

Project	<b>IEEE 802.16 Broadband Wireless Access Working Group</b>	
Title	<b>PHY and MAC considerations for an IEEE 802.16 Common Air Interface Standard</b>	
Date Submitted	<b>1999-10-29</b>	
Source	Robert Nii Wytec, Inc. 3385 Scott Blvd. Santa Clara, CA 95051	Voice: (408) 988-1112 ext. 114 Fax: (408) 988-1113 E-mail: bobn@wytecinc.com
Source	Margarete Ralston Wytec, Inc. 3385 Scott Blvd. Santa Clara, CA 95051	Voice: (408) 988-1112 ext. 117 Fax: (408) 988-1113 E-mail: margareter@wytecinc.com
Re:	802.16 PHY and MAC Task Groups CALL FOR CONTRIBUTIONS – Session #4, Sept. 22, 1999, Document reference “Air Interface Standard”, 8021699_06d0.doc.	
Abstract	This PHY and MAC proposal is based on the DAVIC Ver. 1.3 specifications for LMDS systems. This solution fulfills all of the requirements specified in the 802.16 Systems Requirements while implementing standards based protocols.	
Purpose	The authors contribute this proposal for inclusion in the 802.16 standard.	
Notice	This document has been prepared to provide PHY and MAC layer considerations for the IEEE 802.16 air interface standards. 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 < <a href="http://standards.ieee.org/guides/bylaws">http://standards.ieee.org/guides/bylaws</a> > 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.”	

# PHY and MAC considerations for an IEEE 802.16 Common Air Interface Standard

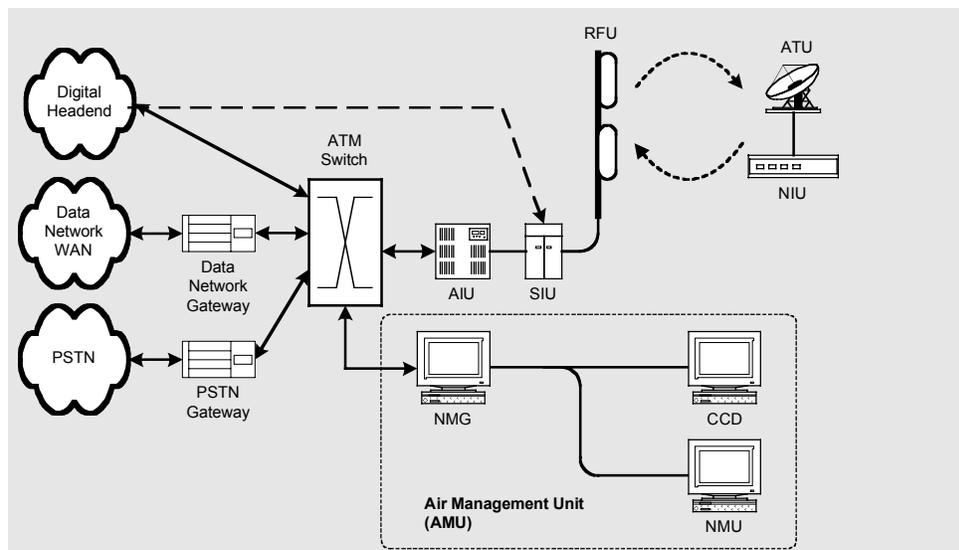
By Robert Nii and Margarete Ralston

Wytec, Inc.

## Introduction

The broadband wireless access equipment described in this discussion pertains to the millimeter wave bands. Base stations are deployed in a cellular architecture to provide local, wireless broadband services to fixed locations. Sectors in each cell increase the coverage area or adapt to geographical constraints such as either tall buildings or valleys. The cell radius typically ranges from 2 to 15 kilometers, depending on the hardware availability specified by the operator, the rainfall expected in the region, and the number of sectors in each cell.

A reference topology for this broadband wireless architecture is shown below. As subsequent paragraphs will show, this topology is intended to be congruent with the 802.16 System Requirements, the DAVIC standard and with other international standards as well. The switch and the gateway equipment are typically located at a Network Distribution Center, which may be a headend, central office, both, or neither. The acronyms are defined briefly below to set a context for the ingredients that are offered for inclusion in the IEEE 802.16.1 Air Interface Standard.



❖ **Figure 1: Network Topology**

In the diagram above, the base station consists of an Air Interface Unit, (AIU), a Radio Frequency Unit (RFU), and a Signal Interface Unit (SIU). The Air Interface Unit (AIU) is the control and processing part of the broadband wireless base station. It connects between the ATM switch and Signal Interface Unit (SIU). The IF signal is then routed to the SIU through an optical fiber link. The Signal Interface Unit (SIU) provides the optical to electrical conversion between the AIU or fiber from a Network Distribution Center (NDC) and the RFU. The Radio Frequency Unit (RFU) includes sector transmitters and receivers. The AIU is indoor equipment, while the SIU and RFU are outdoor equipment.

At the customer premises, there is an Air Transceiver Unit (ATU) for bi-directional transmission. This represents the outdoor unit referenced in the 802.16 System Requirements document. The Network Interface Unit (NIU) is the indoor equipment which interfaces to telephony, data, and video equipment at the customer premises. The Air Management Unit (AMU) consists of a customer configuration database (CCD), a network management unit (NMU), and a Network Management Gateway (NMG) that permits access to network management information over the Internet.

### ***Considerations in Developing a Common Air Interface***

In terms of broadband wireless access frequency planning, it is only the US LMDS A and B block licenses that do not have specific channel plans. For example, in the 39 Ghz band (38.6 to 40 Ghz), the FCC has created two blocks of frequencies that use 50 Mhz paired channels separated by 700 Mhz. In Japan, at 26 and 38 Ghz, ARIB (the FCC equivalent), has created two blocks of frequencies that use 60 Mhz paired channels separated by 1000 Mhz. Within these channels, it is possible to have multiple carriers, effectively creating smaller bandwidth subchannels. The ETSI BRAN standards also allow for a variety of channelization plans which effectively create subchannels. A channelization effort for the LMDS bands should be consistent with the other broadband wireless access allocations at different frequencies. Therefore, a minimum full channel size should be 50 Mhz, and multiple carriers can be used within this 50 Mhz channel to provide subchannels to meet the requirements of narrowband services.

This 50 Mhz minimum channel size:

- provides the most efficient usage of the available spectrum when compared to existing band plans,
- accommodates a full OC-1 bandwidth directly using a QPSK modulated carrier,
- accommodates an OC-3 bandwidth directly using 16 QAM modulation, and
- accommodates the bandwidths required by the 802.16 System Requirements.

In addition, the 802.16 standard should allow channel widths larger than 50 Mhz. The ETSI methodology of allowing channel widths that are multiples of the basic channel is recommended. Thus, it should be permissible to use 100 Mhz channels, 150 Mhz channels, etc. so that vendors can exploit higher speed components as they become available. This strategy will enable manufacturers to produce lower cost equipment by increasing volume of common parts used at different broadband wireless frequency bands.

Furthermore, it should not be a requirement to use the same size channel for upstream and downstream communication. This provides the maximum flexibility to accommodate TDD as well as FDD equipment for broadband wireless access.

The status data used by the AMU is multiplexed onto the IF at the base station. Other monitor data includes base plate and air temperature, humidity, all operating voltages, and LO lock indicator. Heaters are controlled by the status control function. Other status data available for each receiver are unit name, serial number, commission date, hardware version, current boot version, RFU type, and antenna polarization. These parameters are generic and could form a basis for a standard message set used for broadband wireless access network management.

At frequencies below 10 Ghz, frequency reuse may be used to reduce or eliminate adjacent sector interference, and spatial diversity is commonly used to reduce signal dropouts from interference patterns. Polarization diversity is not used at these frequencies because the effects from multipath change the received polarization to arbitrary orientations. At frequencies above 20 Ghz multipath reception is usually not significant, so the received polarization is not compromised, and polarization diversity becomes an excellent tool to reduce adjacent sector interference.

Repeaters are warranted when there is a desirable customer area that is completely blocked from the base station, but within the normal service area of a base station. The IEEE 802.16 air interface standard should include provisions for repeaters with sector antenna sizes as large as 90 degrees.

In the reference architecture, the AIU translates the signal from an ATM or IP based bitstream into a modulated signal on an IF carrier operating in the 950 Mhz to 2050 Mhz range used by cable TV systems and specified in the DAVIC standard. Using this range for IF carriers at the base station and customer site will minimize component costs and maximize interoperability. It is recommended that a Global Positioning System (GPS) receiver at the base station, or other timing reference be required to derive an accurate time and frequency standard for the 802.16 network.

For downstream communication, the reference architecture employs continuous QPSK modulation. In the upstream, burst QPSK is used. Higher order modulation schemes should be allowed, but not mandated in the initial version of the air interface standard. This will allow manufacturers the maximum flexibility in waiting until the cost of higher power millimeter wave devices makes it economical to overcome the required increase in signal-to-noise ratio necessary to provide the same network availability to all subscribers as currently is available with QPSK. Also, greater care in placing base station transmitters will be required to minimize mutual interference when using higher order modulation schemes.

Dynamic modulation allocation is a highly desirable feature, because it provides the potential for substantial improvement in bandwidth utilization, but it adds complexity and cost to an initial system deployment. Again, dynamic modulation allocations should be allowed, but not required in the IEEE 802.16.1 standard, provided all NIUs support QPSK.

Any air link will require error correction coding to provide low bit error rates in transmission. The approach in the reference architecture uses the forward error correction scheme presented in the DAVIC Version 1.3 standard. This standard permits a variety of convolutional encoding rates (for QPSK) as well as Reed-Solomon block error correction codes. Thus, it is recommended for adoption in an IEEE 802.16 network.

At the subscriber site, the Customer Premises Equipment (CPE) consists of two primary units, an outdoor Antenna Transceiver Unit (ATU), and an indoor Network Interface Unit (NIU), connected by a single 75  $\Omega$  coaxial cable. The use of a single cable to carry power and the RF instead of two cables was implemented to lower the cost of materials, lower the cost of installation, and improve the appearance of the installation cabling with no additional loss in signal fidelity. These characteristics are highly desirable from both a cost and implementation perspective. Since other manufacturers have chosen to put the RF and power on separate cables, the IEEE 802.16 air interface standard should be flexible enough to accommodate both implementations.

In the reference architecture, the Network Interface Units (NIUs) have standard telephony (T1/E1, T3/E3, POTS) and Ethernet interfaces. This architecture supports all bearer services described in the current 802.16 Systems Requirements documentation, although in some instances other customer premise connections can be handled by products that are external to the basic NIU.

For QoS based, connectionless bearer services, the MAC protocol allocates bursts of time slots on demand to bearer services that require changes in bandwidth allocation. This type of dynamic bandwidth allocation does not currently extend to connection oriented bearer services. Dynamic bandwidth allocation should be supported for all services in an 802.16 network. Increases in output power will also make the higher order modulation transmissions feasible or required in many situations, but the DAVIC 1.3 standard does not address either dynamic bandwidth or dynamic modulation allocation. For the sake of expedience in establishing and implementing an 802.16.1 air interface standard, it is recommended that the issue of full dynamic bandwidth allocation and dynamic modulation allocation be allowed, but unspecified since there are many algorithmic considerations to be worked out.

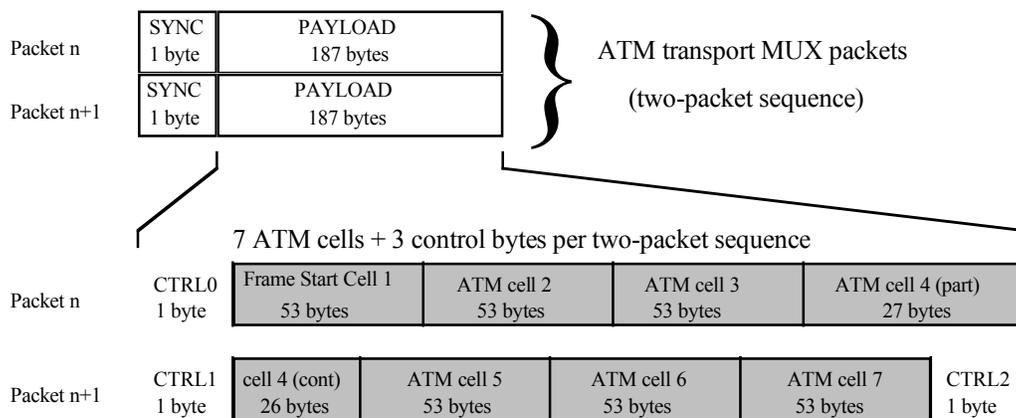
### ***MAC Protocol***

The reference architecture shown in Figure 1 includes a MAC layer implementation from the DAVIC Version 1.3 standard in the IEEE 802.16 air interface standard. The advantage and disadvantage to this implementation is that it uses the ATM transport stream for all services except video. This implementation possesses all of the attributes included in the 802.16 System Requirements. Despite all of its deficiencies, ATM still includes the protocols to manage available bandwidth in an 802.16 environment, and the DAVIC 1.3 standard provides an open standard path to an 802.16 implementation. The following discussion describes one effective and efficient implementation of the DAVIC 1.3 standard in an 802.16 network.

The MAC flow is bi-directional and is supported by modems at the base station and NIU. Messages may be sent either downstream to the NIU, or upstream to the base station. In the case of ATM transport, both the downstream and upstream frames are divided into time slots that encapsulate exactly one ATM cell. In the case of MPEG-2 transport, the downstream frame is divided into time slots that encapsulate one MPEG-2-TS packet, and the upstream frame is divided into time slots which encapsulate one ATM cell. The modulators at the base station transmit one or more downstream frequency channels.

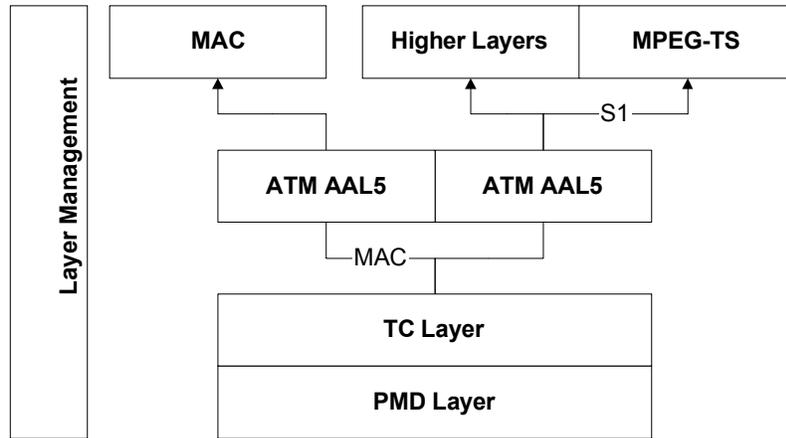
In the case of ATM transport, the MAC flow uses ATM layer encapsulation for all messages. In the case of MPEG-2-TS transport, the MAC flow uses MPEG-2-TS packet encapsulation for all messages.

The downstream MAC Control Message structure that is used when the downstream channel is carrying ATM cells is shown in Figure 2. With ATM transport, the base station transmits a Frame\_Start AAL5 PDU once per frame period. MAC messages can also be sent on individual MAC VCs to minimize processing by each NIU. Note that the first cell of the Frame\_Start PDU does not have to occur as the first cell of a two MUX packet sequence.



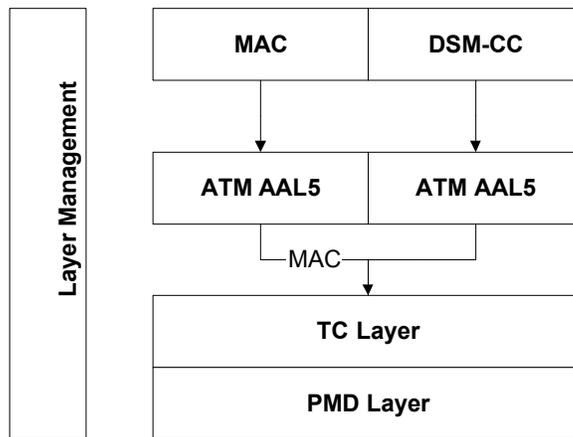
❖ **Figure 2 - Downstream MAC Control Message structure (ATM structure)**

The DAVIC 1.3 protocol stack for ATM transport based systems is shown in Figures 3 and 4. Downstream MAC messages are reassembled out of MPEG-2-TS packets and processed in the NIU. The MAC layer communicates through a Layer Management function to the Transmission Convergence layer to configure such items as the upstream reserved time slot allocation, etc. The MAC layer also communicates to the Physical Medium Dependent Layer to configure the upstream and downstream modulation , FEC parameters and apply timing, frequency, and power corrections for upstream transmissions.



Note: Higher Layers and MPEG-2-TS on ATM AAL5 are shown as an informative example.

❖ **Figure 3 - Downstream MAC Protocol Reference Model, ATM Transport**

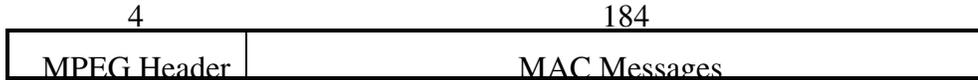


Note: DSM-CC on ATM AAL5 is shown as an informative example.

❖ **Figure 4 - Upstream MAC Protocol Reference Model, ATM Transport**

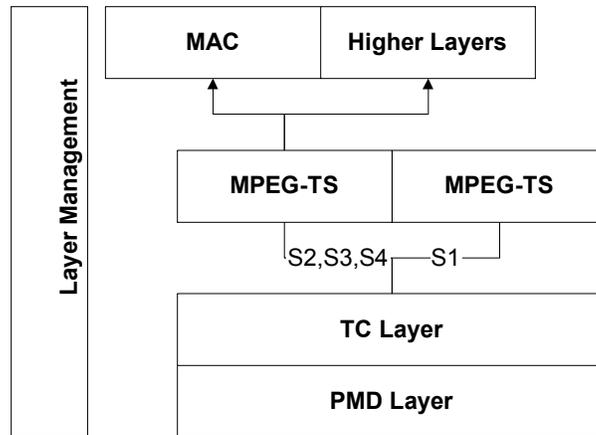
In the case of an MPEG-2-TS based system, the MAC messages are carried in a MAC PID. MAC messages may span more than one MPEG packet in which case an NIU or set top box processor must perform reassembly. Receipt of the first MAC MPEG packet shall be used to synchronize the upstream frame. Because MAC messages will be inserted into the MPEG-2-TS by the final MPEG multiplexer stage, it cannot be guaranteed that the interarrival time between the first MAC packets of each frame will be constant. As a result, each MAC packet include a time stamp that is inserted at the MAC Layer between the MPEG multiplexer and the modulator.

The MAC Control Message structure used in the DAVIC 1.3 downstream channel is shown in Figure 5. The MPEG Header is the 4 byte MPEG-2 Transport Stream Header as defined in ISO/IEC 13818-1 with a specific PID designated for MAC messages.



❖ **Figure 5 - MAC downstream message structure (MPEG-2-TS format)**

The protocol stack for MPEG-2-TS based systems is shown in Figure 6. Downstream MAC messages are reassembled out of MPEG-2-TS packets and processed in the NIU or a set top box for video services. The MAC layer also communicates to the Physical Medium Dependent Layer to configure the downstream modulation and FEC parameters.

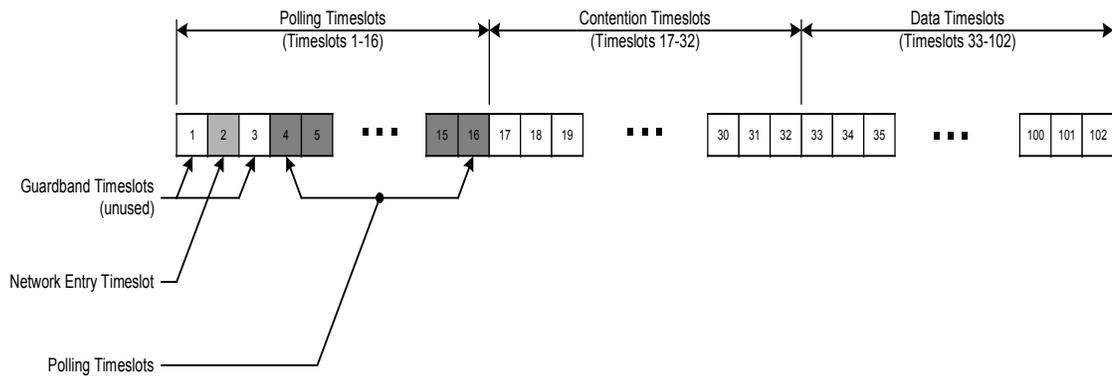


❖ **Figure 6 - Downstream MAC Protocol Reference Model, MPEG-2-TS Transport**

The downstream scheme is time division multiplex and the time slot types are divided into frame start slots and random access slots. The upstream scheme is time division multiple access and the time slot types are divided into polling response slots, contention slots, and reserved time slots. All MAC messages are encapsulated within ATM cells that use the UNI cell header format. The base station does not send more than 7 percent of the frame, which is about 50 cells per 6msec frame for a downstream bit rate of 51 Mbps. These cells, which contain MAC PDUs, include those broadcast via frame start to all NIUs and cells directed to a specific NIU. The poll time slots sent from the NIU only contain MAC messages. The contention time slots sent from the NIU may carry MAC messages or higher layer data. Reserved time slots sent from the NIU carry voice and data ATM cells as well as operations and maintenance (OAM) control message cells. The random access time slots downstream and the reserved time slots upstream transport higher layer data over an ATM virtual connection.

## Telephony Services

The reference architecture implementation uses the base station to provision the upstream bandwidth among the NIUs within a sector's range of coverage. The figure below illustrates one possible allocation of time slots in a single upstream frame. In this illustration, there are 102 timeslots allowing polling, contention, and data flow. Each timeslot has been defined to provide enough bandwidth to support a continuous 64-kbps data stream. The number of timeslots allocated to each type is one of the parameters that can be set on a dynamic basis by the base station upstream provisioning algorithm.



❖ **Figure 7: Timeslot Allocations**

Voice traffic represents a constant bit rate service supported by this network. Voice traffic is based upon 64-kbps (DS0) channels. However, an 802.16 network should be allowed to support voice services at data rates from 8 kbps to 64 kbps, depending on choice of implementation.

The voice traffic flow is described as follows. The signal from the microphone of user's handset is in analog form. The NIU converts the analog data to 8-bit Pulse Code Modulation (PCM) samples. The voice samples are then processed through a  $\mu$ -law or A-law compander. The companded output is then formatted onto an internal TDM bus that is routed within the NIU to the transmission hardware. The companded samples are packetized into an ATM AAL1 data payload according to the ATM Forum Circuit Emulation Services (CES) Structured Data Type (SDT) format.<sup>1</sup> The resulting upstream AAL1 cells are transmitted on an upstream reserved timeslot to the base station. The base station reformats the ATM header for the data cell and outputs it on the ATM link to the ATM switch. The ATM switch routes the cell to the PSTN Gateway.

Voice data from the PSTN network is input into the PSTN Gateway as companded, PCM samples. The PSTN Gateway packetizes the data into ATM Forum AAL1 CES SDT cells and outputs this cell to the ATM switch. The ATM switch routes the cell to the appropriate base station where it is processed and sent over the air to the appropriate NIU.

<sup>1</sup> ATM Forum document AF-VTOA-0078.

In this system, when the user picks up the telephone and dials a phone number, the NIU provides a locally generated dialtone and collects the DTMF digits as the user presses them. It is important that the user experiences the same feedback as using a wired phone line, and the dialtone generated at the NIU provides the immediacy of an active phone line without generating additional traffic over the air link. When the user enters a valid phone number, the NIU software generates a request for upstream traffic for the voice data. This signaling message is collected by the base station and processed in order to (1) allocate the upstream bandwidth necessary to allow the voice traffic to travel over the air link, and (2) generate the required signaling messages necessary to connect the call through the network. Unlike using VoIP, this process and its associated delay are virtually identical to the experience of a wired phone call. Once the signaling has connected the call through the network, the base station enables the data flow from the NIU through to the circuit-switched connection.

Upstream bandwidth is allocated on a frame-by-frame basis. If bandwidth is unavailable, then the request is placed in a queue and prioritized according to the user's service options with respect to other users. This should be an allowable implementation under IEEE 802.16

Desktop video conferencing can be accommodated using desktop video software and hardware products that use computers as a basis. Typically these products permit operation from 64 kbps to 384 kbps using H.323. Group video conferencing can be offered to customers using the E1 or T1 connections provided on the NIUs. This provides better quality than using ISDN or 3 ISDN BRI (384 kbps) connections. Since group video conferencing systems can run at up to E1 rates the IEEE 802.16 network should be capable of supporting implementations beside the H.323 systems. In an 802.16 network, the minimum channel size that should be assigned to a fixed wireless customer is one DS0, or a 64 kbps connection for videoconferencing traffic.

### ***Internet Protocol Service***

For QoS based, connectionless bearer services, the MAC protocol allocates bursts of time slots on demand to bearer services that require changes in bandwidth allocation. This network does not currently transport IP data packets directly over the air link. The NIU encapsulates the IP packet into a series of ATM cells in compliance with the industry standard RFC1483. Data is passed through the ATM switch and routed to the Data Network Gateway, where it is transformed back into an IP packet and offered to a router for processing. The IP service protocol also supports bridged LAN service (802.1G, 802.1Q). At the present time, ATM offers standards-based Quality of Service performance. Although there are several QoS implementations being considered for IP networks, there still is not a level of sophistication that is found in the ATM standards. However, the 802.16 standard should allow ATM and/or IP QoS provisions to be implemented.

In the reference architecture shown in Figure 1, the Data Network Gateway may also connect the base stations to legacy data networks such as those that use Frame Relay or X.25 protocols.

### ***Digital Audio/Video Multicast***

Included are recommended configurations for delivering digital video in this reference network. Digital broadcasting services supported include broadcast TV, pay-per-view, near video on demand, training video delivery, distance learning, high fidelity digital audio, and datacasting. This form of digital broadcast bypasses the MAC protocol layers at both the base station and the

NIU. This data flows downstream only and requires the addition of a standard DVB/MPEG2 set top box. This should be an allowable 802.16 implementation to minimize costs for competitive operators.

The digital video delivery system includes equipment for coding, multiplexing and modulation which conforms to the DVB/MPEG2 standard. This ensures a high level of compression efficiency and programming quality.

The TV signal source may be either analog or digital. If the TV signal is already digital, it must comply with the CCIR 601 standard. When an analog signal is received, an analog to digital converter creates a digital video signal with embedded audio.

The MPEG2 encoders compress the digital audio and video input for each channel. The encoder output is a multiplexed MPEG2 DVB compliant transport stream, which includes the compressed TV channel and auxiliary data.

A statistical multiplexer combines up to 12 MPEG2 Single Program transport streams at an average rate of 4 Mbps. Although the multiplexing equipment may be capable of handling 16 or 20 Single Program transport streams, 12 programs per stream allows studio quality video presentations. Statistical multiplexing capability allows video channels having different MPEG2 encoding rates to be included very efficiently since each channel is given just the bandwidth it requires.

If modulated at the NDC, a QPSK modulator puts one MPEG2 DVB compliant transport stream on a carrier. The resulting signal occupies up to 36 Mhz of bandwidth, just as it would on a DSS video delivery system. Another implementation allows the MPEG2 DVB compliant transport stream to be modulated at the base station when bi-directional services are offered. Both implementations should be included in the 802.16.1 common air interface standard.

When implemented with voice and data services, a telecom network adapter can be used to integrate the video services with the rest of the ATM architecture shown in Figure 1. The telecom network adapter consists of a transmitter and receiver to convey the MPEG-2 transport stream from the digital broadcast headend to the ATM switch. The telecom network adapter can also provide DS-3 or IP connections, so these should be included in an IEEE 802.16 network.

### ***Network Management***

All major elements of the network are accessible and configurable from an Air Management Unit (AMU). This includes provisioning rules for the algorithm allocating upstream channel timeslots, carrier frequency assignments for the downstream and upstream signals, and various other system-wide parameters. Included within this management unit is the ability to allocate and enforce service level agreements (SLAs) with subscribers by managing or restricting access to the air link time slots, thereby dynamically controlling the bandwidth available to the subscriber. A network management gateway provides a web-server, which allows the operator to access the AMU through any Internet browser. This provides the operator with the ability to monitor the network remotely at virtually any location in the world. This should be a requirement of the 802.16.1 standard.

In the reference network, the NIUs continually provide SNMP MIB data through unused bytes in the air link MAC messages. The data is transmitted periodically without requiring a request message from the NMU. This data is also sent without impacting the capacity of the air link. Several different data parameters from the NIU are typically updated depending upon the operator's requirements. This information typically updates every 1 to 10 seconds, depending upon the amount of data required.

To support G.826 performance monitoring, the NIU collects Errored Block (EB) information, tracks Severely Errored Seconds (SES) and Background Block Errors (BBE) over pre-defined intervals. The Severely Errored Second Ratio (SESR) and Background Block Error Ratio (BBER) are computed and periodically sent back to the base station as part of the typical network management traffic.

The failure of the AMU should not affect the normal operation of a broadband wireless access system in an IEEE 802.16 network. Furthermore, all managed elements should be capable of being configured and monitored through a local "craft" terminal. This should be a requirement in addition to allowing for standard SNMP, CMIP, or TMN compliant network management systems.

### ***Backhaul***

Several options exist for providing backhaul to and from each base station site in a broadband wireless network. In general, wireless and wireline backhaul should be supported in an IEEE 802.16 network. The choice of which backhaul configuration to deploy depends on the availability of an existing infrastructure, rights of way for fiber installation, and other factors. Each configuration results in different LMDS and edge network hardware options, which in turn affects the cost of the LMDS network.

### ***Transmit Power Control***

In the reference architecture shown in Figure 1, the output power from the base station transmitters is set to  $P_{1dB} - 15dB$  min to  $P_{1dB} - 1$  dB through a voltage ranging from 0 to 5 volts. Once set, the power is controlled via AGC over temperature and the input dynamic range to ensure the amplifiers remain within  $\pm 1$  dB from the initial set point. Base station transmitter power control should be required in an 802.16 network to minimize interference and maximize system capacity and reliability.

The power from each ATU is controlled by base station commands sent on the downstream channel. This level is set to by the base station to nominally place the received signal power at the input to the base station receiver to approximately 3 dB above the minimum SNR required for acceptable performance. The received power level is allowed to vary from received cell to received cell as long as the variation remains within a certain received power level window. In the reference architecture, this window is nominally set to  $\pm 3dB$ . Once the received power falls below or above this criteria, a MAC message is send to the transmitting NIU to cause the transmit power to be increased or decreased accordingly in 1 dB increments. This is recommended as a step size for an IEEE 802.16 network.

The received power level for every MAC message cell received by the base station is measured by the upstream power control algorithm to determine if a power correction is required. The base station performs the upstream power control calculation on each cell and determines in real time whether an adjustment is necessary. If there are no active connections for the NIU, a status message will be requested periodically (nominally every 2-10 seconds) to allow the base station to measure the received power of the ATU. It is recommended that these or similar intervals be considered in an IEEE 802.16 network.

### ***Authentication and Encryption***

Like a cellular system, the reference network identifies NIUs by their silicon serial number, which is embedded in the NIU hardware, and by a `niu_id`, which is assigned by the network. NIUs are assigned to a base station and a sector by the Customer Configuration Database (CCD). Unlike mobile systems, where all base stations of the system must communicate with a given mobile device, only one specific base station sector is able to communicate with any specific NIU. The network does not acknowledge NIUs which attempt to communicate with other sectors or base stations. Fraudulent NIUs that are exact replicas of the NIU must have the same serial number and can only be used within one base station sector to gain access to the network.

In the reference network, a fraudulent NIU attempting to use the network by mimicking the `niu_id` of a currently signed-on NIU must operate in the same sector as the signed-on NIU. If the fraudulent NIU attempts to access services by requesting upstream bandwidth from the base station, this will cause the base station to send MAC message traffic to both the “legal” and “fraudulent” NIUs simultaneously. This will result in collisions for any traffic on the upstream channels assigned by the base station to both the “legal” and the “fraudulent” NIU. This results in service being denied to both the “legal” and “fraudulent” NIU.

The discussion above indicates a minimum required level of security required for an IEEE 802.16 network. However, additional provisions should be included in the standard to accommodate an Authentication server in the core network that provides a key that can be used to initialize the NIU. The key would be generated from the NIU’s serial number and a pre-defined algorithm embedded in the NIU software. The algorithm should be updatable through the software download mechanism of the network. Authentication measures can also be applied to the `niu_id` by varying this parameter periodically and adding a mechanism to alter this parameter after the NIU has been signed on.

Encryption of the data traffic through a data port can be accommodated by software residing on the user’s computer. Likewise, encryption of the voice traffic can be accomplished via external devices. Simple encryption of all data is possible with the addition of hardware-based solutions at the base station and NIU. Instead of specifying a single encryption algorithm or requiring specific hardware and software implementations for an 802.16 network, a menu of acceptable options should be considered in the standard.