Computer Engineering and Intelligent Systems
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.6, No.1, 2015

A Survey of IP Address for Next Generation Internet Services

Michael F.Adaramola[1*] Michael.A.K.Adelabu[2]
1.School of Engineering, Lagos State Polytechnic, Ikorodu,P.M.B. 21,606, Ikeja. Lagos. Nigeria
2.Faculty of Engineering, University of Lagos, Akoka, Yaba,Lagos. Nigeria
*Email: mfadaramola@yahoo.com

Abstract
This paper surveys the problem of the astronomical growing demand of Internet Systems participating in the public network which has led to the depletion of allocated Internet Protocol version 4.0 (IPV4) addresses. Already, four out of the Regional Internet Registry (RIR) namely: ARNIC, RIPE, LACNIC and ARPIN have exhausted their allocated IPV4 addresses while the fifth AFRICNIC (Africa's RIR) is reportedly depleted. We also examine the limitations of IPV4, the features of IPV6 and different modes of operating IPV6 standard. Findings shows that the current population of the world is over 6billion people with a projection of 9billion people by the year 2050 and IPV6 can conveniently accommodate 2^{128} devices. This paper also proposes the migration from the present Internet Protocol version 4.0(IPV4) to a new Internet Protocol version 6.0(IPV6) addresses. This research work has shown that deploying the IPV6 could only be the possible solution to sustaining Internet Services globally.
Keywords: Internet Systems, Internet Protocol Address, IP address depletion, Migration.

1. Introduction

The Internet has already made an impact in many countries all-over the world, but it is only the beginning. The internet will dominate as the resource for sharing data as networks of the campuses become more powerful and robust. There are many aspects of a seamless communications system, and one of the most important aspects is the ability to interface physical networks with multiple operating systems. The internet protocol is mainly the software designed for this interface. Users, application programs and higher layers of protocol software use the internet protocol addresses to communicate (Comer, 1997). Obviously, this is the essence of the communication that occurs throughout the internet world. The internet protocol remains important issue for several reasons. It is non- proprietary, open, and it offers ways to merge voice and data traffic on a common platform (i.e. convergence). The IP networks meet the requirements for interoperability and integration, scalability, mediation, reliability, manageability, security, and have global reach (Miller, 1998). Each version of the internet protocol has similar characteristics and abilities. IPV6 has taken advantage of IPV4's history and will be the only protocol that will meet the needs of public network in Nigeria. This paper is organized as follows: Section 2 discusses the limitations of the IPV4 addresses. Section 3 studies the various type of IPV6 addresses standard. The various sustainable comparative features of IPV6 addresses were discussed in Section 4. Finally, we conclude this paper in Section 5.

2. Limitations of IP Version 4.0

IPV6 is simpler than IPV4 for a couple of many reasons. The designers had twenty years of experience before IPV6 was designed and implemented. In fact, there has been time to identify the weaknesses in IPV4 and make corrections. Some of these weaknesses are highlighted as follows:

A. Security

Security needs to be present inside and outside of any establishment. Therefore, public networks in Nigeria as an example will not accept outsiders (i.e. intruders) being able to monitor the activities inside the entire organization.

Presently, IP security had been implemented in both IPV4 and IPV6. Since it has been implemented in IPV4, there are very few differences between the two protocols when it comes to security.

IPV4 will not be able to sustain the volume of devices that will be needed in public network. Eventually, Classless Inter-Domain Routing (CIDR) will not provide the level of aggregation required, and Network Address Translation (NAT) will be available. NAT already has limitations and IP security is gaining more popularity because of Virtual Private Networks (VPNs). NAT is just a temporary solution to an existing problem; it is not a long-term solution. CIDR is still not supported in all parts of the internet. Even if the addresses were not completely depleted, the addresses would still need to be managed carefully. It is already difficult to manage a depleting address space and will only become more difficult in the next generation.

B. Volume

The IPV4 is limited to 4.2 billion devices communicating on the global network at any given point in time. For better analysis, IPV4 uses 32 bit, the total addressing space is shown as IPV4 = 2^{32} = 4.2949 x 10^9 = 4.2 Billion.

However, this space will not be enough in the next generation. The volume of devices will increase dramatically as smart devices are developed and incorporated into the public networks in Nigeria. Many establishments today have computers, laptops, palmtops, GSM Mobile phones with internet connections, but this does not resemble the public internet networks of the next generation. They will have a high density of nodes and will consist of many complex systems that are made up of many individual devices.

C. Data Flow

The key to effective data flow is the ability to efficiently handle packets. The less handling that is needed to allow the packets to traverse the network optimally, the more flexible the protocol will be. Obviously, IP has mostly been used for data applications that are suitable for a best effort delivery system. Streaming video and voice has not been widely distributed via the Internet because of bandwidth limitations and the lack of Qualify of Service (QoS).This is very peculiar to the large-scale enterprise WAN and Internet Services. Data flow is not efficient in IPV4. The IPV4 headers vary in size, which means the routers have to calculate the length of an IPV4 payload, which creates additional overhead. IPV4 was not designed to handle the needs of voice, video and other that need quality of service.

3. IP Version 6.0 Address Types

There are three types of addresses in IPV6 addressing – anycast, unicast and multicast. The IPV6 addresses are assigned to interfaces not nodes. It is not necessary for all of the interfaces to have specific IP addresses, thus saving address space. If two nodes are merely passing traffic they do not need to have IPV6 addresses (Loshin, 1999).

A. Anycast

Anycast addresses are a single address assigned to more than one interface and are designed so that only a single node will receive the datagram, usually the closest node. For example, if a request is sent out to get the time from a timeserver, the message will be addressed to any router that has an associated timeserver. However, lit is most effective if the closest available timeserver responds. Once the datagram reaches the closest timeserver, the node will respond and the original datagram will not travel any further. This is helpful for certain types of services that do not require a relationship between the client and the server (Loshin, 1999). The other uses for any cast any identifying a set of routers that belongs to an internet service provider, a set of routers that are part of a particular subnet, and a set of router that provides an entry to a particular routing domain (Miller, 1998). There are currently two limitations placed on anycast addresses. First, an anycast address cannot be used as a source address and second, an anycast address can only be assigned to a router (Buttler, 1999).

B. Unicast

There are several forms of unicast addresses: Aggregatable global unicast (AGU) address, Network Service Access Point (NSAP) address, Internet work Packet Exchange (IPX) hierarchical address, the site- local address, the link- local address and the IPV4 capable address. Unicast addresses are designed assuming that the routing decisions are based on a longest prefix match (Buttler, 1999). The node can be made a ware of as much or a little of the address as needed, depending on the node's function. The address may be viewed as a single piece of information or the information can be parsed into smaller pieces (Ora, 2012). In the end, the address still needs to be 128 – bits, and will identify a node interface. The unicast address is designed to support current provider aggregation and a new type of aggregation called exchanges. The option selected was exchange-based addresses. These addresses are allocated through the internet provider. An address block is assigned to a service provider and the subscriber accesses the network through the provider. There is little maintenance required on behalf of the subscriber (Loshin, 1999).

There are five parts of a unicast address. The first part is the 3-bit prefix (010), which is then followed by the Top Level Aggregator (TLA). The TLA can either be a provider or an exchange point. The routing tables will only need to have one entry per TLA. The TLA's are 13-bits, which imply that there is a possibility of having 8,192 exchange points or backbone providers (Buttler, 1999). There are 8–bits reserved between the TLA and the next frame. The next address component is the Next Level Aggregator (NLA) which is 32–bits long and will be used to allow ISPs to implement their own addressing hierarchy. The site-level aggregation identifier is given to organizations for example, Cadbury Nigeria PLC for their internal network structure and is 10-bits long. This portion of the address supports 65,535 individual subnets per site (Buttler, 1999). This should be sufficient for all but the largest organizations. The last field in the address is the interface identifier. A unicast address may be viewed as a two-field entity, one identifies the network and the other identifies the nodes interface. The interface identifiers are required as part of the addressing architecture, and are based on the IEEE EUI-64. This 64-bit identifier which is used to uniquely identify each and every network interface, which means that there can be 18 billion different addresses, which is only half of the IPV6 addressing space. Mathematically, 2^{64}=1.8447 x 10^{19} Addresses is equivalent to 18 billion addresses.

There are three levels of the hierarchy: public topology, site topology and interface identifier. The public topology is the public internet transit services. This is the global part of the network that requires unique global addresses. There have been two different segments of the address space allocated to support this ability (Loshin, 1999). There are two types of local-use unicast addresses: link–local and site-local. The Link–local addresses are used in auto-address configuration; neighbour discovery, or where there are no routers present. These addresses are intended to identify hosts on a single network link. Site-local addresses are used internally within the site network and cannot be used in the global network. Routers will not forward packets with site-local or link-local source addresses (Miller, 1998).

C. Multicast

With multicast, each transaction is only carried over each link once. The transmission is dropped off' and duplicated at each node. This can lead to great improvements in efficiencies over distributed LANs. In addition, unlike point–to-point communication, multicasting is easily sealable. The network does not feel the brunt of an increase in traffic, even if the number of users is greatly increased; multicasting achieves this by having three basic requirements:

(i) Routers must be able to efficiently locate route to many LANs at once
(ii) Only a single copy of each packet should be sent on any shared link
(iii) Traffic should only be sent on links that have at least one recipient (Ora, 2012).

There are many uses for multicasting. The need for multicasting continues to grow as the number of users increase and new applications are more feasible. Multicasting can add significant functionality without impacting the network (IPMulticast, 2012). There are three general categories for multicast applications:

(a) One-to-many (single source to multiple receivers)
(b) Many-to-One (multiple sources to one receiver)
(c) Many-to-Many (any number to hosts sending to the same multicast group address and receiving from it) (IPMulticast, 2012).

Research work showed that an organization called Mboore Systems Limited was established to implement and test multicasting in the early 1990's. So, Mboore is an overlay network that has been used to accelerate the early usage of multicasting through the internet (Huiterna, 1995). We understand that IPV4 has a designed range of addresses that have been identified for multicast. Although a class of addresses has been identified, a majority of IPV4 routers are not multicast enabled router at the source and the destination. Tunneling is used to forward multicast packets throughout the rest of the network (Whatis, 2012). The Mboore solution does not fully capitalize on the efficiencies and capabilities of a truly multicast enabled network. The packets must be encapsulated and assigned a unicast address while traversing the non-multicast enable portion of the entire Wide Area Network. The designers of IPV6 wanted to ensure that all IPV6 nodes could take advantage of multicasting. The multicast addressing that is used in IPV6 can be identified by all routers and all of the experience that has been gained in Mboore's IPV4 multicasting has been incorporated into IPV6 multicasting. Lastly, multicasting has been part of the development of IPV6 since the beginning, so in a fully deployed IPV6 network multicasting is a seamless and advantageous.

4. IP Version 6.0 Features

A. IPV6 Autoconfiguration

The IPV6 incorporates the Dynamic Host Configuration Protocol (DHCP) which allows the host to obtain all of the relevant information. It also supports automated address changes, mobile hosts, and dead neighbour detection. Link-local addresses can be determined by using the Link-Local prefix and a unique token that will give the node its unique identity. The link-local address is then used to initiate membership in all nodes multicast group. A solicitation message is sent out if a router advertisement message is not received during one of the regular intervals. The solicitation message will be sent three times to ensure that there isn't a router on the network. If no router responds, then the node will continue to use its link-local address and only communicate with the nodes on the local network. After this address is established the node will send out another message with the address that it was assigned. If another node responds, it will reveal a duplication of addresses by exposing a collision. Address resolution and neighbour discovery are handled differently than IPV4. Neighbour discovery combines the Address Resolution Protocol (ARP), the Internet Control Message Protocol (ICMP), Router Discover messages and the ICMP Redirect message found in IPV4. Routers and neighbours will advertise their availability or solicit an advertisement in order to determine if they are available, to verify addresses, and to establish link-layer addresses (Loshin, 1999). Neighbour discovery defines where the node is on the network, and the path that the diagram must travel in order to reach the destination. Nodes also use neighbour discovery to determine the links layer addresses for nodes that are on attached links and to purge addresses that have become invalid. This allows for nodes to determine which routers are will routers are willing

to forward packets on their behalf, and which nodes are reachable and which nodes or not. Neighbour discovery also allows for new paths when the current path fails (Buttler, 1999).

There are a couple of key improvements from IPV4 to IPV6. The first is that router discovery is part of the base protocol set and no additional packet exchange is needed to resolve link-layer address because the router advertisements carry the addresses and prefixes for a link. Router advertisements make address auto configuration possible (McNealis, 1998). More multicast addresses are available to handle address resolution and the address resolution process is much more direct without having to affect unnecessary nodes. Redirects contain more data about the first hop, which means fewer messages will be generated. The protocol is more media- independent than ARP because address resolution is at the ICMP layer, and makes IP authentication and security mechanisms possible (Cisco, 2011).

There are IPV6 advertisements that would replace common IPV4 advertisements. Some of the advertisement is consolidated and some are more efficient to minimize the impact on the network.

B.IPV6 Security

One of the keys of internet-level security is that it simplifies the development of secure applications. It will be the baseline for application developers to build on and it will mean that security is available on all operating system platforms. As more data is shared, the more threats there is to networked systems and the higher the livelihood for invasions of privacy and confidentiality. This is critical in the campus environment where much of the data is extremely official and confidential. Confidentiality must be maintained and only authorized personnel can access the information collected and stored. When IPV6 was in its infancy, security was a high priority. With the onset of a new protocol, the opportunity presented itself to be able to complement security with the data link layer, instead of relying on higher level protocols. IP layer security only protects the IP datagrams. IP security is basically transparent to the user, and can create a foundation for other forms of security to be incorporated. IP traffic is susceptible to interception, sniffers, denial of service and spooling. Interception occurs when the data transmitted from one node to another is taken from an unauthorized third party. A sniffer is a program that monitors and analyzes network traffic, detecting bottlenecks and problems (Whatis, 2012). Some of these sniffers not only analyze traffic, the actual payload data can be read. Denial of service can happen when an authorized user cannot access the network resources. This happen by flooding the host with requests or unnecessarily sending data only to block the flow of other data. Spooling occurs when a packet is altered to misrepresent the packets' origin. For a long time security was not considered important at the internet layer (Loshin, 1999). In most circumstances security issues have been handled in higher layers. Spooling denial of service, hijacking and interception of connections have raised the level of interest of security in the IETF (Cisco, 2012).

IP security (IPsec) is security architecture for the internet protocol. It is not intended to make the internet secure, it is intended to make IP secure. IPsec defines security services that can be used at the IP layer for both IPV4 and IPV6 (Loshin, 1999). The goals for IP security are to authenticate, maintain the integrity and confidentiality of the IP packets. These are three areas that are very important in the campus network. The security services that are a component of IPsec is Access control connectionless integrity, Data origin Authentication Defense against replay attacks, Encryption and Traffic flow confidentiality. All of these functions will be made possible by the use of encapsulating security payload headers and authentication headers (Loshin, 1999). The Encapsulating Security Payload (ESP) Header is designed to allow IP nodes to send and receive datagram whose payload is encrypted. Some of its function overlaps with the authentication headers, but ESP adds a level of confidentiality by transforming the data. This header is designed to provide confidentiality of datagrams through encryption, authentication of data origin through the use of public key encryption, anti-replay services through the same sequence number mechanism and limited traffic flow confidentiality through the use of security gateways (Loshin, 1999).

ESP does allow for attackers to study traffic because it appears to be a regular datagram, the only difference is that the payload is encrypted. Tunneling and security gateways can also be used with ESP. Security associations rely on the use of Keys. This is prevalent in the large enterprise network. Efficient deployment of security will rely on the existence of an efficient key distribution method (Huiterna, 1996). The key management procedures determine the security parameter index as well as providing the keys. There are several proposals that are under examination at the current time. Simple key- management for Internet protocols (SKIP), Internet Security Association and Key-Management Protocol (ISAKMP) and manual key distribution. When IPV6 packets are sent, they all convey a security parameter index (SPI). Each node must know the SPI to determine the security context, whether it is one node or a group of nodes in a multicast environment. Both authentication and encryption are based on a concept of security association (Huiterna, 1996).

A security Association normally includes the parameters listed below, but might indicate additional parameters as well:

- Authentication algorithm and mode of algorithm used with the IP Authentication Header

- Key(s) used with the authentication algorithm in use with the Authentication Header.
- Encryption algorithm, algorithm mode and transformation used with the IP Encapsulating security payload.
- Key(s) used with the encryption algorithm in use with the EPS.

C. IPV6 Data Flow

In public network, Internet bandwidth on demand and the ability to control the flow of packets will be important issues. There will be a need for a constant flow of data in and out of the public networks, which will require steady bandwidth. There will also be a need for data transmission that is busty and sporadic. In addition, there will be voice transmission which is relatively low in bandwidth but requires continuous streaming. Whether it is busty, streaming or real-time, IP is expected to be one protocol that will be able to handle all types of communications. Bandwidth will need to continually increase as files continue to grow in size and more information will be accessed remotely. The arrangement of the IPV4 is shown below:

Version	JHL	Types of service	Total length	
Identification			Flags	Fragment offset
Time-to-leave	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

Fig 1: IPV4 Arrangement (Huiterna, 1996)

Note, the header length field found in IPV4 is not necessary in IPV6 because all IPV6 headers are the same. IPV4 headers can be as short as 20bytes and as long as 60 bytes. The IPV4 datagram length is the entire datagram including headers. Routers calculate the length of an IPV4 payload by subtracting the Header length from the datagram length; IPV6 does not need to process this calculation. The type of service is really made up of two sub-fields precedence and type of service. Precedence is the level of priority and the type of service bits defined, namely: a delay bit, a throughput bit and a reliability bit. These types of service bits were designed to compute a default route, the shortest route, the largest throughput or most reliable route (Huiterna, 1995).The precedence indicator is used for queuing purposes. There are eight preference values, and works on the premises that the packet with the highest priority will be sent first. The fragmentation and reassembly process use the identification, flags and offset fields. When an IPV4 packet is fragmented, it is given complete IP headers, which are copied from the original packet. If one fragment is lost, the entire packet must be resent. In IPV6, only the source router does the fragmentation while in IPV4 fragmentation can be done at any intermediary node. In IPV6, all intermediary nodes ignore the fragmentation extension headers which improve efficiency as the packets are routed (Loshin, 1999).

IPV6 has some major changes over IPV4 when it comes to the header. With all of the additional tools available in IPV6, multimedia will become even more a reality or at least start to address some of the real expectations of multimedia. The timing issues and bandwidth requirements have been addressed with IPV6.

In public network where large amounts of traffic can cause delays and bottlenecks. One of the ways of dealing with vast amount of data is by maximizing the use of bandwidth. Multicasting will be an easy solution of disseminating a large amount of data to many users without typing up valuable network resources. There are applications that will continue to emerge as a result of multicasting. It will be important to have the ability to join a newsgroup and a weather forecasting group. Even when it comes to conducting research such as the census, the many-to-one capability that multicasting offers will be a tremendous help.

In addition, the data that is being sent doesn't have to be broadcast out into the entire world. It is only sent to the users who request it or need to receive it. An Anycast addressing will give the ability for efficiency as well when it comes to keeping all of the docks up-to-date. The other advantage of IPV6 is the source router will fragment the payload prior to sending them into the network if sufficient bandwidth is not provided between the source and destination.

IPV6 Headers includes the following: Version, Class, Flow Label, Payload Length, Next Header, Hop Limit, Source Address and Destination Address. The arrangement of the IPV6 is shown below:

Version	Class	Flow label		
Payload Length			Next Header	Hop Limit
Source Address				
Destination Address				

Fig 2: IPV6 arrangement (Huiterna, 1996)

The IPV6 header, which is 40 octets, is approximately twice the size of an IPV4 header, but provides some simplification from the IPV4 header. All headers have a fixed format, there is no longer a checksum, and the hop-by-hop segmentation procedure has been removed. There are eight (8) fields in the IPV6 header, namely:

i. Version (4 bits)
ii. Traffic class (8 bits)
iii. Flow Label (20 bits)
iv. Payload Length (20 bits)
v. Next Header (8 bits)
vi. Hop Limit (8 bits)
vii. Source Address (128-int)
viii. Destination Address (128-bit)

The version field indicates the version of IP in use. The traffic class filed contains a value that identified the priority level for delivering packets. Each individual packet can have a different priority even if it originated from the same source. There are two ranges of priorities 0–7 and 8–15. Priorities 0–7 are reserved for low priority packets. If traffic is heavy like the large-scale enterprise, the packets will back off. These packets do not need to arrive in real time and can be delayed. Priorities 8-15 are used for non-congestion controlled or real-time traffic. The packets that are sent at 15 are critical for maintaining a constant rate, and the packets at 8 are still real –time traffic, but the transmission would not suffer tremendously if the packet was lost (Goncalves, 1998).
The flow label gives the source the ability to label a sequence of packets, which requires the router to give the packets special handling. All packets belong to the same flow must have the same source, destination, priority and flow label. A flow label can be used to establish routes that give better service, including lower delay or bigger bandwidth. Each and every packet that has flow labels changes the handling within the router, which can cause difficulties within the cache of the router. The payload length defines the length of the packet following the header. The minimum payload is 576 octets which has the ability to have payload greater than 65,535 bytes called Jumbo" payloads. The field identifies jumbo packets by setting the payload length to zero and then specifying the length in the Hop-by-Hop extension header.

The Next Header field identifies the header that is immediately following the IPV6 header. These extension headers are used to specify special case treatment of some packets.

The extension headers could be an Authentication Header, an Encapsulation Security Header, a Routing Header, an upper layer Header, a fragment Header, Destination options Header or a Hop-by-Hop options Header. There is a recommendation for the order in which these extension headers are placed in the IPV6 packet. The Hop Limit identifies the number of hops the packet can travel from its source to the destination. This is a counter that decrements by one at each hop count. Once the field reaches zero, the packet is discarded. IPV6 has the ability to measure the maximum number of hops that can occur as the packet is forwarded. This replaces the Time-to-leave field found in IPV4, and no longer use time as a component. The source address field contains the 128- bit address of the originator and the destination address field contains the destination address.

5. Conclusion

In this paper, the several limitations of IPV4 were fully examined. Study shows that IPV6 does not possess the limitations of IPV4. In a nutshell, there are enough unique addresses available in IPV6 to sustain the expected astronomical growth of network infrastructures and devices well into the next generation. With the 128-bits IPV6 addressing space, we have 2^{128}=3.4028 x 10^{38} possible addresses. No doubt, this expansion of address will accommodate the future growth expected in every sector (Miller, 1998).The urgent need to migrate from IPV4 standard to that of IPV6 now becomes the all-important assignment of every institution of higher learning, enterprise and organization in the nation.

Finally, IPV6 is robust and of high standard. Therefore, it will inevitably sustain the internet backbone of the next generation in Nigeria (Faulkner, 2012).

References

Comer, Douglas (1997), computer Networks and Internets, 2nd Edition, prentice Hall, New Jersey, USA
Miller, Mark A. (1998), Implementing IPV6, 1st Edition, M&T Books, New York. USA
Loshin, Peter (1999), IPV6 Clearly Explained 1st Edition, Morgan Kaufman, San Francisco. USA.
Buttler Lampson, Venkatachary Srinivasan and George Varghese, IP Lookups Using Multi-way and Multicolumn Search IEEE/ACM Transactions on Networks, Vol. 7. June 1999. pp 335-349
www.ora.Com/Reference/dictionary/terms/ip/Internet Protocol Multicast.htm
www.ipmulticast.com/
Huitema, Christian (1995), Routing In the Internet. 1st Edition, Prentice Hall, New Jersey. USA.
www.whatis.com/ip
McNealis, Martin (1998), IP crossroads- Migrate to IPv6 or evolve with IPV4. Packet Magazine Archives

www.cisco.com/ohiostate.edu/hypertext/information/rfc.html
www.cisco.com/warp/public/732/ipV6/index.html.
Huitema, Christian (1996), IPV6-The New Internet Protocol, 2nd Edition, Prentice Hall, New Jersey USA.
Goncalves, Marcus, Niles and Kitty (1998). IPV6 Networks, 1st Edition, McGraw-Hill, New York. USA
www.rit.edu:8080/Proxy/www.faulkner.Com/products/facts/default.html

Michael F. Adaramola was born in Ilara-Mokin, Ondo State, Nigeria on May 15, 1968. He received the B.Eng. degree in Electrical and Electronics Engineering from University of Ilorin, Ilorin in 1991 and the M.Sc. degree in Communication Engineering from University of Lagos, Lagos State in 2012.

Engr. Adaramola had done serious research work on FFT Algorithm and Effects of Data windowing on Power Spectral Estimation during his first degree programme. Additionally, he was engaged in research analysis on Internet Services performance of Institutions of higher learning and University of Lagos was the case study in his second degree thesis. He became a registered member of the Council for the Regulation of Engineering in Nigeria (COREN) on December 21, 2009 where he was awarded the R. Eng. Certification. However, his current area of his research work includes Data Communications with Internet Services, Wireless Communication systems design, GSM Switching system design, millimeter wave engineering and digital signal processing systems design.

Presently, he is the Head of Department in Electrical and Electronics Engineering of the School of Part-Time Regular (SPTSR) of Lagos State Polytechnic, Ikorodu. Lagos State, Nigeria.

Michael A. Kolawole Adelabu was born in Ilesha, Osun State, Nigeria on August 9, 1957. He received the Higher National Diploma (HND) in Electrical Engineering from Yaba College of Technology, Yaba, Lagos in 1977 and the M.Sc. degree in Electronics and Telecommunications from Wroclaw Technical University, Wroclaw, Poland in 1984. He later received the Postgraduate Diploma, PGD degree in Computer Science from the University of Lagos, Akoka, Yaba, Lagos in 1991. He had published 13 research and conference papers in both local and international journals. However, his current area of his research work includes Telecommunication systems, Active Networks – Analysis, Synthesis and Design, VLSI design, Logic design of Digital systems, Digital Signal processing and Microwave engineering. As a veteran Lecturer, he had worked as External Moderator to Federal Polytechnic, Yaba College of Technology and Lagos State Polytechnic from 1995 - 2008, 1996 - 1999 and 1997 – 1999 respectively.

Presently, he is a lecturer and Ph. D student in the department of Electrical and Electronics Engineering, University of Lagos, Yaba, Lagos, Nigeria.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar