

The IEEE 802.16 Standard for Broadband Wireless Access

Carl Eklund

Nokia Research Center - P.O. Box 407, FIN-00045 Nokia Group, Finland
Tel. +358 7180 36566, Fax + 358 7180 36851, e-mail: carl.eklund@nokia.com

ABSTRACT:

The IEEE 802.16 standard for broadband wireless access was recently approved. It defines a physical layer for systems operating at frequency bands between 10 and 66 GHz, a medium access control (MAC) protocol and the convergence layers for carrying protocols such as IP, ATM and Ethernet. An IEEE 802.16 system consists of a base station and one or more subscriber stations. The duplexing scheme is either TDD or FDD. In the FDD case there is seamless support of half-duplex subscriber stations. The transmissions in the downlink direction are done in a TDM fashion, with the possibility of introducing re-synchronization preambles to improve the statistical multiplexing in a deployment with half-duplex FDD terminals. The uplink operates in a TDMA fashion. Adaptive modulation is employed both in the uplink and the downlink. The MAC protocol is connection oriented and is capable of providing QoS. The MAC protocol utilizes variable length PDUs and is thus optimized to carry connectionless traffic such as IP and Ethernet while not sacrificing efficiency when carrying ATM. This paper discusses the main features of the standard with emphasis on the MAC protocol.

INTRODUCTION

Standards for Broadband Wireless Access (BWA) are being developed within IEEE project 802, working group 16 [1], often referred to as 802.16. Several task groups (TGs) operate within the working group. The standards development for BWA point to multi-point systems above 10 GHz was done by TG1 and as a result produced the IEEE 802.16 standard[2]. TG3 develops amendments to 802.16 for operation in the licensed bands under 11 GHz including the unlicensed bands around 5.8 GHz. This amendment is known as IEEE 802.16a. TG2 is concerned with developing recommended practices for co-existence of BWA networks. The IEEE 802.16 standard is to be published during the first quarter of 2002 with the amendments following later in the year.

PROTOCOL ARCHITECTURE

The IEEE 802.16 protocol defines a *Physical Layer* (PHY), *Medium Access Control (MAC) Layer* and *Service Specific Convergence Sublayers* for transport of IP, Ethernet and ATM. The protocol stack is shown in Figure 1. An IEEE 802.16 system consists of a Base Station (BS) and one or more Subscriber Stations (SS). In the downlink direction (from the BS to SS) the system operate in a TDM fashion. In the uplink all SSs share the link capacity on a demand basis. Figure 2 shows a conceptual view of an IEEE 802.16 deployment.

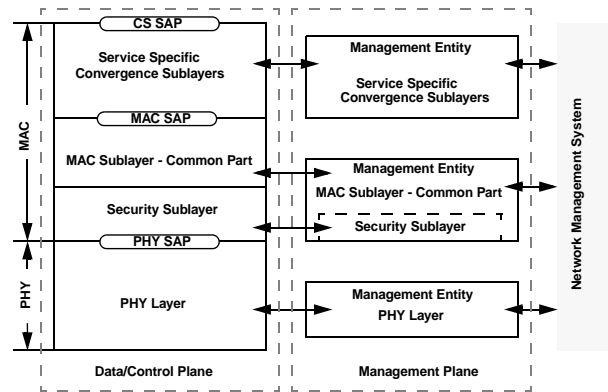


Figure 1—802.16 protocol layering, showing service access points.

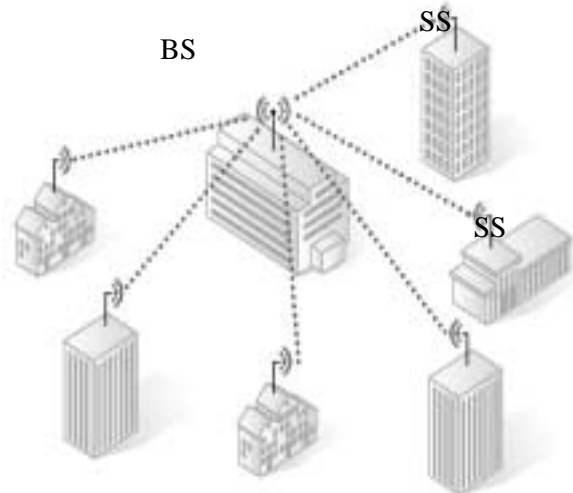


Figure 2—IEEE 802.16 Point-to-Multipoint radio

The MAC protocol is connection oriented. All data transmissions take place in the context of connections. Every service flow is mapped to a connection and the connection is associated with a level of QoS. Connections are unidirectional and are identified using a 16-bit CID. Connections in the downlink direction are either unicast or multicast while uplink connections are always unicast. During initialization of an SS, three particular connections are established in both directions. The *Basic Connection* is used for short time critical messages. The *Primary Management Connection* is used to exchange longer more delay tolerant messages. Finally the *Secondary Management Connection* is intended for higher layer management messages and SS configuration data. The messages on the Secondary Management Connection are carried in IP packets. Each SS comes with an unique 48-

bit MAC address. It merely serves as an equipment identifier. During initialization each SS is also assigned an IP address by means DHCP[3]. This allows the SS to be managed e.g., by means of SNMP[4]. It also allows the SS configuration to be downloaded via TFTP[5].

MAC PDU FORMATS

The MAC PDU format is shown in Figure 3. The MAC



Figure 3—MAC PDU Format

PDU length is variable. Two different MAC PDU headers are defined, the Generic MAC Header and the Bandwidth Request header. The headers are shown in Figure 4 and Figure 5. Subheaders for piggy-backing, fragmentation and packing purposes are also defined. The presence of the subheaders are indicated by the type field of the generic MAC PDU header. The subheaders are considered to be a part of the MAC PDU payload.

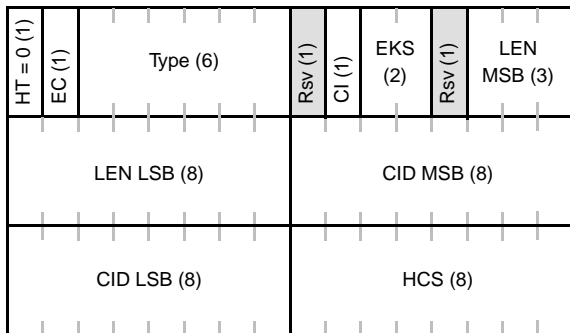


Figure 4—Generic MAC Header Format

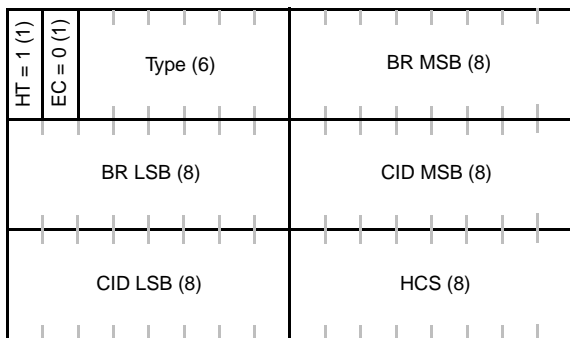


Figure 5—Bandwidth Request Header Format

FRAGMENTATION AND PACKING

Fragmentation is process by which a MAC SDU is split into fragments and transported in several MAC PDUs. The fragmentation subheader includes a control field, indicating whether the PDU contains the first, a intermediate fragment or the last fragment, and a fragment sequence number. The number of fragments is not limited to eight despite the 3-bit sequence number as it can roll

over. Also the number is not reset between MAC SDUs providing additional robustness to the re-assembly process. In fact exactly eight consecutive intermediate fragments have to be lost in order to produce an incorrectly reassembled MAC SDU on the receiver side.

Packing is the process by which several MAC SDUs or fragments thereof are transported in a single MAC PDU. Packing comes in two flavours. One for connections carrying variable length MAC SDUs and another for connections with fixed length MAC SDUs. The scheme for packing fixed length MAC SDUs relies on the fact that the length of each is known in advance. Therefore there is no need to add subheaders between the SDUs. Also fragmentation must be turned off in order for this scheme to work. Subheaders containing the SDU length together with the fragmentation control information are inserted between each SDU when packing variable length MAC SDUs into a MAC PDU. This allows simultaneous packing and fragmentation.

FRAME STRUCTURE

In IEEE 802.16 a framed PHY with a frame duration of 1 ms is employed. A frame time of 1 ms provides a good compromise between delay and statistical multiplexing. From a delay and jitter perspective a shorter frame is preferred while a longer frame provides for more statistical multiplexing.

Each frame starts with a preamble that allows synchronization to the downlink transmission. The preamble is followed by a control portion containing the Downlink Map (DL-MAP) and the Uplink Map (UL-MAP) messages. The DL-MAP message defines the downlink transmission by giving the downlink Interval Usage Codes (IUC) together with the starting instants for each interval. The UL-MAP gives the starting time measured at the BS of each transmission from an SS together with the uplink IUC for each burst. The UL-MAP entries pertain to the following frame.

The IUCs are indices to tables containing the PHY parameters, such as modulation scheme, FEC type and preamble for the downlink and uplink respectively. The parameters of the control portion are well known to all SSs. The mappings between the PHY parameters and the remaining IUCs are dynamically established by the Downlink Channel Descriptor (DCD) and Uplink Channel Descriptor (UCD) messages that are transmitted regularly in the control portion of the frame. The DCD and UCD messages also contain other carrier specific parameters.

The control portion of the downlink frame is followed downlink data transmitted in a TDM fashion. The intervals are in decreasing modulation robustness order. In the case of a FDD deployment the TDM portion of the downlink may be followed by 'TDMA bursts' with resynchronization preambles. Each burst may contain data to several terminals. The the need for resynchronization preambles arises from the fact that half-duplex FDD SSs lose their phase synchronization to the downlink carrier upon switching to transmit mode i.e., without the preambles they would be forced to receive all their downlink

data before transmitting. In a situation where half-duplex FDD SSs are the norm, prohibiting transmissions from occurring prior to reception would significantly reduce the statistical multiplexing gain. Instead the resynchronization preambles are introduced in the downlink and a 'receive whenever not transmitting' regime is mandated for the half-duplex terminals. Also the BS has to take into account the fact that simultaneous transmission and reception is impossible for these SSs. In a TDD system the downlink TDM portion is followed by a transition gap and the uplink TDMA portion. The position of the transition gap within the frame is configurable to better accommodate an asymmetric traffic pattern. The FDD and TDD downlink frames are shown in Figure 6 and Figure 7 respectively.

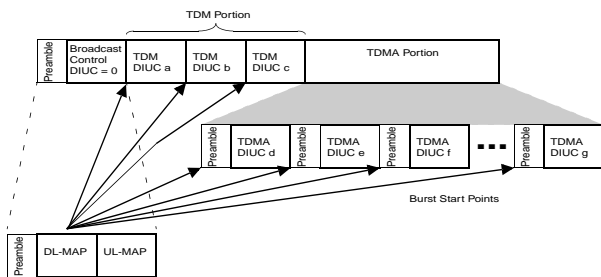


Figure 6—FDD Downlink Structure

In the uplink each burst starts with a preamble. Each burst

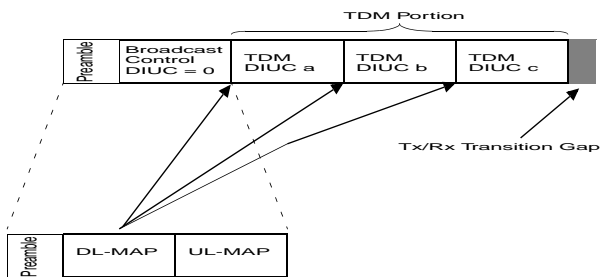


Figure 7—TDD Downlink Subframe

can contain several MAC PDUs. The bursts are separated from another by a short guard time allowing ramp up and ramp down of the transmitters.

SCHEDULING SERVICES

Four *scheduling services* are defined by the standard as mechanisms to meet the quality of service needs of the data flows carried over the airlink in the upstream direction. The scheduling service is associated to each connection at connection setup time. It determines the policy by which the connection (or the SS) is being polled and/or granted transmission opportunities.

To support services that generate fixed size data packets on a periodic basis, such as an E1/T1 carried over AAL1 or an ATM CBR service, the *Unsolicited Grant Service* (UGS) has been defined. Connections with UGS save uplink capacity by not issuing bandwidth requests for data on these connections. Instead the BS will grant a time slot for transmitting a prespecified amount of data at regular intervals.

Clock skew between the network clock and the air-interface clock there will occasionally cause an extra quantum of data to be queued at the terminal. To remove the backlog the SS can set a flag called the *Slip Indicator* to notify the BS of this condition. The BS will then issue an additional grant to remove the excess from the queue. Also to remove the need of additional polling of an SS with an UGS connection a flag called *Poll Me* can be set by the SS to signal that it has data to send on another connection and that it should be issued a poll.

To transport services that need a variable amount of capacity two polling services have been specified. The *Real-Time Polling Service* is intended for flows with real-time requirements while the *Non-Real-Time Polling Service* is for flows with more relaxed delay requirements. The polling services differ only in the frequency of issued polls and both guarantee access to the link also at times when there is congestion on the link. The polls are issued as normal grants in the UL-MAP.

Each MAC PDU transmitted on a connection with either polling service can contain a piggy-backed request for additional bandwidth for the connection.

The *Best Effort* scheduling service provides, as indicated by the name, no guarantees that a connection gets access to the link. The connections are relegated to using contention slots to send bandwidth requests. MAC PDUs on best effort connections may include a piggy backed request for more bandwidth.

BANDWIDTH ALLOCATION

Two methods of bandwidth allocation, *grant per connection* (GPC) mode and *grant per SS mod* (GPSS) are described in the MAC specification. For a system operating in GPC mode each the grants are addressed to a specific connection, requiring multiple entries in the UL-MAP message for a given SS if several of its connections is polled or granted transmission opportunities. This introduces a significant over head. No other connection may utilize this transmission opportunity if there is nothing to send on the connection that was granted the bandwidth. In a system running in GPSS mode the SS is given a single grant for all of its connections. The SS scheduler makes the decision how to allocate the granted capacity to its connections. In doing this the SS has to respect the QoS requirements of its own connections. In either case the bandwidth requests are always issued per connection. This allows the BS scheduler to maintain QoS and fairness between the SSs. Due to its considerable advantages the GPSS mode is mandated for IEEE 802.16 systems.

SECURITY FEATURES

The IEEE 802.16 protocol also specifies protocols for terminal authentication and privacy. The authentication uses X.509v3 certificates signed by the manufacturer with the RSA public key algorithm.[5,6,] Only SSs are authenticated as it is assumed that it is unlikely for BS to be cloned. Also operating an unauthorized BS without disrupting the legitimate service is considered impossible.

Only user data is protected in IEEE 802.16 networks. The control traffic is sent in the clear, but critical management messages are protected against tampering and spoofing by including a message digest. The HMAC protocol together with the SHA-1 secure hash algorithm is used to create the digest[7,8].

Each connection is mapped to a Security Association (SA), that specifies the encryption algorithm to be used, the data authentication algorithm to be used and the algorithm for exchanging the data encryption keys. Data encryption is performed with DES in the CBC mode[9,10]. The DES keys are exchanged using 3DES. Currently the individual MAC PDUs are not authenticated.

SERVICE SPECIFIC CONVERGENCE SUBLAYERS

Service specific convergence sublayers are defined for IP, Ethernet and ATM. For IP the functions include a packet classifier. The packets are classified to the MAC layer connections based on the source and destination addresses, the protocol and ToS/DSCP/Traffic Class fields in the IP header and TCP/UDP/SCTP port numbers.

Classification of plain IEEE 802.3 Ethernet and 802.1Q VLAN are also supported. In the case that IP is carried encapsulated in Ethernet the fields from the IP header mentioned above can be included in the filter. A simple mask based method to suppress the repetitive parts of the IP, Ethernet and 802.1Q headers is also specified.

ATM cells are mapped to MAC connections either based on the VPI (VP switched) or VCI (VC switched) field. The ATM cell header can optionally be suppressed.

CONCLUSIONS

The IEEE 802.16 standard for broadband wireless access is applicable to point-to-multipoint radio systems operating on frequency bands between 10 and 66 GHz. The standard defines a physical layer and a medium access control protocol. In addition convergence layers for transporting IP, Ethernet and ATM have been defined. The protocol is optimized for transport of network protocols with variable sized packets without sacrificing performance when transporting protocols such as ATM.

REFERENCES

- [1] <http://grouper.ieee.org/groups/802/16/>
- [2] IEEE Draft Standard 802.16/D4-2001 - "Local and Metropolitan Area Networks-Part 16: Standard Air Interface for Fixed Broadband Wireless Access"
- [3] Droms, R., "Dynamic Host Configuration Protocol," IETF RFC-2131, March, 1997.
- [4] Schoffstall, M., Fedor, M., Davin, J. and Case, J., "A Simple Network Management Protocol (SNMP)," IETF RFC-1157, May, 1990.
- [5] Sollins, K., "The TFTP Protocol", IETF RFC-1350, July 1992.
- [6] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," IETF RFC-2459, January 1999.
- [7] RSA Laboratories, "PKCS #1 v2.0: RSA Cryptography Standard," October 1, 1998.

[RFC-2104] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," IETF RFC-2104, February 1997.

[8] Federal Information Processing Standards Publication (FIPS PUB) 180-1, "Secure Hash Standard," April 1995.

[9] Federal Information Processing Standard Publications (FIPS PUB) 46-2, "Data Encryption Standard (DES)," December 30, 1993.

[10] Federal Information Processing Standards Publication (FIPS PUB) 81, "DES Modes of Operation," December 1980