A Study Phase Report on

IEEE 802.11 MAC Chip

By:

Agnish Jain
M.E., Microelectronics-2nd Year
I.I.Sc., Bangalore.

Hemant Parate
M.E., Microelectronics-2nd Year
I.I.Sc., Bangalore.

Under the Guidance of:

Mr. Kuruvilla Varghese
CEDT, I.I.Sc., Bangalore.

Mr. Suresh B. G.
Ittiam Systems Pvt. Ltd., Bangalore.

2003-2004
Center for Electronics Design and Technology
INDIAN INSTITUTE OF SCIENCE
BANGALORE -560012.

&

Ittiam Systems Pvt. Ltd.
BANGALORE -560025.

Contents

1. MOTIVATION 2

2. INTRODUCTION 2

3. THE IEEE 802.11 WIRELESS LAN ARCHITECTURE 2

3.1 BASIC TERMINOLOGIES IN IEEE 802.11 3
3.2 IEEE 802.11 SERVICES 5
3.2.1 Station Services 5
3.2.2 Distribution Services 5
3.3 IEEE 802.11 MEDIA ACCESS CONTROL (MAC) 5
3.4 IEEE 802.11 PHYSICAL LAYER (PHY) 7

4. TECHNICAL SPECIFICATIONS 8

4.1 DEMONSTRATION 8

5. MAC ARCHITECTURE PARTITION 9

6. IMPLEMENTATION BLOCK DIAGRAM 11

7. INTERFACE ARCHITECTURE 12

7.1 HOST TO MAC 12
7.1.1 AMBA 12
7.1.2 PCMCIA 13
7.2 MAC TO PHY 13
7.2.1 MII Bus Interface 13

8. PROJECT TIME PLAN 15

9. CONCLUSION 16

10. REFERENCES 16

11. ACRONYMS AND ABBREVIATIONS 17

1. Motivation

Over the past few years, wireless communications have become increasingly popular. One prime example is the mobile phone. Wireless telephony has been successful since it enables people to connect with each other regardless of locations. This new technology targets computer networking, and now the Internet connectivity is implemented successfully by wireless networking technologies. The most successful so far has been the 802.11 wireless LANs.

In 1997, the IEEE adopted the IEEE 802.11 standard (revised in 1999) for wireless computer communications. The IEEE 802.11 defines two layers, Physical layer (PHY), which specifies the modulation scheme used and signaling characteristics for the transmission through radio frequencies, and the media access control (MAC) layer, which decides how the medium is used.

Advent of this standard created an explosive demand for the devices which implement 802.11 standard that provides mobility to the users. This project is aimed to build such a device, which complies with this standard, and provide the benefits of the standard to the users in demand.

2. Introduction

MAC design includes options such as complete implementation in Hardware or complete implementation in Software or a combination of both. However, such implementations are optimized to meet either of the one of the goals of speed, logic resources, power or area.

In our work, we are dividing the MAC architecture into hardware (which will be embedded along with ASIC RF Baseband and PHY on the NIC card) and software running on the Host Processor. This eliminates the need of a dedicated embedded processor such as ARM for software operations requiring more logic resources higher overall power dissipation. The hardware takes care of the functions, which are time critical. Thus, the proposed design is expected to meet the tradeoffs between speed, logic resources, power or area.

3. The IEEE 802.11 Wireless LAN Architecture

IEEE 802.11 addresses local area networking where the MAC conformant devices use the air as a medium to communicate with other MAC conformant devices (stations) those are within close proximity to each other. This report provides an overview of the 802.11 architecture and the different topologies incorporated to accommodate the unique characteristics of the IEEE 802.11 wireless LAN standard. In addition, the report contains the design technique, partitioning of architecture into hardware and software

based on time critical functions and functions which are complex to implement in hardware. The standard is similar in most respects to the IEEE 802.3 Ethernet standard. Specifically, the 802.11 standard addresses-

1. Functions required for an 802.11 compliant device either to operate in a peer-to-peer fashion or integrated with an existing wired LAN
2. Operation of the 802.11 device within possibly overlapping 802.11 wireless LANs and the mobility of this device between multiple wireless LANs
3. MAC level access control and data delivery services to allow upper layers of the 802.11 networks
4. Several physical layer signaling techniques and interfaces
5. Privacy and security of user data being transferred over the wireless media

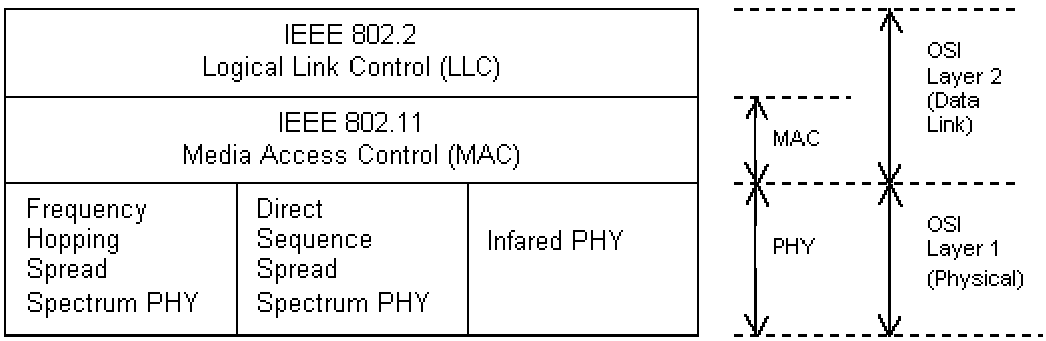


Figure 3.1 - IEEE 802.11 standards mapped to the OSI reference model.

The 802.11 architecture is comprised of several components and services that interact to provide station mobility transparent to the higher layers of the network stack.

3.1 Basic Terminologies in IEEE 802.11

3.1.1 Wireless LAN Station

The station (STA) is the most basic component of the wireless network. A station is any device that contains the functionality of the 802.11 protocol, that being MAC, PHY, and a connection to the wireless media.

3.1.2 Basic Service Set (BSS)

802.11 define the Basic Service Set (BSS) as the basic building block of an 802.11 wireless LAN. The BSS consists of a group of any number of stations.

3.1.3 Independent Basic Service Set (IBSS)

An IBSS is a set of the mobile stations, which have recognized each other. They are connected via the wireless media in a peer-to-peer fashion to communicate directly with each other. This is also called as ad-hoc network and shown in figure 3.2.

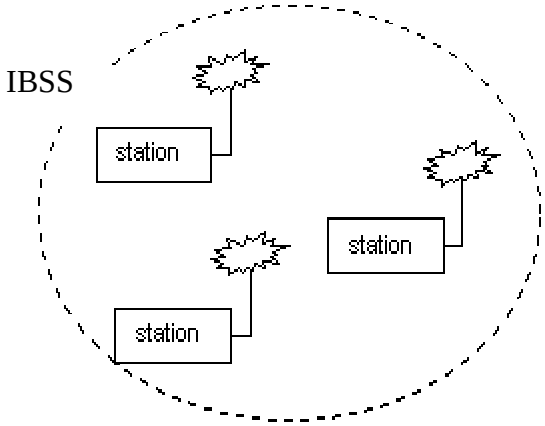


Figure3.2 - Independent Basic Service Set (IBSS)

3.1.4 Access Point (AP)

The access point provides a local relay function for the BSS

3.1.5 Infrastructure Basic Service Set

An Infrastructure Basic Service Set is a BSS with an Access Point (AP). The access point also provides connection to a distribution system.

3.1.6 Distribution System (DS)

The distribution system (DS) is the means by which an access point communicates with another access point to exchange frames for stations in their respective BSSs.

3.1.7 Extended Service Set (ESS)

An extended service set is a set of infrastructure BSSs, where the access points communicate amongst themselves, through the distribution system, to forward traffic from one BSS to another to facilitate movement of stations between BSSs. shown in figure 3.3

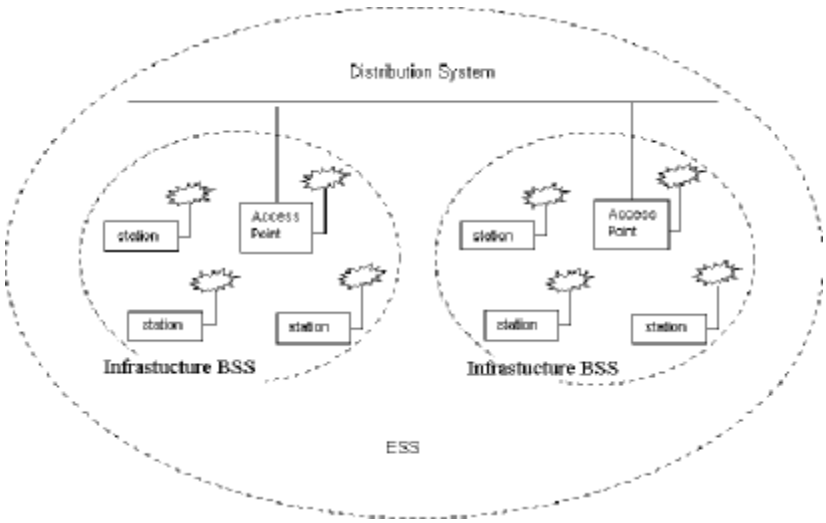


Figure 3.3 - Extended Service Set (ESS) and Infrastructure BSS

3.2 IEEE 802.11 Services

3.2.1 Station Services

- Authentication
  - Open System
  - Shared key
- De-Authentication
- Privacy
- Data Delivery

3.2.2 Distribution Services

- Association
- Re- Association
- Disassociation
- Distribution
- Integration

3.3 IEEE 802.11 Media Access Control (MAC)

1. MAC layer provides functionality to allow reliable data delivery for the upper layers over the wireless PHY media. The data delivery itself is based on an asynchronous, best-effort, connectionless delivery of MAC layer data. There is no guarantee that the frames will be delivered successfully.
2. The 802.11 MAC provides a controlled access method to the shared wireless media called Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA).
3. Protect the data being delivered by providing security and privacy services. Security is provided by the authentication services and by Wireless Equivalent Privacy (WEP), which is an encryption service for data delivered on the WLAN.

3.3.1 CSMA/CA

It Works by a "listen before talk scheme". This means that a station wishing to transmit must first sense the radio channel to determine if another station is transmitting. If the medium is not busy, the transmission may proceed.

Carrier sensing is done by physical and virtual carrier sense mechanism. In physical carrier sense mechanism inter frame spacing (IFS) is used. There are four types of the inter- frame spacing time intervals (in order of time interval)–

1. Short IFS (SIFS) - This is the shortest one.
2. PCF IFS (PIFS) - Used in Point Coordination Function
3. DCF IFS (DIFS)- Used in distributed Coordination Function
4. Extended IFS (EIFS)- it is the longest.

The priority level is highest for SIFS and lowest for EIFS. The following figure shows the relations between the four Inter-frame spaces.

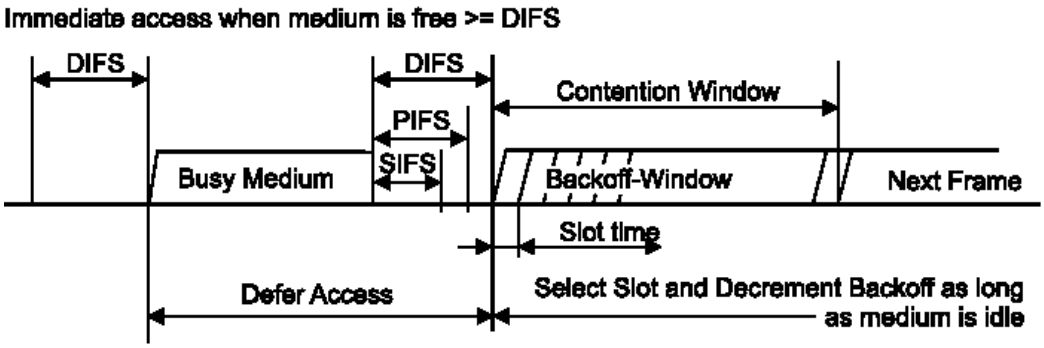


Figure 3.4 Basic access method for node

There are two medium access control schemes in the IEEE 802.11 standard-

3.3.2 Distributed Coordination Function (DCF)

DCF is contention-based scheme and based on two mechanisms i.e. CSMA/CA and random backoff. In DCF, the frame exchange is done using two methods - Minimal frame exchange i.e. two frames and Four-frame exchange.

The problem with the Two frame exchange method is the Hidden node Problem, which is solved by the RTS and CTS frames used in Four frame exchange method. If the collision occurred in the medium, the nodes enter the backoff state. The backoff process is shown in figure below-

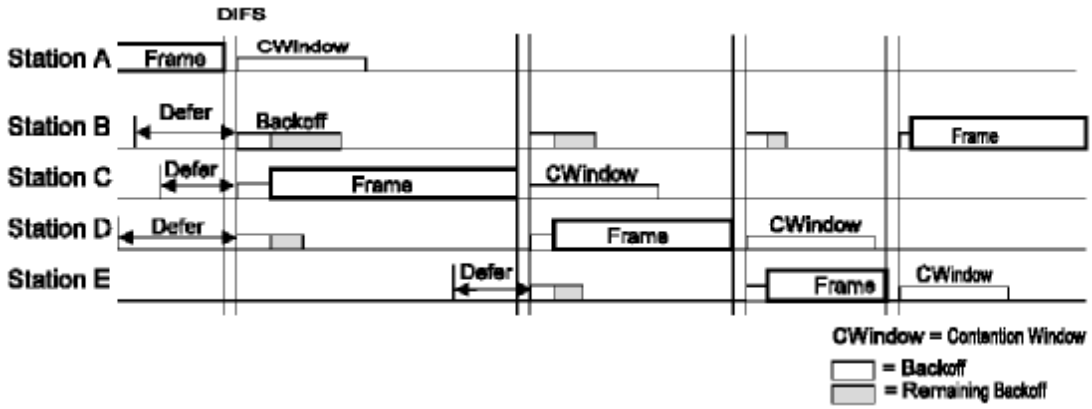


Figure 3.5 Backoff procedure

3.3.3 Point Coordination Function (PCF)

PCF is used for contention free or polling based frame transfer. The essential part of PCF is the Point Coordinator (PC), which should reside in the AP. Frame transfer is centrally controlled by PC. It does not use RTS/CTS in CF period.

3.4 IEEE 802.11 Physical Layer (PHY)

The 802.11 physical layer (PHY) is the interface between the MAC and the wireless media where frames are transmitted and received. The PHY provides three functions, an interface to exchange frames with the upper MAC layer for transmission and reception of data, it uses signal carrier and spread spectrum modulation to transmit data frames over the media, and provides a carrier sense indication back to the MAC to verify activity on the media.

802.11 provides three different PHY definitions: Both *Frequency Hopping Spread Spectrum* (FHSS) and *Direct Sequence Spread Spectrum* (DSSS) support 1 and 2 Mbps data rates. An extension to the 802.11 architecture, 802.11a defines different multiplexing techniques that can achieve data rates up to 54 Mbps. Another extension to the standard; 802.11b defines 11 Mbps and 5.5 Mbps data rates, in addition to the 1 and 2Mbps rates, utilizing an extension to DSSS called High Rate DSSS (HR/DSSS). 802.11b also defines a rate shifting technique where 11 Mbps networks may fall back to 5.5 Mbps, 2 Mbps, or 1 Mps under noisy conditions or to inter-operate with legacy 802.11 PHY layers.

3.4.1 Spread Spectrum

Spread spectrum is a technique trading bandwidth for reliability. The goal is to use more bandwidth than the system really needs transmission to reduce the impact of localized interference on the media. Spread spectrum spreads the transmitted bandwidth of the resulting signal, reducing the peak power but keeping total power the same.

3.4.2 Frequency Hopping Spread Spectrum (FHSS)

Frequency Hopping utilizes a set of narrow channels and "hops" through all of them in a predetermined sequence. For example, the 2.4 GHz frequency band is divided into 70 channels of 1 MHz each. Every 20 to 400 msec the system "hops" to a new channel following a predetermined cyclic pattern. The 802.11 Frequency Hopping Spread Spectrum (FHSS) PHY uses the 2.4 GHz radio frequency band, operating with at 1 or 2 Mbps data rate.

3.4.3 Direct Sequence Spread Spectrum (DSSS)

The principle of *Direct Sequence* is to spread a signal on a larger frequency band by multiplexing it with a signature or code to minimize localized interference and background noise. To spread the signal, each bit is modulated by a code. In the receiver, the original signal is recovered by receiving the whole spread channel and demodulating with the same code used by the transmitter. The 802.11 *Direct Sequence Spread Spectrum* (DSSS) PHY also uses the 2.4 GHz radio frequency band.

3.4.4 Infrared (IR)

The Infrared PHY utilizes infrared light to transmit binary data either at 1 Mbps (basic access rate) or 2 Mbps (enhanced access rate) using a specific modulation technique for each. For 1 Mbps, the infrared PHY uses a 16-pulse position modulation (PPM). The concept of PPM is to vary the position of a pulse to represent different binary symbols. Infrared transmission at 2 Mbps utilizes a 4 PPM modulation technique.

4. Technical Specifications

The specifications are listed below

- Fully compliant to IEEE 802.11 Standard 1999
- Timing Synchronization algorithms
- Compatible with IEEE 802.11 a/b/g, PHY (BB)
- Support for all LLC like SNAP and HDLC
- Complete system featuring dedicated hardware and software
- Flexible design to allows upgrade for 802.11e QoS and 802.11i Security provision
- Portable STA or AP
- Both IBSS (Ad-hoc networks) and Infrastructure network support
- DCF & PCF (optional) operation
- Power Management & control and WEP encryption
- Interface to allows simple bridging to a range of host interfaces
- Verilog HDL source code
- Synthesis and test scripts
- Test vectors & test benches
- Simulation and synthesis reports, user and reference manuals
- High quality design documentation that includes
    1. Hardware architecture Document
    2. Programming guide
    3. Design document
- Fully synthesizable and optimized for low gate count
- Considerations for easy ASIC integration

4.1 Demonstration

There are many ways to demonstrate the project, one such scenario is we can connect the MAC+PHY platform with the MAC implemented by us and existing PHY to a host such as PC, Laptop and demonstrate FTP (File Transfer Protocol). Another way, as suggested in feedback, a procedure in which Processors like MPC860 can be used for forwarding the packets to the hardware.

5. MAC Architecture Partition

The MAC architecture is to be partitioned in Hardware and Software. The criteria behind this partition is higher performance (time critical functions) and lower logic resource functions to be embedded into hardware whereas the one's which requires large logic and infrequently used and less time critical are to be implemented into software.

1. Dedicated Counters for Interframe Spacing
   Hardware
2. Random/ Exponential Back off Algorithm. + NAV Counter.
   Hardware
3. Virtual (+ PHY) carrier Sensing Module
   Hardware
4. CRC and Checksum generator Polynomial and division
   Hardware
5. WEP Encryption and Decryption Module.
   Hardware
   Description: IV + ICV + CRC. Corresponding decryption at reception of secure frame
6. Header Generator Module
   Software
   Description: it collects fields from different modules and pads them together.
7. Data receiving module from LLC
   Software
   Description: It takes the data, calculates the byte length and generates duration field to be used in the header.
8. Frame transmitter module to the PHY
   Hardware
   Description: this will include the header +Actual Data + CRC.
9. Data transmitter module to LLC
   Software
10. Frame receiving module from PHY
    Hardware
    Description: it splits the frame header, actual data and CRC and delivers it to their corresponding modules.
11. RTS threshold, Frame threshold and Sequence Control generator.
    Software
    Description: it decides whether to invoke control frames prior to actual data transmission and whether (fragmentation) needs to be done. It is also responsible for retransmissions if any needs to be done. Actually there will be sub-modules for each of the task to be performed, which will interact with each other.
12. Management Frame Module
    a) Software
    Authentication request, (Algo. No., Seq. no.)
    Association Req. and Reassociation req.,
    AID allotment, SSID

Compatibility information Module (generate this filed depending on the hardware supported)

b) Hardware

Probe Request, Probe Response, Timestamp, Beacon Interval, Passive Scanning

13. MLME, MIB & Station Management Entity (SME)

Software

14. Address Field Module

Software

Description: decides about RA, TA, DA, SA, BSSID etc. by interacting different Modules.

15. Control frame Module

Hardware

Description: responsible for the generation of RTS, listen to RTS, generation of CTS and listen to CTS.

16. Baseband Information Module

Hardware

Description: In some of the management fields the baseband information of DSSS/FH is transmitted.

17. Power Management Module **Hardware (partly in Software)**

Description: Responsible for attributes such as PS Poll, Sleeping interval, listen to TIM generate TIM.

18. Transmitter and Receiver State Machine

Hardware

Description: it invokes the module as par the functionality and is responsible for synchronizing between different modules of the architecture.

19. Receive FIFO and Transmit FIFO

Hardware

20. Beacon frame generator and Monitoring

Hardware

Description: collects all the fields required to be transmitted in the beacon and interprets the incoming beacon frame.

21. IBSS features support. **Hardware (partly in Software)**

Description: provides functions in addition to the operations required in the infrastructure BSS.

22. B/cast and M/cast frame delivery Module

Hardware

(Operation in sync with Beacon frame module)

23. Distribution System Services (DSS) Support

Software

24. Timer Synchronization Function

Hardware

25. Registers for various parameters

Hardware

e.g., RTS Threshold, Basic Rate (Mandatory), Beacon interval etc.

26. DPRAM inbuilt in FPGA as per the requirements. **Hardware**

6. Implementation Block Diagram

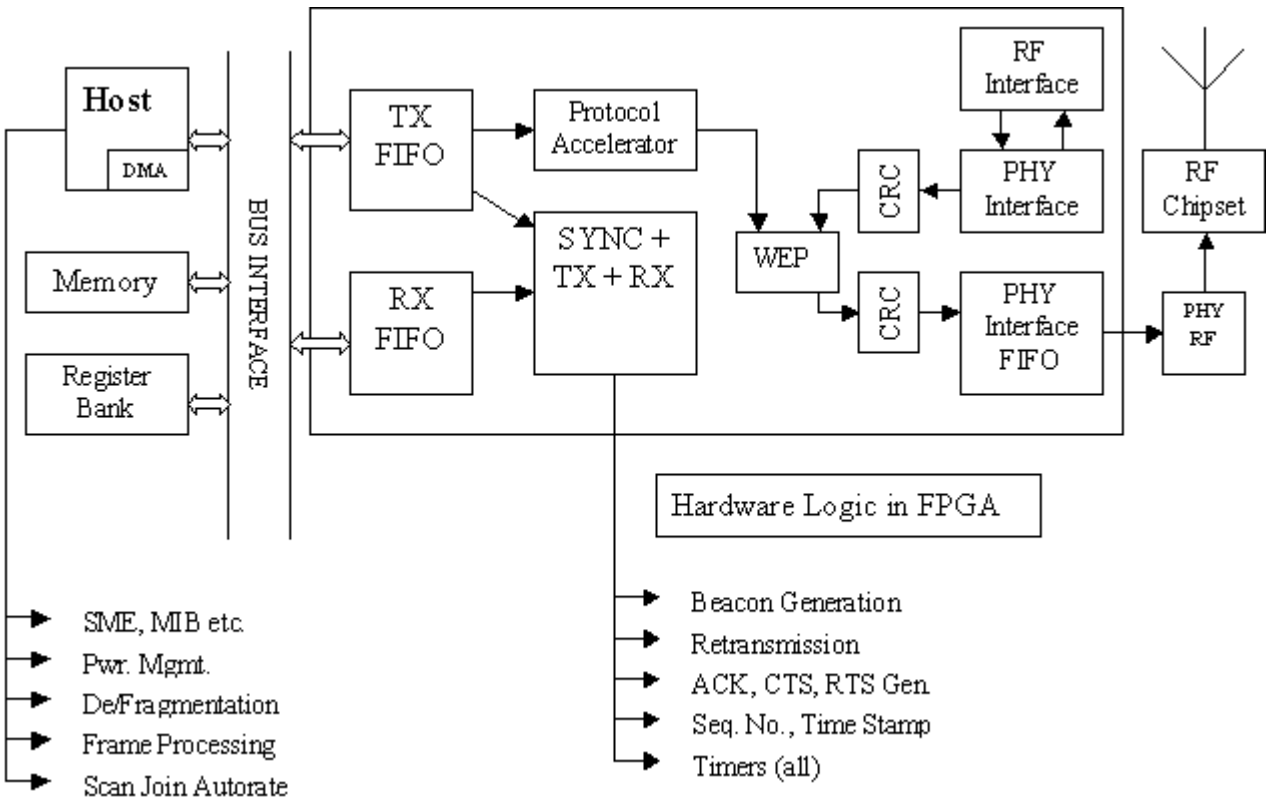


Figure 6.1-block diagram of MAC chip

As we have mentioned above, the complete architecture need to be divided into hardware in an FPGA and partly in host software. As mentioned in section 5, the functionalities are transferred on HOST and FPGA blocks, which is shown in figure above. The bus interface shown on left hand side is used for the HOST to MAC interface. In addition, there is a PHY to MAC interface, which enables us to make the MAC layer media independent. Both the interfaces are explained briefly in section 7 below. The main objective of the interfaces is to satisfy the following requirements-

1. To encourage *modular system design* to improve processor independence, providing a development road-map for advanced cached CPU cores and the development of peripheral libraries
2. To minimize the silicon infrastructure required supporting efficient on-chip and off-chip communication for both operation and manufacturing test.

7. Interface Architecture

The interface architecture for communication from either way is to be designed using following standard bus architecture:

7.1 HOST to MAC

7.1.1 AMBA

An AMBA-based microcontroller consists of a high-performance system *backbone* bus (AMBA AHB or AMBA ASB), able to sustain the external memory bandwidth, on which the CPU, on-chip memory and other *Direct Memory Access* (DMA) devices reside. This bus provides a high-bandwidth interface between the elements that are involved in the majority of transfers. Also located on the high performance bus is a bridge to the lower bandwidth APB, where most of the peripheral devices in the system are located (see Figure 7-1).

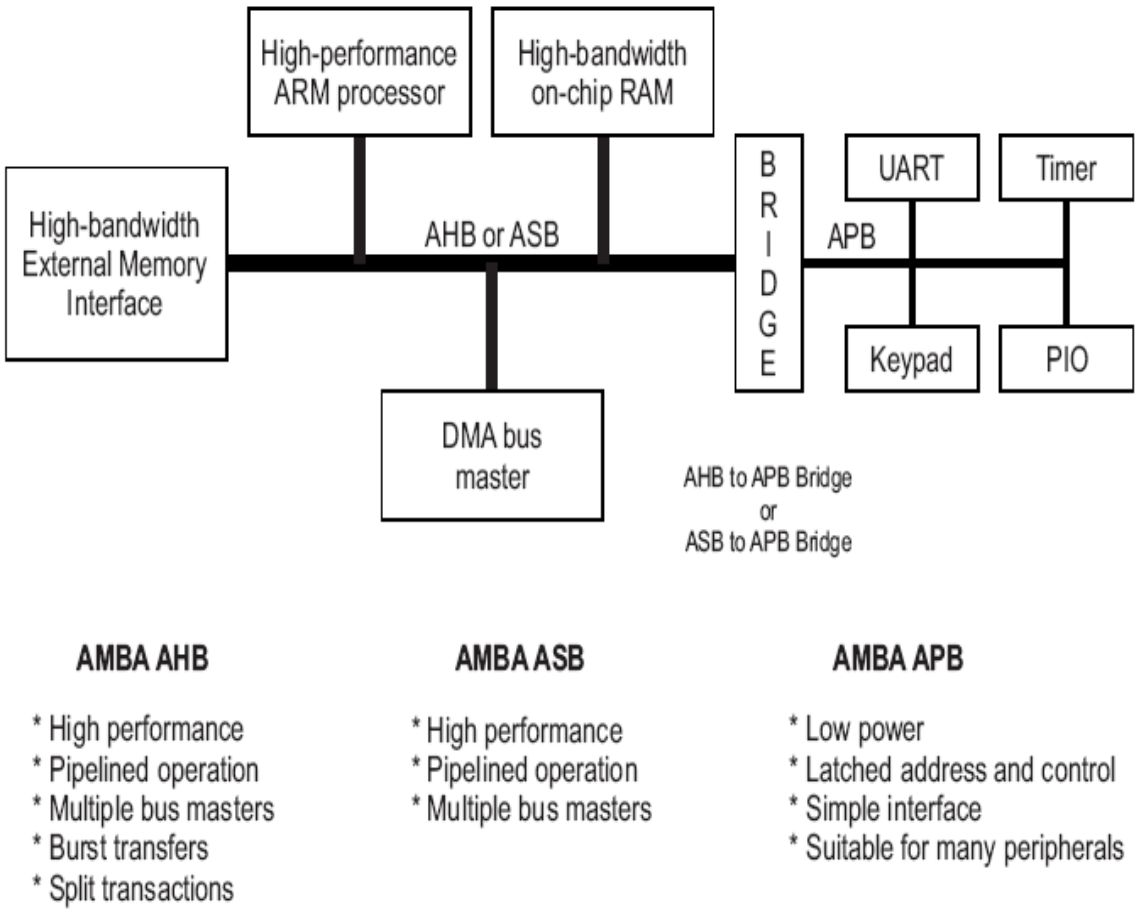


Figure 7.1 AMBA bus Block diagram representation

AMBA APB provides the basic peripheral macro cell communications infrastructure as a secondary bus from the higher bandwidth pipelined main system bus. Such peripherals typically:

1. Have interfaces, which are memory-mapped registers

2. Have no high-bandwidth interfaces
3. Are accessed under program control.

The external memory interface is application-specific and may only have a narrow data path, but may also support a test access mode, which allows the internal AMBA AHB, ASB, and APB modules to be tested in isolation with system-independent test sets.

7.1.2 PCMCIA

For maximum flexibility in address size, address location and access time, the PCMCIA module is implemented with the Address Selectors Modules separate from the PCMCIA module. Two Address Selectors Modules are required, one for the PCMCIA socket and one for the control and status registers. While the Address Selector module for the control and status registers is one byte, the Address Selector module for the PCMCIA socket can be 2 or 4 megabytes. Furthermore, the PCMCIA socket access time can vary between 100ns to 250ns depending of the PCMCIA card. One to four wait states may be required to access the PCMCIA socket depending on the PCMCIA card in use and the clock speed of the E5. One of the wait states may be selected in the Address Selector module. For additional wait states, Wait Control module available in the FastChip IP Module Library need to be used.

7.2 MAC to PHY

7.2.1 MII Bus Interface

The Media Independent Interface (MII) is an 18 wire MAC/PHY interface described in IEEE 802.3u. The purpose of the interface is to allow MAC layer devices to attach to a variety of PHY through a common interface. MII operates at either 100 Mbps or 10 Mbps, depending on the speed of the Physical Layer. The internal registers of a PHY are accessible only through the MII 2-wire Serial Management Interface with the signals MDC (MII management Data Clock) and MDIO (MII management Data Input/Output). PHY Interface Register (PIR) provides a means of accessing PHY internal registers via the MII. MDC is clock to latch the IO data and instructions for PHY. MDIO is bi-directional connection used to write instruction and data to and read data from the PHY.

Gigabit Media Independent Interface (GMII) is an extension to MII used in Fast Ethernet. GMII uses the same management interface as MII and supports 10, 100 and 1000 Mbps data rates. GMII provides separate 8-bit wide receive and transmit data paths, so it can support both full- and half-duplex operational modes. The various layers of the Gigabit Ethernet protocol architecture are shown in Figure 7.2 below.

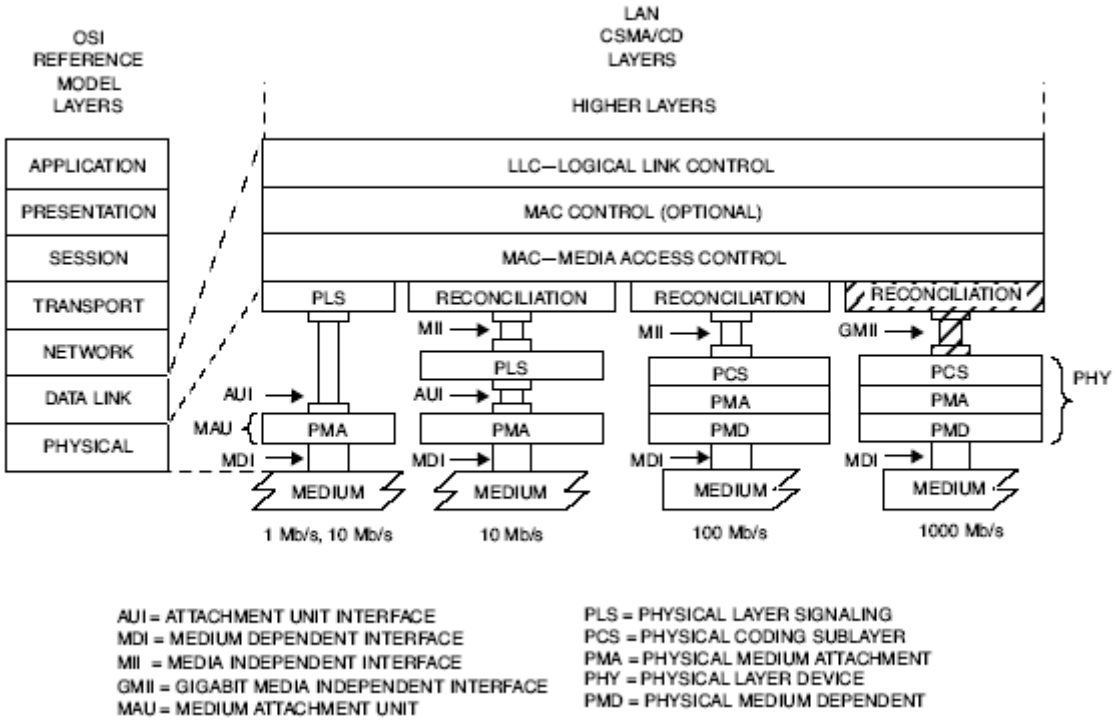
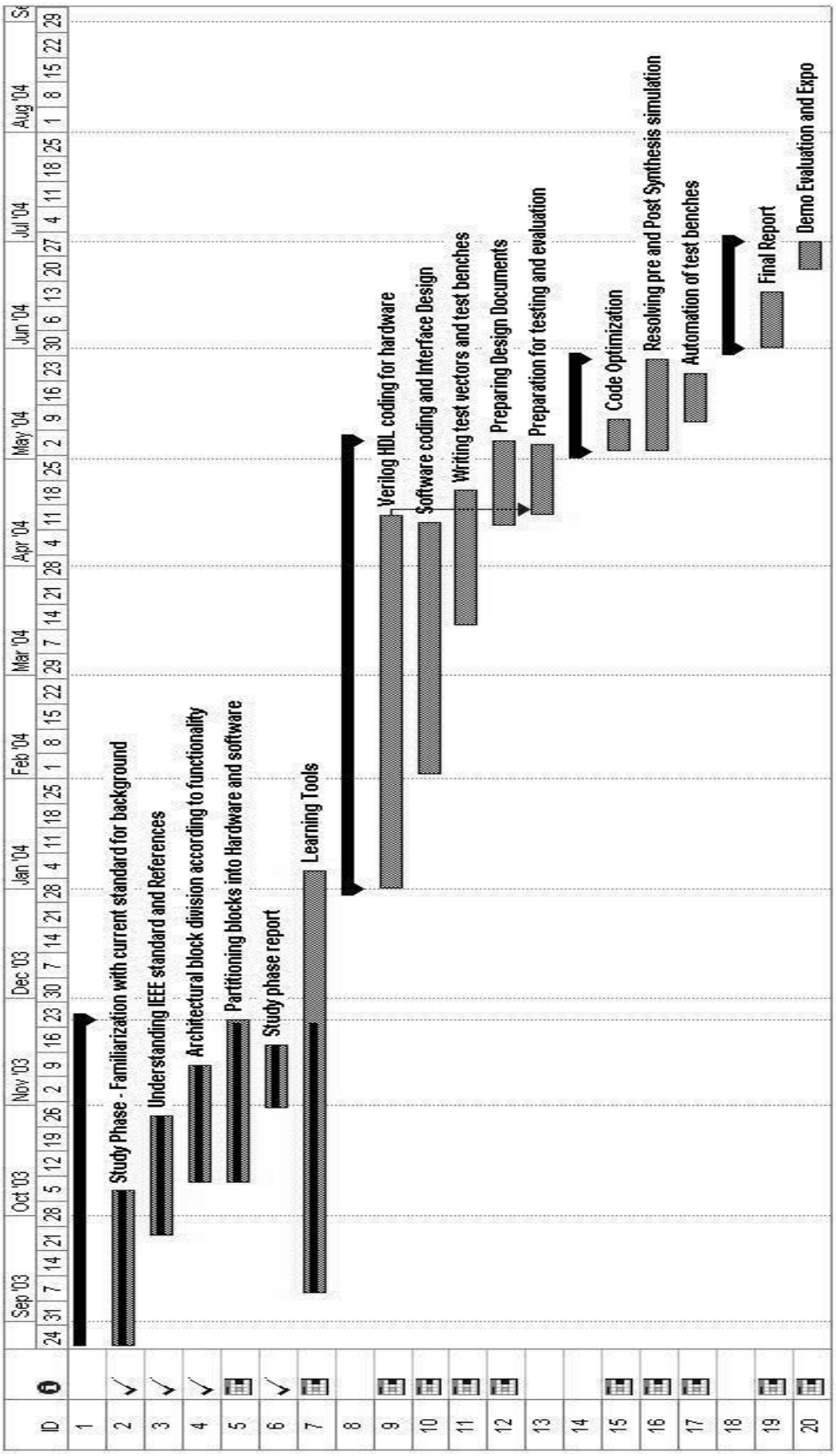


Figure 7.2 MII and GMII in OSI protocol stack

The MII and GMII are IEEE standards and proven, well behaved from a PCB timing perspective, and is low risk choice for interfacing to proven MACs and controllers. However there are few more interfaces, developed by HP, Cicada (Reduced GMII), Cisco (serial GMII), which are with the reduced pin-count to very large extent.

8. Project Time Plan



9. Conclusion

The project goals and deliverables have been well understood during the study phase. Technical specifications have been formulated as per the requirements of the project, the. The MAC architecture is to be implemented in hardware on a NIC card and Software running on Host System.

The focus of the work is the partition of the design in to hardware and software components and designing the hardware targeting Altera FPGA. The environment used would be Altera Quartus II for Synthesis, and Place and Route and, ModelSim for Simulations. The coding would be done in Verilog.

The interface to the device driver needs to be designed. The Host to MAC interface between Host system and the Mac chip, and the MAC to PHY interface between the Mac chip and the RF baseband chip are also to be implemented.

10. References

1. ANSI/IEEE Std 802.11, 1999 Edition.
2. 802.11 WLAN A Perspective Guide By: Mathew S. Gast.
3. PCMCIA System Architecture Second Edition, MindShare, Inc. Don Anderson.
4. AMBA Specification (Rev 2.0) from ARM
5. Ittiam Systems Internal Documents.
6. Performance Analysis of the IEEE 802.11 MAC Protocol, Chuan Heng Foh and Moshe Zukerman ARC Special Research Center for Ultra–Broadband Information Networks EEE Department, The University of Melbourne Parkville, Vic. 3010, Australia
7. Weaknesses in the Key Scheduling Algorithm of RC4 Scott Fluhrer, Itsik Mantin, and Adi Shamir Cisco Systems, Inc.,

11. Acronyms and Abbreviations

ACK:	acknowledgment frame
AP:	access point
BSS:	basic service set
BSSID:	basic service set identifier
CF-End:	contention-free end
CFP:	contention-free period
CF-Poll:	contention-free poll
CSMA/CA:	carrier sense multiple access with collision avoidance
CTS:	clear to send
DCF:	distributed coordination function
DIFS:	distributed interframe space
DS:	distribution system
EIFS:	extended interframe space
ESS:	extended service set
FCS:	frame check sequence
IBSS:	independent basic service set
ICV:	integrity check value
LLC:	logical link control
MAC:	medium access control
MIB:	management information base
MPDU:	MAC protocol data unit
MSDU:	MAC service data unit
NAV:	network allocation vector
PC:	point coordinator
PCF:	point coordination function
PHY:	physical, physical layer
PIFS:	priority interframe space
RTS:	request to send
SIFS:	short interframe space
SSID:	Service set identity
STA:	Station
WLAN:	wireless LAN