# DECLARATION AND AFFIRMATION OF BRENDA RAY

**I, Brenda Ray, being over 18 year of age and duly sworn, depose and say as follows:**

1. I am an employee of the Auburn University Library, and specifically the Document Delivery Unit, located at Auburn University, Auburn, Alabama 36849. I am familiar with the policies and procedures of the Library as they relate to the receipt, cataloging, and tracking of books and I have personal knowledge of the facts set forth below. I am familiar with these procedures because I have been employed by the Library since 1989, where I began in Binding and Receiving, then moved to Serials, then the Science and Technology Department, then the Architecture Library and finally the Document Delivery Unit. I have held my current position in the Document Delivery Unit for the last 17 years.

2. It is and has been standard operating procedure that when an item is received by the Library, it is received, cataloged, physically processed (spine label with call number, tattle-taped, ownership stamp, etc.). The item would then be stamped with date mark. The item would be made available to patrons within a few days of the item arriving at the library.

3. The Auburn University Library holds an original copy of Electronic Design Volume 45, Issue 27, December 1, 1997. I have been asked for information about Electronic Design specifically when this volume was first made publicly available by the Auburn University Library. From my review of the Library's records, and my knowledge of the Library's standard procedures, this issue of Electronic Design was cataloged and publicly available in the Library by no later than December 20, 1997, and was in current issues, shelved in alphabetical order within a few days after the date of December 20, 1997.

4. In my opinion, the journal Electronic Design was cataloged and available at the Auburn University Library on December 20, 1997 based on the date stamp on a preliminary page inside this volume of Electronic Design. I have not seen any indication that this volume of Electronic Design would have been an exception to the Library's standard practice. The Library maintains a searchable and publicly accessible catalog of its publications. Therefore, as of December 31, 1997 any member of the public could have located this volume of Electronic Design by searching our catalog by the title, call number, and/or subject matter.

5. Exhibit A to this Declaration is a true and accurate copy of the cover, table of contents, preliminary page with date stamp and the article "MCNS/DOCSIS MAC Clears A Path For The Cable-Modem Invasion" by Lee Goldberg on pages 69-70, 74, 78, 80 from the journal Electronic Design Volume 45, Issue 27, December 1, 1997, ISSN 0013-4872 from the Auburn University Libraries collection.

I declare and affirm under penalty of perjury that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code. If called to testify, I could and would competently testify under oath to the facts set forth above. Unless otherwise noted, the facts and statements in this Declaration are based on my personal knowledge and my review of the documents discussed herein, and I am competent to testify to these facts.

May 11, 2021

Auburn University Libraries
231 Mell Street
Auburn, AL 36849-5606

Brenda Ray

Brenda Ray
Library Specialist, Tech II

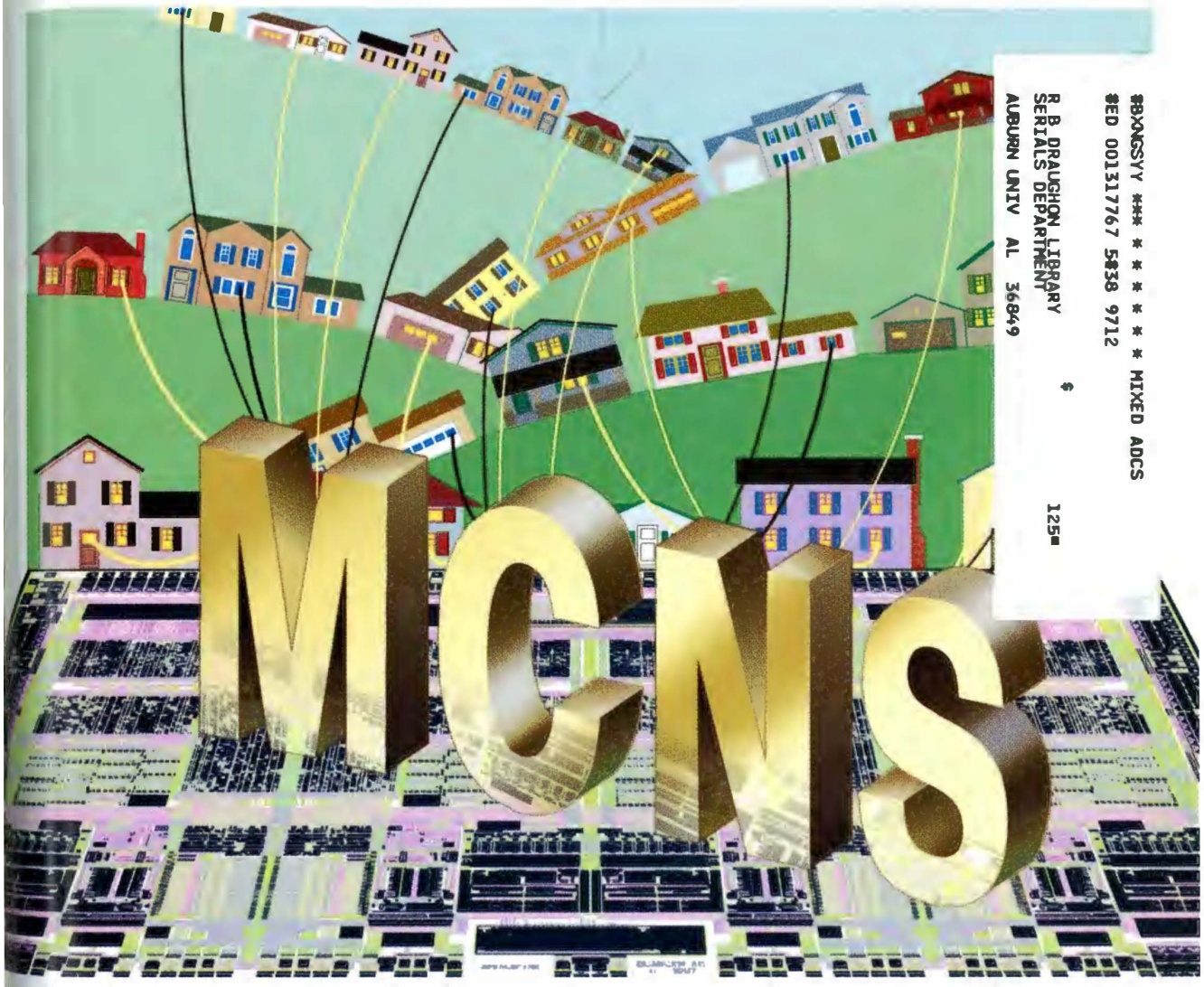
# EXHIBIT A

# ELECTRONIC DESIGN

TECHNOLOGY • APPLICATIONS • PRODUCTS • SOLUTIONS

A PENTON PUBLICATION $10.00

DECEMBER 1, 1997




$BXONGSYY *** * * * * * * MIXED ADCS
$ED 00131767 5838 9712
R.B. DRAUGHON LIBRARY
SERIALS DEPARTMENT
AUBURN UNIV AL 36849
125

## MCNS/DOCSIS MAC Clears Path For Cable-Modem Invasion p. 69

Annual IEDM Conference Examines Leading-Edge Device Developments p. 39

At IEDM: Memory, Logic Power Devices, EDA, Sensors, And Displays p. 40

Line-Driver Design For Broadband Communications Applications p. 81

Parasitic Extraction Tools Aid DSM IC Designs p.97

Harness The Power Of The ACPI/Smart Battery Standard p. 113

Pick The Perfect Chassis To Ensure System




If you're charged with designing low-power applications, this little core is a mighty big friend. Motorola's new M•CORE microRISC engine reduces costs, lengthens battery life and gives you performance for the future. A combination of brains and brawn.

A 48MIPS/50MHz RISC core design with I/O intelligence and interrupt performance built in. Plus, its development tool chains are fully complete and validated to interoperate, greatly reducing design time. In other words, it's ready to fly!

To find out how Motorola can help you save the day, direct your mouse to **www.motorola.com/mcore** or call 800.521.6274.

DEC 20 1997
AUBURN UNIVERSITY

**MOTOROLA**

***Semiconductor Products Sector***

*What you never thought possible.™*

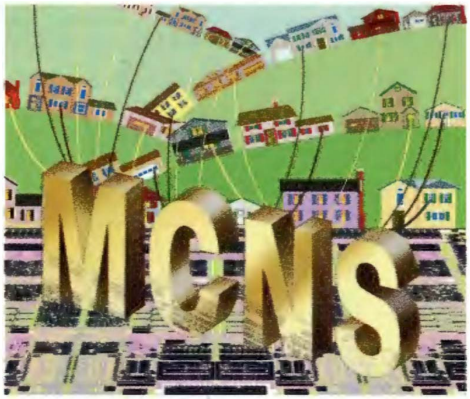
© 1997 MOTOROLA, INC. ALL RIGHTS RESERVED. MOTOROLA AND Ⓜ ARE REGISTERED TRADEMARKS AND THE M•CORE NAME AND LOGO ARE TRADEMARKS OF MOTOROLA, INC. MIGHTY MOUSE, TM & © 1997 VIACOM INT'L. INC.

# ELECTRONIC DESIGN

TECHNOLOGY • APPLICATIONS • PRODUCTS • SOLUTIONS

*December 1, 1997 Volume 45, Number 27*


## EDITORIAL OVERVIEW





**MCNS/DOCSIS MAC Clears Path For Cable-Modem Invasion 69**

**Annual IEDM Conference Examines Leading-Edge Device Developments 39**

**At IEDM: Memory, Logic Power Devices, EDA, Sensors, And Displays 40**

**Line-Driver Design For Broadband Communications Applications 81**

**Parasitic Extraction Tools Aid DSM IC Designs 97**

**Harness The Power Of The ACPI/Smart-Battery Standard 113**

**Pick The Perfect Chassis To Ensure System Longevity 127**


### TECH INSIGHTS


**39 Annual IEDM Conference Examines Leading-Edge Device Developments**
• *Hear about the latest in memory and logic ICs, compound semiconductor devices, simulation tools, and sensors and displays.*

**40 Memory And Logic Structures Are Getting Faster And Denser**
• *Designers detail advanced process techniques and finer-dimension design rules at IEDM to build next-generation memories and logic.*

**48 Rivalries Between Silicon And Exotic Semiconductors Abound At IEDM**
• *SiGe and vanilla silicon move into RF and optical applications as compound semiconductors stake out their niches.*


### TECH INSIGHTS


**50 IEDM Focuses On Advanced Device Models**
• *Models offer new hope in tackling deep-submicron issues dealing with process accuracy and interconnect.*

**60 Sensors And Displays Highlighted At IEDM**
• *Advanced device structures and new technologies are opening the door for emerging display and sensor-based applications.*


### COMMUNICATIONS TECHNOLOGY


**69 MCNS/DOCSIS MAC Paves The Way For A Cable-Modem Invasion**
• *The first standards-compliant chip means affordable, interoperable, cable modems, with speed and security features.*


COVER STORY

### DEPARTMENTS


**Upcoming Meetings . . . 12, . . . . . 16, 18, 54**

**Editorial . . . . . 22**
• *Tiny Engines Fuel A Revolution*

**Technology Briefing . . . . 24**
• *Consumer Electronics' Potential*

**Technology Newsletter . . . . . 27, 30**

**Technology Breakthrough . . . . . 33**
• *35-GHz 0.5-W GaAs pHEMT points the way toward low-cost volume production of MOCVD MMICs*
• *0.1-mm electrostatic microrelays switch at up to 100 GHz*
• *Development of blue phosphor spawns full-color EL displays*

**Info Page . . . . . 10**
*(how to find us)*

**Index of Advertisers . . 184**

**Reader Service Card . . . . 184A-D**



ELECTRONIC DESIGN (ISSN 0013-4872) is published twice monthly except for 3 issues in May, 3 issues in August, 3 issues in October, and 3 issues in November by Penton Publishing Inc., 1100 Superior Ave., Cleveland, OH 44114-2543. Paid rates for a one-year subscription are as follows: $105 U.S., $185 Canada, $210, $255 International. Periodicals postage paid at Cleveland, OH, and additional mailing offices. Editorial and advertising addresses: ELECTRONIC DESIGN, 611 Route #46 West, Hasbrouck Heights, NJ 07604. Telephone (201) 393-6060. Facsimile (201) 393-0204. Printed in U.S.A. Title registered in U.S. Patent Office.



Copyright 1997 by Penton Publishing Inc. All rights reserved. The contents of this publication may not be reproduced in whole or in part without the consent of the copyright owner. For subscriber change of address and subscription inquiries, call (216) 696-7000. Mail your subscription requests to: Penton Publishing Subscription Lockbox, P.O. Box 96732, Chicago, IL 60693. POSTMASTER: Please send change of address to ELECTRONIC DESIGN, Penton Publishing Inc., 1100 Superior Ave., Cleveland, OH 44114-2543.



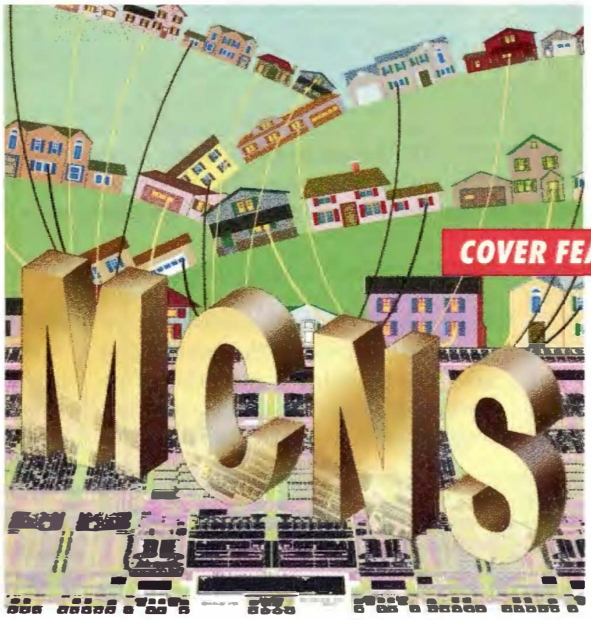


MEDIATEK EX. 1010
Page 6 of 11

# MCNS/DOCSIS MAC Clears A Path For The Cable-Modem Invasion

*The First Standards-Compliant Chip Means Affordable, Interoperable, Cable Modems, With Speed And Security Features.*

**Lee Goldberg**




COVER FEATURE

With the introduction of the BCM3220 multimedia cable networking systems/Data-Over-Cable-Service Interface Specification (MCNS/DOCSIS) compliant media-access controller (MAC) chip, the cable data revolution has begun in earnest. By rolling out the first integrated implementation of the cable industry's recently developed DOCSIS, Broadcom Corporation has paved the way for the rapid development of inexpensive consumer-oriented cable data appliances. This move could provide a critical jump-start for the emerging cable data industry. If the next year goes according to plan, we may see a device that delivers multimegabit downstream Internet access being sold at K-Marts and electronic discount stores at prices comparable to today's 56-kbit POTS modems.

## The Broadband Wars

The development of DOCSIS and the introduction of the BCM3220 mark the first hopeful chapter in the troubled history of cable media's efforts to maintain its dominant role in capturing the hearts, minds, and eyes of the American consumer. In the early nineties, the cable television industry faced a double threat: While saturated subscriber markets yielded flattening revenues, satellite television, sophisticated computer games, and Internet surfing began to erode cable's near-lock on passive leisure activities.

After several ill-fated adventures with video-on-demand, interactive shopping, and other attempts to dictate consumer taste, cable marketeers stumbled over the obvious hot application, broadband Internet access. Once early trials demonstrated the economic potential, it became clear that the only way to achieve a critical mass of users was to develop a transmission standard that would enable the production of mass-produced, inexpensive, interoperable cable modems and set-top boxes *(Fig. 1)*.

Frustrated by the slow progress of the IEEE's 802.14 cable data standards committee, a group of large cable interests formed the MCNS group. Comprised of heavyweights like Comcast and Time-Warner, MCNS teamed with the cable industry's research consortium, Cable Labs, Louisville, Colo., to produce their own open standard for moving data between cable network headends and subscriber's homes.

## Enter DOCSIS

The first fruit of this alliance is the DOCSIS specification, developed by a group of manufacturers, under the direction of MCNS and Cable Labs. Participants in the initial development of DOCSIS included General Instruments, LAN City (now a part of Bay Networks), and Broadcom. This spec outlines the physical layer interfaces, MAC and transport protocols, security provisions, and other specifications necessary for designing interoperable cable data components. Subsequent fine-tuning was performed in an open forum hosted by Cable Labs and attended by most major players in the cable industry. The result is a standard that meets the needs of current users and anticipates the demands of future applications.

DOCSIS is designed to employ one or more unused video channels within the 54-to-860-MHz cable broadcast

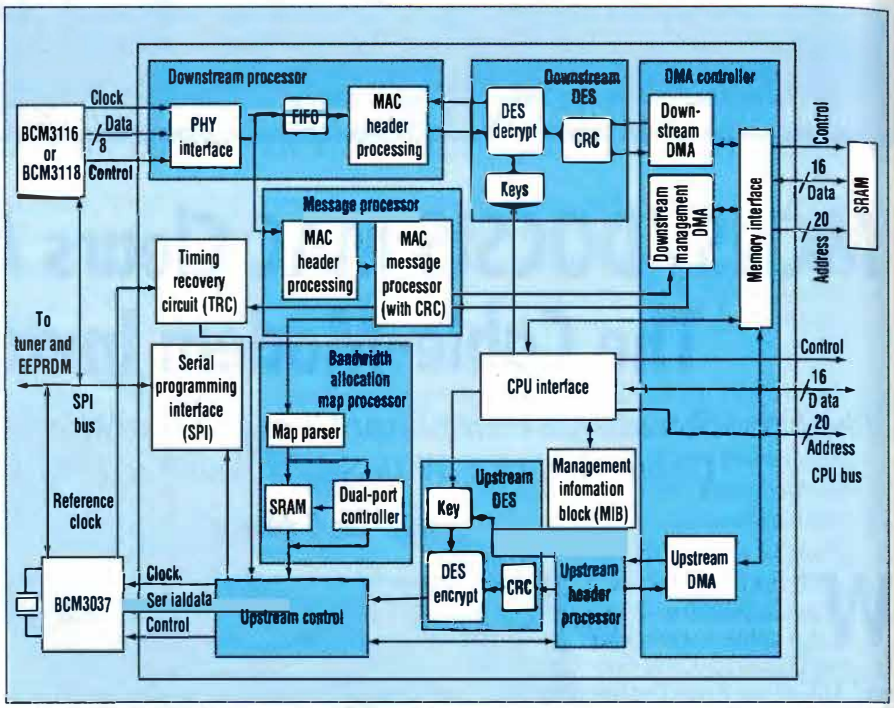


MEDIATEK EX. 1010
Page 7 of 11

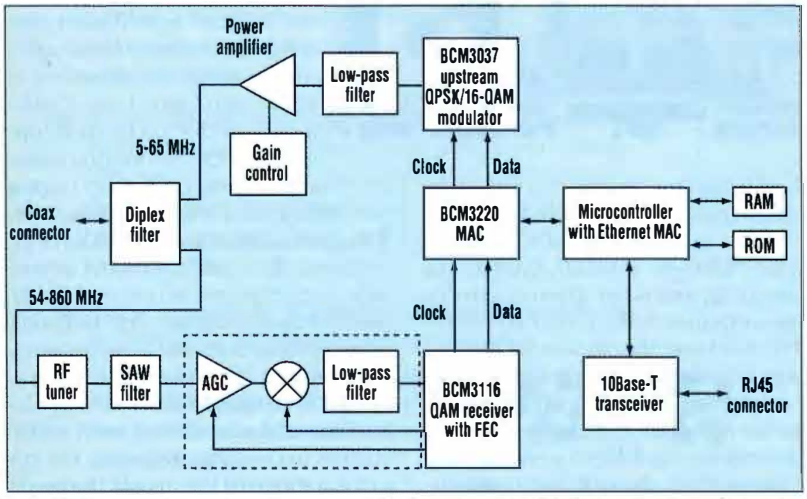
spectrum to transmit IP-based data across hybrid fiber coaxial networks. Complex phase/amplitude modulation enables each 6-MHz downstream channel to bring data into subscribers' homes at up to 38 Mbits/s. Depending on the bit rate selected by the operator, the shared downstream channel uses either 64- or 256-point quadrature-amplitude modulation (QAM). While little is known about what actual bandwidth requirements will be, initial results from field trials suggests that a single channel will provide groups of 200 to 1000 subscribers with Internet access that is substantially faster than today's best POTS-based services.

For communication from the home to headend, DOCSIS uses the 5-to-40-Hz sub-split band as a return path. Using QPSK today, or 16-QAM in subsequent versions, the upstream channel has a theoretical maximum throughput of 10 Mbits/s (*see "Broadband To The Home: Challenges On the Last Mile," Electronic Design, Oct. 2, 1995, pp 67-83).*

Since DOCSIS also is intended to support IP-based video, provisions have been made to support several levels of quality of service (QoS). This feature allows it to accommodate both traditional connectionless Internet traffic, as well as latency-sensitive multimedia streams. Selectable QoS also will let cable companies offer tiered services with various guaranteed bit rates and levels of latency to businesses which need them.




**2. The BCM3220 MAC chip incorporates all control, stream-processing, and security functions required for a MCNS/DOCSIS-compliant cable modem. A memory-based DMA interface assures efficient data transfers to and from the host controller. Both baseline and high-security modes also are supported.**




**1. A DOCSIS-compliant cable modem receives its data over unused 6-MHz video channels within the normal cable spectrum. Upstream traffic is carried back to the system headend in the 5-to-45-MHz sub-split band. To ensure that the modem will operate properly and not interfere with other units, both the downstream receiver and upstream modulator/transmitter operate under the control of the BCM3220, or other DOCSIS-compatible MAC.**

## MPEG Everywhere

One interesting aspect of DOCSIS is that it uses MPEG II transport streams to move IP data. While not essential for today's applications, the standard's developers were looking toward the future. Today, MPEG encapsulation provides DOCSIS with a reliable, well-defined method of setting up multiple channels within a single data stream. In the near future, MPEG encapsulation will allow a single cable modem to support multiple sessions and multiple users, as well as delay-sensitive multimedia streams for voice or video over IP.

Using MPEG II transport streams also will allow DOCSIS to interoperate with the Open Cable standard for digital cable television that is currently under development. Open Cable also employs MPEG II transport streams for all of its media flows. This feature should greatly simplify traffic switching and processing within tomorrow's cable networks

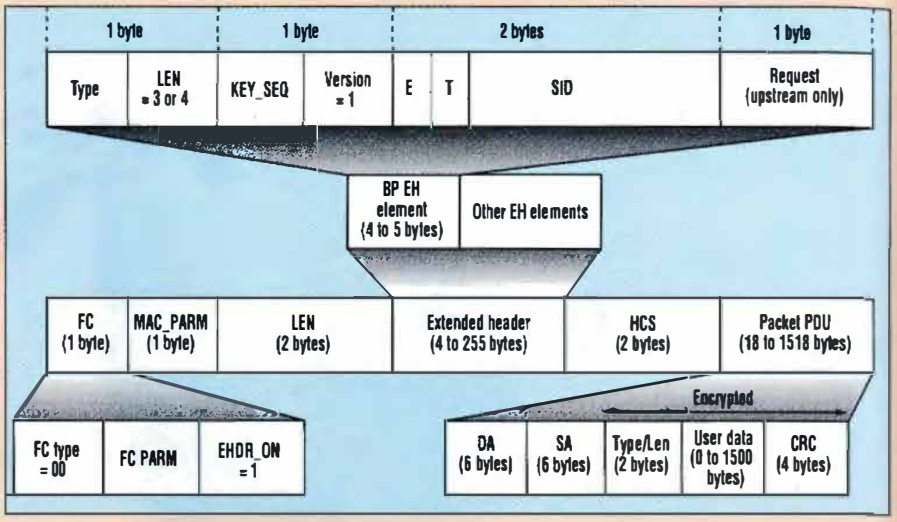
Although it has some similarities to the carrier-sense multiple-access/collision-detect (CSMA/CD) protocol em-



MEDIATEK EX. 1010
Page 8 of 11

# DOCSIS Security: Baseline Privacy

Security for the DOCSIS cable modem system is divided between an elaborate Full-Security Specification with removable, renewable security modules, and a low-cost, simpler scheme called Baseline Privacy (BPI). BPI is based on full-bodied concepts, beginning with the 56-bit Digital Encryption Standard (DES) Cipher Block Chaining algorithm, yet unburdened by some of the more costly and complex security features of its heavy twin. All DOCSIS cable modems are required to support BPI, ensuring that basic data privacy is maintained in the shared cable environment.




Privacy is more than sufficient for Internet access applications because it makes a number of assumptions on the application it serves, namely that Internet access is two way, and therefore not susceptible to passive theft of service; that it's not particularly valuable to anyone, but the user; that really important transactions over the Internet (like banking) will be secured with end to end application layer security; and that by changing keys often, individual keys are not worth the trouble of stealing. It also is much easier to detect clones and unauthorized users of cable modems because the service is two-way. The modem system is unlike broadcast pay-per-view video that can be hacked in private—clone modems must not only listen, but speak to be useful.

DES is a cryptographic algorithm that takes binary coded data and applies a known algorithm using a randomly generated 56-bit key to produce unintelligible or encrypted bits. The algorithm can be known by many but the data will be unintelligible unless the key is shared by both parties. This mutually shared secret allows encrypted traffic to remain private to those who have the keys. A 56-bit key has 70 quadrillion possible values, and the only guaranteed way of discovering a truly random key is to try all of them. Changing keys often reduces the likelihood of success even further. The challenge in this type of cryptography is how to exchange the secret keys easily, yet securely.

Cipher Block Chaining is a form of DES that increases the strength of the encryption by using an initialization vector sent down with the key to preset its encryption hardware state. For each eight-byte block encrypted, instead of resetting or reinitializing, the circuit retains the result from the previous block's encryption. This chaining of results from one block to the start of the next makes the cryptography stronger since a hacker would need to reconstruct the entire sequence to break the code instead of just one block.

Baseline Privacy uses a Service ID (SID) associated with traffic originating from or destined to a particular modem to identify a Traffic Encryption Key (TEK) to use. Each TEK is a pair of even and odd 56-bit keys. Each key also has a corresponding 56-bit initialization vector.

All DOCSIS frames have header fields that are never encrypted and include an optional field called an Extended Header. Mainly for protocol expansion, this variable area in the DOCSIS header is used to contain the Baseline Privacy Extended Header *(see the figure)*. The SID is contained in the BPI Extended Header for each frame to identify which TEK to use.

Each DOCSIS frame that will be encrypted must contain a Privacy Extended Header. The header contains a type and version field as well as the SID identifying a particular encrypted data flow. The SID field also contains an enable/disable bit that controls encryption for that particular frame and a toggle bit. The toggle bit is used to signify the current epoch; that is whether the even or odd key is in use for this frame. This toggle bit allows the protocol to set up a new TEK in the even key slot while actively using the odd key. When the first frame to use the new key is received, the toggle bit indicates that the epoch has changed and that the other key is now in use. The toggle bit also is the least-significant bit of the 4-bit sequence field that is used to track the history of up to 16 keys by the key exchange protocol.

Baseline Privacy encrypts data in both up and downstream directions of the cable plant using the extended headers to indicate what to do. DOCSIS MAC messages allow a simple key exchange protocol to operate between the headend (or cable modem termination system) and the cable modems. Keys are updated frequently and the registration databases are watched vigilantly for clones. This provides subscribers with a low-cost but vey effective "lite" security solution for ensuring data privacy.

*Contributed by Thomas J. Quigley, director of the Residential Broadband Business Unit at Broadcom Corp.*



MEDIATEK EX. 1010
Page 9 of 11

ployed by most other 802-flavored media, DOCSIS employs a time-slotted noncontention access scheme for most ofits communication. In order to maintain order on a busy cable, the MAC chip in each subscriber's modem must keep track of network timing, as well as its place in the overall communications flow. In contrast to Ethernet's CSMA/CD protocol, this more orderly access scheme allows cable operators to fill their pipelines at up to 75% of their theoretical capacity. This factor is critical when subscribers are sharing bandwidth with 200+ neighbors.

To satisfy even the terminally paranoid, two layers of security are provided within DOCSIS, plus the potential for a completely shielded "tunneling" protocol for sensitive data transfers such as personal records or credit card numbers.

If DOCSIS seems a bit complicated, it's because it really is. The standard's rich feature set and traffic control scheme require approximately 100,000 gates (plus RAM) to implement, yielding an effective processing power of 30 to 40 MIPS. In practice, you'd probably need a much faster CPU to make sure it was available for all the demanding real-time operations. Despite the complexity, Broadcom was able to follow the evolution of the standard and deliver a product within nine months of its finalization, thanks to its close participation in the development committee.

Another factor that gave Broadcom an inside edge on delivering the MAC chip is its proprietary silicon compiler technology. Their specially developed software can translate algorithms directly to gate layouts optimized for minimal cross-talk, propagation delay, and other critical parameters. While it is primarily used to implement blindingly fast digital filtering and correlating algorithms in CMOS logic arrays, the same software also has been employed to lay out Fast Ethernet MACs and other control logic requiring complex signal paths and tight timing.

## A Peek Inside

Examining the block diagram of the BCM3220 reveals the basic functions required to support full-duplex communication using the MCNS protocol *(Fig. 2)*. Many complex functions have been implemented plus encrypt/decrypt logic and a DMA-based, shared-RAM host interface that has been optimized for Motorola's QUICC series of 680xx and PowerPC-based controllers. To insure fast, efficient transfers, incoming and outgoing Ethernet packets are exchanged whole-cloth in a single operation, with no buffer copying or other overhead-intensive intermediate steps.

The downstream section of the BCM3220 interfaces directly with the BCM3116 QAM receiver. Since DOCSIS requires that data be encapsulated within MPEG II transport streams, the MAC is responsible for extracting it before passing IP frames to the host system. Broadcom's designers went the spec one better and included an MPEG II filter port in their device. This feature allows the BCM3220 to be programmed to pass through selected MPEG video streams to an external decode circuit— a handy feature when designing a combination cable modem/set-top box.

**To Satisfy Even The Terminally Paranoid, Two Layers Of Security Are Provided Within DOCSIS, Plus A Fully Shielded "Tunneling" Protocol.**

In addition to recovering and processing data, the downstream processor must perform decryption functions and receive synchronization and control messages from the headend. These messages enable the headend to tell the modem to adjust its data rates and other parameters to match changing line conditions.

To avoid conflicts in a shared-media environment, the MAC uses several tools to keep the modem synchronized with its neighbors and headend. First, the time-base recovery (TRC) function detects and interprets broadcast timing information. Since MCNS modems can be programmed for a variety of data rates and transmission parameters, upstream channel description (UCD) messages are used to tell the subscriber equipment what the headend is expecting to see.

## SPI On Board

Part of the BCM3220's job is to interpret these messages and set the transmitter's modulation, timing, and FEC parameters accordingly. With this in mind, the MAC chip sports an industry-standard serial programming interface (SPI) bus master interface which can be used to configure and control both the QAM receiver and Burst modulator chips on the fly. If SPI-capable components are used elsewhere in the modem's design, the BCM3220 also can be programmed to set their operating values, such as tuner frequencies and amplifier gains.

The chip's upstream processing section is responsible for passing data to the headend. Interfacing directly to the BCM3037 QAM/QPSK modulator, it transmits MPEG-encapsulated data within a series of time slots that it shares with the other modems in the network. To accomplish this task smoothly, it places requests to the headend during specially designated time periods.

The BCM3220 MAC keeps these time periods straight by referring to the upstream bandwidth availability map that the headend routinely broadcasts. Stored in on-chip registers, this map tells the modem when it can request an upstream time slot, transmit its data, or perform network maintenance and management functions. For extended data transfers involving more than one block of data, the BCM3220 automatically requests a series of prescheduled piggyback time slots. This technique allows it to use a single transfer request to move multiblock files, increasing throughput and reducing access latency.

## Pretty Darn Good Privacy

Of course, whenever you're using a broadcast media to transmit sensitive data, the issue of security always comes up. According to Tom Quigley, product manager at Broadcom, DOCSIS provides two grades of security at the hardware level. Both employ the date encryption standard (DES) algorithm and Rivest, Shamir, and Adelman (RSA) key exchange. The real difference between the baseline and



MEDIATEK EX. 1010
Page 10 of 11




Turn your **excess inventory** into a substantial tax break and help send needy **kids to college** as well.

Call for your **free guide** to learn how donating your slow moving inventory can mean a generous **tax write off** for your company.

Call (708) 690-0010
**Peter Roskam**
Executive Director

EAL

P.O. Box 3021, Glen Ellyn, IL 60138
FAX (708) 690-0565

*Excess inventory today...student opportunity tomorrow*


full security is the use of a highly secure, removable hardware key for sensitive applications. In addition, full security uses the full authentication protocol and a 1024-bit key to encrypt the exchange of traffic keys.

The BCM3220 supports both levels of security. It performs the DES electronic-code-book (ECB) and cipher-block-chaining (CBC) functions in hardware, along with residual block termination (RBT). Normally, a 56-bit key is employed, although it can be programmed to run with a crippled 40-bit key for export applications. If desired, the MAC chip also lets designers include application-based security measures for a third layer of end-to-end protection *(see "DOCSIS Security: Baseline Privacy," p. 74).*

The advent of the DOCSIS standard may prove to be a crucial turning point in the broadband wars between telephone and cable networks. While a shared-media system like cable will always be a less than optimal way to deliver data to homes, MCNS has done a very good job in making cable media as efficient, reliable, and secure as possible. For more information, contact the MCNS group at: *Cable Labs, 400 Centennial Parkway, Louisville, CO 80027; phone (303) 661-9100; fax (303) 661-9199.*

### Rambo's Uzi

Broadcom's first silicon implementation of the DOCSIS standard will surely give rise to a first generation of low-cost, interoperable cable modems. Telco and xDSL advocates should not take this news lightly. Given the aggressive nature of the cable industry, providing them with a standards-compliant MAC chip like the BCM3220 will be like handing Rambo a loaded Uzi.

### Price And Availability

*Available in sample quantities now, the BCM3220 will be in full production during the first quarter of 1998. Pricing for the part is $30 each, in quantities of 10,000.*

*Broadcom Corp., 16251 Laguna Canyon Rd., Irvine, CA 92618; (714) 450-8700; fax (714) 450-8710; Internet: www.broadcom.com.*
**CIRCLE 551**

| How Valuable | Circle |
|---|---|
| Highly | 552 |
| Moderately | 553 |
| Slightly | 554 |