Palestine Polytechnic University

College of Engineering

Virtualization for Multi-SSID Wireless LANs

By

Shurouq Hrebat **Israa Abusaif**

Supervisor

Dr. Murad Abusubaih

Submitted to the College of Engineering
In fulfillment of the requirements for the degree of
Bachelor degree in communications and electronics Engineering

Hebron, May 2017

Palestine Polytechnic University

Hebron – Palestine

Collage of Engineering

Department of Electrical Engineering

Project:

Virtualization for Multi-SSID Wireless LANs

Team:

Shurouq hrebat Israa abusaif

By the guidance of our supervisor, and by the acceptance of all members in the testing committee, this project is delivered to the Electrical Engineering Department in the College of Engineering, to be as a fulfillment of the requirement of the department for the degree of Bachelor's.

Supervisor signature

The head of department signature

جامعة بوليتكنك فلسطين

الخليل-فلسطين

كلية الهندسة والتكنولوجيا

دائرة الهندسة الكهربائية

اسم المشروع:

Virtualization for Multi-SSID Wireless LANs

أسماء الطلاب:

شروق عايد حريبات إسراء أبوسيف

بناء على نظام كلية الهندسة والتكنولوجيا وإشراف ومتابعة المشرف على المشروع ومتابعة أعضاء اللجنة الممتحنة تم تقديم هذا المشروع الى دائرة الهندسة الكهربائية وذلك استكمالا لمتطلبات درجة البكالوريوس في تخصص هندسة الاتصالات والالكترونيات

توقيع المشرف

توقيع اللجنة الممتحنة

--------------------------- --------------------------- ---------------------------

توقيع رئيس الدائرة

الإهداء :

اذا كان الإهداء يعبر ولو بجزء من **الوفاء فالإهداء**

إلى معلم البشرية ومنبع العلم ... نبينا محمد (صلى الله عليه وسلم)

إلى ينبوع العطاء الذي زرع في نفسي الطموح والمثابرة ... والدي العزيز

إلى نبع الحنان الذي لا ينضب ... أمي الغالية

إلى الذين رووا بدمائهم ثرى فلسطين إلى من هم أفضل منا جميعا إلى الذين ارتقوا إلى السمو ... شهداء فلسطين

إلى الذين عشقوا الحرية التي تفوح منها رائحة الليمون والبرتقال والنرجس... **الأسرى والمعتقلين**

إلى الذين هم رمز للاستبسال والشجاعة ... **أبطال غزة هاشم وأطفالها** وأطفال أهل اليرموك

إلى أعمدة العلم والمعرفة الذين خطوا لي وللآخرين صفحات الإبداع

إلى القلوب الطاهرة الرقيقة والنفوس البريئة إلى رياحين حياتي ... إخوتي

شروق , إسراء

Acknowledgment

First of all, Praise be to Allah, who has sent to his servant the book, the arbiter of success and the most merciful, without his blessing we should be lost!. For those who are giving us the unconditional love, support, advice, night and morning, tears and smiles…to our most beloved persons; dad and mom!. We also would to extend our deepest gratitude to our wonderful family, for their generous intentions and support .

In addition, Thank you to our wonderful supervisor and Deanship of Scientific Research of Palestine Polytechnic University, Dr. Murad Abusubaih, who gave and introduce us to the methodology of work and taking part in useful decision, giving necessary advices and guidance.

We express our deepest thanks to Dr. Gannam Aljaabre who gave us support and provided information in the field of virtualization during published paper .

Finally, it is my radiant sentiment to place on record my best regards, deepest sense of gratitude to many people, especially our classmates, friends and team members itself, who have made valuable work and comment suggestions on this project. We thank all the people for their help directly and indirectly to complete our assignment.

Thanks you,

The team members

Abstract

Nowadays, wireless APs support multi-band. They provide high bandwidth and data rates to support different applications and large number of users. Virtualization is known to be a proper approach for employing different networks over the same physical resources. In this project, we aim to design, configure and implement a network that provides different levels of security over the same access point. different networks on the same access point. The main challenge of this project is the implementation of virtualization mechanism to build different security algorithms over different interfaces.

الملخص

نظرا للتطور السريع في التكنولوجيا والشبكة العنكبوتية (الانترنت)وتزايد عدد المستخدمين له , كان لا بد من ايجاد تقنيات واستخدام قطع الكترونية مطوره للتسهيل على المستخدمين وتلبي استخداماتهم واحتياجاتهم بشكل سريع وسهولة التعامل معه.

مشروعنا عبارة عن تطبيق وتصميم شبكات افتراضية بمستوى عالي من الأمن والحماية , وذلك من خلال اضافة قطعة الكترونية خارجية للكمبيوتر تتصرف كنقطة وصول ,اضافة الى ذلك العمل على برمجتها لتقوم بهذا الهدف , بحيث تبدو للمستخدمين انها شبكة منفصلة عن الاخرى .

Contents

Chapter one: Introduction Page

Chapter two: Theoretical Background Page

Chapter three: Components And System Design Page

Chapter four: Design And Implementation Page

Chapter five: Testing And Results Page

Chapter six: Recommendations And Conclusion Page

CHAPTER ONE

Introduction

1.1 Preface

1.2motivation

1.3 related work

1.4 problem definition

1.5 solution approach

1.6 expected outcomes

1.7 Time Schedule

Chapter One

Introduction

1.1 Preface

In this chapter we introduce the project idea, objectives and expected outcomes. It describes the importance of virtualization technology. Then, it provides a summary about the problem addressed in this work. Related work is also discussed.

1.2 Motivation

In the last few years there has been a very fast growing in communications. Virtualization technology is becoming one of the fastest growing technologies, especially in the 21st century. In other words, virtualization technology now is becoming an important part of modern life. There are many projects and researches in the virtualization field. All aim to make the communications simpler and easier.

In this project it is aimed to use virtualization to create multi Service Set Identifier (SSID) Wireless Local Area Network (WLAN). We aim to design and simulate adapter WLAN cell on one access point (AP). We are interested in applying different security algorithms on adapter. The cell will appear to users as two networks.

To achieve this, it is planned to use external programmable WLAN adapter. The architecture will allow users with different privileges to connect to the network over the same hardware.

1.3 Related works

In [1], the authors introduce a software platform for hosting multiple virtual wireless networks over a shared physical infrastructure by means of open source virtualization techniques. Results have shown that the hosting platform can extend wireless networking into virtualized environments without compromising the performance, isolation, or wireless LAN security mechanisms.

In[2], the authors create virtual network devices that are not bound to any physical device, thus enabling to cope with packets sent over them entirely in software, which is totally different from real network devices. Instead of receiving packets from a physical media, virtual devices receive them from user land application attached to them. This enables the programmer to process the packets sent to this device as desired. The creation of virtual devices on top of wired connections, is mainly dealing with the transmission of IP packets or Ethernet frames coming from the OS to the "wire", without taking the physical medium and the card into consideration. The virtualization of a Wi-Fi interface therefore requires a very tight integration with the MAC sub-layers.

1.4 Problem definition

In previous relevant projects, authors programmed adapter to work as access point only. We intend to implement different security algorithms.

The main challenge of our project is the implementation of virtualization mechanism to build different security algorithms over different virtual interfaces.

1.5 Solution approach

As shown in figure 1. An AP will be used. We will create two virtual interfaces on the AP. The AP will announce adapter and two computers will be connected to SSID,.

Two security algorithms will be implemented on an adapter. The adapter is a Atheros wlan device(TL-WN722N).

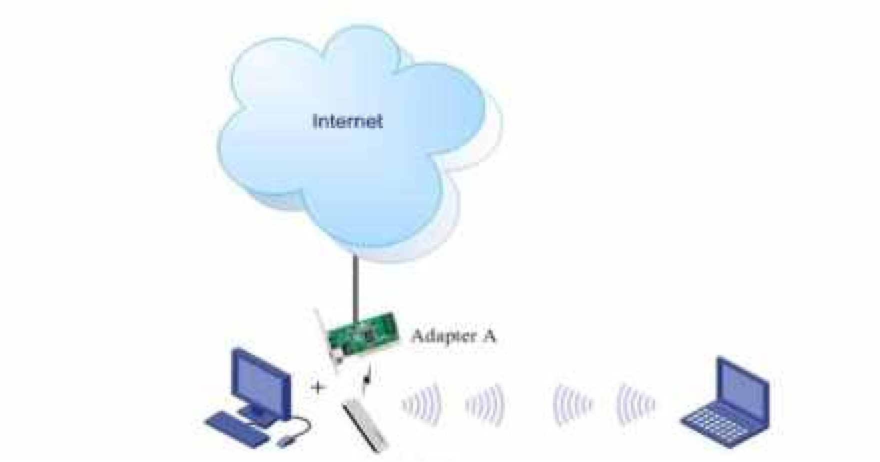


Figure 1: System Model.

1.6 Expected outcome

We expect to implement the different levels of security algorithm on different virtual interfaces.

1.7 Time Schedule

This section lists the phases and time schedule for the project for the first and second semester. Table1.1 and Table1.2 details distribution of the phased among the working weeks.

First semester (introduction to the graduation project)

Stage1: Select and discussion the idea

Determine and select the idea of project, the motivation, solution approach, and the main objective we intend to achieve.

Satge2: Preparing for project and collecting data about the idea

Determine the tasks and steps we want to perform is done, and collect more data and information about the project is prepared.

Stage3: Project analysis

To study all of the possible design options to determine our own design.

Satge4: Project requirement

after determine our design scheme, we specify all the needed requirements for the system, software and hardware.

Stage5: Documentation writing

Documenting the project will begin from the first stage to the last stage.

Time (week)	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
T1	■	■														
T2		■	■	■	■	■	■	■	■	■	■					
T3				■	■	■	■	■	■	■	■	■				
T4								■	■	■	■	■	■	■	■	
T5										■	■	■	■	■	■	

Table1.1: details distribution of the phased among the working weeks.

Second semester (graduation project)

Stage6: Preparing equipment

The needed hardware devices will be brought for the next stages.

Stage7: Programming the APs

The programming the access points of project is started and will be configured on PC.

Stage8: Preparing experiment setup

The programming of the project code is started and will be downloaded to the PC

Stage9: Complete implementation and testing

In this stage all programming and experiment setup will be ready to start testing and give a results. And the project is ready to use.

Satage10: Finishing the final report

Documenting the project will begin from the first stage to the last stage.

Time (week)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
T6	■	■	■	■												
T7					■	■	■	■	■	■	■					
T8							■	■	■	■	■	■	■			
T9									■	■	■	■	■	■	■	
T10										■	■	■	■	■	■	

Table1.2: details distribution of the phased among the working weeks.

CHAPTER TWO

THEORETICAL BACKGROUND

Chapter Two

Theoretical Background

2.1 Preface

This chapter provides a background on WLANs. It explains the differences between wired and wireless LAN, virtualization of WLAN interfaces and security algorithms in WLAN.

2.2 Wireless LAN Technology

Wireless LAN, also referred to as WiFi, is a local area network (LAN) that uses radio frequency (RF) to communicate instead of using wire. Wireless LANs can be used as an extension to an existing wired network or as an alternative to it. The IEEE 802.11 working group specifies the standards for wireless LANs, which govern wireless networking transmission methods.

2.2.1 Wireless LAN Standards

Wireless LAN technology primarily uses two unlicensed frequency bands: 2.4-GHz and 5.0-GHz band. The 2.4-GHz band is the most widely used frequency bands in WLANs. It is used by the 802.11b, 802.11g, and 802.11n IEEE standards. The 2.4-GHz frequency band is subdivided into channels, with 3 non-overlapping channels. The 5-GHz range is used by the 802.11a standard and the new 802.11n standard. The 5-GHz band is also subdivided into channels, with a total of 12 non-overlapping channels [3]. Wireless networks use different modulation techniques to encode data over radio waves, including DSSS, OFDM and MIMO. DSSS (Direct Sequence Spread Spectrum) is used by 802.11b, which uses chipping codes to send redundant data to minimize interference. OFDM (Orthogonal Frequency Division Multiplexing) is used by 802.11a and 802.11g. This technique divides a channel into multiple subcarriers to achieve redundancy and higher data rate. MIMO (Multiple-Input Multiple-Output) is used by the new 802.11n and allows a device to use multiple antennas for receiving signals in addition to multiple antennas for sending signals. MIMO technology can offer data rates higher than 100-Mbps by multiplexing data streams simultaneously in one channel [3]. Table 2.1 provides a comparison between wireless LAN standards.

	802.11b	802.11g	802.11a	802.11n
IEEE Ratified	1999	2001	1999	2008
Frequency Spectrum	2.4GHz	2.4GHz	5GHz	2.4GHz 5GHz
Nonoverlapping Channels	3	3	12	3 12
Modulation Technique	DSSS	DSSS and OFDM	OFDM	MIMO MIMO
Spatial Streams	1	1	1	1,2 and3 1,2 and3
Max Bandwidth	11Mbps	54Mbps	54Mbps	450Mbps 450Mbps

Table2.1: Wireless LAN standards.

The IEEE 802.11 defines various physical-layer (PHY) data rates for different WLAN standards such as 1, 2, 5.5 and 11 Mbps for 802.11b and 802.11g. The PHY rates for 802.11a and 802.11g include 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. 802.11n provides PHY rate up 150-Mbps with 1-stream, 300-Mbps with 2-stream, and 450-Mbps with 3-stream. The data rate is set and changes automatically to match the quality of the radio signal, which varies across the coverage. This process is called rate adaption. The wireless LAN throughput is bounded by the wireless channel bandwidth. It is clear that the actual throughput is generally less than 50% of the theoretical channel bandwidth due to the protocol overhead and other factors. For example, the typical peak throughput of an 802.11a/g wireless connection is actually less than 22Mbps and less than 200Mbps for 802.11n when the peak bandwidth is 450Mbps. In addition, throughput decreases as the wireless client moves further away from the AP and when interference from other wireless devices is present [4].

2.3 Wireless Local Area Network (WLAN)

Wireless networks have fundamental characteristics that make them significantly different from traditional wired LANs. While a wired LAN device must be physically attached to the wire in order to communicate, wireless devices communicate with each other via electromagnetic wave that has no visible boundaries. Any conformant device with reasonable signal reception can share the air medium and establish its own communication link. In the design of wired LANs, it is implicitly assumed that an address is equivalent to a physical location. On the other hand, in wireless LAN, the addressable unit is a station (STA), where each STA indicates a message destination and is not associated with a particular location. We describe Wireless LAN in more details below to facilitate deeper understanding of the differences between wireless LANs and wired LANs.

WLAN systems primarily operate in two unlicensed radio frequency bands: 2.4 GHz band and 5 GHz band. There are 14 channels designated in the 2.4 GHz band and 42 channels designated in the 5 GHz band**.**

Wireless networks are designed to support the same standards and the same protocols as wired networks, but there are some differences between them.

These differences can be summarized as advantages and disadvantages of the wireless local area networks WLAN.

Advantages of WLAN

1. Flexibility: WLAN is very flexible within the reception area, nodes can communicate without restrictions.

2. Planning: wireless ad-hoc networks don't need previous planning, but wired network need previous planning. In ad-hoc mode, the device follow the same standard so they can communicate, but in wired networks additional cabling with the plugs and probably interworking units (for example switch) have to be provided, in other words wired networks need wiring plans.
3. Design: wireless networks don't have wires, there is no wiring difficulties.
4. Cost: adding more devices in wireless network will not increase cost.

Disadvantages of WLAN

Disadvantages and shortcomings of WLANs can be summarized as follows:

1. Quality of service(QOS): wireless networks have less QOS. Wireless networks have less bandwidth compared to wired networks.
2. Safety and security: the protection of the transmission data in wireless networks doesn't exist or it may be less than it in wired networks. Wireless networks have low safety and security.

2.4 Infrared versus radio transmission

WLANs can be set using one of the two different basic transmission technologies, infrared light or the radio transmission.

Infrared technology uses a diffuse light in figure 2.1.wireless transmission medium that carries data through the air using light beams and sending and receiving device must be line of sight. The advantages of this technology are its simple and cheap sender and receiver which are integrated in many mobile devices, in addition to this infrared doesn't need licenses.

The disadvantages of infrared technology are its low band width compared to other LAN technologies, and it is easily shielded. An example of this technology is IrDA(Infrared Data Association) interface available anywhere.

Radio technology uses the license free ISM band at 2.4GHz and 5GHz bands in figure 2.2. Its advantages are in its coverage area. In radio technology, coverage area is large. Radio technology has very limited license for frequency band and this is disadvantage of this technology. An example of radio technology is WLAN in laptop.

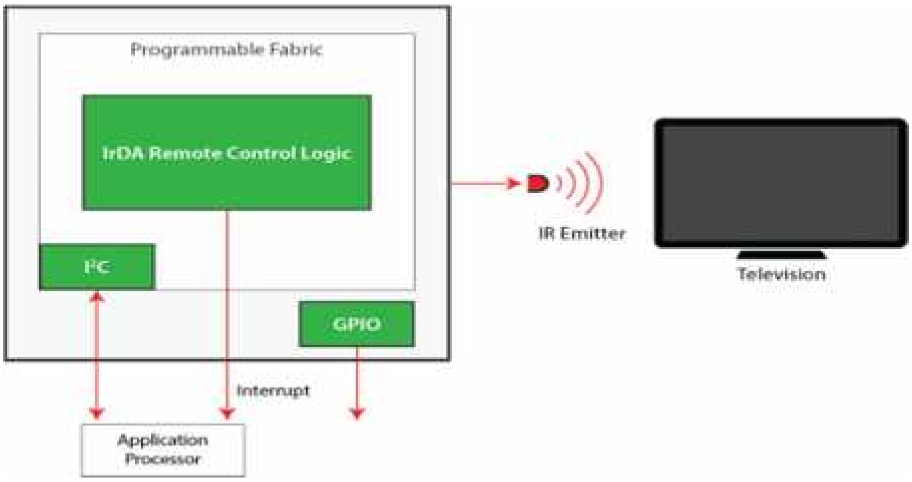


Figure 2.1 Infrared transmission.

Figure 2.2 Radio transmission.

2.5 The architecture of wireless networks

The architecture of the wireless networks is divided into logical architecture and physical architecture.

Logical architecture

It is the structure of the standards and the protocols that make a connection between nodes (physical devices) and control data flowing between them.

This architecture is represented by the seven layers of Open System Interconnect(OSI) network model, and the protocols that operate in this model.

OSI network model

The open system interconnection model divided the application to application connection into seven layers as in figure 2.3.

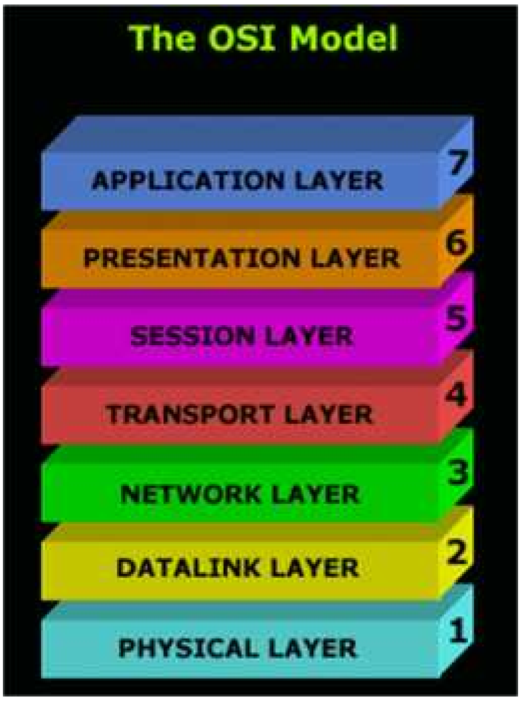


Figure 2.3 OSI model.

Physical architecture

It is represented by wireless networks topologies and hardware devices.

Wireless networks topologies are:

1- Point to point connections:

It has many situations:

a) Peer to peer connections (ad-hoc connection).

A peer-to-peer network allows wireless devices to directly communicate with each other in figure 2.4. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network. This can basically occur in devices within a closed range.

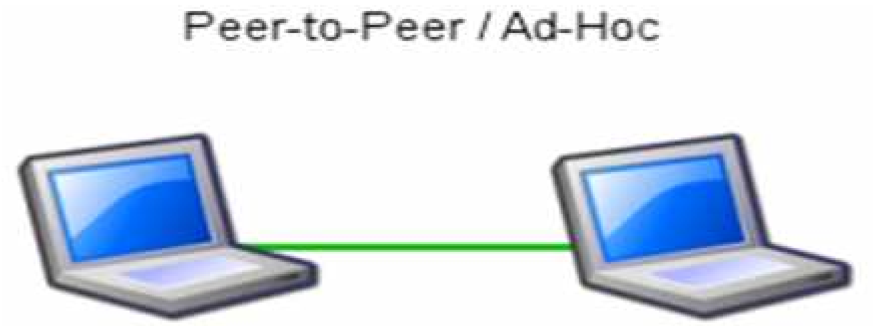


Figure 2.4 Peer to peer connection.

b) LAN wireless bridging.

A bridge can be used to connect networks in figure 2.5, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN.

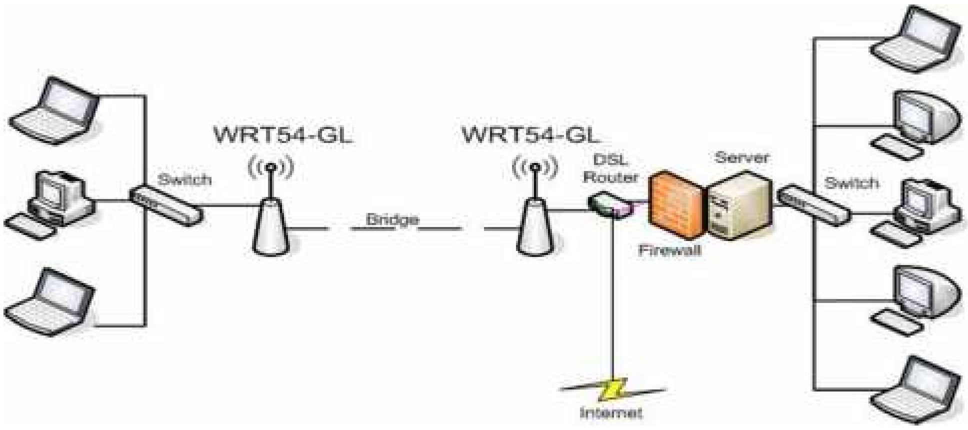


Figure 2.5 Bridging connection.

c) Bluetooth.

It is an open area wireless protocol for exchanging data over short distances (using short length radio waves) from fixed and mobile device in figure 2.6, creating personal area network(PAN).

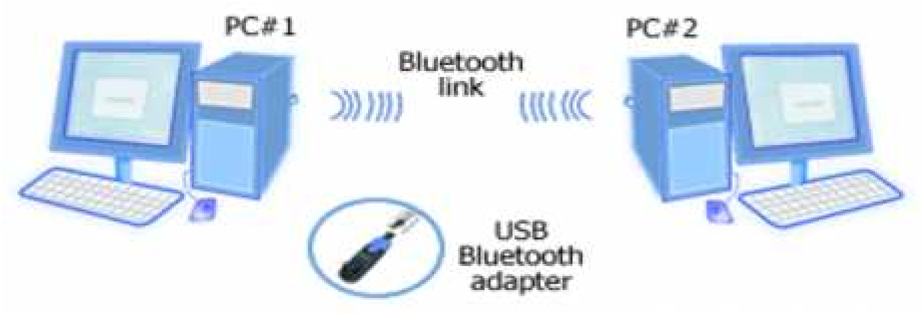


Figure 2.6 Bluetooth connection.

2- Star connection

The node at the center may be a WiMAX base station, WiFi access point, or Bluetooth master device in figure 2.7.

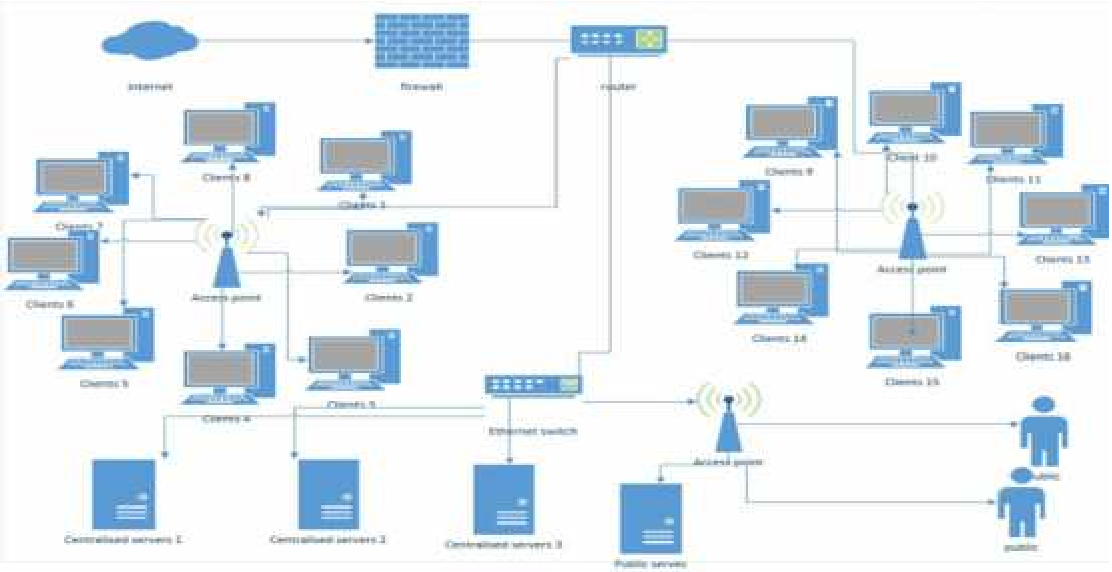


Figure 2.7 Star connection.

2.6 Medium Access Control layer(MAC)

The MAC layer is implemented in every station.

MAC layer has three basic functions:

1- It provides data delivery service to the users of the MAC through frame exchange protocol.
2- It controls access to the shared medium through two access mechanisms, distributed coordination function(DCF) and point coordination function(PCF).
3- Protection the delivering data.

2.7 System Virtualization

System virtualization enables running multiple operating systems (OSs) and applications concurrently on the same physical machine, eliminating the need for multiple physical machines. Each virtual machine (VM) has its own operating system and applications such as the physical machine [5,6,7]. Thus making the applications unaware of the underlying hardware, yet viewing computing resources as shared resource pools available via virtualization. The term guest is usually used to refer to the virtual network (VM) while the host is used to refer to the hosting environment. Virtualization was first developed in the 1960s by IBM company to partition large mainframe computer into several logical instances for better hardware utilization. These partitions allowed mainframes to run multiple applications and processes at the same time [5]. Since mainframes were expensive resources at that time, they were designed for partitioning as a way to reduce the cost and to improve the efficiency.

The primary benefits offered by virtualization are resource sharing and isolation. Unlike real environments where physical resources are dedicated to a single machine, virtual environments share physical resources such as CPU, memory, disk space, and I/O devices of the host machine with several VMs. By isolation, applications running on one VM cannot see, access, and use resources on other VMs [5]. Virtualization provides a software abstraction layer on top of hardware. This layer is called Virtual Machine Monitor (VMM), also known as a hypervisor. The main task of the VMM is to manage the hardware resource allocation for VMs and to provide interfaces for additional administrative and monitoring tools [5]. However, the functionality of the VMM varies greatly based on architecture and implementation.

2.8 Network Virtualization

Network virtualization allows multiple heterogeneous architectures to run concurrently in a shared network environment. Network virtualization often combines hardware and software resources to deploy virtual networks for different architectures. Over the years, the term virtual network has been used to describe different types of network virtualization or traffic isolation. These are:

2.8.1Virtual Local Area Network

A virtual LAN (VLAN) is a group of logically networked hosts with a single broadcast domain regardless of their physical connectivity. All frames in a VLAN have a VLAN ID and network switches with VLAN support use both the destination MAC address and VLAN ID to forward frames. Since VLANs are based on logical instead of physical connections, configuration and management of VLANs are simpler than physical LANs. VLANs provide isolation at Layer 2 [8].

2.8.2 Virtual Private Network

A VPN is a dedicated network connecting multiple sites using private and secured tunnels over shared or public networks like the Internet. In most cases, VPNs connect geographically distributed sites of a single enterprise. Each VPN site contains one or more customer edge (CE) devices that are attached to one or more provider edge (PE) routers [8]. VPNs are implemented in Layer 2, Layer 3 and higher layers.

2.8.3 Overlay Network

An overlay network is a logical network built on top of existing physical network. The Internet itself started off as an overlay on top of the telecommunication network. Overlays in the Internet are typically implemented in the application layer. However, various implementations at lower layers of the network stack also exist [8].

2.9 Virtualization of WLAN interface

World, systems, applications and people need to be permanently connected to the internet, a variety of communications networks and several different devices simultaneously. Ideally, faced with this context, there should be a single device with a single network interface, and a single program that enables several connections and protocols to be used simultaneously, making the entire systems simple to use and easy to install and operate, thus leading to the desired levels of stability and reliability.

Virtualization refers to technologies designed to provide a layer of abstraction between computer hardware systems and the software running on them. By providing a logical view of computing resources, rather than a physical view, virtualization solutions make it possible to do a couple of very useful things: They can allow, essentially, to trick operating systems into thinking that a group of servers is a single pool of computing resources. And they can allow to run multiple operating systems simultaneously on a single machine.

Virtualization of wireless LAN interface is more complicated than for wired network interface because the capacity of wireless channel varies with radio signal strength and interference from other wireless LAN devices. This requires to include complex management functions into wireless devices to achieve efficient and reliable communication. Examples of such management functions include data rate adaption, power management, and power control. The device driver, which is part of the OS, is also involved in such management functions for control and configuration. In contrast, wired LAN devices are data centric and have very little management functions [9,10].

The limitations of full virtualization approach for the wireless network interface come from the difficulty to emulate WLAN management functions. IEEE 802.11 MAC functions are a superset of 802.3 MAC functions, and many management functions will get lost when emulating IEEE 802.11 device as 802.3 devices. Using a paravirtualization approach is technically possible. However, the WLAN management functions are complex and the management interface between host driver and wireless LAN device is often proprietary, which requires support in the hypervisor. With a hardware based virtualization approach such as SR-IOV, the wireless network interface card (NIC) is equipped with multiple radio resources that operate on different channels. This approach significantly increases the complexity and cost of wireless NIC [9].

A typical WLAN device consists of: RF transceiver, Baseband, and MAC layer. The RF transceiver performs radio signal transmitting and receiving, while the Baseband mainly responsible for digital signal processing. RF transceiver and Baseband are generally referred to as PHY layer. The MAC layer often consists of a hardware controller on the WLAN device and a software driver on the host computer. Most of the wireless LAN functions such as authentication and authorization are performed at MAC layer [1,9].

In the beginning, the MAC layer was entirely managed by the firmware on the wireless LAN device. This approach is called Full-MAC, where full MAC layer functionality is executed by the hardware controller on the wireless device. New implementation of wireless LAN devices is based on Soft-MAC approach, where most of the MAC layer functionality is moved to device driver on the host computer, with the firmware providing a set of functional primitives. This approach provides a high degree of software control over the MAC layer functions, while still allowing the PHY layer to define the radio waveform [1,11].

Virtualization of the wireless radio can be achieved in multiple ways such as in space, frequency and time.

Space Division Multiplexing (SDM): This is the simplest approach, where physical resources are partitioned in space. Each physical node hosts one virtual node per running experiment. A wireless experiment is assigned a set of physical nodes such that transmitting nodes from different experiments do not interfere with each other [12].

Frequency Division Multiplexing (FDM): In this approach, different experiments are partitioned in the frequency domain for their communication needs. Each physical node is equipped with multiple virtual nodes, each configured with the frequencies allocated to the corresponding experiment. Interference between the different experiments are avoided by ensuring that different experiments are assigned non-interfering channels [12].

Time Division Multiplexing (TDM): In this case, the entire wireless network is partitioned in time across the different experiments. Each experiment is assigned a time slot during which each physical node in the system activates the virtual node corresponding to this particular experiment [12].

Advantages of virtualization in software and hardware environments

1- Virtualization allows multiple operating systems and applications to reside on a single computer.

2- Virtualization provides consolidated hardware to achieve higher productivity from fewer servers.

3- Virtualization provides a simple IT infrastructure with very low maintenance.

4- Virtualization allows for the deployment of new applications much more quickly than in non-virtual environments.
5- Virtualization helps to reduce the number of hardware resources at a ratio of 10:1 or even better in some cases.
6- Virtualization ensures an environment that is robust, affordable and available all the time.

As the most widely used wireless standard, IEEE 802.11 (WiFi) is considered to be indispensable. Despite the performance of Wifi has been improved dramatically, new techniques are still needed to further enhance it to cope with the ever-growing demand. Virtualization has been proposed as a promising solution. Virtualization has been implemented in network interface and access point (AP).

The WiFi networks have a centralized structure as APs are responsible for almost all the major functions such as managing, scheduling and data transmitting. Each WiFi enabled device is bonded to a certain AP. Any transition from one AP to another AP will cause Quality of Service (QoS) interruption to some extent. This issue is non-negligible in WiFi networks because moving from place to place is very common and most WiFi APs have limited coverage distance. Virtualization by its nature provides the possibility to let one device be virtually connected to several APs simultaneously. This will mitigate the transition effect and thus improve the overall performance[13].

On the other hand, load balancing is another wired networks idea which is not feasible until virtualization is implemented. As the number of APs is increasing, they are overlapping each other more often. Therefore load balancing among APs could bring the benefits like reduced equipment cost and improved reliability to WiFi networks. Load balancing has been proved very effective in wired networks and has even more potential in WiFi networks since the offload from the wired networks to WiFi networks will be dominating in the next decade[13].

Another interesting proposal introduced in is to implement several virtual access points in a single physical AP. This design will enable better sharing of the limited wireless resource. In this case, virtualization happens in the AP which is another approach to applying virtualization in WiFi networks.

2.10 Security algorithms in WLAN

Wireless LAN deployment improves users mobility, but it also brings a range of security issues that affect emerging standards and related technologies.

Many companies, organizations, and even individuals implement wireless local area networks(WLANs) in various locations such as their offices, conference rooms, homes, and business areas. This type of connection offers users **portability** because they can move from one location to another while maintaining access to the corporate network, but it does not offer access between locations. **Mobility**, on the other hand, lets users access the corporate network not only near multiple access locations but also everywhere in between. WLANs let users access a high-speed connection in areas where physically wired networks can't penetrate or are not cost effective[14].

Although WLANs solve some problems that exist in traditional wired LANs, they also introduce new security issues. In this article, we identify wireless security using security encryption, we believe that WLAN security can be enhanced to an acceptable level by a proper combination of countermeasures.

Network security is an important issue especially in wireless networks where the network is open and the network perimeter is not exactly known.

Various wireless security protocols were developed to protect home wireless networks. These wireless security protocols include WEP, WPA, and WPA2, each with their own strengths — and weaknesses. In addition to preventing uninvited guests from connecting to wireless network, wireless security protocols encrypt private data as it is being transmitted over the airwaves.

Although many of these issues have since been addressed, wireless networks are generally not as secure as wired networks. Wired networks, at their most basic level, send data between two points, A and B, which are connected by a network cable. Wireless networks, on the other hand, broadcast data in every direction to every device that happens to be listening, within a limited range.

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

Following are descriptions of the WEP, WPA, and WPA2 wireless security protocols:

1-Wired Equivalent Privacy (WEP): The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well-known security flaws, is difficult to configure, and is easily broken. In the WEP (Wired Equivalent Privacy) encryption security method, wireless stations must use a pre-shared key to connect to your network. This method is not recommended, due to known security flaws in the WEP protocol. It is provided for compatibility with existing wireless deployments.

2-Wi-Fi Protected Access (WPA): Most current WPA implementations use a pre-shared key (PSK), commonly referred to as WPA Personal, and the Temporal Key Integrity Protocol (TKIP, pronounced tee-kip) for encryption. WPA Enterprise uses an authentication server to generate keys or certificates. The WPA-Personal (Wi-Fi Protected Access) security method (also called WPA-PSK) uses MIC (message integrity check) to ensure the integrity of messages, and TKIP (Temporal Key Integrity Protocol) to enhance data encryption. WPA-Personal periodically changes and authenticates encryption keys. This is called rekeying.

This option is recommended for small networks, which want to authenticate and encrypt wireless data.

3-Wi-Fi Protected Access version 2 (WPA2): Based on the 802.11i wireless security standard. The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is sufficient (and approved) for use.

As you may already know, WEP security can easily be cracked -- which is why it is a good idea to upgrade to WPA2 (Wi-Fi Protected Access 2).

WEP security only protects your wireless network from average users. Even newbie hackers can download free tools and follow a tutorial to crack your WEP key. This enables them to connect to your Wi-Fi network and possibly access network shares. Plus it gives them the ability to decode real-time traffic on the network.

In contrast, Wi-Fi Protected Access 2 (WPA2), which uses AES/CCMP(Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) encryption, is the most secure option available to adequately protect wireless network. There are two flavors of WPA and WPA2: Personal or Pre-shared Key (PSK) for home use and Enterprise for business use.

CHAPTER THREE

COMPONENTS AND SYSTEM DESIGN

Chapter three

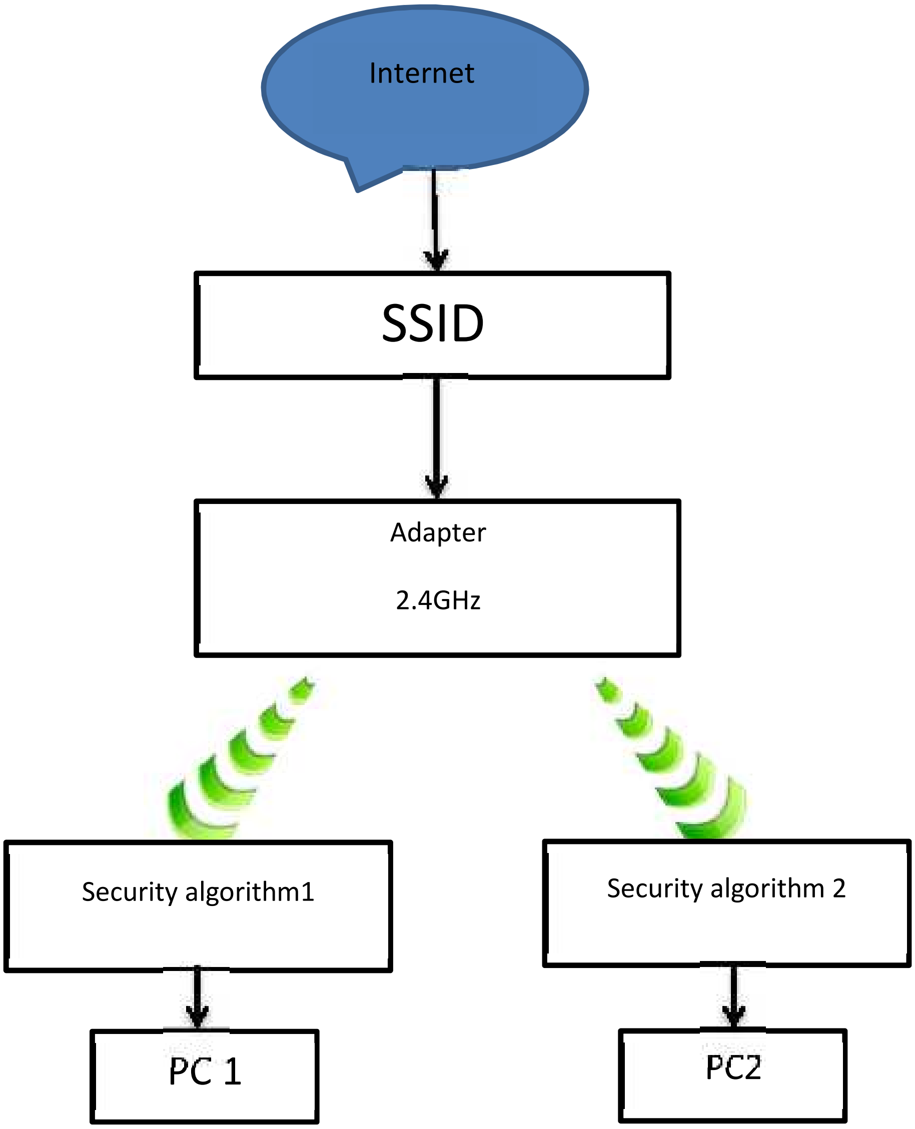
Components And System Design

3.1 Preface

This chapter provides the components of our project and explain it. And this chapter gives more details and information about it to be able to constructs and design the block diagram of our project.

3.2 System block diagram

We will create two virtual interfaces on the AP. The AP will announce two SSIDs and two computers will be connected to each one, each on the same SSID. Two security algorithms will be implemented, each on an SSID. The type of adapter is TP link (TL-WN722N), will work as master mode with different level of security.



3.3 Components

In our project, components are divide into hardware and software components.

3.3.1 Hardware Components

Hardware components is very important parts. So we choose it to be suitable to achieve the aim of our project. For more details in next lines.

1-Adapter

Wireless local area network adapters are add on devices that enable to connect to wireless networks like at office, hotel or house. These adapter can be added to either desktop or laptop computers, so long as the hardware and software are compatible. While wireless adapters enable more mobility and freedom in connecting to networks.

Windows and other operating systems support both wired and wireless network adapters through a piece of software called a device driver. Network drivers allow application software to communicate with the adapter hardware. Network device drivers are often installed automatically when adapter hardware is first powered on.

Some network adapters are purely software packages that simulate the functions of a network card. These so-called virtual adapters are especially common in virtual private networking (VPN) software systems.

The router in our houses is clear across the building from our rooms, which is on the other side. Because of this, we have problems connecting wireless devices to the internet from our rooms. For this reason, we decided to use a wireless dual band PCI express adapter (**TL-WN722N)** we have as an access point in figure 3.1.

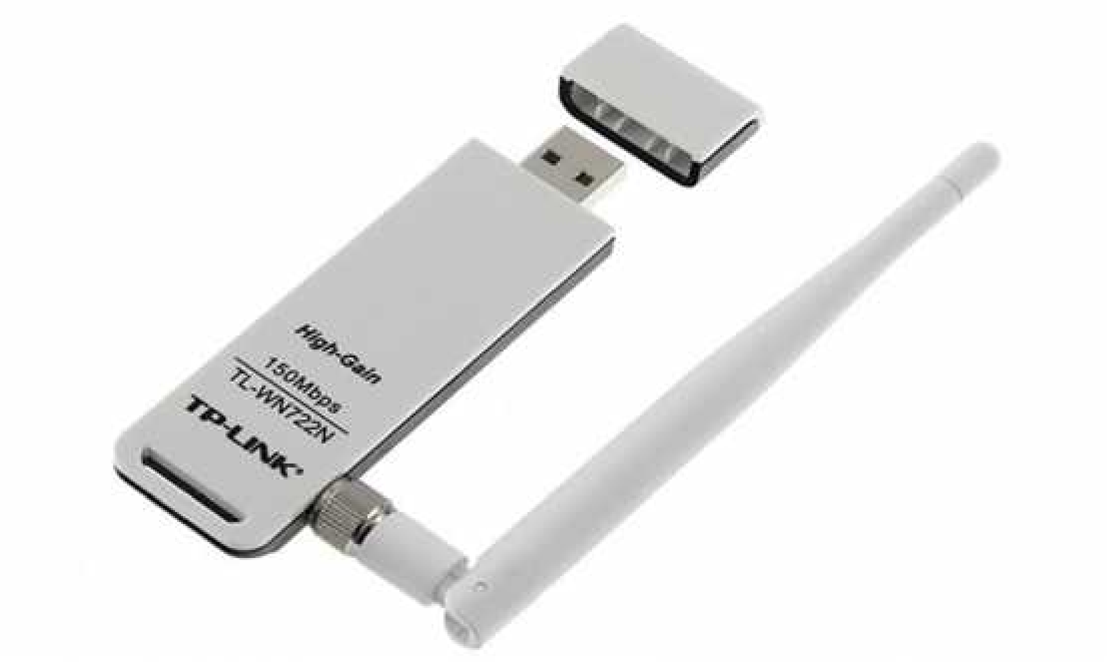


Figure 3.1: TL-WN722N.

The adapter(TL-WN722N) is an 802.11n client device designed to deliver a high-speed and unrivaled wireless performance for your desktop. With a faster wireless connection, it can get a better Internet experience, such as downloading, gaming, video streaming.

With the 802.11n technology, higher throughput improvements using MIMO (multiple input, multiple output antennas), the TL-WN721N/TL-WN722N's auto-sensing capability allows high packet transfer rate up to 150Mbps for maximum throughput. It has good capability on anti-jamming, and it can also interoperate with other wireless (802.11b/g) products. The adapter supports WEP, WPA and WPA2 encryption to prevent outside intrusion and protect personal information from being exposed.

With unmatched wireless performance and security protection, TL-WN721N/TL-WN722N is the best choice for easily adding or upgrading wireless connectivity to desktop.

TL-WN721N features:

1- Complies with IEEE802.11n, IEEE802.11g, IEEE802.11b standards.

2- Supports WPA/WPA2 data security, IEEE802.1x authentication, TKIP/AES encryption, WEP encryption.

3- Supports maximum throughput rate up to 150Mbps for TL-WN721N/TL-WN722N and it can automatically adjust to lower speeds due to distance or other operating limitations.

4- Provides USB 2.0 interface.

5- Supports Ad-Hoc and Infrastructure modes.

6- Good capability on anti-jamming.

7- Supports roaming between access points when configured in Infrastructure mode.

8- Easy to configure and provides monitoring information.

9- Supports Windows XP/7/8/8.1/10 32/64bit, Mac OS X 10.6 - 10.11 and Linux.

10- 4dBi detachable antenna, remarkably strengthen signal power of the USB adapter.

TL-WN722N is an Atheros wlan device, because the Atheros chipset support more than one access point at the same time figure 3.2.

Figure 3.2: Atheros chipset.

Chipset supported:

- AR9271.
- AR7010 USB-PCI bridge with AR928x wireless chips.

Adapter specifications:

Hardware features: table3.1.

Interface	USB 2.0
Button	WPS Button
Dimensions (W x D x H)	3.7 x 1.0 x 0.4 in. (93.5 x 26 x 11mm)
Antenna Type	Detachable Omni Directional (RP-SMA)
Antenna Gain	4dBi

Table3.1: hardware feature of TL-WN722N.

Wireless features: table3.2.

Wireless Standards	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Frequency	2.400-2.4835GHz
Signal Rate	11n: Up to 150Mbps(dynamic) 11g: Up to 54Mbps(dynamic) 11b: Up to 11Mbps(dynamic
Reception Sensitivity	130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Transmit Power	<20dBm
Wireless Modes	Ad-Hoc / Infrastructure mode
Wireless Security	Support 64/128 bit WEP, WPA-PSK/WPA2-PSK
Modulation Technology	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Advanced Functions	WMM, PSP X-LINK(For Windows XP), Roaming

Table3.2: wireless feature of TL-WN722N.

This device supports a maximum of 2 simultaneous AP and 7 clients VIFs w/ **ath9k_htc.** Because of this feature we decide to use this device.

ath9k_htc [15]:

Information:1-Module name(s): ath9k_htc.

2-Authorship tag: vendor, community.

3-Status: in-kernel.

Function:1-MAC architecture / mode: SoftMAC.

2-Driver framework(s): mac80211.

3-Notable limitations: supports a limited number (7 max.) of simultaneous associated clients in AP mode.

Supported Modes: 1- STA (Station) mode: supported.

2-IBSS (Ad-Hoc) mode: supported.

3-AP (Master) mode: supported.

4-P2P mode: supported.

5-Monitor mode: supported.

6-Packet injection: supported.

3.3.2 Software Components

Software components in our project is very important to install external TL-WN722N adapter on computer on linux operating system using IW tools. And implement different security levels on each network.

The main three software component we will use it is linux operating system, Ubuntu and packages must be installed.

1- Linux operating system

Linux is one of popular version of UNIX operating System. It is open source as its source code is freely available. It is free to use. Linux was designed considering UNIX compatibility. Its functionality list is quite similar to that of UNIX.

Components of Linux System

Linux Operating System has primarily three components. In figure3.4:

1-**Kernel** : Kernel is the core part of Linux. It is responsible for all major activities of this operating system. It consists of various modules and it interacts directly with the underlying hardware. Kernel provides the required abstraction to hide low level hardware details to system or application programs.

2-**System Library** : System libraries are special functions or programs using which application programs or system utilities accesses Kernel's features. These libraries implement most of the functionalities of the operating system and do not requires kernel module's code access rights.

3-**System Utility**: System Utility programs are responsible to do specialized, individual level tasks.

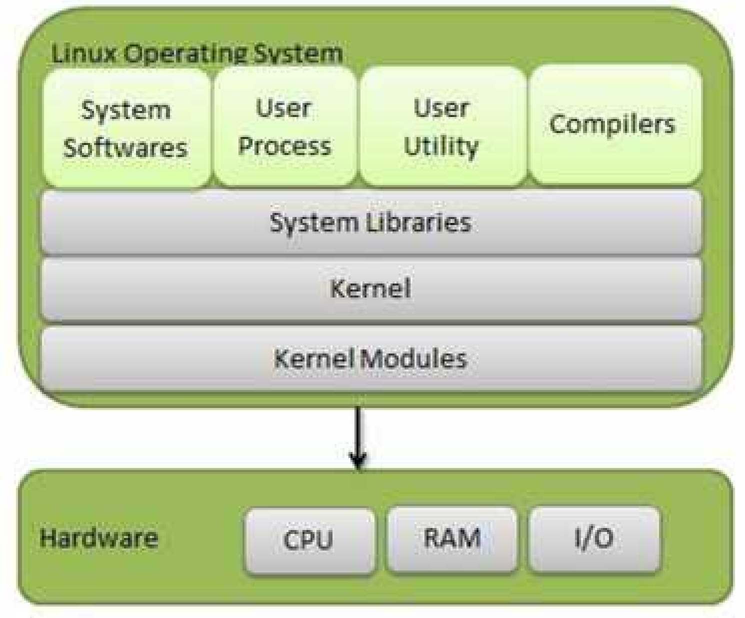


Figure 3.4: Linux components.

Kernel component code executes in a special privileged mode called **kernel mode** with full access to all resources of the computer. This code represents a single process, executes in single address space and do not require any context switch and hence is very efficient and fast. Kernel runs each processes and provides system services to processes, provides protected access to hardware to processes.

Support code which is not required to run in kernel mode is in System Library. User programs and other system programs works in **User Mode** which has no access to system hardware and kernel code. User programs/ utilities use System libraries to access Kernel functions to get system's low level tasks.

Type of command lines:

1- Linux **utility programs** — sort, cut, join, and hundreds of others — are powerful and flexible tools that are ready to run with a few keystrokes. Options let you fine-tune (or completely change) how utilities work.

2- Powerful **I/O redirection** lets you save data to files, read data from files, and connect a series of utilities together in a pipeline that lets you custom-build exactly what you need… again, with just a few keystrokes. GUI applications — which have to pack all possible operations into a set of menus and checkboxes — can't be nearly as flexible or powerful.

3- Linux commands can operate on many files at once. **Filename completion** lets you specify filenames by typing a few characters and the TAB key. **Wildcards**, which let you specify one or many files with just a few keystrokes. The pattern [A-Z]*.txt matches any filename that starts with an uppercase letter and ends with .txt; that could be many files. ([:upper:]*.txt handles non-English filenames too.) Use /home/*/data0[0-5] to match all files named data00 through data05 in all directories under */home* — for instance, */home/amy/data01*, */home/randolph/data06*, and so on.

4- A shell is actually an interpreter for a programming language: the language of command lines. It puts powerful loops, tests, variables, I/O manipulation, error-trapping, and more at your fingertips when you type a command line.

Put these same command lines in a script file, and you have a shell script — which lets you repeat those stored commands anytime you want to. It's the same language from the command line or from a script file. Learn the shell "language" and you can use it both places!

5- **Command substitution** lets you use the output of one command as part of another command line. If you haven't used a shell before, this is hard to explain… but, trust us, it’s very powerful. For instance, you can run a file-search program like find, then run another command on the files that find found.

Following are some of the important features of Linux Operating System:

1-Portable : Portability means software can works on different types of hardware in same way. Linux kernel and application programs supports their installation on any kind of hardware platform.

2-Open Source : Linux source code is freely available and it is community based development project. Multiple teams work in collaboration to enhance the capability of Linux operating system and it is continuously evolving.

3-Multi-User : Linux is a multiuser system means multiple users can access system resources like memory/ ram/ application programs at same time.

4-Multiprogramming : Linux is a multiprogramming system means multiple applications can run at same time.

5-Hierarchical File System : Linux provides a standard file structure in which system files/ user files are arranged.

6-Shell : Linux provides a special interpreter program which can be used to execute commands of the operating system. It can be used to do various types of operations, call application programs. etc.

6- **Security** : Linux provides user security using authentication features like password protection/ controlled access to specific files/ encryption of data.

The following illustration shows the architecture of a Linux system.in figure 3.5.

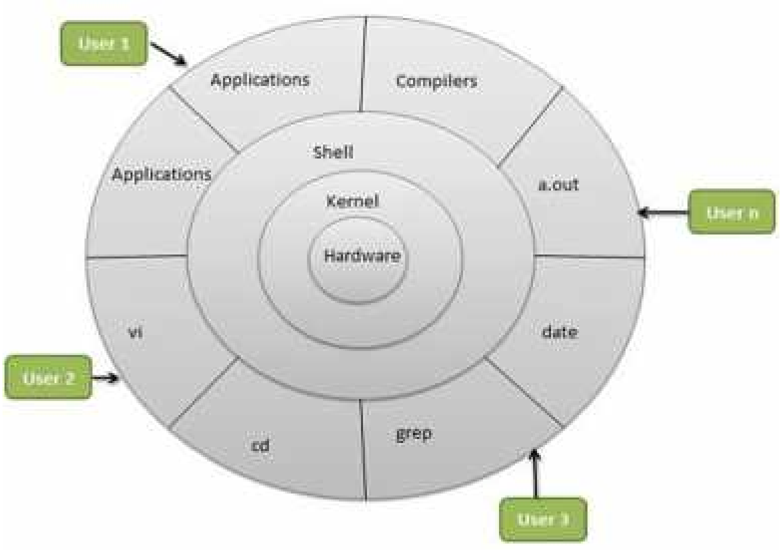


Figure3.5: architecture of a Linux system.

The architecture of a Linux System consists of the following layers

1-Hardware layer : Hardware consists of all peripheral devices (RAM/ HDD/ CPU etc).

2-Kernel : It is the core component of Operating System, interacts directly with hardware, provides low level services to upper layer components.

3-Shell : An interface to kernel, hiding complexity of kernel's functions from users. The shell takes commands from the user and executes kernel's functions.

4-Utilities : Utility programs that provide the user most of the functionalities of an operating systems.

Linux is also distributed under an open source license. Open source follows the following key philosophies:

- The freedom to run the program, for any purpose.
- The freedom to study how the program works, and change it to make it do what you wish.
- The freedom to redistribute copies so you can help your neighbor.

- The freedom to distribute copies of modified versions to others.

The above are crucial to understanding the community that comes together to create the Linux platform. It is, without a doubt, an operating system that is “by the people, for the people”. These philosophies are also one of the main reasons a large percentage of people use Linux. It’s about freedom and freedom of choice.

The most popular Linux distributions are:

- Ubuntu Linux.
- Linux Mint.
- Arch Linux.
- Deepin.
- Fedora.
- Debian.
- openSUSE.

Each distribution has a different take on the desktop. Some opt for very modern user interfaces (such as Ubuntu’s Unity, above, and Deepin’s Deepin Desktop), whereas others stick with a more traditional desktop environment (openSUSE uses KDE). In our project we choose Ubuntu linux.

use the apt-get tool for installing software:

sudo apt-get install **package name**

The sudo command is added because need super user privileges in order to install software.

2- Ubuntu

A community-developed Linux-based operating system that can be used on desktops, laptops and servers. The operating system includes a variety of applications including those for word processing, e-mail applications, Web server software and also programming tools. Ubuntu is free of charge, including enterprise releases and security updates. It also comes with full commercial support from Canonical. Ubuntu is available in both a desktop and server edition.

1-Ubuntu is Free and so any other Linux distro.

2-Ubuntu is more stable.

3-You can update everything on your system with just one update manager. No need to run separate Update manager for all the software you installed. (Saves system resources).

4-old computer will get a second life. Because Ubuntu does not need those high resources as Windows.

5-When we have installed Ubuntu, don't have to install anything else to get started with productivity.

3- Packages

1-iptables

Iptables package is an extremely flexible firewall utility built for Linux operating systems. And is a command-line firewall utility that uses policy chains to allow or block traffic. When a connection tries to establish itself on system, iptables looks for a rule in its list to match it to.

Tables in iptables structure figure3.6:

1. Filter Table

It is the default table in iptables. There is no need to specify the table name for defining the Rules. Different inbuilt chains in this table.

1.1 INPUT Chain

INPUT Chain is for managing packets input to the server. Here we can add Rules to control INPUT connections from remote to the server.

1.2 FORWARD Chain

To add Rules to manage packet connections from one network interface(NIC) to another on the same machine.

1.3 OUTPUT Chain

The OUTPUT Chain control packets from the server to outside. Here we can add different rules to manage outbound connection from the server.

2. NAT table

Network address translation (NAT) is a methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another. The default inbuilt chains for NAT tables are:

2.1 PREROUTING chain

As the name indicates its translate packets before routing.

2.2 POSTROUTING chain

Translate packets after routing completes.

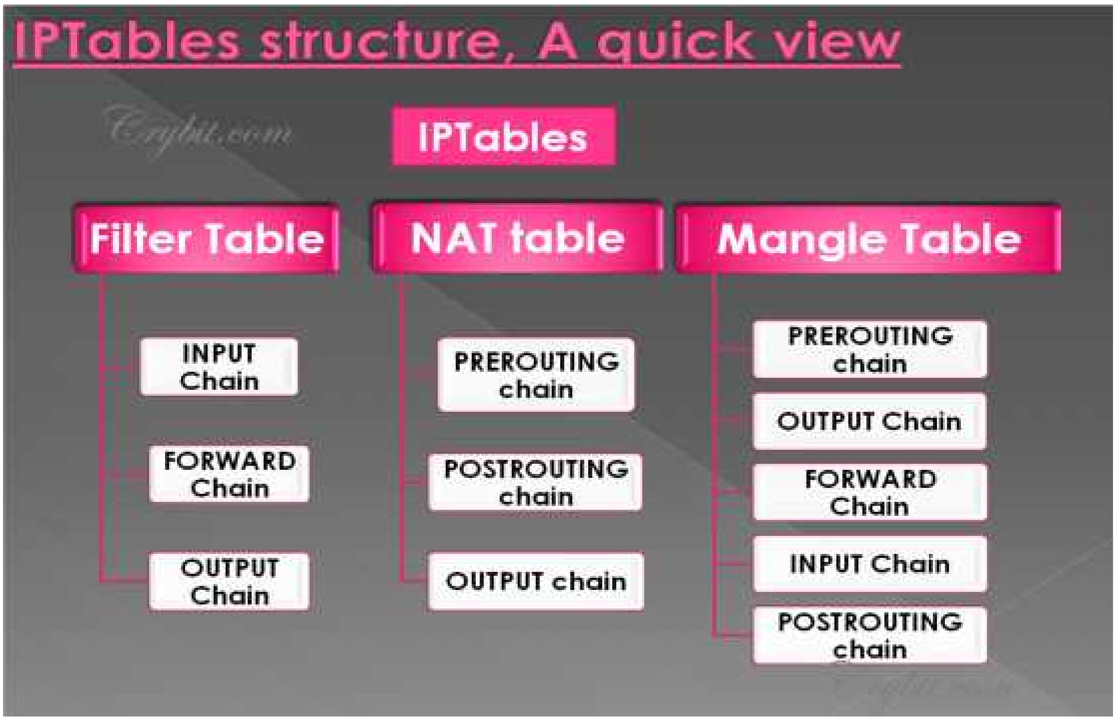


Figure3.6: Tables in iptables structure.

iptables almost always comes pre-installed on any Linux distribution. To update/install it, just retrieve the iptables package:

```
sudo apt-get install iptables
```

2-Hostapd

hostapd is a user space daemon for access point and authentication servers. It implements IEEE 802.11 access point management, IEEE 802.1X/WPA/WPA2/EAP Authenticators, RADIUS client, EAP server, and RADIUS authentication server.

hostapd is designed to be a "daemon" program that runs in the background and acts as the backend component controlling authentication. hostapd supports separate frontend programs.

```
sudo apt-get install hostapd
```

wpa_supplicant/hostapd

wpa_supplicant and hostapd come as a pair of complementary client and host for wireless access points.

That is hostapd allows us to create access points from the command line, which allows one to share one's internet connection wirelessly, while wpa_supplicant allows us to scan and to connect to access points as a client in order to get onto the Internet.

3.4 IW tools

Wireless tools for Linux is a collection of user-space utilities written for Linux kernel-based operating systems to support and facilitate the configuration of device drivers of wireless network interface controllers and some related aspects of networking using the Linux Wireless Extension**.**

Iw is a new nl80211 based CLI configuration utility for wireless devices. It supports all new drivers that have been added to the kernel recently. The old tool iwconfig, which uses Wireless Extensions interface, is deprecated and it's strongly recommended to switch to iw and nl80211[16].

Package tools. In table 3.3.

Package tools	Command form	task
Help	iw help	Just enter.
Getting device capability	iw list	to get device capabilities for all devices, such as band information (2.4 GHz, and 5 GHz), and 802.11n information**.** And display additional information about them that is not displayed by iwconfig.
Scanning	iw dev wlan0 scan	output provides many additional details over the iw list scan output.
Event	iw event	displays wireless events generated by drivers and setting changes that are received through the RTNetlink socket. Each line displays the specific wireless event which describes what has happened on the specified wireless interface.
Event	iw event –t	sometimes timing information is also useful**.**
Name	If rename	allows to rename wireless network interfaces based on various static criteria to assign a consistent name to each interface.
Display	Iwconfig	used to display and change the parameters of the network interface which are specific to the wireless operation**.**
Monitor	Iwspy	used to monitor a set list of nodes and record the link quality of each of them.
Specific details	Iwpriv	used to manipulate parameters and setting of the Wireless Extension specific to each driver (as opposed to iwconfig which deals with generic ones)**.**

CHAPTER FOUR

DESIGN AND IMPLEMENTATION

Chapter four

Design And Implementation

4.1 Preface

This chapter describes a new approach to use only one physical WLAN interface. It also describes the implementation of such approach based on open source virtualization techniques and multi-SSID capability given by Atheros WLAN devices.

4.2 Wireless LAN Virtualization

With the introduction of IEEE 802.11n and the increase in bandwidth, wireless LAN virtualization is required as an alternative approach for deploying multiple wireless networks with different authentication methods. Wireless LAN virtualization enables several virtual wireless networks to coexist on a common shared physical WLAN device. Multiple virtual interfaces can be created on top of the same radio resources, allowing the same functionality as in multi-radio solution.

All virtual interfaces operate concurrently without considering the physical nature of the wireless medium as well as physical management tasks. Each virtual interface abstracts a single wireless device and has its own wireless network and its own unique MAC address. From the application’s perspective, the virtual wireless network behaves like wired Ethernet, but is wireless.

Using the wireless LAN virtualization technique, a virtual interface (VIF) can be configured to operate as virtual access point (AP).

4.2.1 Virtual Access Point

A virtual AP is a logical AP constructed by wireless LAN virtualization technique and is bound to a virtual network interface. Each virtual AP independently keeps the configuration and service of the wireless network. In this way, several virtual APs can be configured on top of solely one physical wireless LAN device.

When a single physical wireless device supports multiple virtual Aps Figure 4.1, each virtual AP appears to users as an independent physical one. Since each virtual AP is logically separated, wireless LAN providers may use virtual APs to offer multiple services on the same physical infrastructure. Alternatively, virtual APs can be shared by multiple providers allowing each provider to offer separate services for their subscribers [17].

Figure4.1: 1-single physical wireless device supports multiple virtual Aps(real implementation of the project).

A virtual AP acts as the master device in a virtual wireless network and operates in much the same way as real AP, allowing wireless devices to communicate with each other by managing. In general, the virtual AP consists of two parts: control plane and forwarding plane. The control plane is concerned with the information that define the functionality of the AP such as SSID, operation mode, and RF channel. While, the forwarding plane defines the part of the AP that uses a lookup table as a base to forward packets to its destinations [18].

HostAP [19] is an open source software for controlling wireless LAN authentication and association. It implements IEEE 802.11 AP management and provide support for several security mechanisms such as WPA, WPA2/IEEE 802.11i, and IEEE 802.1X. The current version of HostAP support Linux operating system and OpenBSD [19].

4.3 Virtual WLAN Approach

The main goal of this approach is to combine wireless network functionality into a common virtualized environment and to achieve performance levels comparable to the native hardware wireless LAN. A similar approach named virtual WiFi [9] has been taken to provide wireless LAN client functionality. However, virtual WiFi approach is intended to support mobile client environments.

This approach is suitable for virtualizing wireless LAN infrastructures, where multiple separate wireless LANs can be deployed on a shared physical infrastructures with different security mechanisms. Since each virtual wireless LAN is logically separated, wireless LAN providers may use virtual WLANs to offer multiple services on the same physical infrastructure. Alternatively, virtual WLANs can be shared by multiple providers allowing each provider to offer separate services for their subscribers [2].

To wireless LAN clients, each virtual WLAN appears to be an independent physical AP or router. In other words, a separate, distinctly configured virtual APs can run simultaneously with different addressing, forwarding, and wireless security settings. For example, one virtual AP can be configured to provide WPA/WPA2 security, while another virtual AP is configured to offer Open or WEP connectivity to clients.

The virtual WLAN approach is based on the Atheros WLAN chipset which supports concurrent wireless connections sharing the same PHY layer of the wireless LAN device.

This capability in wireless LAN devices is also referred to as multi-SSIDs, where each SSID is equivalent to a VLAN on a wired network. I extend multi-SSIDs capability to operate in the virtualization environments, where each virtual WLAN can have its own addressing, forwarding, routing, and security mechanism. In this approach, virtual WLANs belonging to the same wireless network interface share the same radio channel being used and thus the available bandwidth.

To emulate a physical AP, it is necessary to provide the emulation at different layers such as layer 2 (MAC), layer 3 (IP), and above. At the MAC layer, the behavior of a physical AP is being emulated by allocating a distinct MAC address and SSID to each virtual AP. At the IP layer, it is emulated by allocating a distinct IP address and potentially a Fully Qualified Domain Name (FQDN) to each virtual AP. In higher layers, the emulation can be carried out by providing each virtual AP with a unique authentication and accounting configuration such as (a shared key, or EAP methods with RADIUS authentication), or SNMP communities.

In our approach, a virtual wireless AP or router is constructed by configuring the two VIF to operate in AP mode. This sets the main functionality of the wireless AP such as IEEE 802.11 operation mode, SSID, and security mechanism. Once configured, the wireless interface is attached to a virtual switch to enable MAC forwarding similar to a physical AP. Then, the virtual AP interface is connected to a virtual router (VR), in the same way as the virtual Ethernet interface, to enable IP forwarding and routing.

Since this approach adds wireless LAN infrastructure functionality to virtual environments, it can be deployed for different wireless LAN systems on the same host machine such as authentication services and intrusion detection, providing secure virtual wireless LAN solution on the same hardware.

4.4 Benefits of Virtual WLAN Approach

The virtual WLAN approach provides the following benefits:

1- Virtual WLAN approach doesn’t require the use of multi-SSIDs with VLANs to provide traffic differentiation for virtual SSIDs. When using multi-SSIDs, all traffic from each virtual SSID will be handled by a common forwarding table. When using multi-SSID with VLANs, the traffic from each virtual SSID is tagged with a unique VLAN ID to have a unique forwarding table. Although this solution provides traffic differentiation for virtual SSIDs, it requires an additional Ethernet switch to control the traffic for each virtual SSID.

2- Virtual WLAN approach doesn’t require the use of Wireless LAN Controller/Switch to control the wireless network. WLAN Controller is used to manage several lightweight APs from a single location. Unlike standalone APs that require the configuration for each device, a wireless LAN controller/switch can be used as a centralized device for configuration and management. By using the virtual WLAN approach, it is possible to manage the virtual APs representing the virtual WLANs and all wireless parameters like the channel to be used, operation mode, and transmission power from the virtual environment.

3- Each virtual WLAN can have its own access authentication and encryption method.

4- Each virtual WLAN can have its own IP addressing and routing, DHCP (Dynamic Host Configuration Protocol) and DNS (Domain Name System) services, and firewall and IDS (Intrusion Detection System) features.

5- Finally, virtual WLAN approach enables the creation and configuration of different wireless LAN systems without the need to purchase and deploy physical wireless LAN infrastructure.

4.5 Implementation of Virtual WLAN Approach

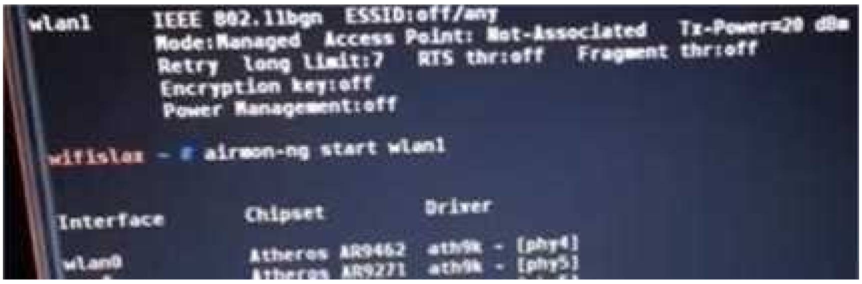
The multi-SSID capability given by the Atheros chipset allows implementing multiple IEEE 802.11 networks on a single physical wireless device with Linux OS (Linux kernel version 2.6.33 and higher), since it includes a wireless device driver supporting this capability.

WLAN device driver in Linux is divided into two modules: kernel module (hardware dependent) and protocol module (SoftMAC). The hardware dependent module varies between wireless device vendors since each vendor provides different hardware capabilities.

The SoftMAC handle most of the MAC functionality with respect to IEEE 802.11 protocol. The SoftMAC implementation in Linux is known as mac80211. The mac80211 depends on a wireless configuration API, namely cfg80211, for both the registration to the networking subsystem and for configuration.

The wireless driver for Atheros WLAN devices was initially developed by the madwifi project, and then became part of the Linux kernel. The implementation model of Linux kernel WLAN driver is currently based on SoftMAC wireless devices. For the time being, Linux kernel supports all wireless modes with PCI/PCI-Express Atheros WLAN devices only.

In order to implement our approach, we used a conventional PC with a wireless LAN card based on the Atheros IEEE 802.11n chipset (ath9k) Figure 4.2. It had an Intel Core 2 processor with VT support, Gigabit Ethernet interface and 2GB RAM. Ubuntu Linux has been chosen to host the virtualization environment for virtual WLAN approach. We used Ubuntu 14.04. With libvirt, there come two management tools: virt-manager as graphical user interface (GUI) and virtsh as command line interface (CLI).

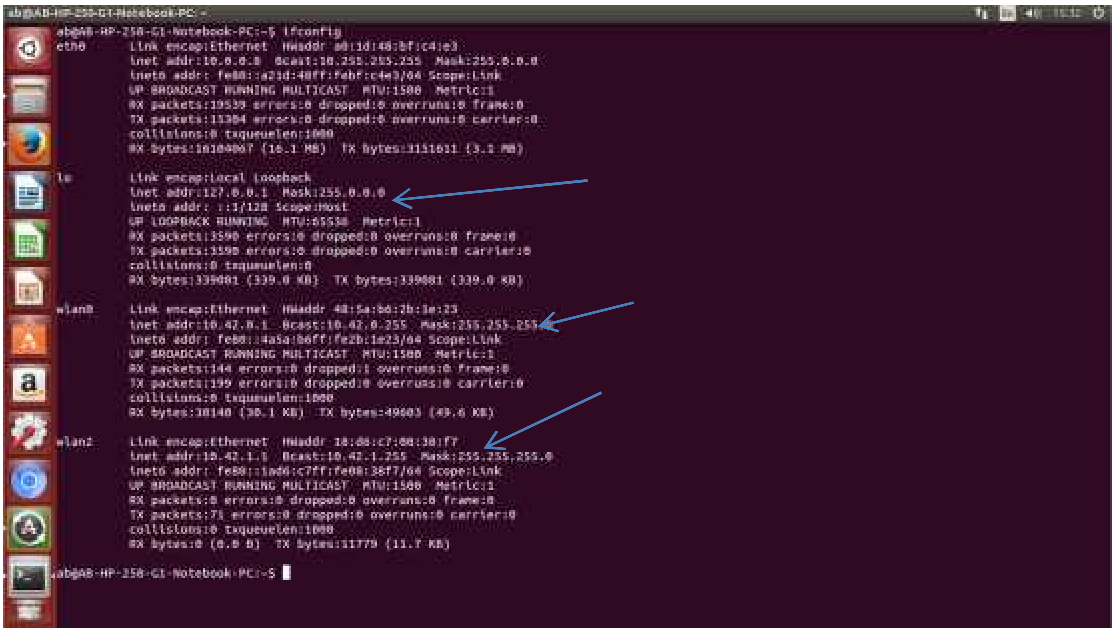


```
wlan1     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

wifislax ~ # airmon-ng start wlan1

Interface       Chipset          Driver

wlan0           Atheros AR9462   ath9k - [phy4]
                Atheros AR9271   ath9k - [phy5]
```

Figure4.2: Atheros IEEE 802.11n chipset (ath9k) .

The virtual wireless interfaces have been created using a CLI configuration utility in Linux named “iw”. Once created, the interfaces have been configured to function as virtual AP. It is essential for all VIFs to have a unique MAC address Figure4.3, which can be assigned with “ifconfig hw” command or “macchanger” utility.

A virtual AP functionality has been implemented using the HostAP userspace. The virtual AP depends on HostAP to handle authenticating clients, setting encryption keys, establishing key rotation policy, and other aspects of the wireless infrastructure. The HostAP use the netlink driver (nl80211) to create an AP mode interface for wireless traffic and a monitor mode interface for receiving and transmitting management frames.



```
ab@AB-HP-250-G1-Notebook-PC: ~
ab@AB-HP-250-G1-Notebook-PC:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr a0:1d:48:bf:c4:e3
          inet addr:10.0.0.8  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::a21d:48ff:febf:c4e3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:19539 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16104067 (16.1 MB)  TX bytes:3151611 (3.1 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:3590 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3590 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:339081 (339.0 KB)  TX bytes:339081 (339.0 KB)

wlan0     Link encap:Ethernet  HWaddr 48:5a:b6:2b:1e:23
          inet addr:10.42.0.1  Bcast:10.42.0.255  Mask:255.255.255.0
          inet6 addr: fe80::4a5a:b6ff:fe2b:1e23/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:144 errors:0 dropped:1 overruns:0 frame:0
          TX packets:199 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30140 (30.1 KB)  TX bytes:49603 (49.6 KB)

wlan2     Link encap:Ethernet  HWaddr 18:d6:c7:08:38:f7
          inet addr:10.42.1.1  Bcast:10.42.1.255  Mask:255.255.255.0
          inet6 addr: fe80::1ad6:c7ff:fe08:38f7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:11779 (11.7 KB)

ab@AB-HP-250-G1-Notebook-PC:~$
```

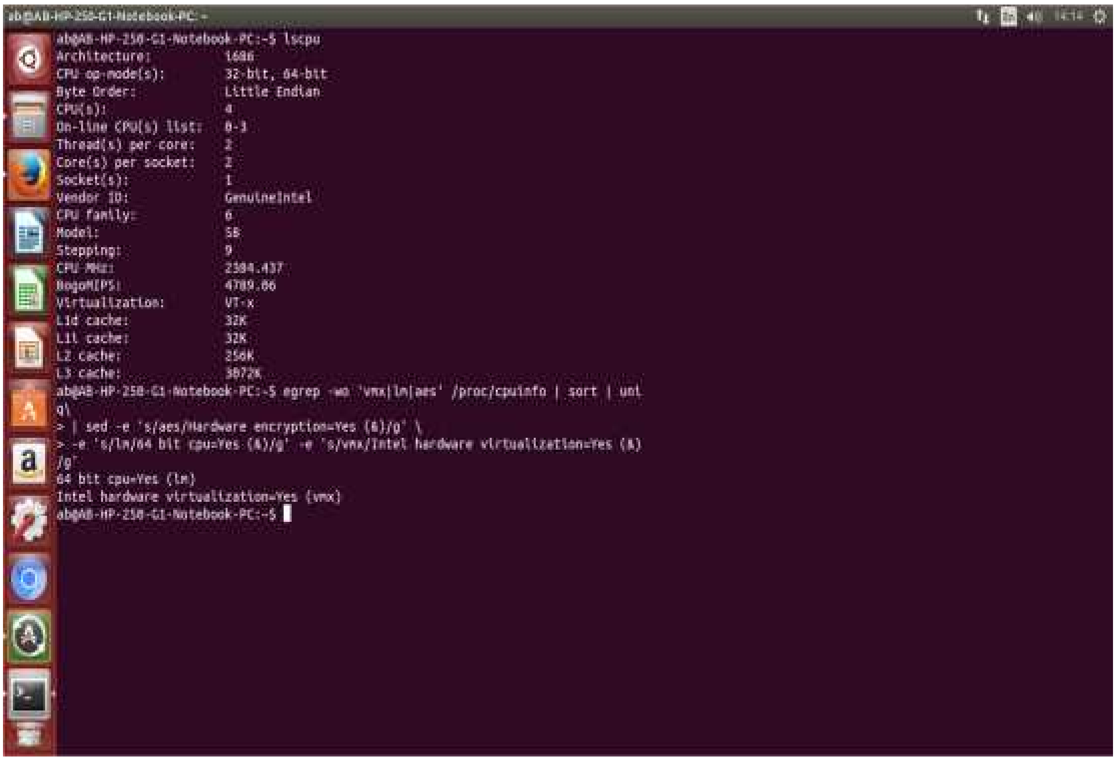
Figure4.3: VIFs have a unique MAC address.

For testing our approach, one PC with a shared Internet connection. We created two virtual APs in IEEE 802.11n operation mode, and two PC. Two virtual APs has one interface using Linux.

virtual router acted as a DHCP server and DNS forwarder for its own virtual WLAN and each virtual AP broadcasted different SSIDs to distinguish the wireless networks. NAT (Network Address Translation) functionality was also added to the virtual interface facing the Internet to maintain public IP addresses and to enhance wireless network security. Using these virtual router, different wireless LAN clients could access the Internet with different wireless LAN security mechanisms. A detailed implementation of the virtual WLAN platform is described in Appendix A.

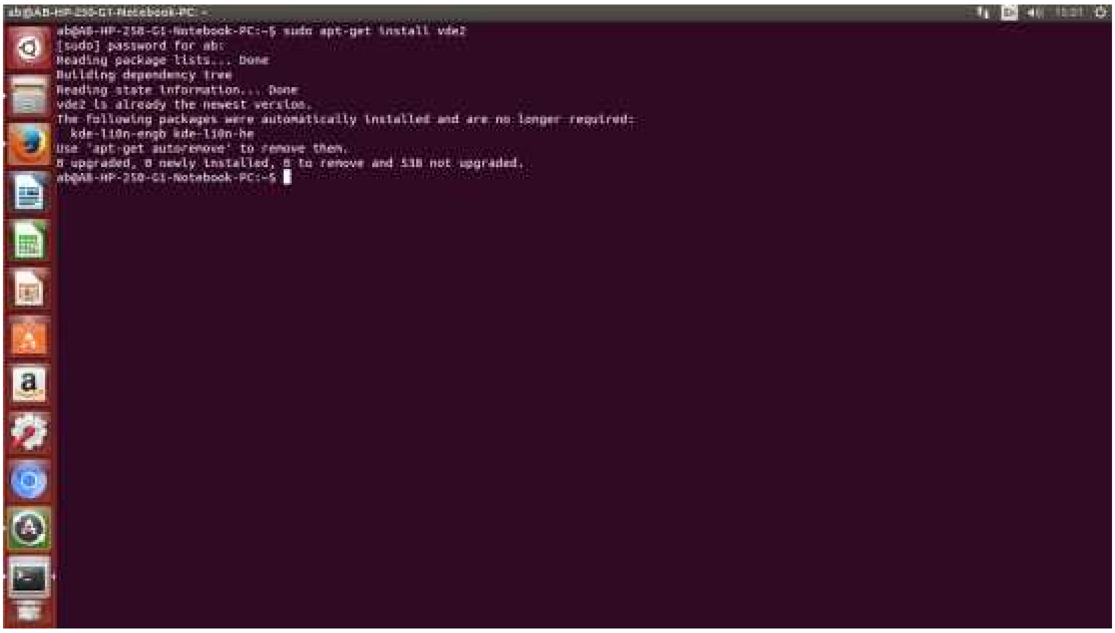
Packages must be installed:

CPU information: cpu must support virtualization Figure 4.4.



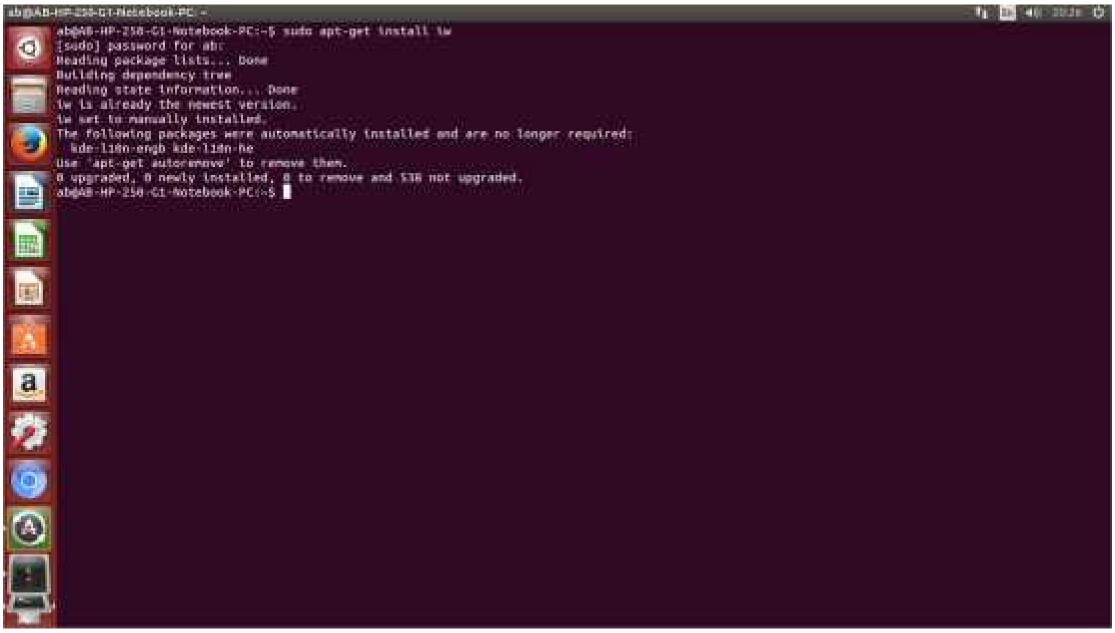
```
ab@AB-HP-250-G1-Notebook-PC:~$ lscpu
Architecture:          i686
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                4
On-line CPU(s) list:   0-3
Thread(s) per core:    2
Core(s) per socket:    2
Socket(s):             1
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 58
Stepping:              9
CPU MHz:               2384.437
BogoMIPS:              4789.06
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              3072K
ab@AB-HP-250-G1-Notebook-PC:~$ egrep -wo 'vmx|lm|aes' /proc/cpuinfo | sort | uni
q\
> | sed -e 's/aes/Hardware encryption=Yes (&)/g' \
> -e 's/lm/64 bit cpu=Yes (&)/g' -e 's/vmx/Intel hardware virtualization=Yes (&)
/g'
64 bit cpu=Yes (lm)
Intel hardware virtualization=Yes (vmx)
ab@AB-HP-250-G1-Notebook-PC:~$
```

Figure4.4: CPU informations.



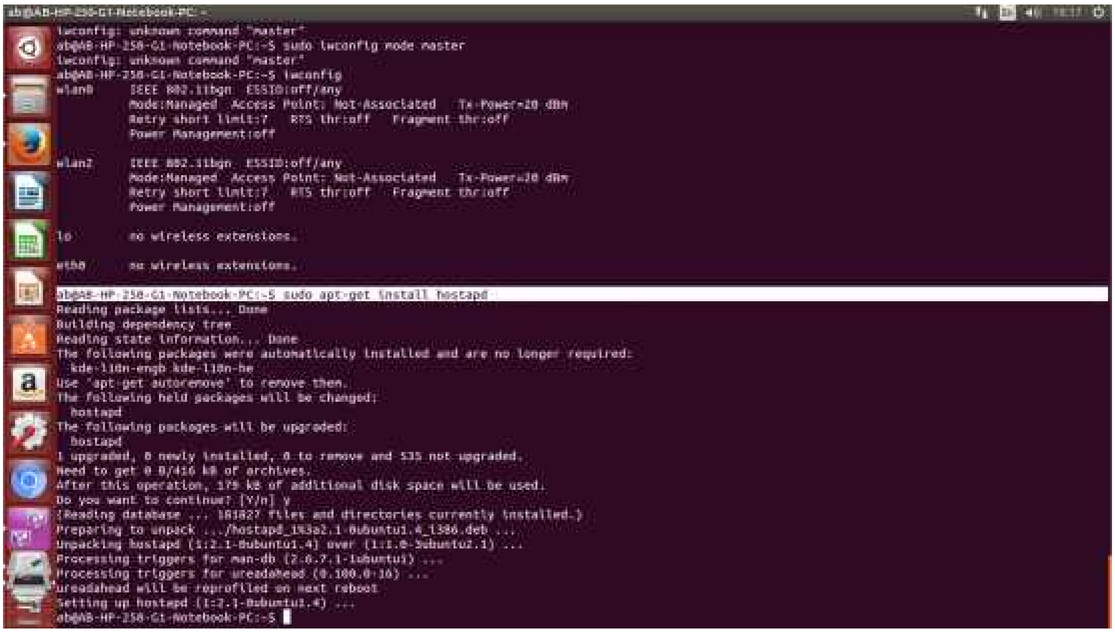
```
ab@AB-HP-250-G1-Notebook-PC:~$ sudo apt-get install vde2
[sudo] password for ab:
Reading package lists... Done
Building dependency tree
Reading state information... Done
vde2 is already the newest version.
The following packages were automatically installed and are no longer required:
  kde-l10n-engb kde-l10n-he
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 538 not upgraded.
ab@AB-HP-250-G1-Notebook-PC:~$
```

Figure4.5: vde2 installed.



```
ab@AB-HP-250-G1-Notebook-PC:~$ sudo apt-get install iw
[sudo] password for ab:
Reading package lists... Done
Building dependency tree
Reading state information... Done
iw is already the newest version.
iw set to manually installed.
The following packages were automatically installed and are no longer required:
  kde-l10n-engb kde-l10n-he
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 538 not upgraded.
ab@AB-HP-250-G1-Notebook-PC:~$
```

Figure4.6: iw tools installed.



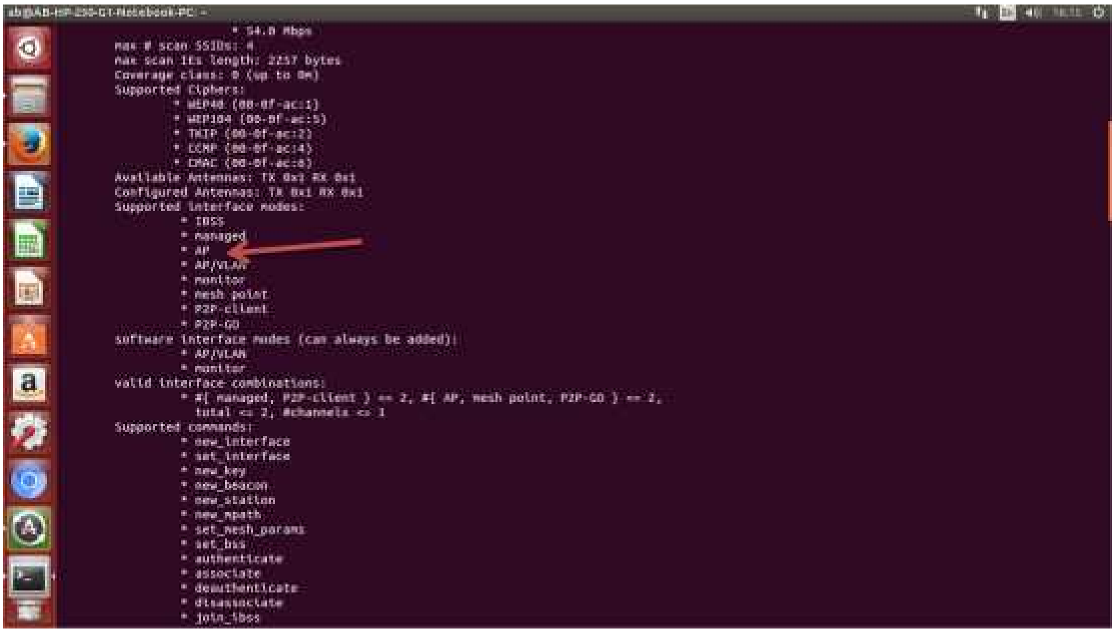
```
iwconfig: unknown command "master"
ab@AB-HP-250-G1-Notebook-PC:~$ sudo iwconfig mode master
iwconfig: unknown command "master"
ab@AB-HP-250-G1-Notebook-PC:~$ iwconfig
wlan0     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

wlan2     IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

lo        no wireless extensions.

eth0      no wireless extensions.

ab@AB-HP-250-G1-Notebook-PC:~$ sudo apt-get install hostapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  kde-l10n-engb kde-l10n-he
Use 'apt-get autoremove' to remove them.
The following held packages will be changed:
  hostapd
The following packages will be upgraded:
  hostapd
1 upgraded, 0 newly installed, 0 to remove and 535 not upgraded.
Need to get 0 B/416 kB of archives.
After this operation, 179 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
(Reading database ... 181827 files and directories currently installed.)
Preparing to unpack .../hostapd_1%3a2.1-0ubuntu1.4_i386.deb ...
Unpacking hostapd (1:2.1-0ubuntu1.4) over (1:1.0-3ubuntu2.1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Processing triggers for ureadahead (0.100.0-16) ...
ureadahead will be reprofiled on next reboot
Setting up hostapd (1:2.1-0ubuntu1.4) ...
ab@AB-HP-250-G1-Notebook-PC:~$
```

Figure4.7: hostapd installed.

Creating Virtual Aps

“AP” mode is supported Figure4.8.

iw list



```
                        * 54.0 Mbps
        max # scan SSIDs: 4
        max scan IEs length: 2257 bytes
        Coverage class: 0 (up to 0m)
        Supported Ciphers:
                * WEP40 (00-0f-ac:1)
                * WEP104 (00-0f-ac:5)
                * TKIP (00-0f-ac:2)
                * CCMP (00-0f-ac:4)
                * CMAC (00-0f-ac:6)
        Available Antennas: TX 0x1 RX 0x1
        Configured Antennas: TX 0x1 RX 0x1
        Supported interface modes:
                 * IBSS
                 * managed
                 * AP
                 * AP/VLAN
                 * monitor
                 * mesh point
                 * P2P-client
                 * P2P-GO
        software interface modes (can always be added):
                 * AP/VLAN
                 * monitor
        valid interface combinations:
                 * #{ managed, P2P-client } <= 2, #{ AP, mesh point, P2P-GO } <= 2,
                   total <= 2, #channels <= 1
        Supported commands:
                 * new_interface
                 * set_interface
                 * new_key
                 * new_beacon
                 * new_station
                 * new_mpath
                 * set_mesh_params
                 * set_bss
                 * authenticate
                 * associate
                 * deauthenticate
                 * disassociate
                 * join_ibss
```

Figure4.8: AP mode must be supported.

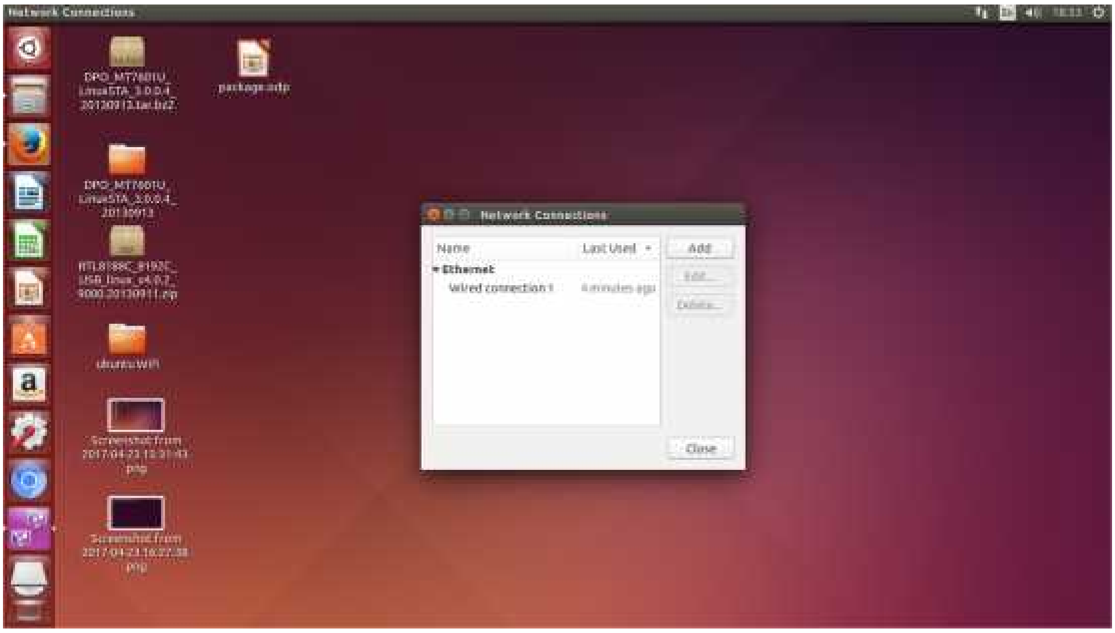
GUI And CLI for VMnet1:

Wifi must be disabled before starting to create virtual networks.

Ubuntu Desktop
DPO_MT7601U_LinuxSTA_3.0.0.4_20130913.tar.bz2
package.odp
DPO_MT7601U_LinuxSTA_3.0.0.4_20130913
RTL8188C_8192C_USB_linux_v4.0.2_9000.20130911.zip
ubuntuwifi
Screenshot from 2017-04-23 15:31:03.png
Screenshot from 2017-04-23 10:27:38.png

Figure4.9: edit connections from panel.

To add first virtual network look to the next figures:



Network Connections

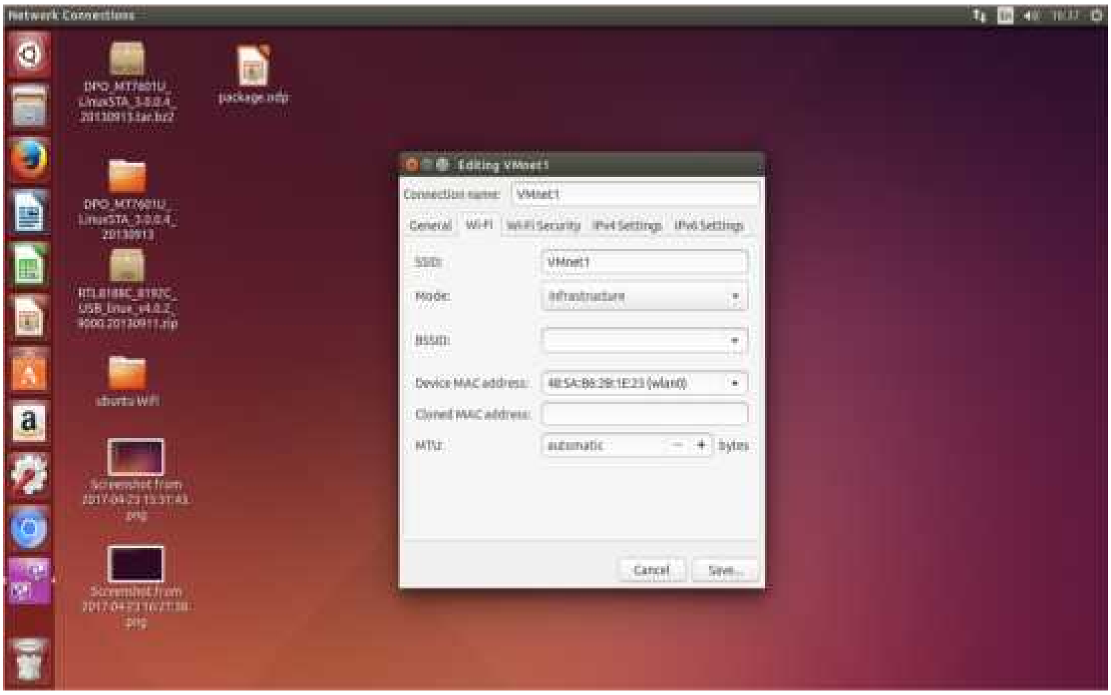
Name — Last Used

Ethernet

Wired connection 1 — 4 minutes ago

Network Connections
DPO_MT7601U_LinuxSTA_3.0.0.4_20130913.tar.bz2
package.odp
DPO_MT7601U_LinuxSTA_3.0.0.4_20130913
RTL8188C_8192C_USB_linux_v4.0.2_9000.20130911.zip
ubuntu wifi
Screenshot from 2017-04-23 13:31:43.png
Screenshot from 2017-04-23 16:27:38.png
Add
Edit...
Delete...
Close

Figure4.10: add and create wifi network.



Editing VMnet1

Connection name: VMnet1

SSID: VMnet1

Mode: Infrastructure

BSSID:

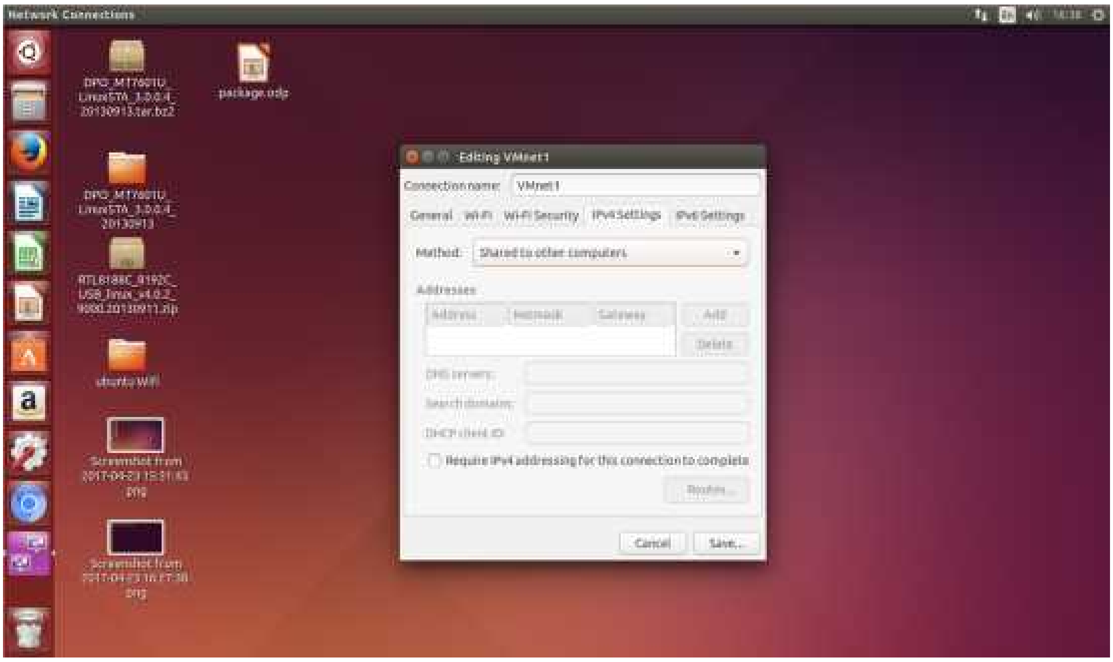
Device MAC address: 48:5A:B6:2B:1E:23 (wlan0)

Cloned MAC address:

MTU: automatic bytes

Network Connections
DPO_MT7601U_LinuxSTA_3.0.0.4_20130913.tar.bz2
package.odp
DPO_MT7601U_LinuxSTA_3.0.0.4_20130913
RTL8188C_8192C_USB_linux_v4.0.2_9000.20130911.zip
ubuntu wifi
Screenshot from 2017-04-23 13:31:43.png
Screenshot from 2017-04-23 16:27:38.png
General
Wi-Fi
Wi-Fi Security
IPv4 Settings
IPv6 Settings
Cancel
Save...

Figure4.11: choose infrastructure mode and interface(wlan0).



Connection name: VMnet1

Method: Shared to other computers

DNS servers:

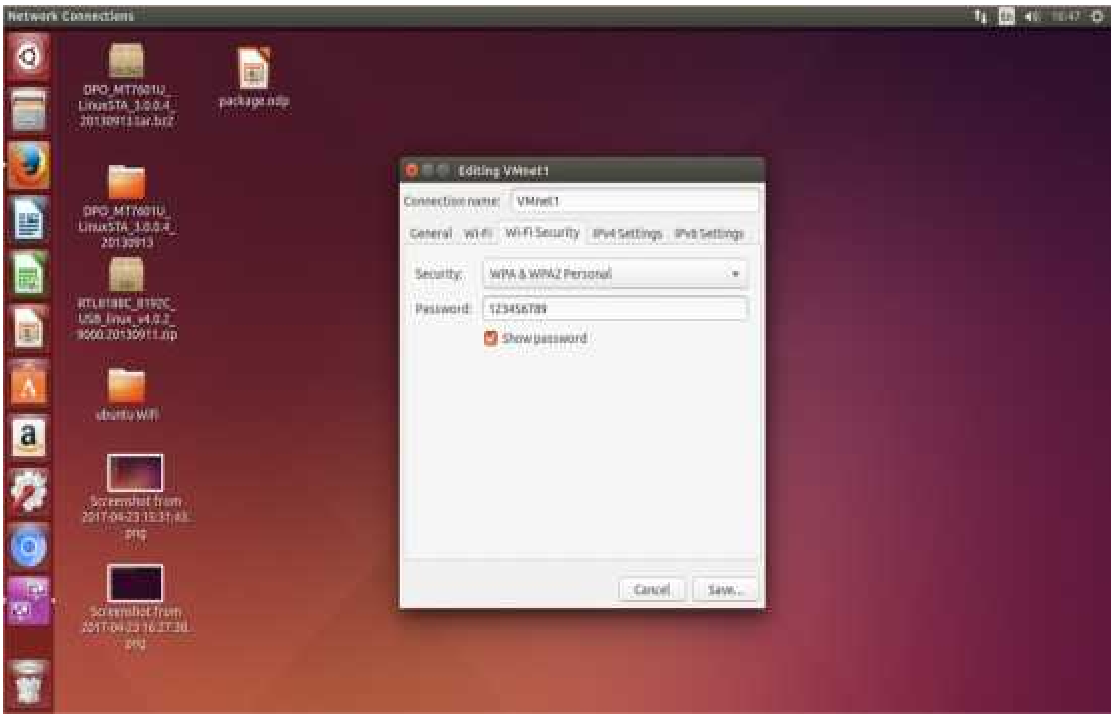
Search domains:

DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

Figure4.12: the network must be shared to other computers.

Implement the first level of security algorithms on the first virtual AP:



Connection name: VMnet1

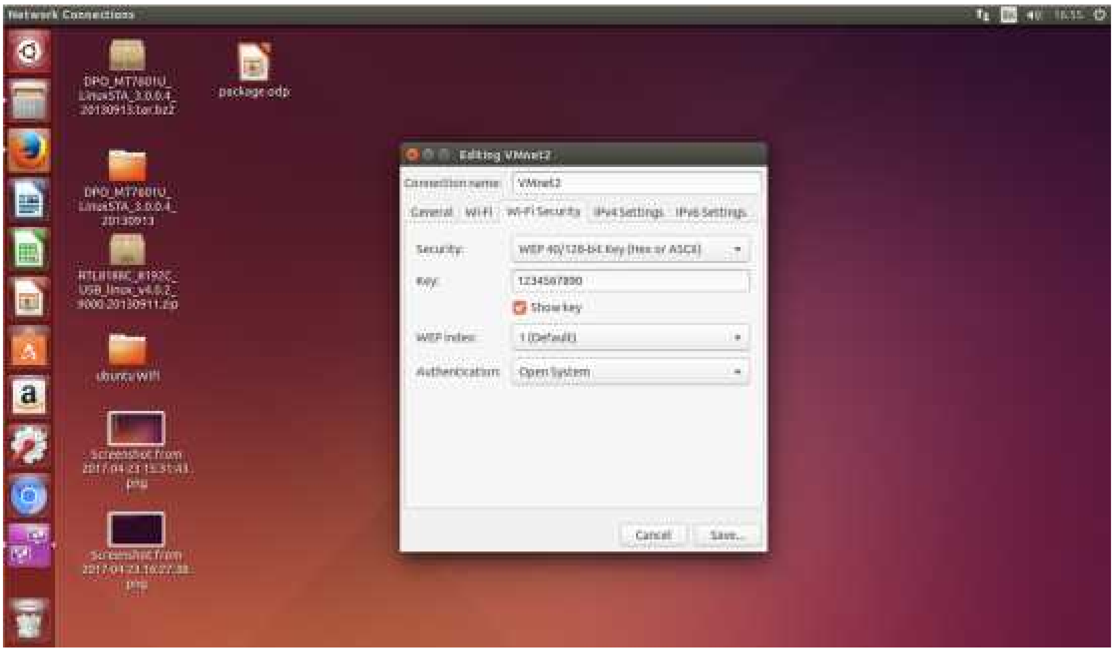
Security: WPA & WPA2 Personal

Password: 123456789

☑ Show password

Figure4.13: first level of security algorithms.

GUI And CLI for VMnet2 as the same of VMnet1, but only difference between them is level of security algorithms figure4.14 and VIF(wlan2) figure 4.15:



Connection name: VMnet2

Security: WEP 40/128-bit Key (Hex or ASCII)

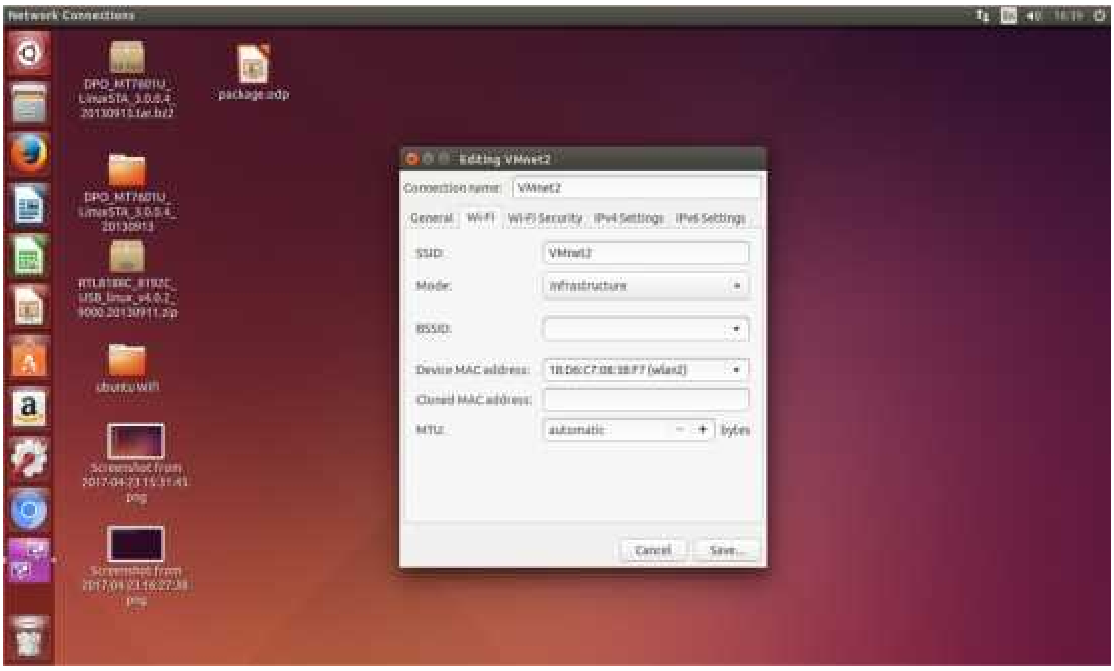
Key: 1234567890

☑ Show key

WEP index: 1 (Default)

Authentication: Open System

Figure4.14: other level of security algorithms.



Connection name: VMnet2

SSID: VMnet2

Mode: Infrastructure

BSSID:

Device MAC address: 18:D6:C7:0E:38:F7 (wlan2)

Cloned MAC address:

MTU: automatic bytes

Figure4.15: other VIF.

After this steps and implement it correctly and enable wifi of panel the VMnet1 and VMnet2 will be created with different level of security algorithms and VIF and there configuration will be saved in network manager.

The physical interface will be divided to two VIFs that act as master mode. Each VIF works as separated AP to other. Multiple virtual wireless LAN networks(multi SSIDs) on top of only one physical wireless LAN card.Therefore, we achieve the main goal of our approach.

CHAPTER FIVE

TESTING AND RESULTS

5.1 Testing.

Chapter Five

Testing And Results

5.1 Testing

This guide explains how to setup a software platform for hosting multiple virtual wireless LAN networks on top of only one physical wireless LAN card. To follow this guide, we need a wireless LAN card based on Atheros IEEE 802.11n chipset, A single computer is used to host two virtual access point.

Installing Ubuntu

1. Download 32-bit version of Ubuntu 14.04 from http://www.ubuntu.com/download/ubuntu/download.

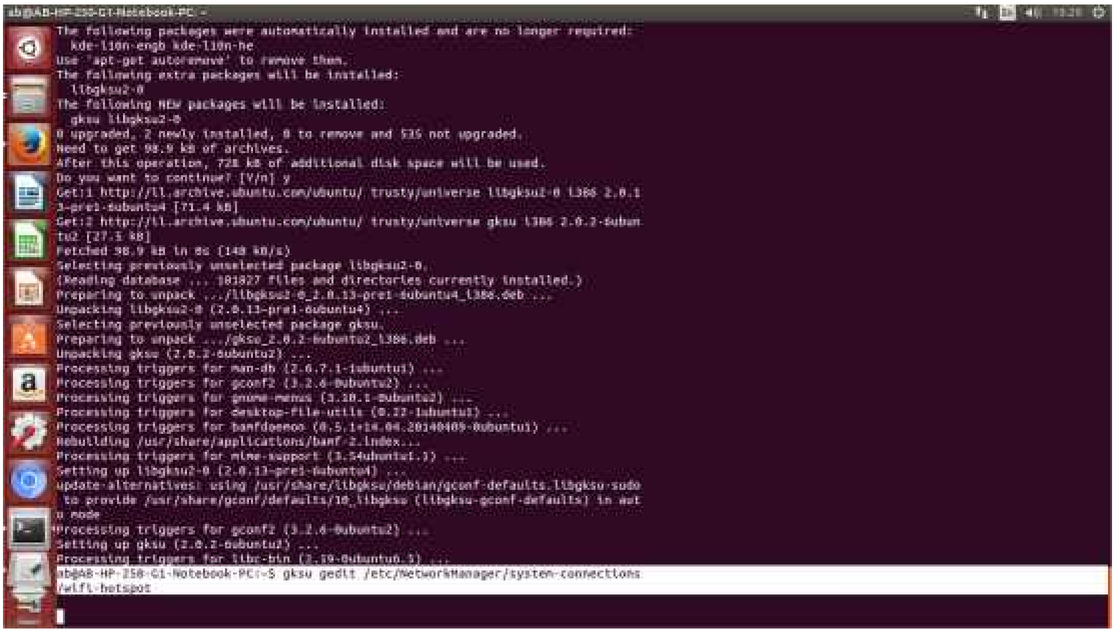
2. Once finished downloading iso file, will need to burn a CD or create a USB drive.

3. When the CD is ready, simply put it in your CD drive, restart computer and follow the instructions that appear on screen.

Results:

applying below command to go to the configuration of VMnet1 that was be saved in network manager figure 5.1.

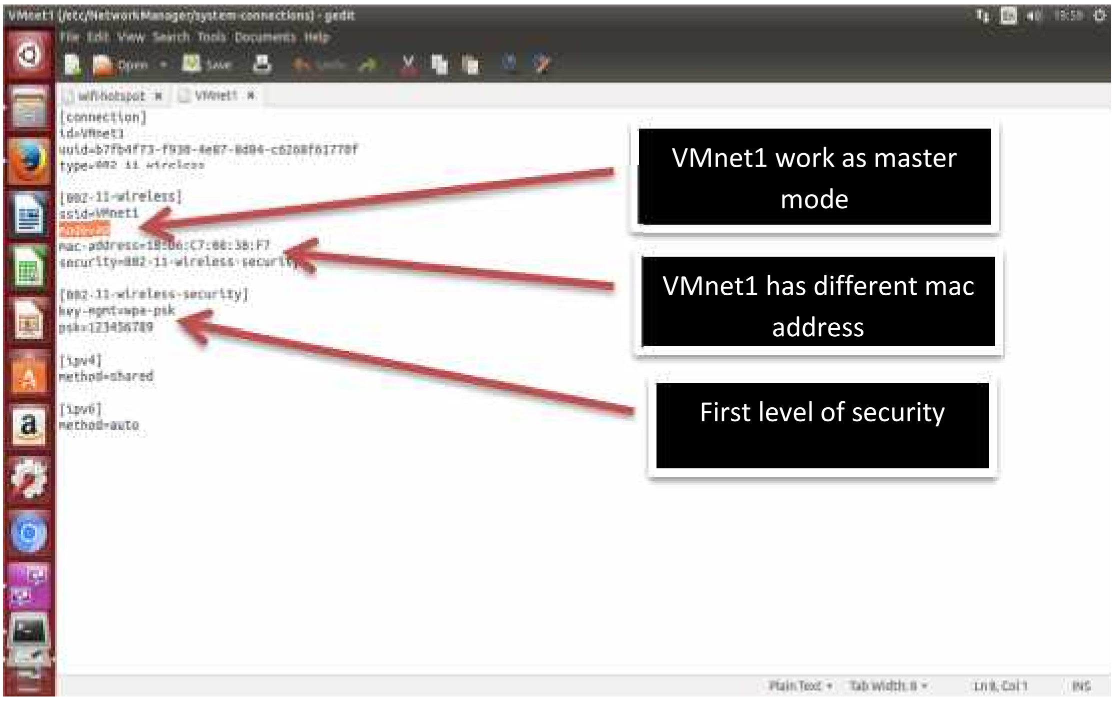
```
gksudo gedit /etc/NetworkManager/system-connections/wifi-hotspot
```



```
The following packages were automatically installed and are no longer required:
  kde-l10n-engb kde-l10n-he
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  libgksu2-0
The following NEW packages will be installed:
  gksu libgksu2-0
0 upgraded, 2 newly installed, 0 to remove and 535 not upgraded.
Need to get 98.9 kB of archives.
After this operation, 728 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ll.archive.ubuntu.com/ubuntu/ trusty/universe libgksu2-0 i386 2.0.1
3-pre1-6ubuntu4 [71.4 kB]
Get:2 http://ll.archive.ubuntu.com/ubuntu/ trusty/universe gksu i386 2.0.2-6ubun
tu2 [27.5 kB]
Fetched 98.9 kB in 0s (148 kB/s)
Selecting previously unselected package libgksu2-0.
(Reading database ... 181827 files and directories currently installed.)
Preparing to unpack .../libgksu2-0_2.0.13-pre1-6ubuntu4_i386.deb ...
Unpacking libgksu2-0 (2.0.13-pre1-6ubuntu4) ...
Selecting previously unselected package gksu.
Preparing to unpack .../gksu_2.0.2-6ubuntu2_i386.deb ...
Unpacking gksu (2.0.2-6ubuntu2) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Processing triggers for gconf2 (3.2.6-0ubuntu2) ...
Processing triggers for gnome-menus (3.10.1-0ubuntu2) ...
Processing triggers for desktop-file-utils (0.22-1ubuntu1) ...
Processing triggers for bamfdaemon (0.5.1+14.04.20140409-0ubuntu1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Processing triggers for mime-support (3.54ubuntu1.1) ...
Setting up libgksu2-0 (2.0.13-pre1-6ubuntu4) ...
update-alternatives: using /usr/share/libgksu/debian/gconf-defaults.libgksu-sudo
 to provide /usr/share/gconf/defaults/10_libgksu (libgksu-gconf-defaults) in aut
o mode
Processing triggers for gconf2 (3.2.6-0ubuntu2) ...
Setting up gksu (2.0.2-6ubuntu2) ...
Processing triggers for libc-bin (2.19-0ubuntu6.3) ...
ab@AB-HP-250-G1-Notebook-PC:~$ gksu gedit /etc/NetworkManager/system-connections
/wifi-hotspot
```

Figure5.1: Cl to go to configuration of two virtual network that be created.

The file of Configuration of each virtual networks will be saved in network manager. Only change the mode to AP figure5.2 and figure5.3.


VMnet1 (/etc/NetworkManager/system-connections) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
wifi-hotspot
VMnet1
Plain Text
Tab Width: 8
Ln 8, Col 1
INS

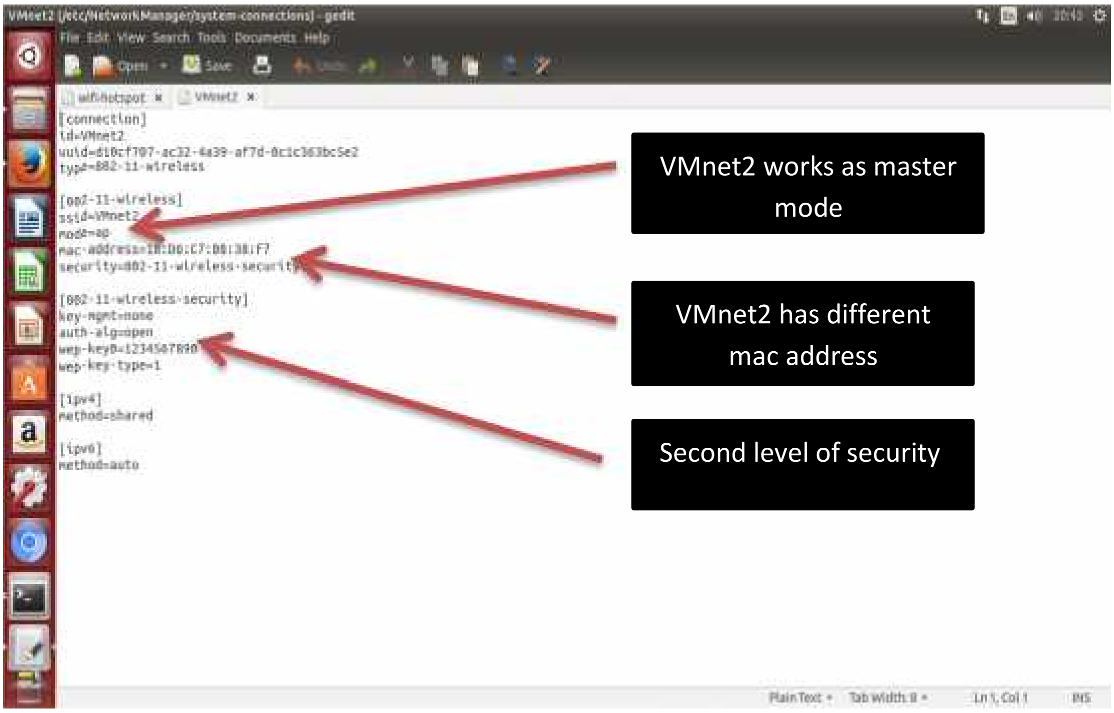
```
[connection]
id=VMnet1
uuid=b7fb4f73-f938-4e87-8d84-c6268f61770f
type=802-11-wireless

[802-11-wireless]
ssid=VMnet1
mode=ap
mac-address=18:06:C7:08:38:F7
security=802-11-wireless-security

[802-11-wireless-security]
key-mgmt=wpa-psk
psk=123456789

[ipv4]
method=shared

[ipv6]
method=auto
```

VMnet1 work as master mode

VMnet1 has different mac address

First level of security

Figure5.2: informations and configuration of VMnet1.


VMnet2 [/etc/NetworkManager/system-connections] - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
wifi-hotspot
VMnet2
Plain Text
Tab Width: 8
Ln 1, Col 1
INS

```
[connection]
id=VMnet2
uuid=d10cf707-ac32-4a39-af7d-0c1c363bc5e2
type=802-11-wireless

[802-11-wireless]
ssid=VMnet2
mode=ap
mac-address=18:D6:C7:08:38:F7
security=802-11-wireless-security

[802-11-wireless-security]
key-mgmt=none
auth-alg=open
wep-key0=1234567890
wep-key-type=1

[ipv4]
method=shared

[ipv6]
method=auto
```

VMnet2 works as master mode

VMnet2 has different mac address

Second level of security

Figure5.3: informations and configuration of VMnet2.

The VMnet1 is the first virtual AP connected to PC, and appears when we check wifi connection on mobile figure5.4.

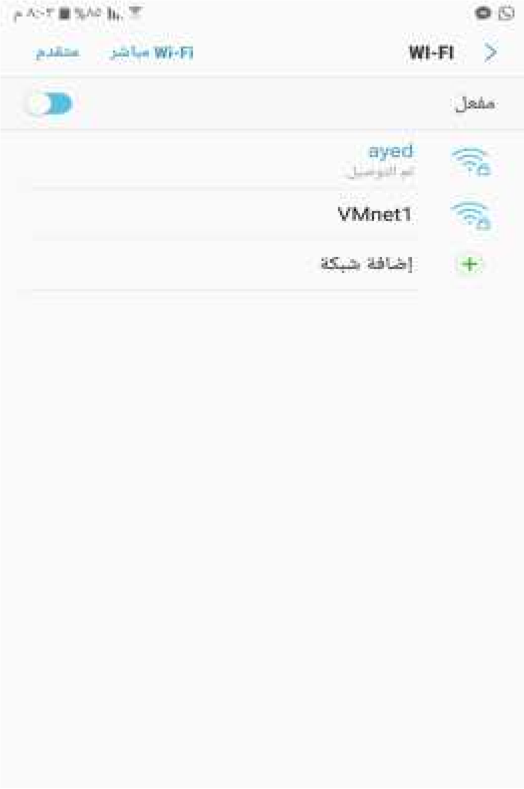
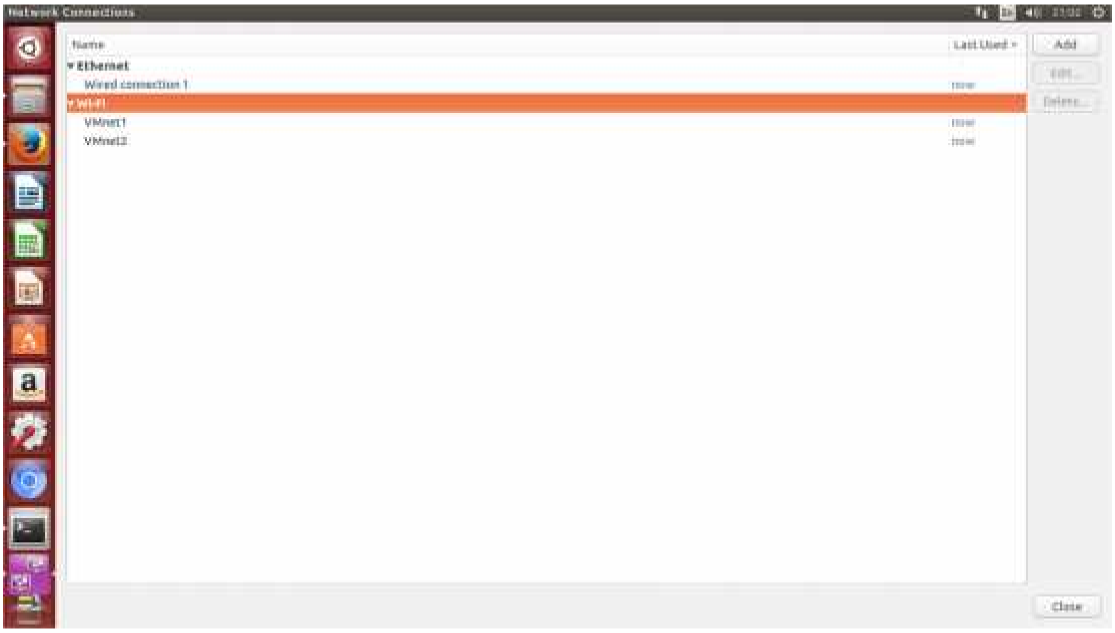


Figure5.4: VMnet1 is one of choice of wifi connections choices.

The VMnet2 is the second virtual AP connected to PC, and appears when we check wifi connection on mobile. And simultaneously with VMnet1 on the same time figure5.5.

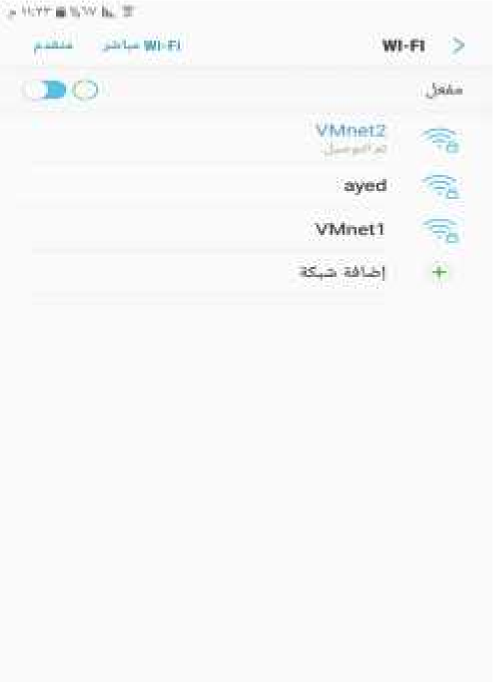


Network Connections

Name	Last Used
▾ Ethernet	
Wired connection 1	now
▾ Wi-Fi	
VMnet1	now
VMnet2	now

Figure5.5: VMnet1 and VMnet2 active, appear and distributed in the same time.

Atheros chipset will distribute VMnet1 and VMnet2 in simultaneously at the same time.



Wi-Fi

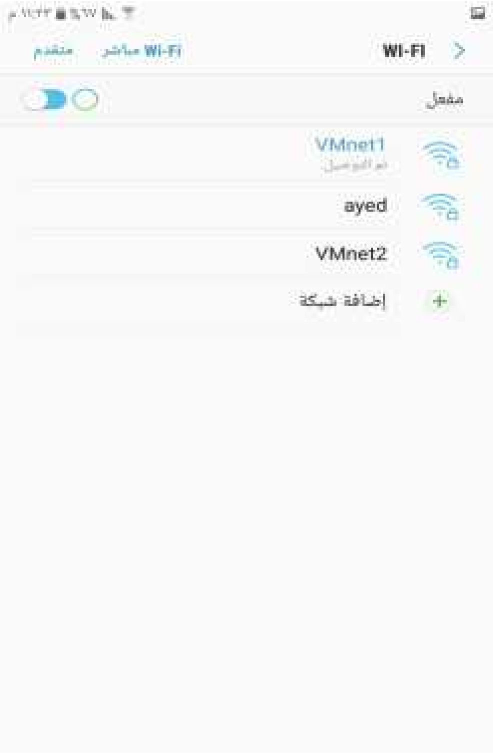
مفعل

VMnet2
تم التوصيل

ayed

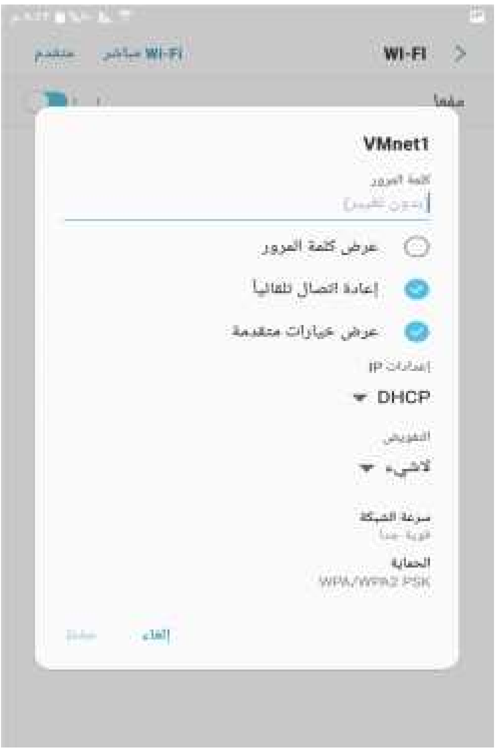
VMnet1

Figure5.6: connect with VMnet2 with stays VMnet1 one of wifi connections choices.



VMnet1
تم التوصيل
ayed
VMnet2

Figure5.7: connect with VMnet1 with stays VMnet2 one of wifi connections choices.



VMnet1

كلمة المرور
(بدون تغيير)

○ عرض كلمة المرور
✓ إعادة اتصال تلقائياً
✓ عرض خيارات متقدمة

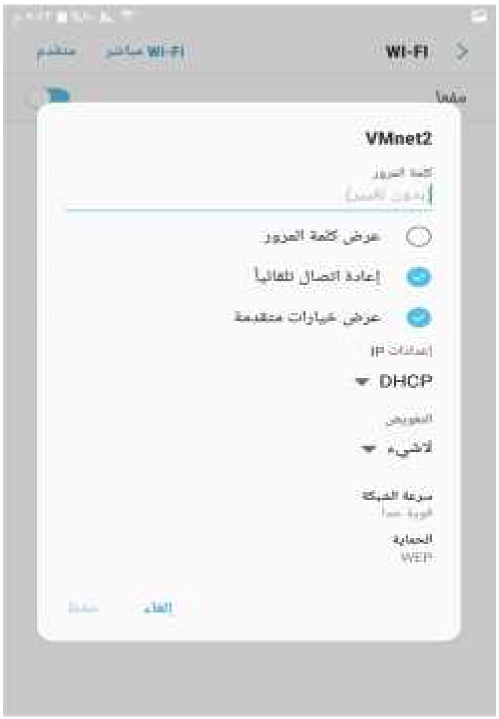
إعدادات IP
DHCP

التفويض
لاشيء

سرعة الشبكة
قوية جداً

الحماية
WPA/WPA2 PSK

Figure5.8: first level of security algorithms.



VMnet2

كلمة المرور

(بدون تغيير)

○ عرض كلمة المرور

✓ إعادة اتصال تلقائيا

✓ عرض خيارات متقدمة

إعدادات IP

DHCP

التفويض

لاشيء

سرعة الشبكة

قوية جدا

الحماية

WEP

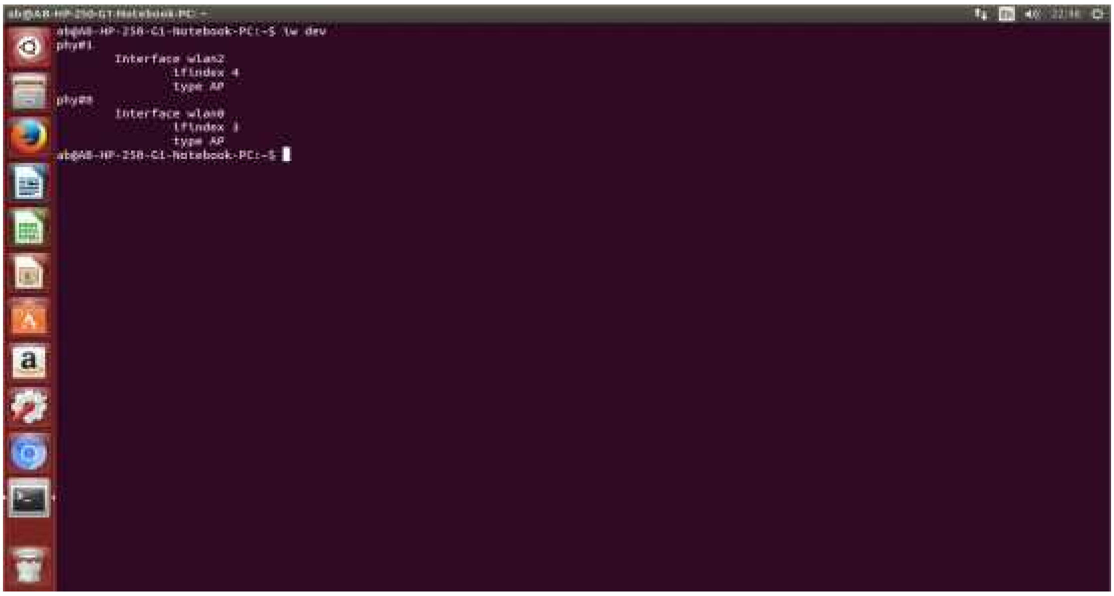
Figure5.9: second level of security algorithms.

After presenting the above results we can say that the main objective of the project has been achieved. It is distribute virtual AP(VMnet1 and VMnet2)that shared on one physical interface with different level of security in simultaneously at the same time and connect with one of them.

Iw CL:

iw dev:

It used to list our device. Physical name could be different figure5.10.

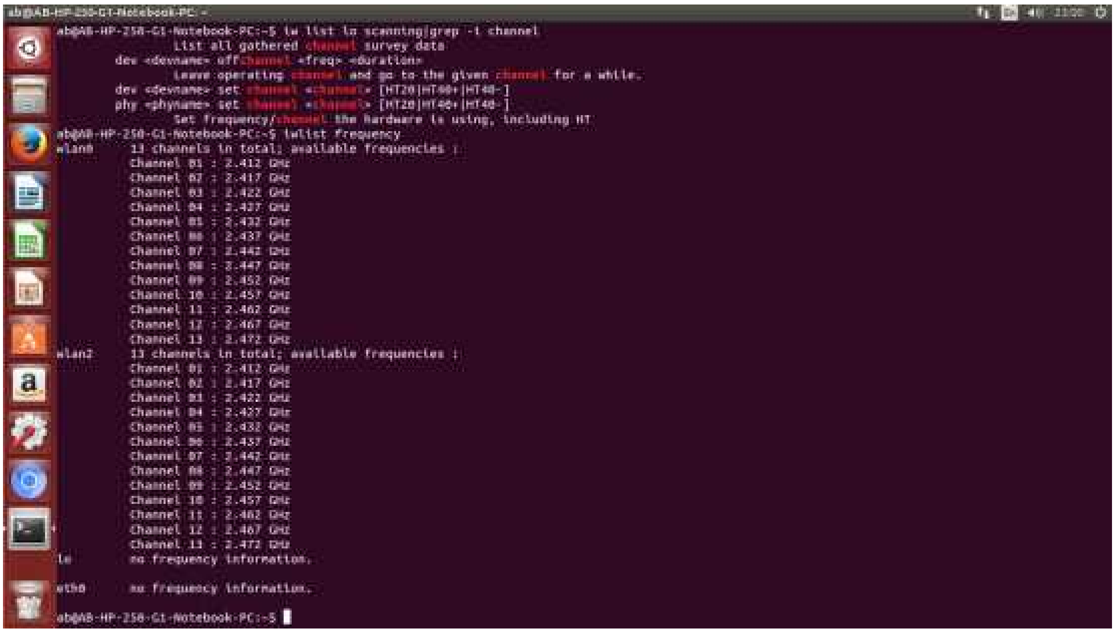


```
ab@AB-HP-250-G1-Notebook-PC:~$ iw dev
phy#1
        Interface wlan2
                ifindex 4
                type AP
phy#0
        Interface wlan0
                ifindex 3
                type AP
ab@AB-HP-250-G1-Notebook-PC:~$
```

Figure5.10: different physical name.

iwlist frequency

It give the list of available frequencies in the device and the number of defined channels figure5.11.

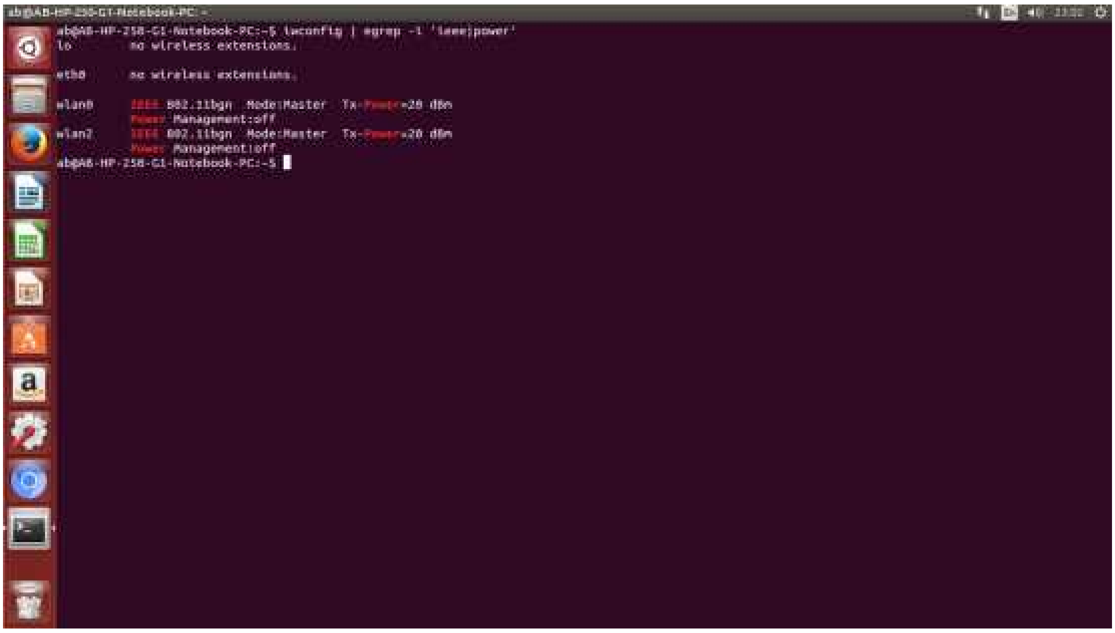


```
ab@AB-HP-250-G1-Notebook-PC:~$ iw list lo scanning|grep -i channel
                List all gathered channel survey data
        dev <devname> offchannel <freq> <duration>
                Leave operating channel and go to the given channel for a while.
        dev <devname> set channel <channel> [HT20|HT40+|HT40-]
        phy <phyname> set channel <channel> [HT20|HT40+|HT40-]
                Set frequency/channel the hardware is using, including HT
ab@AB-HP-250-G1-Notebook-PC:~$ iwlist frequency
wlan0     13 channels in total; available frequencies :
          Channel 01 : 2.412 GHz
          Channel 02 : 2.417 GHz
          Channel 03 : 2.422 GHz
          Channel 04 : 2.427 GHz
          Channel 05 : 2.432 GHz
          Channel 06 : 2.437 GHz
          Channel 07 : 2.442 GHz
          Channel 08 : 2.447 GHz
          Channel 09 : 2.452 GHz
          Channel 10 : 2.457 GHz
          Channel 11 : 2.462 GHz
          Channel 12 : 2.467 GHz
          Channel 13 : 2.472 GHz
wlan2     13 channels in total; available frequencies :
          Channel 01 : 2.412 GHz
          Channel 02 : 2.417 GHz
          Channel 03 : 2.422 GHz
          Channel 04 : 2.427 GHz
          Channel 05 : 2.432 GHz
          Channel 06 : 2.437 GHz
          Channel 07 : 2.442 GHz
          Channel 08 : 2.447 GHz
          Channel 09 : 2.452 GHz
          Channel 10 : 2.457 GHz
          Channel 11 : 2.462 GHz
          Channel 12 : 2.467 GHz
          Channel 13 : 2.472 GHz
lo        no frequency information.

eth0      no frequency information.

ab@AB-HP-250-G1-Notebook-PC:~$
```

Figure5.11: available frequencies.

iwconfig | egrep -i 'ieee|power'

It give information about network interface especially power management information if it off or on (in this device the power management :off) this mean we can't make controlling power figure5.12.



```
ab@AB-HP-250-G1-Notebook-PC:~$ iwconfig | egrep -i 'ieee|power'
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11bgn  Mode:Master  Tx-Power=20 dBm
          Power Management:off
wlan2     IEEE 802.11bgn  Mode:Master  Tx-Power=20 dBm
          Power Management:off
ab@AB-HP-250-G1-Notebook-PC:~$
```

Figure5.12: network interface informations.

CHAPTER SIX

CONCLUSION AND RECOMMENDAIONS

6.1 Conclusion

6.2 Recommendations

Chapter Six

Recommendations And Conclusion

6.1 Conclusion

Many enterprises are adopting virtualization to improve server utilization and consolidation. However, virtualization can also be used to create a virtualized environment for the whole network infrastructure. In this project, we present a review of wlan virtualization techniques and open source implementations. These techniques enable enterprise IT to move forward with virtualization beyond just servers and also virtualize the entire network infrastructure that were traditionally hardware bound.

However, most of the existing virtualization techniques have focused mostly on wired network infrastructure. In this project, we proposed a virtualization approach to realize virtual wireless networks by combining wireless LAN virtualization technique with open source solutions. This approach adds wireless LAN functionality to a virtual environments and enables multiple virtual WLANs to operate over a shared physical infrastructure. The benefits of WLAN infrastructure virtualization, make the implementation of the virtual WLAN approach an excellent platform for the development and testing of different WLAN systems and services. This approach needs extra hardware to ctreate and implement two virtual interface act as AP with multi level of security algorithms and distributes it at the same time and appears one of choice of wifi connection choices on our mobiles, so we can choice any one as we needs.

6.2 Recommendations

For the future, it is planned to review the various open source solutions that can be used to study the impact of virtualization on IT infrastructures and services and to provide a complete open source solution for enterprises to build their own infrastructure as a services (IaaS) clouds.

References:

[1] Hakan Caoskum, Ina Schieferdecker and Yahya Alhazmi, Virtual wlan: Going beyond virtual access points, Workshops der Wissenschaftlichen Konferenz, 2009.

[2] G. Aljabari and E. Eren, “Virtualization of wireless lan infrastructures,” IEEE 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2011.

[3] B. J. Carroll, CCNA Wireless: Official Exam Certification Guide. Cisco, 2009.

[4] Cisco Systems, Enterprise Wireless Competitive Performance Test Results. http: //www.cisco.com.

[5] J. Sahoo, S. Mohapatra, and R. Lath, “Virtualization: A survey on concepts, taxonomy and associated security issues,” Second International Conference on Computer and Network Technology (ICCNT), pp. 222–226, 2010.

[6] P. B. et al., “Xen and the art of virtualization,” ACM Symposium on Operating Systems Principles (OSSP, pp. 164–177, 2003.

[7] VMware, Understanding Full Virtualization, Paravirtualization, and Hardware Assist, 2007. http://www.vmware.com/files/pdf/VMware_paravirtualization. pdf.

[8] N. M. N. K. Chowdhury and R. Boutaba, “Network virtualization: State of the art and research challenges,” IEEE Communications Magazine, pp. 20–26, 2009.

[9] L. X. et al., “Virtual wifi: Bring virtualization from wired to wireless,” ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE), 2011.

[10] D. Raychaudhuri, “Architectures and technologies for the future mobile internet,” IEICE Transactions on Communications, pp. 436–441, 2010.

[11] Linux Wireless Website. http://linuxwireless.org.

[12] G. S. et al., “Wireless virtualization on commodity 802.11 hardware,” second ACM international workshop on Wireless network testbeds, experimental evaluation and characterization (WinTECH), 2007.

[13] Haykin, S; Moher, M., Sistermas Modernos de Communicacoes wireless, Bookman,2008.

[14] "Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards".

[15] https://wikidevi.com/wiki/TP-LINK_TL-WN722N.

[16] iw utilityhomepage.

[17] B. Aboba, “Virtual access points,” 2003. http://aboba.drizzlehosting.com/ IEEE/11-04-0238-00-0wng-definition-virtual-access-point.doc.

[18] T. Hamaguchi, T. Komata, T. Nagai, and H. Shigeno, “A framework of better deployment for wlan access point using virtualization technique,” IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA), p. 968–973, 2010.

[19] HostAP Website. http://hostap.epitest.fi/hostapd.

Appendices

Appendix A: Virtual WLAN Platform

This guide explains how to setup a software platform for hosting multiple virtual wireless LAN networks on top of only one physical wireless LAN card. To follow this guide, we need a wireless LAN card based on Atheros IEEE 802.11n chipset. As illustrated in the figure below, a single computer is used to host two virtual access point. Ubuntu is used as a virtual host for setting up the virtual WLAN platform.

Installing Ubuntu

1. Download 32-bit version of Ubuntu 11.04 from http://www.ubuntu.com/download/ubuntu/download.

2. Once finished downloading iso file, will need to burn a CD or create a USB drive.

3. When the CD is ready, simply put it in your CD drive, restart computer and follow the instructions that appear on screen.

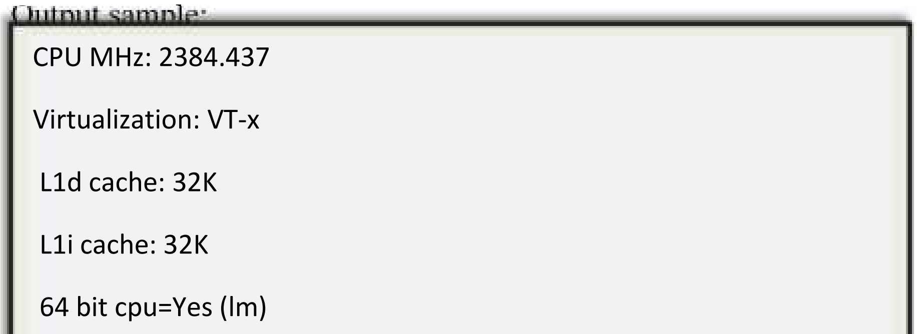
Installing Required Packages

1.To check whether CPU supports hardware virtualization, run the following command:

lscpu

egrep -wo 'vmx|lm|aes' /proc/cpuinfo | sort | uniq\

Output sample:



```
CPU MHz: 2384.437

Virtualization: VT-x

 L1d cache: 32K

 L1i cache: 32K

 64 bit cpu=Yes (lm)
```

2.Install vde2

sudo apt-get install vde2

vde2 provides L2/L3 switching, including spanning-tree protocol and VLANs.

Output sample:

```
[sudo] password for ab:
 Reading package lists... Done
 Building dependency tree
 Reading state information... Done
 vde2 is already the newest version.
The following packages were automatically installed and are no longer required:
kde-l10n-engb kde-l10n-he
```

3.Install iw

Install iw sudo apt-get install iw

iw is a CLI for configuring wireless devices.

Output sample:

```
[sudo] password for ab:
 Reading package lists... Done
 Building dependency tree
 Reading state information... Done
 iw is already the newest version.
The following packages were automatically installed and are no longer required:
kde-l10n-engb kde-l10n-he
```

4.Install hostapd

sudo apt-get install hostapd

hostapd is a user space daemon for wireless AP.

Output sample:

```
sudo] password for ab:

Reading package lists... Done

 Building dependency tree

Reading state information... Done

hostapd is already the newest version.

The following packages were automatically installed and are no longer required:

 kde-l10n-engb kde-l10n-he
```

Creating Virtual Aps

1. First, it is recommended to disable NetworkManager from starting during boot. You have to reboot the computer after that:

sudo mv /etc/init/network-manager.conf /etc/init/network-manager.conf-disabled

2. Check wifi card

we need a wifi card that supports master mode, if we are going to create an access point with it. First, figure out what wifi card is named (look for one starting with ‘wlan’)

ifconfig

Output sample:

```
wlan0              Link encap:Ethernet HWaddr 48:5a:b6:2b:1e:23
                   inet addr:10.42.0.1 Bcast:10.42.0.255 Mask:255.255.255.0
                   inet6 addr: fe80::4a5a:b6ff:fe2b:1e23/64 Scope:Link
                   UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

wlan2               Link encap:Ethernet HWaddr 18:d6:c7:08:38:f7
                   inet addr:10.42.1.1 Bcast:10.42.1.255 Mask:255.255.255.0
```

3.check “AP” mode is supported

iw list

look for something like:

1

2

3

4

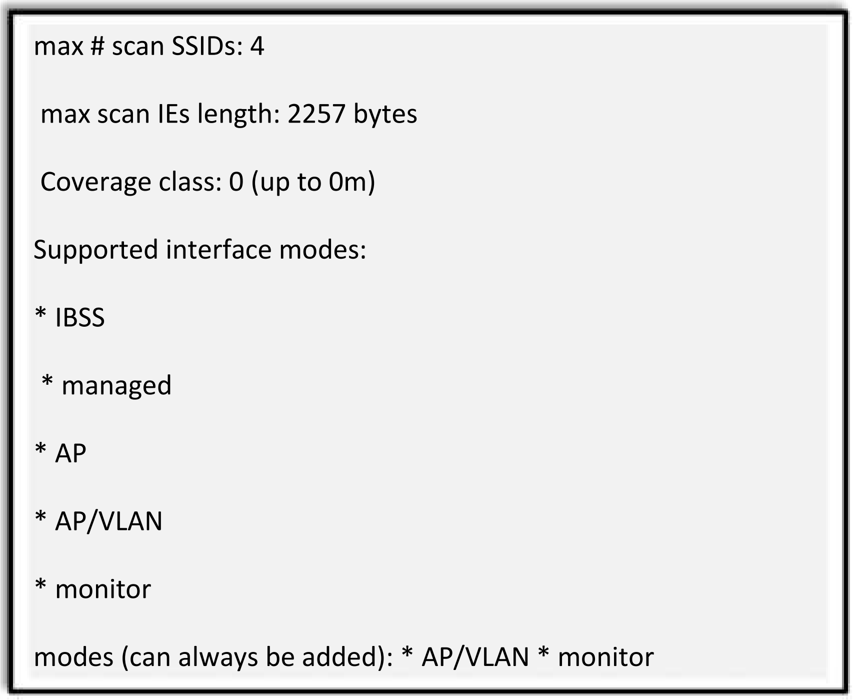
5

6

...

```
Supported interface modes:

        * IBSS

        * AP
```

Output sample:



```
max # scan SSIDs: 4

 max scan IEs length: 2257 bytes

 Coverage class: 0 (up to 0m)

Supported interface modes:

* IBSS

 * managed

* AP

* AP/VLAN

* monitor

modes (can always be added): * AP/VLAN * monitor
```

4. Create the file /etc/hostapd/VMnet1.conf with the following content:

```
[connection]
id=VMnet1
 uuid=b7fb4f73-f930-4e87-8d84-c6268f61770f
 type=802-11-wireless
 timestamp=1494006101
 [802-11-wireless]
 ssid=VMnet1
 mode=ap
 mac-address=48:5A:B6:2B:1E:23
seen-bssids=00:00:00:00:00:00;
security=802-11-wireless-security[802-11-wireless-security]
 key-mgmt=wpa-psk
psk=123456789
[ipv4] method=shared
[ipv6] method=auto
```

5.Create the file /etc/hostapd/VMnet2.conf with the following content:

```
[connection]
id=VMnet2
 uuid=d10cf707-ac32-4a39-af7d-0c1c363bc5e2
 type=802-11-wireless

 [802-11-wireless]

 ssid=VMnet2

 mode=ap

 mac-address=18:D6:C7:08:38:F7

 security=802-11-wireless-security [802-11-wireless-security]

 key-mgmt=none

 auth-alg=open

wep-key0=1234567890

 wep-key-type=1

[ipv4] method=shared

 [ipv6] method=auto
```