Broadband Wireless Internet Forum White Paper

Media Access Protocols: Circuit Switching to DOCSIS

Document Number WP-2_TG-1

Version 1.1

December 5, 2000

About the Broadband Wireless Internet Forum (BWIF)

BWIF, formed in July 2000, is an incorporated, non-profit association of industry-leading companies that will work together to ensure adoption of a single, unified broadband wireless access industry standard. Members of BWIF will drive product roadmaps that will lower product costs, simplify deployment of advanced services, and ensure the availability of interoperable standards-based solutions based on Vector Orthogonal Frequency Division Multiplexing (VOFDM) technology. BWIF members agree to cross-license to other BWIF members, the technologies required to implement the standard on a worldwide, royalty-free basis.

Table of Contents

List of Figures

ABSTRACT

In this white paper, we discuss why DOCSIS has been chosen as the Media Access Control (MAC) protocol of the Broadband Wireless Internet Forum specifications. We describe the evolution of MAC protocols from local area networks to broadband access networking and show why, among existing alternatives, DOCSIS is the best one.

1 Introduction

A MAC protocol allocates the use of a communications channel to independent competing users. Standards organizations have developed or adopted several MAC protocols for various purposes, e.g., IEEE 802.3, 802.11, 802.14, Cable Labs DOCSIS, etc. These different protocols address various types of network environments such as Local Area Networks (LANs), wireless LANs, Hybrid Fiber/Coax (HFC) networks, etc. Other MAC protocols have been designed for cellular mobile networks, satellite networks, etc. The performance of a MAC protocol depends on the network environment and the traffic characteristics. It is extremely important to understand that a MAC protocol that can work sufficiently well with one type of traffic source may perform poorly with another type of traffic source. The performance degradation can be severe. A particular case of very significant performance degradation occurs when circuit switching is used to multiplex bursty data sources. In the early days of networking, circuit switching versus packet switching was studied from a performance and a cost viewpoint (see, for example, [1, 2, 3]). A classical text on the subject states that the exact choice between circuit and packet switching is a difficult one and a satisfactory comprehensive treatment of the various tradeoffs does not exist [4, p. 296]. Nevertheless, a general rule of thumb was accepted: Circuit switching is suitable for networking with constant bit rate voice or video, but packet switching is preferred for bursty data sources such as computer or terminal data [4, p. 296]. The statement that the tradeoff between circuit and packet switching is not understood well may indeed have been true at the time [4] was written (1976) when circuit switching technology was much less expensive and more scalable than packet switching. However, today packet switching is much better developed and its performance and cost tradeoffs are very well understood. In fact, in the new networking paradigm, packet switching is the only multiplexing technique for all sources including voice, video, and data under both Internet Protocol (IP) and Asynchronous Transfer Mode (ATM) scenarios. We will address this issue in detail next.

1.1 Circuit Switching vs. Packet Switching

It is easy to quantify the throughput gain via packet switching for bursty data sources. We will do that by employing an example [5]. Refer to Figure 1. Let λ be the message arrival rate, or equivalently let $1/\lambda$ be the average interarrival time between messages in a session. Let X be the average transmission time of a message over a given link in the path. The ratio of X to $1/\lambda$ or λX is the fraction of time the link is busy. Note that $0 \leq \lambda X \leq 1$ and λX can be used as a figure of merit, representing the occupancy of the link.

Now let T be the allowable delay in transmitting the message from source to destination. Due to the presence of propagation delays, switching delays, queueing delays, etc, we have $X \leq T$ therefore $\lambda X << 1$ if $\lambda T << 1$. Reference [5] states that for many of the sessions carried by data networks, λT is on the order of 0.01. Thus, for such applications, packet switching offers a 100X advantage in throughput as compared to circuit switching. This number is representative of older networking applications, such as point-of-sale terminals.

By looking at typical Web use patterns, one can calculate what kinds of packet switching advantages are likely in today's Internet. A model commonly used in the design of the cable networks states that a typical Web user downloads a file of 50 kB every 15 s where 15 s is the "think time." Thus, for this application, we have $\lambda = 1/15\ s^{-1}$. On the other hand, various studies of computer response times conducted over the last three decades,

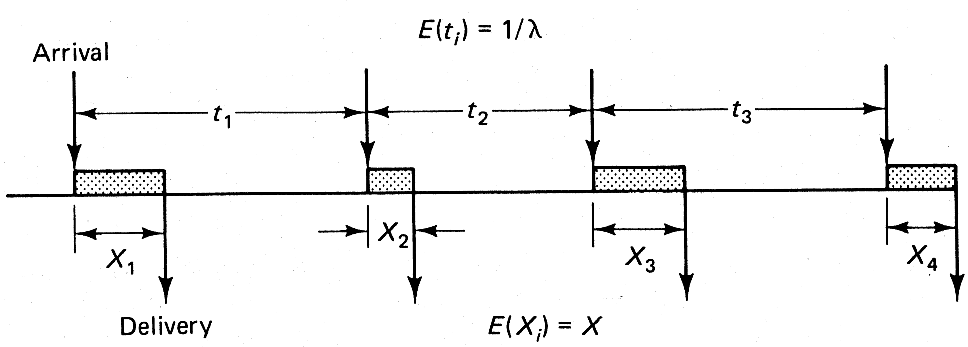

Figure 1: Link utilization. The average transmission time of a message is X. The average interarrival period is $1/\lambda$. Thus, the link is used at most λX of the time.

including Web use studies, indicate the following results regarding computer response times [6, 7]:

- 0.1 s is about the limit for having the user feel that the system is reacting instantaneously,
- 1 s is about the limit for the user’s flow of thought to stay uninterrupted, but the user will notice the delay,
- 10 s is about the limit for keeping the user’s attention focused on the dialogue.

Thus, the target response time for easy Web use is less than 1 s. Consequently, $T < 1$ s and we have $\lambda T < 0.067$, or about a 15X advantage in using packet switching as compared to circuit switching with Web use.

There exist various techniques, known in general as fast circuit switching (see e.g., [8]) that are based on the set up and tear down of a circuit at the beginning and end of each message. Such techniques have milder throughput degradations as compared to circuit switching. However, they suffer from large delays due to the setting up and tearing down of circuits. Also, the large number of signaling messages on the network backbone becomes a significant consideration.

A further advantage of packet switching relates to a subjective advantage, in addition to the throughput, delay, and signaling complexity advantages described above. For a user population of N users, circuit switching can deliver at best $1/N$ of the total channel capacity to each user; whereas with packet switching a user can access the full bandwidth of the channel in an instantaneous manner.

2 Classification of MAC Protocols

MAC protocols are usually classified into the following basic categories

1. Fixed assignment techniques
2. Contention algorithms

3. Demand assignment techniques.

It is possible to combine these techniques, and sometimes a fourth such category, mixed modes, is defined to address the combination.

Fixed Assignment Techniques are essentially circuit switching techniques. They incorporate permanent subchannel assignments. Examples of fixed assignment techniques as MAC protocols are Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), and Code Division Multiple Access (CDMA). As stated above, these classical schemes perform well with stream type traffic where each user transmits a steady flow of messages such as constant bit rate voice or video. The system enables a large percentage of the subchannels to carry user traffic. The result is the high utilization of the communications channel. As shown above, however, fixed assignment techniques are inefficient in bursty traffic applications. A subchannel is wasted whenever its owner does not have anything to transmit.

Contention Algorithms have two general categories. One category is known as *Random Access Algorithms* and the other as *Collision Resolution Algorithms*. Random access algorithms aim to make the full channel capacity available to users, for short periods of time, on a random basis. They are packet oriented, whereas the fixed assignment techniques are channel oriented. They dynamically allocate transmission capacity on a per packet basis. The simplest random access protocol, pure ALOHA, permits users to transmit at will [9]. Whenever one user's transmission overlaps any part of another user's transmission, a collision occurs and both messages must be retransmitted. When the channel is lightly loaded, few collisions occur in ALOHA-based schemes. Thus the expected delay, from the arrival of a packet until its successful transmission, is very small. When collisions occur, users retransmit with random delays. This increases delay and reduces throughput at high loads. In addition, ALOHA schemes are inherently unstable. As an extension of the pure ALOHA algorithm, sensing the channel prior to transmission results in the Collision Sense Multiple Access (CSMA) algorithm. This reduces the number of collisions and consequently, increases throughput and reduces delay. If the users can detect collisions shortly after transmission, then they can use the Carrier Sense Multiple

Access/Collision Detection (CSMA/CD) algorithm. This is the algorithm used in Ethernet (IEEE 802.3). Despite the improvements achieved with carrier sensing techniques, the stability problems of pure ALOHA still persist in CSMA/CD. Furthermore, performance degrades as the maximum propagation delay between users increases. In wireless channels, it is very difficult to sense collisions. For this environment, Collision Avoidance (CA) algorithms have been developed. In these algorithms, a user waits for a random period before transmission after the channel becomes idle; if it does not receive an acknowledgement from the central controller after transmission, it increases the random period before transmission. CSMA/CA is the basis of the IEEE 802.11 standard for wireless LANs.

The second category of contention algorithms is known as Collision Resolution algorithms. These were invented to improve the maximum achievable stable throughput of random access protocols. The basic idea is to assign retransmission times after collisions deterministically to a subgroup of all users so that idle channel periods due to random retransmission times are avoided. There is a family of such algorithms, known as splitting or tree algorithms [5]. Of primary importance, these techniques guarantee system stability, provided the input rate to the network is not too large.

Demand Assignment Techniques achieve high channel throughput by requiring users to reserve communication bandwidth. A portion of the channel capacity is required in this reservation stage. The reservation subchannel is accessed by users according to a multiple access protocol, such as TDMA or Slotted ALOHA. Short reservation packets are sent to request channel time; the shorter they are, the less capacity is necessary for the reservation subchannel. Once channel time is reserved, information packets are transmitted conflict-free. Conflicts occur only on the small capacity reservation subchannel. Users wait for their reservations to be accepted, and are assigned transmission times. Thus, at low throughputs, the message delay is increased over that of random access techniques. This can be remedied by using this reservation channel for the transmission of short data messages, in addition to reservation packets. A special case of demand assignment techniques is *polling* where each user is addressed sequentially by a central station for transmission privileges.

We want to emphasize that for data and voice sources, demand assignment MAC protocols have the best performance. Fixed assignment, or circuit switching, is not acceptable due to its poor delay and throughput performance with data sources. Even fast circuit switching has poor delay performance. In addition, it generates too many signaling messages on the backbone network. Contention algorithms are also not applicable due to their low throughput. Also, they are not suitable for combining voice and video.

3 Demand Assignment Protocol Examples from the Literature

Two demand assignment algorithms are well-known and have been studied in detail in the literature. In Packet Reservation Multiple Access (PRMA), each time slot is recognized as “reserved” or “available” according to an acknowledgement message from the central controller [10]. When a user with a periodic source successfully transmits a packet in an available slot to the central station using the Slotted ALOHA protocol, that slot becomes reserved in future frames and there are no subsequent collisions from other terminals until the end of its burst. At the end of the burst, the reservation is released, leaving the slot empty. Random information packets contend for available time slots using Slotted ALOHA. However, when a random packet is successfully transmitted, the mobile does not obtain time slot reservation. PRMA was the first MAC protocol that described a way to transmit periodic data using a conventional MAC protocol. In other words, it was the first protocol in the literature to combine data and voice. Its performance has been studied extensively in the literature.

Distributed Queueing Request Update Multiple Access (DQRUMA) [11] is a demand assignment protocol where

1. When requests are made the size of the message is declared at the onset (so that, unlike PRMA, a time slot is not wasted at the end to release reservation),
2. If, after the initial request, the user receives further packets to transmit, further reservation requests are piggybacked onto data packets in transmission (rather than going through the reservation channel).

DQRUMA has been introduced recently [11]. Nevertheless, there exist enhancements and performance studies on DQRUMA in the literature. We have introduced PRMA and DQRUMA here since their basic concepts have been employed in the development of MAC protocols for new access networks, for example, in DOCSIS. Also, in the engineering literature, state-of-the-art MAC protocol discussions evolve around PRMA and DQRUMA. MAC protocols developed by the industry can handle more detailed service and transmission types than PRMA and DQRUMA. We will describe these protocols in the next section.

4 Protocol Examples from the Industry

Together with the introduction of HFC networks, three efforts to design MAC protocols begun: IEEE 802.14 and DOCSIS in the U.S. and DAVIC in Europe.

IEEE 802.14 Working Group is a committee of engineers representing the HFC vendor community. This committee has developed a specification for data over cable networking. The group was formed in May 1994 and had intended to develop a specification that would be recognized as an international physical layer and MAC protocol standard for HFC networks. Because of the development of DOCSIS, IEEE 802.14 remains as a draft, it has not been accepted by the IEEE LAN/MAN Standard Committee. IEEE 802.14 chose ATM transfer as its default solution. A byte is added to each ATM cell to form a MAC data Protocol Data Unit (PDU). We will describe channel access in IEEE 802.14 next.

In this protocol, the headend tightly controls the initial access to the Contention Slots (CS) as well as managing the Collision Resolution Protocol (CRP) by assigning a Request Queue (RQ) number to each contention slot. Upon receipt of a data packet, the station generates a Request Minislot Data Unit (RMDU). An admission control scheme for newcomer stations is used to provide differentiated initial contention access. This scheme is based on preassigned priorities and a FIFO service of timestamped requests. The headend controls the station’s entry by sending an Admission Time Boundary (ATB) periodically (refer to Figure 2). Thus only stations with a generated RMDU time less than ATB are eligible to enter the contention process. Once the RMDU is generated, the station

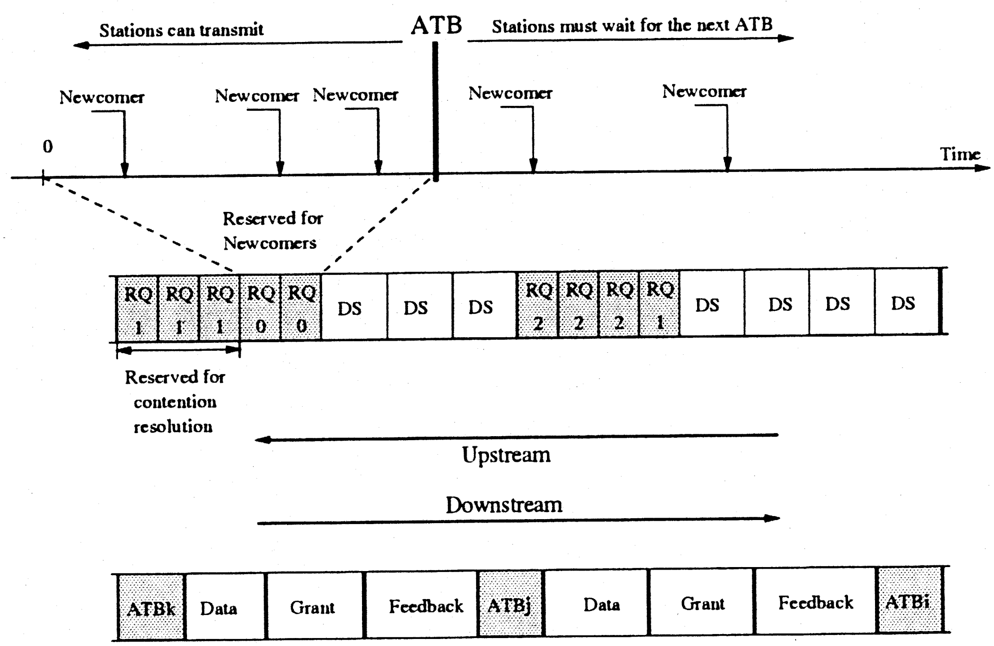

Figure 2: IEEE 802.14 channel access.

waits for a CS Allocation message from the headend that reserves a group of CS with RQ=0 for newcomer transmission. The station randomly selects a CS in that group and transmits its RMDU. Since multiple stations may attempt to send their RMDUs in the same upstream CS, a collision may occur. A feedback message is sent to the station after a roundtrip time (which is also equal to a frame length) informing it of the status of the CS slot used. In the case of a successful request transmission, the station activates its data transmission state machine and exits the contention process. Subsequently a Data Grant message will be sent by the headend. In the case of a collided CS, the feedback message contains a particular RQ number to be used for collision resolution. That is, the station needs to retransmit its request in a CS group with that RQ number. The CS groups are usually located in the order of decreasing RQ values. For each RQ value the headend assigns a group of CS and an associated splitting value (SPL) that is by default equal to 3. A CS within the group is selected randomly in the range [0,…,SPL-1].

DOCSIS stands for Data Over Cable Service Interface Specifications. It is developed by a limited partnership consisting of cable operators, called Multimedia Cable Network System

Partners Ltd. (MCNS). DOCSIS assumes that the packets it transmits are IP packets, although provisions exist for the transmission of ATM cells as well. Next we will describe channel access in DOCSIS.

In DOCSIS, access to the upstream channel is controlled via a backoff window set by the headend. This includes both the initial transmission of a request and any subsequent transmissions of collided requests. The headend controls the initial access to the contention slot by setting an initial backoff window, or Data Backoff Start defined in the Allocation Map (refer to Figure 3). The station then randomly selects a number within its backoff window. The random value indicates the number of contention transmit opportunities, which the station must defer before transmitting. After a contention transmission, the station waits for either a Data Grant or an Acknowledgement in a subsequent Allocation Map. Upon receipt of a station’s request (in the case of a successful transmission), the headend processes it and assigns a data slot to the station by sending a Data Grant in the Allocation Map. The headend may send an Acknowledgement message to the station if it needs more time to process the request before it sends the Data Grant. Since multiple stations may attempt to send their request in the same upstream CS a collision may occur. But, unlike 802.14, the headend does not need to send an explicit

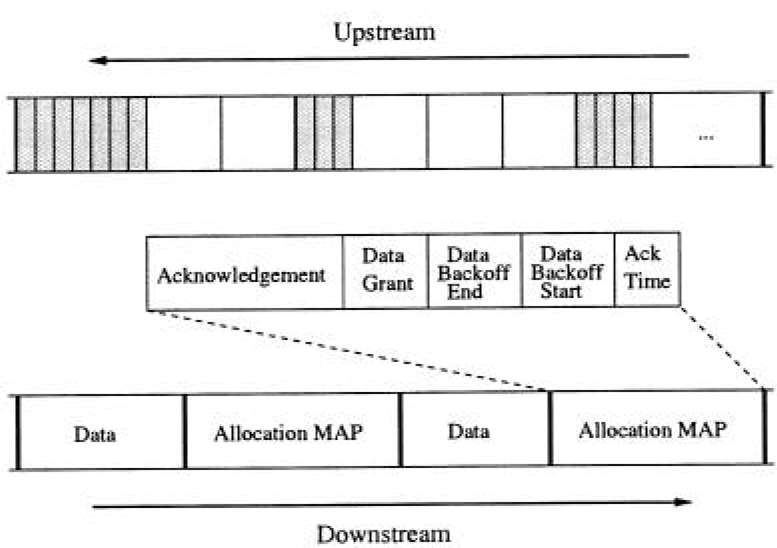

Figure 3: DOCSIS channel access.

feedback message on the status of each CS. The station detects the collided slot when it does not find an Acknowledgement or Data Grant for it in the Allocation Map. The station must then increase its backoff window by a factor of two as long as it is less than the maximum backoff window set in the Allocation Map. The station randomly selects a number within its new window and repeats the contention process described above. After 16 unsuccessful retries the station discards the MAC PDU.

DAVIC stands for Digital Audio Visual Council. This consortium developed a standard for video distribution over cable systems, specifically for Europe. There is a competing form of DOCSIS (DOCSIS Euro), and therefore the future deployment of DAVIC is uncertain. Currently, Version 1.5 of the standard has been defined. Similar to IEEE 802.14, DAVIC has an ATM cell-based transmission format. It specifies ATM framing using LLC/SNAP (RFC 1483) and AAL5 (ITU-T I.363.5) to encapsulate IP (RFC 791) packets.

5 Advantages of DOCSIS

In comparing MAC protocols, the following criteria are used as a minimum:

- Acceptance of a MAC for existing standards,
- Maturity of protocol,
- Wide acceptance and deployment,
- Ability to handle various types of traffic and variable length packets,
- Access delay and throughput, particularly for IP packets,
- Support of QoS guarantees, end-to-end QoS guarantees, and the ability to satisfy customer Service Level Agreements,
- Simplicity of implementation,
- Scalability,
- Robustness,
- Security,
- Authentication,
- Management functions, and
- Ability to work with different physical layers.

As of this writing, DOCSIS is the accepted HFC standard by equipment vendors both in the U.S. and in Europe. It has become an ITU-T standard (J.112). DOCSIS is a mature protocol. It has been widely simulated and tested. It has also been widely deployed in the cable environment. There are some limited wireless MMDS deployments [12].

DOCSIS is based on the transport of IP packets although it supports ATM cell transmission as well. It is a demand assignment protocol. It inherits various properties of PRMA and DQRUMA, as well as having provisions for Quality-of-Service (QoS) guarantees. It serves constant bit rate traffic sources in reservation mode similar to a circuit-switched protocol. Its reservation channel can be used for the transmission of short data packets, as in PRMA; and it has reservation request piggybacking, as in DQRUMA.

DOCSIS is designed to carry IP packets. Simulation studies show that it performs very well (in terms of delay-throughput) in IP packet transport (refer to Figure 4 [13]). Reference [14] studies comparative delay-throughput performance of DAVIC, IEEE 802.14, and DOCSIS for variable length packets, such as IP traffic. Since DOCSIS is the only one among these three MAC protocols that supports variable length packet sizes, it has the best delay-throughput performance [14].

DOCSIS Version 1.0 of the specifications provided for the basic transmission of data for a “best effort” service. DOCSIS Version 1.1 provides enhanced capabilities to better support voice and other applications requiring higher QoS guarantees. These enhanced capabilities are as follows:

- Improved QoS capabilities including multiple service types for scheduling upstream traffic
- Fragmentation of upstream packets for control of upstream latency
- Concatenation of small packets within a single payload for improved efficiency
- Payload header suppression for improved efficiency in both upstream and downstream
- Enhanced security (against theft of service) and privacy (against eavesdropping)
- Support for IP multicast
- Voice over IP (VoIP)

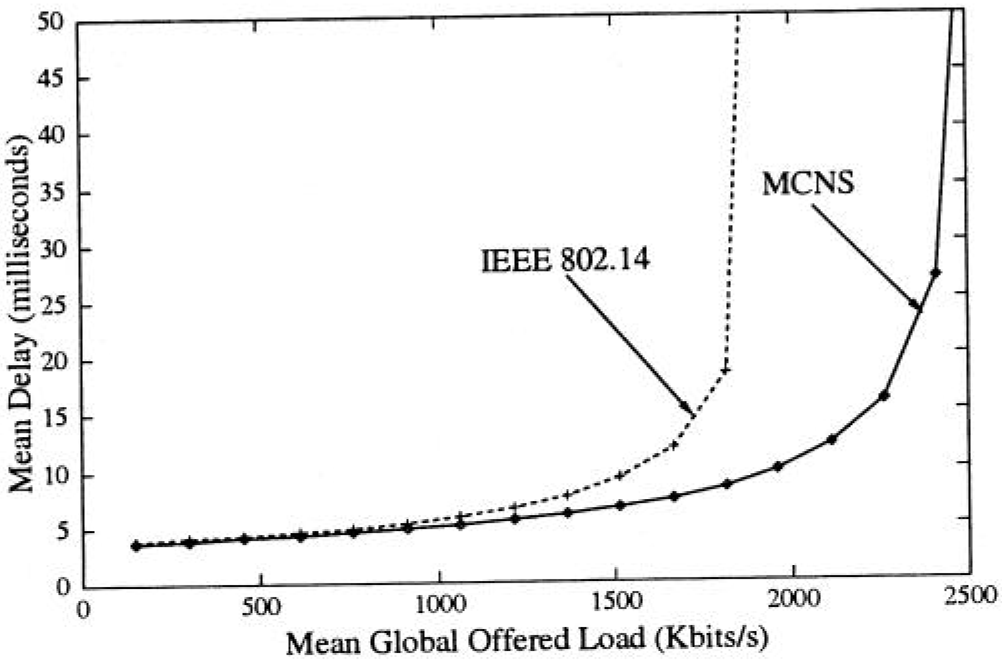

Figure 4: IP transfer delay comparison of DOCSIS and IEEE 802.14.

We would like to stress that although DOCSIS is designed to carry IP packets, it can be part of an access network that has, for example, an ATM backbone. It is extremely important to recognize that the MAC protocol on the shared medium part of an access network need not have the same packet format as on the backbone network. Neither can the QoS guarantees on the backbone network be translated directly to the shared medium part just because the networking protocol is the same. As long as a mapping exists between the backbone network QoS parameters and those of the DOCSIS QoS parameters, end-to-end guarantee of the QoS parameters can be achieved in a statistical sense. In other words, the assumption (sometimes made) that there is a need for an ATM MAC so that ATM QoS guarantees can be satisfied in an end-to-end manner is incorrect. QoS guarantees are the mechanism with which one satisfies the Service Level Agreements (SLAs) in a statistical sense. By means of the QoS mechanisms it has, DOCSIS is able to satisfy customer SLAs.

DOCSIS is implemented in chips, and extensive software has been written and tested for it. Therefore, its implementation can be considered simple by means of off-the-shelf components and their support. It has been designed for scalability to large customer deployments. It has been proven to be robust. It has built-in security, authentication, and management functions. Finally, it is able to work with different physical layers, e.g., Single Carrier Quadrature Amplitude Modulation and Orthogonal Frequency Division Multiplexing.

6 DOCSIS Operation

DOCSIS has five service types to support different QoS requirements on the upstream, described below.

1. *Unsolicited Grant Services (UGS):* This service provides for minimal latency upstream for time-sensitive applications. This service supports CBR-like services (fixed size grants at periodic intervals). Transmission opportunities are periodically granted in the upstream direction without continuing requests from the remote. Grants are issued on previously agreed upon set of service parameters.
2. *Real-Time Polling Service (rtPS):* This service type provides upstream transmission opportunities for real-time traffic in the form of periodic polls (on the order of tens of milliseconds or less). Periodic unicast request opportunities are sent as a means of real-time polls regardless of network congestion. When the source becomes inactive, the transmission reservations are released to other flows.
3. *Unsolicited Grant Service with Activity Detection (UGS-AD):* This service operates as UGS, but reverts back to rtPS in order to conserve upstream bandwidth when grants are not used for a predefined number of opportunities. The base station provides unicast grants when the flow is active, but reverts to providing periodic unicast request opportunities when the flow is inactive. This service is intended for VoIP with silence suppression enabled. This service can also be used for services that are CBR-like but are turned on and off based on activity.
4. *Non-Real-Time Polling Service (nrtPS):* This service provides periodic or nonperiodic polls (on the order of one second or less). This service is intended for non-real-time traffic flows such as high bandwidth file transfer applications.
5. *Best Effort (BE):* With this service, the remote uses all contention and unicast request opportunities as well as all unicast data transmission opportunities.

6. *Committed Information Rate (CIR):* This service can be implemented in several different ways. As an example it could be a BE service with a reserved minimum traffic rate or nrPTS with a reserved minimum traffic rate.

A Service Flow is a particular service defined between the base station and the remote using a set of traffic description parameters. A service flow receives unidirectional transport of packets and shaping, policing, and prioritizing of traffic according to QoS traffic parameters defined for the flow. Each Service Flow is identified by a Service Flow Identifer (SFID). SFIDs are 32 bits long. Active or admitted upstream service flows are assigned Service Identifers (SID) in addition to an SFID. A SID is 14 bits long.

The base station allocates bandwidth to particular SIDs based on the vendor's scheduling algorithm. The allocations are broadcast to remotes as a minislot map transmitted in a MAC management message, as shown in Figure 5. A given map may describe some slots as grants for particular stations to transmit data in, other slots as available for contention

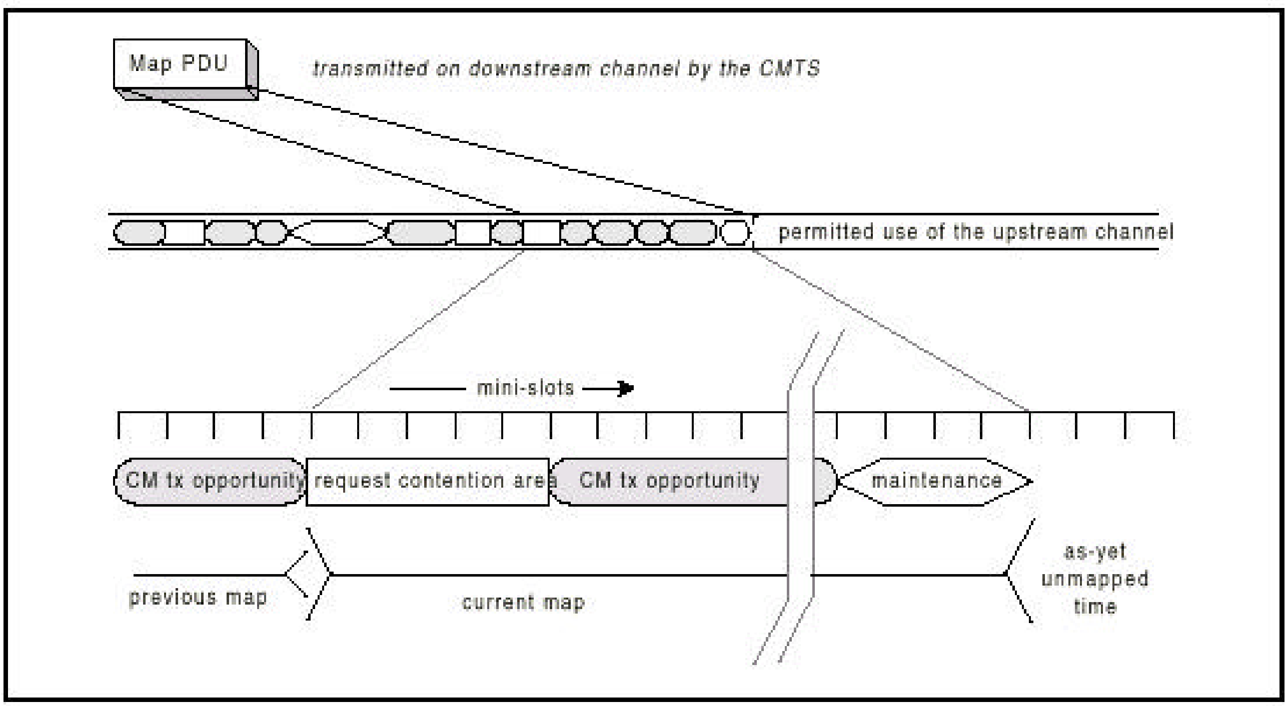

Figure 5: DOCSIS Allocation Map.

transmission, and other slots as an opportunity for new stations to join the system. The base station provides the same kinds of QoS services to downstream service flows using simple SFID based queueing mechanisms.

The same basic structure is used in both the upstream and the downstream directions as MAC frames. A MAC frame is variable in length. It consists of a MAC header and may have a variable-length data PDU. A MAC frame header together with a data PDU is shown in Figure 6. The first part of the MAC frame is the MAC header. The MAC header uniquely identifies the contents of the MAC frame. If the EHDR (Extended Header) indicator is on, there is an Extended Header field following the LEN field. The Extended Header can be up to 240 bytes. DOCSIS supports a variable length Ethernet-type Packet PDU. Normally the Packet PDU is passed across the network in its entirety, including its original CRC. However, in the case of Payload Header Suppression, all bytes except those suppressed are passed across the network and the CRC covers only those bytes actually transmitted.

The downstream bitstream is defined as a continuous series of 188-byte MPEG packets. For DOCSIS data, the packet consists of a 4-byte MPEG header, a pointer field (not present in all packets) and the DOCSIS payload. DOCSIS frames may begin anywhere within an MPEG packet, MAC frames may span several MAC frames, and MAC frames may exist within an MPEG packet.

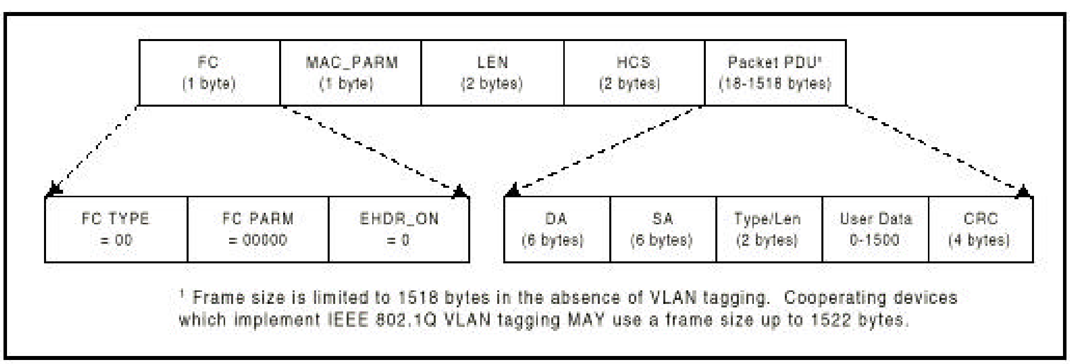

Figure 6: MAC frame header and data PDU format.

7 Conclusions

In summary,

- For data networking, variants of circuit switching or fast circuit switching are not acceptable. These protocols result in increased delay, low throughput, or a large number of signaling messages in the backbone network. In addition, they are limited in terms of the bandwidth, and thus, in terms of the look and feel they can provide to the user.
- Protocols that employ only contention (such as CSMA/CA or 802.11) result in low throughput. In addition, they are not suitable for combining data with voice or video. We are aware of efforts to use these protocols to develop broadband fixed wireless access systems (e.g., [15]). It is important to emphasize that such systems will not be able to provide QoS and SLAs.
- Most efficient MAC protocols to support a combination of data, voice, and video are of demand assignment type. We described demand assignment protocols from the engineering literature and industry, i.e., PRMA, DQRUMA, IEEE 802.14, DAVIC, and DOCSIS. The useful features of PRMA and DQRUMA are absorbed in DOCSIS. In addition, DOCSIS has better IP performance than IEEE 802.14 and DAVIC. Furthermore, DOCSIS has provisions for guaranteeing QoS, built-in security, authentication, and management functions. Finally, DOCSIS is the accepted MAC protocol for HFC networks worldwide. It has been widely implemented and tested.
- It is possible to provide end-to-end QoS guarantees while employing DOCSIS on the wireless link and ATM in the backbone. To this end, the QoS guarantees on the wireless link and the backbone can be mapped to each other. An ATM backbone does not require a MAC whose transmission units are ATM cells.

References

[1] R. Rosner, “Circuit and packet switching: A cost and performance tradeoff study,” *Computer Networks,* Vol. 1, No. 1, pp. 7-26, June 1972.

[2] K. Kummerle, “Packet and circuit switching: Cost/performance boundaries,” *Computer Networks,* Vol. 2, No. 1, pp. 3-17, February 1978.

[3] H. Rudin, “Studies in the integration of circuit and packet switching,” *Proc. ICC ’78,* pp. 20.2.1-20.2.7, 1978.

[4] L. Kleinrock, *Queueing Systems, Volume 2: Computer Applications,* Wiley, 1976.

[5] D. Bertsekas and R. Gallager, *Data Networks,* Prentice-Hall, Englewood Cliffs, NJ, 1987.

[6] R. B. Miller, “Response time in man-computer conversational transactions,” *Proc. AFIPS Fall Joint Computer Conference,* Vol. 33, pp. 267-277, 1968.

[7] J. Nielsen, *Usability Engineering,* AP Professional, Boston, MA, 1994.

[8] E. A. Harrington, “Voice/data integration using circuit switched networks,” *IEEE Transactions on Communications,* Vol. 28, June 1980.

[9] N. Abramson, “The ALOHA systems – Another alternative for computer communications,” *Proc. AFIPS Fall Joint Computer Conference,* Vol. 37, pp. 281-285, 1970.

[10] D. J. Goodman, R. A. Valenzuela, K. T. Gayliard, and B. Ramamurthi, “Packet reservation multiple access for local wireless communications,” *IEEE Transactions on Communications,* Vol. 37, pp. 885-890, 1989.

[11] M. J. Karol, “An efficient demand assignment multiple access protocol for wireless packet (ATM) networks,” *Wireless Networks,* Vol. 1, pp. 267-279, 1995.

[12] B.-Y. Kim, N. K. Shankaranarayanan, P. S. Henry, K. Schlosser, and T. K. Fong, “The AT&T Labs broadband fixed wireless field experiment,” *IEEE Communications Magazine,* Vol. 37, pp. 56-62, October 1999.

[13] N. Golmie, F. Mouveaux, and D. Su, “A comparison of MAC protocols for hybrid fiber/coax networks: IEEE 802.14 vs. MCNS,” *Proc. ICC’99,* Vancouver, Canada,

[14] M. T. Ali, R. Grover, G. Stamatelos, and D. G. Falconer, “Performance evaluation of candidate MAC protocols for LMCS/LMDS networks,” *IEEE Journal on Selected Areas in Communications,* Vol. 18, pp. 1261-1270, July 2000.

[15] http://www.ofdm-forum.com