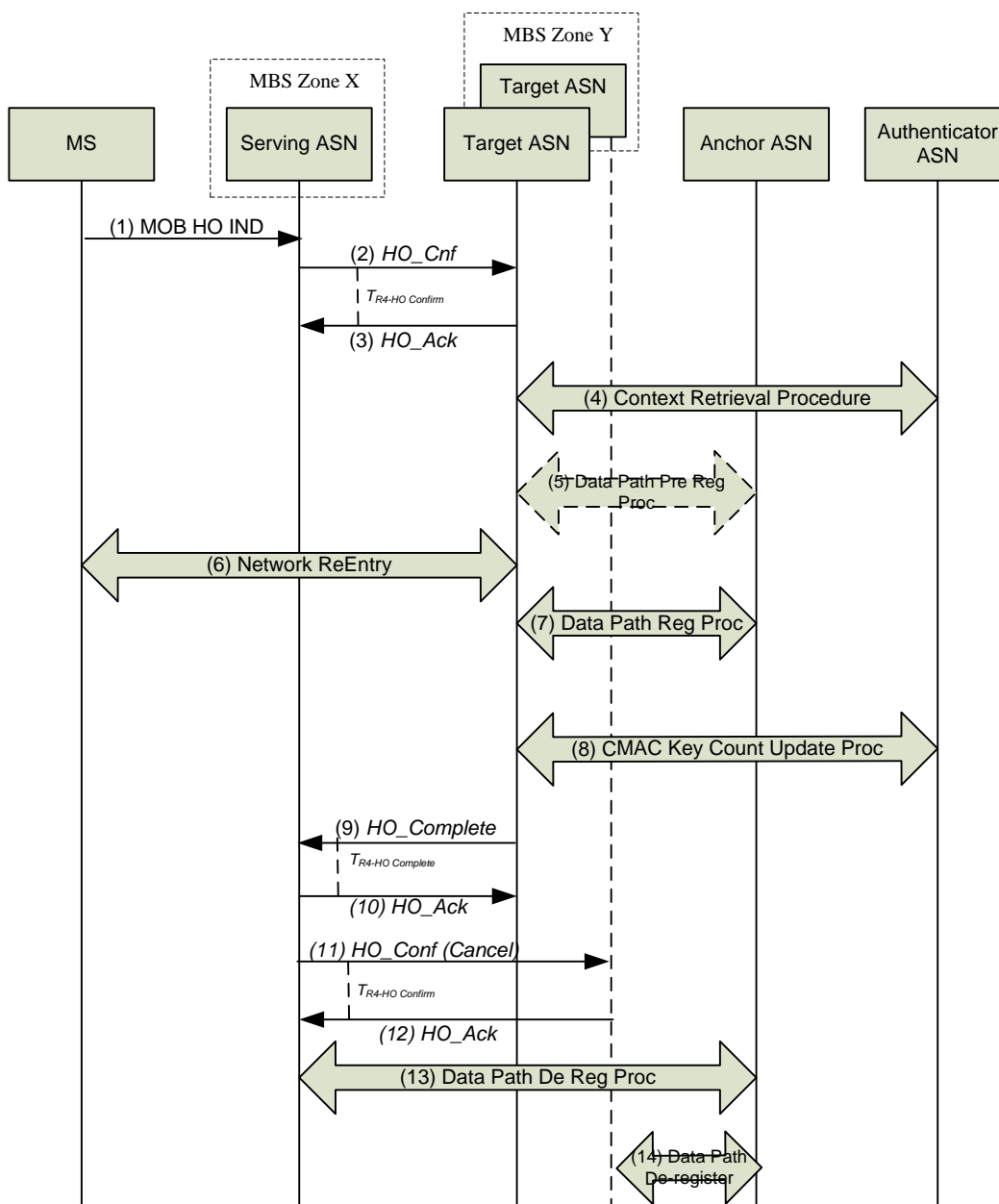


Figure 4-32 : Successful HO Action Phase

STEP 1

No changes.

STEP 2

Upon reception of the MOB_HO-IND the Serving ASN sends an R4 *HO_Cnf* message to the selected Target ASN and starts timer T_{R4-HO-Conf}. The Serving ASN MAY also send R4 *HO_Cnf* message with the value of the HO_Indication type set to “Cancel” to all unselected Target ASN(s) and clear the MS context anytime after receiving MOB_HO-IND message.

In addition, if the MCBCS service is supported by the Serving ASN and is prescribed by the MS, the MS's context regarding the SF Info of MBS service is included as part of the MS context to be forwarded to the Target ASN. Note that, the MS's context regarding the SF Info of MBS service could be transfer by R4 *HO_Req* during HO Preparation phase or by R4 *HO_Cnf* during HO Action phase.

STEP 3 ~ STEP 5

No changes.

Step 6

The MS initiates network re-entry with the Target ASN. If the Target ASN supports the same MCBCS service, however, in a different MBS Zone, the Target ASN SHALL include the appropriate MBS Zone parameters in the REG-RSP encoding TLV of the RNG-RSP to be returned to the MS.

When the MS receives the RNG-RSP with the updated MBS Zone parameters, the MS can then resume the MCBCS programming contents reception by referring to the DCD, DL_MAP, MBS_MAP_IE, MBS_MAP message and the MBS_DATA_IE based on the procedures as described in [3].

STEP 7 ~ STEP 14

No changes.

4.6.3.2 Uncontrolled (Unpredictive) HO with Context Retrieval

In the case when the MS and/or the BS meet the criteria as described in [5] for uncontrolled and un-predictive handover, the procedures in this section apply. In general, the same procedures as described in section 4.7.3 in [5] apply with the addition procedures at the Target ASN to determine whether the Target ASN can continue to provide the same MCBCS service for the given MS.

Once the MS's context is transferred to the Target ASN, the Target ASN recognizes the MCBCS service requirement for the MS and determines the appropriate response back to the MS for the given MCBCS service.

4.6.3.2.1 R4 Message Definitions for Uncontrolled (Unpredictive) HO with Context Retrieval

This section describes the R4 message definitions for Uncontrolled (Unpredictive) HO with Context Retrieval.

Table 4-29 : Context Rpt (From the Serving ASN to the Target ASN)

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
Context Purpose Indicator	5.3.2.36	M	Set to MAC Context Retrieval. Optionally, may include AK Context Retrieval as well.
MS Info	5.3.2.103	M	
>Service Authorization Code	5.3.2.181	O	
>Anchor ASN GW ID	5.3.2.10	O	Identifies the node that hosts the Anchor DP Function in the Anchor ASN. Included if the originator of <i>HO_Req</i> does not host the Anchor DP Function for the MS.
>SF Info (one or more)	5.2.13	O ¹	

IE	Reference	M/O	Notes
>> SF ID		CM	The identifier of service flow
>> MCID	5.2.8	CM	The multicast CID, refer to [3]
>> MCBCS Transmission Zone ID	5.2.6	CM ²	The identifier of MCBCS Transmission Zone
>> MBS Zone ID	5.2.9	CM	The identifier of MBS Zone, refer to [3]
>> PDFID		CM ²	The identifier of packet data flow;
>> MCBCS Service Continuity Indicator	5.2.15	CM	The flag indicate service continuity is required or not
>Authenticator ID	5.3.2.19	O	Identifies the node that hosts Authenticator and Key Distributor Function. Included if the originator of the <i>HO_Req</i> does not host the Authenticator and Key Distributor Function for the MS.
Note: the other TLVs is same as with Table 4-77 in NWG Stage-3 Version 1.3.0			

Notes:

- Here SF Info is for MBS service flow only; SF Info of unicast service flow is same with Table 4-77 in [5]
- PDFID shall be together with MCBCS Transmission Zone to uniquely identify a service flow of MBS.

4.6.3.2.2 Successful Uncontrolled Handover

The following call flow provides an example of a successful uncontrolled handover scenario. A MS begins ranging at Target ASN that wasn't contacted by the Serving ASN to participate in the Handover Preparation phase. Therefore the Target ASN was an unaware of an impending hand-in from the MS. The MS includes the Serving BS ID in the RNG-REQ message. The Target ASN retrieves the MS context and authenticator information, which includes SF Info of MBS service subscribed by the MS

The changes to the existing procedures as specified in Figure 4-72 in section 4.7.3 in [5] is given below.

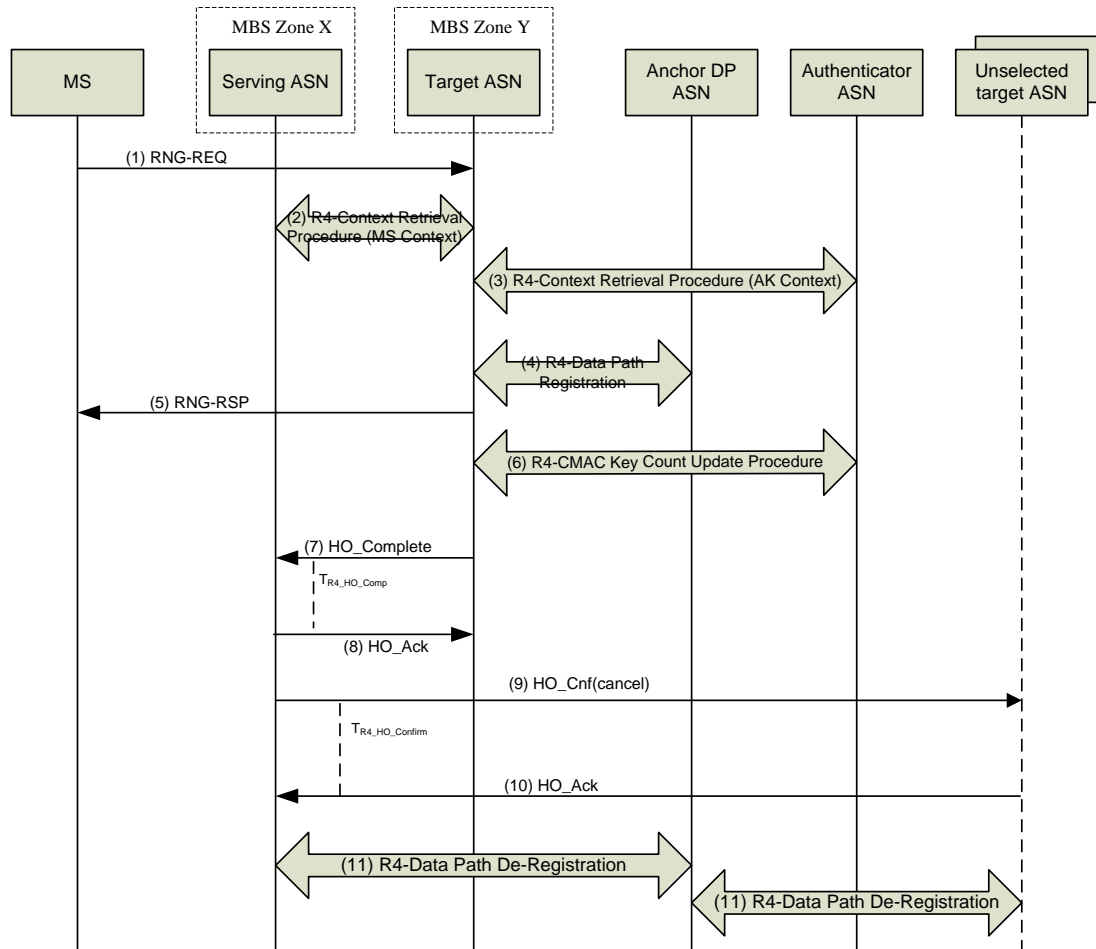


Figure 4-33 : Uncontrolled (Unpredictive) HO

STEP 1

No changes.

STEP 2

The Target ASN initiates a Context Request procedure with the Serving ASN to retrieve context information for the MS. See section 4.13 in [5] for this procedure. The Serving ASN responds by sending the context information which includes the Authenticator ASN ID and Anchor ASN ID. Optionally, if the Target ASN requests also the delivery of AK Context information by setting appropriate bits of Context Purpose Indicator TLV, and if the retrieval of AK Context is supported by the Serving ASN, the Serving ASN may include the AK Context in the response message sent to the Target ASN. If the Authenticator ASN ID and/or Anchor ASN ID was not sent, the Serving ASN hosts the respective functions. In addition, if the MCBCS service is supported by the Serving ASN, the MS's context regarding the SF Info of MBS service is included as part of the MS context to be forwarded to the Target ASN.

STEP 3~ STEP 4

No changes.

STEP 5

Target ASN uses the Authenticator context to authenticate the MS message.

The Target ASN sends a RNG-RSP message to the MS acknowledging the HMAC/CMAC tuple (expedited security authentication) and containing the *HO Process Optimization TLV*.

If the Target ASN supports the same MCBCS service, however, in a different MBS Zone, the Target ASN includes the appropriate MBS Zone parameters in the REG-RSP encoding TLV of the RNG-RSP to be returned to the MS.

When the MS receives the RNG-RSP with the updated MBS Zone parameters, the MS can then resume the MCBCS programming contents reception by referring to the DCD, DL_MAP, MBS_MAP_IE, MBS_MAP message and the MBS_DATA_IE based on the procedures as described in [3].

STEP 6 ~ STEP 11

No changes.

4.6.4 Coexisting unicast service and MBS service

The existing handover procedures for the unicast service flow is not impacted by the intra-MBS Zone transition, based on the understanding that the addition of the MBS related service parameters are required to be included as part of the MS's context that is passed to the Target BS(s) by the Serving BS.

In the case when the MS is approaching or crossing the MBS zone boundary, the MS and the network have to decide which handover policy at the ASN takes the precedence – i.e. unicast service criteria vs. MBS service criteria. Such handover policy may be influenced by the MCBCS Service Continuity Indicator that is part of the MCBCS service policy. It is a local network implementation decision on how to apply the handover policy between unicast and MCBCS services.

4.7 MCBCS Power Saving Support

4.7.1 Power Saving Support for MCBCS during the Intra and Inter MBS Zones Transitions

According to the IEEE 802.16-Rev2 specification [3], the MS can continue to maintain the reception of the MCBCS downlink transmission and still remain in sleep or idle mode. The Network shall maintain the on-going MCBCS program content downlink transmission regardless the mode of MS's operation (i.e. active, sleep or idle mode), or the type of MCBCS services (i.e. broadcast vs. multicast). Prior to MS entry into the Idle mode, the network preserves all the MCBCS related context information, together with other MS context which is accessible by the Paging Controller assigned to the MS.

Even when the MS is in Idle mode, if MCBCS downlink transmission has started, the MS continues to receive the downlink transmission according to the advertised schedule provided within the MBS zone using the IEEE 802.16-Rev2 [3] MBS daisy-chaining downlink transmissions mechanism supported by the IEEE 802.16 MBS_MAP_IE, MBS_MAP message as well as the MBS_DATA_IE. For more details regarding the MBS daisy-chaining mechanism [3], please refer to Annex-C.

When the MS recognizes that it has crossed the MBS Zone boundary, i.e. the Target BS is no longer part of the serving MBS Zone, the MS has to perform a Location Update (LU) procedure in order to obtain the new target MBS Zone to resume the reception of the MCBCS downlink transmission.

During the location update procedure or when the MS exits the Idle mode and based on the MBS service flow information from the anchor PC, the serving BS determines if the MS will be updated with the MBS zone that the serving BS supports in order to allow the reception of the same MCBCS service.

MCBCS-DSx

To support the up-coming and on-going MCBCS operation within the ASN, the MCBCS Sync Controller continues to update the DCD, the MBS_MAP_IE in the DL_MAP, and also the MBS_MAP message in order to describe the downlink transmission of the given MCBCS service. In particularly, the MCBCS Sync Controller leverages the MBS_DATA_IE to daisy chain the list of up-coming downlink MCBCS transmissions within the given MBS Zone so that the MSs who are interested in corresponding MCBCS service can leverage such information to determine the next data reception interval to manage their power saving schedule.

It is the MS's responsibility to examine and refer to the MCBCS downlink transmission schedule that is advertised by the IEEE 802.16-Rev2 [3] airlink protocol (i.e. MBS_MAP_IE, MBS_MAP message and MBS_DATA_IE) and to receive the MCBCS programming contents and to manage its power saving mode operation accordingly.

4.7.2 Location Update

The MS performs the Location Update procedure when it meets the LU condition, MBS Update, as specified in the IEEE 802.16-Rev2 specification [3]. When MCBCS is deployed, an MSs may perform the Location Update triggered by MBS Update procedure also. Additional modifications to support MBS Update are described in the following sections. MBS Update retrieves of the appropriate target MBS Zone ID and MCID(s) for an MS who has crossed the serving MBS Zone (i.e. trigger the MBS Update).

When the network receives a RNG_REQ message from the MS for a MS re-attachment request, the serving BS includes a MBS update indication in the re-attachment request towards the Anchor PC. The Anchor PC will include the MBS service flow information of the MS in the response to the serving BS. If the serving BS determines it supports the same MCBCS service, the serving BS includes the new Target MBS Zone information including the new target MBS Zone ID, the associated MCID(s) and SFID(s) in the RNG_RSP message.

Once the new MBS Zone parameters are sent in the RNG_RSP message to the MS, the MS context shall be updated locally at the MS as well as at the Anchor PC/LR.

When the MS receives the RNG_RSP with the LU RSP TLV including the new serving MBS_Zone_Identifier(s) and the associated MCID(s) corresponding to the existing service flow(s) (i.e. identified by the SFID(s)) for the given MCBCS service, it can resume the reception of the MCBCS programming contents. Internal to the MS, it shall update its MBS Zone ID for the new target MBS Zone. If the MCID has changed, the MS should also update the MCID together with the MBS Zone ID.

If there is no compatible MBS Zone that supports the same MBS service at the serving BS, a NULL MBS Zone information (i.e. #FF) and the associated set of SFID(s) shall be sent to the MS in the RNG_RSP message according to the IEEE 802.16-Rev2 [3]. This implies the disruption of the MBS service for the MS. The mechanism to handle and report the disruption of the MBS service for the MS is implementation detail that is out of scope for this specification.

10.6.1.1 Successful Location Update due to MBS Update triggered by inter-MBS Zone transition

NWG Stage-3 Version 1.3.0, section 4.10.2.1 describes the basic MS initiated successful location update procedure with no Paging Controller relocation. The reference to the existing call flow is shown in the following figure, changes to the existing procedures are alone specified here with respect to the call flow.

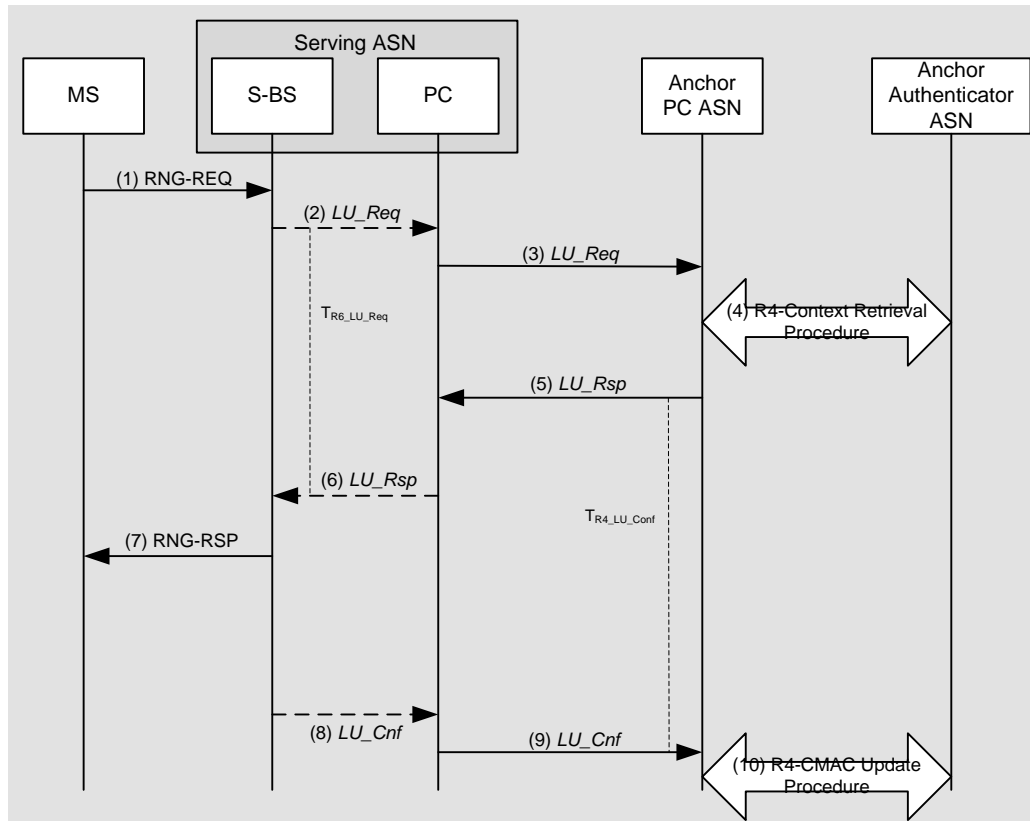


Figure 4-34 : Location Update Procedure due to the trigger of MBS Update for Inter MBS Zone transition case

STEP 1

If triggered by MBS Update, the MS shall send the RNG-REQ including the MBS Update Indicator TLV to indicate the MS's detection of the change of the MBS Zone.

STEP 2

The R6 *LU_Req* message from serving BS to the serving ASN-GW shall include the MBS Update Indicator TLV.

STEP 3

The R4 *LU_Req* message from the serving BS to the Anchor PC ASN shall include the MBS Update Indicator TLV.

STEP 4

No change.

STEP 5

The R4 *LU_Rsp* message from Anchor PC to Serving ASN shall contain the SF Info of MBS service flow which includes the MCBCS Transmission Zone ID, PDFID(s), SFID(s) etc.

STEP 6

The R6 *LU_Rsp* message to the Serving BS from Serving ASN-GW shall contain the SF Info of MBS service flow if they were included in the corresponding R4 message.

STEP 7

The RNG_RSP to the MS which indicates a Successful Location Update contains the New Anchor PC ID as well as the corresponding new target MBS Zone ID(s), the associated MCID(s) and SFID(s). If the MBS Update failed, the corresponding new target MBS Zone ID would be set to NULL (i.e. #FF), this implies the MS can no longer receive the MCBCS downlink transmission from the serving BS. The MS is required to perform the complete network re-entry to learn the correct new target MBS Zone and the associated MCID(s) in order to resume the given MCBCS service.

STEP 8

The Serving BS sends an R6 *LU_Cnf* message to the serving ASN-GW and may include the new MBS Zone ID and new MCID(s).

STEP 9

The R4 *LU_Cnf* message from the Serving ASN to the Anchor PC ASN may contain the new MBS Zone ID(s) and new MCID(s). Upon the receipt of the message, the Anchor PC ASN updates the LR with MCBCS information in the Anchor PC of the MS.

STEP 10

No change.

NWG Stage-3 Version 1.3.0 – section 4.10.2.2 describes the basic MS initiated successful location update procedure with Paging Controller relocation, the reference call flow could be reused, and the changes to the existing procedures for MCBCS are the same as specified above for successful location update procedure with no Paging Controller relocation.

4.7.2.1 Location Update Error Procedures

4.7.2.1.1 MBS Zone Update Failure

In the event when the serving BS does not support the same MCBCS service, NULL target MBS Zone will be returned to the MS in the RNG-RSP. In such event, the MS is required to perform the complete network re-entry if the MS decides to resume the given MCBCS service.

4.7.2.1.2 Message Primitive

The changes to the tables in NWG Stage-3 Version 1.3.0 are highlighted in this section.

Table 4-30 : LU_Req Primitive Structure

IE	Description	M/O	Notes
MBS Zone Update Indicator	11.2.12	CM	If the LU is triggered by MBS Zone update, this TLV is mandatory to be included.
BS Info	5.3.2.26	M	
> BS ID	5.3.2.25	M	BS ID indicating the BS where MS performs location update.
Paging Information	5.3.2.119	M	Paging Information TLV contains PAGING_CYCLE, PAGING OFFSET, PAGING_INTERVAL_LENGTH, and Paging Group ID. The BS may make a suggestion for Paging Cycle and Paging Offset for the MS performing LU.
> Paging Cycle	5.3.2.118	O	
> Paging Offset	5.3.2.120	O	
> Paging Interval Length	5.3.2.135	O	
> Paging Group ID	5.3.2.123	O	
>Anchor PC ID	5.3.2.12	M	“PC ID” field in DREG_REQ on R1 points to MS’s anchor Paging Controller.
>Relay PC ID	5.3.2.117	O	The Relay PC Identifier for the MS in Idle Mode, to be stored in Location Register during Location Update procedure.
>Anchor PC Relocation Destination	5.3.2.13	O	Identifier for destination Anchor PC in the event of Anchor PC relocation.
Network Exit Indicator	5.3.2.109	O	This is in case the LU is caused by Power Down Update.

Table 4-31 : LU_Rsp Primitive Structure

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	This SHALL be mandatory in the event there is a failure due unavailability of Authenticator or if present in Context Rpt. Presence of error code = 0x37 SHALL mean Location Update Status has failed.
BS Info	5.3.2.26	M	
> BS ID	5.3.2.25	M	BS ID indicating the BS where MS performs location update.
> AK Context	5.3.2.6	O	Security context required for BS to validate the received RNG-REQ message from MS and

IE	Reference	M/O	Notes
			respond with RNG-RSP signed by a valid HMAC/CMAC digest.
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
MS Info	5.3.2.103	O	MS Info to be included in the event of PC relocation.
>SF Info (one or more)	5.2.13	M ¹	
>> SF ID	5.3.2.184	M	The identifier of service flow.
>> MCBCS Transmission Zone ID	5.2.6	M ²	The identifier of MCBCS Transmission Zone.
>> MBS Zone ID	5.2.9	O	The identifier of MBS Zone, refer to IEEE802.16 e.
>> PDFID	5.4.2.26	M ²	The identifier of packet data flow.
> Authenticator ID	5.3.2.19	O	
>Anchor ASN GW ID	5.3.2.10	O	This is included if PC Relocation Request has been accepted or is being requested.
Paging Information	5.3.2.119	O	Paging Information TLV contains PAGING_CYCLE, PAGING_OFFSET, PAGING_INTERVAL_LENGTH and Paging Group ID.
>Paging Cycle	5.3.2.118	O	Anchor PC SHALL include this if BS had included a suggestion for this TLV.
>Paging Offset	5.3.2.120	O	Anchor PC SHALL include this if BS had included a suggestion for this TLV.
>Paging Interval Length	5.3.2.135	O	Anchor PC SHALL include this if BS had included a suggestion for this TLV.
>Paging Group ID	5.3.2.123	O	
> Old Anchor PC ID	5.3.2.113	O	This TLV is included in the event of PC relocation.
> Anchor PC ID	5.3.2.12	O	This TLV is included in the event of PC relocation.
>Anchor PC Relocation Request	5.3.2.14	O	“Accept” or “Refuse”. Included only if PC

IE	Reference	M/O	Notes
Response			Relocation is requested in R4 LU_Req
>Location Update Status	5.3.2.88	O	
PC Relocation Indication	5.3.2.122	O	Included by the Current Anchor PC to request PC relocation is included only in R4 LU_Rsp.
Failure Indication	5.3.2.69	O	This SHALL be mandatory in the event there is a failure due unavailability of Authenticator or if present in Context Rpt. Presence of error code = 0x37 SHALL mean Location Update Status has failed.

Notes: 1 Here SF Info is only for MBS Service Flow;

2. PDFID shall be together with MCBCS Transmission Zone to uniquely identify a service flow of MBS.

Table 4-32 : LU_Cnf Primitive Structure

IE	Description	M/O	Notes
Failure Indication		O	Location Update Failure code SHALL be included.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	BS ID indicating the BS where MS performs location update.
> Serving/Target Indicator	5.3.2.182	M	Set to “Serving” if location update is a success else set to “Target”. Shall be included only in R4 <i>LU_Cnf</i>
MS Info	5.3.2.103	O	
>SF Info (one or more)	5.2.13	M ¹	
>> SF ID	5.3.2.184	M	The identifier of service flow.
>> MCBCS Transmission Zone ID	5.2.6	M ²	The identifier of MCBCS Transmission Zone.
>> MBS Zone ID	5.2.9	O	The identifier of MBS Zone, refer to IEEE802.16 e.
>> PDFID	5.4.2.26	M ²	The identifier of packet data flow.
> CMAC_Key_COUNT		M	Includes BS value of CMAC_KEY_COUNT to update an Authenticator.
Paging Information	5.3.2.119	O	The BS SHALL reflect the Paging Cycle, Paging Offset, Paging Interval Length and Paging Group Id received in the LU_Rsp.
>Anchor PC ID	5.3.2.12	O	Included if PC relocation was requested earlier.
>Relocation Success Indicator	5.3.2.149	O	Success if Relocation was accepted by destination and completed.

Notes:

- 1 Here SF Info is only for MBS Service Flow;
- 2 PDFID shall be together with MCBCS Transmission Zone to uniquely identify a service flow of MBS.

4.7.3 MS MBS Idle Mode Exit

When the network receives the RNG_REQ message from the MS for an Idle Mode exit, the serving BS sends the Re-attachment Request towards the Anchor PC indicating the MS is intended to re-enter from idle mode by following the same procedures as described in the existing NWG specification [5]. The Anchor PC then includes the MCBCS Transmission Zone and the MBS service flow information of the MS in the re-attachment response to the serving BS in the serving ASN if the MS has an active MCBCS service.. If the serving BS determines that it supports the same MCBCS service, the serving BS includes the new Target MBS Zone information including the new target MBS Zone ID as well as the associated MCID(s) and SFID(s) in the RNG_RSP message.

Once the new target MBS parameters information is sent in the RNG_RSP message, the MS context is updated locally at the MS.

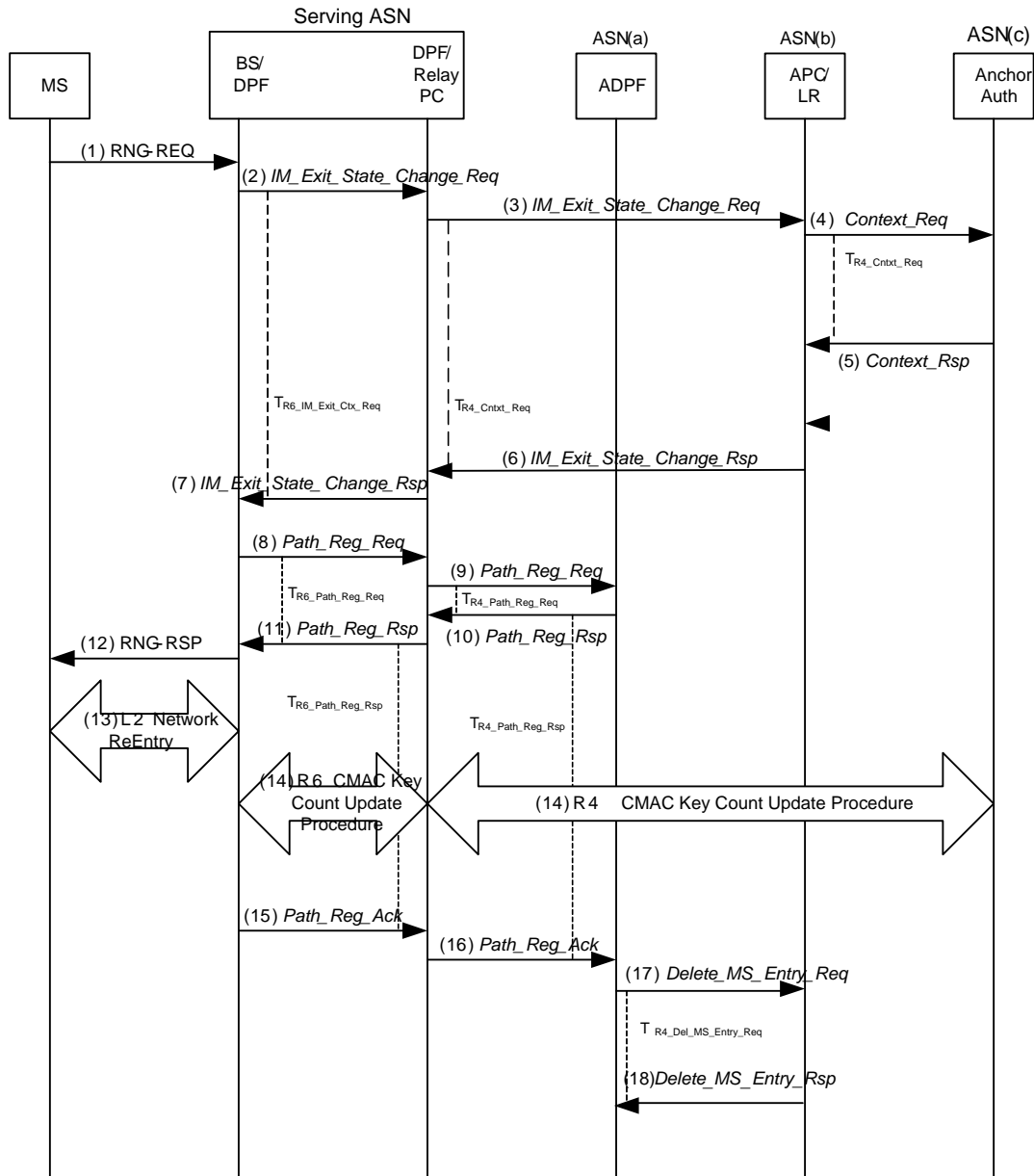
If there is no compatible MBS Zone that supports the same MBS service at the serving BS, a NULL MBS Zone information (i.e. #FF) and the associated set of SFID(s) is returned to the MS in the RNG_RSP message as described in IEEE 802.16-Rev2 [3]. This implies the disruption of the MBS service for the MS. The mechanism to handle and report the disruption of the MBS service for the MS is implementation detail that is out of scope for this specification.

In general, the existing procedures to support the MS exits from Idle mode are re-used with only the addition procedures to retrieve the appropriate new target MBS Zone from the anchor PC if the MS crosses the MBS Zone boundary with the selected target BS. The network shall ensure at Idle Mode re-entry that the MS is in possession of MBS service flow parameters applicable at the re-entry BS.

4.7.3.1 Idle Mode Exit - Serving ASN Has no MS Context

The call flow for a typical scenario for the MS exiting idle mode is shown below. Here it is assumed that when the MS is trying to re-enter the network from idle mode, (i.e., exits from the idle mode), the serving ASN does not have any context for this MS, hence, the entire context has to be retrieved from the Anchor PC.

The changes to the existing procedures as specified in NWG Stage-3 Version 1.3.0 – section 4.10.4.1 are given below.



Note: The serving BS is belonged to a different MBS Zone.

Figure 4-35 : Idle Mode Exit Procedure for Inter MBS Zone case

Flow Description

MS may exit idle mode in two ways Network-initiated or MS-initiated. Although most of the steps in the two scenarios are the same, the sequences are different and some of the steps could be optional.

Case a: Network initiated Idle mode exit (in response to a page)

When MS exits idle mode in response to a prior paging message, it performs Ranging (i.e. RNG_REQ).

Case b: MS initiated Idle mode exit

When MS initiates the exit from Idle mode, it performs the steps given below.

STEP 1

No change.

STEP 2

No change.

STEP 3

No change.

STEP 4

No change.

STEP 5

No change.

STEP 6

Anchor PC/LR, sends R4 *IM_Exit_State_Change_Rsp* to the Relay PC. R4 *IM_Exit_State_Change_Rsp* contains the MS's context stored at the Anchor PC which includes the SF Info of MBS service flows, i.e. MCBCS Transmission Zone ID, PDFID(s), SFID(s) etc, as well as optionally includes the "last" serving MBS Zone ID to allow the serving BS to determine if the MBS Zone ID(s) and corresponding MCID(s) that may need to be updated for the MS.

STEP 7

The R6 *IM_Exit_State_Change_Rsp* shall include the SF Info of MBS service flow if they were included in the corresponding R4 message.

STEP 8

No change. Applicable only to the unicast transport connection(s).

STEP 9

No change.

STEP 10

No change.

STEP 11

No change.

STEP 12

The BS will refer to MS service and operational information indicated by IDLE Mode Retain Info obtained by Step 7 to construct HO Process Optimization TLV (as described in IEEE 802.16-Rev2 [3] parameters) settings in the RNG-RSP based on the local policy; then sends RNG_RSP message to the MS according to IEEE 802.16-Rev2 specification [3]. This message delivers all the required information to resume service according to the Idle Mode Retain Information. In addition, the corresponding new target MBS Zone ID(s), the associated MCID(s) and SFID(s) as specified in the IEEE Std 802.16-Rev2 specification [3], are also provided to the MS if the serving BS supports the MBS service continuity.

However, if the corresponding new target MBS Zone ID is NULL (#FF), this implies the MS can no longer to resume the MCBCS downlink transmission from the serving BS. If necessary, the MS is required to perform the

complete network re-entry in order to learn the correct new target MBS Zone and the associated MCID(s) to resume the given MCBCS service.

STEP 13

No change. Applicable only to the unicast transport connection(s).

STEP 14

No change.

STEP 15

No change.

STEP 16

No change.

STEP 17

No change.

STEP 18

No change.

4.7.3.2 Idle Mode Exit Error Conditions

This section describes error conditions associated with the IM exit procedure.

4.7.3.2.1 MBS Zone Update Failure

In the event when the serving BS does not support the same MCBCS service, no new target MBS Zone will be returned to the MS in the RNG-RSP. In such event, the MCBCS service for the MS will be discontinued. The system handling for the MS of the lost of service is local policy implementation decision.

4.7.3.2.2 Message Primitive

Table 4-33 : IM_Exit_State_Change_Rsp

IE	Description	M/O	Notes
Failure Indication	5.3.2.69	O	Code value = 32. Included in the event of failure.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	ID of the BS from which MS is initiating Idle mode Exit.

IE	Description	M/O	Notes
>AK Context	5.3.2.6	M	AK, AKID, Lifetime, AK Sequence, EIK.
.....		
MS Info	5.3.2.103	M	
>SF Info (one or more)	5.2.13	M ¹	
>> SF ID	5.3.2.184	M	The identifier of service flow.
>> MCBCS Transmission Zone ID	5.2.6	M ²	The identifier of MCBCS Transmission Zone.
>> MBS Zone ID	5.2.9	O	The identifier of MBS Zone, refer to IEEE802.16 e.
>> PDFID	5.4.2.26	M ²	The identifier of packet data flow.
>SBC context	5.3.2.174	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16-Rev2 [3].
Note: the other TLVs is same as with Table 4-138 in NWG Stage-3 Version 1.3.0			

Notes:

1. Here SF Info is only for MBS Service Flow;
2. PDFID shall be together with MCBCS Transmission Zone to uniquely identify a service flow of MBS.

4.7.4 MS MBS Idle Mode Entry

Prior to the entry to the Idle mode, the related MBS context for the MS should have been preserved in the Anchor PC assigned for the MS. So the related MCBCS info should be included in the IM_Entry_State_Change_Req message.

Table 4-34 : IM_Entry_State_Change_Req

IE	Description	M/O	Notes
BS Info	5.3.2.26	M	
> BS ID	5.3.2.25	M	BS ID indicating the Serving BS performing operation.
MS Info	5.3.2.103	M	
> SF Info (one or more)	5.2.13	M ¹	
>> SFID	5.3.2.184	M	The identifier of service flow.
>> MCBCS Transmission Zone ID	5.2.6	M ²	The identifier of MCBCS Transmission Zone.
>> MBS Zone ID	5.2.9	O	The identifier of MBS Zone, refer to IEEE802.16 e.
>> PDFID	5.4.2.26	M ²	The identifier of packet data flow.

IE	Description	M/O	Notes
> Authenticator ID	5.3.2.19	M	ID of Anchor Authenticator.
> Anchor ASN GW ID	5.3.2.10	M	ID of Anchor GW / Anchor DPF.
> SBC context	5.3.2.174	O	Included based on the bits set in the Idle mode retain information TLV from the MS and if cached in the BS apriori
.....		
Note: the other TLVs is same as with Table 4-149 in NWG Stage-3 Version 1.3.0			

Notes:1 Here SF Info is for MBS service flow only; SF Info of unicast service flow is same with Table 4-149 in NWG Stage-3 Version 1.3.0
2. PDFID shall be together with MCBCS Transmission Zone to uniquely identify a service flow of MBS.

4.8 Security

MCBCS Phase-1 supports only the application layer security management and data encryption of which the details of the technical mechanism are outside the scope of the NWG.

MCBCS layer-2 security is deferred to MCBCS phase-2 design consideration and is subjected for further study.

4.9 MCBCS QoS

A MCBCS QoS profile is assigned for service and not assigned for individual MS. In other words, the QoS profile is the same for all the MSs that prescribe to the same MCBCS service.

4.9.1 MCBCS QoS Support for Broadcast/Multicast Transport

4.9.1.1 MCBCS QoS Management Functional Descriptions

The key functional MCBCS QoS components supporting broadcast/multicast transport are:

- Service Policy Control Point:
 - MCBCS Controller/Server
 - AAA/PDF (Note: PDF supports for MCBCS is FFS.)
- Service Policy Enforcement Point:
 - SFA/SFM
 - MBS Proxy
- QoS Bearer Management
 - MBS Sync Functions (i.e. MBS Sync Controller and MBS Sync Executor)
 - MBS Distribution DPF
 - MBS DPF

The reference model for MCBCS QoS management is described as follows:

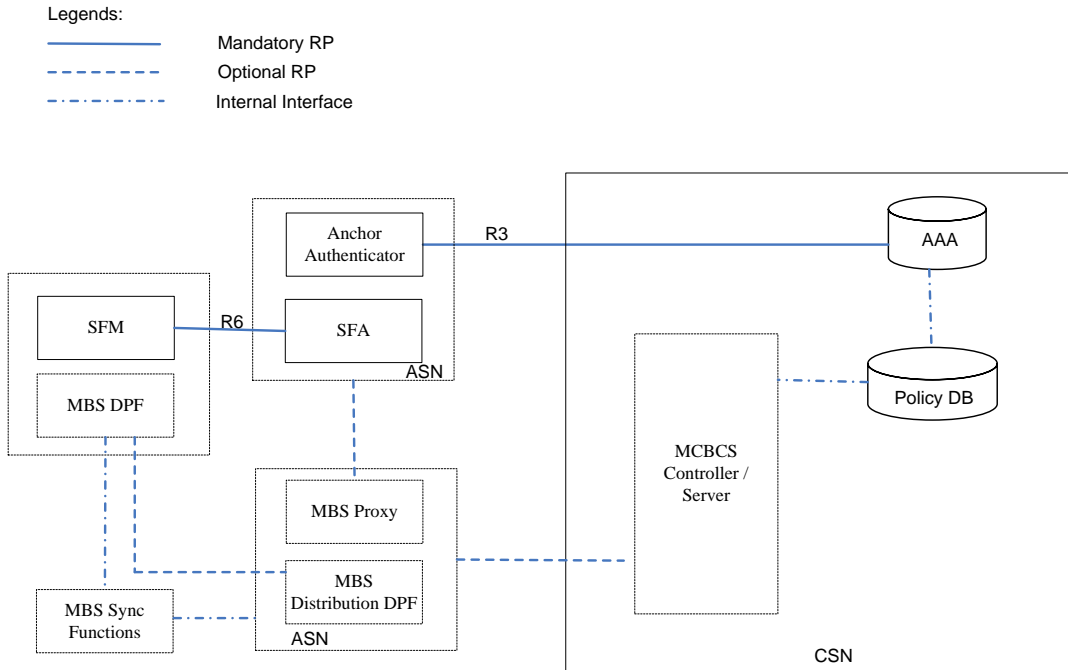


Figure 4-36 : MCBCS QoS Management Functional Model

NOTE: The implementation of the Radio Resource Management (RRM) support for the MBS resource reservation and allocation is FFS.

The MCBCS service profile is provided by the MCBCS Controller/Server as well as by the AAA to enable the MBS Proxy and the SFA respectively, to support MCBCS policy enforcement. From a service perspective, the MCBCS service profile contains all the QoS parameters as well as the service parameters (e.g., IP Multicast Address and port ID, the MCBCS Transmission Zone ID, PDFID, etc.) for a given MCBCS service. The communication between the MCBCS Controller/Server and the AAA, in support of the MCBCS policy control, is outside the scope of this specification.

The MBS Proxy obtains the MCBCS service profile from the MCBCS Controller/Server. The service profile is related to a given MCBCS service on a session-by-session basis.

When the MBS Proxy receives the MCBCS service profile, if the MBS DPs for the given MCBCS service has not been established yet, the MBS Proxy may trigger the MBS Distribution DPF and establish the MBS DPs with all BSs that are part of the MBS Zone. This is done according to the given MBS service policy parameters.

Based on the pre-configured local ASN policy, the MBS Proxy is responsible for mapping the MCBCS Service profile, including the QoS parameters, the MCBCS Transmission Zone ID, and the PDFID(S) that are provided by the MCBCS Controller/Server, to one or more MCID(s) and MBS Zone(s). The decision on MBS Zone organization corresponding to the group of BSs within the ASN, as well as the decision on the MBS data synchronization requirements according to the MCBCS service policy within and across the MBS Zones, are ASN implementation details that are outside the scope of this specification.

The SFA obtains the QoS and MBS service parameters from the MCBCS service profile, provided either by the AAA or the MBS Proxy. The SFA leverages such QoS and service parameters information to communicate with the SFM and trigger the service flow establishment. The SFA also triggers to associate the assigned SFID with the MCID for the given MCBCS service, once the MS access to the given MCBCS service is authorized by NSP. Likewise when the MCBCS session is terminated, the SFA is responsible for deleting the service flow for the given MS and to dis-associate at the BS the MBS SF with the MBS DP.

MCBCS-DSx

The MBS Distribution DPF is responsible for propagating the MCBCS service profile which includes the MBS QoS and service parameters to the target MBS DPFs and the associated BSs belonging to the same MBS Zone. The MBS Distribution DPF, or MBS DPF, shares the MCBCS service profile information with the MBS Sync Function (e.g. MBS Sync Controller) in order to support the MBS data synchronization operation.

The MBS QoS parameters may be carried by the Session Start signaling when the MBS data path has not been established yet and the existing QoS policy for the given MBS data path is required to be overridden before the receiving the downlink transmission. After the transmission of the MCBCS content starts, a Session Update signaling message may be sent from the MCBCS controller to trigger a change of QoS and the priority change of the MCBCS flow.

From the airlink perspective, the RRM function for the radio resource reservation and allocation at the BSs and the RRM information exchange across BSs for scheduling and MBS macro-diversity transmission within the MBS Zone is implementation details not provided in this spec. Likewise, a MBS frame-level coordination within and across the MBS Zones are not specified here either and is subjected of a further study.

4.9.1.2 MCBCS QoS Support for Multicast Distribution Tree

The MCBCS data will be distributed to multiple users through a MCBCS multicast distribution tree that can span many BSs and ASN-GWs. Furthermore in order to save resources, some bearer resources allocated for a multicast distribution tree may be shared between many users accessing the same MCBCS bearer service. As a result, each branch of a MCBCS distribution tree shall be established with the same QoS attributes.

4.9.1.3 MCBCS QoS Support Strategy over WiMAX ASN

It shall be possible for the network to control the QoS parameters for the broadcast/multicast transport of the MCBCS contents or programs. The MCBCS program is a logical concept from the user point of view. A MCBCS program can contain one or multiple contents- e.g. CNN, NBC, file transfer. It is a package that the subscriber typically subscribes to. A MCBCS service is a logical of the data transportation and it is identified by a MCBCS Transmission ID and PDFID(s). It may contain one or multiple contents that share the same QoS requirement, target the same group of users and is mapped to the one or more MCIDs. The following describes key the design considerations for the MCBCS QoS support over the WiMAX network.

1) QoS Classification and Policy Mapping

A MCBCS service is identified by the MCBCS Transmission Zone ID and PDFID(s). The QoS parameters for the MCBCS services are:

- A service profile parameters
- QoS parameters mapped to packet loss rate and packet delay budget values associated with the MCBCS service.

The WiMAX ASN SHALL transmit all the traffic of a given MCBCS service in a manner that allows best reception result of all MBS service flow(s) by the majority of the MCBCS capable users. For example all the MBS service flows of a given MCBCS services are to be transmitted on the same frequency with a macro diversity support within an MBS Zone. This can be specified via a pre-determined modulation coding scheme (MCS), FEC type, Repetition Coding, etc, that best suits the majority of the MCBCS users for the given MBS Zone over a particular geographical region. Such approach significantly enhances the link budget for the MSs and therefore enhances the overall MS reception quality. However, the algorithm for the selection of the MCS, FEC etc. is design implementation that is out of the scope of this specification.

Same as for a unicast service, the MCBCS service requires the local mapping policy of the Service Data (SD) flow to one or more Packet Data (PD) flows for different media components that meet different QoS requirements. For example, a video streaming service might provision PD flow for video (e.g. low error rate, low delay, high

MCBCS-DSx

bandwidth), PD flow for audio (e.g. medium error rate, low delay, low bandwidth) and another PD flow for control traffic, such as traffic key re-keying messages (e.g. a very low error rate, medium delay, very low bit-rate bandwidth). The mapping of packet data flow (PDF ID) to MBS service flow (MCID) is one to one mapping. However, what MCID is assigned to that packet data flow is based on local mapping policy.

2) MCBCS Traffic Management Support

Unicast admission control decision SHALL take into considerations the MBS resource reservation and allocation within the MBS Zone for a given BS. Overlapping MBS Zones contenting for the same radio resource SHALL be prevented and should only be allowed when spatial and time multiplexing are feasible. In the case of a transient BS airlink resource contention, between the unicast and MBS traffic, the MBS downlink transmission schedule SHALL take precedence over the unicast downlink transmission, unless it is higher priority emergency traffic.

Due to the MBS data synchronization support requirement for the MBS downlink transmission, data buffering is an important system requirement. Traffic management operation, such as shaping and packet discard that typically applies to the traffic flow over the R3, R6 and R4 interfaces for the adaption of available resources and changing network conditions are not desirable as it will affect the data synchronization operation among the participated BSs. Traffic engineering and priority handling to ensure the sufficient capacity over R3, R6 and R4 for MBS traffic flow is a more desirable option. The total transfer time is not too critical for non real-time MCBCS services since the content must normally have been received in totality and stored in the MS prior to user access.

For phase-1 MCBCS support, no indication is provided to the MS in case the ASN cannot provide the requested QoS. As a result, some MSs may not receive the MCBCS data or just receive parts of it.

3) MCBCS Data Integrity

When a low SDU error ratios are difficult to achieve, or when prevention of data loss is required, an MCBCS service may perform retransmission or repetitive transmissions over the R6 and R4 interfaces. More details on the MCBCS data integrity support shall be referred to the MBS Data Synchronization section 4.12.

4.10 MCBCS Charging and Accounting

4.10.1 MCBCS Charging/Accounting Support Reference Model

An Accounting Client located at ASN can support statistic collection for the NAP and can provide more relevant bearer information than the Accounting Client located at the CSN. Similar to unicast, the MCBCS Accounting Client can be co-located with the Anchor SFA/Authenticator, and the MBS Accounting Agent is co-located at the MBS Distribution DPF to support the collection of the ASN accounting statistic. Accounting Client located at the ASN can be used to support collection the exact timing of MS authorization for the MCBCS service and the exact duration and volume sent for the specific MCBCS service .

The detailed diagram is as follows:

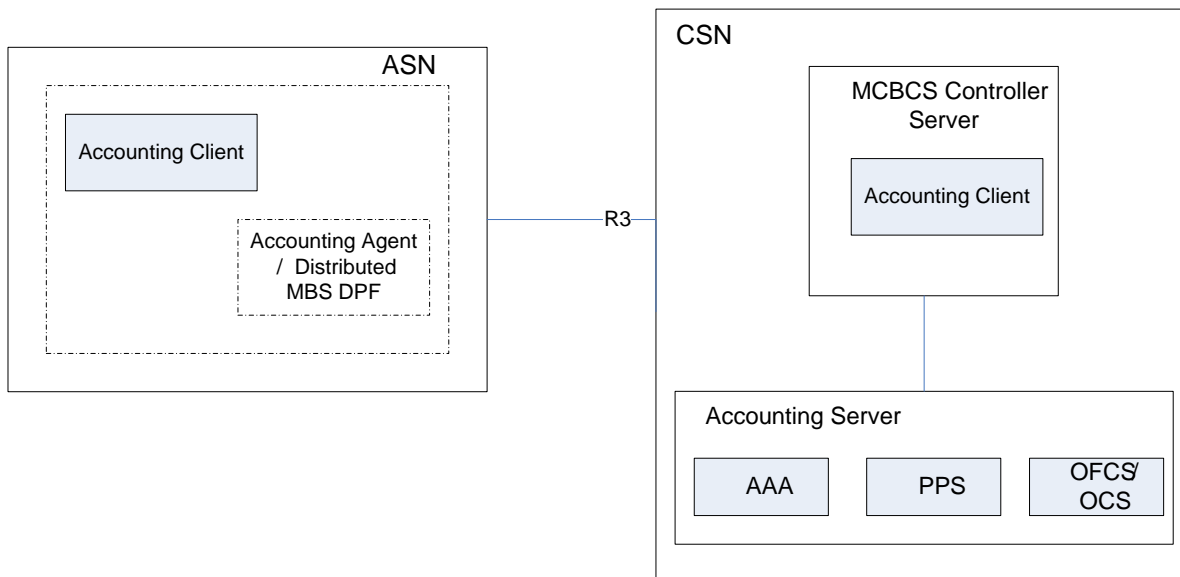


Figure 4-37 : NRM for MCBCS Accounting Records Generation

4.10.2 MCBCS Accounting Record Generation Principles

WiMAX SHALL support the collection of the MCBCS accounting information for the MS that receives the MCBCS service. The MBS Accounting Agent is co-located with the MBS Distribution DPF within the ASN to support volume and time based accounting.

The Accounting Client, via the support of the Accounting Agent, generates accounting information (i.e. UDR) which is keyed on one or more of the following service identifications, for the MCBCS user and/or MCBCS content provider:

- Identification of the source of content (i.e. Program ID, MCBCS Transmission zone ID, PDFID(s) , multicast IP address)
- Type of user service (e.g. streaming, download etc.)
- Type of transport used to deliver content (i.e. broadcast, multicast or unicast)
- Identification of subscribers (e.g. NAI) receiving service

This section describes the terminology and the support of the accounting modes applicable to WiMAX MCBCS service. The following figure shows the different possible levels of the accounting support and the related identifiers.

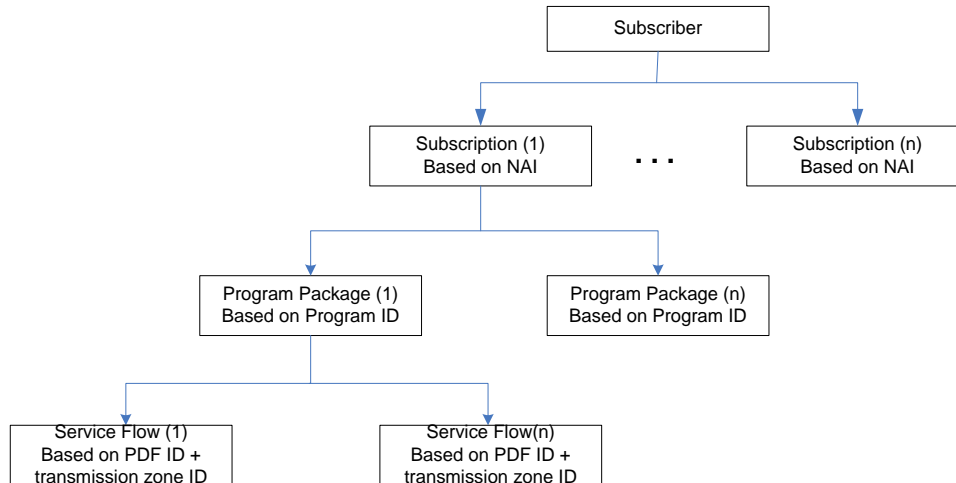


Figure 4-38 : MCBC Service Identifiers for Accounting Support

MCBCS Program is a logical concept from user point of view. A MCBCS Program can contain one or more channels and contents – e.g. CNN, NBC, file transfer. It is the service that MCBCS subscriber subscribes to.

A MCBCS Service Flow is a logical view from data transportation and it is identified by a MCBCS Transmission Zone ID and a PDF ID which is unique within the MCBCS transmission zone. It can be used to correlate the same MCBCS Service Flow content, which the MS can receive from different MBS Zones.

For charging correlation purpose, the Accounting Client includes the MCBCS Program ID as the SDFID and the PDF ID as well as MCBCS Transmission Zone ID in the accounting record.

MCBCS accounting support can be partitioned into service-based accounting and access-based accounting. For the service-based accounting, a user may be charged either by subscription or flat rate.

Service-based Accounting is to identify the type of accounting records for a given MCBCS content, such as video streaming or field downloading. Operator would like to know the type of MCBCS contents for a given accounting records.

Access-based Accounting is to identify the amount of bearer resources that are consumed for the given MCBCS services. The NAP/ASN would like to collect these accounting records and may use this information to charge the NSP or subscriber. The method of charging and the charging architecture is outside scope of this specification

Accounting associated with the service-based option can be treated independently from the accounting associated with the access-based option. If the service-based option is determined, the access-based option can be applied on top to determine the accounting operation.

Table 4-35 : Charging/Accounting Requirements for Service Delivery

Accounting Type	Type of Transport		
	Broadcast	Multicast	Unicast

Service-based (i.e. content type)	Free/Flat rate	Receiving Subscriber paid	Receiving Subscriber paid
Access-based (i.e. bearer resource utilization)	Content Provider paid	Content Provider and/or Receiving Subscriber paid	Content Provider and/or Receiving Subscriber paid

For the access-based accounting, it may be charged based on the session information (e.g. QoS, media type, and MCBCS service coverage within the ASN) as described below:

- Session duration (time from Session-Start and Session-Stop)
- Volume of data during the MCBCS Programming session
- Duration of time once the MS is registered to receive the MCBCS service, or between the joining/leaving the MCBCS service
- Volume of data transferred once the MS is registered to receive the MCBCS service or in the duration that is between the joining/leaving the MCBCS service

Table 4-36 : Applicability of Accounting Measurement

Accounting Measurement	Applicable to (Yes/No)		
	Broadcast	Multicast	Unicast ^{Note 1}
Session Duration (time from Session-Start and Session-Stop)	Yes	Yes	Yes
Volume of data during the MCBCS Programming Session (between session start/stop)	Yes	Yes	Yes
Duration of time once the MS is registered to receive the MCBCS service, or between the joining/leaving the MCBCS service	No	Yes	Yes
Volume of data transferred once the MS is registered to receive the MCBCS service or in duration that is between the joining/leaving the MCBCS service	No	Yes	Yes

Note-1: The support of the unicast MCBCS accounting is not within the scope of phase-1 MCBCS. The present of the information is to provide an example of the complete overview of the MCBCS accounting measurement strategy.

4.10.3 MCBCS Offline Accounting Support

4.10.3.1 Basic Principles

In the case of the service-based accounting, the accounting triggers could be by the Session Control (e.g. Session-Start or Session-Stop) or MS events (e.g. Join or Leave), if large volume of users are expected to use the MCBCS service, generating the charging/accounting information (e.g. UDR) SHALL be performed in a manner that ensures the charging entities and billing domain are not overloaded.

Hence, it is recommended that the accounting records for a given MCBCS service generated by the MBS Accounting Agent that distributes the information to the corresponding MS's associated Accounting Client to generate the UDR if per-MS accounting is enabled.

MCBCS-DSx

Per network policy, if a volume based accounting per MS is needed, the MS Accounting Client can request the volume information from the MBS Accounting Agent.

4.10.3.2 MCBCS Broadcast Services

As there is no per-MS trigger for the accounting event in the case of the MCBCS broadcast services, the statistic collection and the accounting for the MCBCS broadcast services is dependent on either the session duration and/or the volume count within the MCBCS programming session that is triggered by a session start/stop.

4.10.3.3 MCBCS Multicast Services

Unlike the MCBCS broadcast service, the MCBCS multicast services accounting support can be based on user subscription or a flat rate. If a user subscription is chosen, any of the four access-based accounting options as described in above table can be applied.

4.10.4 MCBCS Online Accounting Support

Online charging and accounting support will not be applicable for the MCBCS broadcast service. As for the MCBCS multicast service applicability to the MS, it is FFS.

4.10.5 UDR Generation

Two types of UDR are generated for MCBCS services:

- For user
- For content provider

4.10.5.1 UDRs Related to MCBCS user

MCBCS UDR for the user SHALL be opened for collection as soon as the MS is triggered by RADIUS Accounting-Start packet or Diameter ACR (Start) once the user has completed the successful network entry. The volume for the MCBCS UDR for the user is counted in downlink direction only.

4.10.5.2 UDRs Related to MCBCS Content Provider

MCBCS UDR for the content provider SHALL be opened for collection as soon as the Session Start which triggers Accounting-Start or ACR (Start) once the user has completed the successful network entry. The volume for the MCBCS UDR for the user is counted in the downlink direction only.

4.10.6 MCBCS UDR Collection Scenarios**4.10.6.1 MCBCS UDR for user - Timely Based Accounting Triggered by MS Join/Leave**

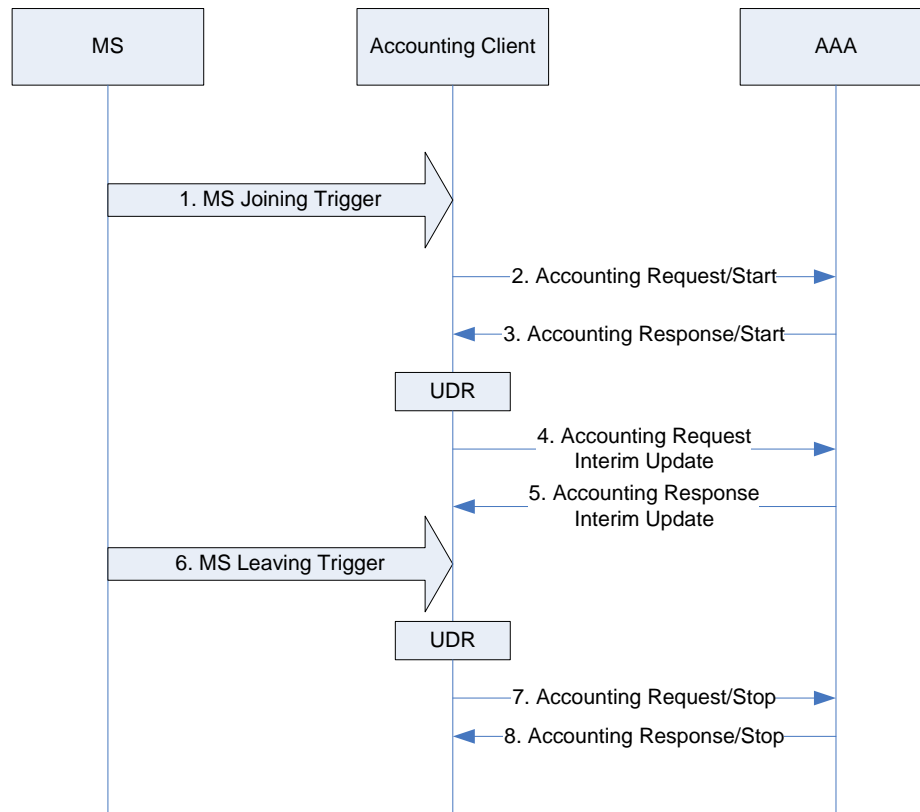


Figure 4-39 : MCBSC UDR for user Timely Based Accounting Triggered by MS Joint/Leave

Step 1.

The MS sends a join trigger to the ASN, to indicate that it is interested in joining one or more MCBSC services. After the MS gets authorized and successfully initiated the DSx procedure, it triggers the Accounting Client to Start collecting accounting information.

Step 2.

Upon the Accounting Client receiving this join trigger, sends an Accounting Request/Start message to the AAA to start the accounting process.

Step 3.

The AAA replies with an Accounting Response/Start message and the Accounting Client starts creating UDR record.

Step 4, 5.

While the user is subscribed to the MCBSC service, the Accounting Client sends Interim Accounting Request to update the accounting information periodically.

Step 6.

If the MS decides to leave the MCBSC services, the MS sends a “leaving” message to the Accounting Client.

Step 7.

Upon receiving the “leaving” message, the Accounting Client generates a UDR record and sends an Accounting Request Stop message stopping the accounting session.

Step 8.

The AAA responds back by sending an Accounting Request Stop message.

4.10.6.2 Volume Based Accounting

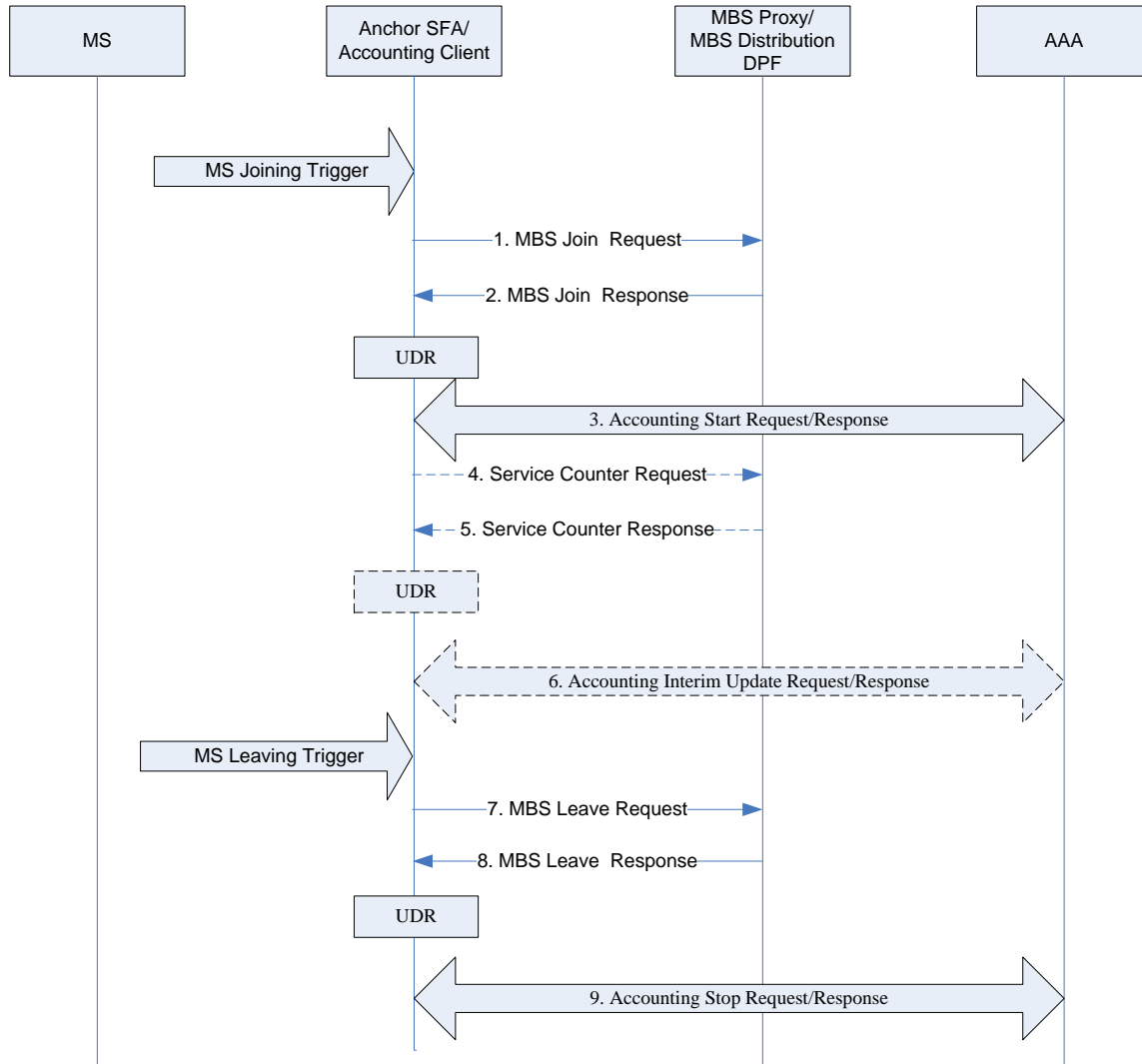


Figure 4-40 : MCBCS volume based Accounting

Step 1.

The MS joins a particular MCBCS service, which may pre-provisioned or dynamically assigned. The Anchor SFA is notified during the joining procedure. The Anchor SFA then relays the MBS join request message to the MBS proxy in order to obtain the associated MCID(s).

Step 2.

The MBS proxy responds back with a MBS join response message to the Anchor SFA. If a volume based accounting is used, there is a counter in the MBS Accounting Agent (which is co-located with the MBS Distribution DPF), that counts the volume of a particular MCBCS service. The MBS Proxy includes the current counter value in the MBS join response message.

Step 3.

Upon receiving this MBS join response message, the Accounting Client records the counter as the initial counter value and sends an Accounting Request/Start message to the AAA starting the accounting process. The AAA responds back with an Accounting Response/Start message.

Step 4.

If the interim accounting update is used, then the ASN (where the Accounting Client is located) sends service counter request message to the MBS Accounting Agent to periodically get the counter value of the particular MCBCS service. Since the counter can be used for all the MSs that receive the particular MCBCS service, the ASN only needs to send one message for all the MSs whose accounting client is located in the same ASN.

Step 5.

The MBS Accounting Agent responds back with a service counter response message including the cumulative counter value of the particular MCBCS service.

Step 6.

Upon receiving the counter, the Accounting Client calculates the volume by subtracting the initial counter value from the received counter value. The Accounting Client reports the UDR using the interim update procedure.

Step 7.

In the MS leaving service procedure, the anchor SFA is triggered to send a MBS leave request message to the MBS proxy.

Step 8.

The MBS proxy responds with a MBS leave response message. If volume based accounting is used, the MBS proxy includes the current counter value in this message.

Step 9.

Upon receiving the message, the Accounting Client calculates the volume by subtracting the initial counter value from the received counter value. The Accounting Client triggers the accounting stop procedure with the generated UDR.

4.11 End-to-end Transport Mechanism for Content Delivery

The end-to-end MCBCS transport mechanism for content delivery can be partitioned into three transport segments:

- 1) Transport from the MCBCS Content Server in the CSN to the MCBCS Distribution DPF in the ASN-GW over R3
- 2) Transport inside the ASN over R6 and/or R4, within the MBS zone or MCBCS Transmission zone, which may or may not be multicast capable.
- 3) Transport on the air interface.

The first two are within the scope of this specification, and the last segment, i.e. the air interface, is described in IEEE802.16Rev2 [3] specification and is not within the scope of this specification.

4.11.1 Data Transportation between CSN and ASN

MCBCS-DSx

The Transport between the CSN and ASN can be achieved via unicast or via multicast methods. Unicast method is similar to the NWG Rel1.0 specs.

In the case of multicast method, a multicast distribution tree is created between MBS Distribution DPF and the CSN MCBCS Controller. Towards the CSN MCBCS Controller, the MBS Distribution DPF connects to the IP Multicast groups corresponding to the MBS Contents it has to distribute inside its MBS Zone. The MBS Distribution DPF connects to the multicast trees as a leaf, using IGMP join procedure, thus the MBS Distribution DPF is IGMP host in IGMP terminology, the Content Server is IGMP source.

Figure 4-41 below describes the scenario of the MCBCS data transportation establishment over R3 which is triggered by MCBCS Session Start procedure.

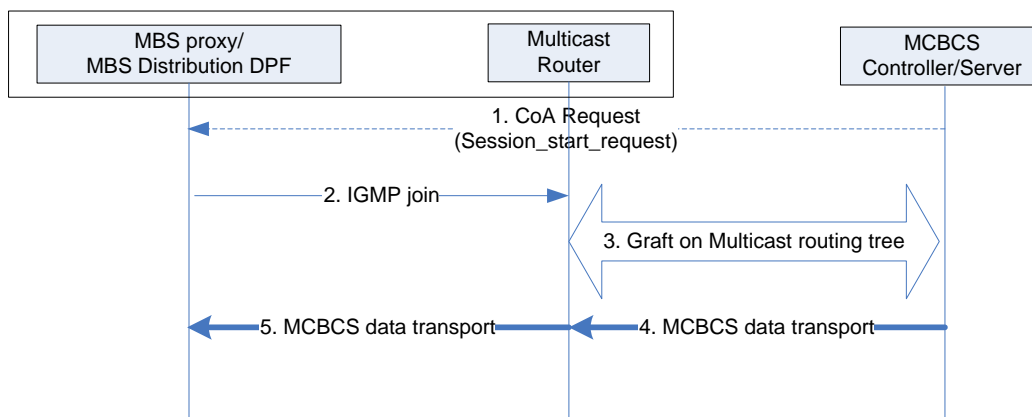


Figure 4-41 : Data transport over R3

STEP 1:

When the MCBCS Controller/Server has a MCBCS data to transmit, it sends a RADIUS CoA message to indicate the MCBCS Session Start request to the appropriate MBS Proxy in the ASN. The service association between the MCBCS Controller/Server with the corresponding MBS Proxy is either pre-configured or dynamically discovered as described in section 4.2.

STEP 2:

MBS distribution DPF sends an IGMP join message to the R3 multicast router to join the CSN multicast group for the MCBCS content.

STEP 3:

Multicast router grafts on the CSN multicast distribution tree using the IP multicast routing protocol like a PIM-SM defined in IETF. At this time, the multicast router becomes a leaf node of the multicast routing tree.

STEP 4:

MCBCS Controller/Server transmits the MCBCS content over the multicast routing tree.

STEP 5:

Multicast Router delivers the MCBCS data to the Anchor MBS Distribution DPF.

4.11.2 Data Transportation within the MCBCS Transmission Zone inside the ASN

There are two ways to support the MBS data transportation across one or more MBS Zones which are within the MCBCS Transmission Zone inside the ASN. One approach is to re-use existing WiMAX Release 1 point-to-point GRE tunnels to build a unicast-based transport distribution tree to the multiple ASN-GWs/BSs. Another approach is to build a multicast-based transport distribution tree across one or more MBS Zones, within the MCBCS Transmission Zone inside the ASN.

4.11.2.1 Unicast based Transport Multicast Distribution Tree Establishment.

The existing (non MCBCS) GRE tunnel can be used to deliver the MBS traffic within an MBS zone or an MCBCS Transmission

For the unicast-based transport multicast distribution, the MBS Distribution DPF uses a unicast-based GRE tunnel to deliver the MCBCS content to the each BS; therefore, all BSs within MBS zone will not share the same GRE key. In the same way as the unicast, when BS receives the Path-Reg-Req message from the MBS distribution DPF, BS assigns a GRE key for DL traffic for each GRE tunnel.

If the anchor MBS Distribution DPF already knows the serving MBS Distribution DPFs, it sends a R4 Path-Reg-Req message to the serving MBS Distribution DPF and the serving MBS Distribution DPF assigns the GRE key for the downlink MCBCS traffic. And then, the serving MBS Distribution DPF creates a GRE tunnel with its BSs belonged to the same MBS zone or the same MCBCS Transmission Zone.

When the anchor MBS distribution DPF receives the MCBCS data over R3, it determines for which the GRE tunnel to transport the MCBCS data towards the target BS within the MBS Zone or MCBCS Transmission Zone.

Figure 4-42 describes the example of the multicast distribution with unicast-based transport which is triggered by the Session Start signaling.

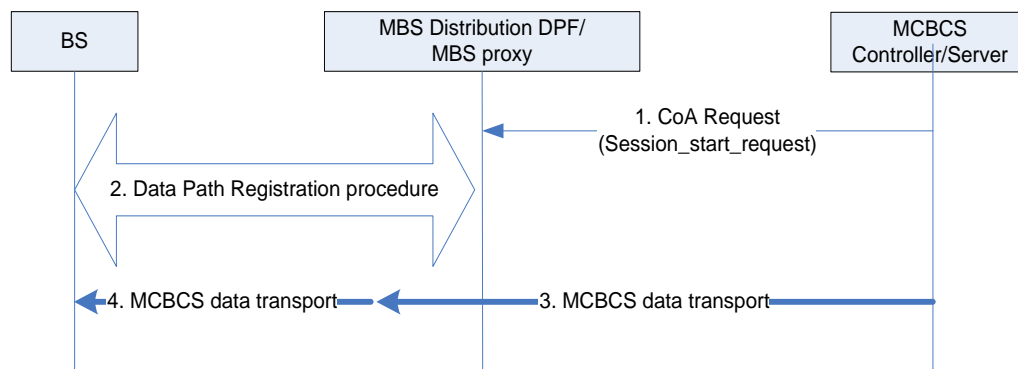


Figure 4-42: Example of multicast distribution with unicast based transport triggered by Session Start

STEP 1:

When the MCBCS Controller/Server has MCBCS data to transmit, it sends a CoA Request (Session Start request) message to the MBS Proxy/MBS Distribution DPF which may trigger the MBS data path establishment if there is no prior MBS data path was established within the ASN. In one particular scenario, the MCBCS Controller/Server may

MCBCS-DSx

use a Session Start request message to trigger a data path creation explicitly when the number of user join reaches a threshold which MAY be defined by operator. The composition of the CoA Request for the Session Start request message is presented in section 5.

STEP 2:

MBS Distribution DPF sends a Path_Reg_Req message to all BSs in MBS zone. BSs assign the GRE key and send a Path_Reg_Rsp message to the MBS Distribution DPF. For the detailed description, refer to Table 4-19 and Table 4-20 respectively.

STEP 3:

MBS Distribution DPF receives the MCBCS data from the MCBCS Controller/Server

STEP 4:

MBS Distribution DPF determines GRE key. Then, the MBS Distribution DPF transports the MCBCS data over the R6 GRE tunnel.

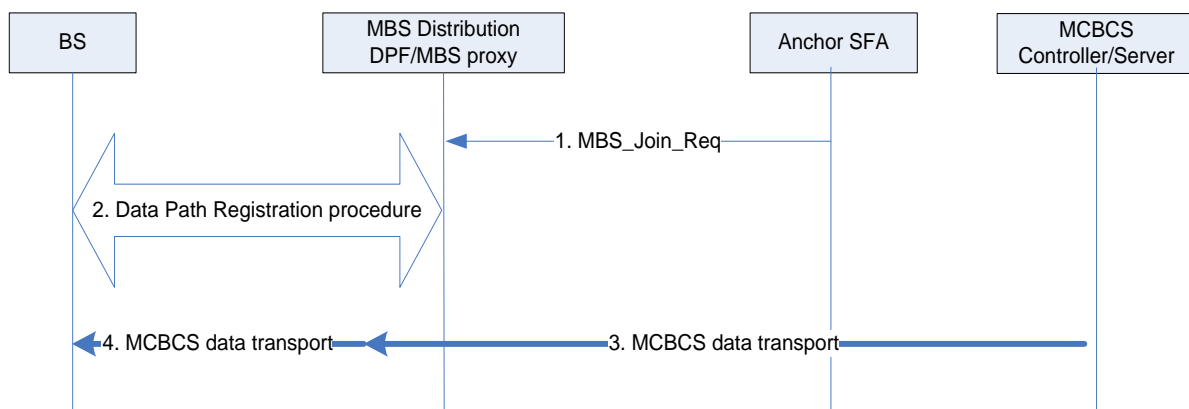


Figure 4-43 : Example of multicast distribution with unicast based transport triggered by the first MS

STEP 1:

After the anchor SFA gets the authorization successful message, the Anchor SFA of MS sends an MBS_Join_Req message to the MBS distribution DPF/MBS proxy. The composition of the MBS_Join_Req message is described in section 5.1.1.

STEP 2:

MBS Distribution DPF sends a Path_Reg_Req message to all BSs in MBS zone. BSs assign the GRE key and send a Path_Reg_Rsp message to the MBS Distribution DPF. For the detailed description of Path_Reg_Rsp message, Table 4-19 and Table 4-20 should be referred.

STEP 3:

MCBCS controller/server transports MCBCS data over multicast routing tree.

STEP 4:

MBS Distribution DPF transports the MCBCS data received from the MCBCS controller/server over R6 GRE tunnel

4.11.2.2 Multicast Distribution using Unicast-based Transport

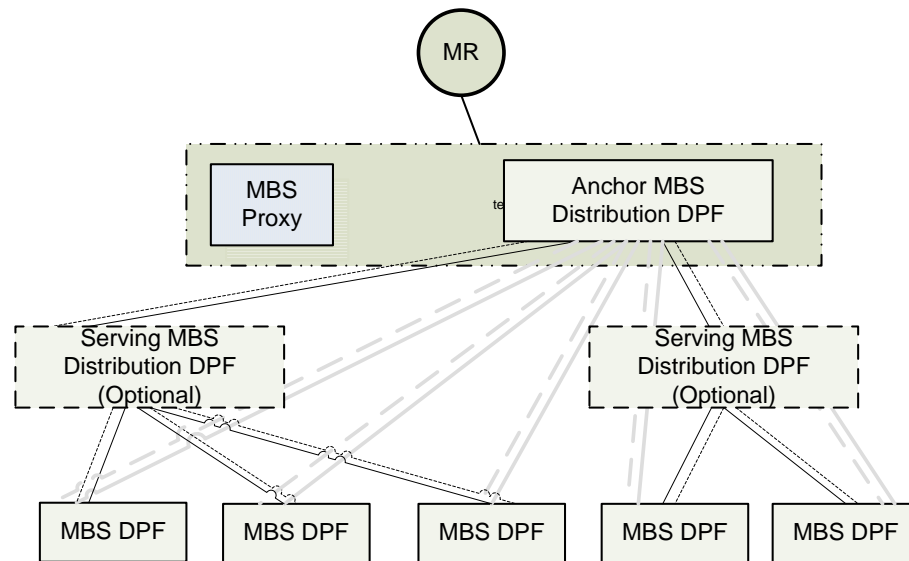


Figure 4-44 : Unicast-based Multicast-Distribution Reference Model

In this scheme, GRE tunnels as in NWG Rel-1.0 are used to deliver the MBS traffic within the MBS Zone or MCBCS Transmission Zone inside the ASN. But, the GRE tunnel for MBS should be differentiated from the one for unicast because of the following reasons:

- Same MBS content is delivered to multiple MBS receivers (i.e. the MSs) over same (common) MCID.
- The content should be delivered to all BSs within an MBS zone or an MCBCS Transmission Zone in the transmission window allowed by sync rule.
- MBS content is not dedicated on a particular MS.

Therefore, GRE tunnel for MCBCS content should be per MCBCS service based and not per MS based, and it should be shared by all the MSs who prescribed to the same MCBCS service. But, all BSs within the MBS zone do not need to share a same GRE key.

GRE tunnel can be pre-configured or can be triggered by the first MS joining the MCBCS Service, or based on session start signaling. If the GRE tunnel is pre-configured, the data path registration procedure is not needed.

4.11.2.3 Multicast Distribution using Multicast-based Transport

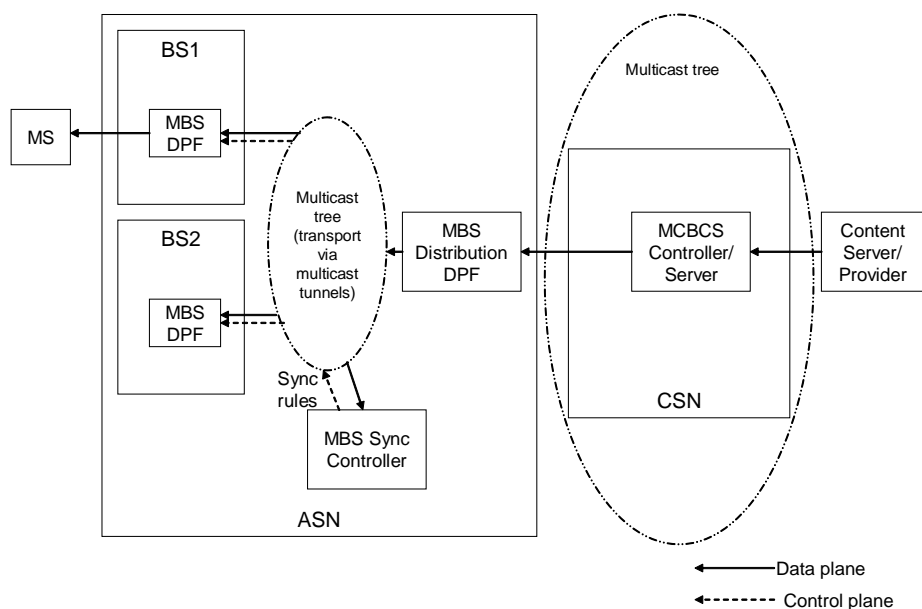


Figure 4-45 : Multicast-based Transport mechanism for Multicast Distribution support for the MCBCS content delivery

The Content Server distributes MCBCS Content via a unique IP multicast address within an ASN in IP multicast packets to the MCBCS Controller. The MCBCS Controller/Server connects to the IP multicast tree sourced by the Content Server if the CSN is multicast friendly via the support of IP multicast routing (e.g. PIM-SM, DVMRP...).

MBS Distribution DPF is located at the ASN-GW and is connected to the CSN multicast tree as a leaf (via IGMP support) and thus receives the MCBCS Contents from MCBCS content server over R3..

4.11.2.3.1 Multicast-based Transport Within the multicast-capable ASN

To support the multicast-based transport, the ASN is required to be multicast capable. Local IP multicast group is created within the MBS zone or within the MCBCS Transmission Zone in an ASN.

The concept of Local IP multicast group described here is referring to two major aspects as follows:

- Multicast data distribution
- Multicast group membership management

A. Multicast data distribution

The concept of the multicast data distribution is referring to the local IP multicast group (one per MBS Zone or per MCBCS Transmission Zone) is pertain with an ASN. Members of each group are the BSs which are part of a given MBS Zone or MCBCS Transmission Zone, and associated with the MBS Distribution DPF and MBS Sync Controller which are dedicated to the same MBS Zone or MCBCS Transmission Zone.

The MBS Sync Controller is member of this local IP multicast group because it needs to receive the MBS data prior to the construction of and the distribution of the data synchronization rules. The multicast-based multicast distribution tree, in this case, may also be used by the MBS Sync Controller to distribute the data synchronization rules within the MBS Zone or within the MCBCS Transmission Zone.

An IP packet sent to a local multicast group address is received by all the members (BSs and MBS Sync Controller) of the MBS Zone or MCBCS Transmission Zone corresponding to such multicast group.

When the MBS Distribution DPF receives a multicast IP packet carrying an MBS Content to be distributed within its MBS Zone or MCBCS Transmission Zone, it encapsulates (tunnels) such packet into an IP packet with destination address corresponding to the multicast group IP address associated with the MBS Zone or the MCBCS Transmission Zone. In other words, the MBS Distribution DPF distributes the content using point-to-multipoint (i.e. IP multicast) tunnels. The replication/distribution along the multicast tree leverages the multicast routing mechanism within the ASN.

B. Multicast group membership management

The concept of multicast group membership management is to refer to the multicast group membership that is managed through the IGMP procedures. In the ASN, each leaf of the local IP multicast tree (BSs or MBS Distribution DPF) is referred as IGMP host who joins the IP multicast group using e.g. IGMP Join procedure for the given MBS Zone or MCBCS Transmission Zone. MBS Distribution DPF is acting as a multicast source according to the concept of the IGMP (i.e. root), for this local IP multicast group.

Towards the CSN MCBCS Controller, the MBS Distribution DPF connects to the IP Multicast groups corresponding to the MBS Content that are distributed within the associated MBS Zone or MCBCS Transmission Zone. The MBS Distribution DPF connects to the multicast trees as a leaf, via the IGMP join procedure; thus, according to the concept of IGMP, the MBS Distribution DPF is the IGMP host, and the Content Server is the IGMP source.

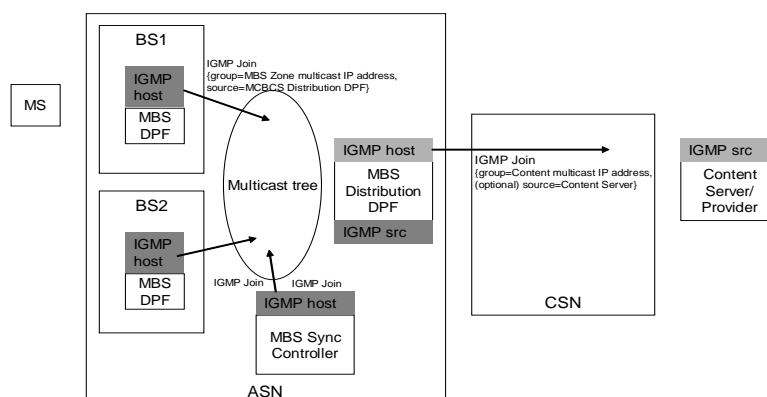


Figure 4-46 : Multicast group membership management

MCBCS-DSx

For the multicast-based multicast distribution tree, Anchor MBS Distribution DPF initiates the R6 data path registration procedure to each BS on the multicast distribution tree for MBS data. During this procedure, Anchor MBS Distribution DPF assigns same GRE key for GRE tunnel to each BS.

The multicast distribution tree is managed dynamically via the support to the IGMP messaging among the BSs within the MBS zone or the MCBCS Transmission Zone. Therefore, it is feasible for the anchor MBS Distribution DPF to also use the multicast IP address to operate and to manage the MBS data path over the multicast distribution tree.

4.11.3 Multicast-based Transport Multicast Distribution Tree Establishment.

Detailed steps for setting up a multicast based Transport Multicast Distribution data path establishment are given below as an example. The multicast leafs must use IGMPv4 or MLDv6 to join the distribution tree, the source of the multicast tree may use IGMP or other means to be part of the multicast tree.

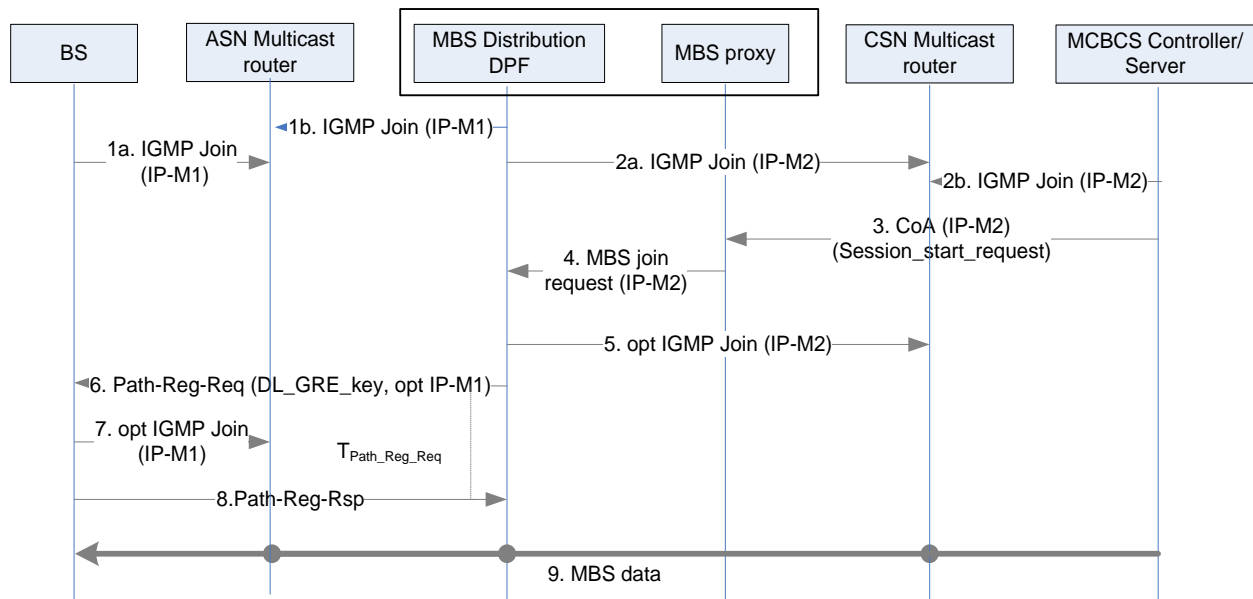


Figure 4-47 : Multicast-based Transport Multicast Distribution Data Path Establishment

STEP 1:

BSs and the corresponding MBS Distribution DPF, which are belonged to the same MBS Zone or MCBCS Transmission Zone, join IP-multicast tree (IP-M1) to establish the IP multicast transport within the ASN via the IP multicast signaling, e.g., IGMP Join (IPv4) or MLD Join (IPv6).

STEP 2:

MCBCS Controller/Server and MBS Distribution DPF, which serves the same MBS Zone or MCBCS Transmission Zone, join IP-multicast tree (IP-M2) across the ASN towards the CSN via the IP multicast signaling, e.g., IGMP Join (IPv4) or MLD Join (IPv6).

STEP 3:

When the MCBCS /Controller/Server has a MCBCS data to transmit, it sends a CoA Request message to indicate the Session Start request to the MBS proxy which may trigger the MBS data path establishment if there is no prior MBS data path was established within the ASN. In one particular scenario, the MCBCS Controller/Server can

MCBCS-DSx

leverage the CoA Request message to indicate a Session Start request to trigger a MBS data path establishment explicitly in the case when the number of user join reaches a threshold defined by an operator. CoA Request message carries the address of the IP multicast tree IP-M2. The composition of the CoA Request message for Session Start is presented in section 5.3.1.2.

STEP 4:

MBS proxy triggers the MBS distribution DPF for MBS data path establishment within the MBS zone or the MCBCS Transmission Zone. This message carries IP-multicast tree address IP-M2. The composition of the MBS_Join_Request message is presented in section 5.1.1.

STEP 5:

If MBS Distribution DPF is not yet part of the IP-multicast tree (IP-M2), it can join it using the IP-multicast address received in step 4.

STEP 6:

MBS distribution DPF sends a Path_Reg_Req message to all BSs in MBS zone. To ensure that downlink GRE tunnels between all BSs and MBS Distribution DPF in the MBS zone to be assigned with the same GRE key, MBS Distribution DPF is responsible for assigning the GRE key for a downlink (DL_GRE_key) and signals it to all BSs in the zone using Path-Reg-Req. Optionally Path-Reg-Req may also include IP-multicast address (IP-M1) to enable BSs joining the multicast tree if they are not yet part of the IP multicast tree.

STEP 7:

If BS is not yet part of the IP-multicast tree (IP-M1), it can join it using the IP-multicast address received in step 6.

STEP 8:

BSs in the MBS zone select the same GRE key for a downlink based on the information that they received in step 4 and send it to MBS Distribution DPF using Path-Reg-Rsp message. The composition of the R6/4 Path_Reg_Req and R6/4 Path_Reg_Rsp message is presented in sections Table 4-19 and Table 4-20.

STEP 9:

MBS data is transmitted over IP multicast distribution.

4.12 MCBCS Network Resource Management

4.12.1 MBS Data Synchronization

MBS data synchronization is designed to coordinate the MCBCS content downlink transmission over a single frequency or multi-frequency WiMAX network within or across one or more MBS zones which are belonged to the same MCBCS Transmission Zone.

For the MCBCS data synchronization support, the current of IEEE 802.16-Rev2 [3] provides mechanisms for the intra and inter MBS zones data synchronization support.

4.12.1.1 Intra-MBS Zone Data Synchronization

Two main mechanisms for intra-MBS Zone data synchronization support:

- Frame-level coordination, and
- Macro diversity

If the frame-level coordination is supported, all BSs that belong to the same MBS Zone, the following coordination shall be assured:

- The set of MAC SDUs carrying MBS content shall be identical in the same frame in all BS in the same MBS zone;
- The mapping of MAC SDUs carrying MBS content onto MAC PDUs shall be identical in the same frame in all BS in the same MBS Zone, meaning, in particular, identical SDU fragments and identical fragment sequence number (block sequence number) and fragment size

Coordination in the MBS Zone assures that the SS may continue to receive MBS transmissions from any BS that is part of the MBS Zone, regardless of the SS operating mode—Normal Operation, Idle Mode—without need for the SS to register to the BS from which it receives the transmission.

If the macro-diversity synchronization is required across the entire set of the BSs that belonged to the same MBS Zone area, in addition to the above considerations, the following synchronization level shall be assured:

- MBS Bursts positions and dimensions as well as PHY parameters associated with each MBS Burst (e.g. FEC Type, Modulation Type, Repetition Coding, Boosting, HARQ Settings) must be identical.
- Mapping SDUs into the MBS Bursts must be identical.
 - SDUs must be identically mapped into MAC PDUs, which implies identical ordering of SDUs; identical Headers and Subheaders used; identical fragmentation, if applicable.
 - Ordering of the MAC PDUs within a Burst must be identical.

MBS Zones may overlap, hence, a BS may participate in more than one MBS Zones. When a BS participates in more than one MBS Zone, the resources (time and frequency) should be synchronously allocated to avoid conflict.

4.12.1.2 Inter-MBS Zones Data Synchronization

For the inter-MBS Zones data synchronization, IEEE 802.16-Rev2 [3] supports the Frame-offset coordination.

Frame-offset coordination implies the transmission of the same MBS service flow within the specified frame-offset boundary across MBS zones. The synchronization of the MBS service flow downlink transmission is coordinated across the MBS Zones via the support of MBS MAP Message over the R1 interface. The synchronization of the MBS service flow shall be conformed to an allowable number of R1 frames that may be arrived earlier or later than the current serving MBS zone for the MS. Thus, the number of R1 frames is specified in term of frame offset. The range of this frame offset is from +7 to -7 frames, inclusive, between any two neighboring MBS zones.

There are two-level of frame-offset coordinations across the MBS Zones:

Level-1: The frame-offset coordination focuses only on the daisy-chaining of the MBS MAP messages without the restriction of the synchronization of user data (i.e. see Level-2 descriptions below). Such level of the frame-offset coordination maintains the power-saving capability for the MS when it is crossing MBS Zones.

Level-2: A more strict form of frame-offset coordination requires that the data transmissions between neighboring MBS zones are synchronized as for the MBS MAP message. In terms of the transmission contents, the data synchronization requirement in this case is the same as for frame-level coordination within an MBS zone. With the Level-2 frame-offset coordination, not only the power savings can be supported via the MBS_MAP message chaining, but also the continuity of data reception can be maintained for the MBS service flow.

4.12.1.3 MBS Data Synchronization Functions

The following diagram highlights the NRM reference model for the MBS data synchronization design:

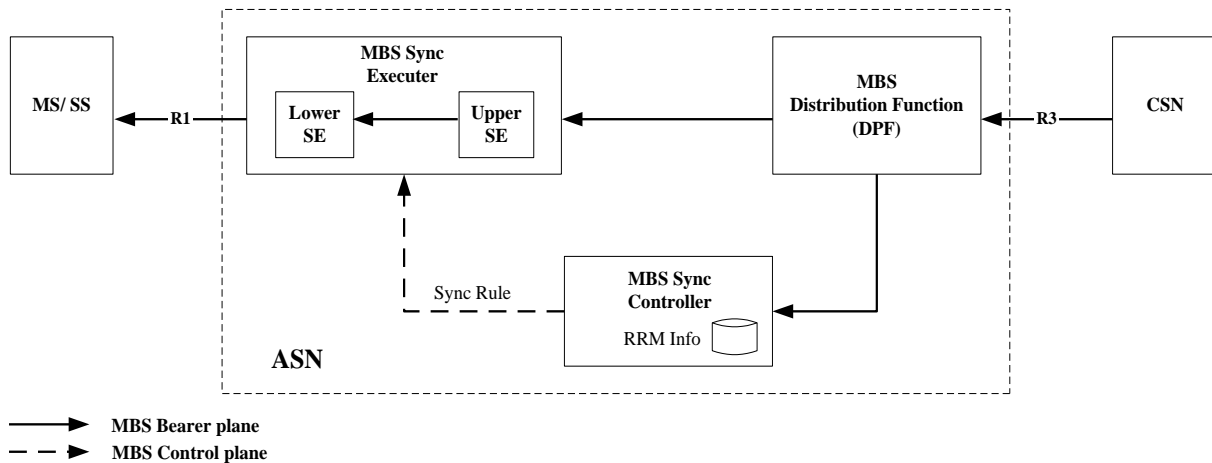


Figure 4-48 : MBS Data Synchronization Generic Reference Model

The key functional blocks of the MBS Data Synchronization functions are summarized as follows:

MBS Distribution Data Path Function:

The MBS Distribution Data Path Function (DPF) is the central MCBCS bearer plane control entity at the ASN-GW to receive and to process the downlink transmission of an MCBCS program sent from the CSN, classifies the incoming SDUs into the appropriate MCBCS Service Flow (e.g. 6-tuple classification) and applies the corresponding WiMAX Convergence Sublayer rules (such as e.g. Packet Header Suppression).

More details on the MBS Distribution DPF shall be referred to section 4.5.

Depending on the MBS Sync functions de-composition - i.e. whether the Upper MBS Sync Executer is co-located with the MBS Distribution DPF or not, different types of MBS traffic payloads will be transported over the R6 data path. The MBS data path payload is identified by the payload type that describes the packaging format of the MBS data sent to a BS. The data path payload for MBS Service Flow can be:

- Raw IP packets (Type 1 data path – as defined in [5]). For Type 1 data path, MBS Distribution DPF assigns GRE Sequence Numbers to each packet (the numbering scope is per GRE Key)
- Pre-processed SDU(s) it is the MAC burst which contains one or more MAC PDUs and each MAC PDU contains one or more IP packets that are being packed or fragmented. Such data path type is referred as Type 3 data path.

Among the two types of data path to support the MCBCS service, Type 1 data path is mandatory and Type 3 is optional.

MBS Sync Controller

MBS Sync Controller is the centralized control functional entity to synchronize the MBS downlink transmission over one or more MBS Zone(s). It is responsible for specifying the synchronization rules, including the timing control, required to support the step-1 to step-5 bearer processing example as shown in Annex-A in the MBS Sync Function operation which includes MBS Sync Controller receiving the MBS data, scheduling the MBS Bursts, determining PHY and MAC parameters of each Burst, determining how data is mapped to the MBS Bursts and finally, distributing this information to MBS Sync Executors in a form of an MBS Sync Rules.

To achieve the effective use of radio resources, the MBS Sync Controller leverages the most recent radio resource management information (RRM) to determine the common availability of the radio resource across all the BSs

which belong to the same MBS zones to deliver the given MCBCS service. The design and implementation of the RRM support for phase-1 MCBCS is outside the scope of this specification.

In order to perform effective scheduling decisions for MBS traffic, the MBS Sync Controller should either be pre-configured with some MBS bearer transport characteristics and QoS requirements, or learn them dynamically.

The MBS synchronization rules should include all the parameters required to perform bearer operations in the MBS Sync Executer in order to enable the macro-diversity or MBS frame-level coordination support within an MBS Zone or frame-offset coordination across MBS Zones, and to construct the corresponding MBS_MAP_IE, MBS_MAP, MBS_Data_IE etc. as specified in [13].

The MBS Sync Controller sends the MBS Sync Rules to the MBS Sync Executer for processing.

MBS Sync Controller should have its clock synchronized with the corresponding BSs that belong to the MBS Zone or the MCBCS Transmission Zone. The specific technique of synchronization between the MBS Sync Controller and the MBS Sync Executer is out of scope of this specification; however, the precision shall be compliant to the IEEE 802.16Rev2 specification [3] for the airlink transmission.

Depending on the network implementation, some parts of the synchronization rules may be preconfigured in the corresponding entities (i.e. Sync Executer).

The MBS Sync Controller shall be located either at the ASN GW (collocated with the MBS Distribution DPF Function entity), and optionally be located at one of the selected BSs belonged to the same MBS Zone.

MBS Sync Executer

MBS Sync Executer is the distributed functional entity that receives MBS payload from the MBS Distribution DPF or from the MBS DPF, and receives the MBS Synch Rules from the MBS Sync Controller. MBS Sync Executer is responsible for executing the provided MBS synch rules and performing the MBS bearer processing operations (as described in step 1 to step 5 in Annex-A).

Given the considerations of different steps of MBS bearer processing (as shown in step 1 to step 5 in Annex A)- may be performed at ASN-GW and at the BS, the MBS Sync Executer is further partitioned into:

- Upper MBS Sync Executer (Upper SE), and
- Lower MBS Sync Executer (Lower SE).

The Upper SE is responsible for the step-1 and step-2 bearer processing operations, while the Lower SE is responsible for the rest of bearer processing operations (i.e. step-3 to step-5) as shown in Annex A.

The Lower SE is always located in the BS. The Upper SE shall be located either in the BS, and optionally be located in the ASN GW (co-located with the MBS Distribution DPF functional entity).

4.12.1.4 MCBCS Synchronization Functions implementation models

With the possible separation of the Upper SE and Lower SE, three possible implementation models are defined in the following. Only Model B is mandatory required to be implemented and the other two Models are optional.

Model A:

The MBS Sync Controller is co-located with the MBS Distribution DPF and the Upper SE in the ASN GW.

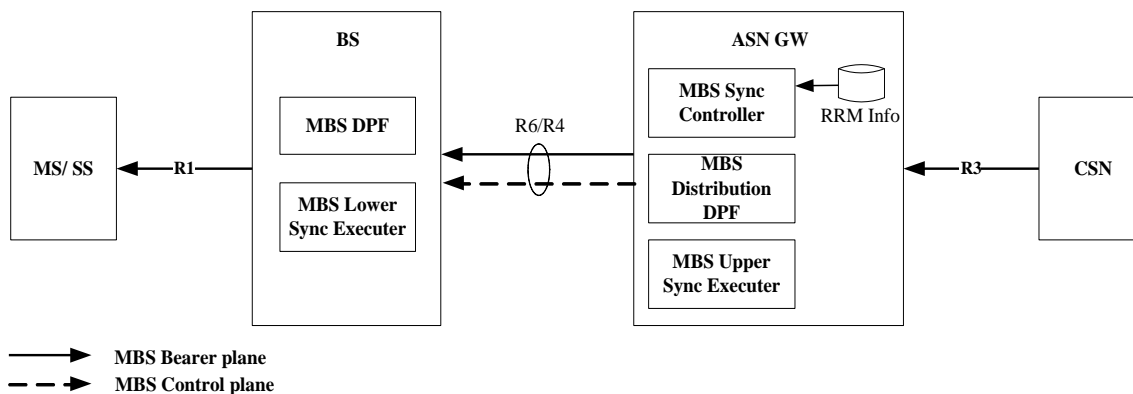


Figure 4-49 : Model A implementation of MCBCS Sync Functions

In this model, R6/R4 Data Path between the ASN GW and the BS uses Type 3 payload and delivers processed SDU(s) with one or more IP packets that are being packed or fragmented into MAC PDU(s) contained in a MAC Burst which is based on the packet processing outcome as described in steps 1-2 of Annex A. The corresponding MBS Synchronization Rules that are used to coordinate all BSs within the same MBS Zone to synchronize the bearer processing as shown in step 3 to step 5 and some datapath control signaling are delivered to all targets BSs over R6/R4 control plane.

Model B:

The MBS Sync Controller is co-located with the MBS Distribution DPF at the ASN GW. Both – the MBS Upper SE and the MBS Lower SE are located in the BS.

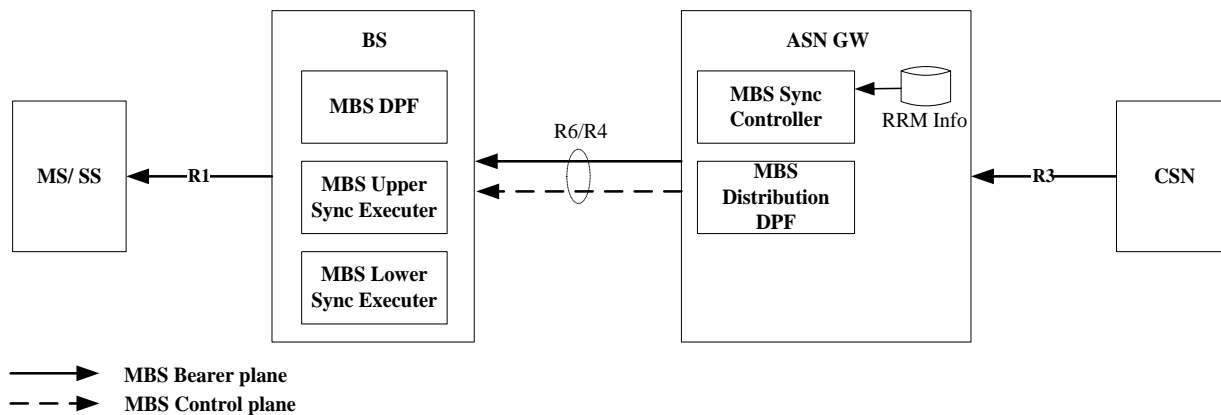


Figure 4-50 : Model B implementation of MCBCS Sync Functions

In this model, R6/R4 Data Path between the ASN GW and the BS uses Type 1 payload (as defined in [5]) and delivers raw IP packets which have been classified for the particular MBS Service Flow and tagged with the corresponding GRE Sequence Number by the MBS Distribution DPF. The corresponding MBS Synch Rules (for step 1 to step 5 bearer processing as described in Annex A, and some data path related control signaling) are delivered to the BSs over R6/R4 control plane from the ASN GW.

Model C:

MCBCS-DSx

- 1 The ASN GW implements the MBS Distribution DPF. Both the MBS Upper SE and the MBS Lower SE are located
 2 in the BS. The MBS Sync Controller is located in one of BSs which are belonged to the same MBS Zone (i.e.
 3 “Super BS”) and also participates in MBS data path (co-located with the MBS DPF).

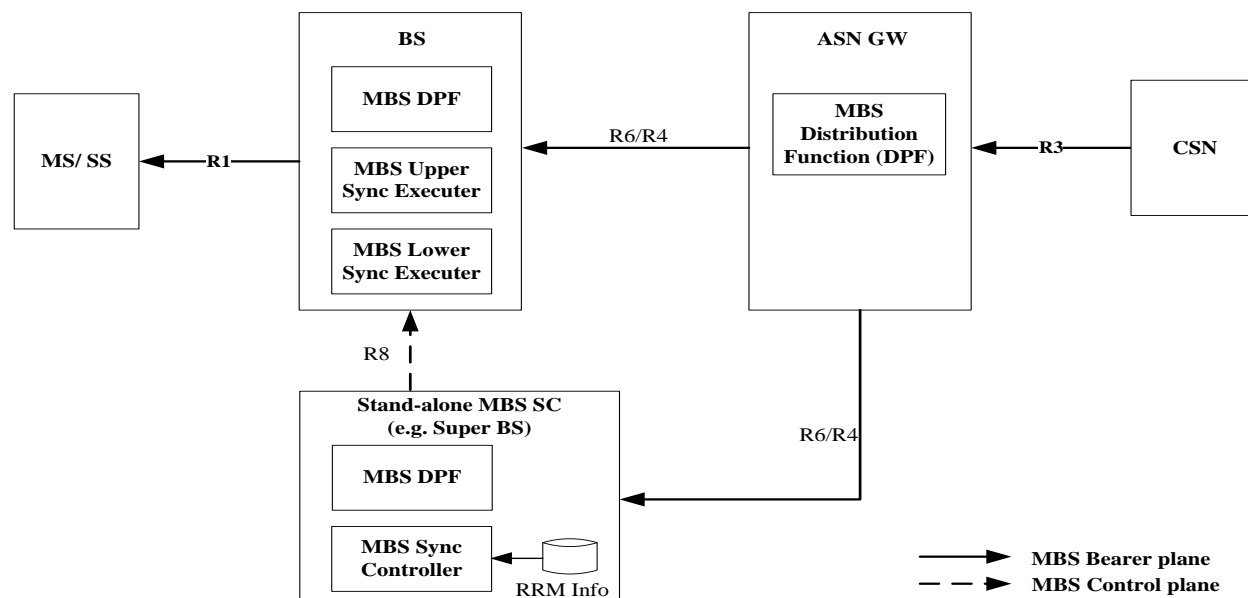


Figure 4-51 : Model C implementation of MCBCS Sync Functions

In this model, R6/R4 Data Path between the ASN GW and the BS uses Type 1 payload (as defined in [5]) and delivers raw IP packets which are classified for the particular MBS Service Flow and tagged with the corresponding GRE Sequence Number by the MBS Distribution DPF (the same as in the Model B). The corresponding MBS Sync Rules (for step 1 to 5 bearer processing as described in Annex A, and some data path control signaling) are delivered to the BSs over R8 control plane sent by MBS Sync Controller which is resided at one of the BSs belonging to the same MBS Zone (e.g. “Super BS”).

4.12.1.5 Implementation models coexistence considerations

It is mandatory to support the MBS Sync Controller at the ASN-GW using Type-1 data path. However, the negotiation of MBS Data Synchronization system capability may occur during the MCBCS service initialization and establishment for the MBS data path. If such negotiation event happens, the entity that does not support the requested capability, e.g. data path payload type, will reject the MCBCS service establishment.

From functional partitioning and data path configuration perspective, there is no difference between Models B and C. If the BS is Model C while the ASN GW is Model B (or vice versa), the data path should be able to be established. Model C BS which supports the MBS Sync Controller capability may be disabled when it receives the MBS Sync Rule from Model B ASN GW. In the case of Model B BS and Model C ASN GW, Model B BS can use MBS Sync Rule provided by the MBS Sync Controller which is resided at the Model C BS. The negotiation between the Model B and Model C system is basically to decide for which the network entity that the MBS Sync Controller, identified by the MBS Sync Controller ID, should be enabled for the given MBS Zone.

4.12.2 Synchronization methodology

It is assumed the MCBCS Services that may benefit from transmission synchronization are delay tolerant. If MBS data traffic is required to be transmitted over the air synchronously towards the target BSs, synchronization of the air transmissions can be achieved only at the expense of some delay. The minimum delay of synchronization is close to the latency introduced by communication between the MBS Sync Controller or MBS Distribution DPF to the most distant MBS Sync Executor or MBS DPF in the network..

From the airlink downlink transmission perspective, within an MBS Zone, MBS Sync Controller may introduce delay of up to 255 airlink frames for which each is 5 msec apart as specified in [3]. However, if MBS service continuity is supported, when across the MBS Zones, up to 262 airlink frames¹ (i.e. 255 + inter MBS Zone offset) can be introduced by the MBS Sync Controller. Never-the-less, one should be aware that the actual tolerant of the delay is dependent on the given MCBCS service.

] To achieve transmission synchronizations, the following methodology is assumed:

- Time is divided into the periods (a multiple of the Frame Length).
- Data, which is accumulated during the period $[T_0; T_1]$ (also referred as an Accumulation Period) will be transmitted during the period $[T_2; T_3]$ (also referred as a Transmission Period).
- Lost data may be recovered during the period $[T_1; T_2]$.
- The intervals must be carefully selected to be long enough to accommodate propagation of the Sync Rule from the Sync Controller to all the BSs as well as the lost data recovery handshake.
- The MBS Sync Controller transmits Current Sync Rule at the expect time which has been indicated by the Previous Sync Rules, and may re-transmit Sync Rule when it was lost and was request by the receiver.

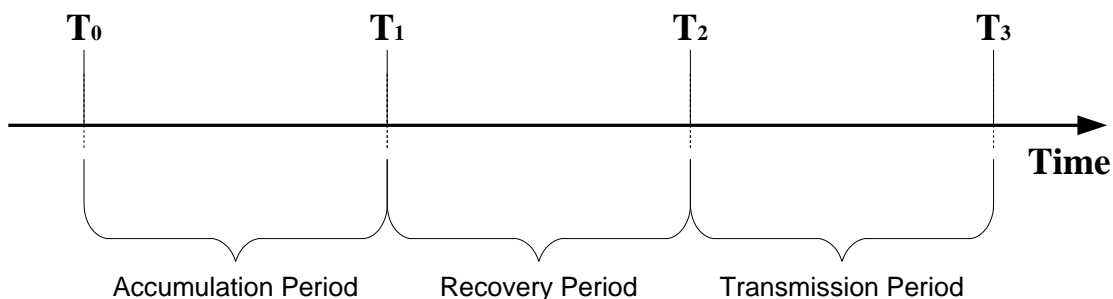


Figure 4-52 : MBS Data Synchronization methodology

MBS Traffic should take precedence over Unicast Traffic except for the emergency traffic; otherwise MBS zone wide synchronization may not be achieved. In the case of conflict over available resources the preference should be given to MBS traffic. MBS Traffic should be also prioritized over unicast in the backhaul unless the bandwidth is guaranteed.

The MBS Sync Controller adds linkage information (such as timing offset) in the provided MBS Synchronization Rule. This allows the MBS Sync Executor to derive the expected time of transmission for the next consecutive Sync Rule and to trigger the recovery mechanism for the MBS Synchronization Rule which is considered lost. Through linkage information, the maximum arrival time of the next MBS Synchronization Rule should be the sum of the *expected time of arrival* for the next MBS Synchronization Rule plus the maximum network propagation delay between the MBS Sync Controller and the MBS Sync Executor.

¹ Based on the IEEE 802.16-Rev2, inter-MBS Zones allows the frame-offset coordination from -8 to +7 between two neighbor BSs which belong to two different neighbor MBS Zones. Hence, the maximum delay can be increased $255 + 7 = 262$ airlink frame

4.12.2.1 MBS Sync Rules Design Considerations

The signaling of the MBS Sync Rules over R6, R4 or R8 based on WiMAX ASN protocol design schematic and can be signaled using either the unicast or the multicast transport.

A recovery mechanism is required for the MBS Sync Rule transport between the MBS Sync Controller and the MBS Sync Executor to ensure the Sync Rule delivery to the MBS Sync Executor. If the Sync Rule is not recovered, the BSs/ MBS Sync Executors that lost it can skip the particular portion or the entire MBS DL transmission. Thus, if the packet loss probability is low enough then the recovery mechanism might be omitted, therefore, the recovery of the MBS Synchronization Rule is optional.

The options for the MBS SyncRule recovery mechanism:

- Preventive repetition transmissions (i.e. sending multiple copies of the same MBS Sync Rule). Such approach is controlled by the MBS Sync Controller to operate this transmission mode, whereas the MBS Sync Executor SHALL be able to discriminate and discard the duplicate copies .
- Explicit query by the MBS Sync Executor when it detects that the MBS Sync Rule is lost after the expected time of arrival which is derived from the maximum network transit delay between the MBS Sync Controller and the MBS Sync Executor. This recovery mechanism uses unicast request/ response transaction between the MBS Sync Executor and the MBS Sync Controller.

Support of the explicit recovery mechanism (i.e. the MBS Sync Executor to query the MBS Sync Controller) may be preprovisioned in the relevant entities or may be negotiated during the MBS service establishment.

MBS Sync Executor processing Sync Rule should perform consistency check between Sync Rule information and the available MBS traffic. In addition, the MBS Sync Executor should be able to handle error conditions (packet duplication, packet loss, etc.) due to the lost of MBS Sync Rule.

4.12.3 MCBCS Data Synchronization Support

4.12.3.1 MBS Sync Rule delivery

4.12.3.1.1 Synchronization Rules announcement

Once the infrastructure for the MBS Service Flow is activated, MBS Sync Controller starts to announce MBS Sync Rules by sending MBS Sync Rule Announcement message.

If unicast infrastructure is used, MBS Sync Controller sends MBS Sync Rule Announcement message directly to the unicast IP address of the corresponding MBS Sync Executors. If multicast infrastructure is used, MBS Sync Controller sends MBS Sync Rule Announcement message to the multicast IP address allocated for Sync Rule distribution in the particular MBS Zone.

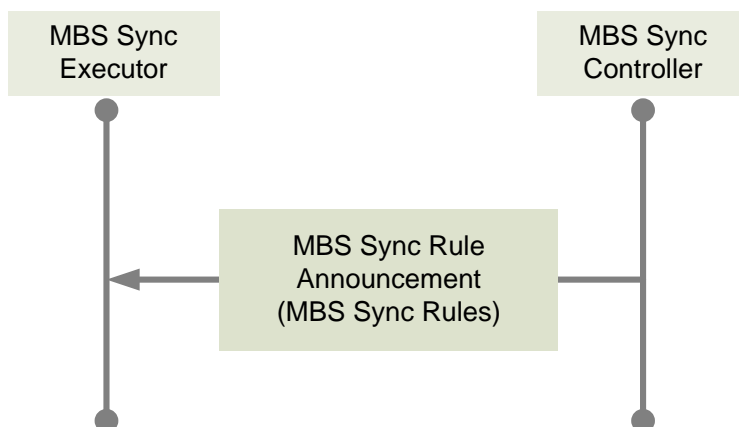


Figure 4-53 : MBS Sync Rule announcement by MBS Synchronization Controller

Depending on the implementation, some parameters in the synchronization rules may be preconfigured in the Sync Executor.

The following text explains Synchronization Rule construction principles:

▪ **Sync Rule and MBS Burst timing**

The expected time of arrival for the next MBS Sync Rule is indicated by Next Sync Rule expected TOA TLV in the previous MBS Sync Rule Announcement message. The MBS Burst shall be transmitted in the air frame indicated by the MBS Burst Frame Offset TLV relative to MBS Sync Rule expected TOA. The time interval between the expected MBS Sync Rule's time-of-arrival and transmission time of the 1st MBS Burst described in the Sync Rule should be long enough to allow Sync Rule message recovery (if it is lost).

The particular MBS Burst may be set into repetitive scheduling by defining the periodicity interval (MBS Burst Scheduling Cycle TLV).

Multiple MBS Burst instances may be defined in the same MBS Sync Rule thus describing some repetitive pattern.

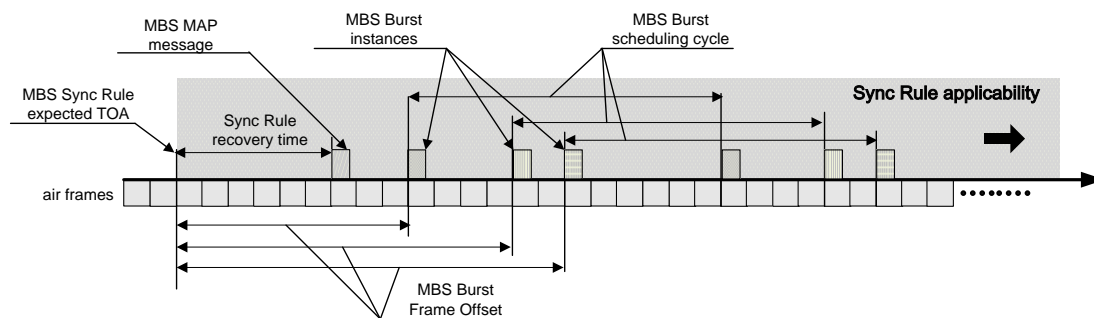


Figure 4-54 : MBS Sync Rule enforcement time and MBS Burst scheduling

Note, that MBS Sync Rule may specify parameters for one or more MBS Burst transmissions for a given MBS permutation zone.

▪ **MBS Burst Size and Position**

MCBCS-DSx

MBS Burst position and size in the air frame are defined in the terms used in MBS MAP IE, and MBS DATA IE – via OFDMA Subchannel Offset, OFDMA Symbol Offset, Number of OFDMA Symbols and Number of OFDMA Subchannels TLVs.

▪ **Rules for mapping the MBS Data into the allocated MBS bursts for a given MBS**

Data buffers in MBS DPF/ SE are indexed by either MBS Zone ID/ MCID pair or R6 data path Tunnel ID (for GRE tunnel it is GRE Key).

The processing the MBS Sync to construct the MBS bursts in BS depends on the data path type and the scheduling decision of the MBS service flow(i.e. MCID) towards a given MBS burst within a given MBS permutation zone for a given downlink subframe .

For Type 3 Data Path:

Type 3 data path delivers MBS MAC Bursts corresponding to one or more MCIDs as a data packet over the R6/ R4 data path tunnel. There will be only one data path tunnel between a BS and an MBS Distribution DPF for every MBS Zone). So, there is no need to provide Data Path Identifier as a part of MBS Burst/ MBS Data Info IEs.

GRE Sequence Number of the particular packet in a data buffer (indexed by the GRE Key) indicates the MBS MAC Burst to be scheduled in the particular MBS Burst instance.

For Type 1 Data Path:

Type 1 data path specifies the 1st SDU Sequence Number and the Last SDU Sequence Number in the Data Buffer to be scheduled in the particular MBS Burst instance. The rule defines MAX PDU Size to be used as a rule for data fragmentation/ packing. The rule also includes the List of SDU Sizes to be used in the case the particular SDU has been lost on the data path (and has not been recovered).

▪ **MBS Burst PHY Parameters**

MBS Burst PHY parameters:

- Randomization
- FEC
- Bit interleaving
- Repetition Coding indication (MBS MAP IE)
- Modulation
- Boosting
- DIUC
- Downlink Burst Profile
- Permutation (MBS MAP IE)
- DL_PermBase
- PRBS_ID

If the value of TLV remains same in the consecutive MBS_Sync_Rule message, the MBS sync controller may exclude these TLVs in the following MBS_Sync_Rule message except the TLVs identifying the Sync Rule (This TLVs shall be included in every MBS_Sync_Rule message.. The parameters that identify the Sync Rule are Sync Rule GPS Timestamp and MBS Zone Id.

Table 4-37 : MBS_Sync_Rule_Announcement from MBS sync controller to MBS sync executor

IE	Reference	M/O	Notes
Sync Rule GPS Timestamp	5.2.17	M	32 bit GPS timestamp value identifying Sync Rule. The same value as used in the previous Sync Rule pointer (Next Sync Rule TOA TLV of the previous Sync Rule) SHALL be used.
Next Sync Rule expected TOA	5.2.49	O	GPS timestamp corresponding the expected Time of Arrival for the next Sync Rule. Used for Sync Rule recovery mechanism. If missing, there is no recovery mechanism.
MBS zone ID	5.2.9	M	See IEEE802.16-Rev2[3] for further details. MBS Zone ID = 0 shall not be used.
MBS Burst	5.2.48	O	Each instance of this compound TLV describes MBS Burst. Zero or more instances of this TLV may be included in the message. If no MBS Burst TLVs are included in the message, then previous MBS Sync Rule is invalid.
> MBS Burst Frame offset	5.2.26	CM	16 bit value, specify the MBS Burst Frame Offset from the time specified in the GPS Timestamp TLV.
> Next MBS Burst Frame offset	5.2.38	O	Should be specified for the next MBS Burst in the sync rule.
> MBS Burst Scheduling Cycle	5.2.50	O	16-bit value. If included, defines the periodicity of MBS burst scheduling (in air frames).
> MBS_Data_Info	5.2.20	CM	MBS data packet information to be applied by the sync rule Multiple instances of this IE may be included for Type 1 data path. The order in which these IEs are included in the MBS Burst instance define the order of MAC PDUs for the corresponding MBS Service Flows in the Burst. For Type 3 data path, only 1 instance shall be included.
>> MCID		M	See IEEE802.16-Rev2[3] for further details. MCID is 12 bits over the R1 interface. Indicates the MCID which corresponds the MBS Service Flow for the particular MBS Zone ID. Valid only in the boundaries of this MBS Zone. May indicate the Data Buffer for Type 1 Data Path. For Type 3 Data Path, multiple instances of this IE may be included to indicate the MCIDs referred in the Burst.
>> MBS MAC Burst SN	5.2.51	O	Shall be included for Type 3 data path (specific for Type 3 data path). Indicates the sequence number of the packet (GRE SN for GRE tunnel) representing the

			MBS MAC Burst to be used in the MBS Burst instance.
>> GRE sequence number start	5.2.21	O	The GRE sequence number of the first MBS data packet (SDU) in the particular Data Buffer to be applied by the sync rule for the particular MBS Burst instance. This IE is specific for Type 1 Data Path.
>> GRE sequence number end	5.2.22	O	The GRE sequence number of the last MBS data packet to be applied by the sync rule. Specific for Option 1 scheduling rule. This IE is specific for Type 1 Data Path.
>> MAX MAC PDU Size	5.2.52	O	MAC PDU size that may be used to define fragmentation/ packing rule for SDUs. May be included for Type 1 Data Path.
>> MBS SDU packet size	5.2.53	O	One or more MBS data packet size in the order of GRE sequence number If there is a MBS data packet loss, BS can use this TLV to assign the air resource for Macro-diversity.. May be included for Type 1 Data Path.
> MBS_DATA_IE_context	5.2.24	O	If Macro diversity is supported, this TLV is mandatory. MBS_DATA_IE context defined in IEEE802.16-Rev2 [3].
>> MBS Burst Frame Offset	5.2.26	CM	See IEEE802.16-Rev2 [3] for further details.
>> Next MBS MAP change indication	5.2.27	CM	See IEEE802.16-Rev2 [3] for further details.
>> Next MBS No. OFDMA Symbols	5.2.28	O	If the Next MBS MAP change indication is 1, this TLV is included. See IEEE802.16-Rev2 [3]for further details.
>> Next MBS No. OFDMA Subchannels	5.2.29	O	If the Next MBS MAP change indication is 1, this TLV is included. See IEEE802.16-Rev2 [3] for further details.
>> MBS DIUC	5.2.30	CM	See IEEE802.16-Rev2 [3] for further details.
>> OFDMA symbol offsets DATA IE	5.2.31	CM	See IEEE802.16-Rev2 [3]for further details.
>> subchannel offset DATA IE	5.2.32	CM	See IEEE802.16-Rev2 [3]for further details.
>> Boosting	5.2.33	CM	See IEEE802.16-Rev2 [3]for further details.
>> No. OFDMA Symbols	5.2.34	CM	See IEEE802.16-Rev2 [3]for further details.
>> No. Subchannels	5.2.36	CM	See IEEE802.16-Rev2 [3]for further details.
>> Repetition Coding indication	5.2.37	CM	See IEEE802.16-Rev2 [3]for further details.
>> Next MBS Burst frame offset	5.2.38	CM	See IEEE802.16-Rev2 [3]for further details.
>> Next OFDMA symbol offset	5.2.39	CM	See IEEE802.16-Rev2 [3]for further details.

MBS_MAP_IE_Context	5.2.25	M	See IEEE802.16-Rev2 [3]for further details.
> MBS permutation zone defined	5.2.40	M	0: MBS data burst is defined 1: MBS permutation zone is defined See IEEE802.16-Rev2 [3]for further details.
> OFDMA symbol offset MAP IE	5.2.41	M	See IEEE802.16-Rev2 [3]for further details.
> subchannel offset MAP IE	5.2.42	CM	If the MBS permutation zone defined is 0, this TLV is included.
> Permutation	5.2.43	CM	See IEEE802.16-Rev2 [3] for further details.
> DL_PermBase	5.2.44	CM	See IEEE802.16-Rev2 [3] for further details.
> PRBS_ID	5.2.45	CM	See IEEE802.16-Rev2 [3] for further details.
> MBS MAP message allocation included indication	5.2.46	CM	See IEEE802.16-Rev2 [3] for further details.
> Boosting	5.2.33	CM	See IEEE802.16-Rev2 [3] for further details.
> MBS DIUC	5.2.30	CM	See IEEE802.16-Rev2 [3] for further details.
> Repetition Coding indication	5.2.37	CM	See IEEE802.16-Rev2 [3] for further details.
> No. Subchannels	5.2.36	M	See IEEE802.16-Rev2 [3] for further details
> No. OFDMA symbols	5.2.34	M	Indication of burst size of MBS MAP message with the number of OFDMA symbols.
> Downlink Burst Profile	5.2.47	O	See IEEE802.16-Rev2 [3] for further details. This TLV is needed when it is the very first time for this burst profile is used. The subsequent MBS Sync Rule to refer to this burst profile is optionally to include this TLV.
BS Info		O	
> BS ID		O	

4.12.3.1.2 Synchronization Rule recovery

MBS Sync Executer keeps track of the expected time of arrival for the next MBS Sync Rule. MBS Sync executor can identify the time of arrival of the next MBS Sync rule using the Next Sync Rule expected Time of Arrival

information in the current MBS sync rule. If the MBS sync executor has not received the next sync rule by the expected arrival time, it considers that the MBS Sync rule is lost and then it sends a MBS Sync Rule Request message to the MBS sync controller requesting a MBS Sync rule. MBS Sync controller retransmits the requested MBS Sync Rule message to the MBS Sync executor (using unicast infrastructure).

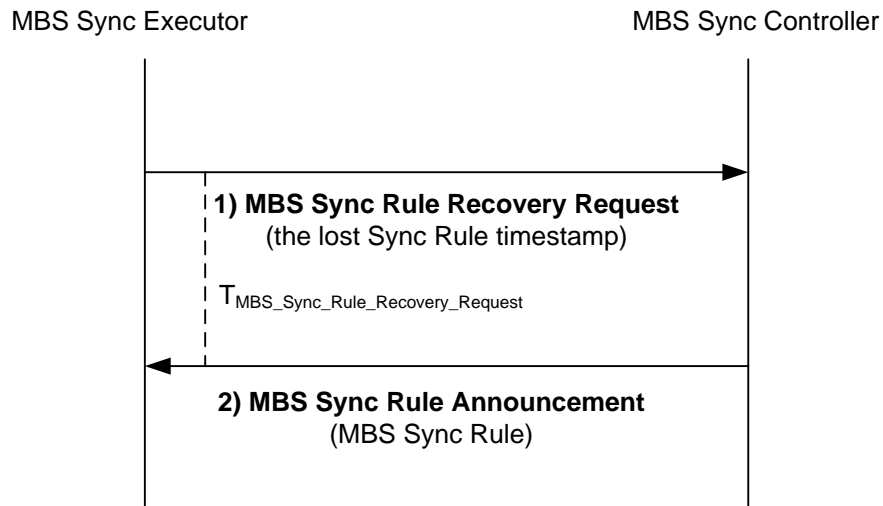


Figure 4-55 : MBS Sync rule recovery

STEP 1

If MBS Sync Executor did not receive the next MBS Sync rule from the MBS Sync controller, it requests a MBS Sync rule by sending a MBS Sync Rule Request message to the MBS sync controller. At this time, the MBS_Sync_Rule_Request message includes the Sync Rule GPS Timestamp referring the missing MBS Sync Rule (as per Next Sync Rule expected TOA of the previous Sync Rule)

Table 4-38 : MBS_Sync_Rule_Request from MBS sync executor to MBS sync controller

IE	Reference	M/O	Notes
Sync Rule GPS Timestamp	5.2.17	M	GPS Timestamp of the missing Sync Rule.
MBS zone ID	5.2.9	M	See IEEE802.16-Rev2 [3] for further details. MBS Zone ID = 0 shall not be used.
BS Info		M	
> BS ID		M	

STEP 2

MBS Sync controller retransmits the MBS Sync Rule Announcement message to the MBS Sync Executor which has requested a retransmission.

4.12.3.1.3 MBS Data Path recovery procedure

To ensure that all the BSs' Sync Executors (and the MBS Sync Controller for Model C) have identical data buffered, a data recovery mechanism over the R6 (and R4) data path may be enabled. If the lost data is not recovered, the MBS DPF in the BS may discard the entire MBS data for the MBS frame or assign the air resource using the MBS SDU packet size in the received MBS Sync rule for the lost packet. Therefore, if the packet loss probability is low enough then the recovery mechanism could be omitted.

In the case of Type 1 data, the length of the packets may be provided as a part of the Sync Rule to support the data integrity. However, for the Type 3 data path, as the entire data burst will be lost any when the packet is lost, Recovery Response message may not worthwhile to implement.

When the packets size is not explicitly specified as a part the Sync Rule, Recovery Response message should be used to provide the MBS DPF in the BS regarding the size of the requested packet(s).

If the explicit recovery function is enabled, the procedures are as follows:

- The MBS DPF in the BS sends a Recovery Request to the MBS Distribution DPF. The request contains Data Path ID (GRE Key) or MBS Service Flow identity and the list of the lost packets (identified by GRE Sequence Numbers).
- The MBS Distribution DPF may send Recovery Response message providing the size of the requested packets (applicable for Type 1 data path when packet size is not specified as a part of the Sync Rule).
- The MBS Distribution DPF may retransmit the lost packets.

As an option for the lost packets recovery, it is possible to use preventive cycling retransmission mechanism (i.e. sending multiple copies of the same packet) on the data plane. This is an implementation option for the MBS Distribution DPF.

Support of the explicit recovery mechanism (e.g. MBS DPF to query the MBS Distribution DPF) may be negotiated during the MBS data path establishment procedure.

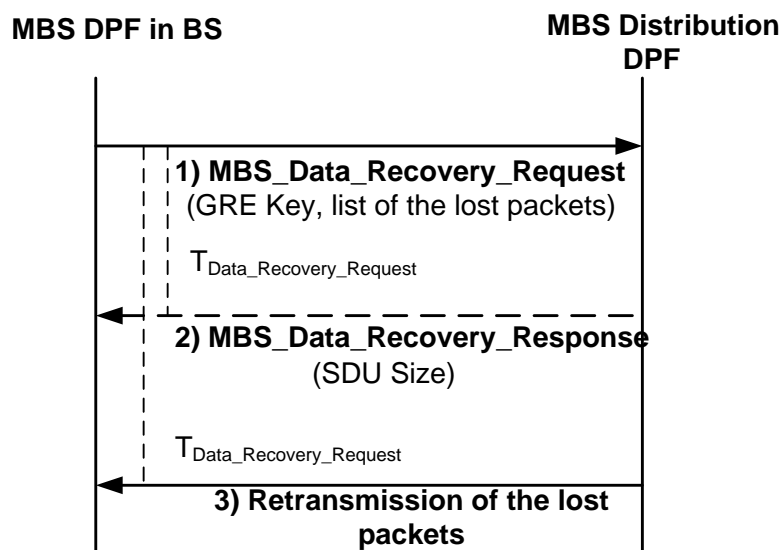


Figure 4-56 : MBS data recovery over the MBS data path

MBS DPF function (located in a BS or collocated to an MBS Sync Controller) may detect SDU(s)/ packets loss by considering GRE Sequence Numbers of the packets received over the MBS data path. When MBS DPF in a BS detects SDU loss it may trigger SDU recovery procedure by sending MBS_Data_Recovery_Request message to the MBS Distribution DPF. MBS Distribution DPF responds back with MBS_Data_Recovery_Response message and may retransmit the lost SDU(s)/ packets. MBS_Data_Recovery_Response message is applicable for Type 1 data path only.

STEP 1

MBS DPF function in the BS detects data packets loss over the data path (using GRE Sequence Number) and MAY trigger MBS data recovery mechanism by sending MBS_Data_Recovery_Request message to MBS Distribution DPF. This MBS_Data_Recovery_Request message will list the missing data path packets by including their GRE Sequence Numbers.

Note, that Data Path recovery mechanism is negotiated during MBS data path establishment.

Table 4-39 : MBS_Data_Recovery_Request

IE	Reference	M/O	Notes
BS Info		M	
> BSID		M	
> SF Info		M	
>> PDF ID	5.3.1.3.1.2	O	Identifies the MBS Service Flow for which SDU recovery is requested (for Type 1 data path). Either MBS Service ID or Data Path Info with Data Path ID shall be included.
>> MCBCS Transmission Zone ID	5.2.6	O	
>> Data Path Info		M	
>>> Data Path ID		M	For GRE tunnel represents GRE Key. Identifies the data path for which SDU recovery is requested (for Type 1 data path).
>>>> Requested packet	5.2.54	M	Data structure for the requested packet on the data path. Multiple instances of this IE may be included.
>>>>> Packet SN	5.2.55	M	GRE Sequence Number of the missing packet.

STEP 2

For Type 1 Data Path, MBS Distribution DPF MAY respond back with MBS_Data_Recovery_Response message providing the Size of the missing SDUs. Whether MBS Distribution DPF uses this step or not is negotiated during the data path establishment.

Table 4-40 : MBS_Data_Recovery_Response

IE	Reference	M/O	Notes
BS Info		M	
> SF Info	TBD	M	
>> Data Path Info		M	
>>> Data Path ID		M	For GRE tunnel represents GRE Key. Identifies the data path for which SDU recovery is requested (for Type 1 data path).
>>>> Requested packet	5.2.54	M	Data structure for the requested packet on the data path. Multiple instances of this IE may be included
>>>>> Packet SN	5.2.55	M	GRE Sequence Number of the packet on the data path.
>>>>> Packet Size	5.2.56	M	The Size of the missing SDU.

Note: MBS_Data_Recovery_Response message is applicable only for Type 1 data path.

STEP 3

MBS Distribution DPF may resend the missing packet identified by GRE Sequence Number.

4.12.3.2 Timers and Timing Considerations

This section identifies the timer entities participating in the sync rule delivery and recovery procedure. The sync rule delivery and recovery procedure employs two timers:

$T_{\text{MBS_Sync_Rule_Recovery_Request}}$: is started by an MBS Sync executor upon sending a *MBS_Sync_Rule_Recovery_Request* message. It is stopped upon receiving a corresponding *MBS_Sync_Rule_Announcement*.

$T_{\text{MBS_Data_Recovery_Request}}$: is started by the MBS DPF when it sends a *MBS_Data_Recovery_Request* message and is stopped upon receiving a corresponding *MBS_Data_Recovery_Response* message or the lost packet.

Table 10-41 shows the maximum value of timers and also indicates the range of the recommended duration of these timers.

Table 4-41 : Timer Values for Sync rule delivery and recovery procedure

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
$T_{\text{MBS_Sync_Rule_Recovery_Request}}$			TBD
$T_{\text{MBS_Data_Recovery_Request}}$			TBD

4.12.3.2.1 MBS sync rule and data recovery error handling

The following table shows details on the corresponding actions after the maximum number of retry. A recovery message is repeated up to the maximum number of retry with resetting the timer. Upon reaching the maximum retry, the corresponding action(s) should be performed as indicated in Table 4-42.

Table 4-42 : Action on the Recovery Failure

Timer	Entity where Timer Started	Action(s)
$T_{\text{MBS_Sync_Rule_Recovery_Request}}$	MBS Sync Executor	MBS Sync executor discards the received MBS data until the next MBS sync rule is received successfully.
$T_{\text{MBS_Data_Recovery_Request}}$	MBS DPF	MBS DPF may discard the entire MBS data for the MBS frame or assign the air resource using the MBS SDU packet size in the received MBS Sync Rule Announcement message for the lost packet and transmits the MBS frame.

4.12.3.3 MBS Data flow level of synchronization across MBS Zones

The size of the MBS Zone may be restricted by:

- the geography requirements (there may be no benefit to having excessively large MBS Zones);
- MBS Data traffic propagation delays in excess of tolerable QoS delay;

MCBCS-DSx

- the requirements to have different radio configuration parameters in the different BSs (e.g. multi-frequency deployments, deployments with reuse ≥ 1 or deployments with the mixed Pico, Femto and Macro cells). This may require different MBS Sync Controllers to specify different Sync Rules.

When there is a requirement for MBS frame-level coordination across multiple MBS Zones that are belonged to the same MCBCS Transmission Zone for the particular MBS Content, the following conditions shall be achieved across the MBS Zones:

1. MBS payload synchronization – different MBS Sync Executors shall be able to identify the same MBS packet (e.g. in the case of Type 1 data path, it means the GRE sequence numbering for MBS packets must be preserved across the MBS Zones). This would require synchronization among the hierarchical MBS Distribution DPFs (or cascading of MBS Distribution DPFs).
2. MBS Sync Rule synchronization – different MBS Sync Executors shall be able to schedule the specified MBS packets in the particular downlink radio frame or some time interval (which may include multiple radio frames). This would require some level of coordination controlled by the MBS Sync Controller(s).

To achieve MBS frame-level coordination across MBS Zones within the MBS Transmission Zone, different combinations of the MBS Sync Rule and MBS payload synchronization scenarios should be considered by referring to the following sub-sections, e.g. :

- A single MBS Distribution DPF and co-located with a MBS Sync Controller;
- A single MBS Distribution DPF with hierarchical MBS Sync Controllers;
- Hierarchical MBS Distribution DPFs and collocated with a MBS Sync Controller;
- Hierarchical MBS Distribution DPFs with hierarchical MBS Sync Controllers;
- Etc.

Some implementation models may be limited to a subset of the presented options.

4.12.3.4 MBS payload synchronization

To achieve MBS payload synchronization among the MBS Zones, the following options are applicable:

Option 1 – having a Single MBS Distribution DPF (and Upper Sync Executor in the case of Model A implementation) classifying and distributing the MBS traffic to the MBS Sync Executors across the multiple MBS Zones of the MBS Transmission Area.

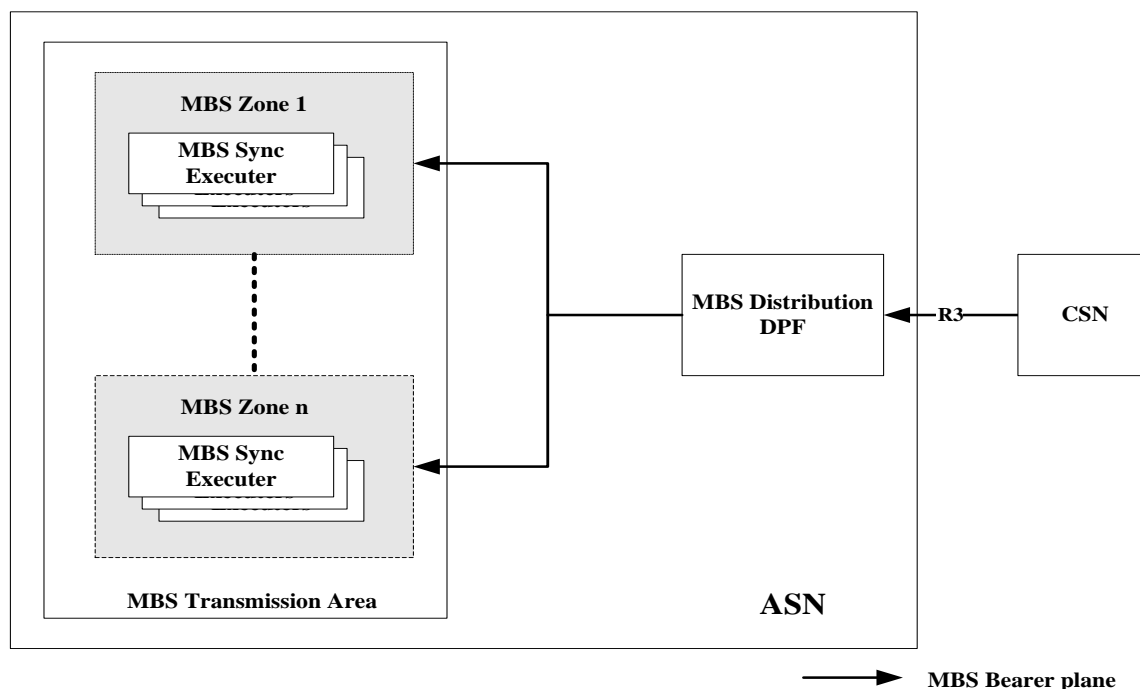


Figure 4-57 : MBS payload synchronization across MBS Zones – option 1

Option 2 – Creating a hierarchical MBS Distribution DPFs.

This option may allow overcoming some possible ASN transport network restrictions, such as e.g. having IP multicast network segments limited to the MBS Zone.

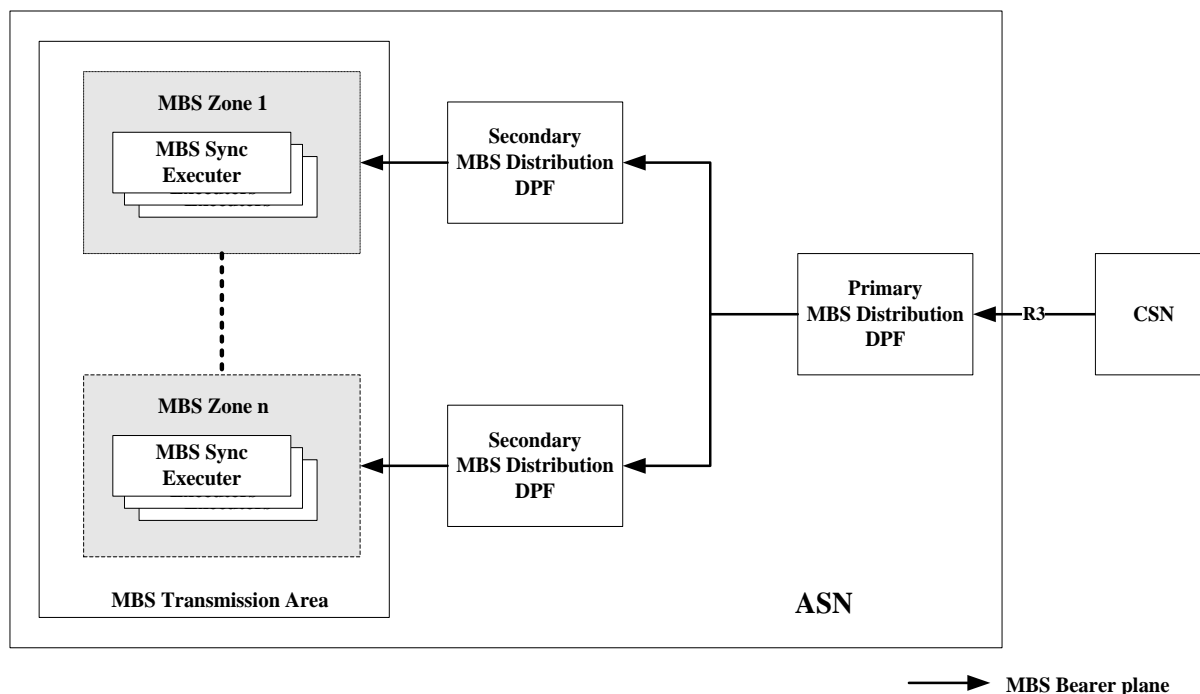


Figure 4-58 : MBS payload synchronization across MBS Zones – option 2

The MBS Distribution DPF is responsible to classify MBS traffic and distribute it to the all MBS Sync Executors for the particular MBS Zone.

For Model A implementation, the Primary and/ or Secondary MBS Distribution DPF will be collocated with the MBS Sync Controller and the Upper Sync Executer and will apply bearer steps 1–2 pre-processing as described in Annex A.

For Models B and C, the Primary MBS Distribution DPF is responsible to tag the classified MBS packets (per MBS Service Flow/ data path) with the corresponding GRE sequence numbers. The Secondary MBS Distribution DPFs should not modify this sequence numbering.

The Primary MBS Distribution DPF does not have to serve by itself as a Distribution DPF for the particular MBS Zone, but this is not restricted.

The selection of the Primary MBS Distribution DPF is out of the scope of this specification.

The R4 data path operations (including payload type negotiation during data path establishment) between the Primary MBS Distribution DPF and the Secondary MBS Distribution DPF follow the NWG Rel.1 specification (for data path control procedures over R4).

Note that, for phase-1 MCBCS support, only a single MBS Distribution DPF is assumed. Hierarchical MBS Distribution DPFs support is FFS.

4.12.3.5 MBS Sync Rule synchronization

MBS Sync Rule synchronization among the MBS Zones requires some level of coordination among the MBS Sync Controllers of these MBS Zones. To achieve it, the following options are applicable.

Note, that in all the presented scenarios, it is assumed that:

- MBS Sync Controllers are receiving MBS traffic (co-located with MBS Distribution DPF or MBS DPF), and
- MBS payload synchronization is achieved as discussed in 4.12.3.4

Option 1 – A centralized MBS Sync Controller responsible for sending the MBS Sync Rules to the different MBS Zones within the MBS Transmission Zone.

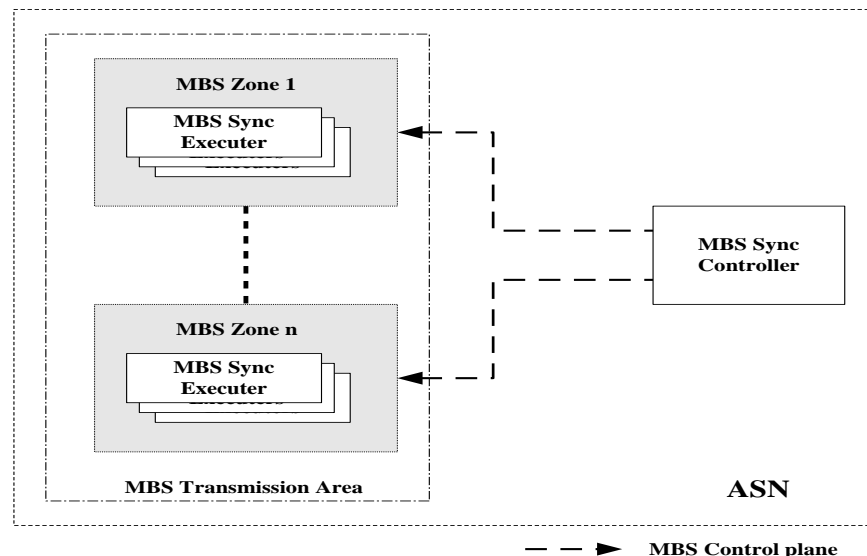


Figure 4-59 : MBS Sync Rule synchronization across MBS Zones – option 1

This scenario assumes a single logical MBS Sync Controller entity for all MBS Zones belonged to the same MBS Transmission Zone. The MBS Sync Rules generated for different MBS Zones may be different, but will achieve coordinate MBS traffic scheduling (up to the level of the particular downlink radio frame within the accuracy of a permitted time interval).

The entity hosting the centralized MBS Sync Controller is required to have access to the updated RRM information and receives MBS traffic of all the MBS Zones.

Option 2 - Creating a hierarchical MBS Sync Controllers structure.

This option allows localization of MBS Sync Controller which is RRM aware of its MBS Zone.

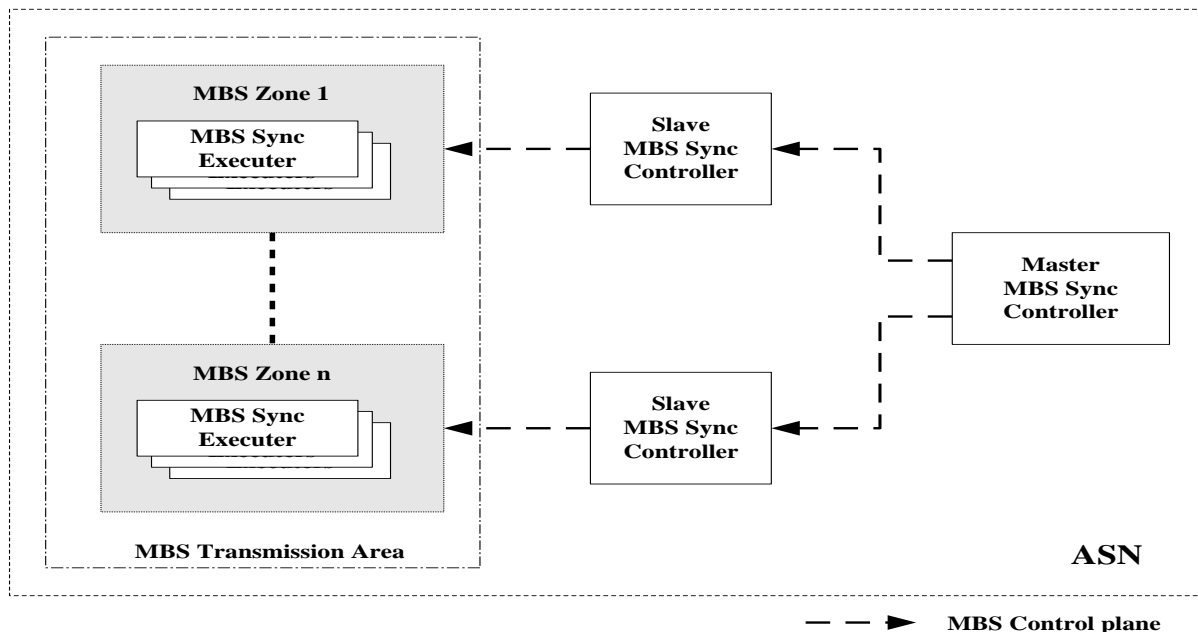


Figure 4-60 : MBS Sync Rule synchronization across MBS Zones – option 2

The Master MBS Sync Controller is responsible for specifying the MBS Sync Rule to support the Frame-offset Coordination the MBS SDU and/or SDU fragment levels of synchronization for the radio frames which are within a specified frame offset between the MBS Zones. The Slave MBS Sync Controller MAY specify Sync Rules up to the macro-diversity level of synchronization.

Note that, for phase-1 MCBCS support, only a single MBS Sync Controller is assumed. Hierarchical MBS Controllers support is FFS.

4.12.4 Overlapping MBS Zones

A BS can be a member of more than one MBS Zone Area. Two MBS Zone Areas are overlapping if there is at least one BS that belongs to both areas as presented on the figure below:

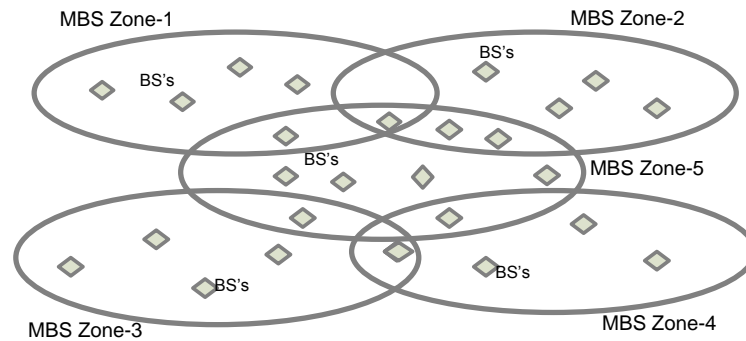


Figure 4-61 : Example of overlapping MBS Zone Areas

Overlapping of MBS Zones may be reasonable for the different MBS contents (there is no sense to have overlapping MBS Zones for the same content – which would result in duplication of over-the-air content transmissions).

The overlapping Zones must not use the same sub channels at the same time. Thus the MBS Burst allocations for MBS transmissions should take into account the topology of the MBS Zones. Radio resource allocation for MBS transmissions in the BSs located in the “overlapping areas” should be arranged in a way that will ensure a separate “transmission region” for every MBS content. This requires coordination of radio resource allocations between MBS Sync Controllers responsible for Sync Rules generation for the overlapping MBS areas, - i.e. MBS Sync Controllers of the “directly” overlapping MBS Zones should operate with different transmission regions (time/ frequency).

MBS Zone areas may be modeled as a graph where each vertex represents Zone area and each edge represents overlapping between two areas. The graph can be colored in a way that no two adjacent vertexes share the same color. The MBS Zones that share the same color may use the same subchannels at the same time. Those with different colors must not use the same subchannels at the same time. Thus each color represents a certain resource assignment. For arbitrary random generated graphs the coloring problem may be complex. However good approximate polynomial time solutions exist. In structured graphs coloring can be trivial.

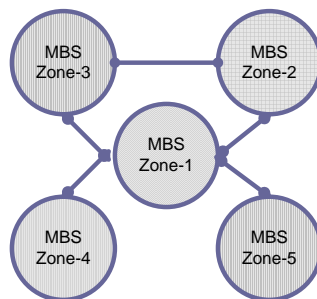


Figure 4-62 : Example of MBS Zones colouring graph

Two MBS Zones really overlap only if both have some data to transmit. In this case the graph can be formed and colored dynamically during Accumulation Period. The operator will have to plan the Overlapping MBS Zone areas carefully so the resulting graph will have a regular structure enabling quick enough coloring calculation.

The solution may be achieved by the multiple ways:

- Option 1: Radio resources for overlapping MBS Zones are engineered and pre-configured in advance – i.e. each MBS Zone/ Sync Controller is pre-allocated with its own non-overlapping resources (time/ frequency);

MCBCS-DSx

- Option 2: There is a common Sync Controller (or collocated Sync Controllers) allocating resources for overlapping MBS Zones in such a way that will ensure non-overlapping “transmission regions” for MBS Service Flows.

The Option 2 assumes the common Sync Controller has access to the updated RRM info and receives MBS traffic of all the controlled MBS Zones. This could be considered less efficient option. For a chain of overlapping MBS Zones, this would result in having a single MBS Sync Controller for the whole network.

As an alternative for such a scenario (with a chain of overlapping MBS Zones), a mix of Option 1 and Option 2 may provide a solution:

- “Directly” overlapping MBS Zones are controlled by a single (co-located) MBS Sync Controller (Option 2).
- MBS Sync Controllers of “non-directly” overlapping MBS Zones are engineered and pre-configured with its own non-overlapping transmission regions (Option 1).

Selection of Option 1 vs. Option 2 solution is implementation specific.

5 Message and Parameter Definitions

5.1 Message Definitions and Construction Rules

5.1.1 MBS Join Request

Function Type	Message Type	Top Level TLVs	
13	11	TLV Name	M/O
		MCBCS Service Info	M

5.1.2 MBS Join Response

Function Type	Message Type	Top Level TLVs	
13	12	TLV Name	M/O
		Failure Indication	O
		MCBCS Service Info	M

5.1.3 MBS Leave Request

Function Type	Message Type	Top Level TLVs	
13	13	TLV Name	M/O
		MCBCS Service Info	M

5.1.4 MBS Leave Response

Function Type	Message Type	Top Level TLVs	
13	14	TLV Name	M/O
		Failure Indication	O
		MCBCS Service Info	M

5.1.5 MBS Service Counter Request

Function Type	Message Type	Top Level TLVs	
13	15	TLV Name	M/O
		MCBCS Service Info	M

5.1.6 MBS Service Counter Response

Function Type	Message Type	Top Level TLVs	
13	16	TLV Name	M/O
		Failure Indication	O
		MCBCS Service Info	M

5.1.7 MBS Sync Rule Announcement

Function Type	Message Type	Top Level TLVs	
13	17	TLV Name	M/O
		Sync Rule UTC Timestamp	M
		Next Sync Rule expected TOA	O
		MBS zone Identifier	M
		MBS Burst	O
		MBS_MAP_IE_Context	M
		BS Info	O

5.1.8 MBS Sync Rule Request

Function Type	Message Type	Top Level TLVs	
13	18	TLV Name	M/O
		Sync Rule UTC Timestamp	M
		MBS zone Identifier	M

Function Type	Message Type	Top Level TLVs	
		BS Info	M

5.1.9 MBS_Data_Recovery_Request

Function Type	Message Type	Top Level TLVs	
13	19	TLV Name	M/O
		BS Info	M

5.1.10 MBS_Data_Recovery_Response

Function Type	Message Type	Top Level TLVs	
13	20	TLV Name	M/O
		BS Info	M

5.2 TLV Encoding

5.2.1 MBS Proxy and MCBCS Controller/Server Service Association SPI

Service Association SPI

Type	518
Length in octets	2
Value	16-bit unsigned integer.
Description	Index a MCBCS Proxy service association with the MCBCS Controller.
Parent TLV(s)	

5.2.2 MCBCS Controller/Server IPv4

Type	519
Length in octets	4 bytes
Value	IPv4 address
Description	IPv4 address of MCBCS Controller/Server.

Parent TLV(s)	MCBCS Controller/Server Info
----------------------	------------------------------

5.2.3 MCBCS Controller/Server IPv6

Type	520
Length in octets	16bytes
Value	IPv6 address
Description	IPv6 address of MCBCS Controller/Server.
Parent TLV(s)	MCBCS Controller/Server Info

5.2.4 MCBCS Controller/Server FQDN

Type	521
Length in octets	Variable up to 256 octets
Value	ASCII String
Description	MCBCS Controller/Server character string. Fully qualified domain name of the MCBCS Controller for the given MCBCS service
Parent TLV(s)	MCBCS Controller/Server Info

5.2.5 MCBCS Service Info

Type	522	
Length in octets	Variable	
Value	Compound	
Description	Description of MCBCS Service	
Elements (Sub-TLVs)	TLV Name	M/O
	MCBCS Transmission Zone ID	O ^a
	PDF ID	O ^a
	R3 Multicast IP Address	O ^a
	MCID	O
	MBS Zone ID	O
	QoS Parameter	O
	Volume Required	O
	Current Volume Counter	O
Message Primitives That Use This TLV	MBS Join Request, MBS Join Response, MBS Leave Request, MBS Leave Response, MBS Service Counter Request, MBS Service Counter Response	

Note a: At least one of these Identifiers should be present in this TLV.

5.2.6 MCBCS Transmission Zone ID

Type	523
Length in octets	Variable
Value	ASCII String.
Description	MCBCS Transmission Zone ID.
Parent TLV(s)	MCBCS Service Info

5.2.7 R3 Multicast IP Address

Type	524
Length in octets	4 or 16
Value	128-bit unsigned integer.
Description	The R3 Multicast IP address of the MCBCS Service
Parent TLV(s)	MCBCS Service Info

5.2.8 MCID

Type	525
Length in octets	2
Value	16-bit unsigned integer.
Description	Multicast Connection ID definition as per 802.16.
Parent TLV(s)	MCBCS Service Info, MBS_Data_Info

5.2.9 MBS Zone ID

Type	526
Length in octets	1
Value	7-bit unsigned integer.
Description	MBS Zone Identifier definition as per 802.16. This parameter indicates a MBS zone through which the connection or virtual connection for the associated service flow is valid.
Parent TLV(s)	MCBCS Service Info

5.2.10 Volume Required

Type	527
Length in octets	1
Value	0x00 - Required; 0x01 – Not Required
Description	To indicate whether MBS Accounting Agent should return the volume of particular Service
Parent TLV(s)	MCBCS Service Info

5.2.11 Current Volume Counter

Type	528
Length in octets	4
Value	32-bits unsigned integer
Description	The current volume of the particular Service
Parent TLV(s)	MCBCS Service Info

5.2.12 MBS Zone Update Indicator

Type	529
Length in octets	1
Value	. Octet enumeration with the following values: 0 = Locate update is not triggered by MBS zone update 1 = Locate update is triggered by MBS zone update others = Reserved
Description	This flag indicates the location update is triggered by MBS zone update.
Message Primitives That Use This TLV	LU_Req

5.2.13 SF Info (Refer to 5.3.2.185 in NWG Release v1.3.0)

Type	185
Length in octets	Variable
Value	Compound
Description	Service Flow Description.

Elements (Sub-TLVs)	TLV Name	M/O
	Failure Indication	O ¹
	SFID	M
	Reservation Action	O ¹
	Reservation Result	O ¹
	ARQ Enable	O ¹
	ARQ Context	O ¹
	Direction	O ¹
	CID/MCID	O ²
	SAID	O ¹
	Packet Classification Rule / Media Flow Description (one or more)	O
	QoS Parameters	O
	Paging Preference	O ¹
	CS Type	O
	Data Path Info	O
	SDU Info	O ¹
	PHS Rule	O ¹
	Accounting Extension	O
	SA Descriptor	O ¹
	Correlation ID	O
	Data Delivery Trigger	O ¹
	MCBCS Service continuity indicator	O ³
	MBS Zone ID	O ³
	MCBCS Transmission Zone ID	O ^{3,4}
	PDFID	O ^{3,4}
Parent TLV(s)	MS Info, BS Info	

Notes: Multiple instances of SF Info may be included in one message

1. TLV is not applicable for Service Flow for MCBCS;
2. MCID is use for service flow for MCBCS;
3. TLV is only applicable for Service Flow for MCBCS;
4. PDFID shall be used together with MCBCS Transmission Zone to uniquely identify a service flow of MBS within MCBCS Transmission Zone;

5.2.14 CID/MCID (Refer to 5.3.2.29 in NWG Release v1.3.0)

Type	29
Length in octets	2
Value	16-bit unsigned integer.
Description	CID/MCID definition as per 802.16.
Parent TLV(s)	SF Info

5.2.15 MCBCS Service Continuity Indicator

Type	530
Length in octets	1
Value	. Octet enumeration with the following values: 0 = Not support 1 = Support others = Reserved
Description	The indicator for the MCBCS service continuity support within MCBCS Transmission Zone.
Parent TLV(s)	SF Info

5.2.16 QoS Parameters (Refer to 5.3.2.141 in NWG Release v1.3.0)

Type	141	
Length in octets	Variable	
Value	Compound	
Description	This compound TLV contains all Parameters pertaining to a specific QoS Description.	
Elements (Sub-TLVs)	TLV Name	M/O
	BE Data Delivery Service	O
	UGS Data Delivery Service	O
	NRT-VR Data Delivery Service	O
	RT-VR Data Delivery Service	O
	ERT-VR Data Delivery Service	O
	Global Service Class Name	O
	Service Class Name	O

	Media Flow Type	O
	Media Flow Description in SDP Format	O
	Reduced Resources Code	O ¹
	Data Integrity	O ¹
Parent TLV	SF Info	

If no Data Delivery Service Sub-TLV is included then the Data Delivery Service defaults to BE Data Delivery Service with Traffic Priority equal to zero and Request Transmit Policy equal to zero.

Note: 1 TLV is not applicable for service flow for MCBCS.

5.2.17 Sync Rule GPS timestamp

Type	531
Length in octets	4
Value	32-bit unsigned integer.
Description	This indicates GPS timestamp value
Message Primitives That Use This TLV	MBS_Sync_Rule_Announcement , MBS_Sync_Rule_Request

5.2.18 OFDMA frame offset

Type	532
Length in octets	1
Value	8-bit unsigned integer.
Description	This TLV specifies the OFDMA Frame Offset from the time specified in the UTC Timestamp TLV
Parent TLV	Time_Sync_Info

5.2.19 MAC PDU Size

Type	533
Length in octets	2
Value	16-bit unsigned integer.
Description	This TLV specifies the size of MAC PDU.
Parent TLV	MAC_Context

5.2.20 MBS_Data_Info

Type	534	
Length in octets	Variable	
Value	Compound	
Description	MBS data description	
Elements (Sub-TLVs)	TLV Name	M/O
	GRE sequence number start	M
	GRE sequence number end	M
	MCID	M
	MBS MAC Burst SN	O
	MAX MAC PDU Size	O
	MBS SDU packet size	O
Parent TLV	MBS Burst	

5.2.21 GRE sequence number start

Type	535
Length in octets	4
Value	32-bit unsigned integer.
Description	The GRE sequence number of the first MBS data packet to be applied by the sync rule
Parent TLV	MBS_Data_Info

5.2.22 GRE sequence number end

Type	536
Length in octets	4
Value	32-bit unsigned integer.
Description	The GRE sequence number of the last MBS data packet to be applied by the sync rule
Parent TLV	MBS_Data_Info

5.2.23 MBS data packet size

Type	537
Length in octets	2
Value	
Description	MBS data packet size in the order of GRE sequence number
Parent TLV	MBS_Data_Info

5.2.24 MBS_DATA_IE_Context

Type	538	
Length in octets	Variable	
Value	Compound	
Description	Describes the contexts for MBS_DATA_IE	
Elements (Sub-TLVs)	TLV Name	M/O
	MBS Burst Frame Offset	CM
	Next MBS MAP change indication	CM
	Next MBS No. OFDMA Symbols	O
	Next MBS No. OFDMA Subchannels	O
	MBS DIUC	CM
	OFDMA symbol offsets DATA IE	CM
	subchannel offset DATA IE	CM
	Boosting	CM
	No. OFDMA Symbols	CM
	No. Subchannels	CM
	Repetition Coding indication	CM
	Next MBS Burst frame offset	CM
	Next MBS OFDMA symbol offset	CM
Parent TLV	MBS Burst	

5.2.25 MBS_MAP_IE_Context

Type	539	
Length in octets	Variable	
Value	Compound	
Description	Describes the contexts for MBS_MAP and MBS_MAP_IE	
Elements (Sub-TLVs)	TLV Name	M/O
	> MBS permutation zone defined	M
	> OFDMA symbol offset MAP IE	M
	> subchannel offset MAP IE	CM
	> Permutation	CM
	> DL_PermBase	CM
	> PRBS_ID	CM
	> MBS MAP message allocation included indication	CM
	> Boosting	CM
	> MBS DIUC	CM
	> Repetition Coding indication	CM
	> No. Subchannels	M
	> No. OFDMA symbols	M
	> Downlink Burst Profile	M
Message Primitives That Use This TLV	MBS_Sync_Rule_Announcement	

1

2 5.2.26 MBS Burst Frame Offset

Type	540
Length in octets	1
Value	2 bit
Description	This indicates the burst located by this IE will be shown after MBS Burst Frame Offset +2 frames. as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context, MBS Burst

3

4 5.2.27 Next MBS MAP change indication

Type	541
Length in octets	1
Value	2 bit
Description	This indicates whether the size of MBS MAP message of next MBS frame for these Multicast CIDs included this IE will be different from the size of this MBS MAP message, as defined in the IEEE802.16-Rev2 [3].

Parent TLV	MBS_DATA_IE_Context
-------------------	---------------------

5.2.28 Next MBS No. OFDMA Symbols

Type	542
Length in octets	1
Value	6 bit
Description	It is to indicate the size of MBS_MAP message in Next MBS portion, as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context

5.2.29 Next MBS No. OFDMA Subchannels

Type	543
Length in octets	1
Value	6 bit
Description	It is to indicate the size of MBS_MAP message in Next MBS portion, as defined in the IEEE802.16-Rev [3].
Parent TLV	MBS_DATA_IE_Context

5.2.30 MBS DIUC

Type	544
Length in octets	1
Value	4 bit
Description	It is to indicate MBS DIUC, as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context, MBS_MAP_IE_Context

5.2.31 OFDMA symbol offsets DATA IE

Type	545
Length in octets	1
Value	8 bit
Description	It is to indicate OFDMA symbol offset with respect to start of next (MBS Burst Frame offset + 2)the frame, as defined in the IEEE802.16-Rev [3].
Parent TLV	MBS_DATA_IE_Context

5.2.32 Subchannel offset DATA IE

Type	546
Length in octets	1
Value	6 bit
Description	It is to indicate OFDMA subchannel offset with respect to start of next (MBS Burst Frame offset + 2) the frame, as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context

5.2.33 Boosting

Type	547
Length in octets	1
Value	3 bit
Description	It is to indicate boosting, as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context, MBS_MAP_Context

5.2.34 No. OFDMA Symbols

Type	548
Length in octets	1
Value	7 bit
Description	It is to indicate the size of MBS data, as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context

5.2.35 No. OFDMA Subchannels

Type	549
Length in octets	1
Value	6 bit
Description	It is to indicate the size of MBS data, as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context

5.2.36 No. Subchannels

Type	550
Length in octets	1
Value	6 bit
Description	It is to indicate the size of MBS data, as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context

5.2.37 Repetition Coding indication

Type	551
Length in octets	1
Value	2 bit
Description	0b00 – No repetition coding 0b01 – Repetition coding of 2 used 0b10 – Repetition coding of 4 used 0b11 – Repetition coding of 6 used Refer the definition in IEEE 802.16-Rev2 [3] spec.
Parent TLV	MBS_DATA_IE_Context

5.2.38 Next MBS Burst Frame offset

Type	552
Length in octets	1
Value	8 bit
Description	It is to indicate the relative value from the current frame number in which the next MBS MAP message will be transmitted, as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context , MBS Burst

5.2.39 Next OFDMA Symbol offset

Type	553
Length in octets	1
Value	8 bit
Description	It is to indicate the offset of the OFDMA symbol in which the next MBS portion starts, measured in OFDMA symbols from the beginning of the DL frame in which the MBS_MAP is transmitted, as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_DATA_IE_Context

5.2.40 MBS Permutation Zone Defined

Type	554
Length in octets	1
Value	1 bit
Description	0: Non Macro-Diversity enhanced zone 1: Macro-Diversity enhanced zone Refer a definition in IEEE802.16-Rev2 [3] spec.
Parent TLV	MBS_MAP_Context

5.2.41 OFDMA symbol offset MAP IE

Type	555
Length in octets	1
Value	1 bit
Description	The offset of the first OFDMA symbol of the MBS region measured in OFDMA symbols from beginning of this DL frame as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_MAP_Context

5.2.42 Subchannel offset MAP IE

Type	556
Length in octets	1
Value	6 bit
Description	The lowest index OFDMA subchannel used for carrying the burst, starting from subchannel 0 as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_MAP_Context

5.2.43 Permutation

Type	557
Length in octets	1
Value	2 bit
Description	0b00: PUSC permutation 0b01: FUSC permutation 0b10: Optional FUSC permutation 0b11: Adjacent subcarrier permutation Refer the definition in IEEE 802.16-Rev2 [3].
Parent TLV	MBS_MAP_Context

5.2.44 DL_PermBase

Type	558
Length in octets	1
Value	5 bit
Description	Refer the definition in IEEE 802.16-Rev2 [3]
Parent TLV	MBS_MAP_Context

5.2.45 PRBS_ID

Type	559
-------------	-----

Length in octets	1
Value	2 bit
Description	Refer the definition in IEEE 802.16-Rev2 [3].
Parent TLV	MBS_MAP_Context

5.2.46 MBS MAP message allocation included indication

Type	560
Length in octets	1
Value	1 bit
Description	It is to indicate if the MBS MAP message allocation parameters are included as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_MAP_Context

5.2.47 Downlink Burst Profile

Type	561
Length in octets	1
Value	4 bit
Description	It is to indicate a definition of MBS DIUC as defined in the IEEE802.16-Rev2 [3].
Parent TLV	MBS_MAP_Context

5.2.48 MBS Burst

Type	562	
Length in octets	Variable	
Value	Compound	
Description	Each instance of this compound TLV describes MBS Burst. Zero or more instances of this TLV may be included in the message. If no MBS Burst TLVs are included in the message, then previous MBS Sync Rule is invalid.	
Elements (Sub-TLVs)	TLV Name	M/O
	> MBS Burst Frame offset	CM
	> Next MBS Burst Frame offset	O
	> MBS Burst Scheduling Cycle	O
	> MBS_Data_Info	CM
	> MBS_DATA_IE_Context	M
Message Primitives That Use This TLV	MBS_Sync_Rule_Announcement	

5.2.49 Next Sync Rule expected TOA

Type	563
Length in octets	4
Value	32-bit unsigned integer.
Description	GPS timestamp corresponding the expected Time of Arrival for the next Sync Rule. Used for Sync Rule recovery mechanism. If missing, there is no recovery mechanism.
Message Primitives That Use This TLV	MBS_Sync_Rule_Announcement

5.2.50 MBS Burst Scheduling Cycle

Type	564
Length in octets	2
Value	16 bit
Description	Defines the periodicity of MBS burst scheduling (in air frames).
Parent TLV	MBS Burst

5.2.51 MBS MAC Burst SN

Type	565
Length in octets	4
Value	32-bit unsigned integer
Description	Indicates the sequence number of the packet (GRE SN for GRE tunnel) representing the MBS MAC Burst to be used in the MBS Burst instance.
Parent TLV	MBS_Data_Info

5.2.52 MAX MAC PDU Size

Type	566
Length in octets	2
Value	16-bit unsigned integer.
Description	MAC PDU size that may be used to define fragmentation/ packing rule for SDUs. May be included for Type 1 Data Path.
Parent TLV	MBS_Data_Info

5.2.53 MBS SDU packet size

Type	567
Length in octets	2
Value	16-bit unsigned integer

Description	One or more MBS data packet size in the order of GRE sequence number If there is a MBS data packet loss, BS can use this TLV to assign the air resource for Macro-diversity.. May be included for Type 1 Data Path.
Parent TLV	MBS_Data_Info

5.2.54 Requested packet

Type	568	
Length in octets	Variable	
Value	Compound	
Description	Data structure for the requested packet on the data path.	
Elements (Sub-TLVs)	TLV Name	M/O
	Packet SN	M
	Packet size	M
Parent TLV	Data Path Info	

5.2.55 Packet SN

Type	569
Length in octets	4
Value	32-bit unsigned integer.
Description	GRE Sequence Number of the missing packet on the data path.
Parent TLV	Requested packet

5.2.56 Packet size

Type	570
Length in octets	2
Value	16-bit unsigned integer.
Description	The Size of the missing SDU.
Parent TLV	Requested packet

5.2.57 MBS Distribution DPF ID

Type	571
Length in octets	Variable (could be of three fixed sized 4, 6, and 16 octets)
Value	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	This is Identifier for the MBS Distribution DPF
Parent TLV	DP Info

5.3 RADIUS Messages and Attributes

5.3.1 WiMAX RADIUS Message Definitions

5.3.1.1 Radius Message between the NAS and AAA for the support of Dynamic Discovery of MCBCS Controller/Server

The following table adds the attributes to the RADIUS message between NAS and AAA to enable the MCBCS Controller/Server attributes exchanged between the AAA and the Anchor Authenticator of the MS.

Table 5-1 : MCBCS Controller/Server Attributes in Final RADIUS Access-Accept from AAA to ASN

Attribute	Type	Description	Access Request	Access Challenge	Access Accept	Access Reject
MCBCS-Controller-Server-IPv4	26/106	The IPv4 address of MCBCS Controller/Servers.	0	0	1-n[s]	0
MCBCS-Controller-	26/107	The FQDN of MCBCS	0	0	1-n[s]	0

Server-FQDN		Controller/Servers				
MCBCS-Controller- Server-IPv6	26/108	The IPv6 address of MCBCS Controller/Servers.	0	0	1-n[s]	0
MCBCS-Service- Association-SPI	26/109	MCBCS Service Association Information	0	0	1-n[u]	0

Notes

[s] This attribute is only present when the serving ASN supports the MCBCS service.

[u] This attribute is only present when the MS has subscribed to the MCBCS service.

5.3.1.1.1 WiMAX Radius VSA Definition for MCBCS Controller/Server Discovery

The following MCBCS Controller/Server (SIP) VSAs specify IP addresses or FQDNs of MCBCS Controller/Server provided to the ASN for the MS. The MCBCS Controller/Server addresses SHALL be provided in order of preference.

5.3.1.1.1.1 MCBCS-Controller-Server-IPv4

```

0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|RADIUS TYPE 26 | Length          |                               Vendor-Id          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Vendor-Id (cont)          | WiMAX TYPE      |   Length      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Continuation |   MCBCS Controller/Server IPv4          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

WType-ID	106 for MCBCS-Controller-Server-IPv4
Description	MCBCS Controller/Server IPv4
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	The value of this AVP is encoded as an IPv4 address

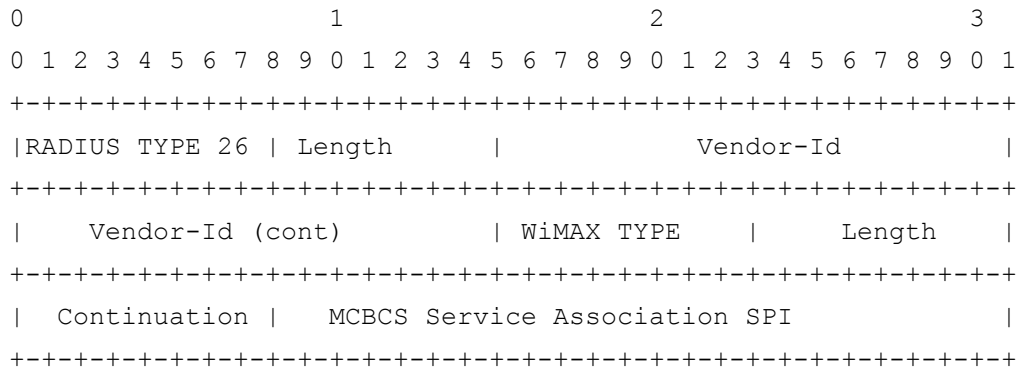
5.3.1.1.1.2 MCBCS-Controller-Server-IPv6

5.3.1.1.1.3 MCBCS-Controller-Server-FQDN

[illegible]

WType-ID	107 for MCBCS-Controller-Server-FQDN
Description	Fully qualified domain name of the MCBCS Controller/Server for the given MCBCS service.
Length	6 + 3 + Length of FQDN of the MCBCS Controller/Server
Continuation	C-bit = 0
Value	Octet string containing a Domain Name (most significant octet first)

5.3.1.1.1.4 MCBCS-Service-Association-SPI



WType-ID	109 for MCBCS-Service-Association-SPI
Description	Index a MCBCS Proxy service association with the MCBCS Controller/Server.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

5.3.1.2 Radius Message between the ASN and the CSN to Support MCBCS Service Initialization and Establishment as well as MS MCBCS service provisioning

New RADIUS MCBCS service attributes are added to support the R3 messaging for the MCBCS service initialization and establishment as well as for the MS service provisioning which are exchanged between the AAA and the Anchor Authenticator located in the ASN, and between the MBS Proxy and MCBCS Controller/Server, respectively. The following table contains the MCBCS service profile for the given MCBCS program.

Table 5-2 : RADIUS Access Messages for MCBCS between MBS Proxy and MCBCS Controller/Server

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
MCBCS-Service-Association-SPI	26/109	MCBCS Service Association Information	0-1	0	0	0
MCBCS-Program-Descriptor	26/110	Refer to Qos stage3 contribution	1-n	0	1-n	0
Packet-Flow-Descriptor	26/28	Refer to Qos stage3 contribution	0	0	1-n	0
Qos-Descriptor	26/29	Refer to Qos stage3 contribution	0	0	0-n	0

Notes:

Table 5-3 : RADIUS Access Messages for MCBCS between ASN and AAA

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
MCBCS-Service-Association-SPI	26/109	MCBCS Service Association Information	0-1	0	0-1	0
MCBCS-Program-Descriptor	26/110	Refer to Qos stage3 contribution	0	0	1-n	0
Packet-Flow-Descriptor	26/28	Refer to Qos stage3 contribution	0	0	1-n	0
Qos-Descriptor	26/29	Refer to Qos stage3 contribution	0	0	0-n	0

Table 5-4 lists the RADIUS attributes that appear in a COA message used for MCBCS service that MS subscribed for. The procedure for sending COA messages as described in [3] are supported with the additional information as specified by this table. The following table contains the MCBCS service profile for the given MCBCS program.

Table 5-4 : RADIUS COA Message for MCBCS from AAA to ASN NAS

Attribute	TYPE	Description	COA-Req	COA-ACK	COA-NAK
User-Name	1	The NAI of the MS as received during Access-Authentication.	1	0	0
Calling-Station-Id	31	The MAC address in binary format of the MS.	1	0	0
WiMAX-Session-ID	26/4	The NAI contained in the User-Name and the WiMAX-Session-ID forms a unique identifier of the session at the NAS.	1	0	0
Packet-Flow-Descriptor	26/28	Packet flow descriptor for the MCBCS Service flow	1-n		
QoS-Descriptor	26/29	QoS for MCBCS Service flow	0-n		
MCBCS Program Descriptor	26/110	Identify the MCBCS Program	1-n	1-n	
R3 Multicast IP address		Identify the content multicast IP address which user subscribed for	1		
MCBCS-Controller-Server-IPv4	26/106	MCBCS Controller/Server IPv4 Address	1	0	0
MCBCS-Controller-Server-IPv6	26/108	MCBCS Controller/Server IPv6 address	1	0	0
MCBCS-Controller-Server-FQDN	26/107	MCBCS Controller/Server FQDN	1	0	0

Attribute	TYPE	Description	COA-Req	COA-ACK	COA-NAK
MCBCS-Service-Association-SPI	26/109	MCBCS Service Association Information	0-1	0	0
Acc-Interim-Interval	85	Indicates the number of seconds between each interim update in seconds for this specific session.			

5.3.1.3 RADIUS MCBCS service attributes which are required to support the MCBCS session management messaging exchanged between the MBS Proxy and MCBCS Controller/Server

Table 5-5 : CoA Message (for session Start/Stop)

Attribute	TYPE	Description	COA-Req	COA-ACK	COA-NAK
Message-Authenticator	80	Provides integrity protection for the RADIUS packets as required by [RFC 3579]	1	1	1
Error-Cause	101	Error Codes generated during access authentication [RFC 3576]	0	0	0-1
Session-ID	26/xx	A unique identifier identifies the session between proxy and MCBCS controller	1	0-1	0-1
MCBCS Program Descriptor	26/110	A unique identifier for this MCBCS Program.	1	1	0
Packet-Flow-Descriptor	26/28	The corresponding Service Flows	0-n[b]	0	0
QoS-Descriptor	26/29	The QoS descriptor for the corresponding flows	0-n[a]	0	0

Notes:

- [a] Conditional mandatory: see requirements for Packet Flow Descriptor.
- [b] The complete QoS-profile must be transferred as the original context in ASN will be replaced. See the description of Packet Flow Descriptor for further details.

In Session Start case, MCBCS Controller sends CoA Request message to MBS Proxy including the particular MCBCS Program Descriptor and the corresponding Packet Flow Descriptor and QoS Descriptor.

In Session Stop case, MCBCS Controller sends CoA Request message to MBS Proxy including the particular MCBCS Program Descriptor with any Packet Flow Descriptor. According Release 1.5 Qos Specification, PacketDataFlows which are not present anymore SHALL be deleted.

Table 5-6 : CoA Ack (Session Start/Stop RSP Message)

IE	Description	M/O	Notes
void			

5.3.1.3.1 WiMAX Radius VSA Definition for MCBCS Session Management and Service Profile

5.3.1.3.1.1 MCBCS-Program-Descriptor

```

0          1          2          3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|RADIUS TYPE 26 | Length          | Vendor-Id          |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont) | WiMAX TYPE | Length          |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Continuation | TLV
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Type-ID	110 for MCBCS-Program-Descriptor
Description	This attribute describes a MCBCS Program.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR	COA Req	COA ACK	COA NAC
1	MCBCS Proram ID	2+2	0-1	1	0	0	1	1	1
2	MCBCS Transmission Zone ID	2+2	0-1	1	0	0	1	1	1
3	PDFID	2+2	0-n	1-n	0	0	1-n	0	0

TLV ID	1 for MCBCS Program ID
Description	The identifier of MCBCS Service package.
Length	2+2
Value	Unsigned Short representing the MCBCS Program identifier (most significant bit first). A value of zero(0) is invalid,

TLV ID	2 for MCBCS Transmission Zone
Description	The identifier of MCBCS Transmission Zone.

Length	2+ variable
Value	String

TLV ID	3 for PDFID
Description	This attributes identifies a packet data flow instance. The identifier is assigned by the home network and is unique per mobile session or per MCBCS service for the entire session. PacketDataFlow-IDs 1 to 20 are assigned for the packet data flow of the Initial Service Flow (ISF). If PacketDataFlow-ID is used for MCBCS service, it SHALL be used together with MCBCS Transmission Zone ID to uniquely identify the MCBCS service within the MCBCS Transmission Zone.
Length	2+2
Value	Unsigned Short representing the flow identifier (most significant bit first). A value of zero(0) is invalid,

5.3.1.3.1.2 Packet-Flow Descriptor [Refer to 5.4.2.28 in NWG Release v1.3.0]

[Editor Note: This modification needs to be transferred to the Rel-1.5 Baseline text.]

```

      0          1          2          3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
| RADIUS TYPE 26 | Length | Vendor-Id |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont) | WiMAX TYPE | Length |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Continuation | TLV
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Type-ID	28 for Packet-Flow-Descriptor
Description	This attribute describes a packet flow. A packet flow may describe a uni-directional flow and bidirectional flow. The packet flow descriptor may be pre-provisioned. A packet flow descriptor references one or two QoS specifications.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR	COA Req	COA Ack	COA NAK
1	PacketDataFlowID	2+2	0	1	0	0	1	0	0
2	ServiceDataFlowID	2+2	0	0-1	0	0	0-1	0	0
3	ServiceProfileID	2+4	0	0-1[a]	0	0	0-1[a]	0	0
4	Direction	2+1	0	0-1[b][f]	0	0	0-1[b][f]	0	0

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR	COA Req	COA Ack	COA NAK
5	ActivationTrigger	2+1	0	0-1[b][f]	0	0	0-1[b][f]	0	0
6	TransportType	2+1	0	0-1[b]	0	0	0-1[b]	0	0
7	UplinkQosID	2+1	0	0-1[c][f]	0	0	0-1[c][f]	0	0
8	DownlinkQoSID	2+1	0	0-1[d]	0	0	0-1[d]	0	0
9	UplinkClassifier	2+Length	0	0-n[c][f]	0	0	0-n[c][f]	0	0
10	DownlinkClassifier	2+Length	0	0-n[d]	0	0	0-n[d]	0	0
11	Paging Preference	2+1	0	0-1[e] [f]	0	0	0-1[e] [f]	0	0
13	Start Time	2+Length	0	0-1 [g]	0	0	0-1 [g]	0	0
14	End Time	2+Length	0	0-1[g]	0	0	0-1[g]	0	0
15	MCBCS Service Continuity Indicator	2+1	0	0-1[g]	0	0	0-1[g]	0	0

1 **Notes:**

- [a] If ServiceProfileID is provided then TLV IDs greater than 3 overrides the QoS parameter settings of the related ServiceProfile according to the TLV-value. The order in which the Packet Flow Descriptor will be mapped to the pre-configured flows at the ASNGW shall be the same in which they are received.
- [b] If ServiceProfileID is not provided these RADIUS attributes are MANDATORY. If the RADIUS attributes are missing then the NAS SHALL silently discard this RADIUS attribute and should reject the network entry of the MS.
- [c] This attribute SHALL be present if ServiceProfileID is not present and:
Direction is Uplink or
Direction is bi-directional and the flow is symmetrical
If the attribute is missing then the NAS SHALL reject the network entry of the MS.
- [d] This attribute SHALL be present if ServiceProfileID is not present and:
Direction is Downlink or
Direction is bi-directional and not symmetrical.
If the attribute is missing then the NAS SHALL reject the network entry of the MS.
- (e) This attribute is applicable to the downlink service flow only
- [f] This attribute is not applicable for MCBCS service;
- [g] This attribute is only applicable for MCBCS service;

2

TLV ID	1 for PacketDataFlow-ID
Description	This attributes identifies a packet data flow instance. The identifier is assigned by the home network and is unique per mobile session or per MCBCS service for the entire session. PacketDataFlow-IDs 1 to 20 are assigned for the packet data flow of the Initial Service Flow (ISF). If PacketDataFlow-ID is used for MCBCS service, it SHALL be used together with MCBCS Transmission Zone ID to uniquely identify the MCBCS service

	within the MCBCS Transmission Zone.
Length	2+2
Value	Unsigned Short representing the flow identifier (most significant bit first). A value of zero(0) is invalid,

1

TLV ID	2 for ServiceDataFlow-ID
Description	This attribute is used to group of one or more packet data flows belonging to the same service instances (e.g., a combined voip/video call). The number is assigned by the home network and is unique per mobile session or per MCBCS service for the entire session. The same Service Data Flow ID may appear in more than one Packet Data Flow ID. ServiceDataFlow-ID of 1 is assigned for the Initial Service Flow.
Length	2+2.
Value	Unsigned Short representing the Service flow identifier (most significant bit first). This value is assigned by the home network and is unique per mobile session or per MCBCS service for the life of the session. A value of zero(0) is invalid.

2

TLV ID	13 for Start Time
Description	The time of packet data flow start; (UTC time format)
Length	2+Length of time
Value	

3

TLV ID	14 for Start Time
Description	The time of packet data flow End; (UTC Time format)
Length	2+Length of time
Value	

4

TLV ID	15 for Service Continuity Indicator
Description	The Flat whether support service continuity among MBS Zones which belong the same MCBCS Transmission Zone
Length	2+1
Value	Octet enumeration with the following values: 0 = Not support 1 = Support others = Reserved

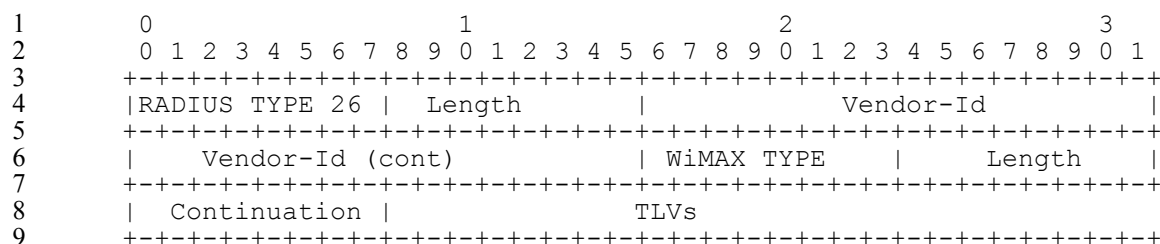
5

6

7 **5.3.1.3.1.3 QoS-Descriptor [Refer to 5.4.2.29 in NWG Release v1.3.0]**

8

MCBCS-DSx



Type-ID	29 for QoS-Descriptor
Description	This attribute describes over the air QoS parameter that are associated with a flow. The QoS-Descriptor is only valid for the actual RADIUS transaction.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types are described below.

10

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR	COA Req	COA Ack	COA NAK
1	QoS ID	3	0	1	0	0	1	0	0
2	Global Service Class Name	2+6	0	0-1	0	0	0-1	0	0
3	Service Class Name	2+Length	0	0-1	0	0	0-1	0	0
4	Schedule Type	3	0	1	0	0	1	0	0
5	Traffic Priority	3	0	0-1[a][b]	0	0	0-1[a][b]	0	0
6	Maximum Sustained Traffic Rate	6	0	0-1[a]			0-1[a]		
7	Minimum Reserved Traffic Rate	6	0	0-1[a]	0	0	0-1[a]	0	0
8	Maximum Traffic Burst	6	0	0-1[a]	0	0	0-1[a]	0	0
9	Tolerated Jitter	6	0	0-1[a]	0	0	0-1[a]	0	0
10	Maximum Latency	6	0	0-1[a]	0	0	0-1[a]	0	0
11	Reduced Resources Code	3	0	0-1[a][g]	0	0	0-1[a][g]	0	0
12	Media Flow Type	2+1	0	0-1[a]	0	0	0-1[a]	0	0
13	Unsolicited Grant Interval	4	0	0-1[a]	0	0	0-1[a]	0	0
14	SDU Size	4	0	0-1[a]	0	0	0-1[a]	0	0
15	Unsolicited Polling Interval	4	0	0-1[a]	0	0	0-1[a]	0	0
16	Media Flow Description in SDP Format	2 + Length	0	0-1[c]	0	0	0-1[c]	0	0
17	Transmission policy	1	0	0-1[f]	0	0	0-1[f]	0	0

Notes:

- [a] The inclusion of these attributes are as per the value of the Schedule-Type in accordance to the Networking Stage-3 Base Specification.
- [b] If omitted the traffic priority is assumed to be 0.
- [f] If omitted the Transmission policy is assumed to be 0. If included, the ASN MAY ignore it.
- [g] This attribute is not applicable for MCBCS Service.

5.3.1.4 Radius Related messages for MCBCS Accounting

5.3.1.4.1 Status and Type

Table 5-7 : Status and Type for RADIUS Accounting Start/Stop/Interim Messages

Name	Type	Description	Start	Int	Stop
MCBCS-Service-Type	111	Indicates the type of MCBCS service (e.g. streaming, download etc.)	1	0-1	0-1
Transport-Type	112	Indicates the type of transport used to deliver content	1	0-1	0-1
Acct-Status-Type	40	Indicates the record type: Start, Stop, Interim	1	1	1
Acct-Terminate-Cause	49	Indicates why the session stopped.	0	0	0-1[1]
Session-Continue	26/21	True indicates that the stop is immediately followed by a start. If the attribute is missing or FALSE it means that this is the final stop.	0	0	0-1[5]
Beginning of Session	26/22	True: a new flow is starting. False or missing, this is a continuation of a previous flow.	0-1[5]	0	0
IP technology	26/23	Proxy CMIP4, CMIP4	0-1[5]	0-1[5]	0-1[5]
Hotline-Indicator	26/24	Indicates that the flow is hotlined	0-1[4]	0-1[4]	0-1[4]
Prepaid-Indicator	26/25	Indicates that the flow is being prepaid	0-1	0-1	0-1
Class	25	SHALL be inserted by the accounting client if received in Access-Accept.	0-1[2]	0-1[2]	0-1[2]
Idle-Mode-Transition	26/44	Indicates idle mode entry (1) or exit (0)	0	0-1[3,5]	0
Count-Type	26/59	Unsigned Octet value used to indicate if the record represents	0	0-1[6]	0-1[6]

Name	Type	Description	Start	Int	Stop
		compressed counts over-the-air. 0x00 = Uncompressed counts 0x01 = Compressed counts			

Notes:

- [1] Only included in Stop record when the session has terminated.
- [2] Class SHALL be included if received in RADIUS Access-Accept.
- [3] Only included when supported by the NAS and Idle Mode Notification has been requested by the HAAA. Never appears in messages from the HA.
- [4] If the session is hotlined, and the NAS received this in an Access-Accept or a COA message, then the NAS SHALL include this attribute as received in the Accounting messages.
- [5] SHALL NOT be included if accounting is from an HA.
- [6] Included whenever counter information is supplied

5.3.1.4.2 Record Correlators

Table 5-8 : Record Correlators for RADIUS Accounting Start/Stop/Interim Messages

Name	Type	Description	Start	Int	Stop
Acct-Session-Id	44	Used to match Starts, Stop, and Interim. It is generated by the accounting client and is unique per start/stop pair.	1	1	1
Acct-Multi-Session-Id	50	This identifier is set to the value of WiMAX-Session-ID which is generated by AAA after a successful initial network entry with authentication. It is delivered to the NAS in an Access-Accept message. It is unique per CSN and is used to match all accounting records within a session.	1	1	1
SDFID	26/27	This value matches all packet data flows from the same service data flow.	0-1 [2,4]	0-1 [2,4]	0-1 [2,4]
Framed-IP-Address	8	The IPv4 address assigned to the MS by HCSN. This identifies the IP-Session	0-1[3]	0-1[3]	0-1[3]
Framed-IPv6-Prefix	97	The IPv6 prefix assigned to the MS by HCSN. This identifies the IP Session.	0-1[3]	0-1[3]	0-1[3]
Framed-Interface-Id	96	The IPv6 interface id assigned by the Home CSN to be used for the MS. Used only for DHCPv6-based address configuration.	0-1[3]	0-1[3]	0-1[3]

Name	Type	Description	Start	Int	Stop
Visited Framed-IP-Address	26/79	The IPv4 address assigned to the MS by VCSN. This identifies the IP-Session	0-1[5]	0-1[5]	0-1[5]
Visited Framed-IPv6-Prefix	26/80	The IPv6 prefix assigned to the MS by VCSN. This identifies the IP Session.	0-1[5]	0-1[5]	0-1[5]
Visited-Framed-Interface-Id	26/81	The IPv6 interface id assigned by the visited CSN to be used for the MS. Used only for DHCPv6-based address configuration.	0-1[5]	0-1[5]	0-1[5]
PDFID	26/26	This value matches all records from the same packet data flow. PDFID is assigned by the CSN and remains constant through all handover scenarios.	0-1 [1,4][6]	0-1 [1,4][6]	0-1 [1,4][6]
MCBCS-Transmission-Zone-ID	26/113	Indicates the MCBCS Transmission Zone for a given MCBCS Service.	0-1 [1,4][6]	0-1 [1,4][6]	0-1 [1,4][6]

Notes:

- [1] SHALL be included when flow based accounting is being performed. SHALL not be included when Session-based accounting.
- [2] SHALL not be included when session based accounting. Included if available when flow-based accounting is used.
- [3] Either Framed-IP or Framed-IPv6 SHALL be present in Accounting messages. If both are present then the HAAA SHALL discard the Accounting message.
- [4] SHALL NOT be included with messages coming from an HA.
- [5] If VCSN is assigning IP address either Visited Framed-IP or Visited Framed-IPv6-Prefix SHALL be present in Accounting messages. If both are present then the VAAA SHALL discard the Accounting message.
- [6] PDFID shall be used together with MCBCS Transmission Zone to uniquely identify a service flow of MBS within MCBCS Transmission Zone;

5.3.1.4.3 User Identification

Table 5-9 : User Identification for RADIUS Accounting Start/Stop/Interim Messages

Name	Type	Description	Start	Int	Stop
User-Name	1	The identity and realm of the user used in the outer NAI during network access authentication and authorization	1	1	1
CUI	89	Chargeable User Identity. It is a unique temporary handle to the user responsible for paying the bill.	0-1[1]	0-1[1]	0-1[1]

Name	Type	Description	Start	Int	Stop
Calling-Station-Id	31	The MAC address in binary format of the MS	0-1[2]	0-1[2]	0-1[2]

Notes:

- [1] SHALL be included if received in an RADIUS Access-Accept packet.
- [2] SHALL be included from messages coming from a NAS. SHALL NOT be included from messages coming from an HA

5.3.1.4.4 Time

Table 5-10 : Time for RADIUS Accounting Start/Stop/Interim Messages

Name	Type	Description	Start	Int	Stop
Acct-Session-Time	46	The number of seconds the flow or session was active.	0	0-1	0-1
GMT-Time-Zone-Offset	26/3	The offset in seconds from GMT at the NAS or HA.	0-1	0-1	0-1
Event-Timestamp	55	The time the event occurred.	1	1	1
Active-Time	26/39	The time in which the MS is active as opposed to idle mode.	0	0-1[1]	0-1[1]

Notes:

- [1] SHALL NOT be reported by a HA.

5.3.1.4.5 L3 Counters

Table 5-11 : L3 Counters for RADIUS Accounting Start/Stop/Interim Messages

Name	Type	Description	Start	Int	Stop
Acct-Output-Octets	42	The total number of octets in IP packets sent to the user or MBS Distribution DPF, as received at the accounting agent from the IP network (i.e. prior to any compression and/or fragmentation).	0	0-1	0-1
Acct-Input-Octets	43	The total number of octets in IP packets sent by the user. Counted after de-compression and de-fragmentation at the accounting agent.	0	0-1[3]	0-1[3]

Name	Type	Description	Start	Int	Stop
Acct-Output-Packets	47	The total number of IP packets sent to the user or MBS Distribution DPF, as received at the accounting agent from the IP network (i.e. prior to any compression and/or fragmentation).	0	0-1	0-1
Acct-Input-Packets	48	The total number of IP packets sent by the user. Counted after de-compression and de-fragmentation at the accounting agent.	0	0-1[3]	0-1[3]
Acct-Output-Gigawords	52	Incremented when attribute 42 overflows	0	0-1	0-1
Acct-Input-Gigawords	53	Incremented when attribute 43 overflows	0	0-1[3]	0-1[3]
Control-Packets-In	26/31	Packet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.	0	0-1	0-1
Acct-Output-Packets-Gigaword	26/48	Incremented when attribute 47 overflows	0	0-1	0-1
Acct-Input-Packets-Gigaword	26/49	Incremented when attribute 48 overflows	0	0-1[3]	0-1[3]
Control Octets In	26/32	Octet counts for incoming Mobile IPv4, DHCP, ICMP messages etc.	0	0-1[1]	0-1[1]
Control Packets Out	26/33	Packet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.	0	0-1[1]	0-1[1]
Control Octets Out	26/34	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.	0	0-1[1]	0-1[1]

Notes:

- [1] SHALL NOT be reported by a HA.
- [2] SHALL Not be reported in Unicast case
- [3] SHALL Not be reported in MCBCS case

5.3.1.4.6 Granted-QoS

Table 5-12 : Granted-QoS for RADIUS Accounting Start/Stop/Interim Messages

Name	Type	Description	Start	Int	Stop
Uplink Granted-QoS	26/30	Uplink QoS granted to the MS	0	0-1[1][2]	0-1[1][2]

Name	Type	Description	Start	Int	Stop
Downlink Granted-QoS	26/63	Downlink QoS granted to the MS or MCBCS Service	0	0-1[1]	0-1[1]

Notes:

[1] Attribute SHALL NOT appear when Session-based accounting is performed or from an HA.

[2] SHALL Not be reported for MCBCS Service

5.3.1.4.7 Flow Specification

Table 5-13 : Flow Specification for RADIUS Accounting Start/Stop/Interim Messages

Name	Type	Description	Start	Int	Stop
Uplink Flow-Description	26/50	IPFilter Rule that describes an Uplink PD flow with the header fields.	0	0-n[1] [2]	0-n[1] [2]
Downlink Flow-Description	26/62	IPFilter Rule that describes a Downlink PD flow with the header fields.	0	0-n[1]	0-n[1]
Flow-Description V2	26/83	Classifier that describes the flow. Direction is included as a part of the Classifier definition.	0	0-n[1] [2]	0-n[1] [2]

Notes;

[1] Attribute SHALL not appear when Session-based accounting is performed.

The MS's IP address (HoA) SHALL be included as either in the source address or destination address depending on the PD flow direction.

The IP address of the correspondent node may be included.

The port number for each end may be included. The protocol field may be included.

If a specific field in the IPFilterRule is wild-carded, that field is not used while matching a PD flow against the IPFilterRule.

SHALL NOT be reported by a HA.

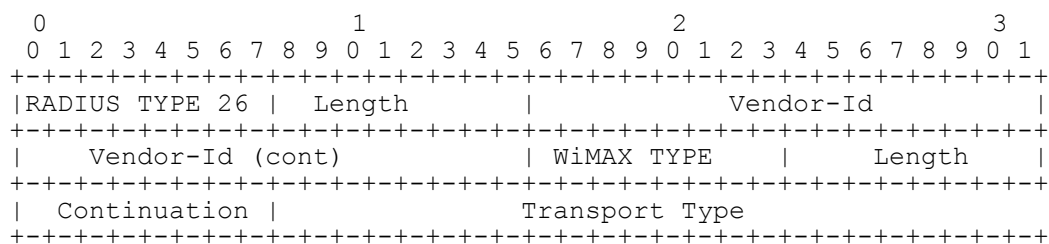
[2] SHALL Not be reported for MCBCS Service

All the attributes that are not addressed here for UDR structure, please refer to NWG Rel 1.3 for more details.

5.3.1.4.8 RADIUS VSA Definition for MCBCS Accounting Support

5.3.1.4.8.1 MCBCS service Type

5.3.1.4.8.2 Transport Type



WiMAX FORUM PROPRIETARY AND CONFIDENTIAL – SUBJECT TO CHANGE WITHOUT NOTICE

Annex A: IEEE 802.16 MCBCS Synchronization Support (informative)

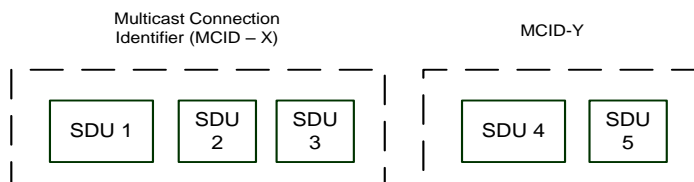
This section provides overview of bearer processing required to achieve macro-diversity level of synchronization as defined in [IEEE 802.16]. Note, that the primary document providing R1 (radio interface) specification is [IEEE 802.16].

In the context of the MCBCS synchronization description, the term “MBS Permutation Zone” is used to refer to the reserved dedicated radio resource that is allocated for a given MCBCS programming transmission. The MBS Permutation Zone is dedicated to a single MBS zone.

When the ingress of the wireless access network (ASN) receives the incoming MCBCS data, the following set of operations happen to the bearer plane processing.

0. Packet classification and IP flow identification

The process is to perform the classification process to determine of which particular incoming Service Data Units (SDUs) are belonged to the appropriate service flow(s) or connection(s) for the corresponding MCBCS programming(s).



Annex A - Figure- 1: Packet Classification into Service Flow / CID

1. MBS MAC PDU construction

This is a MAC layer function. Once the SDU is classified to a given service flow or connection, the MAC PDU processing begins:

a. Fragmentation and packing

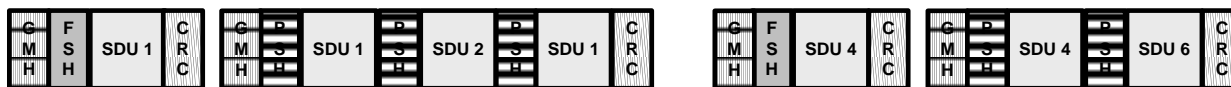
Dependent on the size of the SDU and QoS requirements, the SDU may be fragmented into multiple MAC SDUs or packed into a single MAC SDU.

b. MAC header encapsulation

Once the MAC SDU is constructed, the fragmentation subheader or packing subheader may be attached and then the Generic MAC header will be attached.

c. Checksum calculation

The final step of the MAC PDU construction is to calculate the checksum for the MAC PDU.



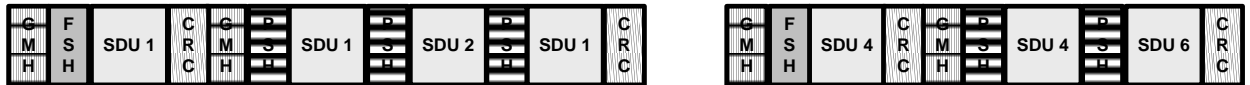
Annex A - Figure- 2: MBS MAC PDU construction

2. MBS MAC Burst construction

This is a MAC layer process of packing a groups of MAC PDUs which may be belonged to one or more Multicast Connection IDs (MCIDs) into a pre-determined data region within a dedicated MBS permutation zone.

According to the IEEE 802.16 specification, a permutation zone is a number of contiguous OFDMA symbols, in the downlink or uplink, that use the same permutation formula.

In OFDMA, a data region is a two-dimensional allocation of a group of contiguous subchannels, in a group of contiguous OFDMA symbols. All the allocation refers to logical subchannels.



Annex A - Figure- 3: MBS MAC Burst Construction

3. MBS PHY Burst construction

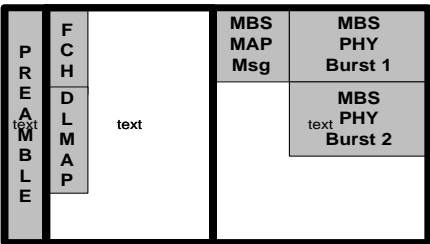
A MAC Burst will be transformed into a PHY Burst in a form of bit stream after applying the channel coding procedures in the following order, i.e. Randomization, Forward Error Correction (FEC), Bit Interleaving, Repetition and Modulation.



Annex A - Figure- 4: MBS PHY Burst Construction

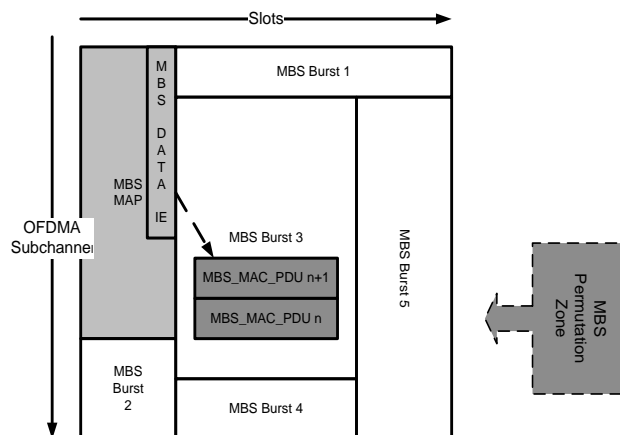
4. MBS Permutation Zone construction

This is a PHY layer process of packing different PHY Bursts into a reserved location of the RF region in a downlink subframe.



Annex A - Figure- 5: MBS Permutation Zone Construction

Each MBS permutation zone is identified by the MBS Zone ID. MBS MAP message, if present, always locate at the beginning of each MBS permutation zone, it contains the MBS_DATA_IE is used to describe of which the MBS Burst corresponding to a given MBS region contains the MBS_MAC_PDU which is index by the MCID that carries the given MCBCS program content. With the MCID and MBS Zone ID as the DL subframe descriptor of the MBS permutation zone, the MS's MAC/PHY can selectively decode only the MBS_MAC_PDUs associated with the corresponding MCBCS program content that the MS is interested in. The following figure summarizes the descriptions above.



Annex A - Figure- 6: Example of MBS Permutation Zone Organization

5. MBS Permutation Zone scheduling

This is a PHY layer process that schedules the MBS specific downlink transmission over the air.

Annex B – Synchronization among the multiple MBS Distribution DPFs (informative)

Having more than one MBS Distribution DPFs that cooperate in processing and distributing the same content, requires certain support from the Multicast Routing infrastructure. If the Multicast Routing Infrastructure supports sequence numbering (assigned by the traffic source) and, optionally, lost data recovery, then it would become possible to build a synchronized network with multiple MBS Distribution DPFs. The core of such a network will consist of general purpose multicast routers, while the MBS Distribution DPF will mediate between the internal and the external protocols – i.e. MBS Distribution DPF will use R3 MBS payload information to define sequence numbering of MBS packets after classification. MBS Distribution DPF terminates the Reliable Multicast Transport. The rest of the ASN and the MS remain agnostic to this functionality.

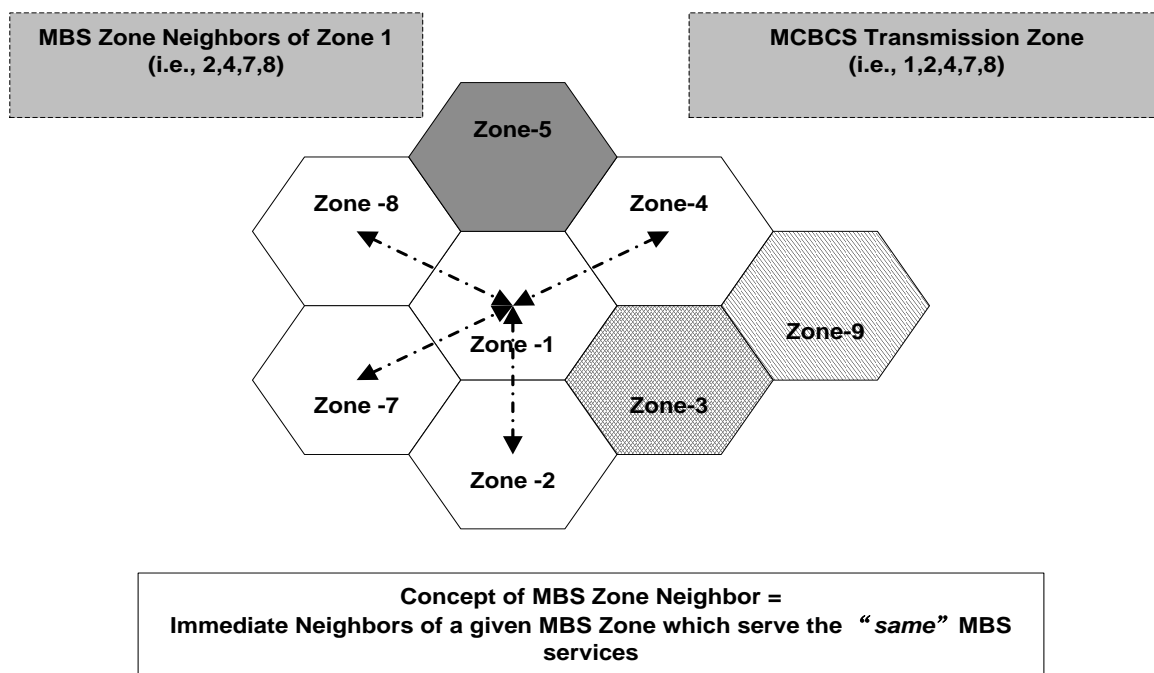
Reliable Multicast Routing Infrastructure is described in several IETF RFCs, e.g. RFC 3208 (PGM), RFC 3940 (NORM), RFC 4410 (SRM), so there is no need to standardize it in WiMAX. The selection of the Reliable Multicast Routing mechanism is out of the scope of this specification.

Standardization of this option is FFS.

Annex C – IEEE 802.16 Service Continuity Support Capabilities

Annex C - 1 MBS Zone Neighbor Concept from IEEE 802.16-Rev2 to Support Inter-MBS Service Continuity

MBS Zone neighbors are the immediate neighbor zones of the current serving MBS Zone to support the same MCBCS service that has been provided to the MS. When the MS crosses the MBS zones, the network may use such MBS Zone neighbors concept to identify the new target MBS Zone for the MS to make the transition to. The concept of the MBS Zone neighbors is described as follows:



Annex C - Figure 1 : The concept of the MBS Zone Neighbors

Annex C - 2 MBS DL Transmission Daisy Chaining Concept via the support of IEEE 802.16-Rev2 MBS_MAP_IE, MBS_MAP Message and MBS_Data_IE for the support of Service Continuity

When MS moves to new BS within the same MBS zone, the daisy-chaining mechanism provided by the MBS_DATA_IE as specified by the IEEE 802.16 specification that is described in [MBS Data Sync section] to keep track of the MCBCS program content DL transmission throughout the intra and inter MBS Zones. In any event when the MS lost sync with the network, the regular Handover (HO) or location update (LU) procedure should allow the MS to re-gain the system parameters for the same MBS Zone, and therefore, to resume the reception of the MCBCS program content DL transmission.

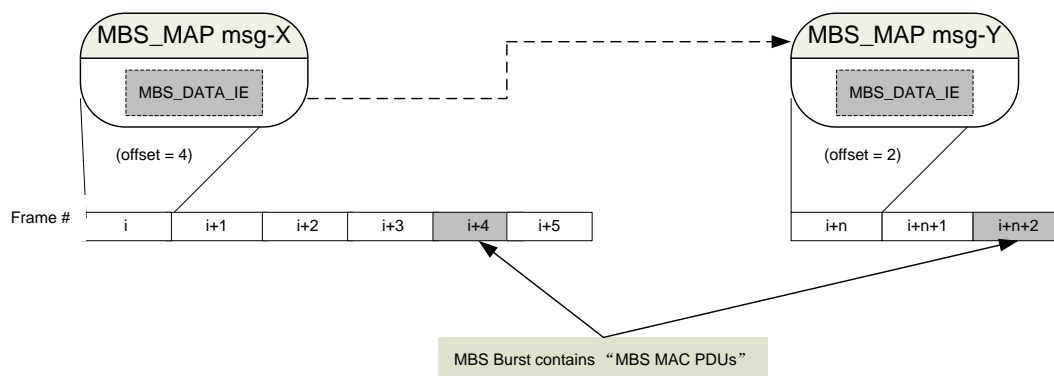
For more information on how the MBS_MAP_IE, MBS_MAP message and MBS_DATA_IE supports the daisy chaining should be referred to [HO and Power Saving sections].

MCBCS-DSx

The following figures describe the IEEE 802.16-Rev2 on how the MBS_DATA_IE supports the daisy-chaining for the MCBCS DL transmission.

Level-1: Inter MBS-MAP message interval that is used to indicate the next segment of MCBCS program content DL transmission interval via the daisy-chaining mechanism supported by the MBS_DATA_IE (Note: up to 255 frames.)

Level-2: Inter MBS burst interval via the offset of 2-5 frames (i.e. indicating what is the range of the next offset of the MBS burst that could contain the MBS MAC PDUs.)



Annex C - Figure 2 : Daisy-chaining support via MBS_MAP_IE, MBS_MAP msg and MBS_DATA_IE

