Evaluation of Network Architecture and Its Implication on Connectivity and Data Security

Emerole Kelechi C
Department of Electrical and Electronics Engineering
Federal Polytechnic Nekede
Owerr, Nigeria
kelechiemerole@gmail.com

Nwadike Stanley
Department of Electrical and Electronics Engineering
Federal Polytechnic Nekede
Owerri, Nigeria

Nwogu Uchenna
Department of Electrical and Electronics Engineering
Federal Polytechnic Nekede
Owerr, Nigeria
losengineering@gmail.com

***Abstract*—**Networking offers the framework to congregate largely heterogeneous entities so that they can communicate. In this paper we review aspects of Network architectural design that aims to ensure connectivity and data security for network users. Security protocols like the Internet Protocol Security (IPsec) ensures data security for users of a Virtual Private Network which provides encryption, tunneling and authentication services. Virtual Local Area Networks plays a role in network management and security. Access Control lists provides an overview of rights granted to users to access network resources thereby reducing incidence of hacking to the minimum. Combining these techniques in a network would ensure uninterrupted service and data security to network users.

Keywords*-Virtual Local Area Network, Access Control List,Voice over Internet Protocol,Generic Routing Encapsulation, Scalability*

*****

INTRODUCTION

Network designs, encompasses all areas of human enterprise. We find networks in the home, marketplace, offices and schools making it possible for resources to be shared in a consolidated platform. Security, high speed access and performance are considered in the design of networks [1]. One of such key performance indicator is how flexible a network can be without a compromise on its objective. It combines hardware, software, cables, operating systems, switches, routers, hubs for communication to take place [2]. Network offer the following services file and print transfer, e-learning and video conferencing. Protocols are set up to define communication standards existing on networks. Networks have categories [3];

a) *Local Area Network*: This is a network over a short distance of few kilometres; Personal computers can share computing resources which include files, printers, servers, application programmes [4].
b) *Metropolitan Area Network*: This is a network that connects organizations within a city together example is a cable network [2].
c) *Wide Area Network*: This is a network that encompasses a wide geographical area which comprises of cities, continents or the world. An example of such a network is the internet.

Networking plays a critical role in business performance of any organization. Efficiency and communication is guaranteed in a well designed network. A network is apt for the focus of this project which is to improve the teaching and research capabilities of polytechnic institutions in Nigeria. The important networking devices are server, router, switch, adaptive security appliance, intrusion prevention systems [5].

a) *Server*: The server is a network equipment with an operating system that manages access to network resources like files, printers e.t.c. it has an inbuilt processor that carries out processing of requests[6].
b) *Router*: It employs routing techniques to transmit data packets across the network. The router serves as an interface between one network protocol and the other. It operates in layer 3 of the OSI model suite. They exist at network edges to route data packets through the best path to its destination. They also send updates to entries to their routing table to other routers [2][7].
c) *Switches*: Switches are network devices that connect personal computers, servers, printers within a local area network [6].
d) *Intrusion Prevention Systems*: These systems monitor network operations and guard against bugs and malicious activity that would compromise network performance. A record of this activity is acted upon and necessary action to correct this anomaly is taken[8].

II. NETWORK DESIGN CONSIDERATIONS

Hierarchical model is employed in LAN designs [11]. In a hierarchical model designs are done in layers. We have three layers; the access layer, the aggregation layer and the core layer.

 ISSN: 2321-8169
3945 - 3950

a) *The Access Layer*: This layer connects end users to the network
b) *The Aggregation layer*: This layer serves a buffer retransmitting several data packets from the access layer throughout the network to the core layer
c) *The Core layer*: This layer transmits several packets from the aggregation layer to the internet.

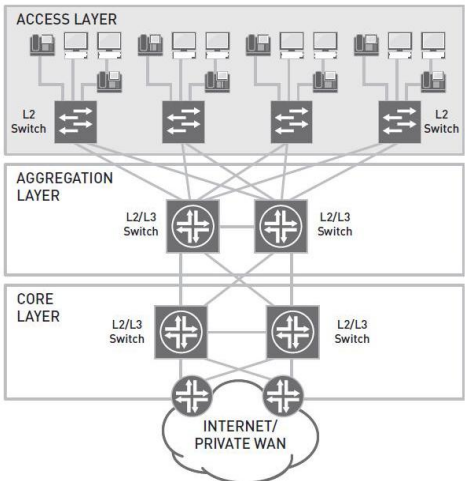

Figure 1 Hierarchical Model in LAN design [4]

In order for a LAN to offer audio-visual services, the following which would be enumerated in the preceding sections would be incorporated in the design of any network.

A. *Voice over Internet Protocol*

This is an IP based network that transmits voice and data signals over public communication channels. It employs IP phones, mobile devices and VoIP gateways for this purpose[9]. This protocol employs Internet Protocol in the transmission of data packets across the network. Voice signals are sampled and converted to digital signals and then final conversion to data packets is made before transmission. Signalling information is exchanged between communicating entities before communication can take place. This involves call set-up, termination, call addressing and control[9]. Voice Over Internet Protocol find applications in Video conferencing, multimedia, e-learning, web development, streaming and distance learning[10]. Data call has been recommended for long-distance communication because of its cost implications as compared to voice calls. VOIP also employs software for its communication and requires high speed internet for operation[11]. Limitations on the capacity of VOIP to meet traffic demands can affect the quality of service.
VOIP can be categorized using the following level of service[11]

a) *Residential VOIP*: These services are offered to residential subscribers and home users
b) *Hosted VOIP*: These services are offered to business owners. It employs a switchboard for call routing.
c) *Long-distance bypass*: These services are offered to users for long distance calls over public switched networks
d) *IP trunking*: Connects Public switched networks through the IP infrastructure
e) *Voice-capable network devices*: These are network devices capable of transmitting voice traffic over the internet

1) *Key Performance Parameters*

The parameters define the quality of service obtainable from any VOIP infrastructure [9]

a) *Voice Clarity*: An acceptable delay which will enable effective communication across the network should be set. Unnecessary delay can slow down the network and degrade performance.
b) *Interoperability*: This means that different product offering from different should not only conform to standard but come to agreement on its usability.
c) *Security*: Security of data packets is guaranteed by the use of encryption facilities. This ensures data integrity.
d) Scalability: The services offered by VOIP will parallel those offered by voice calls at a competitive cost.

B. *Virtual Private Network*

This is a network that provides data encryption, tunnelling and authentication facilities for its users over a public network backbone like the internet to build a private network [12][13]. Services offered include sharing of network resources like printers, applications, web tools etc. it has the advantage of greater savings in cost of acquiring dedicated leased-line infrastructure. It is divided into three categories [14].

a) Intranet VPN: This connects all the branches of an enterprise network together.
b) Remote Access VPN: This connects network users to the server. It offers encryption, tunnelling and authentication services. Tunnelling encapsulates data packets for efficient transmission over the internet and is supported by Point to Point Transmission Protocol [12] and IPsec protocol.
c) Extranet VPN: Provision of security for data transmission over the internet. Security is supported by MPPE and IPsec.

 ISSN: 2321-8169
3945 - 3950

For continuous and uninterrupted services there is a provision for redundant equipment that would replace any equipment pulled out of service due to degradation. Authentication mechanisms in VPN include RADIUS, LDAP, SecurID , PAP, CHAP, Tokens and X.509[12]

1) Internet Protocol Security(IPsec)

IPsec is a VPN security protocol that offer encryption and tunnelling services to VPN users and ensures that there is a smooth protocol communication between VPN and the internet(TCP/IP) [12]. It analyzes data packets to guarantee its structure, has not been tampered with that is data integrity. It also identifies and authenticates data. IPsec is made up of Authentication Header, Encapsulation Security Payload and the Internet Key Exchange [12]. The Authentication Header provides authentication and ensures data integrity by generating a Hash Message Authentication Code [15]. The Encapsulation Security Payload encapsulates and encrypts the data packet.

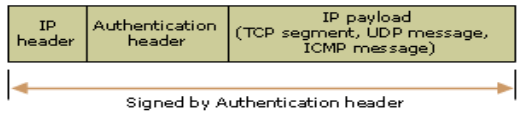

Figure 2 Authentication Header [13]

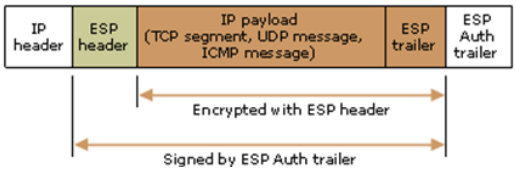

Figure 3 ESP Header [13]

The Internet Key exchange identifies and authenticates data from two communicating entities in the network and then provides data security using survival time, identity authentication algorithm, hash algorithm, encryption algorithm and DH algorithm for efficient and reliable communication. IPsec has two modes tunnel mode which encapsulates IP packets but leads to higher system costs and transmission mode that provides secure transmission. The Internet Key Exchange has two modes; Main mode were the communicating entities exchange packets to to get the symmetric key ID(SKEYID) which is made up of authentication key, encryption key and the quick mode key[16]. These keys secure the communication channel before packet transmission.

2) Generic Routing Encapsulation

GRE enable the interoperability between VPN and other IP network protocols like IP, Appletalk etc by encapsulating IP packets and transmitting across heterogeneous networks [12] . GRE doesn't offer encryption services but supports tunnelling and the overhead is lower than the IPsec. The RFC1701/RFC 1702 defines the GRE standard. It also supports other IP routing protocols like RIP, OSPF, IGRP, EIGRP and so on.

3) SSL/TSL Protocol

This protocol provides data integrity and encryption services for packets sent between clients in a VPN network[57]. Figure 4 shows the basic operation of the protocol. After exchanging messages between the client and server, TLS compresses and encrypts the packets.

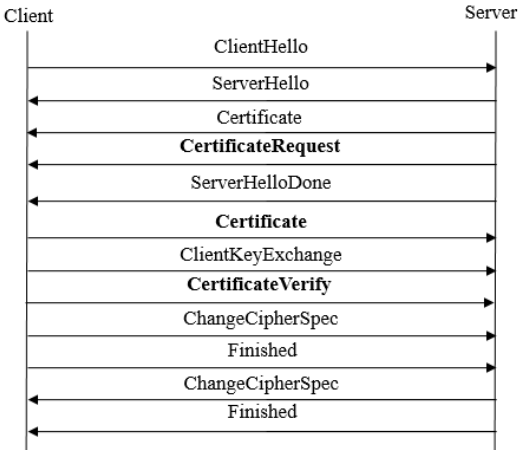

Figure 4 SSL/TSL Protocol [13]

4) VPN Attacks

There are several activities that limit the performance of VPN as an efficient medium of data transfer across private networks. These attacks modify data thereby affecting its integrity and confidentiality [15]. This is an example of an intrusive attack. In figure 5 [15], CE represents client which are connected to VPN1 and VPN2 while PE represent Internet Service Provider. External sites can be inserted into the communication channel which may constitute serious attack on data integrity

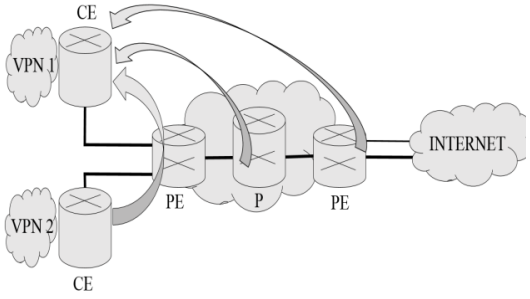

Figure 5 Intrusion in VPN [13]

Denial of Service can lead to congestion of the communication channel by transmitting large amount of data that would degrade the capacity of VPN equipment to process data by consuming computing resources [18]. Black holes, tear drop, ping of death are instances of these attacks. They can take advantage of loopholes in network security to

ISSN: 2321-8169
3945 - 3950

attack targets and deny access to services offered by the network. There are two divisions of this attack;

a) *Distributed denial of service*: Through the internet, malicious programs are installed in computer systems to monitor internet relay chats and generate traffic that would affect system performance [19].

b) *Distributed deflection denial of service*: Using the MAC address of computer systems, several ping messages are sent and on responding to these messages useless traffic are generated [18][20].

Network devices have anti-DoS and anti-spoofing settings which can be configured to mitigate against these attacks by closing any open connections in the network and limiting capacity for any network intruders to hide[21]. Filtering facilities can be implemented to control the amount of traffic on network links at any point in time.

C. Virtual LAN (VLAN)

This is a group of networks within a particular network with common properties(bandwidth) that communicate even though physically they are not connected together. Each group is a separate broadcast domain [22][23]. The advantage is that unauthorized access to these networks can be stopped. Also incidence of packet-sniffing is reduced to the minimum. Protocols can be confined within each group, so that relevant traffic is routed. These provide the facility for independent IP networks to exist within a network. VLAN operation includes configuring switches, tagging Ethernet frames and MAC address lookup [24]. To configure VLANs we use the IEEE 802.1Q standard. Other standards that exist include Cisco's Inter Switch Link and 3Com's Virtual LAN Trunk. These standards are owned by individual vendors. The tagging process for the IEEE 802.1Q involves modifying the Ethernet frames cause there is a field inside the frame for this purpose. VLAN is at the second layer of the OSI model. The tag header is 4-byte long with a 2-byte tag protocol identifier and a 2-byte tag control information. A network link called trunk can carry several VLANS with separate tags and run them into switches. VLAN identifiers between 1 and 1005 are used for Local Area network technologies while VLAN identifiers between 1006 and 4094 are used for Wide Area network technologies. A database vlan.dat stores information about switch management. IP addresses and subnet masks are assigned to computers in a network and the switch configured. These entire configurations must be consistent with the VLAN protocol of such network segments.

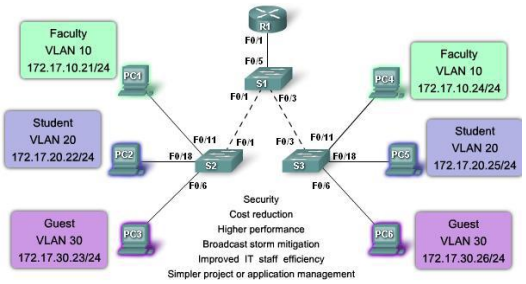

Figure 6 VLAN Design 2 [25]

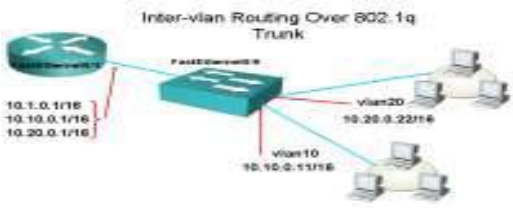

Figure 7 VLAN Design 2 [26]

We define types of VLAN

a) *Data VLAN*: This is a VLAN that is configured to carry network data. This data could be voice, video or switch management.

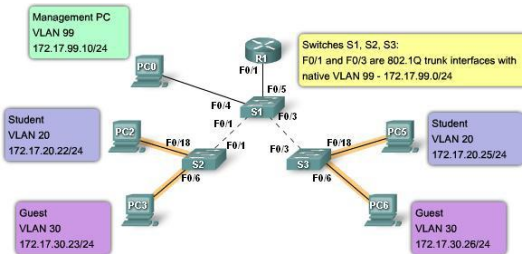

Figure 8 Data VLAN [25]

b) *Default VLAN*: The default VLAN for Cisco devices is VLAN 1. When switch ports are initialised they are connected to the default VLAN.

c) *Native VLAN*: The Native VLANs conforms to the IEEE 802.1Q standard though it deals with untagged Ethernet frames. Computers attached to the Native VLAN generates untagged Ethernet frames[27]

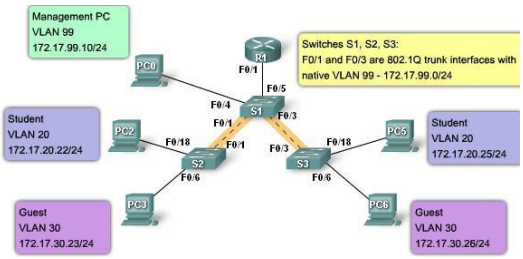

Figure 9 Native VLAN [25]

d) *Management VLAN*: This is a VLAN that carries switch management data. Switches are managed

 ISSN: 2321-8169
3945 - 3950

through HTTP, Telnet and SNMP. The protocol for managing switches is the VLAN trunking protocol and only stores identifiers within the normal range between 1 and 1005.

e) *Voice VLAN*: This is a VLAN that carries voice traffic used especially in VoIP networks. It is important that voice traffic is assured the highest priority in order to provide the required services like voice clarity. Voice VLAN provides the bandwidth and the security feature that would enable voice traffic to be routed through the network thereby improving quality of service.

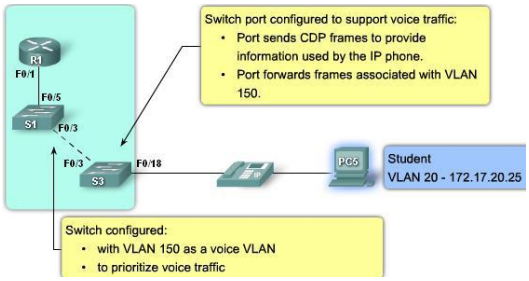

Figure 10 Voice VLAN [25]

D. Access Control List

This is a list that shows the users, nodes, resources and operations that are granted permission to use any resource like files. When a particular operation is needed to be carried out like a user wants to read a file, write to a file or execute a file, the ACL tells the operating system is checked to see whether such an operation has been granted permission[34]. ACL are set up to control the inflow and outflow of data packets through a network. Windows NT/2000 and UNIX-based systems make use of ACLs. There are two categories of ACL:

a) *Standard ACL*: This is a list of IP addresses from the source network which is applied to the destination network to either grant or deny access. Their range is from 1 to 99

b) *Extended ACL*: This is a list of source IP address, destination IP address, protocols and applications. Their range is from 100 to 199.

E. Wake-on-LAN(WoL)

This is a protocol that allows a system to be turned on remotely using magic packets, packet filtering and wake-on-ring[28][29]. WoL is platform independent and supports different version of operating system. It is usually employed during maintenance and scaling network resources. This grants the network administrator with the capacity boot up systems in a large network without necessarily turning it on physically. There are loopholes in the implementation of this standard in enterprise networks and one of them deals with its security implications[30]. It is recommended that an Access control list be created that would limit broadcast of magic packets to the computers to be turned on. A computer in a network sends data frames(magic packets) encapsulated in IP packet containing sixteen repetition of the MAC address of the computer to be turned on to all Network Interface cards connected to other computers. Once the computer receives the magic packets, it immediately turns on. The packets are transported efficiently by the Transport layer protocols. WoL system requirements can be a problem for large networks yet to implement although this has been overcome in present designs. When the packet arrives at the destination, delivery confirmatory messages are not sent, though magic packets are generated to lead to minimal resources usage. Turning the computer can lead to malicious activities that would prey on the computer's resources to avoid security measures should be put in place such as passwords [31].

REFERENCES

[1] Gerdes, J. and Tilley, S. "A conceptual overview of the virtual networking laboratory," in 8th ACM SIGITE conference on Information technology education, 2007, pp. 75-82.

[2] Graziani, R. & Johnson, A. "Routing protocols and concepts": CCNA exploration companion guide. Cisco Press, 2008.

[3] Harkins D. and Carrel D., "The Internet Key Exchange", Sterling, USA, Internet Engineering Task Force, 1998.

[4] Ahuja, A., Gupta N., Dewan K., Sood M. (2014). Deploying Pragramatic Techniques for Campus Network Design. In: Proceedings of SARC-IRF International Conference, 12th April-2014, New Delhi, India, ISBN:978-93-84209-03-2

[5] Purbo, Onno W. Jaringan Workgroup, LAN & WAN. Jakarta: PT Elex Media Komputindo, 1998.

[6] Patrick Luberus and Alfandika Nyandoro(2014). Implementing Wake-on-LAN in Institutional Networks. Journal of Applied Business and Economics Vol. 16(1) 2014.

[7] Davies J. Understanding IPv6. Microsoft Press. Second Edition. January , 2008.

[8] Muhammad Irfan Ashraf, Saman Iftikhar, Umer Sarwar and Aatzaz Latif(2013).Comparative Analysis of Link State and Hybrid Routing Protocols. International Journal of Computer Science and Management Research, Vol. 2, Issue 4, April 2013.

[9] Exposito J., Trujillo V., and Gamess E., Easy-EIGRP: A Didatic Application for Teaching and Learning of the Enhanced Interior Gateway Routing Protocol. In: Proc. of the Sixth International Conference on Networking and Services(ICNS). Cancun, Mexico. March, 2010.

[10] Guo Ning(2011). Construction and Implementation of Innovative Computer Network Praatical Teaching

System. Internaational Journal of Education and Management Engineering, 2011 Vol. 2, pp 97-102

[11] http://www.sans.org/reading_room/whitepapers/applications/approach-applications-security_16 accessed at 14th September 2014.

[12] Chong Wang, Jing-you Chen, "Implementation of GRE Over IPsec VPN Enterprise Network Based on Cisco Packet Tracer" International Conference on Soft Computing in Information Communication Technology(SCICT 2014).

[13] Diab W., S. Tohme and C. Bassil, "VPN Analysis and New Perspective for Securing Voice Over VPN Network", presented at the Fourth International Conference Networking and Services 2008, pp. 73-78

[14] Wen-Hwa Liao, Shuo-Chun, A Dynamic VPN Architecture for Private Cloud Computing, "Utility and Cloud Computing, IEEE International Conference". Pp. 409-414.

[15] S. Tanebaum, "Computer Networks", New Jersey, Prentice Hall, 2003. Pp. 773.

[16] R. Barbieri, D. Bruschi and E. Rosti." Voice over IPsec: Analysis and Solutions". 18th Annual Computer Security Applications Conference San Diego California, Dec 2002.

[17] Agbogun, Joshua Babatunde and Elijah, Fredrick(2013). Network Security Management:Solutions to Network Intrusion Related Problems. International Journal of Computer and Information Technology(ISSN:2279-0764), Vol 2, Issue 4, July 2013.

[18] Whitman M., H. J. Mattord, Principles of Information Security. Cenage Learning EMEA, 2009, 289.

[19] Boyles T., CCNA Security Study Guide: Exam 640-553. John Wiley and Sons, 2010, 249-280

[20] Oleg Sotnikov, Ammar Musheer and Shahram Shah Heydari(2011). Building Interactive Multi-User In-Class Learning Modules for Computer Networking. In: Proc. of the Seventh International Conference on Networking and Services(ICNS) 2011.

[21] Xiapu Luo Edmond W. W. Chan, Rocky K. C. Chang: Detecting Pulsing Denial-of-Service Attacks with Non-deterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing(2009).

[22] David Passmore and John Freeman, "The Virtual LAN Technology Report", 3COM White Paper, May 1996.

[23] Mosharaf M., Kabir Chowdhurry and Raouf Boutaba, "Network Virtualization: State of the Art and Research Challenges", IEEE Communications Magazine, July 2009.

[24] Forouzan B. H., Data Communication and Networking, TMH Pubilcations 4th Edition.

[25] Mohammad Serazul Islam, Md. Javed Hossain and Mohammed Humayun Kabbir(2014). Virtualization of Campus LAN and analyzing traffic issues of these VLANs. International Journal of Scientific & Engineering Research, Vol. 5, Issue 1, January 2014.

[26] Haris Mahmood Ansari, Abhinav Sharma and Harsh Singh Bhal(2013). Company Network Architecture. ER Publications, Vol. 2, Issue 7, July 2013.

[27] Rajul Chokshi and Dr. Chansu Yu, "Study on VLAN in Wireless Networks", 2007.

[28] Catalyst Layer 3 Switch for Wake-on-LAN Support Across VLANs Configuration.(2007). Retrieved from http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_example09186a008084B55C.shtml

[29] Raj Jirapure and Sanket Jirapure(2013). A Critical Review of Security Mechanisms in Virtual Private Networks. International Journal of Scientific Engineering and Technology, Vol 2, Issue 12, pp: 1168-1172, 1st Dec. 2013.

[30] Remote Management using Intel AMT.(2012). Retrieved from http://www.opengear.com/SP-AMT.html.

[31] Wake-on-LAN Packet Sniffer.(2011) Retrieved from http://profshutdown.com/wakeonlan_troubleshppt.aspx