Project	**IEEE 802.16 Broadband Wireless Access Working Group <http://ieee802.org/16>**
Title	Procedures Clarifications and Improvement for MBS Logical Channel support in 802.16REV2
Date Submitted	**2008-04-20**
Source(s)	mailto:
	Jonathan Segev, Comsys — jonathan.segev@comsysmobile.com
	Tricci So, ZTE — tso@zteusa.com
	Jerry Chow, ZTE — jchow@zteusa.com
Re:	P802.16Rev2/D4, LB26c
Abstract	The current definition of Logical Channel support for MBS has deficiencies in the areas of CS classification and CS SAP, and in the support for packing and robustness in the presence of MAC header detection errors for multi-PDU MBS bursts on the MAC data path.
Purpose	Adoption toward REV2/D5
Notice	*This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups.* It represents only the views of the participants listed in the "Source(s)" field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.16.
Patent Policy	The contributor is familiar with the IEEE-SA Patent Policy and Procedures: <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and <http://standards.ieee.org/guides/opman/sect6.html#6.3>. Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and <http://standards.ieee.org/board/pat>.

Procedures Clarifications and Improvement for MBS Logical Channel support in 802.16REV2

Jonathan Segev (Comsys)

Jerry Chow (ZTE), Tricci So (ZTE)

Problem Statement:

The current IEEE 802.16 standard allows the support for packing multiple MBS content channels which share the common service characteristics and parameters (e.g. QoS, DL transmission opportunity etc.) into a same MBS service flow or MBS connection. This mechanism suits well to MBS "data cast" services which bundle multiple TV or video or radio channels into a single service-pack for the MBS subscribers. Such service offering greatly simplifies both the network and subscriber service provisioning, configuration and management. In addition, it also optimizes the MS's operation to receive DL transmissions during the mobility and power saving mode..

The definition of MBS logical channel support within the current IEEE 802.16 standard, however, is not complete in a couple of areas:

- Lack of descriptions of how classification applies to the MBS Service Flow to map SDUs to logical channels

- Lack of identification of the logical channel to which, a MAC SDU or SDU fragment within a MAC PDU, belongs to an MBS connection that the logical channel support is enabled. Missing the logical channel identification information within the MAC PDU hinders certain MAC PDU processing features, such as SDU packing and recovery from Generic MAC Header detection errors within a multi-PDU burst, that are currently available for a connection to be properly supported.

This contribution provides remedies for these deficiencies in the current IEEE 802.16 standard so that the logical channel feature for MBS is complete.

Background:

The intent of this proposal is to describe the how to support the MBS logical channel by performing the MBS classification to map the corresponding MBS content channel to a given {MCID, LCID} tuple for the MAC SAP.

**Conceptual View of the MBS Policy Management** (see the following figure)
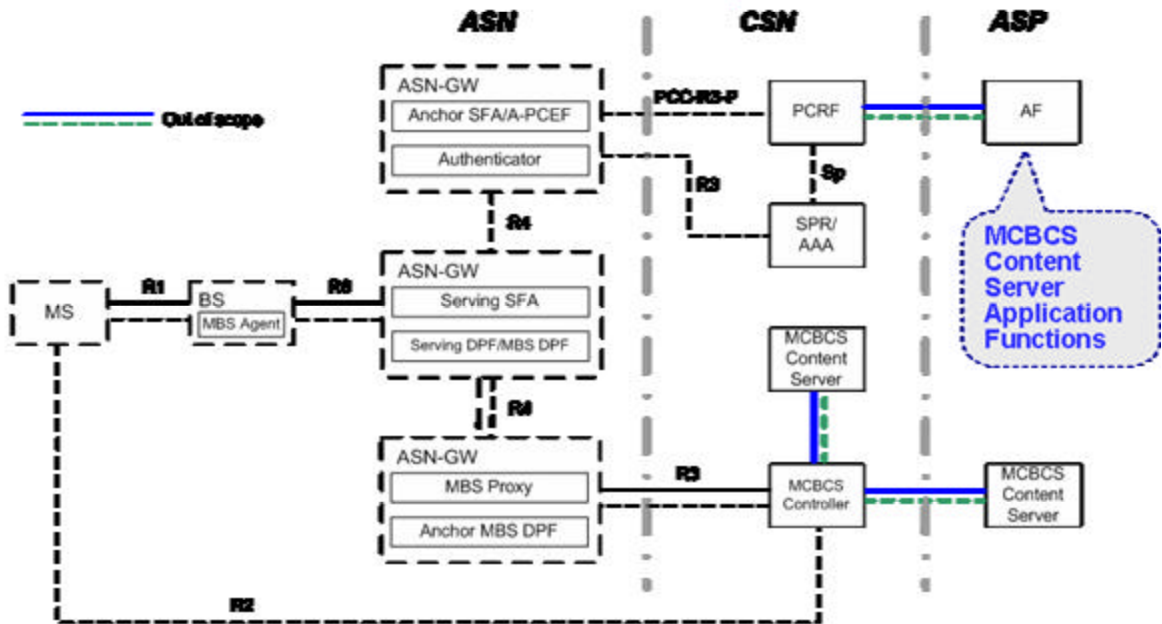
Curtesy of the Huawei's proposal to NWG MCBCS subteam for MCBCS policy function support

Facts for MBS Classification Support

1. Today IEEE 802.16e supports more than one set of classifiers for each service flow and the classifiers can be prioritized based on the network service policy.

2. In today NWG Rel-1.0 unicast support, the set of classifiers are associated with the Packet Service Data Flow (i.e. SDFID) and it is up-to the access network (i.e. ASN) to determine how to partition the service policy (e.g. classifiers) into one or more Packet Data Flow (PDFID) at the CSN which is then mapped to the WiMAX service flow (i.e. PDFID-to-SFID) at the ASN.

3. In summary, the application's service policy provides the set of classifiers to be assigned and associated with the WiMAX service flow in the ASN.   The ASN will then determine how to associate the service flow to the CID in the case of unicast support.

4. When the MBS logical channel is supported, each MBS content channel is assigned with a given MBS content ID by the MBS service policy and will have their own unique set of classifiers for one or more classification rules for the given MBS service flow –   the basic concept of the service flow classification has not changed for the support of the MBS logical channel.   It is **IMPORTANT** to point out that, the same classification operation will be applied to the MBS service flow even without the implementation of the MBS logical channel in the ASN.

5. The duty of the MBS Service Flow Agent (SFA) in the ASN is to determine how to leverage this additional information provided by the policy server to the CS SAP and to the MAC SAP to support the classification and CID/LCID mapping respectively – i.e. managing the set of classifiers that are associates each content ID to a logical channel. Once the logical channel is identified, the extended sub-header will be assigned to each logical channel as the MAC PDU delimiter to support packing and FEC operation.

Highlevel view on the MBS Transport Connection Classification
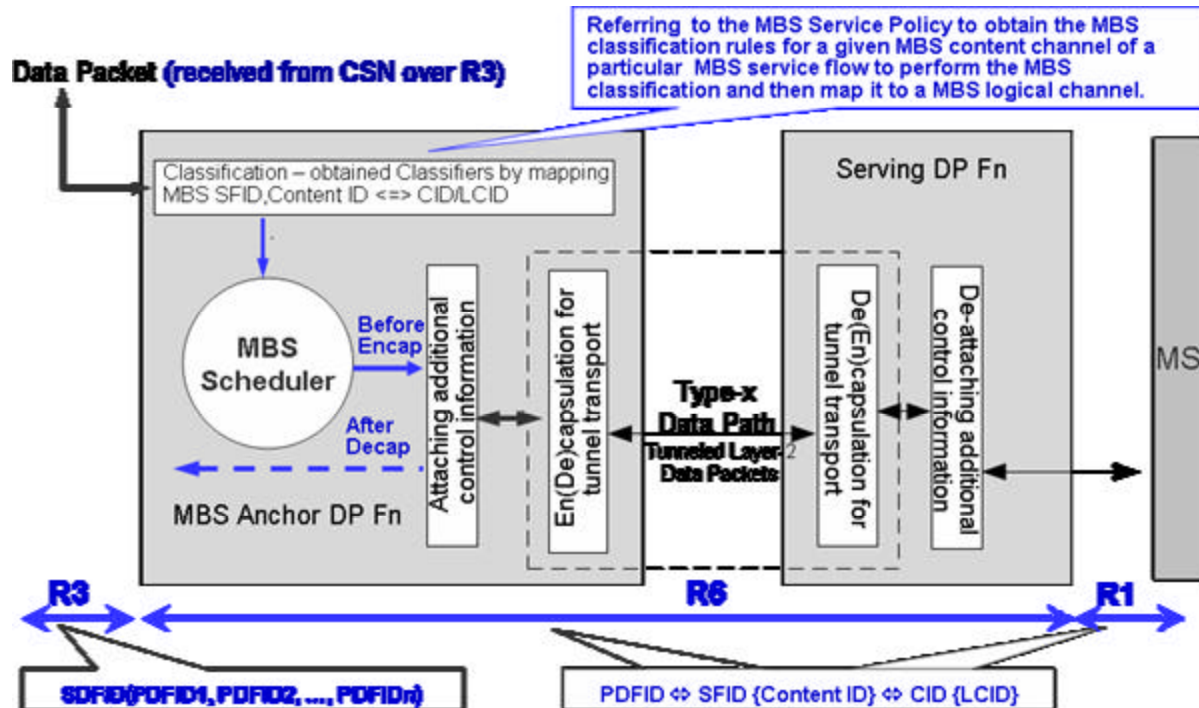
As shown in the above figure, the MBS classification process at the ASN-GW is driven by the service policy which provides the MBS classification rules for the given MBS service during the MBS bearer path establishment. The service policy will not dictate if the MBS logical channel option shall be implemented at the ASN. It is the ASN's local implementation policy decision to determine if the given MBS content channel to be associated with either the MBS MCID or MBS {MCID, LCID} tuple during the classification operation of a given MBS service flow.

In addition, due to the functional behavior of the multi-BS MBS scheduling, it is expecting that, the MBS SDU and PDU processing as well as the scheduling will not be belonged to the same functional entity to handle the unicast SDU and PDU processing and scheduling. Hence, the legacy unicast MAC PDU processing at the BS and MBS MAC PDU processing are independent operation.

To clarify the MBS logical channel support in today IEEE 802.16e specification, the proposed modified text is described in details in the following sections.

Proposed Modified Text to IEEE 802.16eRev2_D4:

5.2 Packet CS

The packet CS resides on top of the IEEE 802.16 MAC CPS. The CS performs the following functions, utilizing the services of the MAC:

    a)   Classification of the higher layer protocol PDU into the appropriate transport connection or if applicable, into the logical channel of an MBS transport connection.

b) Suppression of payload header information (optional) (Note: The payload header suppression would not be applicable to the MBS logical channel support.)

c) Delivery of the resulting CS PDU to the MAC SAP associated with the service flow for transport to the peer MAC SAP

d) Receipt of the CS PDU from the peer MAC SAP

e) Rebuilding of any suppressed payload header information (optional) (Note: the reassembly of the suppressed payload header may not be applicable to the MBS logical channel support.)

The sending CS is responsible for delivering the MAC service data unit (MAC SDU) to the MAC SAP. The MAC is responsible for delivery of the MAC SDU to peer MAC SAP in accordance with the QoS, fragmentation, concatenation, and other transport functions associated with a particular connection's service flow characteristics. The receiving CS is responsible for accepting the MAC SDU from the peer MAC SAP and delivering it to a higher layer entity.

The packet CS is used for transport for all packet-based protocols as defined in 11.13.19.3.

5.2.1 MAC SDU format

Once classified and associated with a specific MAC transport connection and if applicable, with a specific logical channel within an MBS transport connection, higher layer PDUs shall be encapsulated in the MAC SDU format as illustrated in Figure 9. The 8-bit PHSI (payload header suppression index) field shall be present when a PHS rule has been defined for the associated connection.
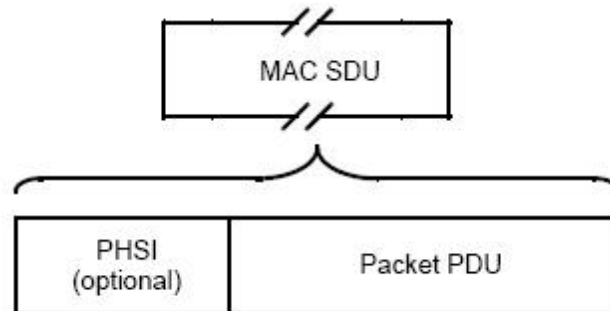
PHS is described in 5.2.3.

Figure 9—MAC SDU format

5.2.2 Classification

Classification is the process by which a MAC SDU is mapped onto a particular transport connection or onto a particular logical channel within an MBS transport connection for transmission between MAC peers. The mapping process associates a MAC SDU with a transport connection or a logical channel of an MBS transport connection, which also creates an association with the service flow characteristics of that connection. This process facilitates the delivery of MAC SDUs with the appropriate QoS constraints.

A classification rule is a set of matching criteria applied to each packet entering the IEEE 802.16 network. It consists of some protocol-specific packet matching criteria (destination IP address, for example), a classification rule priority, and a reference to a CID and if applicable, to a Logical Channel ID of an MBS transport connection. If a packet matches the specified packet matching criteria, it is then delivered to the SAP for delivery on the connection defined by the CID or on the logical channel, defined by the Logical Channel ID of an MBS transport connection by the multicast CID. Implementation of each specific classification capability (as, for example, IPv4 based classification) is optional. The service flow characteristics of the connection provide the QoS for that packet.

Several classification rules may each refer to the same service flow. The classification rule priority is used for ordering

the application of classification rules to packets. Explicit ordering is necessary because the patterns used by classification rules may overlap. The priority need not be unique, but care shall be taken within a classification rule priority to prevent ambiguity in classification. DL classification rules are applied by the BS to packets it is transmitting and UL classification rules are applied at the SS. Figure 10 and Figure 11 illustrate the mappings discussed in the previous paragraph based on the scenario when classification is applied to a CID.

It is possible for a packet to fail to match the set of defined classification rules. In this case, the CS shall discard the packet.
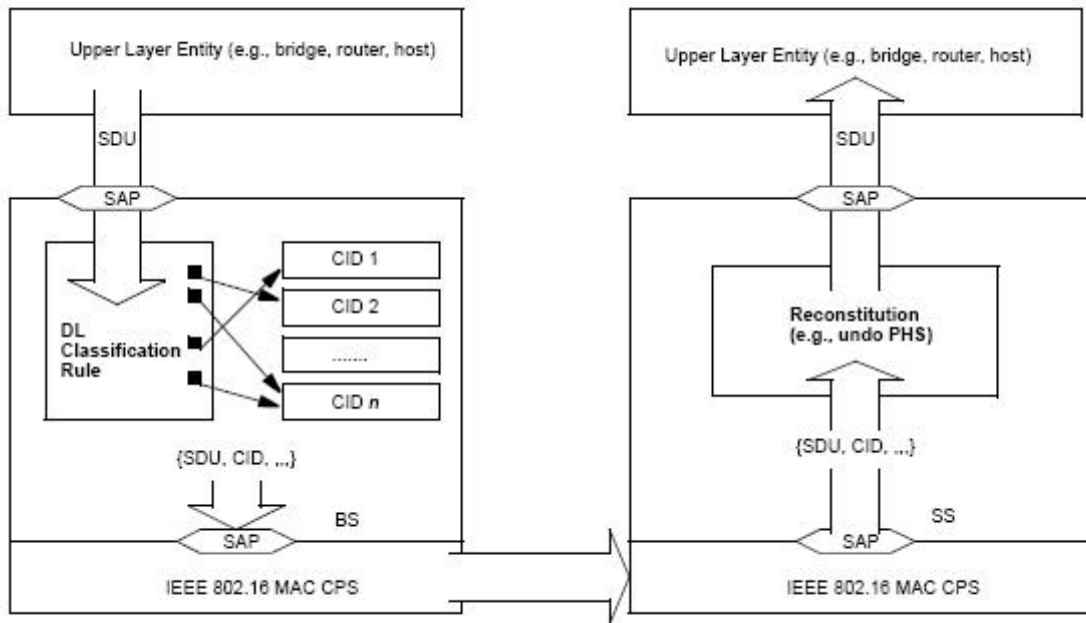
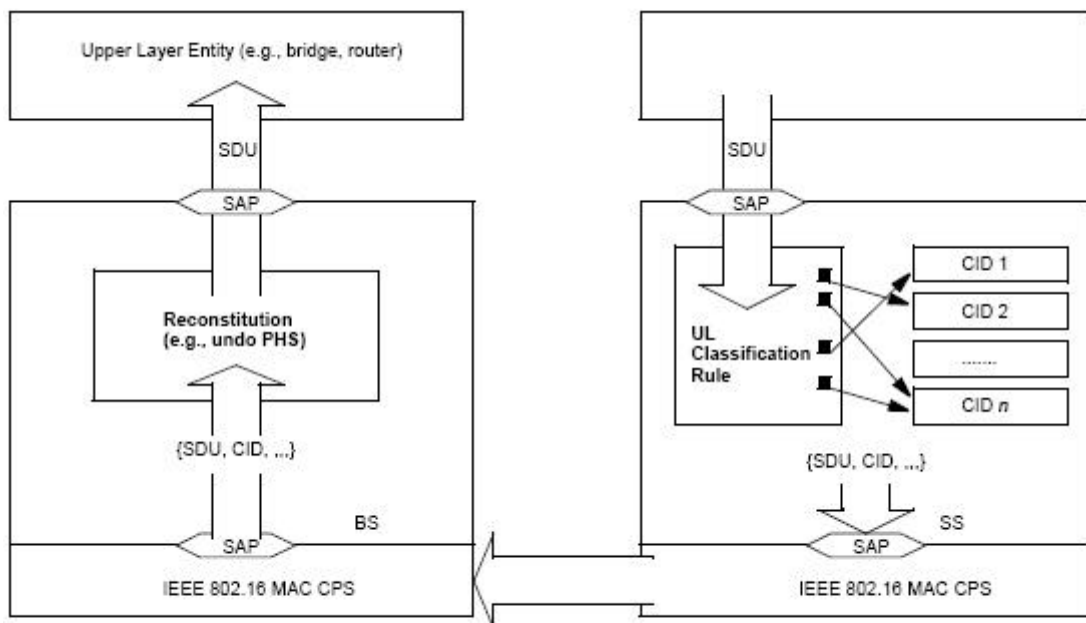Figure 10—Classification and CID mapping (BS to SS)

Figure 11—Classification and CID mapping (SS to BS)

[Editor Note: Is there a need to add new figure for Classification to LCID mapping?]

5.3 Generic Packet Convergence Sublayer (GPCS)

The Generic Packet CS (GPCS) is an upper layer protocol-independent packet convergence sublayer that supports multiple protocols over 802.16 air interface. It is defined as follows:

- GPCS provides a generic packet convergence layer. This layer uses the MAC SAP and exposes a SAP to GPCS applications
- GPCS does not re-define or replace other convergence sublayers. Instead, it provides a SAP that is not protocol specific
- With GPCS, packet parsing happens "above" GPCS. The results of packet parsing are classification parameters given to the GPCS SAP for "parameterized classification," but upper layer packet parsing is left to the GPCS application
- With GPCS, the upper layer protocol that is immediately above the 802.16 GPCS is identified by a TLV parameter, GPCS protocol type, as defined in 11.13.19.5.1 . The GPCS protocol type shall be included in C-SFM primitives and DSx messages during connection establishment.
- GPCS defines a set of SAP parameters as the result of upper layer packet parsing. These are passed from upper layer to the GPCS in addition to the data packet. The SAP parameters include SFID, MS MAC Address, data, length and if applicable, the MBS Content ID of an MBS connection. Each is defined in section 5.3.3.
- GPCS allows multiplexing of multiple layer protocol types (e.g., IPv4, IPv6, Ethernet) over the same 802.16 connection. An appropriate upper protocol layer that supports protocol multiplexing is used to do this, and it is signaled in the GPCS_PROTOCOL_TYPE TLV in DSx messages to indicate that mul-tiple protocols are supported for a connection/service flow. It is outside the scope of the GPCS to spec-ify how the upper layer multiplexes and demultiplexes multiple protocol data packets over an 802.16 connection/service flow.
- For interoperability, upper layer protocol type may need an interface specification. Such a standard specification is out of scope of this document.
- With GPCS, the 802.1D bridging will be supported transparently by 802.16 air interface, because the GPCS requires the upper layer to provide the MS MAC Address and SFID with every packet, where the MS MAC Address and SFID can represent a port and a port is either a unicast port or broadcast port.
- PHS as defined in 5.2.3 defines rules how packets with suppressed fields are reconstructed based on the PHSI and the associated PHS rule. This reconstruction method can also be applied on packets transfered over the GPCS. Details are given in chapter 5.3.6.
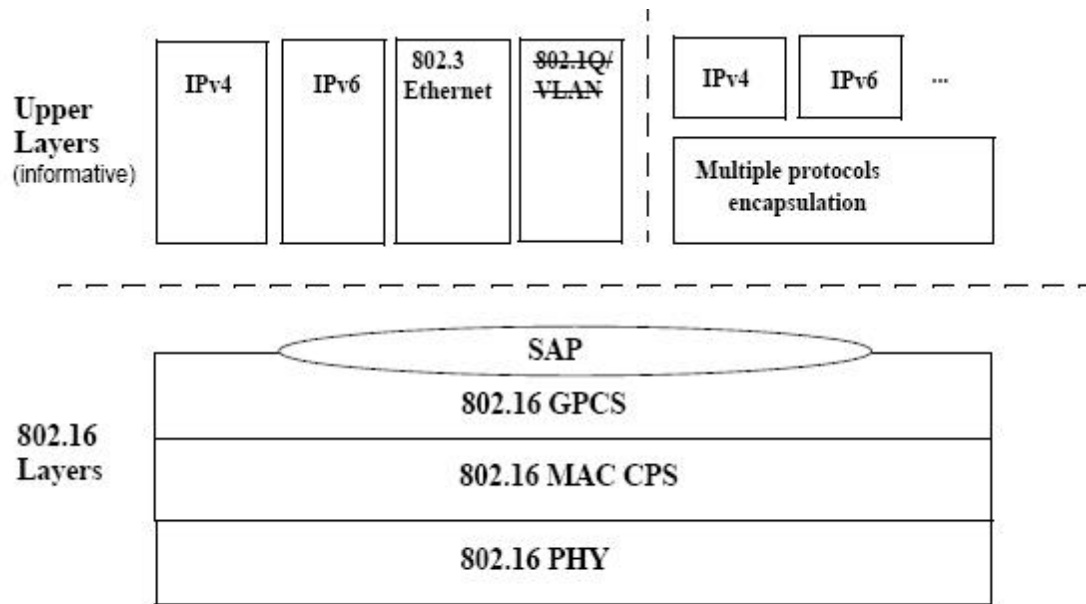
Protocol structure with the Generic Packet Convergence Sub Layer (GPCS)

Figure 21—GPCS Layering Model

5.3.1 Mapping of the GPCS service to upper layers

In the case where a GPCS instance services only a single GPCS peer on an SS, the MS MAC Address field of the GPCS_DATA primitive shall be constant and set to the MAC address of the SS. The SFID field of the GPCS_DATA primitive shall be set to the SFID of the service flow being carried.

In the case where a GPCS instance services more than one SS, the MS MAC Address field of the GPCS_DATA primitive will indicate the SS that is the source or destination for the PDU. The SFID field of the GPCS_DATA primitive shall be set to the SFID of the service flow being carried.

5.3.2 Operation of GPCS with SSs that do not support the GPCS

A BS that supports GPCS may interoperate with an SS that does not support GPCS. It can be observed that a GPCS service with GPCS_PROTOCOL_TYPE 0x0000 (Ethernet MAC Service) carries packets formatted identically to the packets used in the 802.3 specific part of the Packet CS. Also, a GPCS service with GPCS_PROTOCOL_TYPE 0x0003 (Raw IP) carries packets formatted identically to the packets used in the IP specific part of the Packet CS.

A BS may operate using GPCS at the base station, locally using GPCS_PROTOCOL_TYPE=0x0000, while signaling to the SS during connection setup that the 802.3 specific part of the packet CS is being used.

A BS may operate using GPCS at the base station, locally using GPCS_PROTOCOL_TYPE=0x0003, while signaling to the SS during connection setup that the IP specific part of the packet CS is being used.

5.3.3 GPCS SAP parameters

The GPCS uses the GPCS SAP, an instance of the logical CS SAP. The GPCS SAP parameters enable the upper layer

protocols to generically pass information to the GPCS so that the GPCS does not need to inter-pret upper layer protocol headers in order to map the upper layer data packets into proper 802.16 MAC con-nections. Since the SAP parameters are explicit, the parsing portion of the classification process is the responsibility of the upper layer. The parameters are relevant for SAP data path primitives, GPCS_DATA.request and GPCS_DATA.indication as described in sections 5.3.4 and 5.3.5, respectively.

Service flow ID (SFID)
Unique identifier to identify a unidirectional service flow for an MS. A GPCS implementation shall map the combination of SFID and MS MAC Address directly to a MAC connection ID. During con-nection / service flow establishment, the 802.16 control plane function shall provide GPCS the map-ping information.

MS MAC Address:
48-bit unique identifier used by MS.

DATA:
The payload delivered by the GPCS upper layer to the GPCS, or by the GPCS to the upper layer.

LENGTH:
Number of bytes in DATA.

MBS Content ID:

A 2 bytes long MBS Content IDs is used to identify that the data is associated with a particular content flow within the Service Flow that carries MBS data. MBS Content ID is vendor-specific and is dependent on application-level implementation. MBS Content ID is assigned by the MBS application and is relayed by the policy server to the upper layer of the GPCS. This parameter is only present for a Service Flow that carriers MBS data and for which MBS Content IDs have been assigned.

5.3.4 GPCS_DATA.request

Function:

This primitive defines the transfer of data from the upper layer to the GPCS.

Semantics of the service primitive:

The parameters of the primitive are as follows:

GPCS_DATA.request
(
        SFID,
        MS MAC Address,
        length,
        data,
        MBS Content ID (Note: Only applicable to MBS connection with logical channel support.)
)

The parameters, SFID, MS MAC Address, length, data and if applicable, the MBS Content ID are described in section 5.3.3.

When generated:

This primitive is generated by an upper layer protocol when a GPCS SDU is to be transferred to a peer entity or entities.

Effect of receipt:

The receipt of this primitive causes GPCS to map the SFID, and if present, the MBS Content ID as well as the MS MAC Address to a ser-vice flow and thereby a connection. GPCS invokes MAC functions, for example the MAC SAP (an example MAC SAP definition is provided in Annex C) to effect transfer of the SDU to the MAC layer.

5.3.5 GPCS_DATA.indication

Function:

This primitive defines the transfer of data from the GPCS to an upper layer protocol.

Semantics of the service primitive:
The parameters of the primitive are as follows:

> **GPCS_DATA.indication**
> (
> > SFID,
> > MS MAC Address,
> > length,
> > data
>)

The parameters, SFID, MS MAC Address, length, and data are described in section 5.3.3.

Note that SFID MS MAC Address are not transferred over the 802.16 air interface. The GPCS shall map the CID to SFID and MS MAC Address, and then pass them to the upper layer of the GPCS through GPCS_DATA.indication, where the CID provided in MAC SAP.

When generated:

This primitive is generated by GPCS whenever a GPCS SDU is to be delivered to an upper layer protocol resulting from receipt of a MAC PDU.

Effect of receipt:

The effect of receipt of this primitive by the upper layer protocol entity is dependent on the validity and con-tent of the SDU.

5.3.6 PHS operation

PHS header suppression and reconstruction according to Section 5.2.3 may be deployed on particular GPCS service flows by installing PHS rules at the receiving side of the service flow using the procedures described in chapter 5.2.3.2.

C.1.1.1.10 MAC_DATA.request

C.1.1.1.10.1 Function

This primitive defines the transfer of data to the MAC entity from a CS SAP.

C.1.1.1.11 Semantics of the service primitive

The parameters of the primitive are as follows:

MAC_DATA.request
 (
 Connection ID,
 length,
 data,
 discard-eligible flag.
 Logical Channel ID (Note: Only applicable to MBS connection with logical channel enabled)
)

The Connection ID and, if present, the Logical Channel ID parameters specify the connection and if applicable, the logical channel over which the data is to be sent; the service class is implicit in the Connection ID parameter. The length parameter specifies the length of the MAC SDU in bytes. The data parameter specifies the MAC SDU as received by the local MAC entity.

The discard-eligible flag specifies whether the MAC SDU is to be preferentially discarded by the scheduler in the event of link congestion and consequent buffer overflow. The encryption flag specifies that the data sent over this connection is to be encrypted, if ON. If OFF, then no encryption is used.

C.1.1.1.11.1 When generated

This primitive is generated by a CS whenever a MAC SDU is to be transferred to a peer entity or entities.

C.1.1.1.11.2 Effect of receipt

The receipt of these primitives causes the MAC entity to process the MAC SDU through the MAC and to pass the appropriately formatted PDUs to the PHY TCS for transfer to peer MAC entities, using the CID, and if applicable, the Logical Channel ID as specified.

C.1.1.1.12 MAC_DATA.indication

C.1.1.1.12.1 Function

This primitive defines the transfer of data from the MAC to the CS. The specific CS to receive the indicate message is implicit in the CID.

C.1.1.1.12.2 Semantics of the service primitive

The parameters of the primitive are as follows:

 MAC_DATA.indication
 (
 Connection ID,
 length,
 data,
 reception status,
)

The Connection ID parameter the connection over which the data was sent. The length parameter specifies the length of the data unit in bytes. The data parameter specifies the MAC SDU as received by the local MAC entity. The reception status parameter indicates transmission success or failure for those PDUs received via the MAC_DATA.indication.

C.1.1.1.12.3 When generated

This primitive is generated whenever an MAC SDU is to be transferred to a peer convergence entity or entities.

C.1.1.1.12.4 Effect of receipt

The effect of receipt of this primitive by a convergence entity is dependent on the validity and content of the MAC SDU. The choice of CS is determined by the CID over which the MAC SDU was sent.

C.1.1.2 MAC service stimulation of DSx messages

This subclause describes the logical interaction between the MAC Service primitives and the DSx messages. The sequence of logical MAC SAP events and the associated actual MAC events effecting a CS-stimulated connection creation are shown in Figure C.2.

Figure C.2—MAC SAP event and MAC event sequence for connection creation stimulated by CS

The sequence of logical MAC SAP events and the associated actual MAC events effecting a CS-stimulated connection change are shown in Figure C.3.
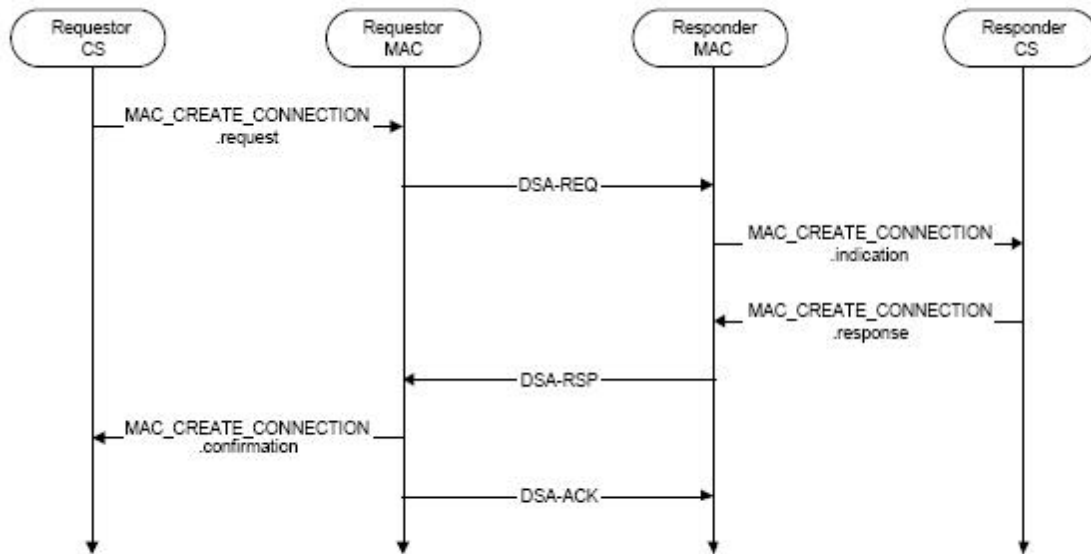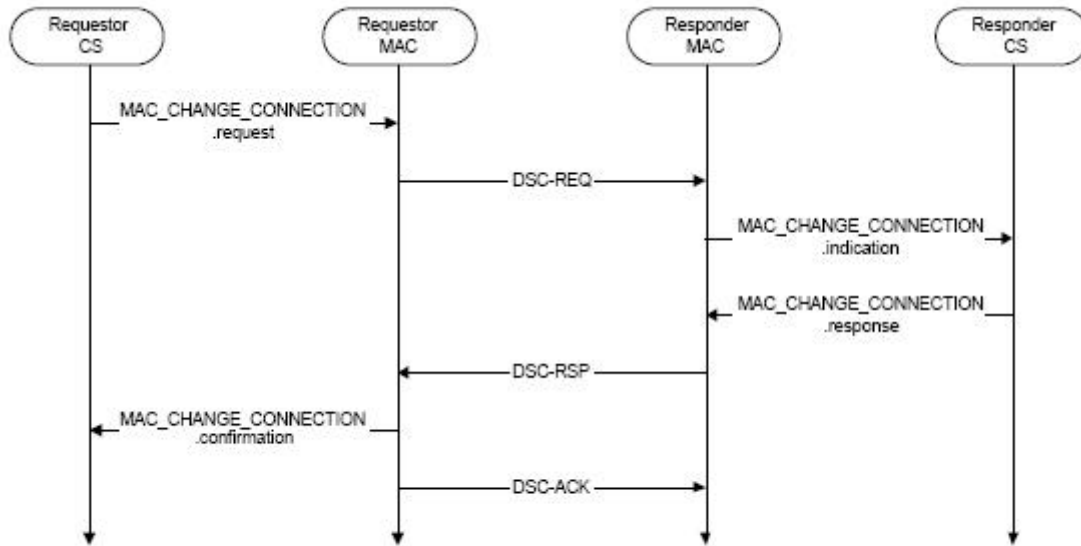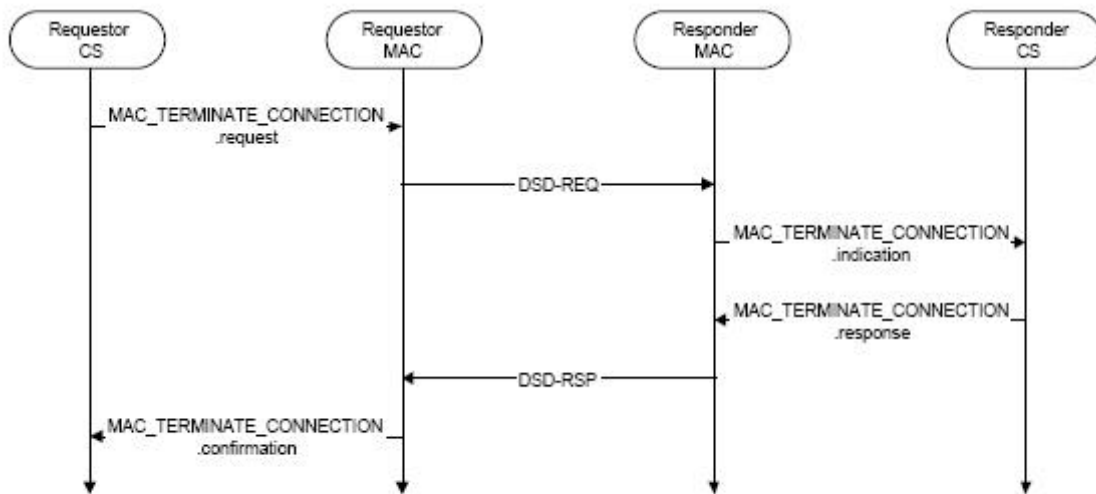
Figure C.3—MAC SAP event and MAC event sequence for
connection change stimulated by CS

The sequence of logical MAC SAP events and the associated actual MAC events effecting a CS-stimulated connection deletion are shown in Figure C.4.

Figure C.4—MAC SAP event and MAC event sequence for
connection deletion stimulated by CS

6.3.23.1 Establishment and maintenance of MBSs

Establishment of MBSs with respect to certain service flow is always performed when SS is in Normal Operation with a serving BS. MBSs are associated with multicast and broadcast service flows. Multicast and broadcast service flows are not dedicated to the specific SS and are maintained even though the SS is either in awake/sleep mode or in the idle mode. When an SS is registered at a BS for receiving MBS, multicast and broadcast service flows shall be instantiated as multicast connections. Data of multicast and broadcast service flows may be transmitted from BS and received at SS also regardless of what mode the SS is currently in. The BS may establish a DL MBS by creating a multicast and broadcast service flows when the service commences. Mapping of multicast and broadcast SFIDs to

CIDs shall be known to all BSs belonging to the same MBS zone. The method of making all BS in the same MBS Zone aware of MBS flows and associated MBS Service Flows—including multicast CID, and if applicable, logical Channel ID assignment, QoS parameter set, and Classification Rule(s)—is outside the scope of the standard. As the classification and transmission of MBS flows may be supported on a BS in an MBS Zone regardless of the presence or absence of any SS in Normal Operation receiving the service, the BS may retain MBS service flow management encodings sufficient to do classification and scheduling of received MBS flows, even when no SS participating in the service is active on the BS.

When the SS registers at the BS for receiving multicast and broadcast services, the BS or SS may initiate the DSA procedure with respect to multicast and broadcast connections. Such knowledge may be used to initiate bi-directional upper layers communication between the SS and the network for the purpose of configuration of multicast/broadcast service. After successful configuration, the SS shall reuse the same configuration when it moves to another BS without re-configuration.

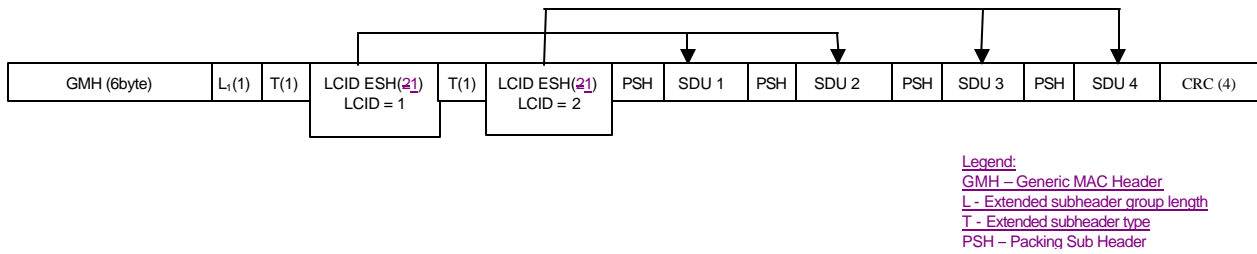*[Note to editor: insert a new subsection 6.3.2.2.7.9 as follows]*

6.3.2.2.7.9 LCID extended subheader
The LCID extended subheader shall only be sent by a BS on a MBS connection and only if LCID extended subheader capability is supported (negotiated through the REG-REQ/RSP) and LCID extended subheader is enabled for the MBS connection (negotiated in the DSA-REQ/RSP).

Name	Size (bit)	Description
Logical Channel ID	8	Logical channel ID of a sequence of one or more SDUs/SDU fragments within PDU

If more than one LCID ESH is used, the LCID ESH shall concatenated and appear in order of SDU/SDU fragments they refer to figure xxx

[note to editor: insert a new figure here]

| GMH (6byte) | L₁(1) | T(1) | LCID ESH(21) LCID = 1 | T(1) | LCID ESH(21) LCID = 2 | PSH | SDU 1 | PSH | SDU 2 | PSH | SDU 3 | PSH | SDU 4 | CRC (4) |

Legend:
GMH – Generic MAC Header
L - Extended subheader group length
T - Extended subheader type
PSH – Packing Sub Header

11.7.25 MAC header and extended subheader support

The MAC Header and Subheader Support field indicates whether the MS and BS support various types of MAC header and extended subheaders. This field may be sent by either BS or MS. Omission of this field from the REG-REQ/RSP message indicates that none of the headers or subheaders are supported.

Type	Length	Value	Scope
		Bit 0: BR and UL Tx power report header support	REG-REQ, REG-RSP
		Bit 1: BR and CINR report header support	
		Bit 2: CQICH allocation request header support	
		Bit 3: PHY channel report header support	
		Bit 4: BR and UL sleep control header support	
		Bit 5: SN report header support	
		Bit 6: Feedback header support	
		Bits 7–10: SDU_SN extended subheader support and parameter	
		Bit 7: SDU_SN extended subheader support	
		Bits 8–10 (=p): period of SDU_SN transmission for connection with ARQ disabled = once every 2_p MAC PDUs	
		Bit 11: DL sleep control extended subheader	
		Bit 12: Feedback request extended subheader	
		Bit 13: MIMO mode feedback extended subheader	
		Bit 14: UL Tx power report extended subheader	
		Bit 15: Mini-feedback extended subheader	
		Bit 16: SN request extended subheader	
		Bit 17: LCID Extended Subheader	
		Bits 18–23: *Reserved*	
		Bits 17–23: *Reserved*	

A bit value of 0 indicates "not supported" while 1 indicates "supported".

[Note to editor: modify subsection 11.13.37 as follows]

11.13.37 MBS contents IDs

 MBS contents IDs values shall be composed of 2 byte-long MBS Contents IDs to distinguish the logical MBS connection for each MBS contents. MBS Contents IDs is vendor-specific and dependent on application-level implementation and is not specified in this standard.

A 1 byte-long Logical Channel ID, which pairs with Multicast CID in Extended MBS_DATA_IE, is allocated to each

2 byte-long MBS Contents IDs in order that it is included in MBS content IDs value. For example, Logical Channel ID 0 is allocated to MBS Contents ID(0), Logical Channel ID 1 is allocated to MBS Contents ID(1) and so on. Logical Channel ID is used for MS to discriminate the MBS message in MBS data burst.

Type	Length	Value	Scope
[145/146].43	*variable (2 × n)*	MBS Contents ID(0), MBS Contents ID(1), ... MBS Contents ID(n–1)	DSA-REQ, DSA-RSP, , DSC-REQ, DSC-RSP

[Note to editor: insert a new subsection 11.13.40 as follows]

11.13.40 MBS LCID Enabled field

The MBS LCID Enabled field indicates whether LCID is supported for the connection. A value of 0 indicates that LCID is not enabled. A value of 1 indicates that LCID is enabled and usage of LCID ESH is allowed.

Type	Length	Value	Scope
[145/146].49	1	0: LCID support is disabled (default) 1: LCID support is enabled	DSA-REQ, DSA-RSP