Project	**IEEE 802.16 Broadband Wireless Access Working Group**
Title	**Nokia proposal for 802.16 MAC**
Date Submitted	**1999-10-29**

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 CALL FOR CONTRIBUTIONS- Session #4.
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 of Nokia for the 802.16 MAC

Carl Eklund, Juha Pihlaja and Kari Rintanen

Introduction

This paper proposes and discusses the MAC functionality of 802.16.

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 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.

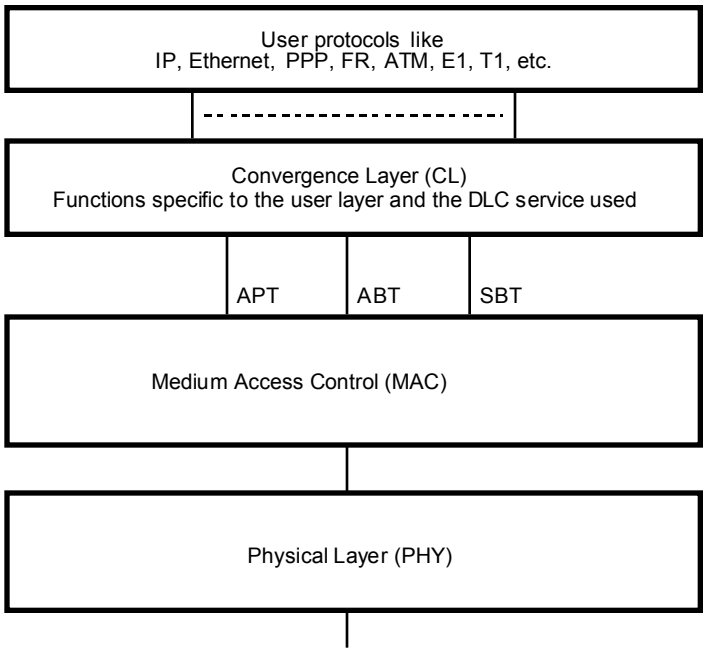

Figure 1 Layer architecture of the system

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)
- Synchronous Byte Transfer (SBT)

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.

SBT relies on the frame structure, which is synchronized to digital PSTN; i.e. the frame rate is traceable to the national reference frequency, the Primary Reference Source (PRS). Several synchronous channels can be position multiplexed into an SBT stream.

Physical Layer performs forward error correction, modulation and RF channelization. Figure 2 shows the mapping of the most important functions to layers.

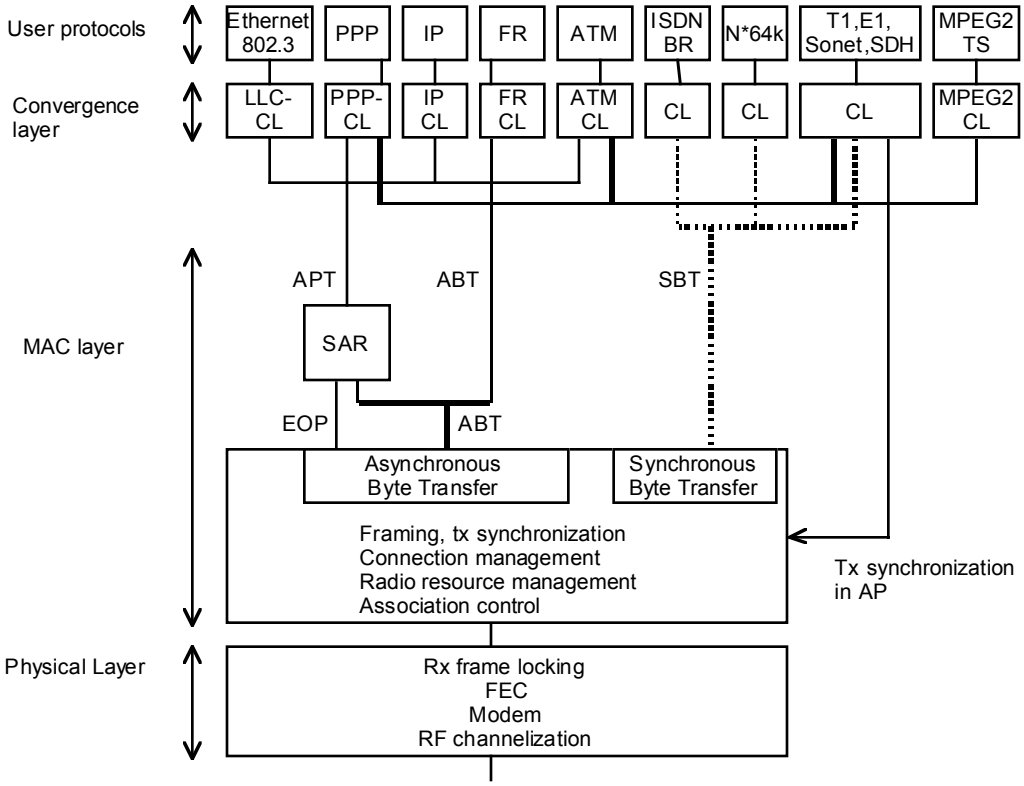

Figure 2 Layer architecture of the system with functions allocated to layers

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 AP, and is based on received frame in AT.
- 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 and SBR 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.

SBT is based on transferring a fixed amount of bytes once in a frame/ in every *n* frames between the base station and a subscriber station.

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.

Method of over-the-air transport

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.

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 station can be allocated a fixed 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.

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 and the random access segments are transmitted in the broadcast message. The position of the uplink segments is given in the downlink segments.

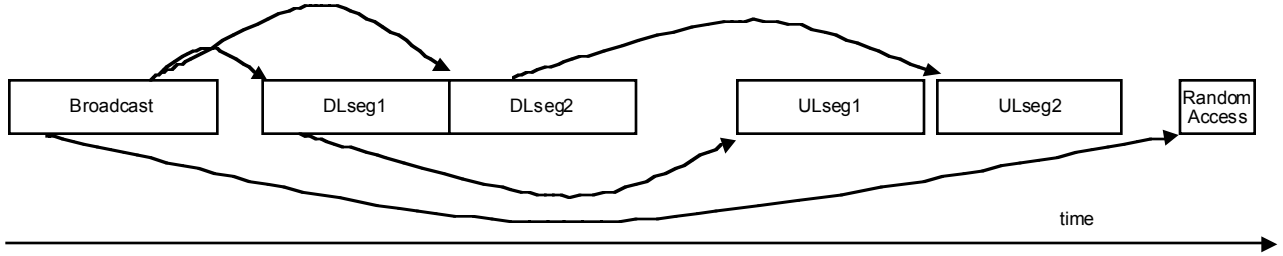

Figure 3 Pointer structure of MAC protocol

Frame synchronization and FAWs

The transmission frame has a length of one millisecond. A Frame Alignment Word (FAW) marks the beginning of the frame. In H-FDD operation where the terminals are divided into two sets there are two interleaved frames with 0.5ms offset. Thus there is an even FAW transmitted at the start of the frame and an odd FAW 0.5ms later. A terminal synchronizes itself to either type of FAW and disregards the other. During operation the base station can order the terminal to re-synchronize to the FAW of opposite parity.

The distance between two equal parity FAWs is thus always 1 ms. Synchronization with 8 kHz telephone

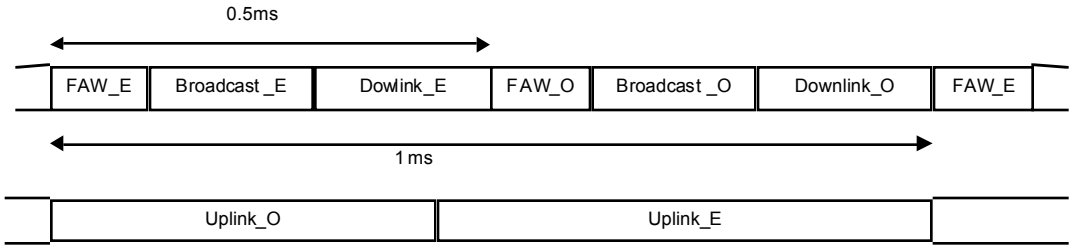

Figure 4 Operation in H-FDD mode with the terminals in two groups.

network is derived from the FAWs. PABXs connected to terminals are synchronized to the PMP frame rate.

Downlink segments

Broadcast segment

Following each FAW there is a broadcast segment. Only subscriber stations deriving their frame synchronization from the FAW must listen to this broadcast segment. The broadcast segment is always transmitted using the lowest level modulation.

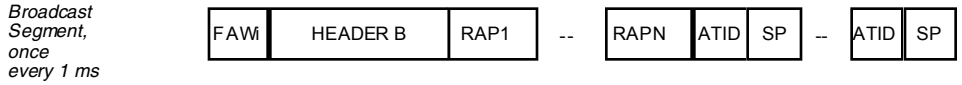

Figure 5 Broadcast segment.

FAWi Frame Alignment Word i (i = 1 or 2)
Header x A header consisting of information such as segment type, length of segment, control bytes, etc.
ATID The subscriber terminal identifier
SP Start Pointer. The first 2 MS bits indicate the modulation; the rest of the bits constitute the pointer to the downlink segment. The FAW is the reference for the pointers.
RAP Random access slot pointer

The broadcast segment consists of a header (Header B) followed by records specifying the location of random access and ranging slots (RAP). The remaining part of the broadcast gives the pointers to the downstream terminal segments (ATID+SP).

Random access acknowledgements

The random access acknowledgements acknowledge successful random access transmissions.

Downlink terminal segment

A Downlink terminal segment in general contains information for an individual subscriber station. The whole downlink data segment is modulated using the same modulation level indicated in the broadcast segment. The segment consists of Header D, Grant for the particular terminal to send uplink data, synchronous data (SBT data), a list of records containing the connection identifiers (CID) and corresponding end pointers (EP), and ABT data units. 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 MSb of the EP field can be used for end-of-packet indication.

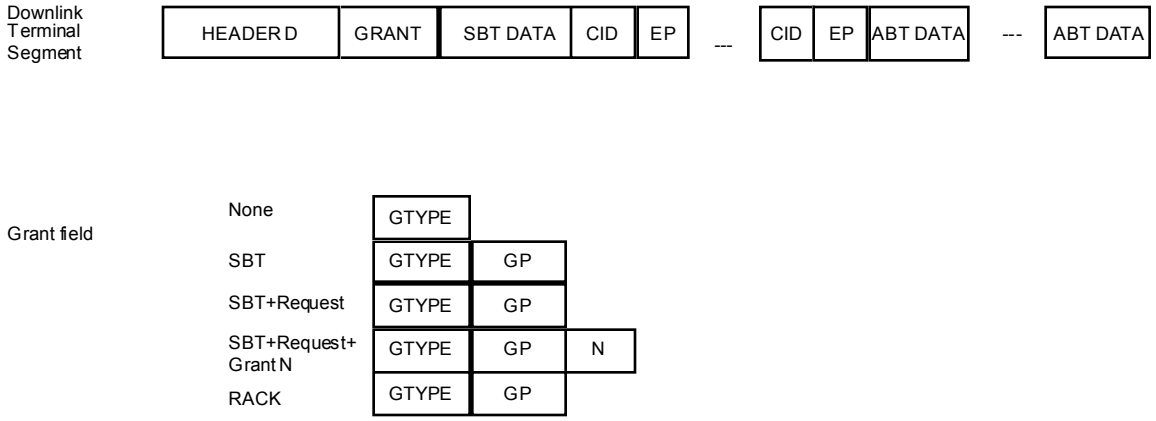

Figure 6 Downlink terminal segment and Grant field

SBT Synchronous Byte Transfer, data bytes from PABXs, ISDN terminals etc.
CID MAC Connection ID
EP End pointer (in bytes). Points to the last byte of the data for a connection.
ABT Asynchronous Byte Transfer, data bytes of asynchronous connections
GTYPE Grant type. The type of grant (permission to transmit) that is given to the terminal. The existence of the [GP] and [N] fields depends on the value of GTYPE.
GP Grant pointer. Granted slot pointer. The GP points to the time instant (measured in modulation symbols) in the upstream when the subscriber station may transmit. The pointer reference is the FAW symbol.
N The field N expresses the number of bytes that subscriber station can transmit including the necessary CIDs and EPs.

Grant field

Grants are given per terminal and not per connection. The terminal is responsible for allocating capacity fairly to the active connections. There are three types of grants:

- SBT (synchronous) grant. Time slot has been granted to a subscriber station for transmitting e.g. nx64 kb/s data. A subscriber station does not need to request for this grant. It is given automatically once in every frame or once in a number of frames. If the subscriber station has SBT data to send the subscriber station responds with uplink segment containing SBT data only. No requests and nor ATB data can be transmitted.
- REQ grant (polling). In addition of sending SBT data (if subscriber station has it), the subscriber station can request for an ABT/APT data transmission.
- NBYTES grant. In addition of sending SBT data and a REQ, a subscriber station can transmit N bytes of ABT/APT data (including headers). This grant is only given as a response to a REQ by a terminal.

PHY related downlink aspects

Prior to each FAW 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 needed 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.

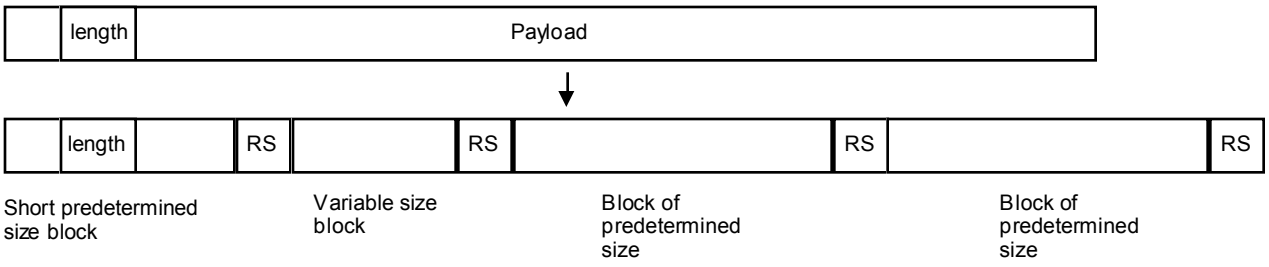

Figure 7 Coding of variable length segments with RS codes

Uplink segments

The terminals send data only when they are given a grant, i.e. a time slot to transmit. The grant specifies the time instant (symbol) when subscriber station burst must arrive at the base station and the amount of data the terminal can send.

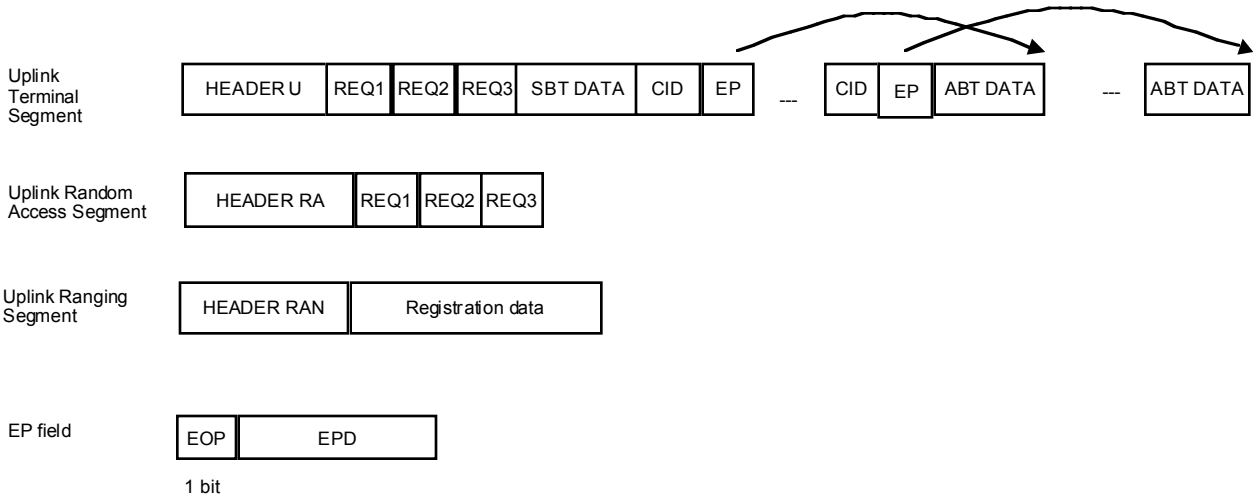

Figure 8 Uplink terminal segment

REQi Request to send for priority i, i = 1…3 (in number of bytes)
EOP End of packet indication

Uplink terminal segment

Uplink terminal segment consists of all or part of the following fields: Header U, three request fields for uplink data of three priorities, respectively, synchronous data (SBT data), connection identifiers (CID) and corresponding end pointers (EP), and data units (ABT data).

- Random access request slot. Any subscriber station can send a channel request message in this slot. The format of the message is similar to
- Ranging slot. This grant is given and is used primarily for registration of new ATs, which have not been assigned an ATID (format for further study).

PHY aspects of upstream transmissions

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

Packet delineation

The frame structure allows packet delineation based on the End of Packet indication (EOP). Alternatively, the user protocol may contain its own packet delineation mechanism, for example the flags and zero bit insertion in Frame Relay. Figure 4 illustrates these two methods.

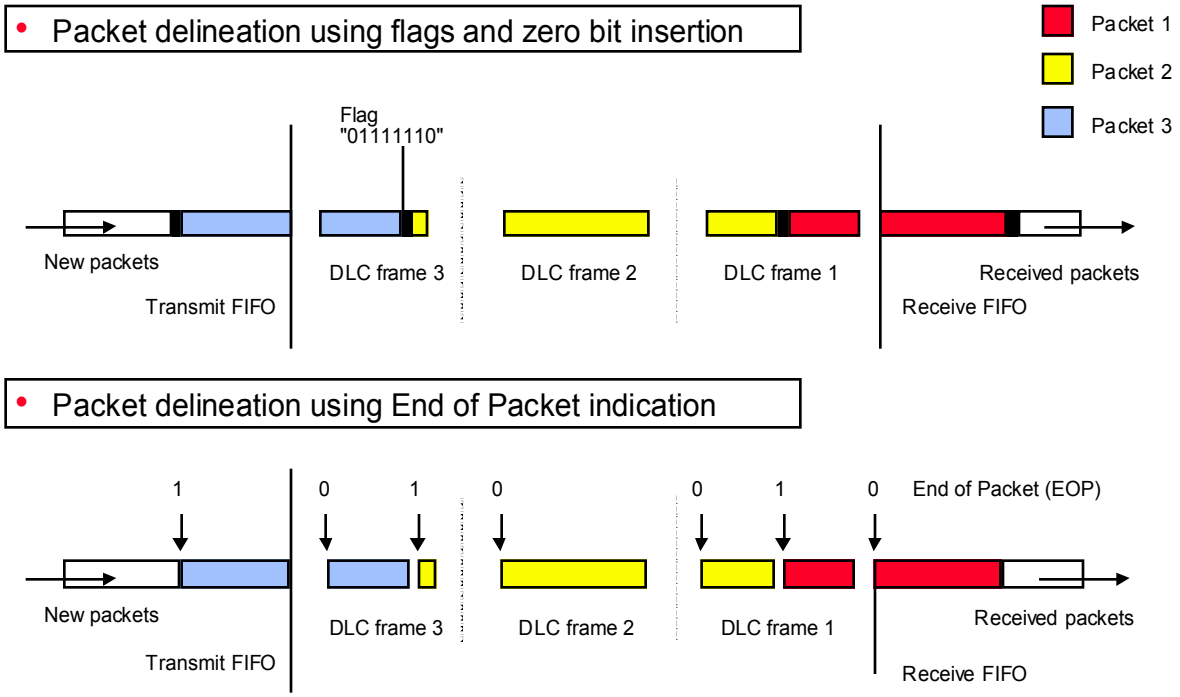

Figure 9. Packet delineation based on (1) flags and zero bit insertion and (2) End of Packet indication (EOP).

Security

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.

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.

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).

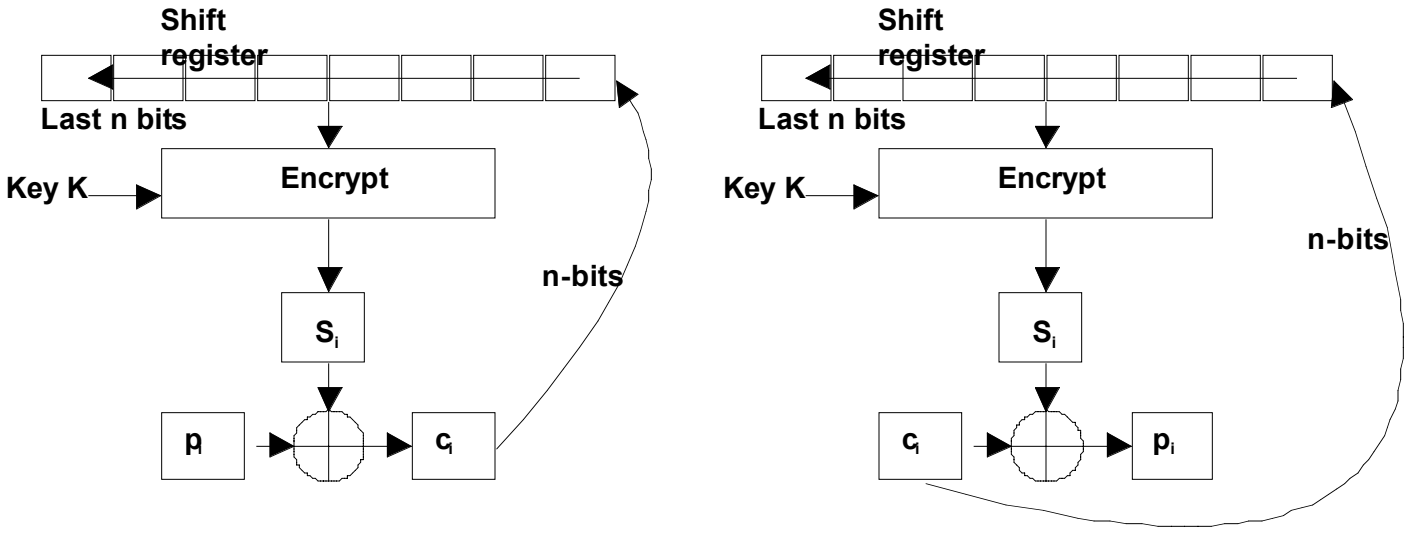

Figure 10 Cipher feedback mode

Relation to existing standards

The proposal has some similarities with ETSI/BRAN/Hiperlan2. However, significant changes have been made compared to it. The proposal has also been submitted to ETSI/BRAN/Hiperaccess. The security scheme is influenced by DOCSIS BPI+.

Benefits of the proposed MAC

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. An optimized convergence layer for ATM could be developed.

Requests and grants

To reduce the overhead associated with requests and grants, Nokia proposes that the requests will be made per priority, and not per MAC connection. The grant for a terminal to send will be made for all MAC connection of the terminal together, not per MAC connection. The terminal has to use some intelligence to divide the granted capacity to its MAC connections. These changes significantly reduce the number of needed requests and grants.

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.
We would like to minimize the size of BCS. Thus we would propose to give the uplink grants in the downlink terminal specific data segments.
The use of several broadcast segments allows the use of smart antennas.

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.

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.

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.

Conclusions

A MAC protocol suitable for 802.16.1 that can support a multitude of bearer services has been presented.