Model SS45M-D

Model Super Sonic 45 Motherboard- Design

By

Barry L. Crouse

Introduction

Today is 11/05/2011 University Place, Washington. I would like to thank you for taking the time reading this scientific work. I have attempted to build upon the SS34M-D motherboard design by making and improving the design and employing some of the previous U.S. Copyrights registered for the purpose of taking theory's I have written and creating practical visual application to new theory's.

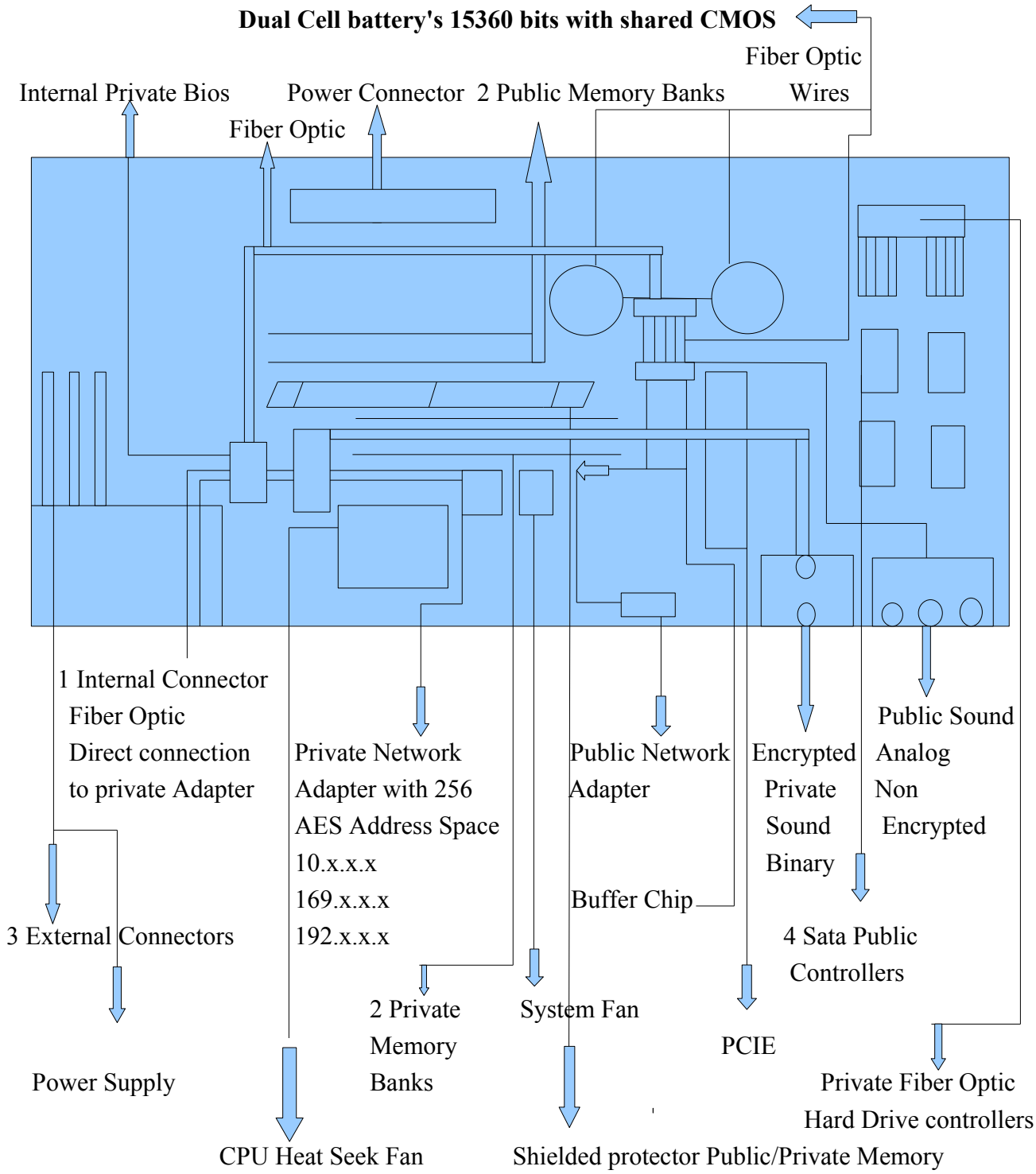
The Theory's I have written in my previous copyrights needed a answer as to how can a theory be made useful in everyday lives. Complex Theory, Design, and development is much like a ladder it takes gradual steps to arrive at a solution. I hope that if you have read my previous works you will find that in this paper some of the previous works being demonstrated such as Thoughts on Rotating Black Holes, OSI theoretical discussion, Visual Arts Equations, Temporal Spatial Equations, Visual Non-Symmetrical String Application Design and other works as a example that answers the question above. I want to take the time to thank you once again for reading and studying this paper.

The New Design feature's include the following improvements

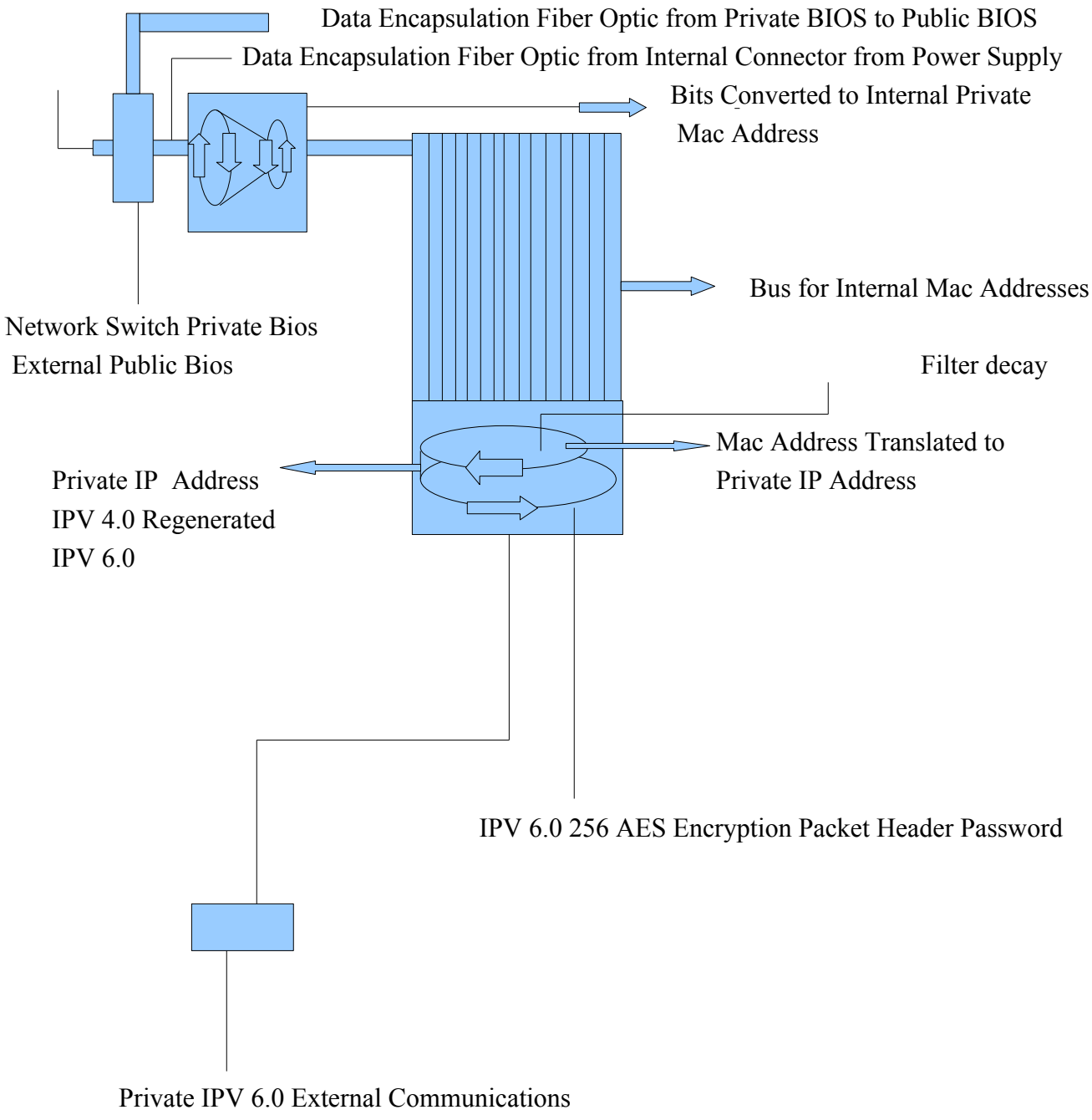
1). Private Sound Digital Binary Encrypted Format
2). Public Sound Analog Non Encrypted Format
3). Encrypted File Systems Private and Public
4).256 AES Bit Encryption Private Network Adapter

Model SS45 M-D

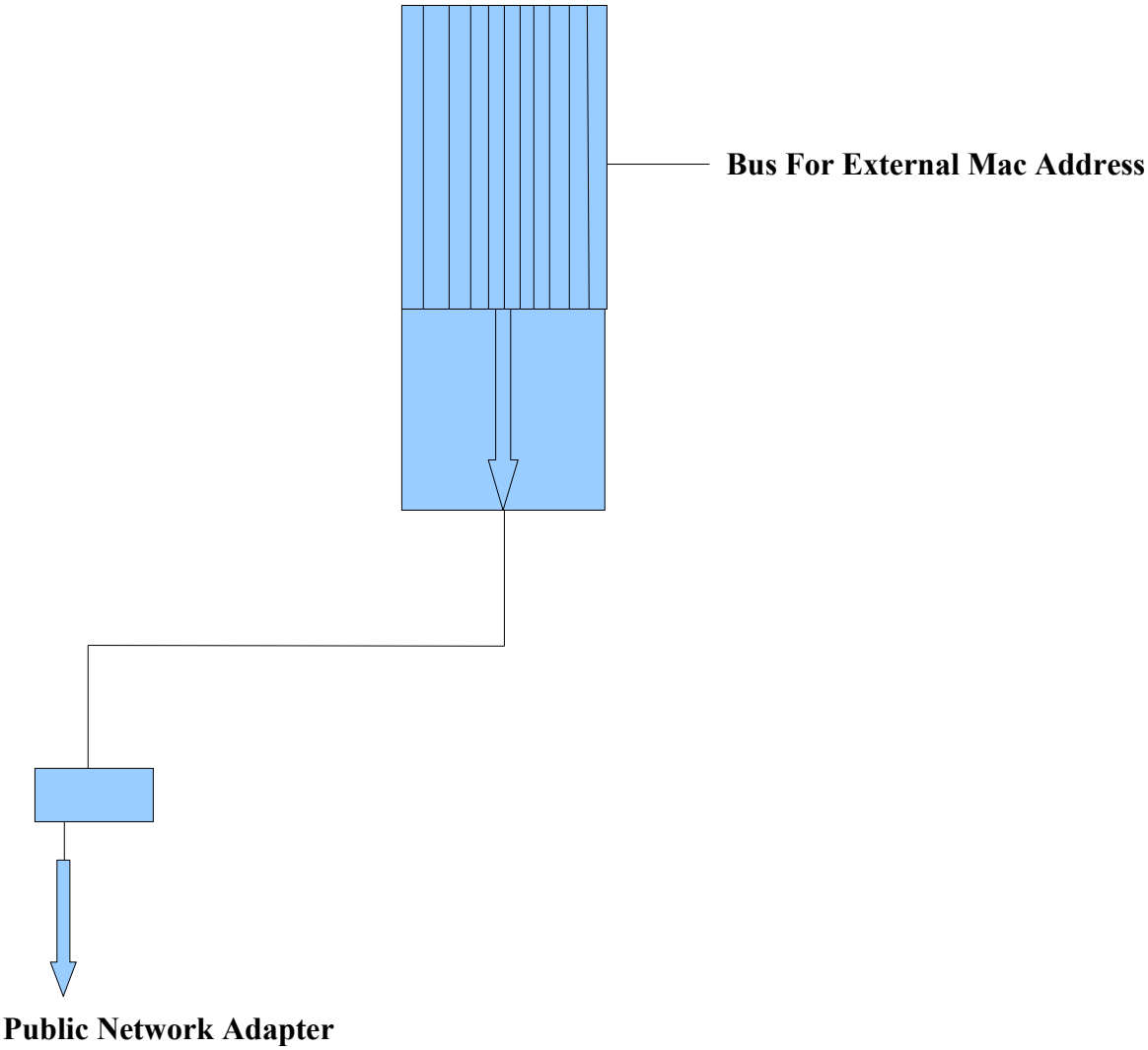
Model Super Sonic 45 Motherboard- Design



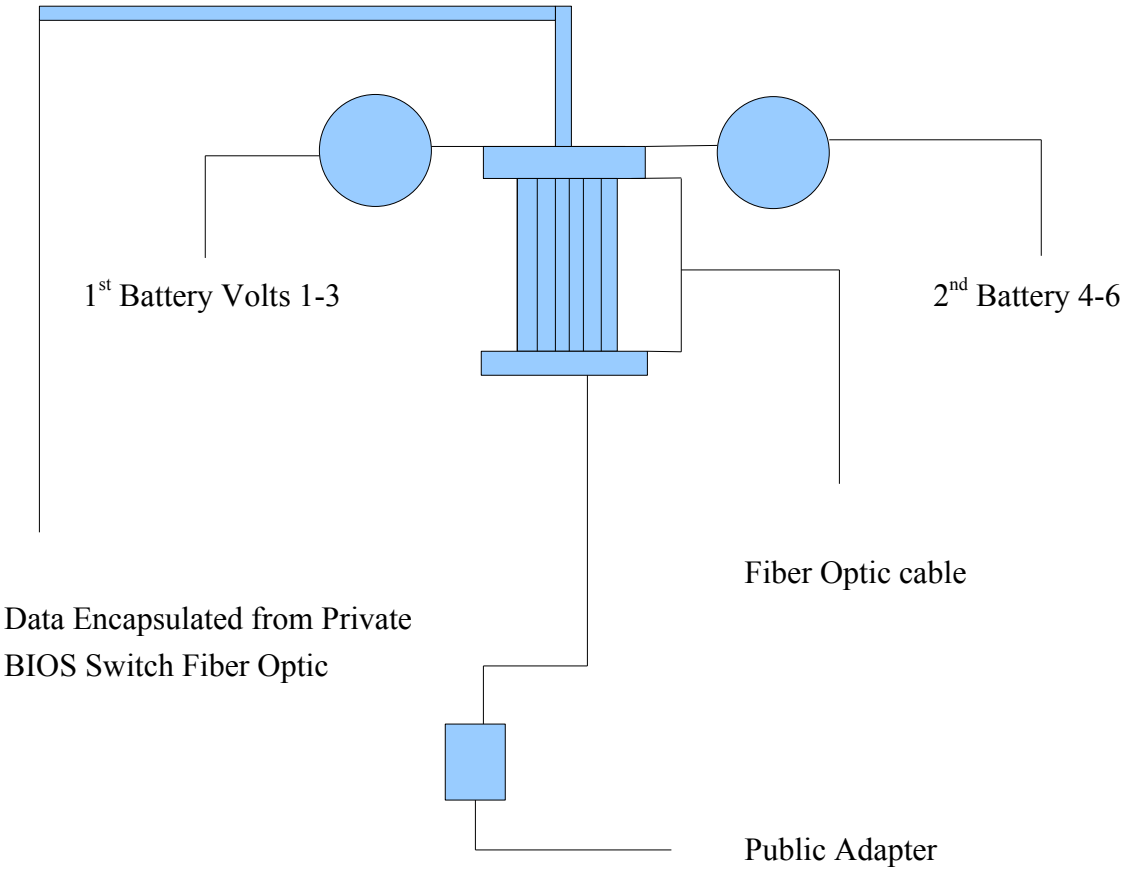
Internal Private Switch



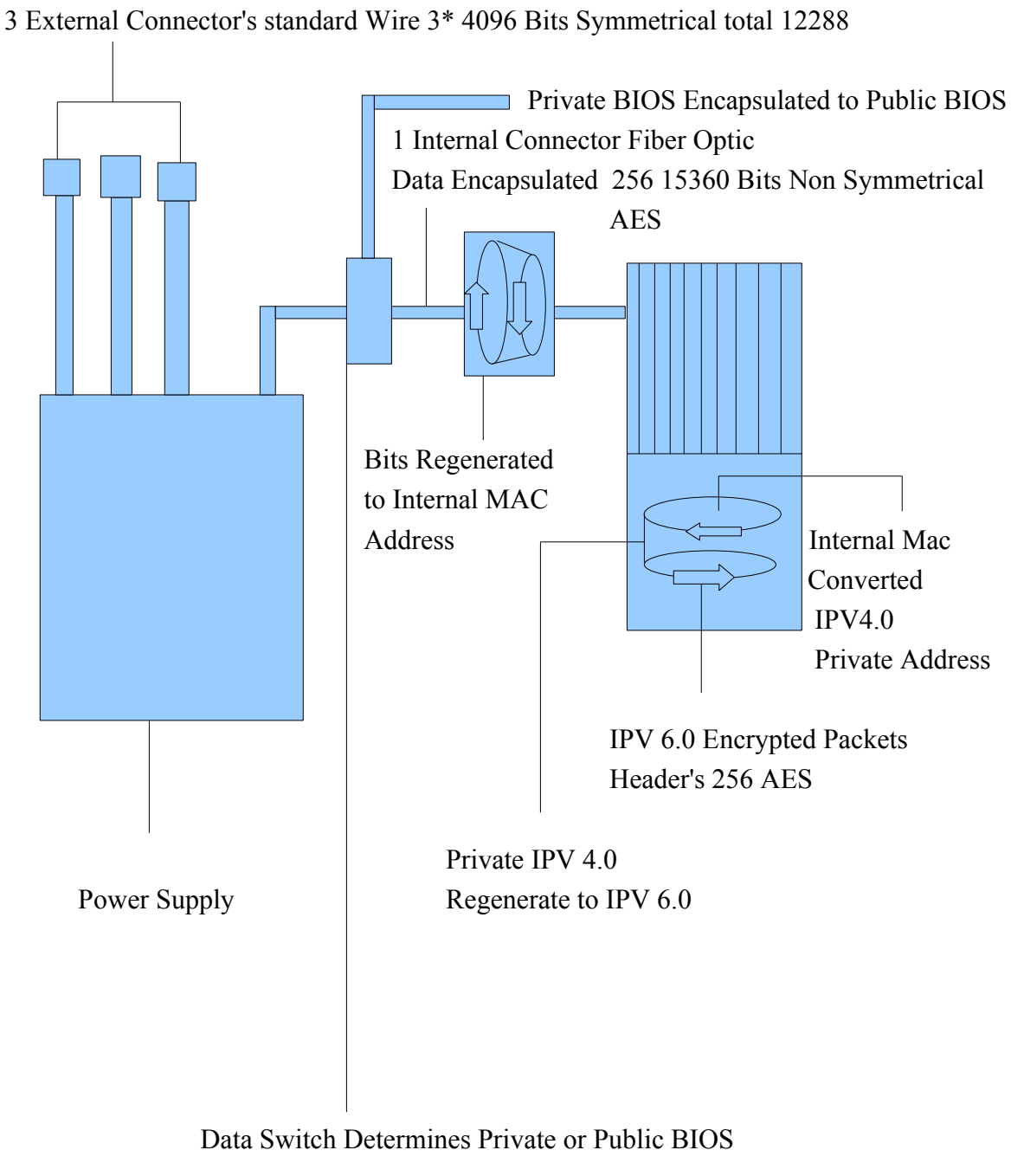
Internal Public Switch IPV 4.0



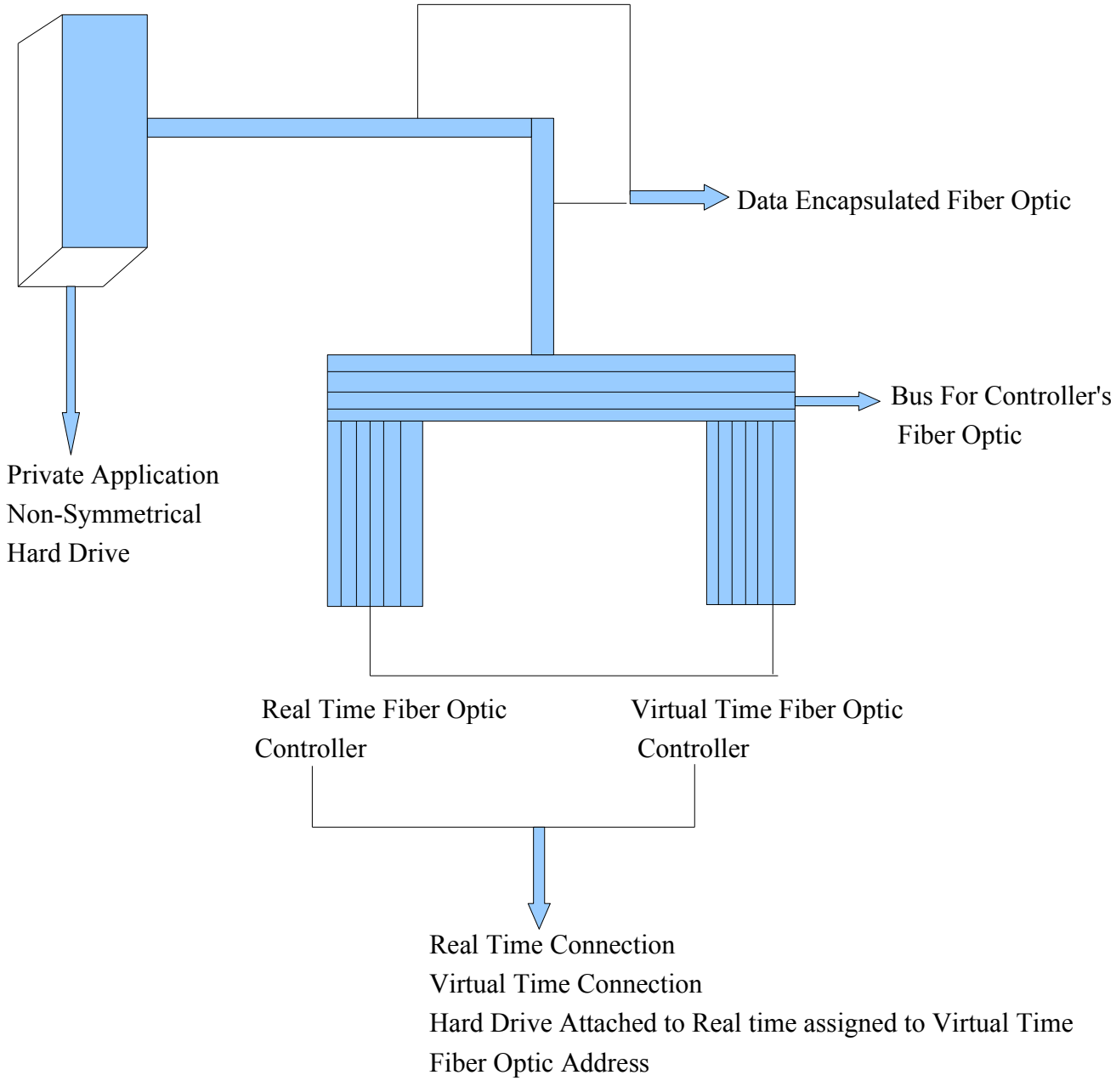
Dual Cell battery's 15360 bits with shared External CMOS



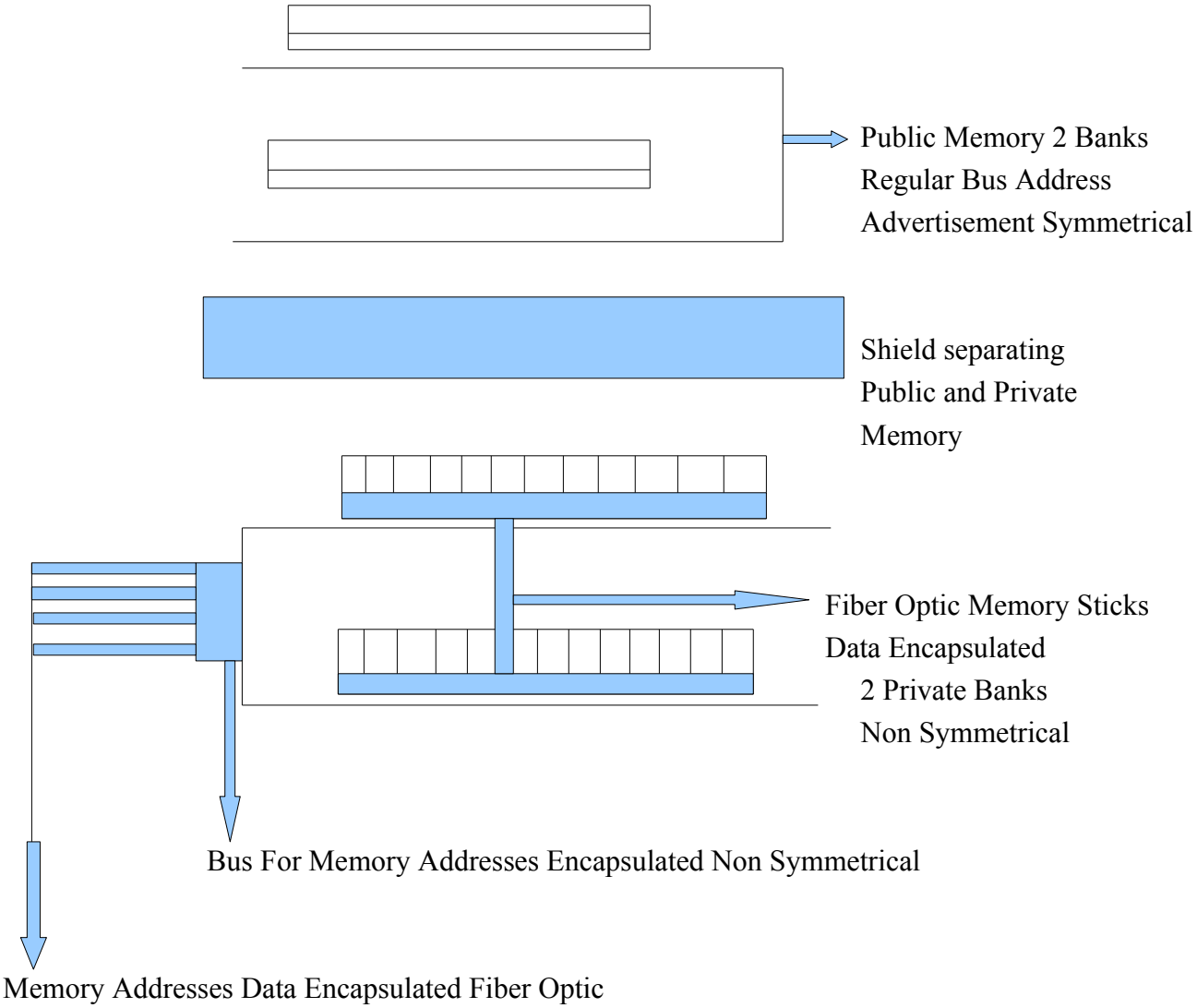
Power Supply



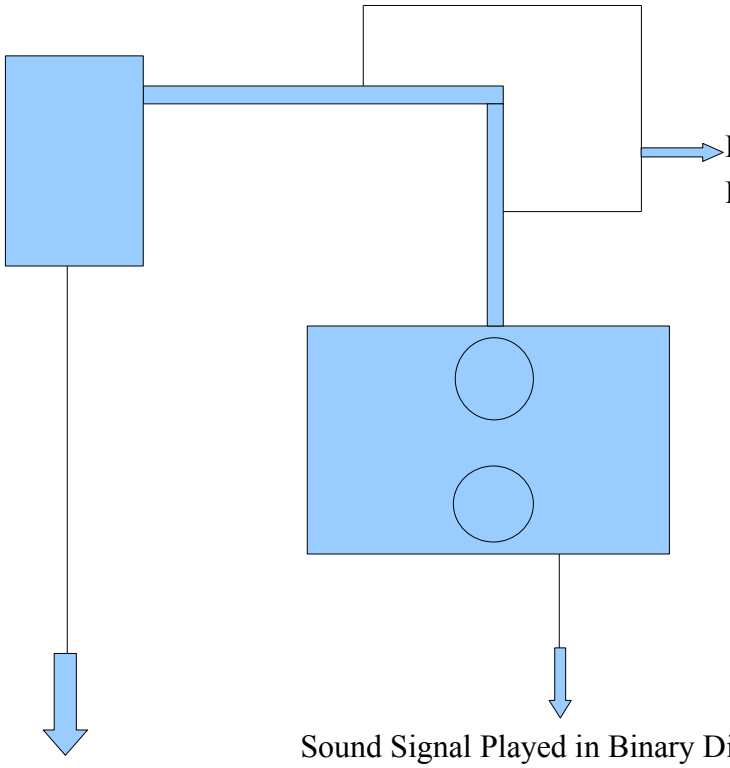
Private Hard Drive and Non Symmetrical Fiber Optic Controller's



Private Non Symmetrical and Public Symmetrical Memory



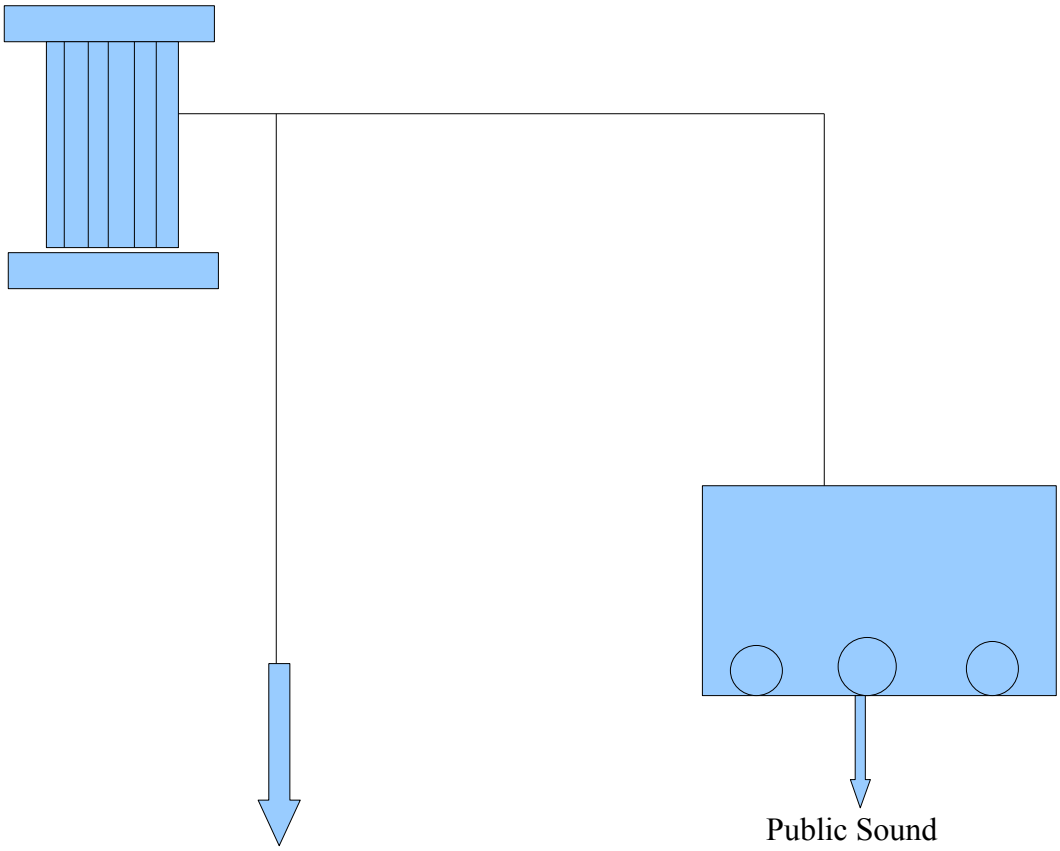
Private Sound Binary Digital Based Encrypted



Sound Signal Played in Binary Digital Encrypted Format

BIOS Encapsulated
From Private Switch
Data Encapsulated
In Binary Digital Format
Encrypted

Public Sound Analog Based Non Encrypted



Sound loaded from Public
Bios and Mac Address

Public Sound
Analog Based
Non Encrypted

Processing Features of SS45M-D Design

The Power Supply has a Fiber Optic Cable that employs Data Encapsulation thus it prevents less bit decay and promotes data security in a Internal Environment. The next step is it goes to a Data Switch requesting either a Private or a Public Bios. If it goes to the Public Bios the Data is encapsulated via Fiber Optic to prevent external environmental corruption it than proceeds with normal symmetrical processing which is Public Address spaces. If it goes to the private Bios, The file system is encrypted Than it goes through a Rotating Black hole taking charged particles volts and Regenerating from Bits to a Internal Mac Address . Addresses are loaded from Private Memory Banks that are Non-Symmetrical and Applications are accessed from a Private Hard-Drive that is also Data Encapsulated. A Random Encrypted 256 AES key is generated to send the Private BIOS to the Private Hard drive this unlocks the harddrive's applications,objects, and file system.

1. Private Encrypted Private BIOS Key must = Private Hard drive for access
2. Public Non-Encrypted. Public BIOS = Public Hard drive

Please note This is critical because Network Security involves managing objects, file's and Property rights by defining what is Private and Public this will enhance IT security by keeping Public Applications, file's and objects non-accessible to Private Administration by defining the processes as symmetrical and Non Symmetrical, File systems Encrypted and Non-Encrypted.

In previous works, I have basically shown When Hardware and Software from a System standpoint is to be loaded with Security and Privacy feature's. I am now attempting to create a Dynamic environment by showing Devices to be Dynamic by creating instant creation of Environments by Intelligent design either Public or Private. A question maybe asked as to how Private Applications can be used and placed on a private Hard Drive ? One solution is to define Flash Drives as to whether they are Symmetrical or Non Symmetrical meaning if a Symmetrical Flash drive attempts to access a Private Hard drive it will not be permitted because it is programmed within a shell or Internal Environment as defined parameters of that device and within the Encrypted MAC Address that contains the Internal Private key to unlock the Private Hard-drive.

External Power Connector's Voltage to Bits Chart

1st Battery Voltage/Bits produced

1st Volt	1024
2nd Volt	2048
3rd Volt	4096

2nd Battery Voltage/Bits Produced

4th Volt	8192
5th Volt	12288

6th Volt Reserved for Reallocation and Distribution

This is a conversion chart to show how many volts are to be converted from volts to bits. In my OSI Theoretical discussion I proposed a sub Physical layer at the lower stack of the OSI Please view the following

Network Layer frames assembled to packets IP Routing begins here
Data Link Layer Bytes into Frames Bridging begins here Non- Rout able
Physical Layer Bits into Bytes
Sub-Physical Voltage into Bits
Atomic Sub Particle layer Electrons, Proton Nucleus

Summary of New Features of SS45M-D Motherboard Design

Today is 11/05/2011 University Place, Washington. I would like to go over my new board design with the new features that builds upon the SS34M-D Motherboard design and Architecture.

After reviewing the design diagrams, You will notice that I have added new design features in my SS34M-D motherboard design and architecture. Some of the new features are the following

1. Separate Sound Systems

   a). Private utilizes Binary signals in Encrypted format from the Private Bios switch utilizing fiber optic format in Data Encapsulated form MAC Addresses are Advertised in protected mode through Fiber Optic Encapsulated

   b). Public utilizes Analog Signals in Non Encrypted format from the Public BIOS NON Encapsulated MAC Addresses are advertised in NON Protection Mode across normal wires.

2). File System is Encrypted once the choice is made to utilize Private Bios. The process is

   a.) End-User chooses Private Bios
   b). File System is encrypted
   c). Encrypted key is generated and sent to the Private Hard drive to unlock the Applications, objects, and File System for the Private User

3). Implementation of 256 AES Encryption instead of MD5 and 128 bit AES. It has been understood that MD5 and some AES encryption methods are subject to brute force attacks coupled with Wireless Roaming signals and Social Networks.

Feasibility of Design Applications

I would now like to present some of the tests I performed

1. Using Ubuntu Linux Gnome and Kde desktop Non encrypted file system caused My sound system to be disrupted ;however, When encrypting the file system, My sound was not hampered or disrupted and was fully functional.

2). I tested the ALSA Linux with the different music, video formats and I encountered temporary disruption because even though ALSA offers many File formats they are unsecured because of property and object rights that are manipulated and accessed through a unsecured Public Network. In essence encrypting the file system and controlling who has access in the File, object property rights through SE Policy helps cut down on viruses, malaware, and Trojans.

3). When creating Private Address Spaces such as 192.168.x.x, I was better able to control the End-User point of communication and security by requiring stricter LDAP X.500 standards such as SSL/password security also please note some E-mail addresses use encrypted links that were hidden from view thus the links are accessed by unknown 3rd party cookies and load Malicious programs. When stricter Directory requirements were implemented the hidden contacts in the Directory became known and deleted so what this says System and Application software developer's should create a better interface regarding Private and ISP services by allowing the usage of TLS 1.1 RSA 2048 bits. The bottom line is ISP services should allow easier interfaces with End-Users who must require greater security through the usage of Private address Spaces. I was successful in interfacing with the ISP services regarding this. Please note this does not fix all the problems but it does cut down a lot of security issues.

4). After researching some of the Encryption methods, I found that some such as MD5 and 128 AES were subject to brute force attacks ;however, in AES there are 128,256, 512 so to prevent further problems updated hashing and Algorithms were tested using 256 AES TLS 1.1 2048/4096 3 years ago utilizing Opera and at the time I had a 60/70 percent chance the IP packets would be accepted but because the need for stricter security requirements is now the success rate will probably be better due to fixing system and application bugs.

Summary of design Considerations

In conclusion, I have attempted to build upon my SS34M-D Motherboard design by Encrypting the file system, generating Internal 256 AES Encryption Random Keys, Creating Dynamic environments using devices such as sound ;thereby, allowing Public Analog signal Non secured or Private sound using binary digital encrypted format. Secured.

I would like to build upon my previous Pseudo code that could be used for processing Public and Private Data and Applications.

Pseudo Code for Processing Address Spaces

A = Private Bios

B = Public Bios

Default = Public Bios Default

```
If A
    then
    Goto Private BIOS processing
    Else
If  B
    then

    Goto Public Bios processing
    Else
    Goto Public Bios
```

Private Bios Processing

Non Symmetrical Processing begins
Encrypting File System begins
Internal Mac Address is Data Encapsulated
Mac address is sent to the Private Device Sound System in binary encrypted format
Network Processing begins
Bits are filtered and decay begins at the 1st Event
Bits are processed into Bytes which are converted into Internal Mac addresses
MAC addresses are loaded into a table for Private Memory Storage Encapsulated
Random Internal Private Encryption 256 AES is Generated to unlock the Hard drive address
Private Hard Drive Pulls Memory Addresses to load Applications
with 256 AES Random Encryption key
Internal Mac address are converted into Private IPV 4.0 addresses
2nd Event Private IPV 4.0 are Regenerated into IPV 6.0 with Packet Encryption and Headers using AES
Packets ready for Private communications employing Privacy and Security

Public Bios processing

Symmetrical processing begins
Data Encapsulated from Private BIOS via Fiber Optic
Public Mac Addresses are loaded into tables Public Memory Spaces
Public Hard Drive Pulls Memory Addresses for Applications
Analog Sound System is initiated
Public BIOS settings loaded using IPV 4.0 utilizing Public Switch.

End

The processes outline show how important it is to define devices that access the BIOS and how to prevent Environmental pollution in a unsecured Public Network. This is accomplished through Encrypting the File System, Beefing up security utilizing 256 AES Encryption methods, Separating Devices such as sound by defining the Private Environment as Binary Encrypted and digital while the Public sound system accesses the Analog signals in a unsecured Public Network useful in Social Networks.

Initial Bios Boot Up Screen

BIOS Consumer End-User Select Screen

1). Select 1 For Private Bios For Privacy and Security

2). Select 2 for Public Bios For Social Networks

Default is Public Bios if 1 or 2 Not selected after 10 Seconds.

Conclusion and Summary

The objective accomplished was to provide practical application to the previous U.S. Copyrights written because I believe it is not enough to write a theory and not provide a useful application to the theory proposed some examples are thoughts on Rotating Black holes, OSI theoretical discussion, Linear Cryptographic in Real time mode, Temporal Spatial Equations and Dynamic usage of Time and Space, and Why the Big Bang Theory is a Myth. If you are interested in other works that incorporate Physics, Mathematics, and Computers, Please visit my web site below.

Dated 11/05/2011

Barry L. Crouse

Web Site http://barrycrouse.angelfire.com

Email at bcrouse2011ad@gmail.com