Project	**IEEE 802.16 Broadband Wireless Access Working Group**
Title	**Refined proposal for 802.16.1 MAC**
Date Submitted	**1999-12-23**

Source	Carl Eklund Nokia Research Center P.O. Box 407, FIN-00045 Nokia Group, Finland	Voice: +358 40 749 9036 Fax: +358 9 4376 6851 E-mail: carl.eklund@nokia.com
	Juha Pihlaja Nokia Research Center P.O. Box 407, FIN-00045 Nokia Group, Finland	Voice: +358 9 4376 6579 Fax: +358 9 4376 6851 E-mail: juha.pihlaja@nokia.com
	Kari Rintanen Nokia Networks P.O. Box 372, FIN-00045 Nokia Group, Finland	Voice: +358 9 511 63735 Fax: +358 9 51163743 E-mail: kari.rintanen@nokia.com

Re:	802.16 Medium Access Control Task Group INVITATION TO CONTRIBUTE- Session #5.
Abstract	A MAC supporting efficient transport of synchronous as well as asynchronous packet based services.
Purpose	Proposal to serve as a baseline for 802.16.1 MAC standard
Notice	This document has been prepared to assist the IEEE 802.16. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor acknowledges and accepts that this contribution may be made public by 802.16.
IEEE Patent Policy	The contributor is familiar with the IEEE Patent Policy, which is set forth in the IEEE-SA Standards Board Bylaws <http://standards.ieee.org/guides/bylaws> and includes the statement: "IEEE standards may include the known use of patent(s), including patent applications, if there is technical justification in the opinion of the standards-developing committee and provided the IEEE receives assurance from the patent holder that it will license applicants under reasonable terms and conditions for the purpose of implementing the standard."

Proposal for the 802.16.1 MAC

Carl Eklund, Juha Pihlaja and Kari Rintanen

1.1.1 Introduction

This paper proposes and discusses the MAC functionality of 802.16.1.

2 Overview and reference model

This section describes reference model, interfaces to the PHY and the higher (convergence) layer. It outlines functions of the MAC layer.
The P-MP system consists of

one base station, which is the central unit
multiple subscriber terminals, which exchange data with base station.

The system supports the following duplexing methods:
Time Division Duplex (TDD)
Frequency Division Duplex
Half-duplex Frequency Division Duplex (H-FDD)

A fixed length frame structure is used. Within the frame up- and downstream capacity is dynamically allocated. In TDD mode the base station sends data in the beginning of the frame to the terminals in TDM fashion. During the rest of the frame the terminals send data one at a time (TDMA). In FDD mode data is transmitted in both directions simultaneously. In H-FDD mode the base station operates in full duplex mode (duplex filter is used). The H-FDD terminals operate in half duplex mode (duplex switch is used). Thus a subscriber station can send only when it does not receive.

The layer architecture of the system consists of Physical Layer (PHY), Medium Access Control layer (MAC), Convergence Layer (CL), and user layers. Examples of user layer protocols are Internet Protocol (IP), Point-to-Point Protocol (PPP), Frame Relay (FR), ATM, Ethernet/802.3, ISDN BR, ISDN Primary Rate, E1/T1, and MPEG-2 video. Figure 1 shows the layer architecture.

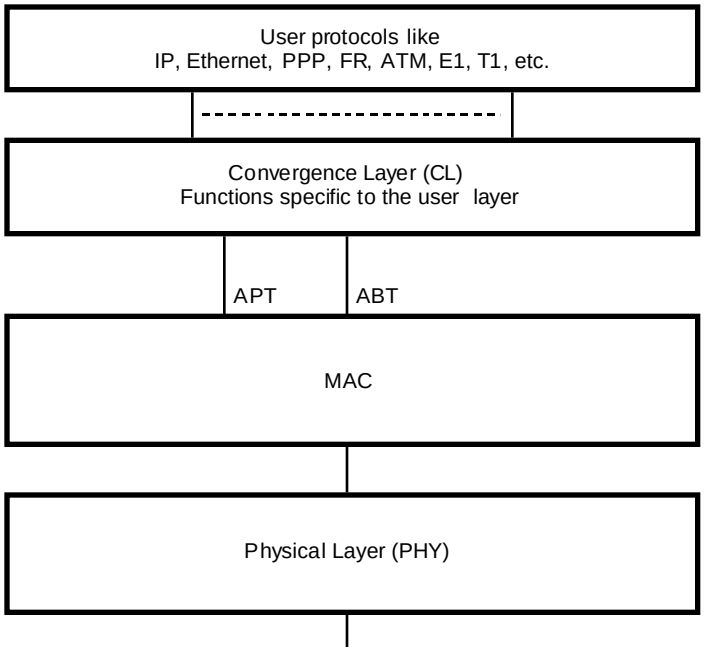

Figure 1 Layer architecture of the system

The Convergence Layer provides functions to map the user protocols to the services provided by the MAC layer. The MAC layer services are

- Asynchronous Packet Transfer (APT)
- Asynchronous Byte Transfer (ABT)

MAC is based on connections between the base station and the subscriber terminals. A subscriber station could have one or more active connections to the base station. A connection is related to one of the MAC services and one of the user protocols. All of the MAC services are based on the transfer of variable length data units in the MAC layer.

An APT connection carries variable length packets. It provides a packet delineation mechanism.

An ABT connection carries a byte stream, which could be of constant or variable rate. The upper layer is supposed to have its own synchronization mechanism, e.g. flags and zero bit insertion like in Frame Relay.
Physical Layer performs forward error correction, modulation and RF channelization. Figure 2 shows the mapping of the most important functions to layers.

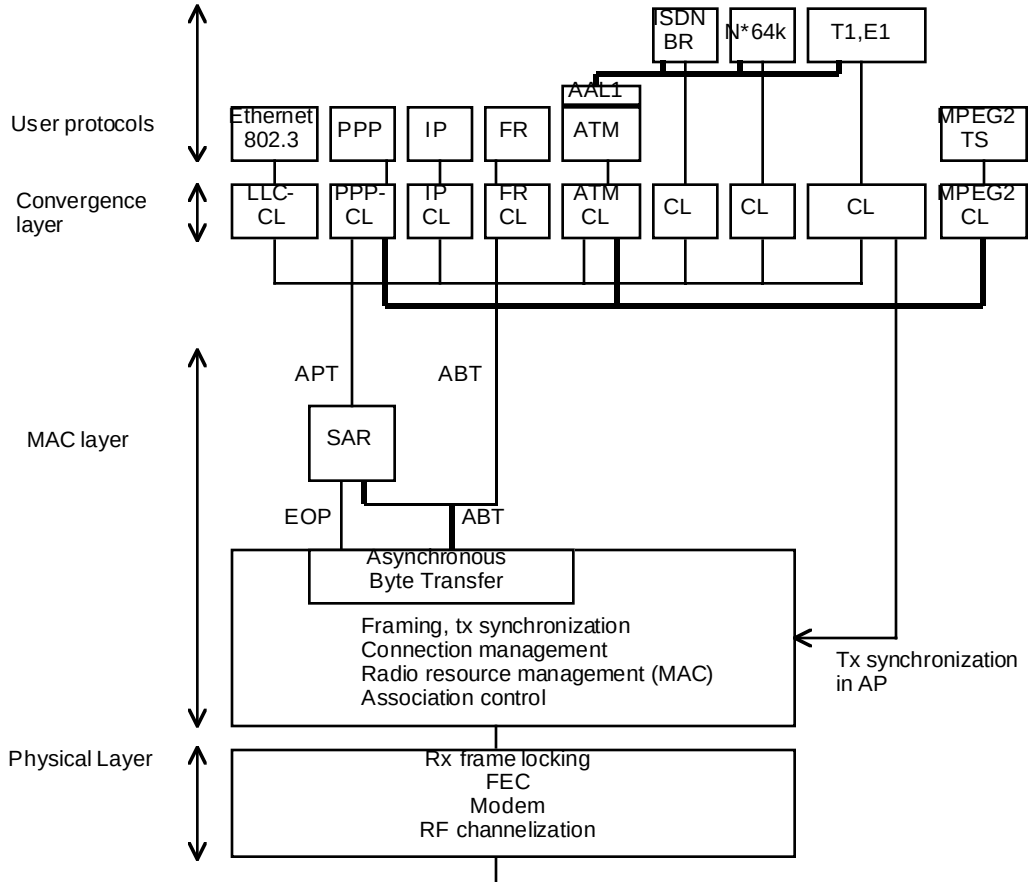

Figure 2 Layer architecture of the system with functions allocated to layers

The physical layer performs

- RF channelization
- Modem
- Forward error correction

- Rx frame locking.

It is expected that the physical layer needs the knowledge of frame synchronization and some fields of the frame.

The MAC layer performs

- Tx frame synchronization based on the clock from interfaces connected to the digital PSTN in BS, and is based on received frame in the subscriber terminal.
- Set up and closing of MAC connections
- Radio resource management consisting of management downlink TDM and uplink TDMA, and management of physical layer resources like RF channels and modulation.
- Association control manages associations between base station and subscriber terminals. It consists of registration of new terminals and closing of associations.
- Handling of the frame and offering the ABT, APT services described below to the convergence layer

ABT provides transmission of constant or variable rate byte stream. It does not afford for packet delineation or error detection.

The APT provides for delivery of packets of variable length and includes SAR functionality. The APT service uses the ABT service combined with an end of packet indication mechanism to deliver the packets.

The convergence layer performs functions needed to map user protocols to the selected MAC services. Figure 2 shows possible mappings. In cases where the higher level protocol does not provide for error detection this function can be implemented in the convergence layer. Functions such as header compression and empty cell discard are also performed at the convergence layer. The mapping functions should be based on requirements of the user protocols and ease of interfacing to the networks, that the base station and subscriber stations are connected to. Details are for further study.

3 Method of over-the-air transport

3.1 General

The MAC protocol supports TDD, FDD and, H-FDD access modes. On bands where only one frequency channel is available, TDD operating mode is used.

In H-FDD mode it is assumed, that base station is full duplex, i.e. the base station can transmit and receive at the same time, and the subscriber station is half-duplex, i.e. subscriber station cannot transmit and receive simultaneously. There is also a turnover time, during which a subscriber station switches from receiving to transmission and vice versa. In order to utilize the channel capacity fully terminals in a sector are divided into two groups. If smart antennas are used more than two groups may be needed.

3.2 Addressing

Each station has an unique EUI-64 identifier. This is hardwired in the station and is only used for registration purposes. During operation each subscriber terminal is assigned one or more 12-bit access terminal IDs (ATID). ATIDs 0x000 to 0x030 are used for special purposes or are reserved.

3.3 Connections

For each ATID there can be several connections. The connection is identified by a 8-bit connection identifier (CID). CIDs 0x00 to 0x03 are defined as follows.

CID	Purpose
0x00	EOL (end of list)
0x01	Upstream grant

0x02	Bandwidth request
0x03	MAC messages

3.4 Uplink channel acquisition

The proposed MAC protocol supports the following mechanisms for subscriber terminals to acquire the channel:

- The base station can poll terminals for data to be transmitted by granting the terminal an upstream timeslot.
- The subscriber terminal can set a poll-me bit, when sending data.
- The subscriber station can be allocated a fixed size time slot.
- The terminal can send a request for transmission time as a part of an upstream data transmission.
- The terminal can send a request for the channel in a Random Access Slot.

3.5 Frame structure

The MAC employs a constant length frame. Within a frame a broadcast segment, a number of down- and uplink segments and random access slots are allocated. The allocation is by means of absolute pointers referenced to the start of the frame. Pointers to the downlink uplink and the random access segments are transmitted in the broadcast message. The position of the uplink segments is given in the downlink segments or in the broadcast segment. In TDD mode pointers to the downlink segments are not used. In TDD mode downlink segments are organized in starting from lower order modulation first and highest order modulation last. Pointers are used to mark the instants of modulation changes.

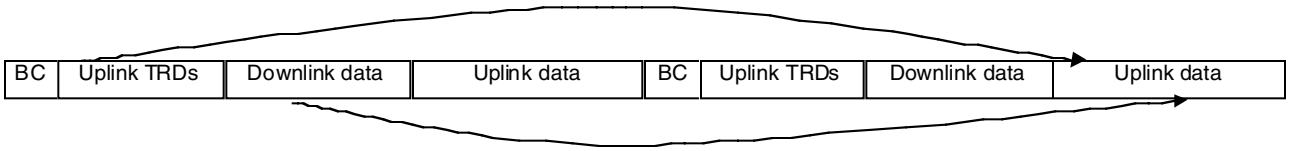

Figure 3 Pointer structure in TDD mode

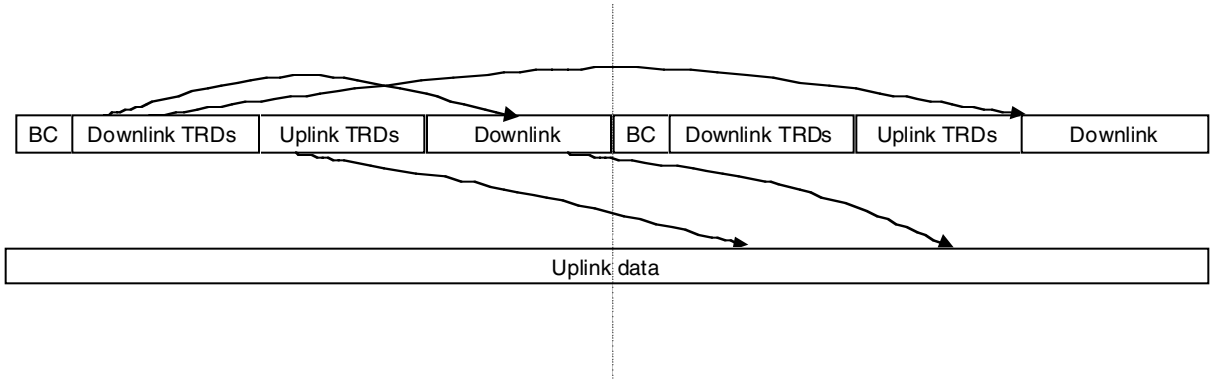

Figure 4 Pointers in H-FDD mode

3.5.1 Frame synchronization

The transmission frame has a length of one millisecond. The beginning of the frame is signalled by the physical layer. Each frame has a serial number expressed by 4 bits.

The distance between two Broadcasts s is thus always 1 ms. The frame structure is synchronized to the digital telephone network at base station. Synchronous equipment, like PABXs connected to terminals are synchronized to the PMP downlink frame rate.

3.5.2 Downlink message segments

3.5.2.1 Broadcast segment

At the beginning of each frame there is a broadcast segment. Only subscriber stations not scheduled to send during the broadcast listen to the it. The fact that the broadcast is of variabele length may lead to a subsrciber station being able to listen to only a part of the message. In this case the entire broadcast shall be disregarded.. The broadcast segment is always transmitted using the lowest level modulation

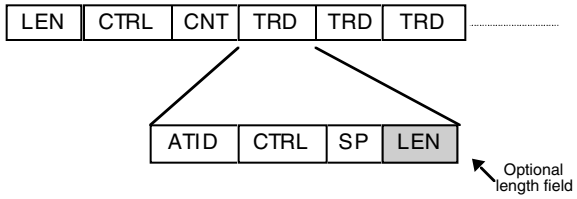

Figure 5 Broadcast segment

The broadcast segment consists of a header followed by transmission descriptor records. The header contains the length of the broadcast message, four control bits and a serial number expressed with four bits. Each transmission descriptor record contains the ATID, control bits, a start pointer (SP) and if indicated by the control bits a length field. The broadcast need not contain a descriptor for a given terminal. It may contain more than one descriptor for a given terminal.

Table 1 Broadcast control word

Field	Length	Description
B/D	1 bit	Broadcast /Downlink_segment
F/T	1 bit	FDD /TDD
CU	2 bits	Reserved

Table 2. The transmission descriptor. The shaded fields are contained in the control word.

Field	**Length**	**Purpose**
LEN	16 bits	Length of transmission in bytes
U/D	1 bit	Upstream if set/Downstream if clear
L	1 bit	Length included
MOD	2 bits	Modulation level
SP	16 bits	Start pointer
LEN	16 bits	Length of transmission in bytes

If an upstream descriptor (with the U/D bit set) has no length field the transmission is given by a default value. This is useful for polling purposes.

3.5.2.2 Start pointer reference points

A downlink SP (U/D clear) transmitted in frame number *n* uses the first symbol of the LEN field in the broadcast header of frame number *n* as reference point.

An uplink SP (U/D set) transmitted in frame number *n* uses the first symbol of the LEN field in the broadcast header of frame number *(n+1 MOD 16)* as reference point.

3.5.2.3 Random access slot descriptors

Random access slot descriptors are sent to random-access-group-ATIDs. The U/D bit must always be set. The Length field indicates the number of contiguous slots.

3.5.2.4 Ranging slot descriptors

Ranging slot descriptors are sent to ATID 0x000. The U/D bit is always set. No length field is present. A new terminal wanting to register itself to the network uses this descriptor.

3.5.2.5 Ranging response descriptors

Ranging response descriptors are sent to ATID 0x000. The U/D bit is always clear. No length field is included.

3.5.2.6 Random access acknowledgements

The random access acknowledgements acknowledge successful random access transmissions. The message is a transmission descriptor with the SP value of 0x0000.

3.5.2.7 Downlink segment

A downlink terminal segment contains information for an individual subscriber station or a multicast group. The structure is shown in figure 6. The whole downlink data segment is modulated using the modulation level indicated in the transmission descriptor. The segment consists of a header, a list of records containing the connection identifiers (CID) and corresponding end pointers (EP), convergence layer control flags and MAC payload units. The details are given in table 4. The EP points to the last byte of the MAC payload unit for the connection specified by the CID. The reference for the EP is the most significant byte of the LEN field. It should be noted that an error in one EP does not destroy the whole remainder of the segment, like chaining of pointers would do.
The broadcast header contains the ATID, the segment length and control bits. The encoding of the control bits is shown in table 3.

Table 3 Downlink control word

Field	Length	Description
B/D	1 bit	Broadcast /Downlink_segment
CU	1 bit	Reserved
PC	2 bits	Power Control 1

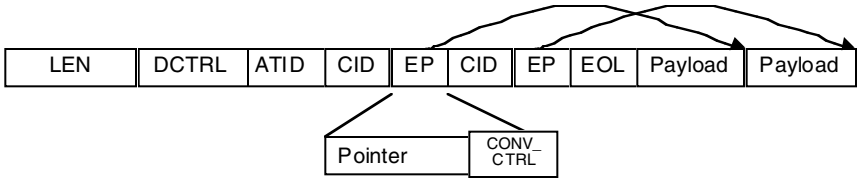

Figure 6 Downlink segment

Table 4 Downlink segment fields

Field	Size	Description
LEN	2 bytes	Length of the segment
CRTL	4 bits	Downlink control word
ATID	12 bits	Terminal ID
CID	1 byte	MAC connection ID
EP	12 bits	End pointer. Points to end of payload data
CL_ctrl	4 bits	Convergence layer specific ctrl bits
EOL	1 byte	End of list (CID=0x00)

3.5.2.8 Upstream Grant message

Upstream grants are given per ATID. The terminal is responsible for allocating capacity fairly to the active connections based on their QoS requirements. Grants are sent on the grant connection with CID=0x01. The payload of the grant message is the number of bytes that can be transmitted.

3.5.2.9 Modulation change descriptor

When operating in TDD mode the downlink transmission are sorted according to modulation level. The modulation change descriptors anounces the instant when the modulation level changes. The modulation change descriptor is adressed to ATID=0x001. The U/D bit is clear and the MOD bits gives the modulation after level starting at the symbol number given by the SP.

3.5.3 PHY related downlink aspects

Prior to each frame there is a preamble allowing a terminal to synchronize its receiver to the transmission.
Downlink transmissions are sent as a continuous stream of modulation symbols. However, the modulation type changes from one downlink segment to another. Thus a short preamble is present between downlink segments.
Error control is assumed to be taken care of by sufficient error control coding. No ARQ mechanism is envisaged.
The figure below shows how the variable length segments can be coded with a block code such as Reed-Solomon.
As the subscriber terminal has the best knowledge of the S/I at the terminal, it suggests which modulation to use for downlink transmissions.

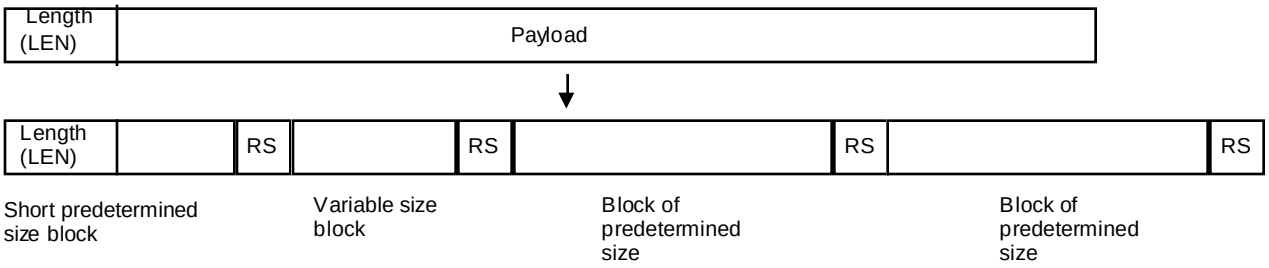

Figure 7 Coding of variable length segments with RS codes

3.5.4 Uplink segments

The terminals send data only when instructed to by a transmission descriptor. It specifies the time instant (symbol) when subscriber station burst must arrive at the base station and the amount of data the terminal can send.

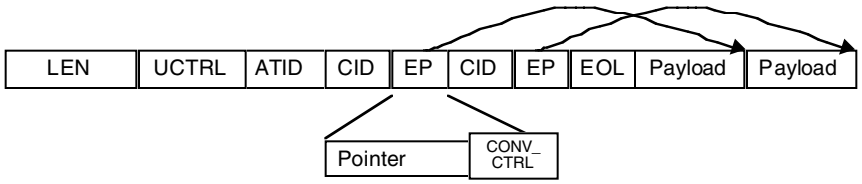

Figure 8 Uplink segment

3.5.4.1 Uplink segment

The structure is shown in figure 8. The whole downlink data segment is modulated using the modulation level indicated in the transmission descriptor. The segment consists of a header, a list of records containing the connection identifiers (CID) and corresponding end pointers (EP), convergence layer control flags and MAC payload units. The details are given in table .5 The EP points to the last byte of the MAC payload unit for the connection specified by the CID. The reference for the EP is the most significant byte of the LEN field. It should be noted that an error in one EP does not destroy the whole remainder of the segment, like chaining of pointers would do.
The broadcast header contains the ATID, the segment length and control bits. The encoding of the control bits is shown in table 3.

Table 5 Uplink segment

Field	Size	Description
LEN	2 bytes	Length of the segment
CRTL	4 bits	Uplink control word
ATID	12 bits	Terminal ID
CID	1 byte	MAC connection ID
EP	12 bits	End pointer. Points to end of payload data
CL_ctrl	4 bits	Convergence layer specific ctrl bits
EOL	1 byte	End of list (CID=0x00)

Table 6 Uplink control word

Name	Length	Description
MOD	2 bits	Modulation_suggestion
CU	1 bit	Reserved
PM	1 bit	Poll_me

Uplink terminal segment consists of a header, connection identifiers (CID) and corresponding end pointers (EP), and payload data. The header

3.5.4.2 Bandwidth requests

Bandwidth requests are sent on the bandwidth request connection with CID=0x02.The message contains a list of requests. Each request contains

- The CID of the connection for which the request is made
- The number of bytes requested.

3.5.5 PHY aspects of upstream transmissions

Burst modulation is used for upstream transmissions (from subscriber station to base station). Network Entry

3.5.6 First Time Entry

3.5.6.1 Scanning and Synchronization to Downstream

The subscriber station will passively scan the frequency band to find a central station. The allowed frequency bands and channel widths are pre-configured. After determining the correct channel it wills start scanning for the recurring broadcast preamble. Once the preamble has been found repeatedly the PHY layer signals synchronization to the MAC frame and passes the assumed broadcast frame to the MAC layer. The MAC inspects the BC/DL bit to verify, that the frame indeed is a broadcast.

3.5.6.2 Obtaining Upstream Parameters

The terminal once synchronized to the frame starts listening to the broadcasts. At the same time it will measure the received power. Once it hears the PHY parameter announcement it will calculate the required transmission power from it's own measurement and the information provided in the message.
The PHY parameter announcement includes:

- the transmission power level of the base station
- the power level on which the base station expects the transmissions to arrive at the base station
- the center frequecy(ies) of the upstream channel

3.5.6.3 Message Flows During Scanning and Upstream Parameter Acquisition

3.5.6.4 Ranging and Automatic Adjustments

Once the terminal has learned the upstream PHY parameters it scans the broadcast for a transmission descriptor indicating an initial ranging slot. It sends a ranging MAC message to the base station. The terminal assumes no propagation delay when sending the message. The message includes

- a timestamp which in this case is equal to the SP value given in the transmissin descriptor
- the EUI-64 identifier of the subscriber equipment

The base station measures the arrival time and power of the ranging message and calculates the needed time and power adjustments. The base station responds with a ranging response message containing the following information:

- the EUI-64 identifier of the subscriber equipment
- the ATID assigned to the subsrciber equipment
- the center frequency of the upstream channel to which the subscriber equipment is assigned
- the correction to the upstream tranmission power
- the amount of time advance for upstream transmissions

The ATID must be considered temporary as the legitimacy of the terminal in question has not yet been established.

3.5.6.5 Initial Connection Establishment

Connections with CID values 0x01 to 0x20 are considered always active and need not explicitly be established. Connections for data transfer are established using the normal connection establishment procedure after successful authorization.

3.5.7 Recurring Entry

Recurring entry procedure happens after power has been lost in the subscriber equipment. Or when terminals have explicitly been told to re-enter the network.

3.5.7.1 Scanning and Synchronization to Downstream

The subscriber station will passively scan the frequency band on which it was previously active. The terminal starts scanning for the recurring broadcast preamble. Once the preamble has been found repeatedly the PHY layer signals synchronization to the MAC frame and passes the assumed broadcast frame to the MAC layer. The MAC inspects the BC/DL bit to verify the that the frame indeed is a broadcast.

3.5.7.2 Obtain Upstream Parameters

The upstream parameters are obtained in the same manner as for initial network entry.

3.5.7.3 Message Flows During Scanning and Upstream Parameter Acquisition

3.5.7.4 Ranging and Automatic Adjustments

3.5.7.5 Initial Connection Establishment

3.5.8 Re-initialization

Re-initialization proceeds exactly as recurring network entry

3.6 Media Access Control Protocol Operation

3.6.1 Connection Establishment

Connections are established by either part sending a connection setup request. The other part answers with a connection setup response, which is acknowledged. The base station has the authority to decide the connection parameters.

3.6.2 Connection release

Either part sends a connection teardown request, which is acknowledged by a connection teardown response.

3.7 MAC Link Management

3.7.1 Power and Timing Management

Power management is done by two mechnisms:

- The base station regularly sends PHY parameter anouncements.
- Each downlink frame contains placeholders for power adjustment commands.

Timing management (after the initial ranging) is done by means of timing adjust messages. The basestation continuously monitors the reception to detect if the timing of a subscriber station is slipping. If this is the case the basestation asks the subscriber station to delay/advance its symbol clock.

3.7.2 Bandwidth Allocation Management

3.7.3 Channel Error Management

3.7.4 Link Management Messages

3.7.4.1 PHY parameter anouncement

The PHY parameter announcement includes:

- the transmission power level of the base station
- the power level on which the base station expects the transmissions to arrive at the base station
- the center frequecy(ies) of the upstream channel

3.7.4.2 Modulation index correction

Contains the correction for the modulation index (only relevant for TFM modulation)

3.7.4.3 Timing Adjustment

Gives the number of symbols with which to adjust the timing.

4 Convergence layers

4.1 ATM convergence layer

The ATM convergence layer header consists of a 4-bit convergence layer tag (CL_tag) and a 4-bit convergence layer flag (CL_flag). The CL_ctrl bits are also used to give the number of ATM in a MAC payload. ATM cells must not be fragmented.
Connections in ATM are identified by a <VPI,VCI> duple. When transporting ATM the <VPI ,VCI> is mapped to a <CID,CL> tag duple. The mapping is established at connection setup. The payload type (PT) and cell loss priority bit (CLP) are conveyed in lower portion of the CL_flag. The GFC and HEC fields of the header are not transported.

Up to 16 ATM cells can be transported in the same MAC payload. The CL_ctrl field gives the number of cells exceeding one.

The following rules apply:

1. Multiple ATM-connections referenced by the duple <VPI, VCI> can be multiplexed on one DLC-user connection.
2. Each ATM-connection that is multiplexed on one MAC-connection must be assigned a unique CL_Tag. The CL_Tag is conveyed as part of the MAC-payload.
3. The mapping for the duple <VPI, VCI> and the duple <CID, CL_Tag> must be configured upon connection set-up and should not change during the lifetime of an ATM-connection.
4. The mapping of the particular ATM-connection identifier <VPI, VCI> into <CID,CL_Tag> should be cleared once the connection is released. The freed duple <CID, CL_Tag> can be re-used for new connections.
5. Upon reception of a packet, the CID of the received DLC-SDU and the CL_Tag of the CPCS-PDU map into a unique combination of <VPI, VCI
6. In case the values of <VPI, VCI > or <DLCC_ID, CL_Tag> are not configured, an Error is reported to the MAC Management.
7. The GFC and HEC fields that are part of an ATM cell shall not be transmitted. It is assumed that the service shall compute the HEC for the received SDU, if necessary. Any information that conveyed in the HEC field is lost during the transmission.
8. The duple <VPI, VCI> at the receiver shall be the same as the <VPI, VCI> duple at the sender.

4.2 Generic packet convergence layer

Any kind of packet data can be transported over the generic packet convergence layer. The convergence layer provides for fragmentation of packets

4.2.1 Packet fragmentation

Bits 3:2 of the CL_ctrl field are used for indication of packet limits. A packet must start and end on a MAC payload boundary.

Table 7 Encoding of fragmentation bits

CL_ctrl 3:2	Interpretation
00	No packet limit
01	Beginning of packet
10	End of packet
11	Unfragmented

4.3 IPv4 convergence layer

The IPv4 adds IP header compression and DiffServ functionality. Details are to be determined later.

4.4 IPv6 convergence layer

The IPv4 adds IP header compression and DiffServ functionality. Details are to be determined later.

4.5 STM convergence layer

The most important STM (Synchronous Transfer Mode) transmission needs are:
- N*64 kbit/s for PBXs and other equipment
- 144 kbit/s ISDN basic rate
- 1.4 Mbit/s and 2 Mbit/s signals.

A stream of bytes can have STM channels position multiplexed in it. The stream of bytes can be carried by CID packet payload, or using ATM/AAL1.

Alternatively, each STM channel can be carried by a packet based channel, either CID payload or a short packet carried in the CID payload (for further study). Or ATM/AAL2 can be used to carry each channel on packet basis. Managing packet channels is supposed to be easier than managing of position multiplexing.

5 MAC messages

MAC messages are sent over the connection with CID=0x03. Each message has the general format shown in figure 9.

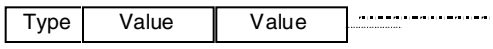

Figure 9 General MAC message fromat

Table 8 MAC message fields

Name	Length	Description
Type	1 byte	Gives the type of MAC message
Value	Variable	Parameter value

5.1 *Management Messages*

5.1.1 Upstream channel descriptor

This defines the characteristics of the upstream channel.

5.1.2 Upstream bandwidth allocation control

Parameters set include: Random access ACK timeout, Random Access Bakeoff window.

5.1.3 Ranging request

This message is sent by a SS in a ranging slot at network entry or at Ranging requests can also be sent at regular intervals as instructed by the BS.

5.1.4 Ranging response

The message is sent by the BS in response of a ranging request or unsolicited. The ranging response message containing the following information:

- the EUI-64 identifier of the subscriber equipment
- the ATID assigned to the subscriber equipment
- the center frequency of the upstream channel to which the subscriber equipment is assigned
- the correction to the upstream tranmission power
- the amount of time advance for upstream transmissions
- The correction for the modulation index

5.1.5 Registration request

The registration request is sent by the SS to the BS after establishing connectivity. The request contains

- the EUI-64 identifier
- the RSA public key
- the X.509 certificate
- a list of supported cryptographic modes
- the primary security association ID

5.1.6 Registration response

This message is sent by the BS in response to a Registration Request. It contains

- a terminal master key
- a key lifetime
- a key sequence number
- a list of all security associations for which the terminal is entitled to get a key
- a HMAC message digest.

5.1.7 Registration acknowledgement

Acknowledges processing of the registration response. Must contain

- the serial number
- the condition code for the response
- a HMAC message digest

If condition codes indicate an error the acknowledgement must include the error codes.

5.1.8 Connection setup request

A request to open up a new connection between the BS and SS. Connection setup can be initiated by either the BS or the SS. The message contains

- a serial number,
- the connection ID

- connection QoS parameters
- a HMAC message digest

May contain

- packet classifier parameters
- payload header suppression parameters

5.1.9 Connection setup response

A response to the connection setup request. It contains

- the serial number of the corresponding request
- a condition code

It may contain

- connection QoS parameters
- packet classifier parameters
- payload header suppression parameters.
- a HMAC message digest.

If the condition code indicates an error the error codes must be included.

5.1.10 Connection setup acknowledgement

Acknowledges the successful establishment of connection or reports errors in the connection setup. It must contain

- the sertial number of the corresponding response
- a HMAC message digest

If errors occurred it must also contain the error codes

5.1.11 Connection tear-down request

A request to teardown a MAC connection. The message contains

- a serial number
- the connection ID of the connection to be torn down
- a HMAC message digest.

5.1.12 Connection tear-down response

The connection teardown response contains

- the serial number of the corresponding request
- a condition code.

6 Security

6.1 Authorization and key exchange

The registration and authentication procedures in the PMP radio system make use of public key cryptographic methods. Terminals keep in addition to a public key and EUI-64 identifier a X.509 certificate binding together the unique MAC address and the public key. The manufacturer issues the certificate. This assumes that the operator trusts the manufacturer and has obtained the manufacturers public key by secure means.

Upon power-on a terminal synchronizes to the transmission and determines a random access ranging time slot in which it can announce its presence. After a successful notification, time and power ranging is performed after which the base station assigns the terminal a temporary ATID and downloads the operational parameters to the terminal. Next the terminal sends an authorization request to the to the base station. The request contains the EUI-64 identifier, the RSA public key, the X.509 certificate, a list of supported cryptographic modes and the primary

security association ID. The AP validates with the help of the manufacturers public key the validity of the certificate and thus gets assurance of the terminal's identity. The base station also checks for the terminals network authorization. Assuming the terminal is authorized the base station assigns a permanent ATID and sends a message to the terminal containing a master key, a key lifetime, a key sequence number and a list of all security associations for which the terminal is entitled to get a key. The master key is encrypted using the RSA public key of the terminal.
After receiving the master key, the transmission key exchange begins. The terminal requests a transmission key for each security association. The key requests contain the EUI-64 identifier of the terminal, the security association ID and a HMAC SHA-1 keyed message digest authenticating the key request. The base station generates the transmission key and encrypts it using the public RSA key of the terminal. The key together with lifetime, key sequence number and the initialization vector is sent in a HMAC authenticated message to the terminal. Two simultaneous key-sets must be supported to provide for uninterrupted service.

6.2 Security associations

Security associations (SA) are records shared between the base station and the terminal, containing security information. Security associations are established between the base station and one or more terminals. There are three kinds SAs: provisioned SAs, permanent SAs and dynamic SAs. Each terminal establishes at least one unicast SA, the primary SA. All upstream data as well as most unicast data in the downstream direction is sent over the primary SA. The provisioned and dynamic SAs are utilized for downstream multicast transmissions. Each SA has its own set of transmission keys.

6.3 Encryption of data transmissions

The MAC payload is transmitted in encrypted form while headers are unencrypted. Block ciphers run in the cipher feedback mode are used for payload encryption. Cipher feedback mode provides self-synchronization and data can be transported in arbitrary size chunks without padding. The feedback size of the cipher is equal to the block size to minimize error propagation due to bit errors. For sufficient security a cipher with 128-bit key should be chosen. Twofish is a good candidate as it is free, efficient and secure. The final choice of algorithm is likely to be influenced by the outcome of the AES process (Twofish is a finalist).

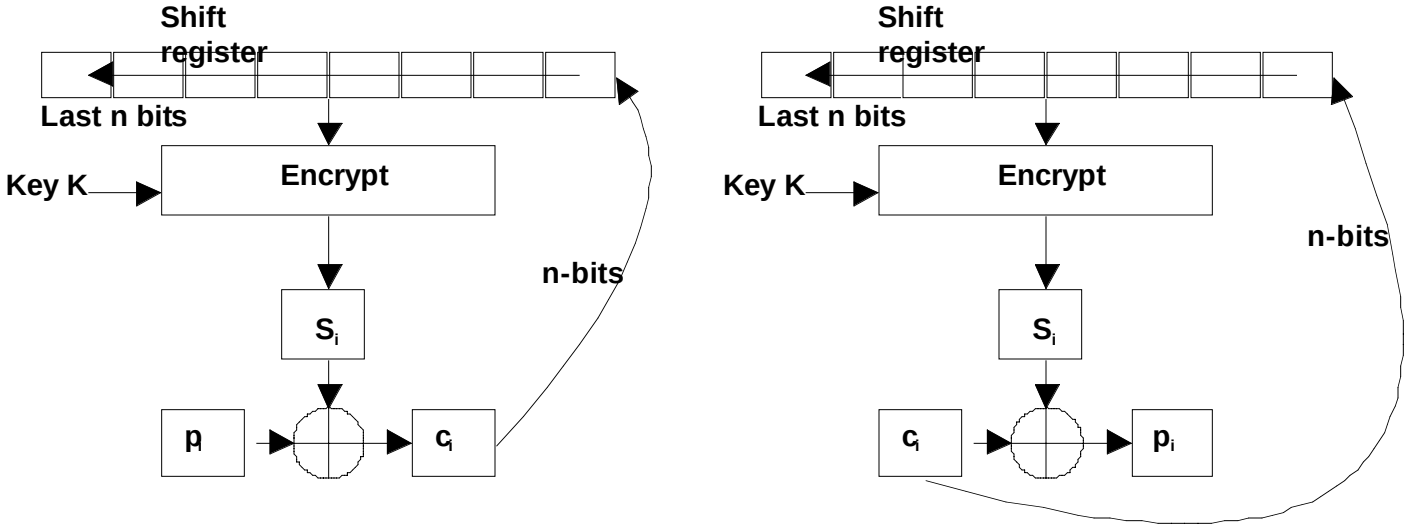

Figure 10 Cipher feedback mode

7 Relation to existing standards

. The proposal has also been submitted to ETSI/BRAN/Hiperaccess. The security scheme is influenced by DOCSIS BPI+.

8 Benefits of the proposed MAC

8.1 Segmentation to variable length transport units

ATM uses fixed length transport units with the payload of 48 bytes. If we adopted the same principle and would adapt variable length IP packets similarly to AAL5, then this would result in the need of padding of 24 bytes in average in the last transport unit of the packet. Assuming the current distribution of IP packet sizes, we estimated that padding would result in wasting of 5-10% in payload carrying capacity. In the future the wasted capacity may be even greater, if the volume of voice over IP traffic with its short packets will become significant.
Instead, Nokia proposes that a variable length transport unit will be used. This will eliminate the need of padding, and the operator has the possibility of 5-10% more revenue, which will significantly increase the profit margin of the operator. When ATM needs to be transported, then several ATM cells can be placed into the payload of the variable length transport unit.

8.2 Broadcast segment

The BCS gives general information of the sector to the terminals, and it also indicates each terminal, when to receive data, which allows the terminals to reduce power consumption during other times. Power consumption is important, when battery back up is needed e.g. due to lifeline telephone requirement in some countries.
The use of several broadcast segments allows the use of smart antennas.

8.3 Encryption scheme

By running the cipher in CFB mode no padding is added due to encryption as opposed to the commonly standardized CBC mode. The self-synchronizing feature of the cipher is also advantageous. Furthermore the scheme easily accommodates ciphers with different block lengths.

9 Drawbacks of the proposed MAC

Due to variable length transport unit, the requests and grants should be given on byte basis. This will result in 6 bit longer numbers in requested and granted amounts compared to system using fixed units of ATM type.

10 Statement of intellectual property rights

Nokia may have IPR in the standards under consideration. If Nokia has any applicable essential patents, it will comply with the IEEE IPR rules regarding disclosure and licensing.

11 Evaluation criteria for session #5

1. Meets system requirements:
   The proposed MAC protocol has been designed especially for BWA access systems meeting IEEE 802.16 functional requirements.

2. Mean access delay and variance:
   The MAC supports constant capacity allocation, polling and random access. In addition a short (1ms) frame is used. Together these allow for short access delays and low jitter for sensitive traffic. Bandwidth requests can also be piggybacked on data transmission.
   By utilizing either the constant allocation (for CBR traffic) or an appropriate polling interval the delay can be controlled.

3. Payload and bandwidth efficiency:
   The MAC has been designed with bandwidth efficiency in mind. The protocol can support several modulation levels within a single frame. Thus the capacity of the cell doesn't need to be determined by the terminal operating in the worst conditions. No padding is required when transporting variable length payloads. The overheads for some example payloads are:
   A single ATM cell 11 bytes. Note that the ATM cell header is suppressed, so the total number of bytes for the first ATM cell is 59. For each additional cell sent in the same burst the overhead grows by 4 bytes per cell.
   A single IP packet:10 bytes regardless of size, 3 bytes per each additional packet of any size
   A single IP over PPP packet:10 bytes. 3 bytes per each additional packet of any size.

4. Simplicity of implementation/low complexity:
The proposed MAC has been designed to use well-known technology. Thus implementation should be straightforward.

5. Scalability:
The MAC supports bandwidths for a single terminal from 0 bits/s to the full system capacity. A single sector can contain 2000 terminals each with 256 connections of any service mix.

6. Service support flexibility:
The MAC supports both real-time and non-real-time traffic. The MAC supports IP / IPover PPP, 802 LAN bridging and ATM with minimum overhead. Telephony, E1/T1 service can be provided by ATM/CES. The architecture is such that a new service can be added by designing a new service specific convergence layer.

7. Robustness:
The MAC can recover from unexpected shutdown. The sign on process is automatic and thus requires no intervention by the operator.
The MAC layer is designed to tolerate errors. The design is auto synchronizing (this also includes security features). Parts of the MAC frame can be lost without disrupting operation completely.

8. Security:
Several levels of security can be implemented. Strong authentication methods are used for terminal authorization. The MAC also supports privacy. Various encryption algorithms can be used. The protocol design is independent of cipher block size. Encryption introduces no additional overhead and error extension has been minimized.

9. Maturity:
The MAC protocol is in the process of being implemented.

10. Sign-on process:
The MAC protocol resolves the initial time ranging on single modulation symbol accuracy. Initial power ranging is accomplished by using open loop power control.
The sign on process is automatic with no user or operator intervention required.

11. Adequacy of management functions:
Timing is adjusted at registration time. The MAC provides a mechanism for adjusting timing during operation without performing the full ranging procedure.
Power is adjusted at registration time. A closed loop power control mechanism provides for continuos adjustment of the SS transmission power.
Frequency management TBD

12. Convergence with existing protocols:
The adaptation of the MAC to LAN and WAN protocols is by means of a protocol specific convergence layer. For packet or cell based protocols the adaptation is almost trivial. For TDM type of services existing adaptation layers can be utilized.

13. Ability to work with PHY layer variations, e.g. duplexing, constellation, etc.
The MAC supports efficiently both TDD and half duplex-FDD. The MAC provides support for several modulation levels within one frame both in the upstream and downstream directions.