Project	**IEEE 802.16 Broadband Wireless Access Working Group**
Title	**DOCSIS 1.1 based MAC layer proposal for BWA**
Date Submitted	**1999-11-05**

Source		
	Chet Shirali Phasecom Inc. 20400 Stevens Creek Blvd, 8th floor Cupertino CA 95014	Voice: 408-777-7793 Fax: 408-777-7787 E-mail: cshirali@speed-demon.com
	Menashe Shahar Phasecom Ltd. 11 Kiriat Hamada Street Building 6, 1st Floor Har Hotzvim, Jerusalem, Israel	Voice: +972-2-5889-813 Fax: +972-25889-889 Email: mshahar@phasecom.co.il

Re:	This is the improvement on the original document submitted by Chet Shirali. The document number is IEEE 802.16mc-99/03 This is further submitted in response to call for contributions from the IEEE 802.16 chair on September 22, 1999 for submission of MAC proposals for BWA
Abstract	The DOCSIS 1.1 based MAC proposals with the recommended enhancements is submitted for consideration to be accepted as MAC standard for BWA
Purpose	This proposal should be accepted for accepted as a MAC standard for BWA
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."

DOCSIS 1.1 based MAC layer proposal for BWA

Menashe Shahar, Chet Shirali

Phasecom, Inc.

DOCSIS is an IP centric point to multipoint standard that was developed for broadband Internet access applications over Cable TV networks. As such, the DOCSIS standard is designed to support all existing as well as known future IP based services.

The DOCSIS standard was developed for a typical CATV network. It assumes that all the upstream and downstream channels are equally available to all the users all the time. This means that all the upstream and downstream channels that are used in a specific serving area support the performance requirements as per paragraph 2 of the DOCSIS RFI specifications (SP-RFIv1.1-I03-991105) for all the users within the serving area, all the time. As a result, the selection/assignment of a pair of upstream and downstream channels per user is relatively fixed in time and does not involve any RF performance optimization. It involves primarily traffic balancing and QoS considerations.

DOCSIS has been an evolving standard. The DOCSIS 1.1 Specification builds upon the DOCSIS 1.0 specification and adds new features that are necessary for applications that require special treatment from the network. DOCSIS 1.1 has additional features, which allows the operator to offer ATM like services. The DOCSIS 1.1 features are:

1. **Quality of service**

- Data and Voice/video applications
- Service flows
- Classifiers
- Scheduling types
- Dynamic service establishment

2. **Fragmentation**: Allows segmentation of large packets simplifying bandwidth allocation for CBR-type services
3. **Concatenation**: Allows bundling of multiple small packets to increase throughput
4. **Security Enhancements (Authentication):** Baseline Privacy plus, which builds on the Baseline Privacy available in DOCSIS 1.0. This enhanced feature provides authentication as well as in-line DES encryption/decryption
5. **Encryption support for Multicast Signaling** (IGMP- Internet Group Management Protocol)
6. **Payload Header Suppression:** Allows suppression of unnecessary Ethernet/IP header information for improved bandwidth utilization.

Thus the key additions are:

- Multiple Service Class support.
- Dynamic Service Management.
- Support for real-time services.
- Cryptographic authentication of the modem.

The Multiple Service Class support means that it is possible to define more than one kind of network access for a wireless Modem. One can browse with pre-defined network settings but at the same time can use the Modem to make phone calls. This was not possible in DOCSIS 1.0 specification since there was not enough detail to support Multiple Service Classes in a vendor independent way.

Dynamic Service Management provides a way to supply valuable services on-demand. For example when one has a VoIP telephone the bandwidth is reserved only when the call is to be placed.

The real-time support provides a consistent way to support time-critical applications. For example, in VoIP application it is possible to define how much delay and jitter is tolerated. Since the time-critical services are much more valuable than the usual ISP services, making sure that a modem is identified correctly become very important. DOCSIS 1.1 defines a cryptographic way to identify modems reliably.

It is possible to summarize the situations that require DOCSIS 1.1 support as:

Mixture of transaction processing or real-time traffics with low-priority web browsing and bulk file transfer on a user-by user level. For example, DOCSIS 1.1 would allow a user's business-related data to be set at a higher priority than casual web browsing. In general, situations like this require multiple Service IDs (SIDs) stored within each modem --- a defining characteristic of DOCSIS 1.1.

Integrated enterprise backbones, combining data traffic, teleconferencing, and telephony over a single channel. So-called network "policy management" decisions are enabled via the DOCSIS 1.1 specification.

Mixture of protocols that may require short transit times to avoid protocol timeouts and retransmissions with bulk traffic.

Sharing of channel bandwidth by different organizations that want to apportion costs through Service Level Agreements. Constant Bit Rate services are one example of this type of tiered bandwidth allocation application, and customers wishing to receive such a service would be required to have a DOCSIS 1.1 modem.

The table below gives ATM like feature offered by DOCSIS 1.1 specification:

	ATM	**DOCSIS 1.1**
1.	Virtual Circuit	Service ID
2.	Cell based	Fragmentation
3.	CBR Support	Unsolicited Grant
4.	Real time- VBR Support	Real time-polling
5.	Switched VC	Dynamic Service Establishment

DOCSIS 1.1 based wireless modem systems will provide users with high-speed access to packet-based data services. These services include Internet access, packet telephony, video conferencing and telecommuting (i.e., remote access to enterprise networks). Security threats associated with these services fall into two general categories: security of data transport services and security of CPE devices, which will use wireless modems to attach to public data networks.

The DOCSIS architecture includes security components that secure data transport services across the shared-medium network. DOCSIS data transport security provides modem users with data privacy and prevents unauthorized access to DOCSIS data transport services across the network.

Any CPE device attached to a public network will be subject to security threats. Given that the purpose of an access network is to provide subscribers with data access to public networks, the access network cannot take full responsibility for protecting subscriber systems from attacks originating from that public network. DOCSIS-based networks will provide, as do dedicated subscriber line systems, traffic filtering, which reduces threats from attacks that may target specific operating system features common to many of the attached CPE devices. (For example, filtering traffic on UDP/TCP ports 137, 138 and 139 to prevent unintentional Microsoft Windows SMB/NetBIOS file and print sharing.)

Regardless of whether a user employs cable, wireless, telephone, or DSL access networks, that user cannot rely solely on the access network to protect his or her system from attack. Subscribers to these services MUST, in all cases, take precautions to secure their systems prior to attaching them to a public network.

The situation is analogous to how an individual protects his or her home. While the individual trusts that the local police will do a good job protecting the neighborhood from burglary, the homeowner still locks the doors in the evenings or when absent from the home. The more populated the community, the greater the potential security risk, and thus the more caution demonstrated by the homeowner.

Attaching one's computer to the Internet is like living in a large urban area. There is much to gain in terms of the wealth of information, however accompanying that access are risks associated with having a direct ramp onto a global information highway.

Security of Data Transport Services

DOCSIS data transport security will provide modem users with data privacy across the network by encrypting traffic flows between the Wireless Modem (WM) and the Wireless Modem Termination System (WMTS) located in the base station of the wireless network.

In addition, DOCSIS security will provide operators with protection from theft of service. Protected DOCSIS MAC data transport services fall into three categories:

1. best effort, high-speed, IP data services;
2. premium quality-of-service (QoS) data services; and
3. IP multicast group services.

The DOCSIS system prevents unauthorized access to these data transport services by the WMTS enforcing encryption of the associated traffic flows across the wireless network, and employing an authenticated client/server key management protocol in which the WMTS (the server) controls distribution of keying material to client WMs.

DOCSIS data transport security has two protocol components:

- An encapsulation protocol for encrypting packet data across the network.
- A key management protocol for providing the secure distribution of keying material from the WMTS to client WMs.

The encapsulation protocol defines the:

- frame format for carrying encrypted packet data within DOCSIS MAC frames,
- set of supported data encryption and authentication algorithms, and
- Rules for applying the cryptographic algorithms to a DOCSIS MAC frame's packet data.

DOCSIS currently employs the Cipher Block Chaining (CBC) mode of the U.S. Data Encryption Standard (DES) to encrypt a DOCSIS MAC Frame's packet data. The protocols are extensible, can support multiple encryption algorithms and will, in all likelihood, be extended to support the new Advanced Encryption Standard (AES) once it is in place.

WMs use the DOCSIS key management protocol to obtain authorization and traffic encryption material from a WMTS, and to support periodic reauthorization and key refresh. The key management protocol uses X.509 digital certificates, RSA public key encryption and triple DES to secure key exchanges between the CM and the WMTS.

DOCSIS data transport security provides a level of data privacy across the shared-medium network equal to, or better than, that provided by dedicated-line network access services (e.g., telephone, ISDN or DSL). It should be noted, however, that these security services apply only to the access network. Once traffic makes its way from the access network onto the Internet backbone, it will be subject to privacy threats common to all traffic traveling across the Internet, regardless of how it got onto the Internet. If a subscriber's concerns over communications privacy go beyond the access network, he or she should be using higher-level security solutions: for example, VPN technology, to tunnel private data securely across public networks, or application-layer security (e.g., PGP or privacy-enhanced mail for email, SSL for Web-based transactions).

Lastly support for ATM cell transport is targeted to be available in DOCSIS. ATM cell PDU has been reserved for ATM cell transport. This is not covered in the current DOCSIS specifications. Each DOCSIS frame consists of DCOSIS header and an optional PDU. The PDU types are:

- Variable-length PDU
- ATM cell PDU (not defined in current specifications)
- Reserved PDU
- DOCSIS MAC-specific PDU

Modifications required for the wireless applications

The major assumptions made by DOCSIS with respect to the performance of the upstream and downstream channels are:

1. Downstream performance:

- Carrier to noise ratio in a downstream 6 MHz channel > 35dB
- Typical multipath (micro-reflections in the cable) < 1.5 Us
- Carrier frequency offset between head-end modulator and CPE demodulator - negligible
- RX power level at the CPE - relatively fixed (non fading)

2. Upstream performance:

- Carrier to noise in the upstream channel (including Ingress noise) > 25 dB.
- Typical multipath < 1.5 Us
- Carrier frequency offset – negligible
- RX power level at the CPE - relatively fixed (non fading)

The typical wireless network differs from the above in the following characteristics (this will be demonstrated by graphs during presentation).

1. Downstream performance:

- Limited Carrier to noise ratio –determined mainly by the TX level, antennas gain, distance, link budget and the receiver noise figure.
- Narrow band and burst interference from other transmitters (Harmonics and inter-modulation of PCS, AMPS, TV, Radar, etc.)
- Interference from Co-Channels, and reused frequencies
- Multipath, typically higher than 5uS (10uS for long distance). This is determined by the RX Antenna, and by the Symbol Rate.
- Higher Carrier frequency offset between head-end modulator and CPE demodulator.
- High dynamic range and Fading RX power level at the CPE.

2. Upstream performance:

- Limited carrier to noise ratio –Determined mainly by the CPE TX level, Antennas Gain and Link Budget.
- Narrow band and burst type interference from other transmitters (Harmonics and inter-modulation of PCS, AMPS, TV, Radar, etc.)
- Interference from Co-Channels, and reused frequencies
- Typical Multipath more then 5uS (10uS for long distance. Influenced by the RX Antenna, and by the Symbol Rate)
- Carrier frequency offset between head-end modulator and CPE demodulator up to 50 kHz.

- Fading RX power level at the base station.
- Required high dynamic range at the base station receiver, or at the CPE transmitter.

The different characteristics of the wireless network relative to the Cable TV network as outlined above, indicates that the DOCSIS standard as it is, will limit large scale broadband wireless deployment unless it is modified. The modifications are required at both the MAC and the PHY layers. The required modifications are further described below.

Modifications at the PHY Layer

The PHY scheme should be robust enough to enable operation over a wireless network. In particular, it needs to address the C/N and multipath requirements. Several non-DOCSIS PHY schemes have been proposed for wireless:

1. QPSK and 16QAM – This is the same as per DOCSIS for the upstream channel. In the downstream direction however, DOCSIS specifies 256QAM and 64QAM. As for multipath, DOCSIS specifies 5 upstream symbol rates schemes (160, 320, 640, 1,280 and 2,560 Msymbol/sec) which may be used to increase the robustness against multipath. As for the downstream, DOCSIS specifies a single downstream symbol rate of 5.056 Msymbol/sec for 64QAM. The addition of lower symbol rates on the downstream together with more powerful equalizer provides the required multipath robustness in the downstream as well.
2. OFDM could as well be considered to provide a robust PHY.

Modifications at the MAC Layer

1. The MAC scheme should support the optimization of upstream and downstream channel per user. It should allow for continuous monitoring of the individual CPE performance and the dynamic modification of the upstream and downstream operational parameters of the CPE based on its performance. The following describes schemes to perform this dynamic modification of upstream and downstream communication parameters relative to the DOCSIS MAC.

2. Dynamic modification of upstream operational parameters:

First, the DOCSIS initialization process allows the modem to acquire an upstream channel from a list of available multiple upstream channels using a two-stage procedure:

- A temporary phase in which the modem scans the Upstream Channel Descriptor (UCD) messages that are transmitted in the downstream channel. The modem employs the first usable channel for which a UCD message was received. This upstream channel is used by the modem to complete the registration process.
- A permanent upstream channel is then defined to the modem in the configuration file that is downloaded to the modem.

Following registration, the WMTS may direct the WM to change its upstream channel. This may be done for traffic balancing, noise avoidance or any other reason. The WMTS can use for this purpose the DOCSIS Upstream Channel Change (UCC) message procedure which allows the CM to switch to the new channel using one of the following procedures:

- Perform initial maintenance on the new channel
- Perform only station maintenance on new channel
- Use the new channel directly without performing initial or station maintenance

The third alternative will provide the fastest transition time but it requires the ranging information to be known in advance. In the case of Cable TV network, it can be assumed that the ranging parameters (time offset, TX power level and frequency offset) on the new upstream channel are quite similar to the previous channel but this is not likely to be the case in wireless. The MAC protocol is therefore required to support evaluation of the modem performance on other upstream channels in the background. This can be accomplished by adding a global periodic ranging procedure that will provide opportunities for the modem, to perform ranging on all the available channels. The ranging parameters of the modem relative to each of the upstream channels can then be stored in the modem or

in the WMTS. The WMTS will run an upstream performance table, which will be used by the WMTS to select the alternate channel for a modem if the performance on the current channel is not acceptable.

3. Dynamic modification of downstream operational parameters:

- DOCSIS supports a multiple downstream channel scheme with fixed characteristics per downstream channel (e.g., modulation scheme) that will allow each modem to select the best available downstream channel. This may lead to a relative high number of channels and the use of more bandwidth than is actually required.

- The number of channels can be reduced if the characteristics of the downstream channel will be allowed to change to provide the best fit per modem. This will turn the DOCSIS downstream channel into a bursty channel with burst profiles similar to those used for the upstream channels.