International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

Experimental Analysis of Wireless Local Area Network Implementation for Airport based Internet Access in Nigeria

[1]Eke Christopher I; [2]Nweke Henry F & [3]Adoga Haruna U
[1] Computer science Department, Federal University Lafia Nigeria
[2] Computer Science Department, Ebonyi State University, Abakaliki Nigeria
[3]Computer science Department, Federal University Lafia Nigeria
[1]eke.ifeanyi@fulafia.edu.ng, [2]ufoo2010@yahoo.com, haruna.umar.adoga@gmail.com

Abstract

In recent years,the internet has become a very strong communication source around the globe more than ever before, businesses, financial institutions, the aviation sector, the healthcare sector, education sector and lots more rely on the internet as their backbone for functioning effectively and efficiently as we now live in what is referred to as the "Information Age". Thanks to Wireless technologies, users are provided with ease of staying connected with no geographical limitations. One of the strongest demands in computer networks is Wireless Local Area Network (WLAN) which provides us with seamless access to resources on the internet unlike Local Area Network (LAN), and is considered to save cost interms of design and implementation as the use of cables for interconnectivity is eliminated. This paper presents the design and implementation of wireless LAN in Airport departures lounge, it also provides the detailed simulation of a WLAN network which ensures that users accessing this network are satisfied with the quality of service in terms of high network availability, low latency and delay in the transmission of voice, video and data packets. Cisco routers, switches and access points were used for the simulation, dual Internet Service Providers are used to allow for fail over between links in an event of a downtime from one of the providers. User authentication is handled by a windows machine, as login credentials will be checked before users can get connected, this is to prevent unauthorised access to the network for users with malicious intent.

Keyword:
Wireless LAN simulation; Network Implementation; Network Address Translation; Packet Tracer Simulator

1 Introduction

The increased demands for mobility and flexibility in our daily life has led to the development of Wireless Local Area Networks (WLAN). This technology has found extensive applications in different areas such as educational institution, companies, hospitals and colleges where it offers unlimited access to internet and other network resources without the hurdles of layering, drilling into walls or putting up wired/ Ethernet cables through an office building or homes. With the huge benefits offered by wireless LAN, many international and Local Airports have started to build wireless "**hot spot**" to enable customers and officials have access to internet resources while they wait for their flights [**1**]. Nigeria as a developing nation is not an exception to this technological developments.

Wireless local area network (WLAN) makes it possible to connect computing devices locally and by breaking the data into packets. Very recently, wired internet network is migrating to wireless internet network. This is as a result of increase in speed, security and reduction in cost and risk found in the wireless network.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

WLAN are deployed as a result of the following advantages. E.g., easy deployment and self-organizing, heterogeneous nature of the network and cost saving. Despite these advantages, there are still challenges that are inherent in the network. Notable among the challenges confronting and inherent in WLAN are- limited bandwidth, security issues and interference in the access point. Defining the word Wireless Networks or (WLAN) is a bigger picture to understand for users with lack of technical background in computer networking. In a simple form, wireless networking is a way of connecting devices to the internet with a low cost infrastructure for a purpose of data communication without a cable attached to the computer, or mobile devices such as PDAs, Pagers. Smart Phone and Laptops to mention but a few. Wireless Local Area network Can also be seen as cellular architecture where the system is subdivided into cells known as Base Service set which is controlled by a Base station (Access Point).There are number of components needed for the implementation of wireless Local area networks, These include; Access point which helps to transmit and receive WLAN signals, Wireless medium which is responsible for the transmission and exchange of data from workstation to ISP, Work stations which could be a PC, Laptop or a PDA that enjoy the freedom communicating into a networks and Internet Service provider (ISP), that basically provide the internet to the Airport or other establishment [**2**].

There are basically two main architecture and methods for connecting the above listed components into the WLAN network architecture, and these are defined as an *infrastructure-less (Ad Hoc network)* and *Basic Service set* (BSS)

Infrastructure-less are a set of PC or a set of nodes that are connected with each other through a wireless medium without an infrastructure or an Access Point (AP). Figure 1 below describes an Infrastructure-less which is a set of 3 nodes communicating over a network. **[3]**

Basic service set is different from the above services. BSS has a numbers of nodes which are connected into the network via an Access point (AP).BSS is also called an infrastructure network or a centralised network, in which nodes receive signals broadcasted by the Access Point.The figure 2 below describe that nodes connected to network needs AP assistance to be able to transmit and receive information. Basically BSS is similar to the Infrastructure-less but has an access point as root unit. These architectures are as shown in figure 1 and 2

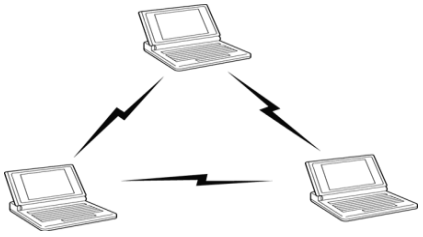

Figure 1: Basic Service Set

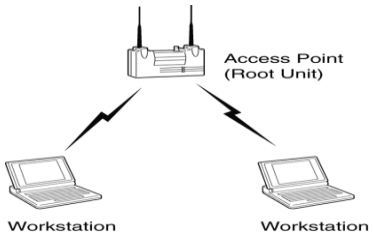

Figure 2: Extended Service Set

Most Airport implement the Basic Service set architecture (Ad hoc mode) as it provide best method to share resources and fast internet connection within the environment without huge infrastructure need. The above architecture can be connected to form Extended Service set (ESS) which consist more than 2 Basic Service set (BSS) Access Point as shown in figure 3

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

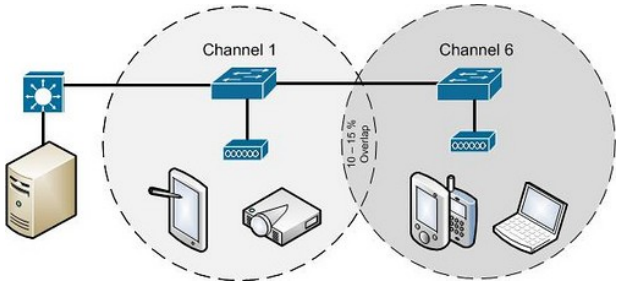

Figure 3: Extended Basic Service Set

In Extended service Set, the AP are connected via a distribution system or a Wired LAN that forward the traffic and also monitor the move of a mobile devices. The figure also shows that BSS-transition can move to another access point with condition of one ESS that is communicating with. **[3][4].**

In Wireless LAN OSI model (layer 2) Mac Access Control is very important for sending and receiving the packet across the network.Two main protocols for transmission of packets in Wireless LAN are*Distributed Coordinated Function (DCF)*and *Point Coordinated Function (PCF)* [**5**].

Distributed Coordinated Function (DCF) support Quality of service (Qos) based on MAC layer multimedia traffic that run on ***Carrier sense Multiple Access with Collision Avoidance (CSMA/CA)***that operates on back-off algorithm, that is it listen for the media Chanel if the media is free will starts to transmit packets, but if the media channel is busy the CSMA/CA wait until the media is free. DCF also uses back-off that enable the station to defer with an extra time until the channel is clear. DCF operate via ***Distributed Interframe space*(DIFS)** which waits for an amount of time before sending a packet, and***Request to Transmit Signal* (RTS) that**takes the control of the frame. The receiving stations listen and wait for a short of time ***short inter-frame space*(SIFS)** while receiving the RTS and replay with a **Clear to Send(CRT)** frame. The station that sends the packet waits similar to the DISF and send the data. The last stage once receiving the data, the station reply with an Acknowledgment to confirm the safety successful transmission

Point Coordinated Functions(PCF) on the other hand, works at ***Media Access Control*** (MAC) which is used in IEEE 802.11 standard in wireless LAN. PCF is the main terminology for coordinating the communication between the Access point and the stationthat coordinates which station must transmit first for a short time.Also PCF supports connection-free frames transfer, which means the Point takes the control and scans all station that that have PCF and poll them to transmit one at the time. For example, in a wireless network point coordinator is similar process in polling voting station in which all the votes are gathered and coordinators are able to count one box at the time and can only move to the next box when the contents of the first box are completely counted, in this scenario point coordinators poll the workstation A and only workstation A can transmit at that time the frames, once the workstation A is clear then the point coordinator will pull the next work station and counting the polling list in a process that each workstation has a chance that may send data.

In today's market,wireless LAN is dominating the market and there are number of standards out there that give the freedom mobility to the users. It is very important to discuss different standards deployed in Wireless Local area networks as it is vital in this experimental studies. The standards are deployed to meet users' need and flexibility when we talk about the bandwidth and coverage areas. As mentioned earlier, users sometimes complain

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

of receiving poor signal strength because of the distance of the access pointsand also the building walls, taking this into account IEEE has continue to develop new solution to meet users' Quality of service (QOS), better coverage, higher speed and more flexibility**[6][7]**. The IEEE 802.11 Standards are summarised in this section and **Table 1** below. Some of these standard has been explained below to enable organisations to know the standard to implement in terms of security, Quality of service and Speed.

- **802.11a Transmission**

802.11a technologies operate fully on 2.4 GHz frequency band based on ***Direct Sequence Spread Spectrum (DSSS)*** which is a modulation transmission technology that works when signal is transmitted from a workstation and expand the bandwidth to a higher bandwidth on a spectrum. Also this technology uses "***chips"*** to combined the spreading code over the spectrum and this shows that when a transmission signal is transmitted, it will be increase compare to original bit that is transmitted.This helps in a situation where if one of the sending original signal is lost during a transmission period then it can be recover using the redundancy transmission.

- **802.11b Transmission**

Comparing with 11a transmission technologies 11b uses***Orthogonal Frequency Division Multiplex*** (short named as OFDM) and is different transmission technology from DSSS. It operates at 5 GHz frequency band and has up to 23 channels. OFDM is a multi-digital carrier that use orthogonal to carry a multiple large amount of data that are defined as sub-carrier in respect to modulator that divide the radio signal to a multiple sub-signals and this process is then transmits continually to a frequencies from the receiver.

- **802.11g Standard Transmission**

11g transmission process is defined as above takes both those standards of modulation for transmitting the signal form a short distance range up to 54 Mbps at the 2.4 GHz band **[9].**These standards and more are summarised in **Table 1**

Table 1: Wireless LAN Standards

Task Group	Task
IEEE 802.11	Wireless LAN PHY and MAC specifications (infrared and 2.4GHz band
IEEE 802.11a	Wireless LAN PHY and MAC specification for 5GHz radio band
IEEE 802.11b	Higher-Speed (5.5Mbps and 11Mbps) wireless LAN and MAC specifications for 2.4 GHz radio.
IEEE 802.11c	Bridge operations with IEEE 802.11 MACs (incorporated into 802.11d)
IEEE 802.11d	Extensions to 802.11 for operation in additional regulatory domains
IEEE 802.11e	802.11 MAC Quality of Service (QOS) for advanced applications
IEEE 802.11f	Multivendor access point interoperability across distribution systems: IAPP
IEEE 802.11g	Higher Rate extensions in the 2.4 GHz radio band
IEEE 802.11h	Enhancements for dynamic channel selection and transmit power control
IEEE 802.11i	Enhancement for security and authentication
IEEE 802.11n	Design to improve throughput by giving enhancement such as multiple antennas, smart antenna change to signal encoding scheme and media access control (MAC) protocol. It has a data rate of 600Mbps and operates at 2.4GHz band.
IEEE 802.11x	Provide Security using Extensible Authentication Protocol and verify every workstation connected to the network

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

2. WLAN Security

Security is one of the major issues in any network setup including WLAN. Some preventive measures need to be carried out in order to protect bandwidth and reduce the workload to the access point which could cause delay to the network. Some of the security measures are:

- **Changing default setting of ESSID**

The default set of the ESSID is usually "101" which could be reset to a word length of between 0-256 characters. The resetting should be assumed a strong password using a long name and alphanumeric character when setting after which the AP needs to be configured to prevent ESSID broadcasting. This will only permit legal connection to the access point. **[8]**

- **MAC address filtering**

This is an inbuilt unique identity in every network card. It is static and implementing it will aid AP to maintain a group of MAC address and offer connection access to such group and discards the rest.

- **Encryption**

The network could be encrypted using temporal key Integrity Protocol (TKIP) and Wi-Fi protected Access (WPA).

- **Temporal key Integrity Protocol (TKIP)**

This is the WLAN security protocol that fixed the problem associated with WEP like small initialization vector and short encryption key. It also gets rid of collision attack that is also common in WEP by ensuring that key generation is different for every packet through the sequence number. TKIP also contain features referred to as message integrity check (MIC) which locks the whole where the hacker inputs data to get key stream used for encryption **[9][10].**

- **Wi-Fi protected Access (WPA)**

This encryption protocol uses master password that generates a dynamic key with the use of a protocol called temporal key integrity protocol. Such key is used once hence reducing the probability of the key discovery by the hacker **[11][12][13].**

3. Experimental and Design principle

At design stage,the following technical requirements such as access point's vendors and also standards (e.g. 802.11b or 802.11a) including the software and hardware components which are needed for design are considered. Radio frequency was another subject which focuses on how to determine the location and numbers of access points within an area.It was simulated usingCisco Packet tracer simulation tools to consider the complex of the network that was giving a better view and a decision making by the researchers.

The experimental analysis takes into consideration the Airport lounge in order to provide a flexible and reliable internet access to a higher of numbers of passengers.Their authentication will be via a (a third party authentication) "***Integrating Wireless Access Points with RADIUS"*** which will deal with payments and authentication codes based on numbers of hours the passengers will chose if need be.

Access points chosen above have been demonstrated and tested inCisco Packet tracer simulation to support all versions of IEEE 802.11a, IEEE 802.11b/g and IEEE 802.11n.Addition backup line was sourced from different supplier to make sure that customers have no network disruption while accessing the internet in case a primary line fails. Firewalls are configured on higher security by blocking some sites based on a log to be reviewed. A strong security method will be advocated to be taken by security Solutions

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

Company to provide users with a login mechanism and payments.
The area coverage are coved by four (4) access points which are all connected over the main core switch, and all the access points are tested to cover a minimum of 20-30m Radios. Thisis based on walls, reflection of the building and others access within departure lounge such as the Bar, restaurant, and duty free area.

Quality of service, QoS will also be considered and tested to ensure high quality when accessing different applications, for example the Skype or messengers' users which runs VOIP (Voice over IP) that packet travel form the sending station is guaranteed while the data flow and no packet dropping. Figure 6 below shows the typical wireless LAN architecture adopted for this experiment.

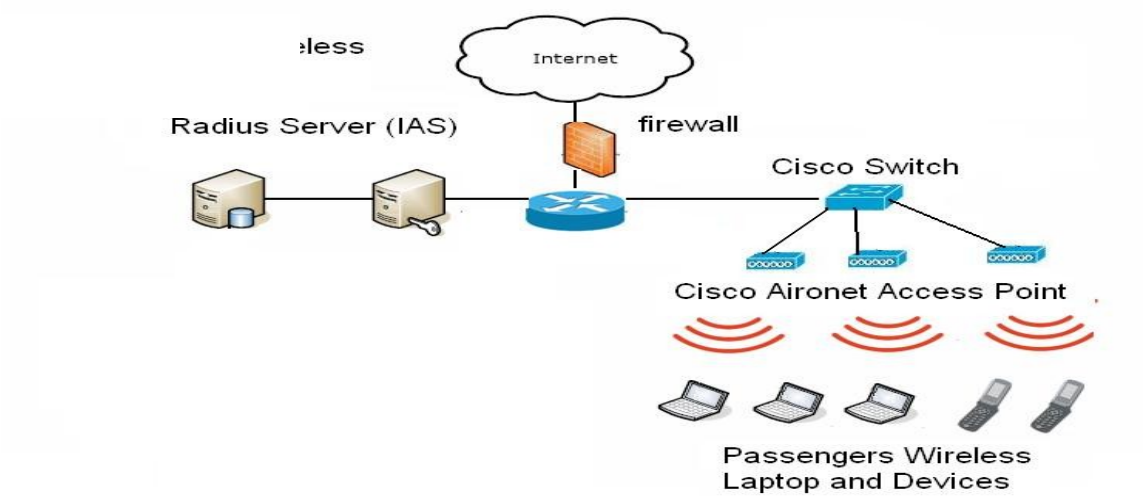

Figure 4: Typical wireless LAN Architecture

Figure 4 depicts the overview on how the network will look like after the installation. There is a firewall that filters the network from unauthorized access while allowing authorized communication. And a router that route the packet to the right destination. There is also a core switch that all four (4) access points are connected and finally passengers are connected with their devices via the access point.The design was carried out using the Cisco Packet tracer simulation software so that full functionality can be achieved since virtually all devices on the network are Cisco devices, the devices were added to the network and configured for testing.
Based on the requirement of the organization, in this case Airport, the access points will be situated in strategic locations in the airport departure lounge for passengers waiting to board airplanes in the airport.

Network Equipment for effective Experiment and Simulation :

1. Cisco 1841 Router
2. Cisco Ethernet switch 2960
3. Aironet Cisco 1200 Access point(s)
4. Client computers (Wireless device and Pc)
5. Radius server for user Authentication
6. Internet Service Providers (ISPs)

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

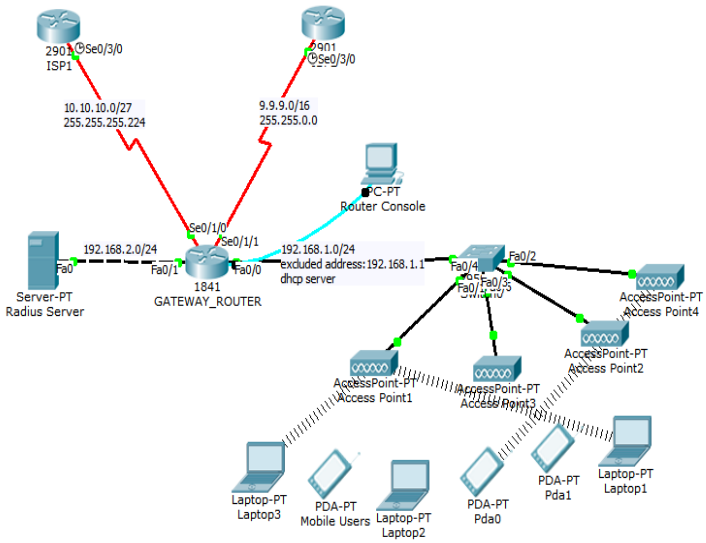

Figure 5 : Simulated Network topology using Cisco Packet Tracer Simulator

A Wide Area Network (WAN) connection is being simulated in the network to serve as the links coming from the Internet Service Providers (ISPs), note that two service providers are being considered for the network design hence the need for load balancing traffic between the two providers.

Table 1 : IP addressing Scheme

Simulated Device/Description	Network Address	Subnet Mask	Subnet prefix	Local interface IP address	Remote interface IP address
ISP1	10.10.10.0	255.255.255.224	/27	10.10.10.2/27	10.10.10.1/27
ISP2	9.9.9.0	255.255.0.0	/16	9.9.9.2/16	9.9.9.1/16
Authentication Server	192.168.2.0	255.255.255.0	/24	192.168.2.2/24	192.168.2.1/24
Gateway Router (Local LAN)	192.168.1.0	255.255.255.0	/24	192.168.1.1/24	DHCP clients
Gateway Router (Serial 0/1/0)	10.10.10.0	255.255.255.224	/27	10.10.10.1/27	10.10.10.2/27
Gateway Router (Serial 0/1/1)	9.9.9.0	255.255.0.0	/16	9.9.9.1/16	9.9.9.2/16
Gateway Router (Fa0/1)	192.168.2.0	255.255.255.0	/24	192.168.2.1/24	192.168.2.2/24

The addressing scheme used for the network design is for simulation purposes only just so the network behaviour can be simulated, tested and monitored before deployment. Public ip addresses will be provided by the Internet Service Providers (ISPs), these addresses will be translated into private ip addresses using Network Address Translation on the router.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

The Cisco 1841 router has been configured as the gateway device that the ISP links are connected to, since there will be two ISPs for the airport network, the router will also perform load balancing in the event that the backup link is going to be used for connectivity.

The fa0/0 interface of the router has been configured to perform Dynamic Host Configuration Protocol (DHCP) features, this helps in assigning IP addresses and default gateway parameters to hosts that are trying to connect to the network automatically, this implies that clients need not configure IP addresses on their devices manually when they need to connect to the wireless network in the airport. The figures6 to 8 below show the output of the experimental analysis running-config command on the command line interface (CLI) of the router.

The two serial interfaces that are connecting to the public internet are configured to perform network address translation (NAT), here the addresses coming from the local LAN in the airport are being translated into public IP addresses that can be used to access the internet, the figure below shows the configuration that was carried out using the router Command Line Interface (CLI), the show running-config command was used to get the output shown below.

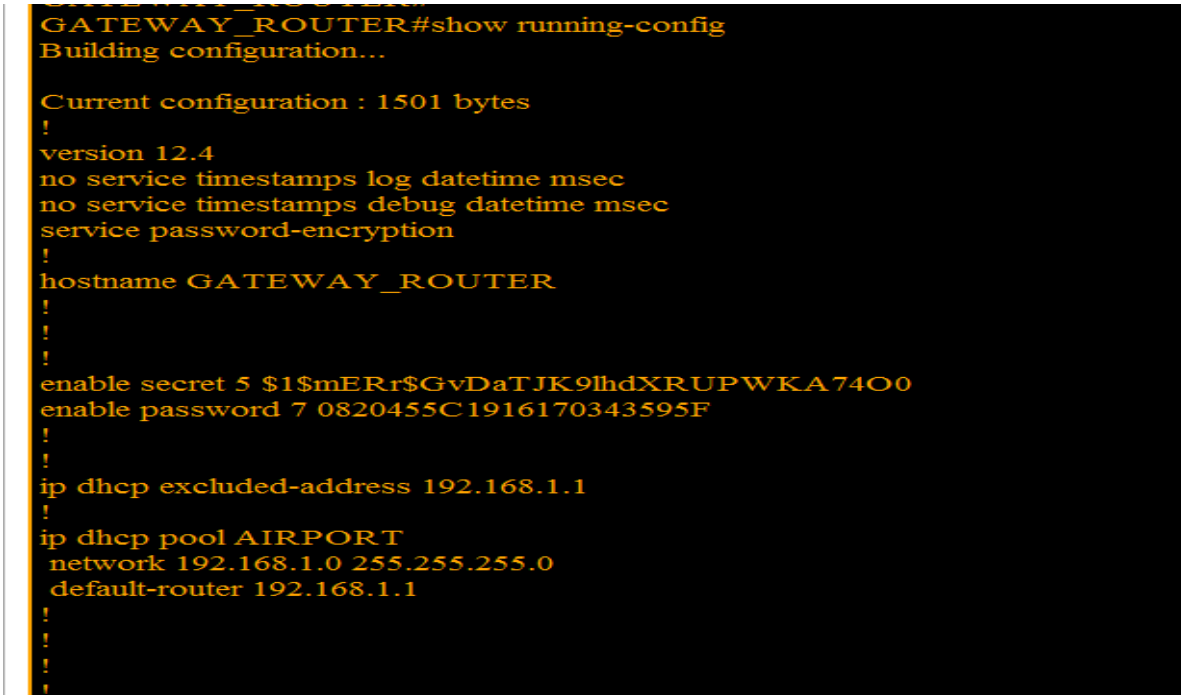

Figure 6: show running-config command output showing the DHCP configuration on the gateway router.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 4, April 2015
Available at http://internationaljournalofresearch.org

```
ip nat pool ISP1 10.10.10.1 10.10.10.200 netmask 255.255.255.0
ip nat pool ISP2 9.9.9.1 9.9.9.254 netmask 255.255.0.0
ip nat inside source list 1 pool ISP1
ip nat inside source list 2 pool ISP2
ip classless
!
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 2 permit 192.168.1.0 0.0.0.255
!
!
radius-server host 192.168.2.2 auth-port 1645
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 exec-timeout 0 0
 password 7 0820455C1916170343595F
 login
line vty 5 15
 exec-timeout 0 0
 password 7 0820455C1916170343595F
 login
```

7: Network Address Translation (NAT) as shown from the output of show running-config command.

```
 description LOCAL LAN
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface Ethernet0/0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/1/0
 description LINK TO ISP2
 ip address 10.10.10.1 255.255.255.224
 ip nat outside
!
interface Serial0/1/1
 description LINK TO ISP2
 ip address 9.9.9.1 255.255.0.0
 ip nat outside
!
```

Fig 8: Interface statuses and configuration as displayed by the show running-config command on the router CLI

The essence of experimental analysis of network design before implementation is to determine the number of users and data rate when the network is built. As noted by Offor et al [**14**], a single IEEE 802.11g link may use 54Mbps radio, but it will only provide up to 22Mbps of actual throughput while the rest are need to coordinate protocol signal.

Because the network will provide applications such as Email services, web browsing, Streaming audio and video which require large bandwidth for as long as it plays, Voice over IP and peer-to-peer file sharing applications. There is need to design a wireless LAN that can withstand high volume of traffics and users with enhanced quality of service.

The DHCP server was configured and simulated to distribute IP address within 192.168.1.1 with strong password authentication to ensure security of data. This simulation also provided an avenue to evaluate user experience before actual implementation,

5. Conclusion and future work

The benefits of wireless Local Area Networks (WLAN) in enhancing business process and quick access to network resources cannot be over emphasized. This has prompted many airport administrators and managements to implement different "hot spot" across different airport. The main issues faced during such implementation is how to determine the performance of these networks.

This paper outline the step by step experimental analysis of such projects. It provided simulated design of Wireless LAN using Cisco Packet Tracer ™ software implementation of such system.

References

[1]. William Stallings (2004). IEEE 802.11: Wireless LANs from a to n, IT professional, Vol. 6, no. 5 Pp 32-37.

[2]. Wan, X. Wang, X. Heo, U. Choi, J.(2010). A New AP-Selection Strategy for High Density IEEE802.11 WLANs, *2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*pp.52-58

[3]. FitzGerald J. Dennis A (1999) *Business Data Communication and Networks*.(6th ed) John Wily & Sons Inc USA

[4]. Khan J and Khwaja A. (2003) *building secure wireless networks with 802.11*. Wiley publishing Inc USA

[5]. Steven J. Vaughan-N. (July 2003) The Challenge of Wi-Fi Roaming*IEEE computer society pp*. 17-19

[6]. Available at http://www.comptechdoc.org/independent/networking/terms/wireless.html [Access on 12 November 2010]

[7]. Nitin, V. Anurag, D. Seema, G. Paramvir, B. (2005) Distributed Fair Scheduling in a Wireless LAN. *IEEE Transactions on Mobile Computing* pp. 616-629

[8]. David G. Leeper (2001)"A Long-Term View of Short-Range Wireless" *IEEE computing* pp. 39-44

[9]. Mohammad H, M. Gion R ,C. Chadi, B. Turletti, Th.(2005).Performance Analysis of the IEEE 802.11 MAC and Physical Layer Protocol, *Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks*pp. 88-97

[10]. H, L, Tsung. Marshall, A. Zhou, B.(2006). A QoS-based Rate Adaptation Strategy for IEEE a/b/gPHY Schemes using IEEE 802.11e in Ad-hoc Networks, *IEEE International conference on Networking and Services (ICNS'06)* pp. 113

[11]. Muelder, Ch. Ma K,L. Bartoletti T.(2005). A Visualization Methodology

forCharacterizationof Network Scans, *IEEE Workshops on Visualization for Computer Security* pp. 4

[12]. Tang, Y. (2006). Sharing Session Keys in Encrypted,*Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems*pp. 23-34

[13]. Mohammad, S. Khatib, I, Al. (2006). Performance of Secure Ad Hoc Sensor Networks Utilizing *IEEE802.11b WEP,2005 Systems Communications (ICW'05, ICHSN'05, ICMCS'05, SENET'05)* pp. 68-72

[14]. Offor, Kennedy J.; Obi, Patrick I.; Nwadike Kenny T. and Okonkwo I.I (2013). Structured Network Design and Implementation for Small Office Home Office-Tutorial Report. *International Journal of Engineering Research and Technology (IJERT)*, Volume 2, Issue 8. Pp 1342-1347.