Project	IEEE 802.16 Broadband Wireless Access Working Group
Title	MAC document based on DOCSIS 1.1 (SP-RFv1.1-I02-990731)
Date Submitted	1999-09-10
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
Re:	stds-802-16: MAC Call for Contributions dated 6 Aug 1999 This is an initial document. This contains material for IP based MAC for the 802.16 Medium Access Control Task Group
Abstract	This document provides an overview of the Data Over Cable System Interface Specifications (DOCSIS). This protocol with wireless extensions will provide mechanisms, which will be useful in developing a data standard for the wireless.
Purpose	This document outlines mechanisms within existing protocols with extensions needed for wireless operations that will be useful for the MAC layer of the 802.16 protocol.
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 publicly available by 802.16.

DOCSIS 1.1 MAC protocol for 802.16

Chet Shirali

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 by itself will not work for LMDS/LMCS applications. Following wireless delta extensions will be needed:

- Support of QPSK and 16QAM on the downstream.
- Automatic downstream QPSK and 16QAM acquisition.
- Downstream IF of 44 MHz at the WMTS modulator.
- Upstream IF of 5 to 65 MHz edge frequency at the input to the burst receiver.
- Support of IF frequency offset on the upstream channel (i.e., the WMU transmits at Frequency 1 and the WMTS receives at Frequency 2 on the same microwave channel).
- Frequency tolerance and tracking of +/- 1 MHz on the downstream input to the modem.
- Modem upstream output of 5 to 65 MHz.

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.

CMs use the DOCSIS key management protocol to obtain authorization and traffic encryption material from a CMTS, 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 CMTS.

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