Parametric Evaluation of IAPP using Software Access Point and Hardware Access Point

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Computer Science and Engineering

Submitted By
Sukhvinder Singh
(800932022)

Under the supervision of:
Dr. Maninder Singh
Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004

June 2011

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*Parametric Evaluation of IAPP using Software Access Point and Hardware Access Point*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in Computer Science and Engineering submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of Dr. Maninder Singh and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Sukhvinder Singh)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Maninder Singh)
Associate Professor
Computer Science and Engineering Department

Countersigned by

(Dr. Maninder Singh)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. K. Mohapatra)
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

No volume of words is enough to express my gratitude towards my thesis supervisor **Dr. Maninder Singh**, Head of Department, Computer Science & Engineering, whose guidance, wisdom and invaluable help has aided me in the completion of thesis. He has helped me to explore numerous topics related to the thesis in an organized and methodical manner and provided me with many valuable insights into various technologies.

I am also thankful to **Mr. Karun Verma**, P.G. Coordinator, for the motivation and inspiration during the thesis work.

I would also like to thank the staff members and my colleagues who were always there at the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis work.

Most importantly, I would like to thank my parents and the Almighty for showing me the way and encouraging me through the difficult times I encountered during the completion of my thesis work.

ABSTRACT

User mobility in the wireless data networks is increasing because of advancement in the networking and computing technologies. In Large scale IEEE 802.11 Wireless Local Area Network (WLAN) deployments, supporting user and devices mobility is a critical issue, continuous transmission connectivity is highly desirable for most of the networks and its applications. It has been generally seen, in the distribution environment user of one access point moves to another access point and both AP's are of different vendor than the support for the multi-vendor access point interoperability is highly recommended to have a seamless data transmission and fast handoff. In order to ensure all relevant information is delivered to the correct AP to which the station is associated, an Inter Access Point Protocol is required. This protocol enables multiple AP to communicate and pass information regarding the location of associated stations.

This thesis is on the setting up of a small home network. Instead of affording the costly hardware, one can use freeware software in Linux to build Software Access Point in a personal desktop/Laptop as well as measures its performance against Hardware Access Point on a number of relevant metrics.

TABLE OF CONTENTS

LIST OF FIGURES

Readings taken at 10.15am

Reading taken at 5:30pm

LIST OF TABLES

Reading taken at 10.15am

Reading taken at 5:30pm

CHAPTER 1

INTRODUCTION

Communication is one of the most important parts of human society. Human have tried to communicate over long distances for reasons of commerce, defence, family etc .

Wireless communication may be used to transfer information over short distances (a few meters as in television remote control) or long distances (thousands or millions of kilometers for radio communications). The term is often shortened to "wireless". It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of wireless technology include GPS units, garage door openers or garage doors, wireless computer mice, keyboards and headsets, satellite television and cordless telephones. Wireless communication may be used to transfer information over short distances (a few meters as in television remote control) or long distances (thousands or millions of kilometers for radio communications).

1.1 Wireless Communication

There are many communication network standards[23] designed for wireless communication. Some of them are as follows:

i. Wi-Fi

   Wireless Fidelity (Wi-Fi) is a group of wireless standards belonging to the IEEE 802.11 family. A Wi-Fi enabled device such as a personal computer, video game console, Smartphone, and digital audio player can connect to other devices on the network or to the Internet through a wireless network connected to the Internet.

ii. WiMax

Worldwide Interoperability for Microwave Access (WiMax), also known as 802.16, combines the benefits of broadband and wireless. access to large areas such as cities.

iii. Bluetooth

Another standard 802.15, is used for Wireless Personal Area Networks (WPANs). It covers a very short range and is used for Bluetooth technology. It is a packet based protocol with a master slave structure.

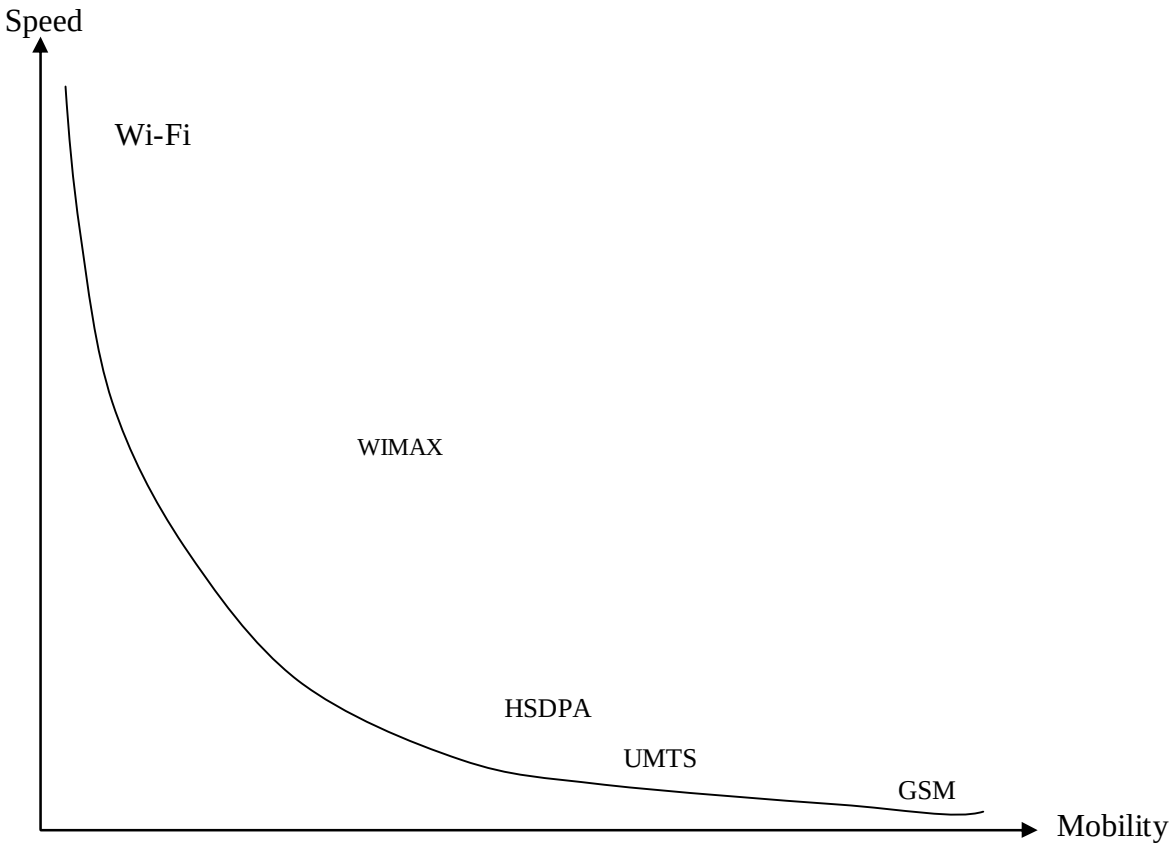


Figure 1.1 Speed vs Mobility between various wireless technologies

1.2 Wireless Fidelity (Wi-Fi) is a wireless standard for connecting electronic devices. A Wi-Fi enabled device such as a personal computer, video game console, Smartphone, and digital audio player can connect to the Internet when within range of a wireless network connected to the Internet. The coverage area of an access point is dependent on the basis of usage; access point for home usage will have less coverage as compared to an enterprise access point which needs to support much more connections. Coverage is of low power access points can be overlapped to provide wireless connection over larger area.

"Wi-Fi" is supported by the Wi-Fi Alliance, a non-profit group comprised of companies like Cisco, Motorola and others. Which is composed of companies and the term was originally created as a simpler name for the IEEE 802.11 standard. Wi-Fi is used by over 700 million people, there are over 4 million hotspots (places with Wi-Fi Internet connectivity) around the world, and about 800 million new Wi-Fi devices every year. Wi-Fi products that complete the Wi-Fi Alliance interoperability certification testing successfully can use the Wi-Fi certified designation and trademark.

A wireless network uses radio waves just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens:

i. A computer's wireless adapter translates data into a radio signal and transmits it using an antenna.
ii. A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection.

The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

The radios used for Wi-Fi communication are very similar to the radios used for walkie-talkies, cell phones and other devices. They can transmit and receive radio waves, and

they can convert 1s and 0s into radio waves and convert the radio waves back into 1s and 0s.

1.3 Wireless Networking Standards

They use 802.11 networking standards[32], which come in several flavors:

i. **802.11a** transmits at 5 GHz and can move up to 54 megabits of data per second. It also uses **orthogonal frequency-division multiplexing** (OFDM), a more efficient coding technique that splits that radio signals into several sub-signals before they reach a receiver. This greatly reduces interference.

ii. **802.11b** is the slowest and least expensive standard. For a while, its cost made it popular, but now it's becoming less common as faster standards become less expensive. 802.11b transmits in the 2.4 GHz frequency band of the radio spectrum. It can handle up to 11 megabits of data per second, and it uses **complementary code keying** (CCK) modulation to improve speeds.

iii. **802.11g** transmits at 2.4 GHz like 802.11b, but it's a lot faster -- it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a.

iv. **802.11n** is the newest standard that is widely available. This standard significantly improves speed and range. For instance, although 802.11g theoretically moves 54 megabits of data per second, it only achieves real-world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second. The standard is currently in draft form -- the **Institute of Electrical and Electronics Engineers (IEEE)** plans to formally ratify 802.11n by the end of 2009.

Other 802.11 standards focus on specific applications of wireless networks, like wide area networks (WANs) inside vehicles or technology that lets you move from one wireless network to another seamlessly.

Wi-Fi radios can transmit on any of three frequency bands. Or, they can "frequency hop" rapidly between the different bands. Frequency hopping helps reduce interference and lets multiple devices use the same wireless connection simultaneously.

As long as they all have wireless adapters, several devices can use one router to connect to the Internet. This connection is convenient, virtually invisible and fairly reliable; however, if the router fails or if too many people try to use high-bandwidth applications at the same time, users can experience interference or lose their connections.

1.4 Roaming/Mobility is defined as being the process where mobility stations(notebook computers, palmtops, laptops, handheld computers), equipped with wireless network adapters, connected to a LAN via access points, are handed over from one access point to another when they move out of coverage of one AP and into that of another. The objective being that the user of the mobile equipment remains connected.

Whenever a mobile host roams to another subnet, its home agent will encapsulate all the packets destined for the mobile host sent to the original subnet, and then forward the encapsulated packets to the mobile host according to its new location. In this way, the mobile host can roam among various subnets and can still receive and transmit data as usual. Thus, even if mobile hosts roam to another subnets, their on-going data transfer can still proceed.

1.5 Access Point

An Access point is a hardware device, which transmits and receives communication signals with wireless devices connected to it. Wireless networking, also called Wi-Fi or 802.11 networking, is comprises of number of access points use to connect wireless devices. Access point made the wireless networking so widespread that can access the

Internet just about anywhere at any time, without using wires.

Figure 1.2 A typical wireless network [24]

Figure 1.1 shows a typical network that connects together a number of wireless devices like Laptops, Personal Digital Assistant, and Smartphone using a hardware wireless access point. Wi-Fi has a lot of advantages. Wireless networks are easy to set up and inexpensive. They're also unobtrusive -- unless on the lookout for a place to use a laptop, may not even notice when in a hotspot.

1.6 Wi-Fi Hotspots

Figure 1.3 Wireless adapters for computer's PC card slot or USB port.[29]

Figure 1.3 shows the hotspots used to make the laptop to work as wireless device.

Most new laptops and many new desktop computers come with built-in wireless transmitters. If laptop doesn't have wireless transmitters, then needs to buy a **wireless adapter** shown in Figure 1.3 that plugs into the PC card slot or USB port. Desktop computers can use USB adapters, or can buy an adapter that plugs into the PCI slot inside the computer's case. Many of these adapters can use more than one 802.11 standard.

Once wireless adapter is installed and the drivers that allow it to operate, the computer should be able to automatically discover existing networks. This means that when computer on in a Wi-Fi hotspot, the computer will inform that the network exists and ask whether want to connect to it. If the computer is very old then, may need to use a software program to detect and connect to a wireless network. [31]

Being able to connect to the Internet in public hotspots is extremely convenient. Wireless home networks are convenient as well. They allow easily connect multiple computers and to move them from place to place without disconnecting and reconnecting wires.

1.7 Creating a Simple Wireless Network

Figure 1.4 A wireless router [25]

Figure 1.4 shows a wireless router uses an antenna to send signals to wireless devices and a wire to send signals to the Internet

If already have several computers networked, they can create a wireless network with a **wireless access point**. If having several computers that are not networked, or want to replace Ethernet network, then it may require a wireless router. This is a single unit that contains:

i. A port to connect to your cable or DSL modem
ii. A router
iii. An Ethernet hub
iv. A firewall

v. A wireless access point

A wireless router enables the use of wireless signals or Ethernet cables to connect devices like computer to another device like a printer or the Internet. Most routers are Omni-directional to a range of about 100 feet (30.5 meters), although reflective metallic objects can create problems of connectivity. Usually extenders or repeaters are used to increase the routers signal range like in a big building or public parks.

Most routers can use more than one 802.11 standard. Routers based on older technology are less expensive like those based on 802.11b, but are much slower than those based on new standards like 802.11g and 802.11n or newer revisions of existing standards like 802.11a. 802.11g is the most popular option due to its speed and reliability.

Once plug in to the router, it should start working at its default settings. Most routers use a web interface to change its settings. The selectable values are:

i. The name of the network, also known as its service set identifier (SSID), default setting is usually the device manufacturer's name.
ii. The channel used by a router is 6 by default. The problem of interference experienced in an environment where a number of devices are being used can be solved switching to a different channel should eliminate the problem.
iii. Most routers have a bare minimum of security implemented by setting the same default user and password, usually the company’s name.

Security is an important part of a home wireless network, as well as public Wi-Fi hotspots. If router is set to create an open hotspot, anyone who has a wireless card will be able to use your signal. Most people would rather keep strangers out of their network, though. Doing so requires taking a few security precautions.

It's also important to make sure security precautions are current. The Wired Equivalency Privacy (WEP) security measure was once the standard for WAN security. The idea behind WEP was to create a wireless security platform that would make any wireless network as secure as a traditional wired network. But hackers discovered vulnerabilities

in the WEP approach, and today it's easy to find applications and programs that can compromise a WAN running WEP security.

To keep network private, one of the following methods can be used:

i. **Wi-Fi Protected Access** (WPA) is a step up from WEP and is now part of the 802.11i wireless network security protocol. It uses temporal key integrity protocol (TKIP) encryption. As with WEP, WPA security involves signing on with a password. Most public hotspots are either open or use WPA or 128-bit WEP technology, though some still use the vulnerable WEP approach.

ii. **Media Access Control** (MAC) address filtering is a little different from WEP or WPA. It doesn't use a password to authenticate users -- it uses a computer's physical hardware. Each computer has its own unique MAC address. MAC address filtering allows only machines with specific MAC addresses to access the network. Must specify which addresses are allowed when set up a router. This method is very secure, but if buy a new computer or if visitors to want to use network, needs to add the new machines' MAC addresses to the list of approved addresses. The system isn't foolproof. A clever hacker can **spoof** a MAC address that is; copy a known MAC address to fool the network that the computer he or she is using belongs on the network.

Wireless networks are easy and inexpensive to set up, and most routers' Web interfaces are virtually self-explanatory.

1.8 The IEEE 802.11 Wireless LAN Architecture

The IEEE 802.11 architecture [12] is comprised of several components and services that interact to provide station mobility transparent to the higher layers of the network stack. The basic architecture is depicted in Figure-1 Several entities can be distinguished, namely the Wireless Station or Mobile Host, the Basic Service Set, the Distribution System and the Access Point.

i. **Wireless LAN Station**: The station (or Mobile Host, MH) is the most basic component of the wireless network. A station is any device that contains the functionality of the 802.11 protocol, that being MAC, PHY, and a connection to the wireless media. Typically the 802.11 functions are implemented in the hardware and software of a Network Interface Card (NIC). A station could be a laptop PC, handheld device, or an Access Point. Stations may be mobile, portable, or stationary and all stations support the 802.11 station services of authentication, de-authentication, privacy, and data delivery.

ii. **Basic Service Set (BSS)**: as the basic building block of an 802.11 wireless LAN. The BSS consists of a group of any number of stations.

iii. **Extended service set (ESS**): An extended service set (ESS) is a set of connected BSSs. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

iv. **Distribution System (DS):** is the means by which an access point communicates with another access point to exchange frames for stations in their respective BSSs, forward frames to follow mobile stations as they move from one BSS to another, and exchange frames with a wired network.

As IEEE 802.11 describes it, the distribution system is not necessarily a network nor does the standard place any restrictions on how the distribution system is implemented, only on the services it must provide. Thus the distribution system may be a wired network like 803.2 or a special purpose box that interconnects the access points and provides the required distribution services.

v. **Access Point**: is a fixed entity in the network that connects the mobile hosts with the Distribution System.

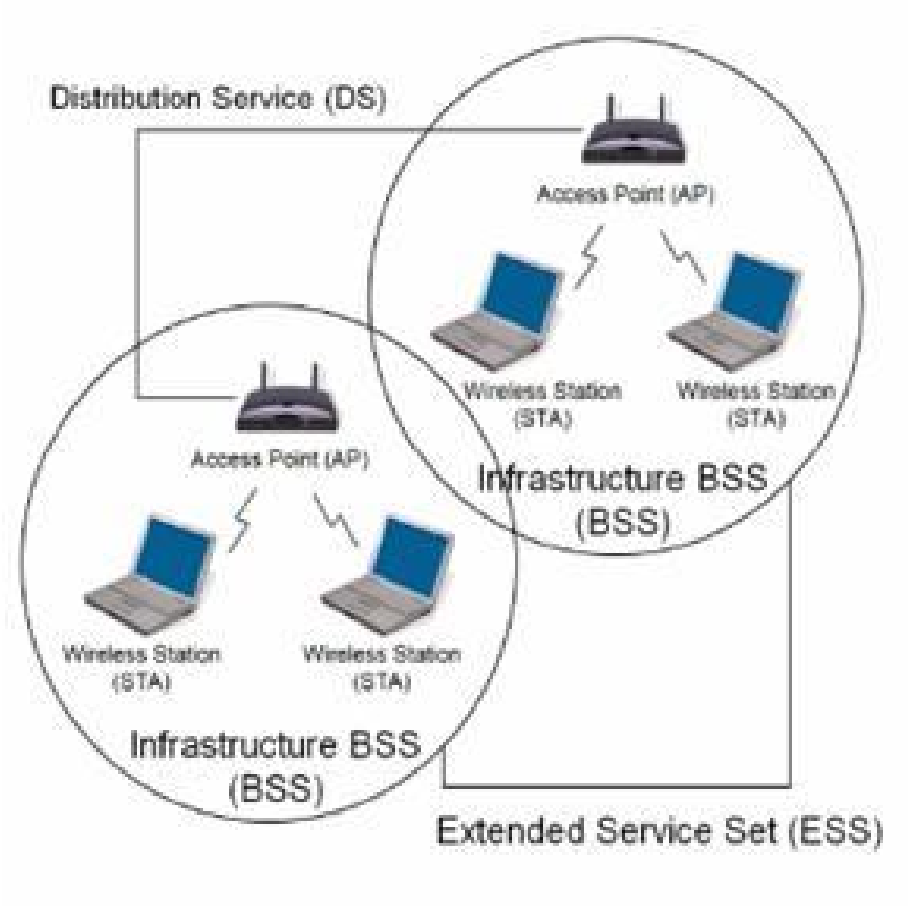


Figure 1.5 Basic Architecture of an IEEE 802.11 Wireless LAN [26]

The coverage area of the wireless LAN can be extended via an **Extended Service Set (ESS).** An extended service set is a set of infrastructure BSS's, where the access points communicate amongst themselves to forward traffic from one BSS to another to facilitate movement of stations between BSS's.

1.9 IEEE 802.11 distribution system services

The IEEE 802.11 standard specifies the following distribution system services as the communication between an access point and mobile hosts or distribution system:

i. **Association** : When a mobile host initially starts, it receives the beacon from an access point, and then sends out association request to inform the access point of its entrance into the BSS. After confirmation, the mobile host can then communicate with other networks via this access point.
ii. **Disassociation :** This service is used to notify the access point that the mobile host has left the BSS served by it.
iii. **Reassociation :** When a mobile host roams into another BSS served by a new access point, it then sends out a reassociation request to inform the new access point of its entrance into the BSS. Again, after confirmation, the mobile host can then communicate with other networks via this new access point.
iv. **Distribution :** This service is used when an access point wants to use a distribution system to communicate with other networks.
v. **Integration :** This service is used for a non-802.11 wireless network to communicate with a distribution system.

1.10 IEEE 802.11 Topologies

The 802.11 standard describes two modes of deployment for the WLAN

i. Infrastructure mode
ii. The Ad-Hoc mode.

The most basic wireless LAN topology is a set of stations, which have recognized each other and are connected via the wireless media in a peer-to-peer fashion. This form of network topology is referred to as an *Independent Basic Service Set* (IBSS) or an *Ad-hoc* network.

In an IBSS, the mobile stations communicate directly with each other. Every mobile station may not be able to communicate with every other station due to the range limitations. There are no relay functions in an IBSS therefore all stations need to be within range of each other and communicate directly.

Figure 1.6 The ad-hoc mode [27]

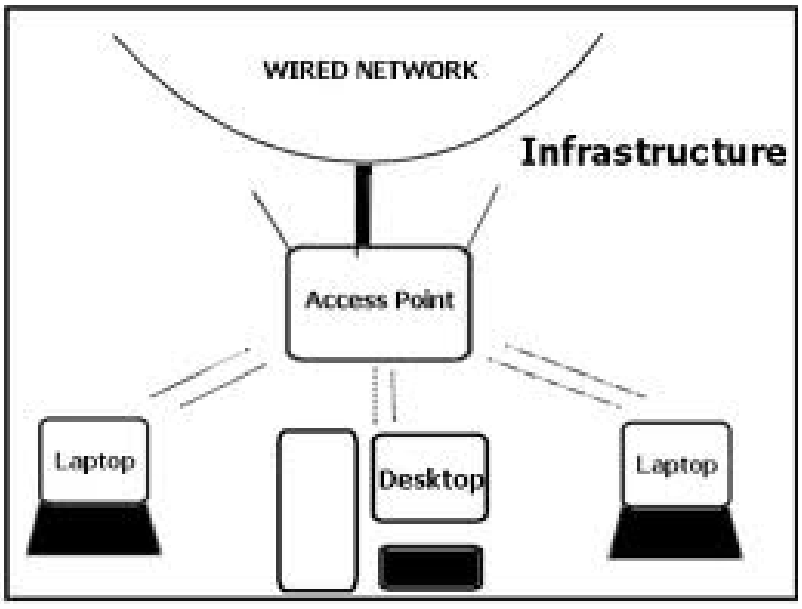


Figure 1.7 Infrastructure mode [28]

An Infrastructure Basic Service Set is a BSS with a component called an *Access Point* (AP). The access point provides a local relay function for the BSS. All stations in the

BSS communicate with the access point and no longer communicate directly. All frames are relayed between stations by the access point. This local relay function effectively doubles the range of the IBSS.

1.11 IEEE 802.11 Handoffs

The handoff procedure of IEEE 802.11[21][11][2] can be divided into two steps:

i. Discovery
ii. Re-authentication.

Discovery: In order to find a nearby AP, a MH scans all channels either passively or actively. In passive scanning, a MH listens to AP's periodic beacon messages to know their parameters, such as beacon interval, capability information, BSSID, supported rate, etc. In active scanning, for every channel, a MH will broadcast a probe request and expect probe responses from APs.

Re-Authentication: This typically involves the authentication and re-association procedures. The re-authentication phase transfers the credentials of the MH from the old AP to the new AP.

Below Figure-1.8 shows the steps involved during handoff. Whenever the station is on, it starts the scans for APs by either sending probe request messages (active scan) or by listening for beacon message (passive scan) broadcast by AP. In Figure-3 message A through D shows the active scan. A probe request (message A and C) is sent by the STA and probe responses (messages B and D) are received from the AP to station. After scanning all intended channels, the station selects the AP based on data rates and signal strength. After probe a station and AP exchange authentication (message E and F). After authentication station sends a re-association request to AP (message G) and receives a re-association response from the AP (message H). During re-association, the APs involved exchange station context information.

At last the mobile host successfully connects with the Access point.

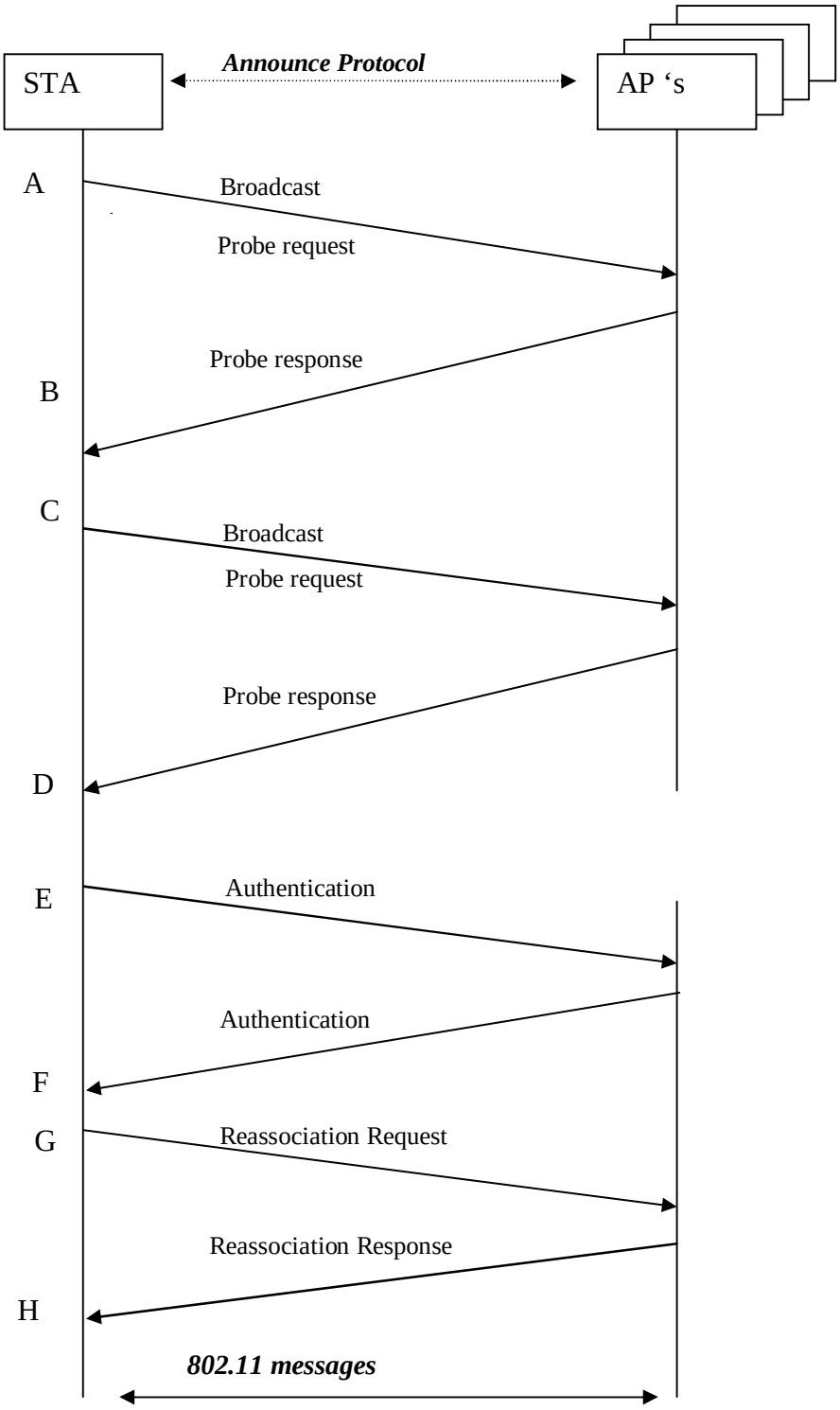


Figure 1.8 Handoff procedure by IEEE 802.11

1.11 Structure of thesis

Chapter 2: In this chapter the Literature survey is carried out.

Chapter 3: In the chapter the Problem statement is defined, also set the objectives and methodology used is mentioned.

Chapter 4: In this Chapter the Configuration details is shown, the Software Access Point and Hardware Access point results have been obtained and analysis is carried out. IAPP implementation in Software AP and messaging is also shown between Software AP and Mobile Hosts

CHAPTER 2

LITERATURE REVIEW

To provide integrated networking service, Helal et al. (2000) presented architecture for integration between wireless LANs and wireless WANs. Similarly, their architecture uses Mobile IP as an integrative layer a top different LAN/WAN networks. However, reducing the handoff latency is not discussed in their paper.

Several studies have focused on reducing the handoff latency for mobile hosts to roam across IP networks or across access points in various aspects. Fikouras et al. (2001) proposed a method using the link-layer information to accelerate Mobile IP handoff. Through link-layer information such as the 802.11b Service Set Identifier (SSID) that provides the identity of Mobile IP agent, Mobile IP mechanisms for movement detection and periodic Mobile IP agent broadcast advertisements are not necessary. Therefore, faster Mobile IP hand-offs can be achieved. However, this method should assume that the link-layer is capable of delivering information to Mobile IP layer regarding the identity of Mobile IP agent. In contrast, our approach maintains the layer independence and uses packet filter in access point's bridge program to reduce unnecessary broadcast advertisements from Mobile IP agent.

Mishra et al. (2004)[2] proposed proactive caching to avoid handoff delay caused by IAPP communication between two access points as well as access point and RADIUS server. Current access point of a mobile host distributes the security context of the mobile host to its neighboring access points in advance. So that when the mobile host is re-associating to its neighboring access point, context transfer from old access point to new access point is not needed. They also devised an efficient data structure, neighbor graphs (Mishra et al., 2004), to dynamically determine the set of potential neighboring access points without examining network topology and manually creating the set. Currently, the proposed proactive caching is included in the IAPP recommended practice (IEEE, 2003).

Shin et al. (2004) devised a discovery method using neighbor graphs and non-overlap graphs in the probing process to find a new access point with the best signal quality with respect to the mobile host. Their goal is to reduce the total number of probed channels as well as the total time spent waiting on each channel.

Pack and Choi, 2002a and Pack and Choi, 2002 proposed a fast inter-access point handoff scheme for public wireless LAN. They use predicative authentication scheme to minimize the handoff latency caused by authentication procedures at the new access point. Whereas, our work focuses on the implementation of the system supporting IAPP protocol and using dual packet filtering technique to reduce traffic on wireless networks and improve transmission performance.

Chun-Ting Chou and kang G. Shin[1], Fellow, IEEE proposed Enhancement relies on the access point's interoperability with other APs, provided by the IP-Based IAPP, so as to enable the intra and inter-subnet link-layer frame buffering-and-forwarding. They used ns-2 simulation results show that the inter-subnet handoff process is transparent to the mobile host's TCP session. The enhanced IAPP supports higher user mobility and achieves a higher TCP throughput.

Sourav Pal1, Sumantra Kundu3, Preetam Ghosh2, Kalyan Basu3,andSajalDas3, 1 Microsoft Corporation, 2 USM, 3 CReWMaN Lab[13], UTA describe the design, implementation, and evaluation of a software based framework that facilitates seamless and transparent handoff between different APs in standard IEEE802.11 based wireless local area networks (WLANs). Although different solutions are available in the literature that seeks to address the handoff latency, most of them propose changes that are outside the purview of the current 802.11 standards. They have specifically kept such compatibility restrictions in mind and have devised a software based client side solution that is capable of reducing handoff delays to an average value of 20ms. They have successfully implemented and tested our proposed solution framework on Atheros AR5212 chipsets using the open source MadWifi driver.

Kumudu S. Munasinghe and Abbas Jamalipour[19], School of Electrical and Information Engineering, They presents an analytical model for evaluating signaling cost of vertical handoffs in a heterogeneous mobile networking environment at the core network level for a roaming user. The numerical analysis and evaluation is based on a framework designed for interworking between Universal Mobile Telecommunications System (UMTS), CDMA2000 technology, and mobile WiMAX (Worldwide interoperability for Microwave Access) Networks. Results and analysis illustrate the behavior of the signaling cost metric against session arrival rate, network mobility rate, and the call-to-mobility rate.

Li Jun ZHANG & Samuel PIERRE 2006[18], proposed A New Seamless Method to Support CDMA2000/WLAN Vertical Handover and demonstrated the effectiveness of their Numerical results show that the new method has better performance than the brute force handoff the seamless handoff and the optimized seamless handoff.

Ping-Jung Huang, Yu-Chee Tseng, and Kun-Cheng Tsai 2006[7], wireless networks. This paper proposed a fast and seamless handoff solution for IEEE 802.11 wireless LAN with IAPP. It is based on a concept of neighbor graph, which describes the nearby access points (APs) that a mobile host (MH) may find. Then we further derive selective scanning with unicast in power-save mode, pre-registration of IAPP, and frame forwarding-and-buffering mechanisms. Selective scanning allows a MH to only try potential handoff targets. Pre-registration allows early transfer of a MH's security context from its old AP to new AP. The forwarding-and-buffering mechanism is to solve the packet loss problem during handoff. There performance evaluation shows that the proposed solution can result in 90% reduction in the handoff latency from standard handoff procedure.

Lei Zan, Jidong Wang and Lichun Bao[12], Bren School of Information and Computer Sciences, University of California, Irvine, CA 92697 2005, roaming capabilities. They propose a mobility management scheme, called Personal AP, to support station mobility efficiently. In Personal AP mobility support system, the mobility context of each mobile station is defined by the relevant state information at the currently associated access

point, including the MAC layer association states at the access point. When the mobile station roams, the access point context follows the mobile station from one physical access point to another, thus creating the “ghost” access point following the mobile station and eliminating the mobile station from re-associating with new access points.

Mobile IP2 David J. Y. Lee and William C. Y. Lee, Group Technology Strategy 2001[8], they proposed a mean for ubiquitous network access for consumers in both wired and wireless environments. We introduce the concept of multiple-interfaced multiple-connection to support high-speed handoff and seamless roaming between different networks (wired and wireless). This is implemented by improving current mobile IP concept, extending existing IP (specifically CMIP and Am) functions and enhancing current PC device drivers and software.

Behcet Sarikayaa and Timucin Ozugur[10], Computer Science Department, University of orthern British Columbia, Prince George, B.C., Canada, 2004, they design a protocol for paging (tracking agent based paging or TAP) IEEE 802.11 wireless LAN hosts. Mobile nodes in IEEE 802.11 BSS constitute a Layer-2 paging area. The tracking agent (TA) is in charge of the paging state, and TA continuously updates the paging state after each Layer 2 handoff. Paging on the wireless link is done by extended beacons, and does not involve periodic layer-3 messages. Signaling in TAP is based on IEEE’s IAPP with minor extensions. They evaluate the performance of TAP and show that TAP achieves superior power savings.

SeongSoo PARK[17], New Technology Development Team, Network R&D Center, SK Telecom 2004, They describe the roaming service with mobile IP between public WLAN and cdma2000 lx Ev-Do design, and implemented. In terms of network Configuration, the coverage of public WLAN network is overlapped with that of Ev-Do network. In this Configuration, mobile terminal will decide the access system among the available systems. They propose the roaming method based on measuring the power of WLAN signal in hybrid network environments, and implement it.

M.S. Bargh, R.J. Hulsebosch, E.H. Eertink A. Prasad, H. Wang, P. School 2004[16], They analyses the applicability of IEEE 802.11f and Seam by solutions to enable fast authentication for inter-domain handovers and proposes a number of possible changes to these solutions (typically in terms of network architectures and/or required trust relationships) for inter-domain operation.

Cheng-Shong Wu et al[15], they propose a cross-layer fast handoff scheme in order to provide seamless mobility support to the mobile hosts in IEEE 802.11 wireless networks. They modify the enhanced IAPP to fit real-time traffic and extend the function of an IEEE 802.11 Access Point to co-operate with cross layer considerations. The link layer handoff latency has been improved by proposed scheme.

Ian Herwono et al[20], this paper demonstrates how the Inter Access point Protocol (IAOO) can be used to improve the performance in a Media Point systems. They present three mechanisms to improve performance. First, IAPP allows reducing the required signaling by means of an extended EAP-TLS authentication procedure. Second, IAPP can be used to trigger an abbreviated DHCP procedure. Third they present a pre-caching mechanism for the hierarchically structured media point network.

Sangho Shin, Anshuman Singh Rawat & Henning Schulzrinne[21], discovered the new handoff procedure which helps the mobile station to perform a Handoff whenever it moves out of the range of one access point (AP) and tries to connect to a different one. This takes a few hundred milliseconds, causing interruptions in communication. They developed a new handoff procedure which reduces the MAC layer handoff latency, in most cases, to a level where communication become seamless. This new handoff procedure reduces the discovery phase using a selective scanning algorithm and a caching mechanism.

Jungwook Choi $ Hyukjoon Lee[41], In this paper, they describe a seamless handover scheme for an IEEE 802.11p-based wireless access system that take advantage of the fixed-order placement of the RSUs and unidirectional movement of the vehicle along the highway. More specifically this handover scheme utilize the IEEE 802.11 disassociation

message as to signal the old RSU of an on-board Unit's (OBU) departure from its coverage area. The subsequent downstream data frames can be proactively forwarded to the new RSU for delivery to the OBU after its link establishment with the RSU.

A.Gueroui and S.Boumerdassi[33], In this paper the effect of handovers in the fixed part of a cellular network by defining two new algorithms. These algorithms are based on two different schemes: pre-establishment with prediction and uniform pre-establishment. Their goal is to improve two parameters of the quality of service: blocking calls and dropping handovers.

Masugi Inoue, Khaled Mahmud, Homare Murakami, Mikio Hasegawa, and Hiroyuki Morikawa [34], An out-of-band Basic Access Signaling (BAS) protocol is introduced for use in heterogeneous wireless networks. The BAS protocol enables a mobile terminal to communicate with an agent in a fixed network through any radio access network (RAN) chosen by the user as the Basic Access Network (BAN). The agent uses information on the location of mobile terminals and on the availability of RANs to decide which RAN to use, taking the user's preferences into account. This protocol was implemented in a demonstration system using existing radio systems and the standard Mobile IP protocol. The separation of the signaling path from the data paths was found to save energy and to facilitate handover between RANs

Alex Yiu-Man Chan and Wen-Pai Lu[35], This paper presents an architecture for wireless access in vehicles, to facilitate real-world deployments. A Mobile Access Router provides network connectivity to multiple wireless networks, from wireless LANs to wide area mobile networks such as CDPD or CDMA, in a size ideal for vehicles. A wireless LAN allows a low-cost deployment of high-speed wireless networks in a metro area. In addition, by using Mobile IP, VPN, and other intelligent network services, the networked vehicle can achieve seamless roaming and secured network connectivity anytime and anywhere. The possibility for innovative, multimedia applications on this versatile architecture is endless.

N. Olaziregi, A.H. Aghvami[36], This paper analyzes the management requirements to control the reConfiguration process of terminals. Accordingly, a supporting network element and subsequent software architectural design are proposed. In particular the components allowing for soft handovers are addressed. In addition, features to shorten the service outage time at mode selection are also described.

Ronald Beaubrun, Samuel Pierre, Paola Flocchini & Jean Conan[37] This paper presents an efficient approach which facilitates interoperability between heterogeneous networks during global roaming situations. Preliminary results reveal that such an approach significantly improves the performance of the NG wireless systems in terms of generated signaling traffic and response time during the global roaming process. Global Roaming Management in the Next-Generation Wireless Systems

Murad Abusubaih, James Gross, and Adam Wolisz [38], this paper presents and valuates an Inter-Access Point Coordination protocol for dynamic channel selection in IEEE 802.11 WLANs. It addresses an open issue for the implementation of many distributed and centralized dynamic channel selection policies proposed to mitigate interference problems in Wireless LANs (WLANs). The presented protocol provides services to a wide range of policies that require different levels of coordination among APs by enabling them to actively communicate and exchange information. An Intra-Cell protocol that enables interaction between the AP and its accommodated stations to handle channel switching within the same cell is also presented.

Farouk. Belghoul, Yan. Moret, Christian. Bonnet[39], In this paper they propose to analyze current handover approaches in main IP-based mobility protocols in terms of complexity, efficiency, and effect on TCP performances; we discuss number of issues that motivate each handover design. A number of key design choices are identified and exploited from this analysis to present our new IPv6-based soft-handover approach.

Eric Y. Chen and Mistutaka Itoh [40], In this paper, they presented Virtual Smartphone over IP system that allows smartphone users to create virtual images of Smartphone in the cloud and access these images remotely from their physical Smartphone. The

prototype we implemented integrates the remote environment with the local environment and allows users to run remote applications as they would locally. Through our prototype, mobile applications installed in the cloud can access sensor readings on the physical Smartphone. Our prototype also boosts the performance of mobile applications by providing virtually unlimited computing resources at user's fingertips, without draining the device battery.

CHAPTER 3

PROBLEM STATEMENT

3.1 Problem Definition

Wireless enabled systems have become fairly ubiquitous, with Wi-Fi accessibility being available not only with laptops but also cell phones, DVD-players, televisions and other electronic devices. The increase in number of devices with Wi-Fi capability has helped against the cable clutter, but a wireless network requires investment in a hardware wireless access point device to transmit and receive signals from all the Wi-Fi enabled device. These devices are preprogrammed and cannot be customized as per user requirements and needs. In some networks most of the communication takes place between just a client and server, like streaming a movie from a storage server to a display device. Hardware access points are not necessary for such simple loads. The Hardware access point has the mobility problem.

IAPP IEEE802.11f standard was proposed for smooth hand-off from one access point to another, while client is on move. We wish to implement IAPP using Linux hosted access points

3.2 Objectives

- To design and implement a Linux Access Point.
- To compare the Software Access point with Hardware Access Point, emphasis IAPP Implementation.
- To evaluate and validate the test results.

3.2 Methodology

- Set-up Isolated network using 2-3 wireless enabled laptops/Desktops (Linux platform)
- Install the hostapd a freeware and configure it to work as an Access Point.
- Install and configure the dhcpd server so that the IP addresses can be released by the Access point, while probed by the Mobile Hosts.
- Use Configuration stubs to test Linux Hosted Access Point functionality
- Start the Wi-Fi adapter of Laptop or Desktop into Master Mode to work as a Software Access Point.
- Compare the Announce protocol of Hardware Access Point vs Software Access Point using ping and test it by sending the different size of payloads.

CHAPTER 4

LINUX BASED SOFTWARE ACCESS POINT

A wireless access point running on Linux can be configured to operate as a bridge, by simply forwarding packets between the wireless network and the local Ethernet. This allows wireless devices to be switched on and connected to an existing network with Configurations to the host computer systems wireless network adapter.

The first step in setting up a system that can act as a Software Access Point we need a Linux OS. The test system used uses the Ubuntu variant of Linux.

4.1 Ubuntu

Ubuntu is, and always will be, absolutely free. Created by the best open-source experts from all over the world, Ubuntu is available in 24 languages and available free for download. Ubuntu is a fast, secure and easy-to-use operating system used by millions of people around the world. Thousands of free applications are freely available in the Ubuntu Software Centre, which can be customized as required.

Ubuntu works brilliantly with a range of devices. No installation CDs. No fuss. And it’s compatible with Windows also.

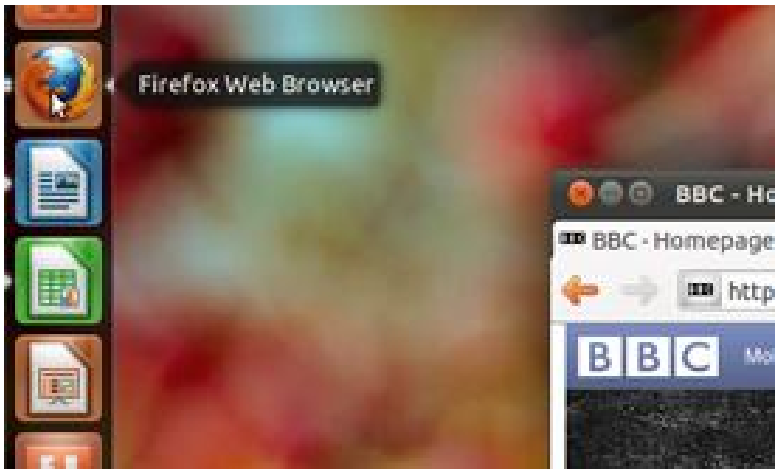


Figure 4.1 a Fresh look of Ubuntu

Ubuntu loads quickly on any computer, but it's super-fast on newer machines. With no unnecessary programs and trial software slowing things down, booting up and opening a browser takes seconds. Unlike other operating systems that leave staring at the screen, waiting to get online. And Ubuntu won't grow sluggish over time. It's fast. And it stays fast.

Global community is made up of thousands of people who want to help build the best open-source operating system in the world. They share their time and skills to make sure that Ubuntu keeps getting better and better. From IBM to Google, Firefox to Wikipedia – some of today's best software is based on an open-source model. Shared efforts. Shared principles. No cost.

The best feature is that whether want to browse the web, email and chat, create documents or edit videos, Ubuntu's got it all. Also Ubuntu does everything you need it to. It'll work with your existing PC files, printers, cameras and MP3 players.

4.2 Access Point setup

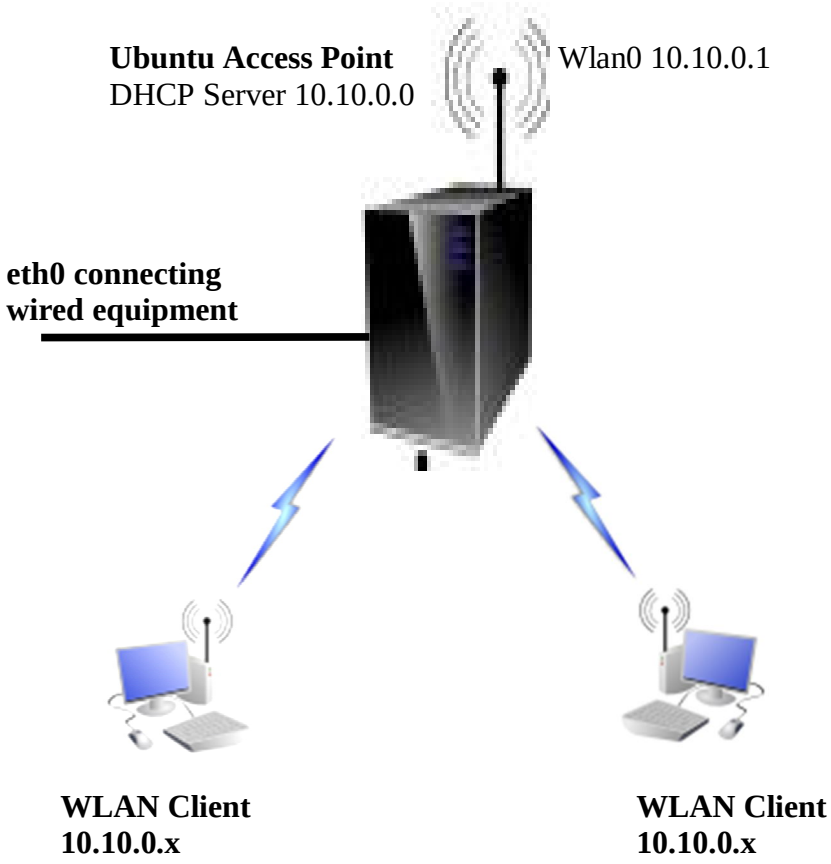


Figure 4.2 Ubuntu Access Point

Figure 4.2 shows that the desktop computer system having Wi-Fi supported adapter is configured as a Access Point. The interface wlan0 is configured as DHCP server (10.10.0.0) and an IP pool is assigned to it. Whenever any wireless enabled device is found within this Ubuntu Access Point Premises, it lease the IP to the client, after the clients acquires the IP automatically they are ready for communicating with each other. The information received at eth0 (wired connected network) can also be broadcasted to the wireless part of the network using routing technique.

4.3 Concept

Used an application called hostapd and put it into the master mode, which allows the Wi-Fi adapter to work as Access Point, where the SSID name, channel, hardware mode etc is defined. To connect the client to the Access Point an IP address is required for that the DHCP is used which lease the IP's to the probing clients.

4.4 Important Configuration details

(NOTE: The actual Configuration files used are shown as **Annexure as mentioned below)**

The steps to configure a Software Access Point on host computer system are as follows:

All the command to be in sudo mode

Installing the required packages for the Access Point is dhcp-server3 and hostapd. The command used to install this package is

sudo apt-get install dhcp3-server hostapd

Once the packages are installed,

i. modify the hostapd.conf and do the following Configuration. (Annexure-I)

```
interface = wlan0
driver = nl80211
ssid = MyAP
hw_mode = g
channel = 11
IAPP_interface=eth0
```

ii. Configure the Dynamic Host Control Protocol (DHCP) on the interface wlan0 . (Annexure-II)

```
Subnet 10.10.0.0 netmask 255.255.255.0 {
        Range 10.10.0.2 10.10.0.50;
}
```

Start the dhcpd daemon

iii. Configure the new interface. (Annexure-III)

```
iface wlan0 inet static
address 10.10.0.1
netmask 255.255.255.0
```

Now restart the network daemon and dhcpd daemon.
Now the dhcp is ready to lease the IP address to the Mobile Host, DHCP configuration is bounded to the wlan0 interface.

iv. NAT Configuration with IP Tables

Set up IP Forwarding and Masquerading

```
iptables --table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE
iptables --append FORWARD --in-interface eth1 -j ACCEPT
```

Enables packet forwarding by kernel

```
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Run the hostapd and this will display the messages on the consoles

```
hostapd -dd /etc/hostapd/hostapd.conf
```

This will show the probes being done by other hotspot devices and also show its association and inactivity details frequently.

4.5 Testing Platform

The tests were conducted on a Computer system Intel Core 2 Duo 2.10 Ghz CPU, 3GB RAM, computer system has 1397 WLAN Mini-Card for Wireless, Installed OS Ubuntu 10.04.

4.6 Results

i. From Ubuntu based Access Point

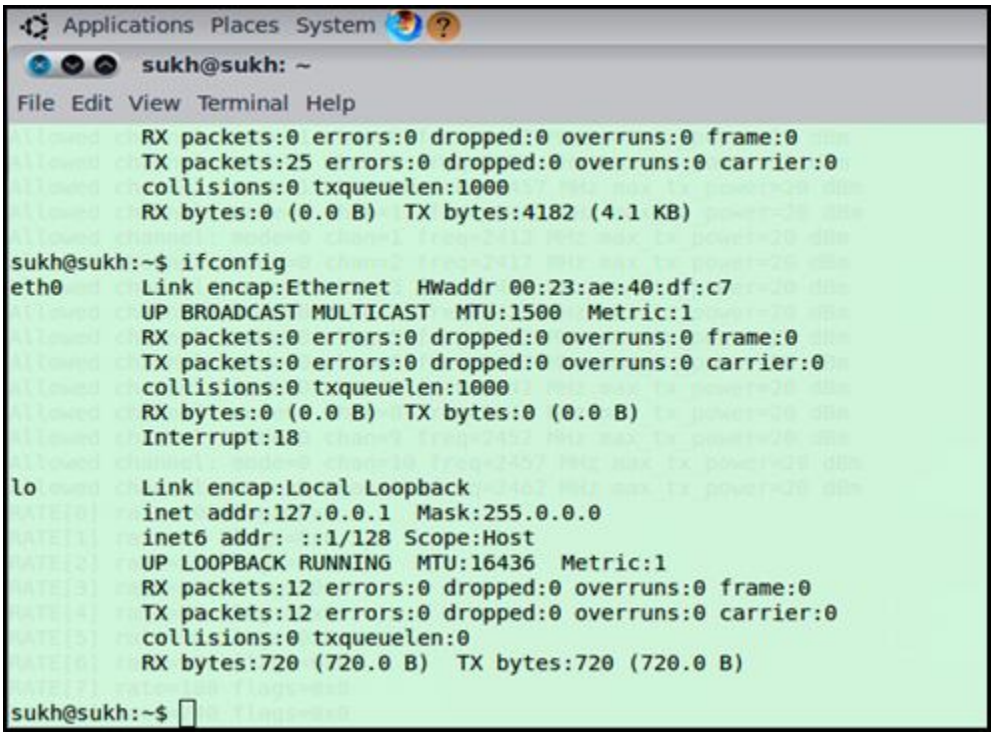


Figure 4.3 System ifconfig details prior to AP mode

It shows the laptop ifconfig details where the wlan0 is not present means the Laptop is at present working as normal Computer not an Access Point.

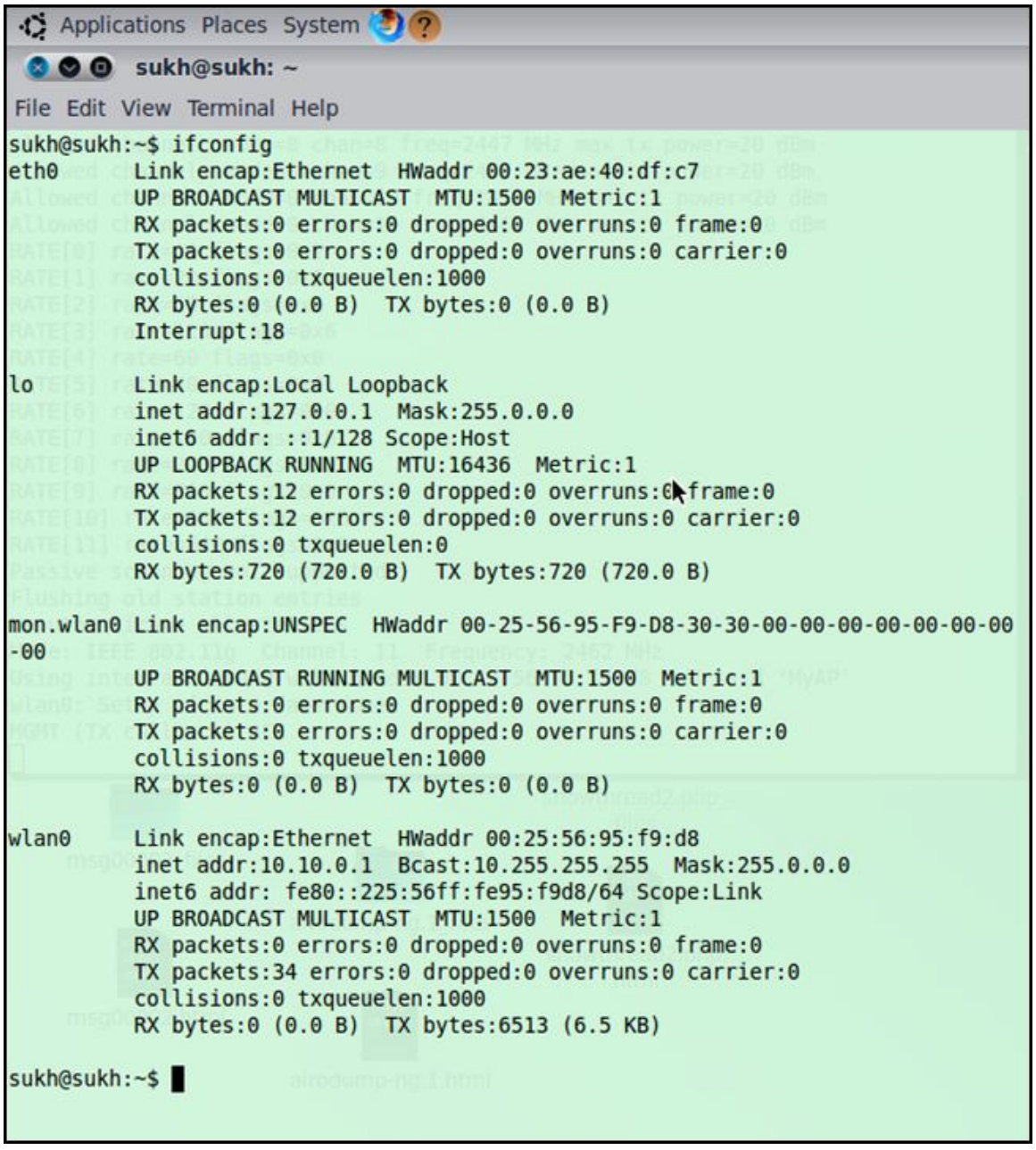


Figure 4.4 System ifconfig details after AP mode

Figure 4.4 shows the Laptop ifconfig and at this movement the Wi-Fi adapter(i.e wlan0 interface) of this Laptop is in Master Mode means working as Access Point with the IP Address of 10.10.0.1.

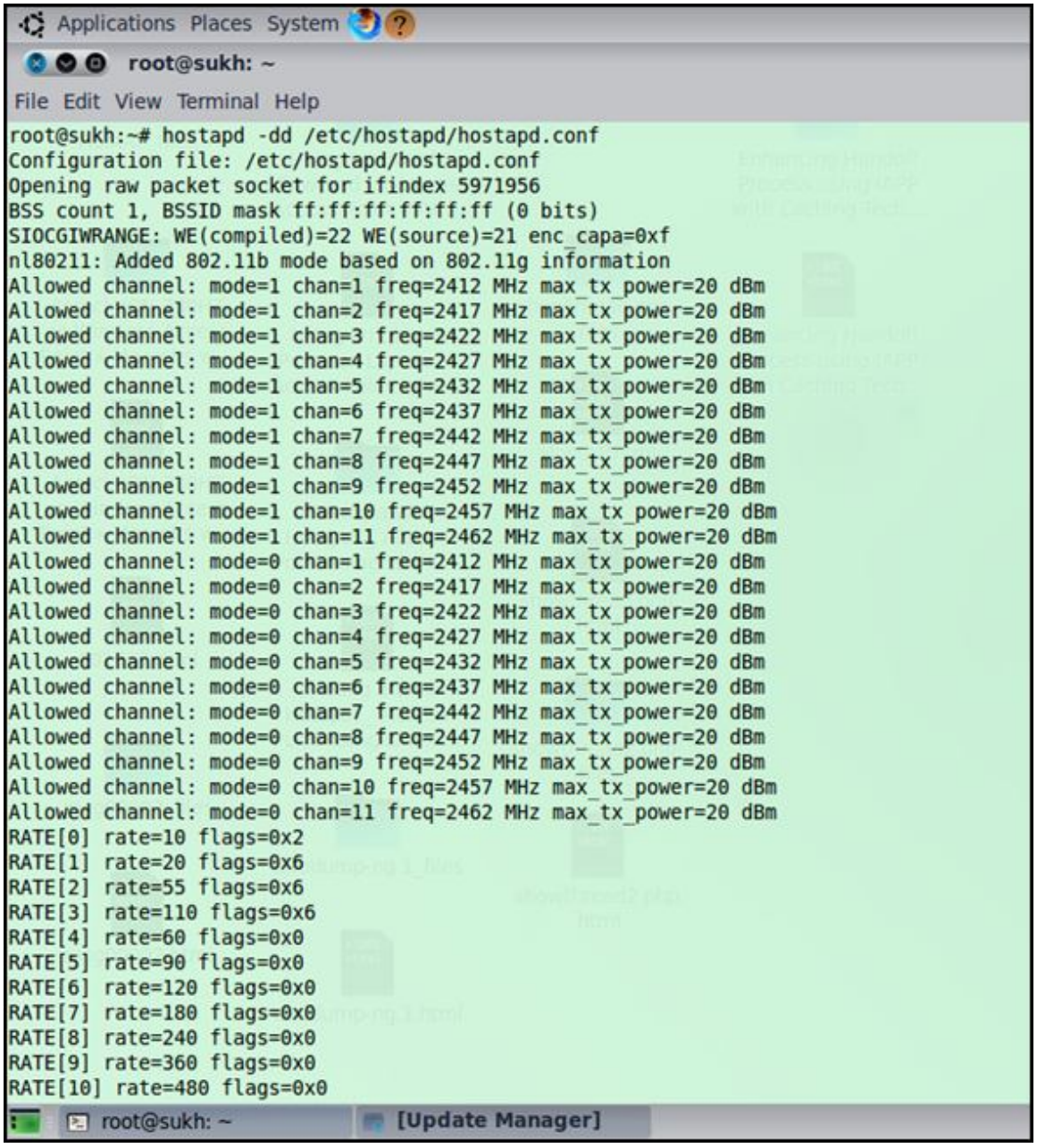


Figure 4.5 Running AP showing the allowed channel for communication

Figure 4.5 shows the Wi-Fi adapter is running as Access Point and allowing the channels to be probed by the Mobile Host.

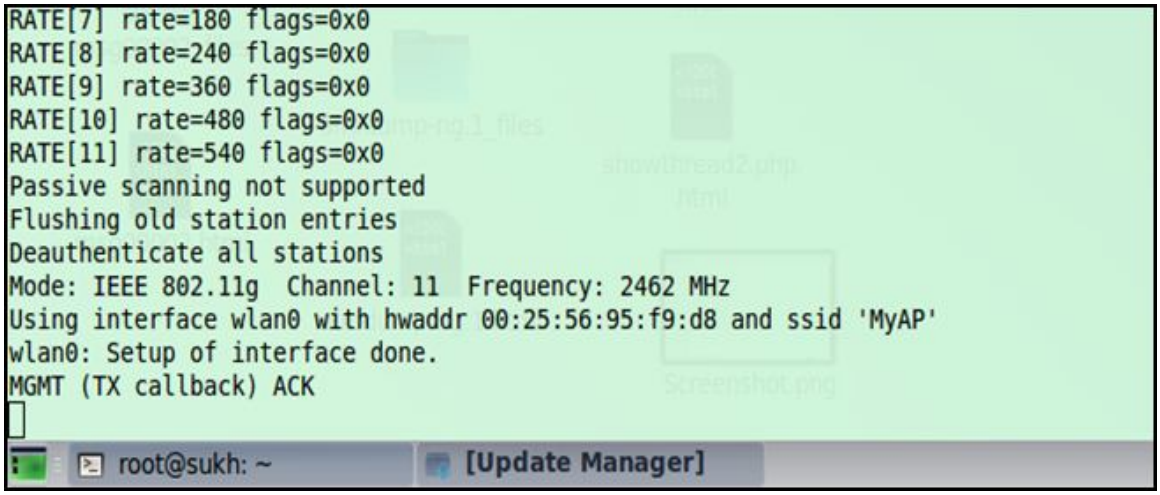


Figure 4.6 MyAP interface done and ready to receive at channel 11

Figure 4.6 shows that, the Laptop is on the IEEE 802.11g mode with channel 11 and the SSID is MyAP. Now it is ready to acknowledge the probe signals of the Mobile Hosts.

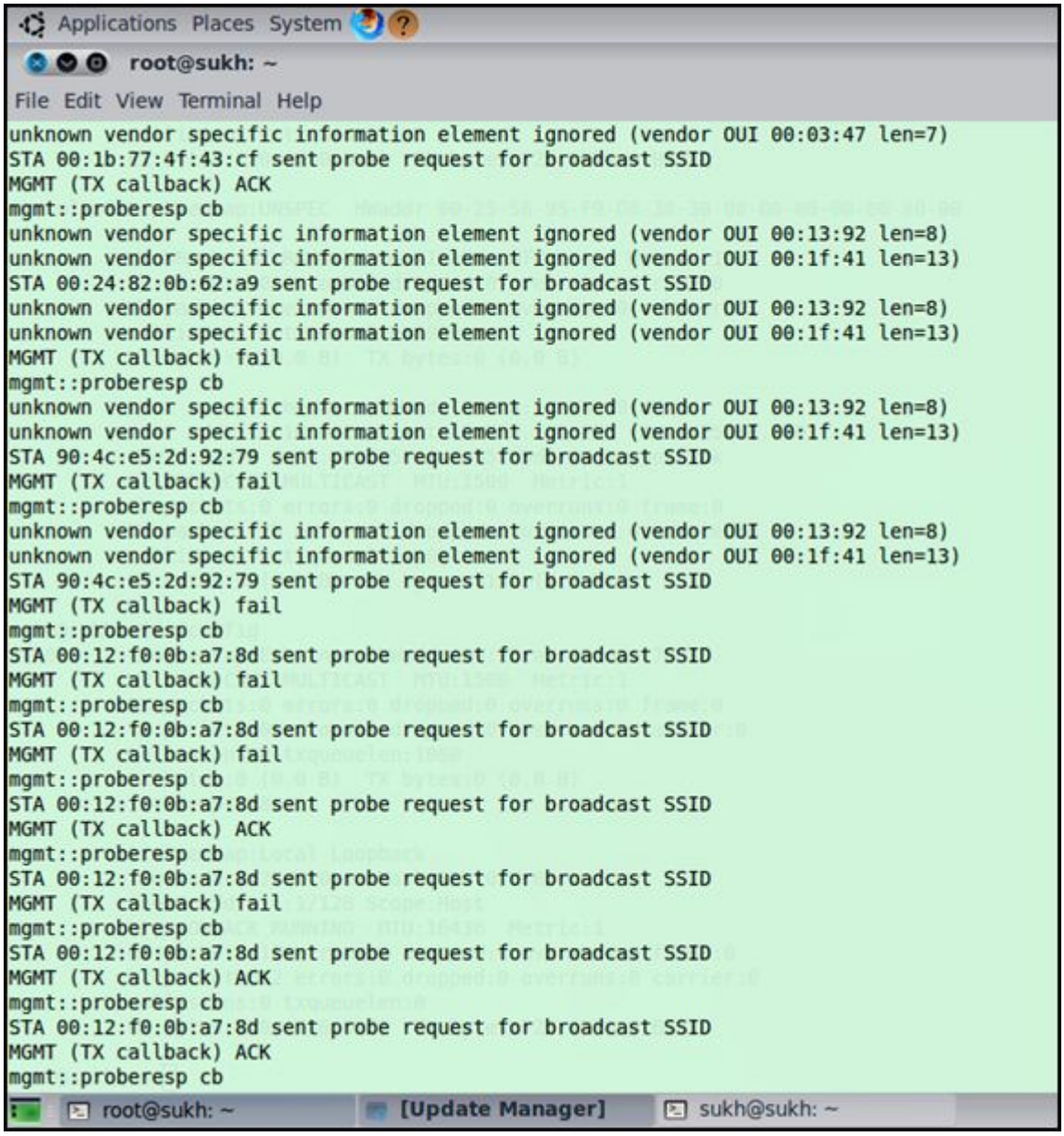


Figure 4.7 Probe request for broadcast SSID to Mobile Hosts

Figure 4.7 shows the probe signals received from the Mobile Hosts to the Software access point

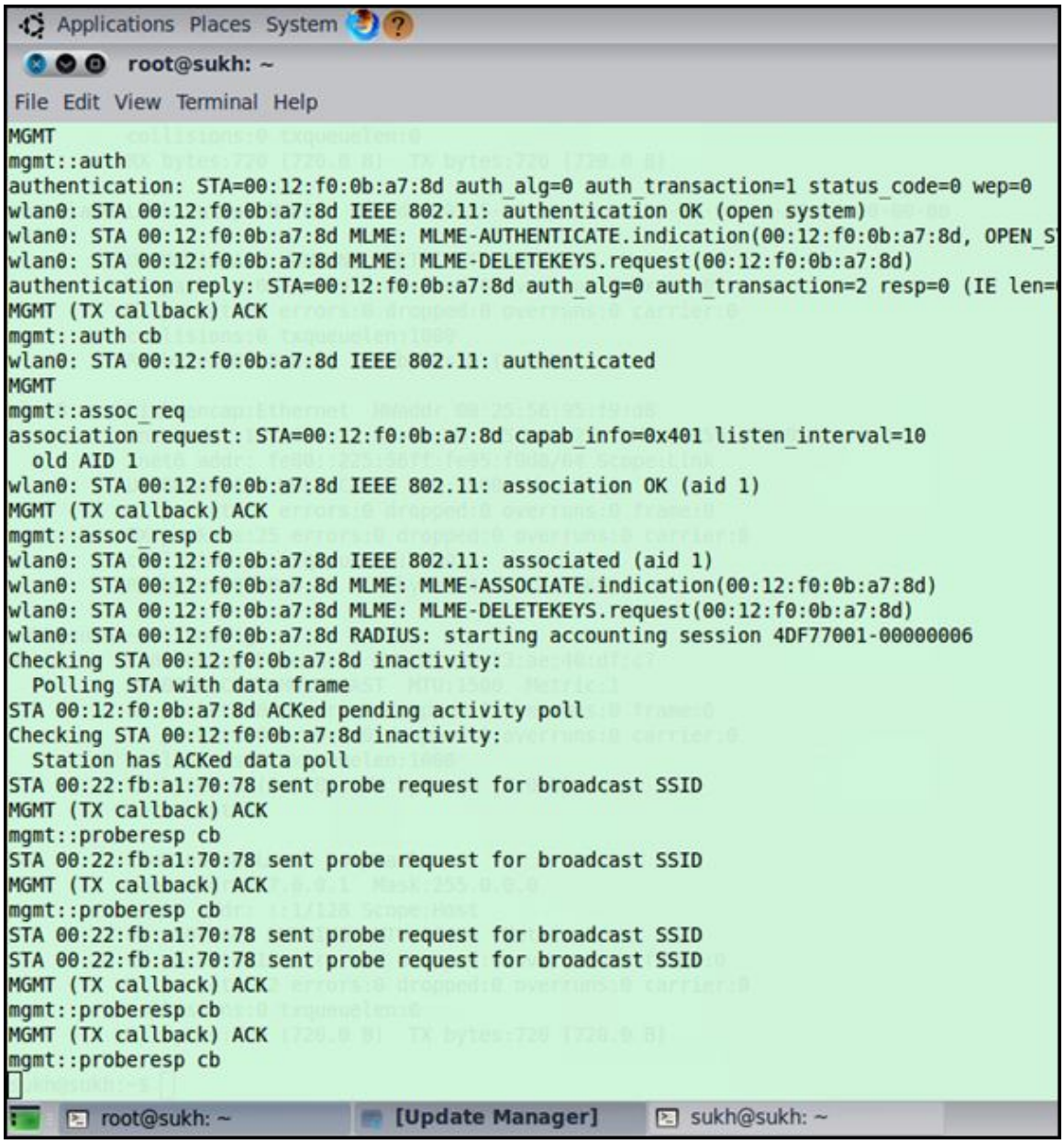


Figure 4.8 Association established with station

Figure 4.8 shows, as the Software Access Point Acknowledges the Mobile Host request, then it authenticates and the association request is sent, once accept the association is established.

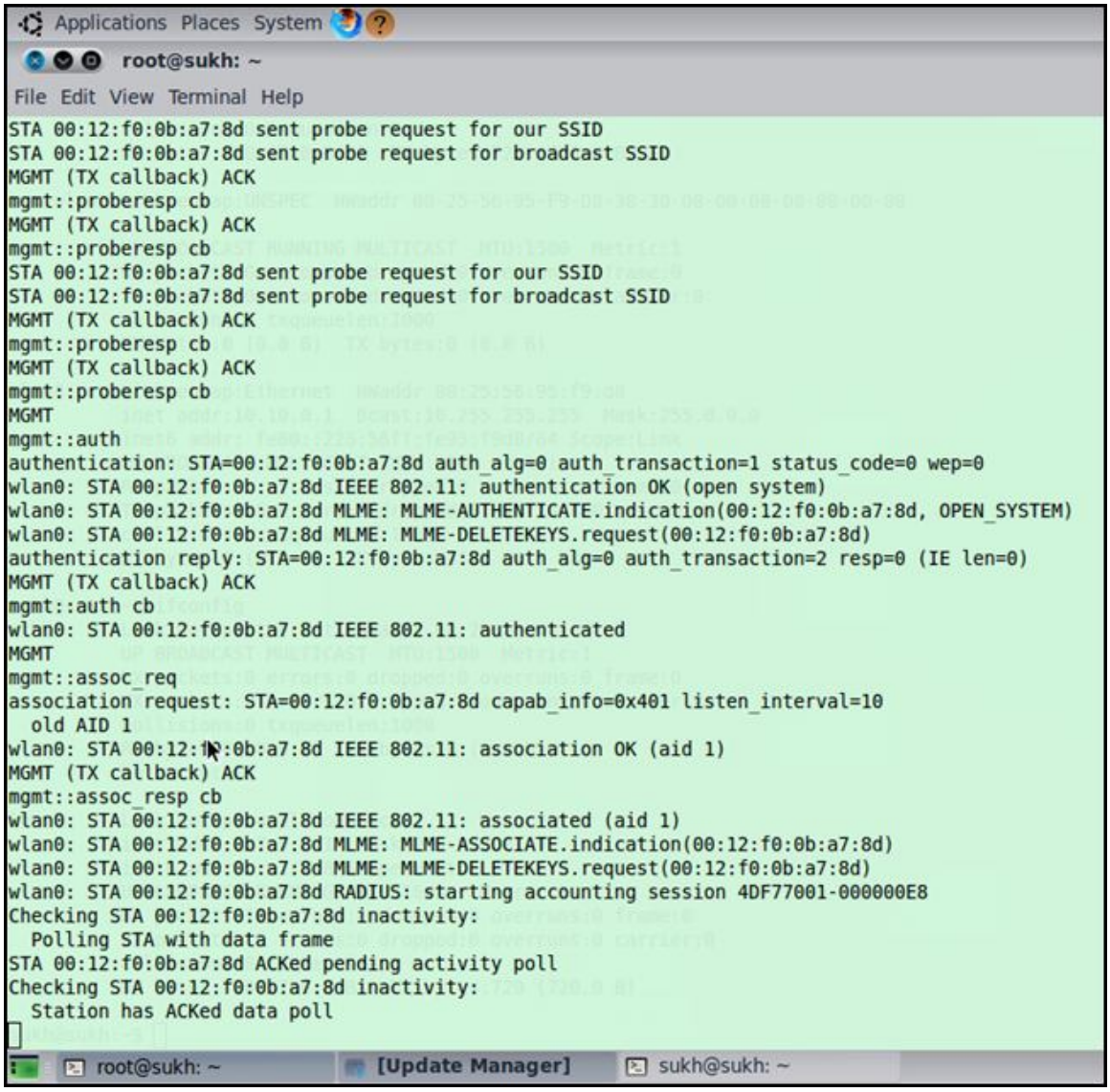


Figure 4.9 Probing and checking the station inactivity

Figure 4.9 shows, inactive scanning. Once the association is established between Software Access Point and the Mobile Host the Access point Keep on checking the status of the Mobile Hosts which are associated with the Access Point. This ensures that the Mobile Host's are active or inactive.

ii. Client end Screenshots

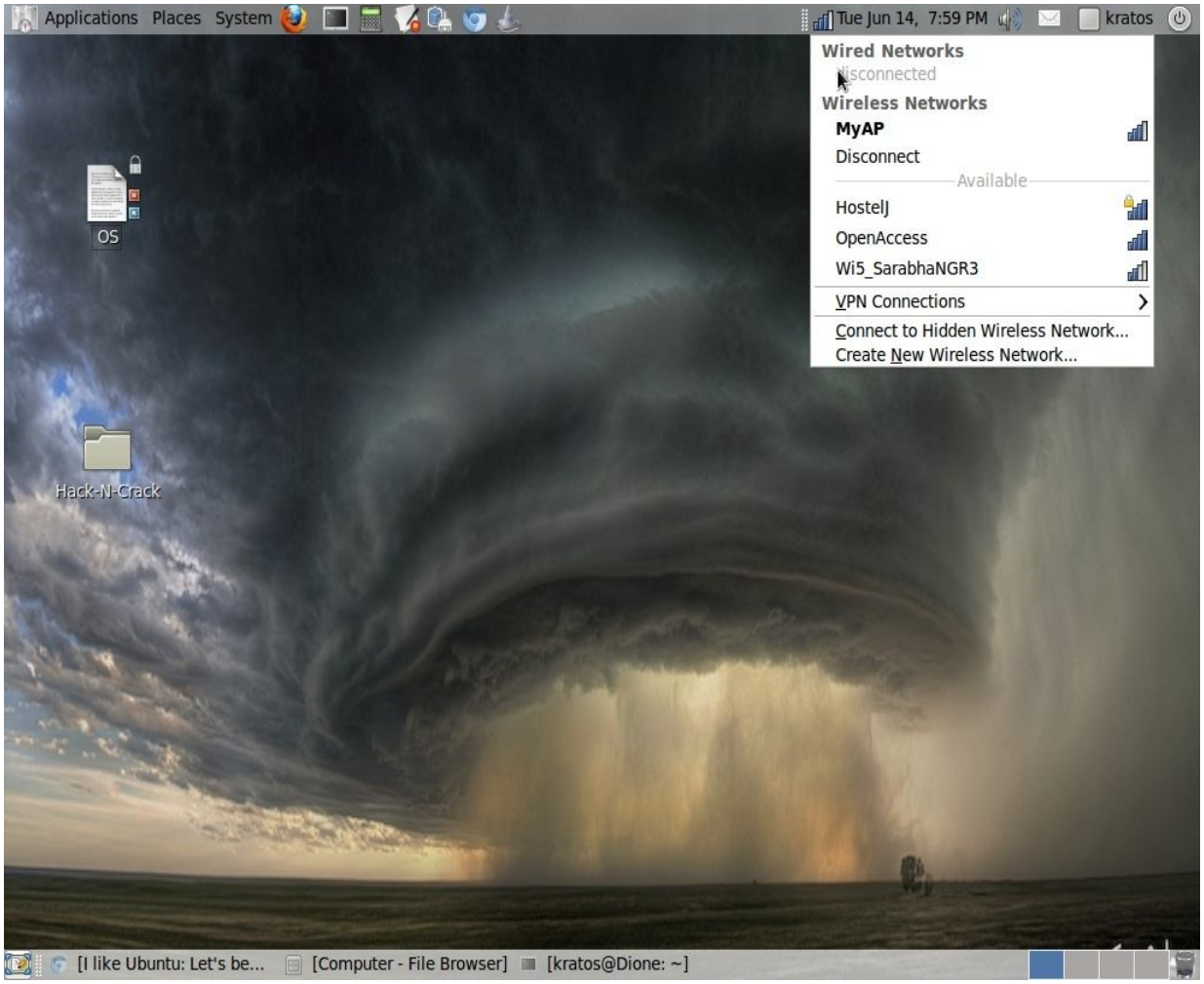


Figure 4.10 Station connected with MyAP (a software AP)

Figure 4.10 shows that the Mobile Host is established an association with the MyAP SSID of Software Access Point.

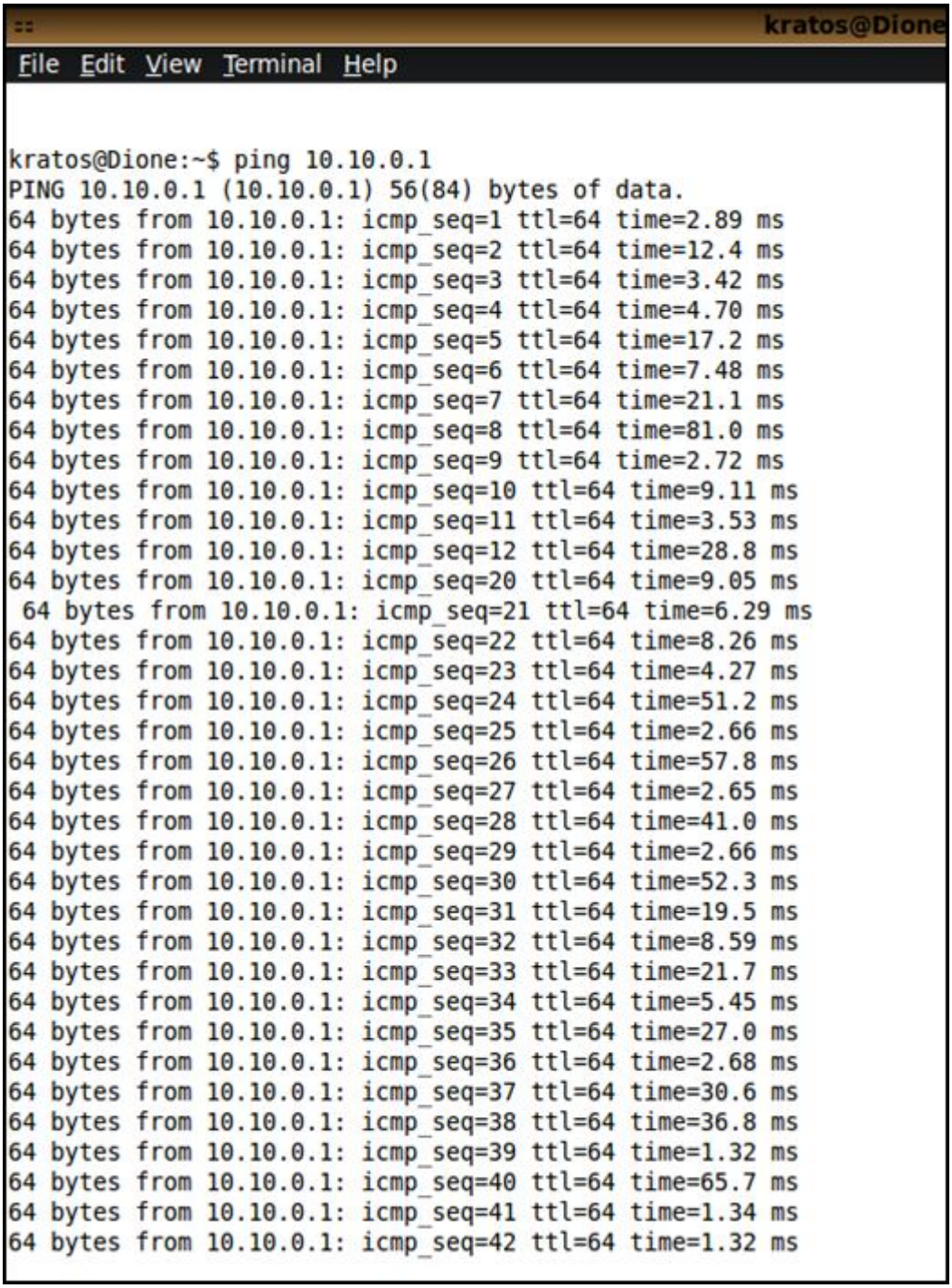


Figure 4.11 Latency measures to transfer the payload of 64 bytes from client to software AP

iii. Latency Performance measurements between Hardware and Software access points (Reading timing 10.15 am).

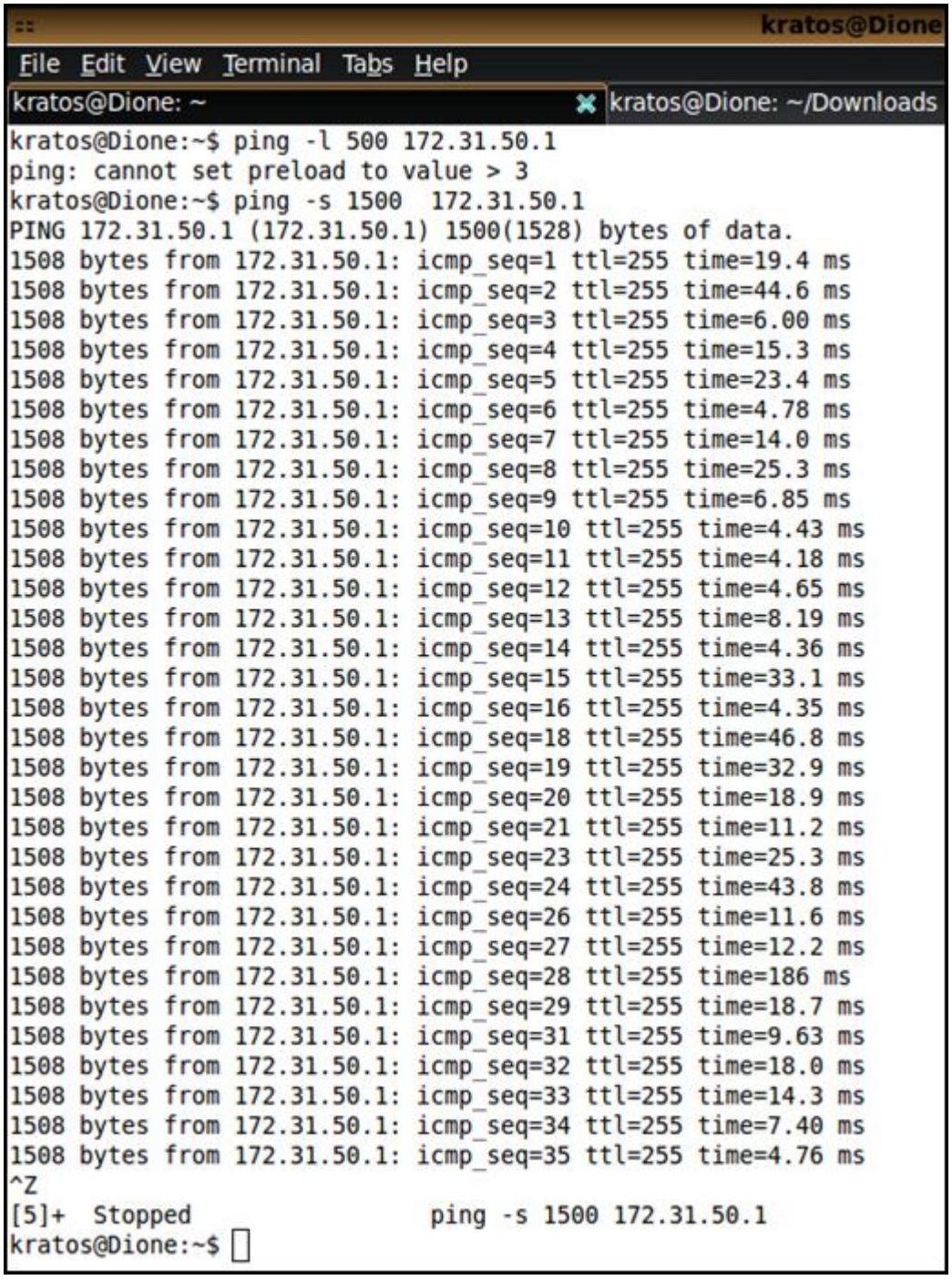


Figure 4.12 Latency measures while sending payload of 1500 to hardware AP from MH

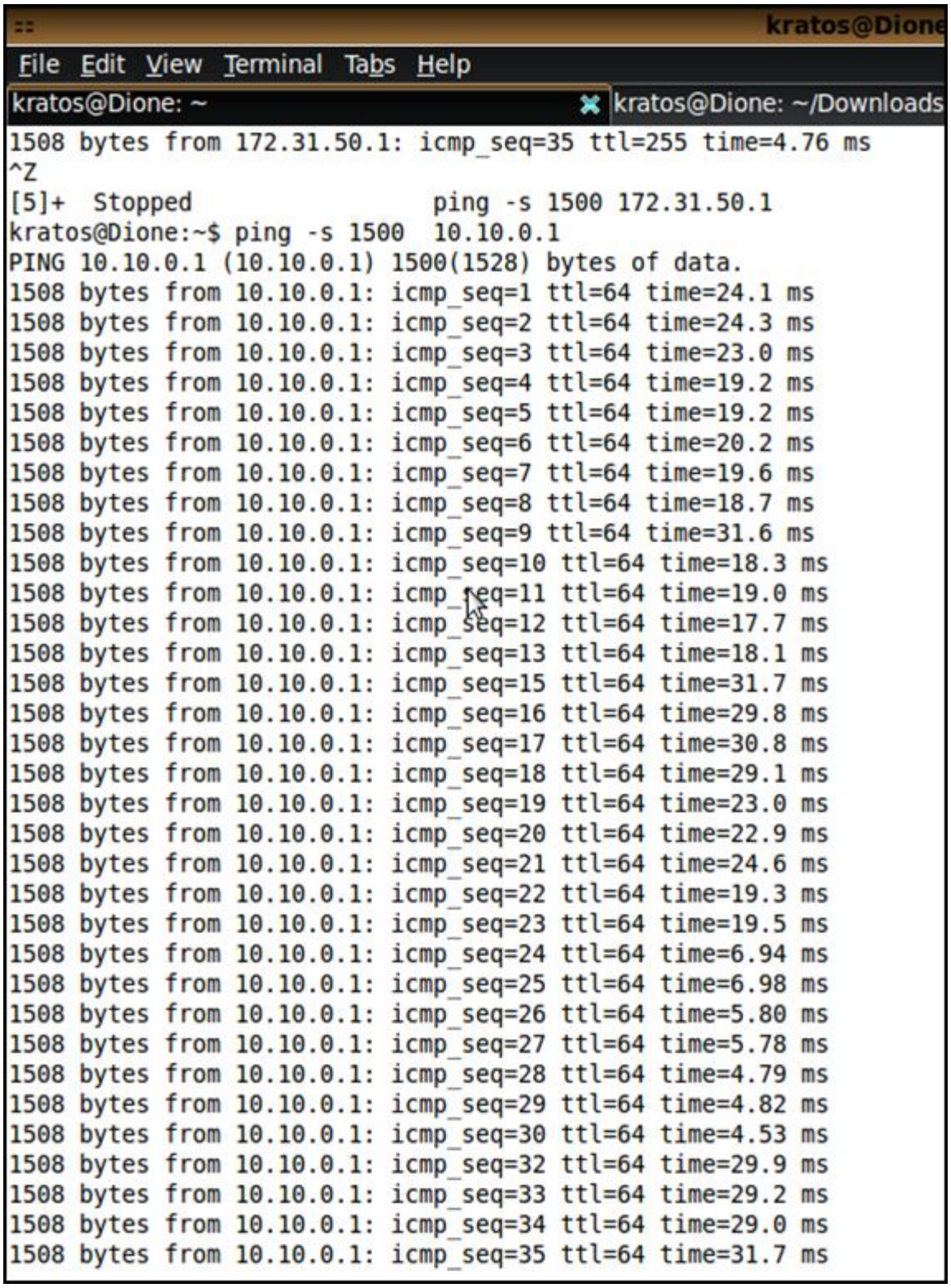


Figure 4.13 Latency measures while sending payload of 1500 to Software AP from MH

S.No	RTT taken for software AP	RTT taken for Hardware AP
1	24.1	19.4
2	24.3	44.6
3	23.0	6.00
4	19.2	15.3
5	19.2	23.4
6	20.2	4.78
7	19.6	14.0
8	18.7	25.3
9	31.6	6.85
10	18.3	4.43
11	31.6	4.18
12	18.3	4.65
13	19.0	8.19
14	17.7	4.36
15	18.1	33.1
16	31.7	4.35
17	29.8	46.8
18	30.8	32.9
19	29.1	18.9
20	23.0	11.2
21	22.9	25.3
22	24.6	43.8
23	19.3	11.6
24	19.5	12.2
25	6.94	186
26	6.98	18.7
27	5.80	9.63

28	5.78	18.0
29	4.79	14.3
30	4.82	7.40
31	4.53	4.76

Table 1 Round Trip Time taken to send payload of 1500 bytes by Software AP and hardware AP

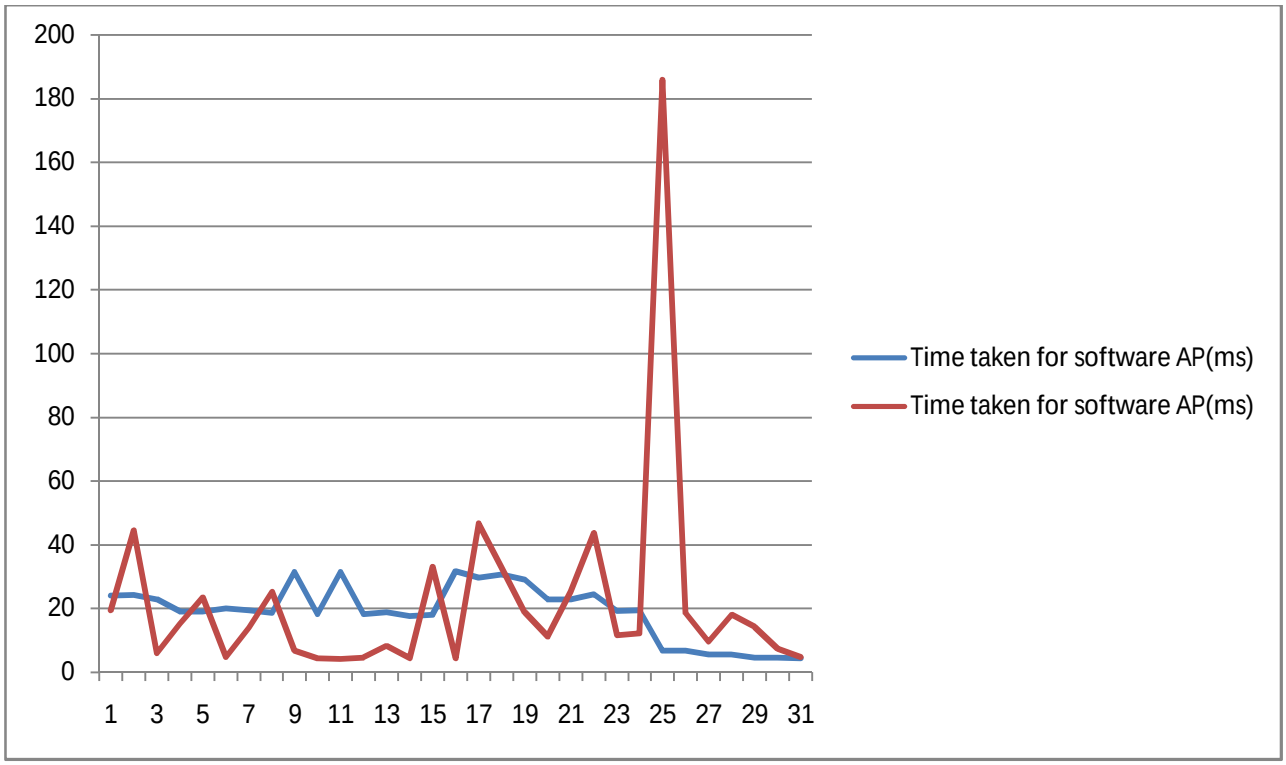


Figure 4.14 Graph showing Round Trip Time of 1500 bytes payload send to Software Access Point and Hardware Access Point

Figure. 4.14 shows the Round Trip Time (RTT) taken by both software and hardware Access Point. It shows when the Client station sends the payload of 1500 byte to the

hardware access point the RTT shown a huge variation, while in the software Access Point when the same payload is sent the RTT is very steady or it is almost constant.

The maximum RRT taken by software Access Point is 31.6ms as per the 9 and 11 reading shown in the Table-1 where as in hardware Access Point it reached upto 186ms as per 25 reading shown in the table-1which is very high. With this result it has been show that the Hardware Access Point takes the more RTT to sent the payload to the destination

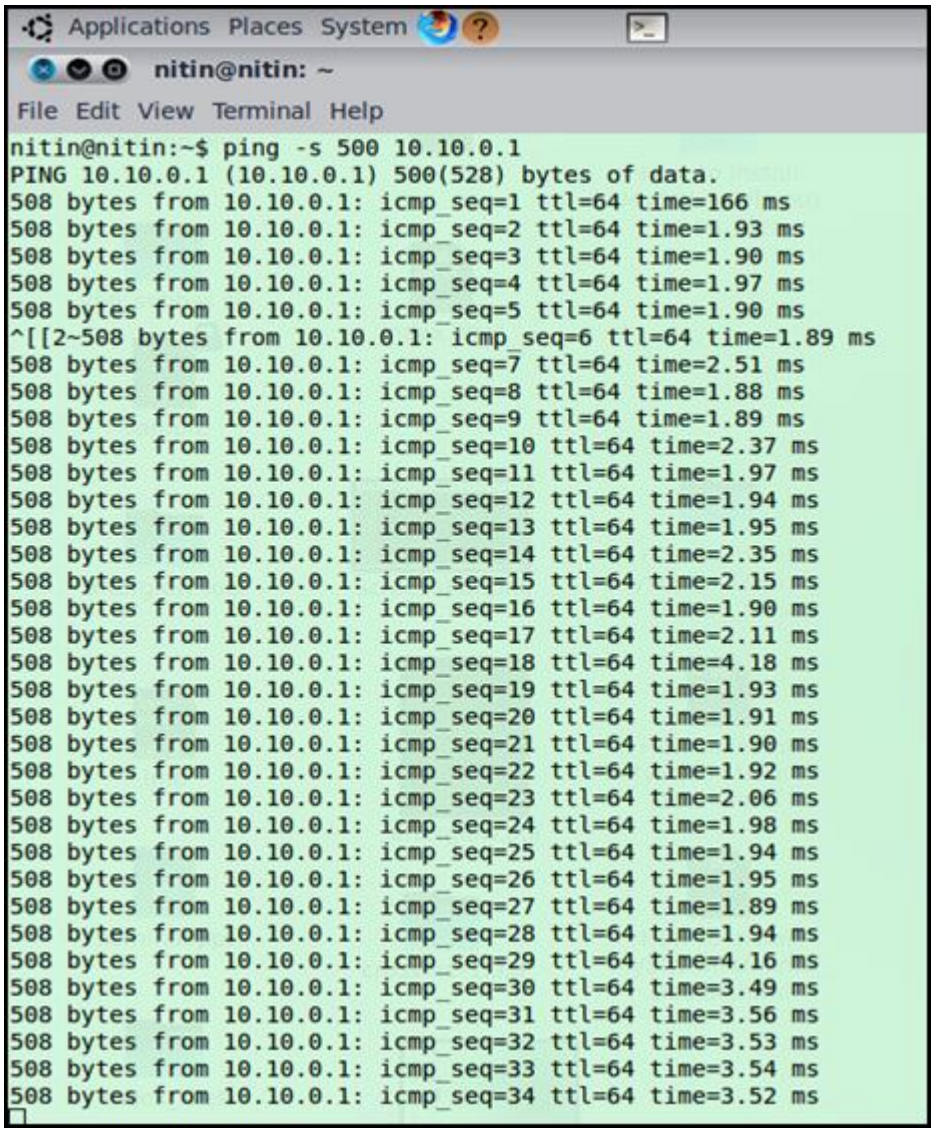


Figure 4.15 Latency measures while sending payload of 500 bytes to Software AP from MH

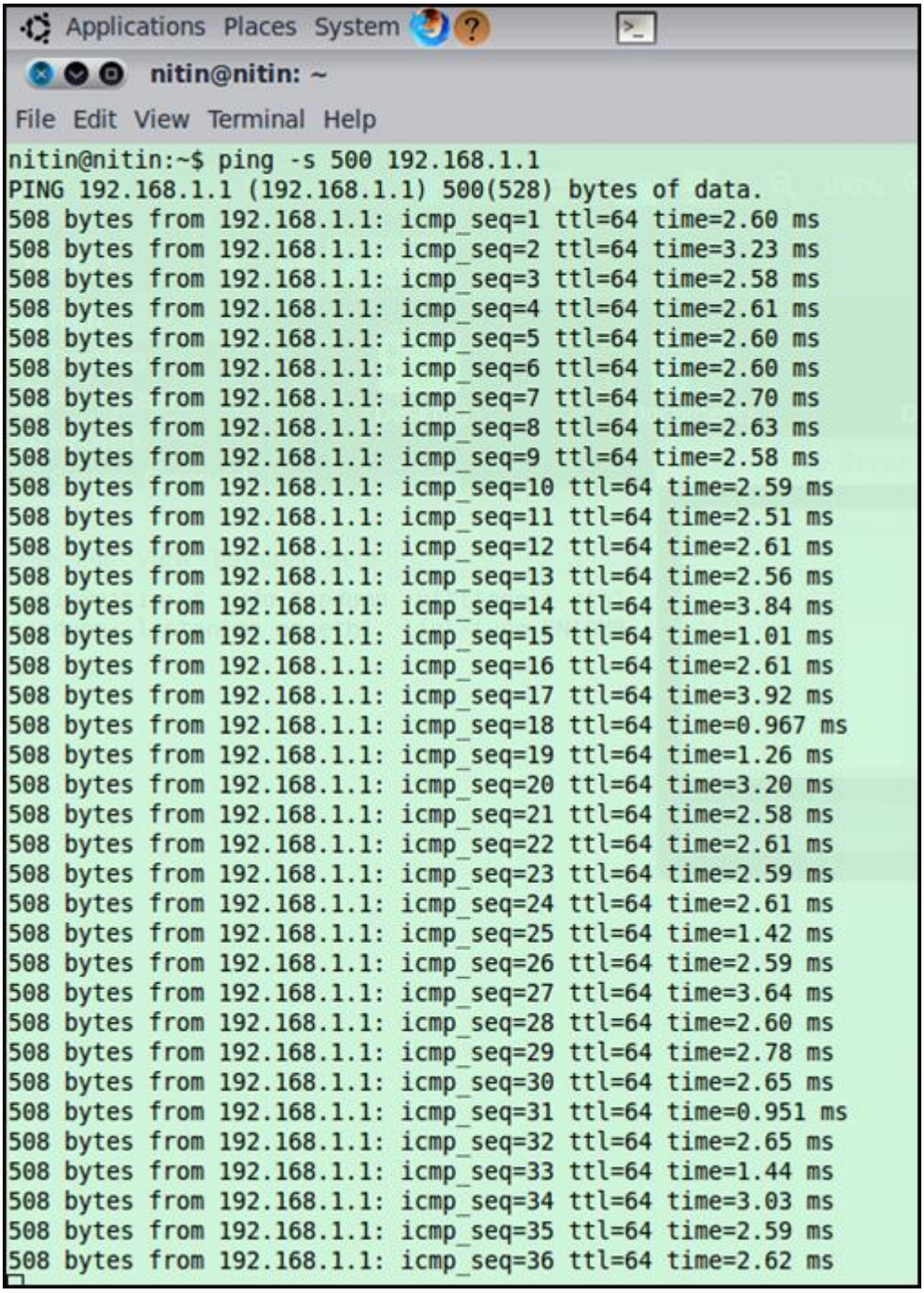


Figure 4.16 Latency measures while sending payload of 500 to Hardware AP from MH

S.No	RTT Time taken for software AP	RTT Time taken for Hardware AP
1	166	2.6
2	1.93	3.23
3	1.9	2.58
4	1.97	2.61
5	1.9	2.6
6	1.89	2.6
7	2.51	2.7
8	1.88	2.63
9	1.89	2.58
10	2.37	2.59
11	1.97	2.51
12	1.94	2.61
13	1.95	2.56
14	2.35	3.84
15	2.15	1.01
16	1.9	2.61
17	2.11	3.92
18	4.18	0.967
19	1.93	1.26
20	1.92	3.2
21	2.06	2.58
22	1.98	2.61
23	1.94	2.59
24	1.95	2.61
25	1.89	1.42
26	1.94	2.59
27	4.16	3.64
28	3.49	2.6
29	3.56	2.78
30	3.53	2.65
31	3.54	0.951
32	3.52	2.65

Table 2 Round Trip Time taken to send the payload of 500bytes by Software AP and Hardware AP

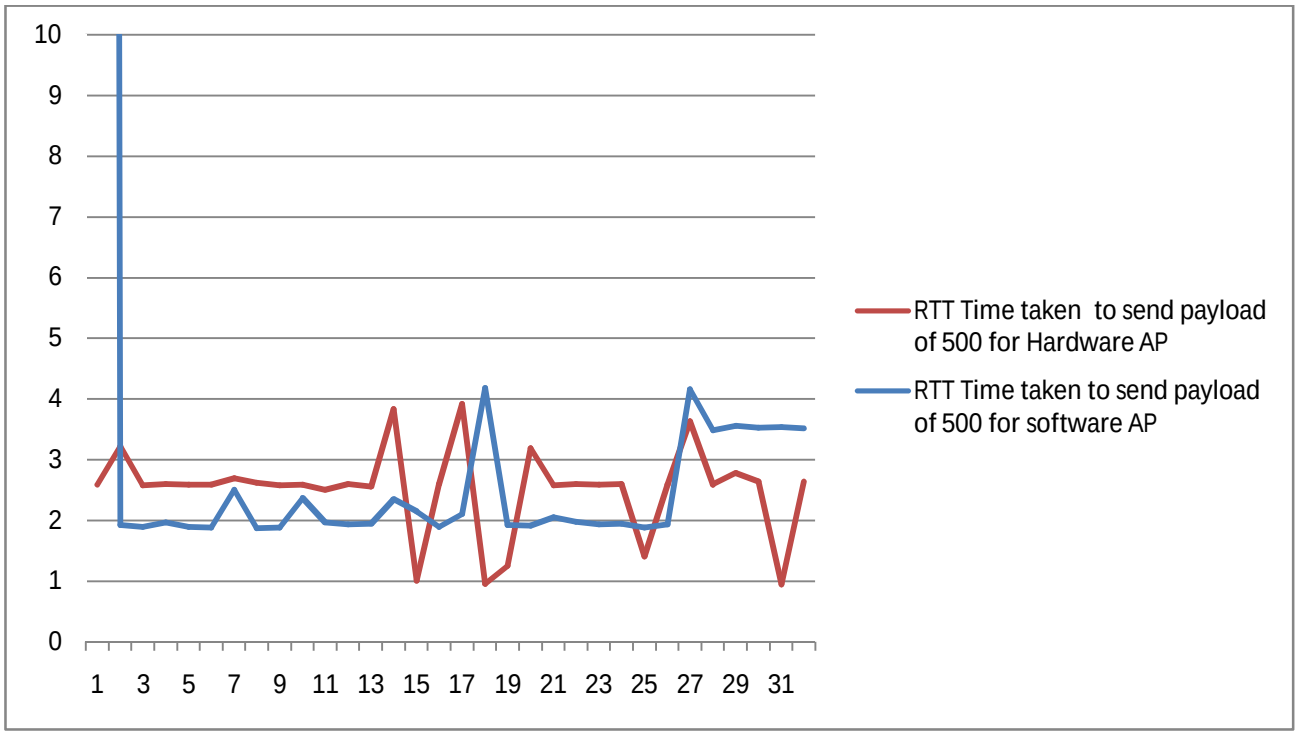


Figure 4.17 Graph showing Round Trip Time of 500 bytes payload send to Software Access Point and Hardware Access Point

Figure 4.17 shows the Round Trip Time to send a payload of 500 bytes from mobile host to the Software Access Point and Hardware Access Point.

It has been seen that at the starting of the Software Access Point, the first payload which has been sent by the Mobile Host to the Software Access Point took long time to send i.e166ms. after that it remains steady till 17th (i.e around 1.5ms - 2ms) reading (Table 2). In the 18th reading it took 4,18 ms(Table2) to send the payload of the 500 bytes from Mobile Host to Software Access Point. Once again from 21-26th (1.5ms – 2ms) reading very steady(Table 2). The 27th reading of Table-2 onwards the payload is sent with the latency of 3ms-4ms.

Whereas the Hardware Access point for the initial time it is bit steady till reading 13th of Table 2 then a big hick in the 14th (i.e 3.84ms)and then a sudden drop in the next reading (i.e 15th with the latency of 1.01ms), after that there is a big variations throughout as shown in the Figure 4.17 the latency varies very frequently from 1ms to 4ms. It can be

seen with this the Software Access Point is also give good performance this might be because the Software Access point is Built on the Laptop and the Laptop has its own additional computational power. When the Laptop processor is free or not performing any other task, then the Software Access point gives very good results as shown in the Figure 4.17.

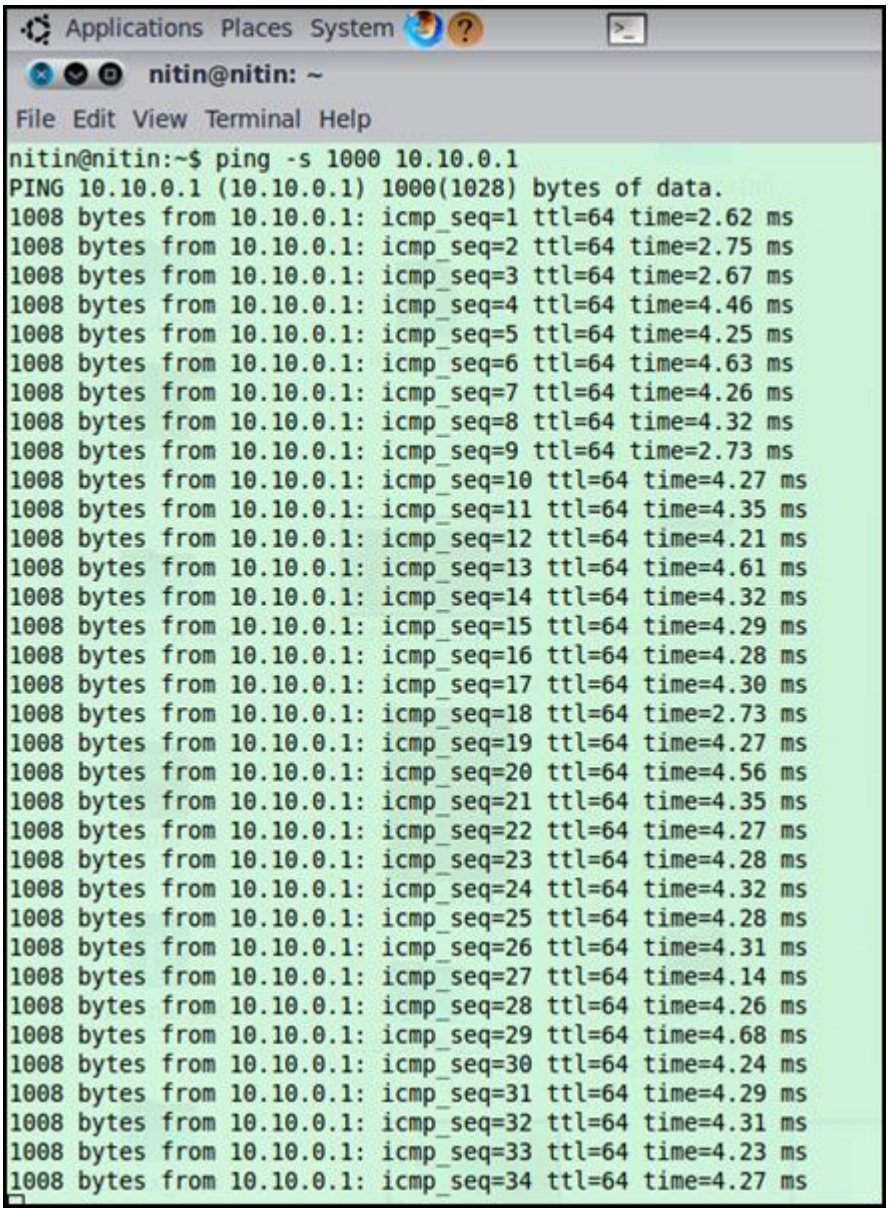


Figure 4.18 Latency measures while sending payload of 1000 to Software AP from MH

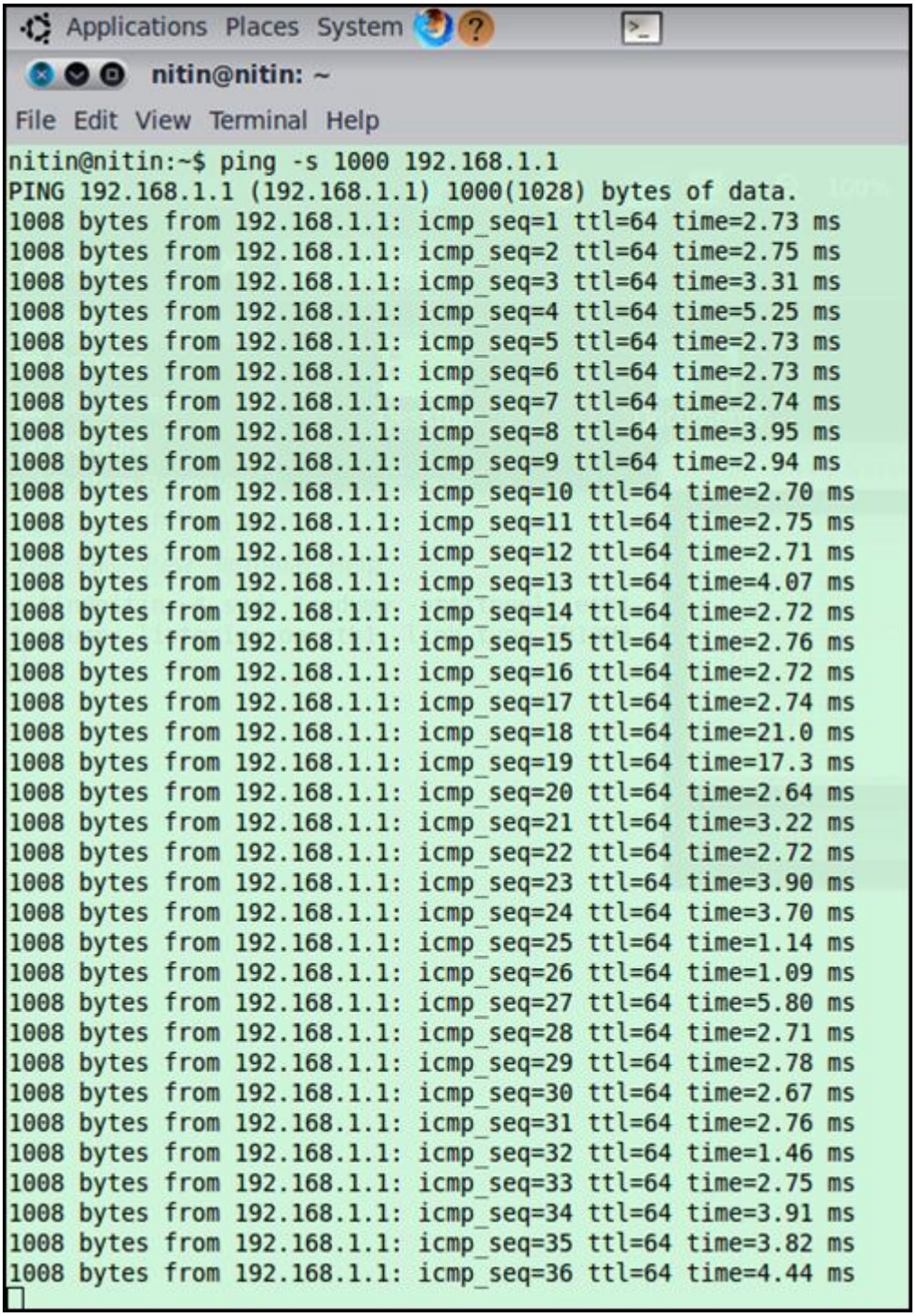


Figure 4.19 Latency measures while sending payload of 1000 to Hardware AP from MH

S.No	RTT Time taken for software AP	RTT Time taken for Hardware AP
1	2.62	2.73
2	2.75	2.75
3	2.67	3.31
4	4.46	5.25
5	4.25	2.73
6	4.63	2.73
7	4.26	2.74
8	4.32	3.94
9	2.73	2.94
10	4.27	2.7
11	4.35	2.75
12	4.21	2.71
13	4.61	4.07
14	4.32	2.72
15	4.29	2.74
16	4.28	21
17	4.3	17.3
18	2.73	2.64
19	4.27	3.22
20	4.56	2.72
21	4.35	3.9
22	4.27	3.7
23	4.28	1.14
24	4.32	1.09
25	4.28	5.8
26	4.31	2.71
27	4.14	2.78
28	4.26	2.67
29	4.68	2.76
30	4.29	1.46
31	4.31	2.75
32	4.23	3.91
33	4.27	4.44

Table 3 Round Trip Time taken to send the payload of 1000bytes by Software AP and Hardware AP

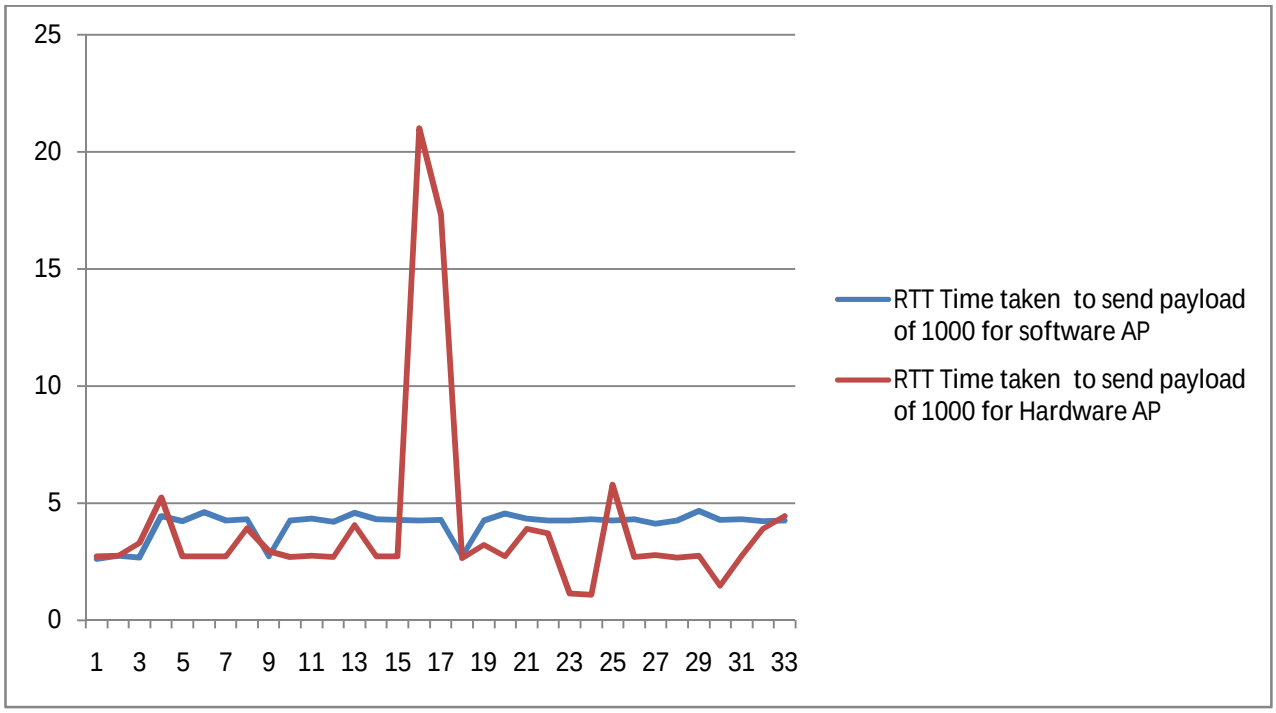


Figure 4.20 Graph showing Round Trip Time of 1000 bytes payload send to Software Access Point and Hardware Access Point

Figure 4.20 shows the Round Trip Time to send a payload of 1000 bytes from Mobile Host to the Software Access Point and Hardware Access Point.

It can be seen that the readings obtained by the Software Access Point is very steady Most of the readings are of the latency of 4 ms-4.5 ms as per the Table 3. As per Figure 4.20 to send the pay load of 1000 bytes from Mobile Host to the Software Access Point the latency is almost same throughout.

Whereas, when the same payload (i.e 1000 bytes) is send to the Hardware Access Point from the same Mobile Host the latency varies frequently as in Table 3. Latency obtained while sending the payload 16^{th} and 17^{th} it took 21ms and 17.3ms respectively, which is very high with respect to other readings which are between 1ms-6ms as per Table 3.

Hence, it can be seen that even the payload size increases the software AP give the same performance as previously shown.

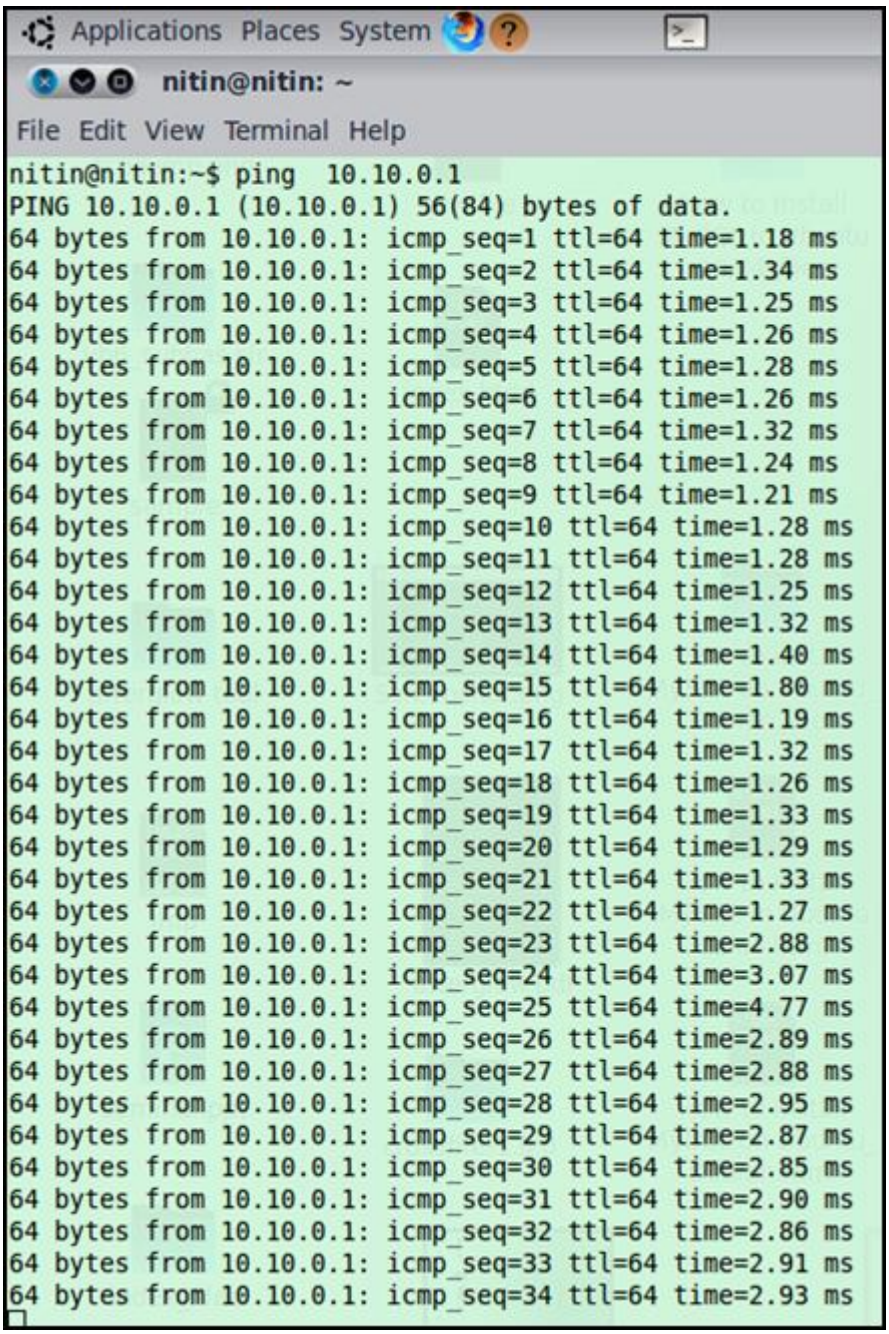


Figure 4.21 Latency measures while sending payload of 64 bytes to Software AP from MH

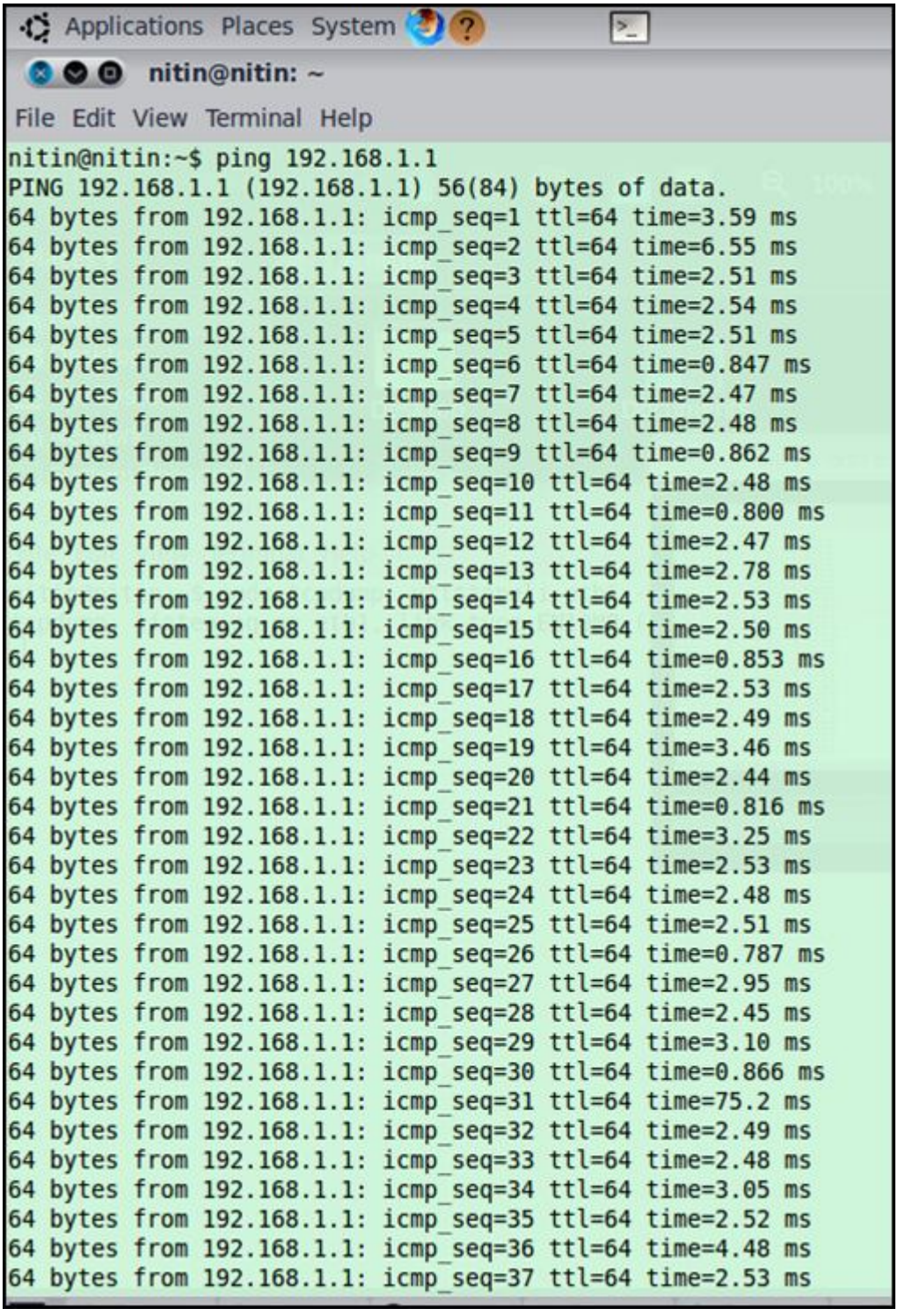


Figure 4.22 Latency measures while sending payload of 64 bytes to Hardware AP from MH

S.No	RTT Time taken for software AP	RTT Time taken for Hardware AP
1	1.18	3.59
2	1.34	6.55
3	1.25	2.51
4	1.26	2.54
5	1.28	2.51
6	1.26	0.847
7	1.32	2.47
8	1.24	2.48
9	1.21	0.862
10	1.28	2.48
11	1.28	0.8
12	1.25	2.47
13	1.32	2.78
14	1.4	2.53
15	1.8	2.5
16	1.19	0.853
17	1.32	2.53
18	1.26	2.49
19	1.33	3.46
20	1.29	2.44
21	1.33	0.816
22	1.27	3.25
23	2.88	2.53
24	3.07	2.48
25	4.77	2.51
26	2.89	0.787
27	2.88	2.95
28	2.95	2.45
29	2.87	3.1
30	2.85	0.866
31	2.9	75.2
32	2.86	2.49
33	2.93	3.05

Table 4 Round Trip Time taken to send the payload of 64bytes by Software AP and Hardware AP

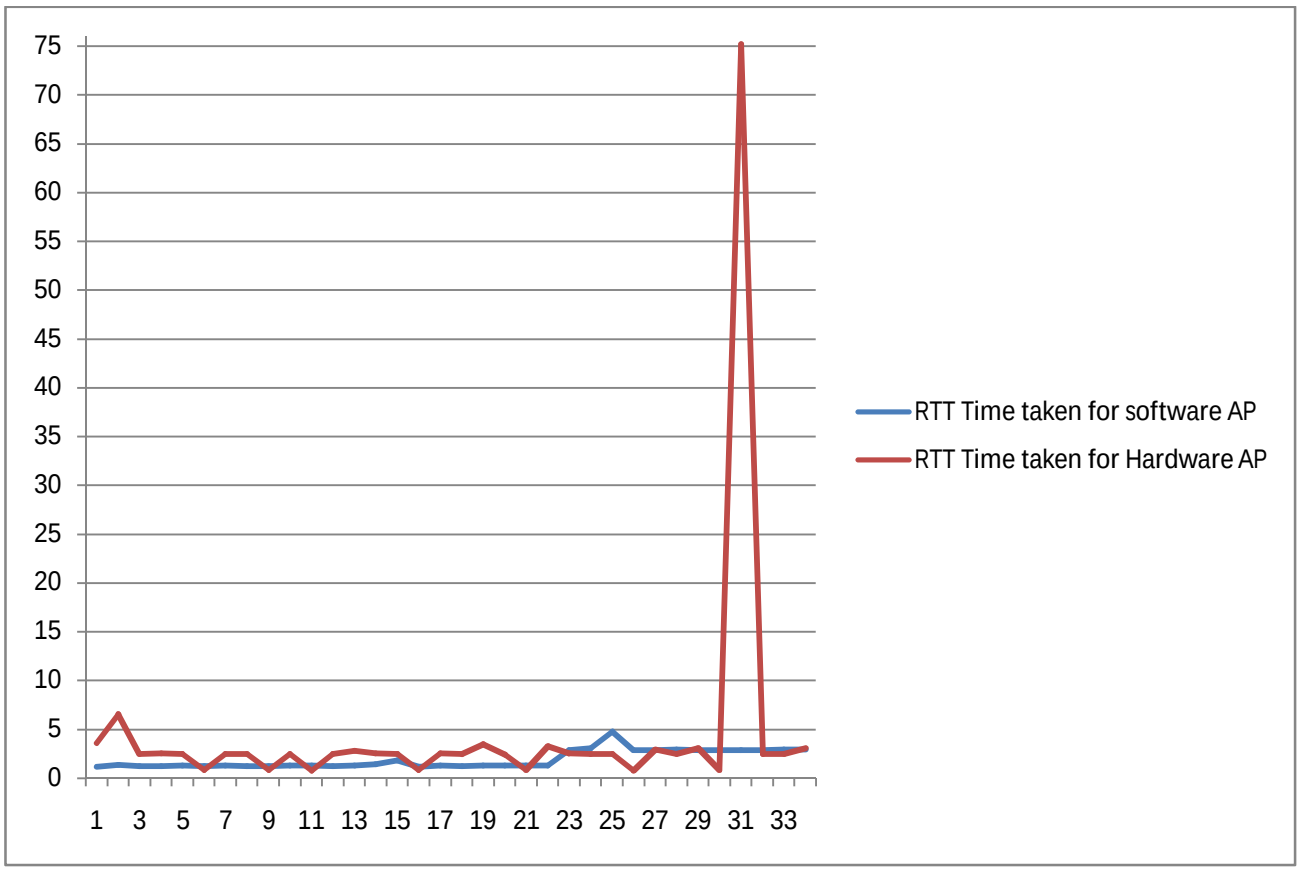


Figure 4.23 Graph showing Round Trip Time of 64 bytes payload send to Software Access Point and Hardware Access Point

Figure 4.23 shows the Round Trip Time to send a payload of 64 bytes from Mobile Host to the Software Access Point and Hardware Access Point.

Here the Figure 4.23 show the Software Access Point is very steady and in the starting of Software Access Point, when the Mobile Host sent a payload of 64 bytes to the Software Access Point the latency found is 1ms-1.8ms from reading 1st to 22st as per Table 4. And in the last ten readings the latency found to send the payload of 64 bytes is 2ms-3ms as per Table 4.

Whereas in Hardware Access point the latency keeps on changing sometimes it is more or sometimes it is very less like the minimum latency found in the reading 26 is 0.787 as per Table 4 and the maximum latency captured in reading 31st is 75.2ms as per Table 4

Hence, by this all results it has been proved that the Software Access Point can also give the good performance with respect to Hardware Access point.

iv. Latency Performance measurements between Hardware and Software access points (Reading timing 5.30 pm).

S.No	RTT Time taken to send payload of 64 for software AP	RTT Time taken to send payload of 64 for Hardware AP
1	5.12	3.33
2	6.03	4.74
3	3.79	10.3
4	3.23	2.44
5	4.8	2.47
6	5.92	2.49
7	4.04	2.48
8	6.09	2.55
9	1.48	2.5
10	4.79	4.29
11	5.59	3.88
12	1.14	3.37
13	157	2.53
14	5.6	2.85
15	4.58	3.71
16	4.3	4.59
17	4.57	4.01
18	1.15	2.59
19	5.29	2.93
20	1.16	6.81
21	4.59	4.99
22	4.04	2.48
23	4.55	3.07

24	5.87	7.21
25	1.45	3.73
26	3.87	1.41
27	1.14	2.64
28	6.09	6.52
29	5.2	2.56
30	1.2	10.3
31	4.45	6.59
32	4.68	2.52
33	3.86	3.68
34	4.08	21.1
35	3.64	13.5
36	4.67	2.52
37	5.74	2.59

Table 5 Round Trip Time taken to send the payload of 64bytes by Software AP and Hardware AP

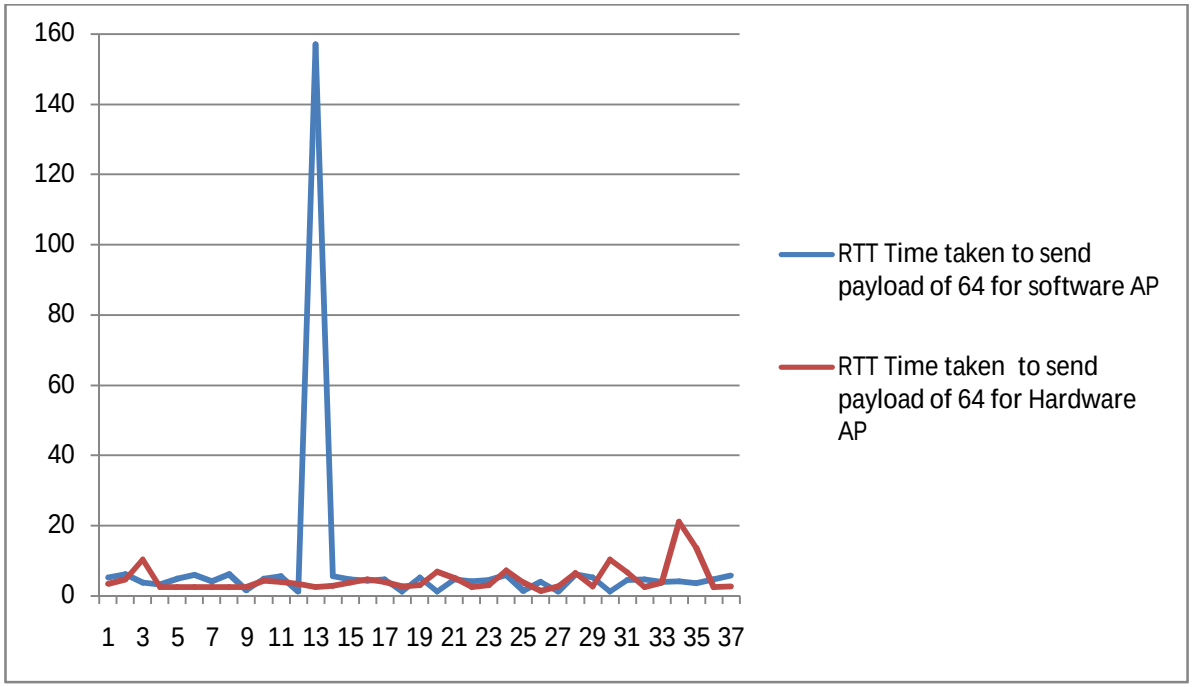


Figure 4.24 Graph showing Round Trip Time of 64 bytes payload send to Software Access Point and Hardware Access Point

At this particular time the reading of Table 5 shows that, except the reading 13th ,of Software Access point and the reading 34th of Hardware Access Point which took the latency of 157ms and 21.1ms respectively, the both Software Access Point and Hardware Access Point Round Trip time is almost same.

S.No	RTT Time taken to send payload of 500 for software AP	RTT Time taken to send payload of 500 for Hardware AP
1	9.28	2.68
2	10.5	2.85
3	10.7	2.5
4	9.53	3.52
5	10.5	2.79
6	11	2.69
7	11.2	5.36
8	10	20.5
9	12.6	3.35
10	10.2	2.6
11	11.2	6.99
12	11.1	4.38
13	10.1	2.65
14	11	3.64
15	10.8	2.63
16	9.46	3.68
17	10.7	2.68
18	10.7	5.79
19	9.82	4.43
20	9.04	1.42
21	11.4	1.95
22	10.3	2.65
23	10.2	2.66
24	10.5	2.63
25	9.84	2.67
26	10.4	10.8

27	11.1	2.69
28	11.7	2.83
29	9.23	2.88
30	10.9	5.73
31	3.82	2.64
32	10.8	2.6
33	19.8	2.94
34	55.6	3.12
35	9.23	4.23
36	9.57	5.09
37	12	2.64

Table 6 Round Trip Time taken to send the payload of 500 bytes by Software AP and Hardware AP

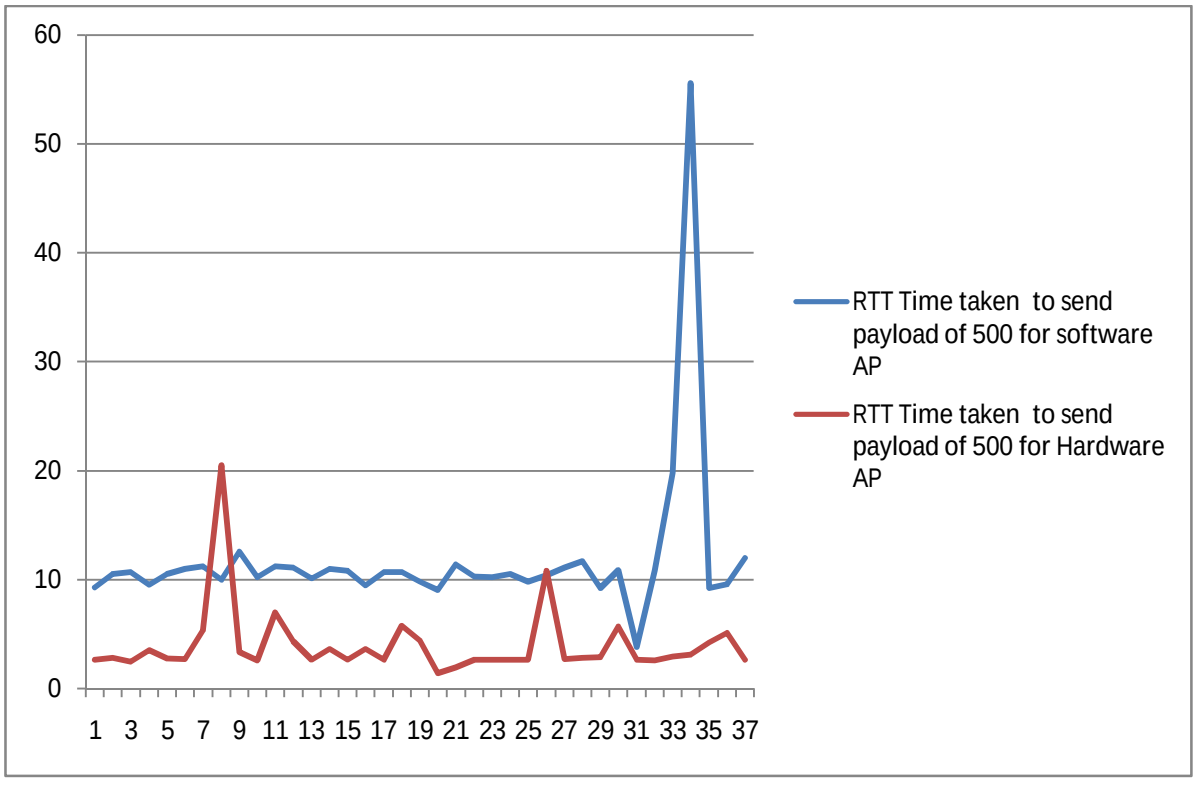


Figure 4.25 Graph showing Round Trip Time of 500 bytes payload send to Software Access Point and Hardware Access Point

Figure 5.22 shows that, to send the 500 bytes of payload at this particular time the the latency of Hardware Access Point and the Software Access Point is very different. As per the Figure 5.22 the latency of Software Access Point is more than Hardware Access Point this may be because of the usage of the other application by the Laptop while this reading was taken (the telnet is used here shown in Figure 5.26). Hence, it has been seen that, when the other tasks were performed by the process, the latency of Software access Point increases.

S.No	RTT Time taken to send payload of 1000 for software AP	RTT Time taken to send payload of 1000 for Hardware AP
1	16.2	2.8
2	15.2	3.17
3	16.3	2.78
4	14.2	2.79
5	14.9	2.73
6	19.4	4.33
7	16.2	2.79
8	16.1	2.76
9	16.7	2.73
10	14.6	2.78
11	15.7	5.95
12	16	5.82
13	14.3	2.75
14	15.9	13.6
15	13.7	3.42
16	15.2	2.74
17	5.62	28.9
18	14.5	40.8
19	15.9	4.85
20	15	2.68
21	14.5	4.78
22	16	4.19
23	16	1.33

24	16.1	2.69
25	15.8	3.09
26	14.3	4.02
27	14.7	2.71
28	15.7	6.77
29	14.9	6.24
30	15.2	2.7
31	14.6	5.06
32	14.7	3.13
33	14.6	4.03
34	15.6	7.15
35	14.3	2.86
36	15	2.74
37	4.09	3.76

Table 7 Round Trip Time taken to send the payload of 1000 bytes by Software AP and Hardware AP

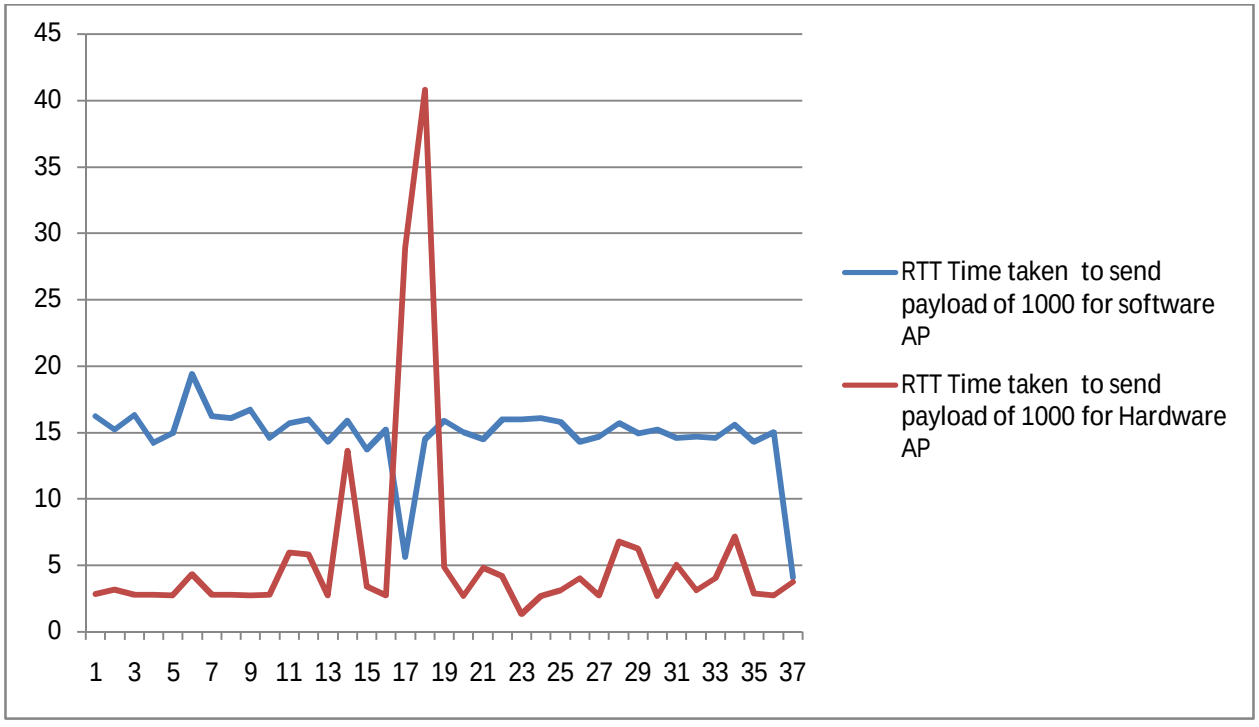


Figure 4.26 Graph showing Round Trip Time of 1000 bytes payload send to Software Access Point and Hardware Access Point

S.No	RTT Time taken to send payload of 1500 for software AP	RTT Time taken to send payload of 1500 for Hardware AP
1	18.5	8.79
2	18	10.4
3	19	4.43
4	18.4	11.8
5	19	4.83
6	18.1	3.85
7	18.7	4.18
8	23.5	5.49
9	26	4.44
10	21.2	9.58
11	22.9	9.91
12	24	9.16
13	24.8	6.28
14	21.1	3.79
15	23	3.45
16	23.5	11.6
17	21.7	17.6
18	21	3.72
19	23.9	3.06
20	20.1	6.14
21	20.3	12.6
22	21.3	2.26
23	19.9	9.27
24	21.7	16
25	23.7	10.9
26	20.6	4.31
27	22.6	19.7
28	23.2	4.23
29	23.2	9.21
30	22.4	8.82
31	20.3	6

32	24.5	3.43
33	22.7	2.42
34	20.6	5.84
35	17.2	10.09
36	23.7	4.91
37	19.7	7.51

Table 8 Round Trip Time taken to send the payload of 1500 bytes by Software AP and Hardware AP

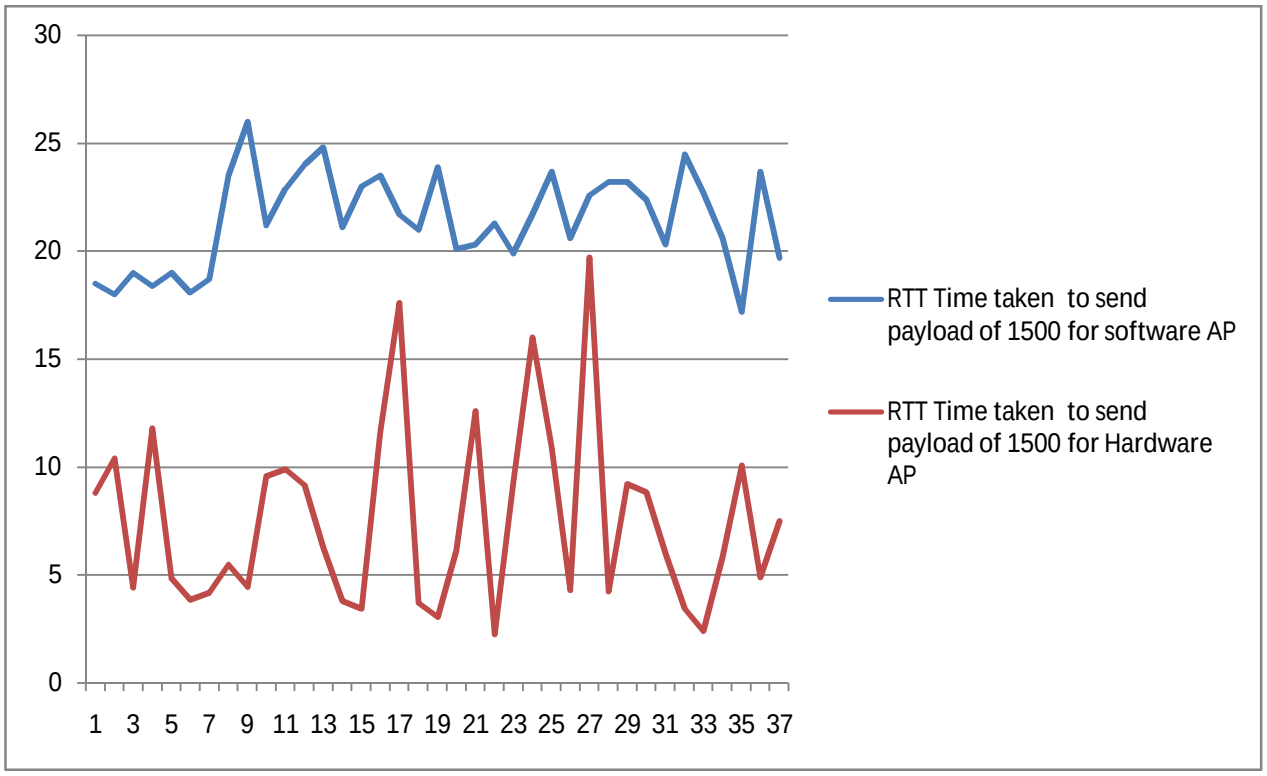


Figure 4.27 Graph showing Round Trip Time of 1500 bytes payload send to Software Access Point and Hardware Access Point

Figure 4.25, Figure 4.26, Figure 4.27 Shown, as the payload increases the Latency of the Software Access point and the Hardware Access Point also increases respectively.

Figure 4.25,4.26,4.27 the latency of Software Access Point is more than Hardware Access Point this may be because of the usage of the other application by the Laptop while this reading was taken (the telnet is used here shown in Figure 4.28). Hence, it has been seen that, when the other tasks were performed by the process, the latency of Software Access Point increases.

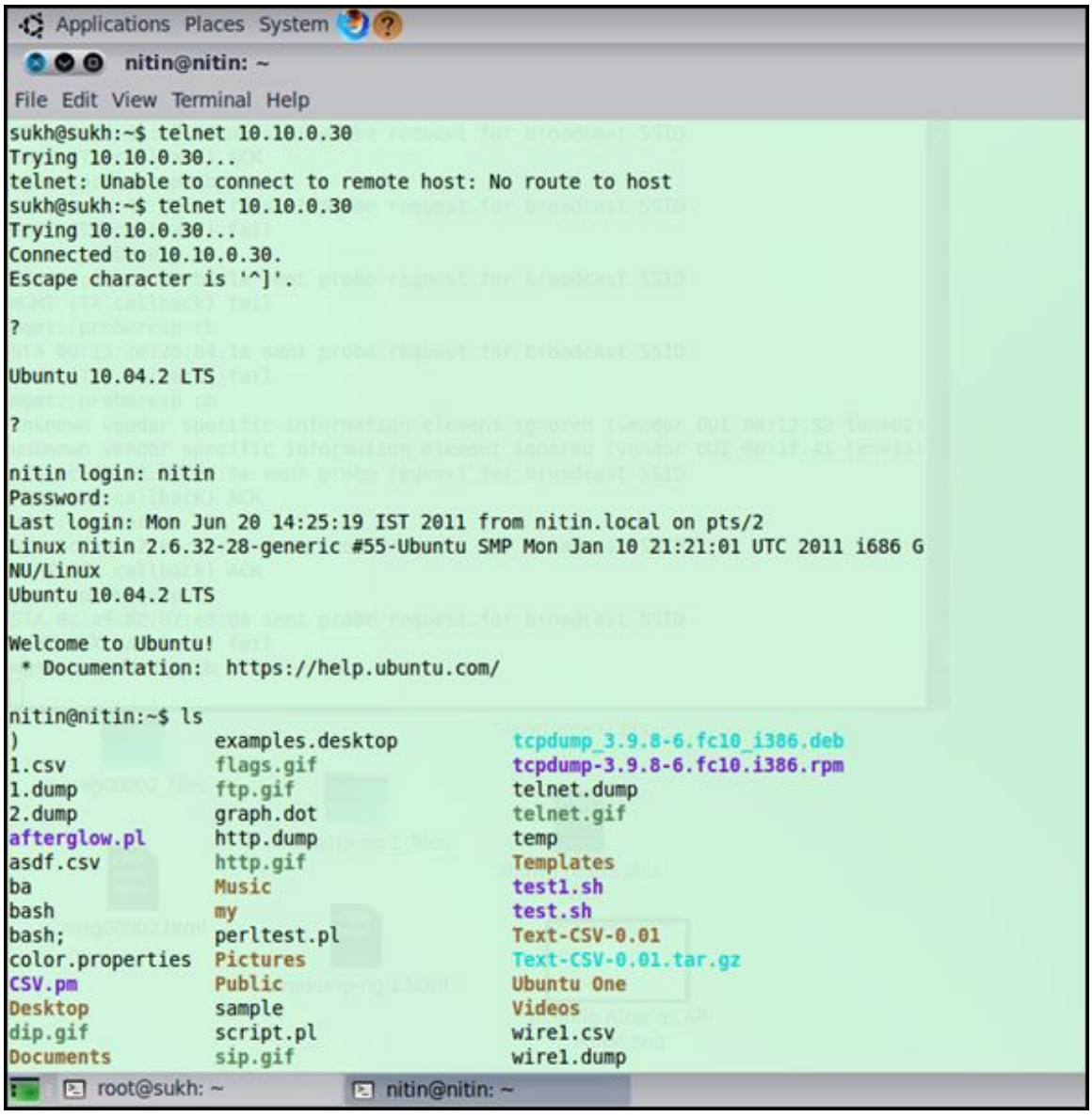


Figure 4.28 Telnet to the Mobile Host from Software Access Point

Figure 4.28 shows that the other application like Telnet, FTP etc. can also be done with good performance using Software Access Point. Here, (Figure 4.28 Telnet is shown) the Software Access Point connects the Mobile Host i.e. 10.10.0.30 and successfully connected and the files of Mobile Host is displayed in the Software Access Point Desktop.

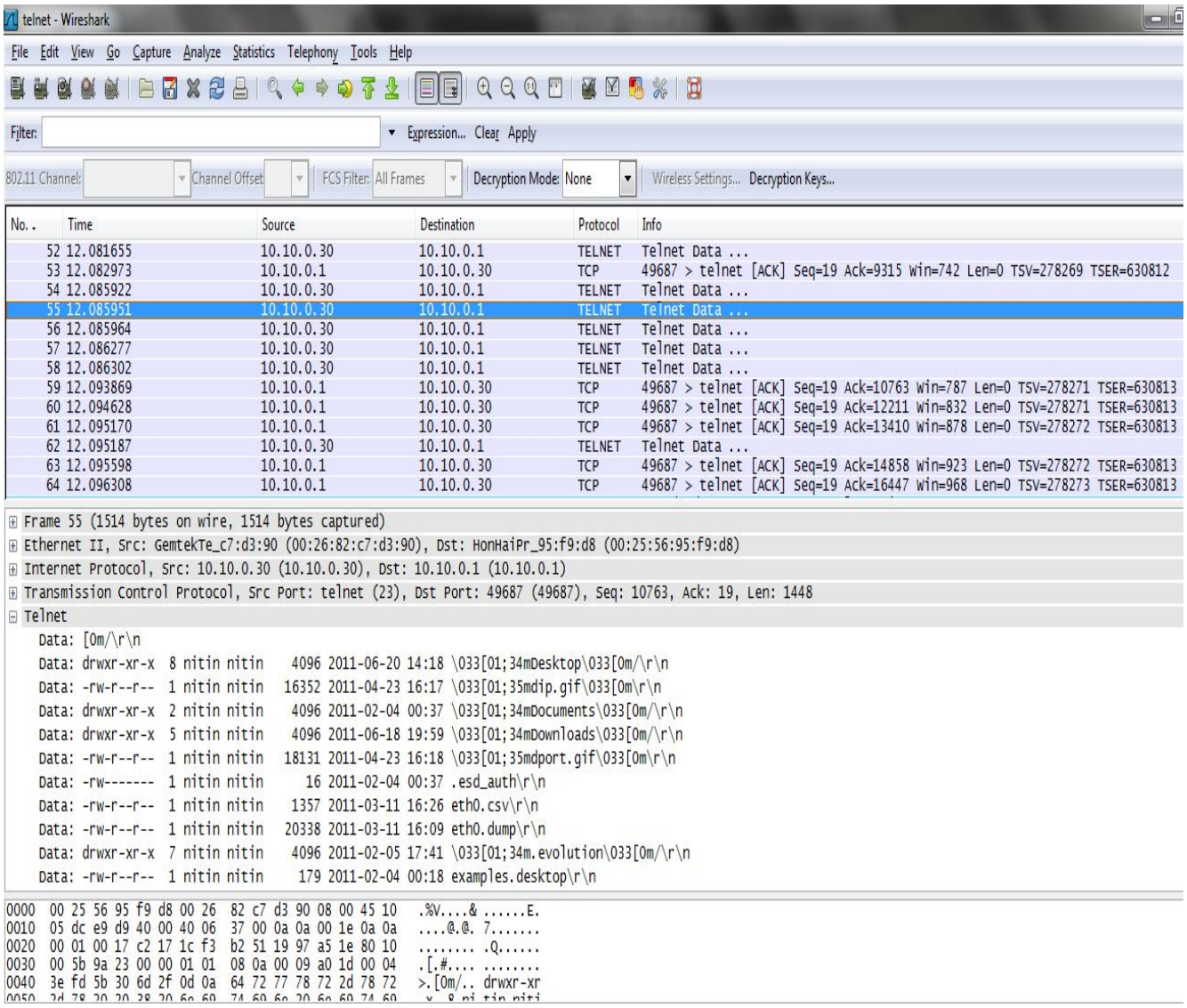


Figure 4.29 Wireshark showing the Telnet to the Mobile Host from Software Access Point

Figure 4.29 shown the data of the telnet to the Mobile Host (10.10.0.30) from the Software Access point (10.10.0.1). Here the Telnet data shows the ls command is executed by the Software Access Point to the Mobile Host.

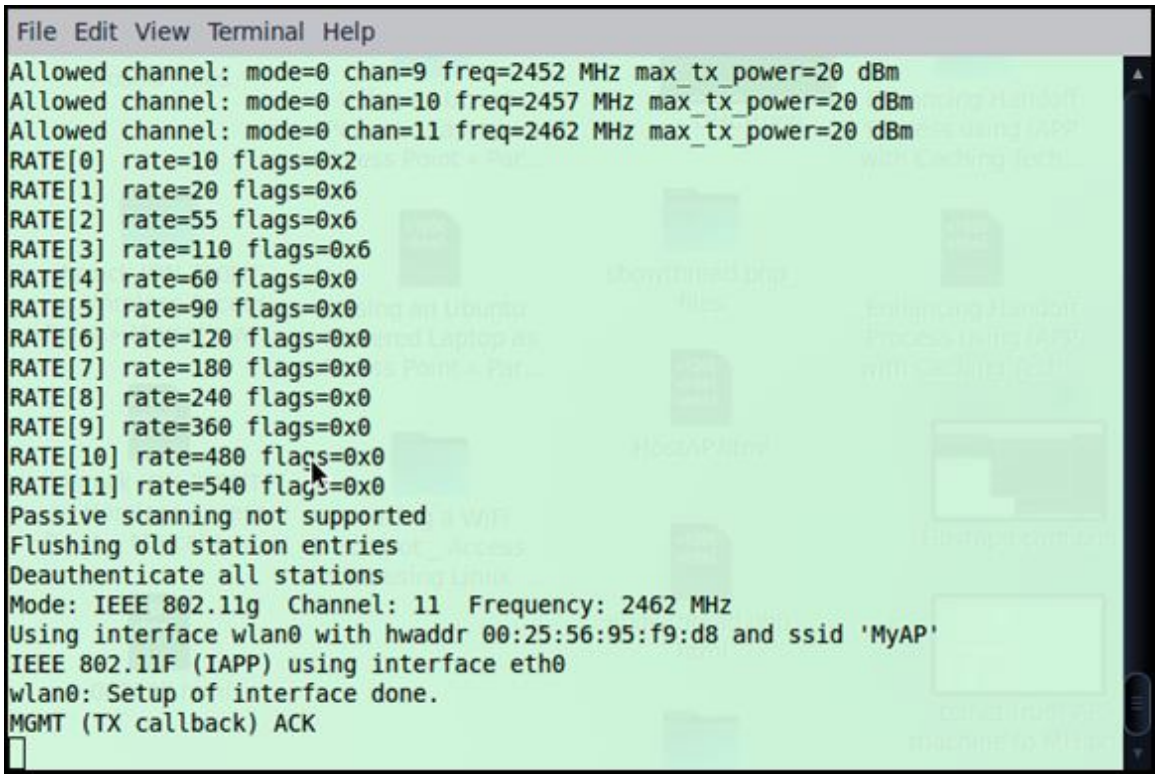


Figure 4.30 IEEE 802.11F (IAPP) interface is shown

In the hostapd.conf file iapp_Interface parameter is set. This helps the Software Access Point to run an Inter Access Point Protocol as shown in Figure 4.30. Here the IAPP interface is ready to broadcast beacon signal for the Mobile Hosts.

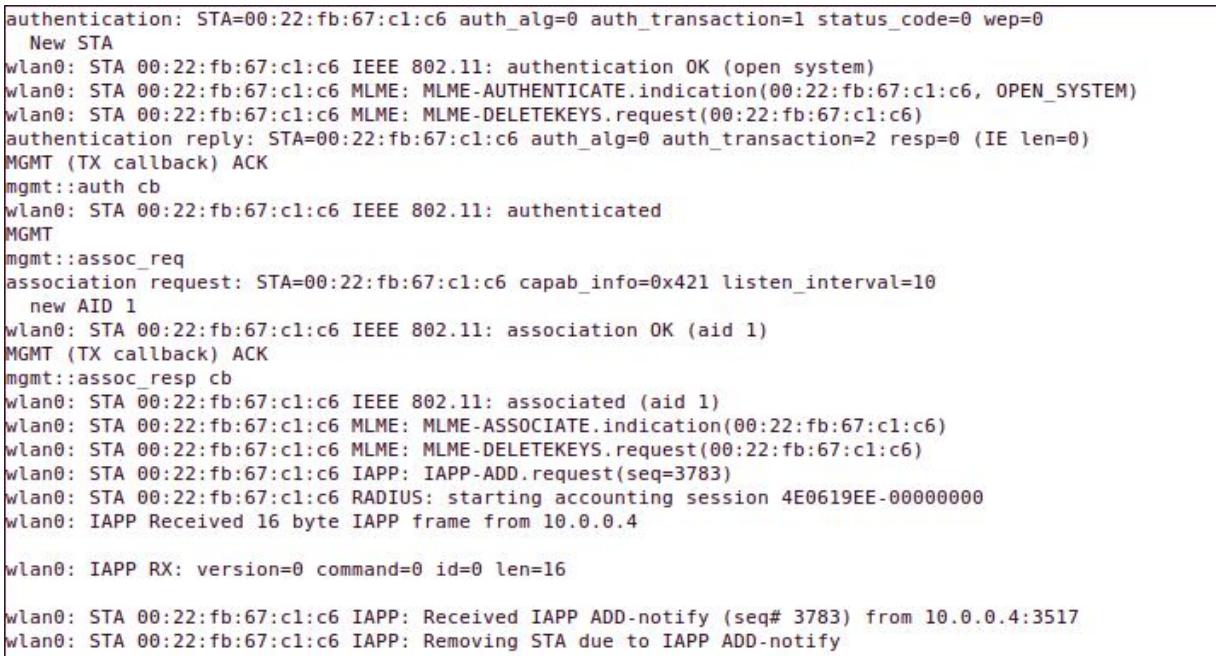


Figure 4.31 IAPP messaging between Software Access Point and Mobile Host.

Figure 4.31 shows the messaging between Software AP and Mobile Hosts. Once the probe request is received by the Software AP it recognize the Mobile Host as a new station and authenticates it after this as association request is accepted. When the Mobile Host starts roaming between different Software AP configured with IAPP. The IAPP.ADD request is sent by the station; once the IAPP received this frame the AP send ADD-notify as shown in Figure 4.31, which ensures that the system is associated or not. To make the IAPP functional the Linux kernel multicast config parameter must be enabled.

CHAPTER 5

CONCLUSION

5.1 Conclusion

A software access point is easily configurable to support any number of devices with Wi-Fi capability. It can be concluded that software access points can easily replace hardware access points where the coverage area of wireless network is not required to be large. Also, when the number of devices connected to the network is not large then a software access point can be easily used as the hardware on which the computer system runs software AP is not designed to handle simultaneously large amount of concurrent communication. Software access point give freedom of customization to change the specifications as per the user requirements, it can be changed into devices with enhanced functionality like Network Address Translation (NAT) , IPtables for better routing providing more facilities to the user. It cannot be used in critical infrastructure or commercial environment, though it is very useful to transfer data among devices that support full Wi-Fi data transfer rates. Also software access points provide real time data stream of information about connected devices so any unauthorized devices information can directly be logged. We may finally conclude that though software AP may not be a replacement for hardware AP but it is a viable solution with enhanced functionality that is either not present or is very expensive to purchase as part of hardware AP.

5.2 Future scope

- Software Access point can be configure as IEEE802.11f (Inter-Access Point Protocol). To implement IAPP protocol and allow the mobile hosts to roam across Linux hosted AP's and to ensure the seamless data transmission and smooth handoff. Till date no such research paper is seen on the IAPP Implementation on

Software Access Point, Further it can also be implemented in the Hardware Access point.

- Smarter algorithms for congestion control of communication between connected devices.

- The functionalities of various network devices and protocols can be embedded into a single computer system based software access point, giving massive savings in terms of hardware cost and maintenance.

REFERENCES

[1] Chun-Ting Chou and Shin, K.G, ”An enhanced inter-access point protocol for uniform intra and intersubnet handoffs,”Mobile Computing, IEEE Transactions, Volume 4, Issue 4, July-Aug. 2005, pps. 321-334.

[2] A. Mishra, M.H. Shin and W. A. Arbaugh, “Context Caching using Neighbour Graphs for Fast Handoffs in a Wireless Network,” in Proc of IEEE INFOCOM, Hong Kong, Mar. 2004.

[3] A. Mishra, A Shin, and W. Arbaugh, “An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process,” ACM SIGCOMM Computer Comm. Rev., vol. 33, no. 2, Apr. 2003.

[4] C. Rigney et al., “Remote Authentication Dial In User Service (RADIUS),” RFC 2058, Jan. 1997.

[5] IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, IEEE Std 802.11f, Jul. 2003.

[6] Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE 802.11, 1999.

[7] PING-Jung Huang, Yu-Chee Tseng, Kun-Cheng Tsai, “A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks,” 2006 IEEE.

[8] David J.Y.Lee and William C.Y .Lee, “ Mobile IP$^{2”}$ 2001 IEEE

[9] Ronald D. Ryan, “Romain Between Hetrogeneous 3rd Generation Wireless Networks,” 1999 IEEE

[10] Behcet Sarikaya and timucin Ozugur, " Traking Agent Based Paging for Wireless LANs," 2004 IEEE

[11] ORiNOCO Techinical Bulletin 021/A, "…roaming with ORiNOCO/IEEE 802.11," December 1998,1999,2000,2001 Agere System

[12] Lei Zan, Jidong Wang and Lichun Bao, " Personal AP Protocol for Mobility Management in IEEE 802.11 Systems," 2005 IEEE

[13] Sourav Pal, Sumantra Kundu, Preetam Ghosh, Kalyan Basu,and SajalDas, " A Framework for Fast Handoff in IEEE 802.11 Based Systems,"

[14] Ian Herwono,Joachim Sachs, R Alf Keller, " Performance Improvement of Media Point Network using the Inter Access Point Protocol according to IEEE 802.11f," IEEE 2004

[15] Cheng-Shong Wu, Ming-Ta Yang, Koa-shing Hwang, " Fast-handoff Schemes for inter-subnet Handoff in IEEE 802.11 WLANs for SIP/RTP Applications" IWCMC'07

[16] M.S. Bargh, R.J. Hulsebosch, E.H. Eertink, A.Prasad, H. Wang, P. Schoo, " Fast Authentication Methods for Handovers between IEEE 802.11 Wireless LANs", WMASH'04

[17] SeongSoo PARK,"Implementation of Seamless Roaming Service in Hybrid Network",IEEE 2004

[18] Li Jun ZHANG, Samuel PIERRE & Laurent MARCHAND,"Anew Seamless Method to Support CDMA2000/WLAN Vertical Handover", IEEE CCECE/CCGEL, 2006

[19] Kumudu S. Munasinghe and Abbas Jamalipour,"Analysis of signal cost for a Roaming user in a Heterogenous Mobile Data Network", IEEE 2008

[20] Ian Herwono et al,"Performance Improvement of Media Point Network using the Inter Access Point Protocol according to IEEE 802.11f",

[21] Sangho Shin, Anshuman Singh Rawat & Henning Schulzrinne,"Reducing MAC layer Handoff latency in IEEE 802.11 Wireless LANs, MobiWac'04

[22] http://oob.freeshell.org/nzwireless/fdl.txt , "GNU Free Documentation License Version 1.2, November 2002"

[23] H. Labiod, H.Afifi, C. DE Santis," Wi-Fi™, Bluethooth™, ZigBee™ and WiMax™", Springer

[24] Typical Wireless Network:
URL:http://www.howstuffworks.com/wireless-network.htm accessed on 14-06-2011
[25] Wireless network Access point :
URL:http://ec1.images-amazon.com/media/i3d/01/ …/MANUAL000000673.pdf accessed on 14-06-2011

[26] Architecture of an IEEE 802.11 Wireless LAN :
URL:http://www.davidrust.com/Wiki/doku.php?id=tommy_s_part_of_the_survey accessed on 14-06-2011

[27] WLAN Ad-hoc Mode :
URL:http://www.eusso.com/Models/Wireless/UGL2430-U2HA/Diagram_Ad-Hoc.jpg accessed on 14-06-2011
[28] WLAN Infrastructure Mode:
URL:http://www.virtual-hideout.net/reviews/
belkin_wireless_80211b_adapter/infrastructure.png accessed on 14-06-2011
[29] Wireless Hotspot :
URL: http://ecx.images-amazon.com/images/I/41Po%252B8bbXtL.jpg accessed on 14-06-2011

[30] Creating a simple wireless Network
URL:http://computer.howstuffworks.com/wireless-network3.htm accessed on 20-06-2011

[31] Wi-Fi Hotspot
URL:http://computer.howstuffworks.com/wireless-network2.htm accessed on 20-06-2011

[32] http://computer.howstuffworks.com/wireless-network1.htm

[33] A.Gueroui and S.Boumerdassi ," A Handover Optimisation Scheme in Cellular Networks", IEEE 2009

[34] Masugi Inoue, Khaled Mahmud, Homare Murakami, Mikio Hasegawa, and Hiroyuki Morikawa." Design and Implementation of Out-of-Band Signaling for Seamless Handover in Wireless Overlay Networks", IEEE Communications Society pp3932-3936 0-7803-8533-0/04/$20.00 (c) 2004 IEEE

[35] Alex Yiu-Man Chan and Wen-Pai Lu," Architecture for Wireless Access in Vehicles", 0-7803-7954-3/03/$17.00 ©2003 IEEE. pp3336-3340.

[36] N. Olaziregi, A.H. Aghvami," A Novel Approach for Rec:onFigureurable Systems at RAN Level", 0-7803-7661-7~03~$17.0002003 IEEE pp1120-1125.

[37] Ronald Beaubrun, Samuel Pierre, Paola Flocchini & Jean Conan," Global Roaming Management in the Next-Generation Wireless Systems", 0-7803-7400-2/02/$17.00 © 2002 IEEE pp2070-2074.

[38] Murad Abusubaih, James Gross, and Adam Wolisz." An Inter-Access Point Coordination Protocol for Dynamic Channel Selection in IEEE802.11 Wireless LANs", 1st IEEE Workshop on Autonomic Communications and Network Management (ACNM'07), Munich, Germany, May 2007 pp17-24.

[39] Farouk. Belghoul, Yan. Moret, Christian. Bonnet," IP-based Soft Handover in All-IP wireless networks", Institute Eurécom 2229 Route des Crêtes, BP 193 F-06904 Sophia Antipolis Cédex, France Research report N° RR-02-071.

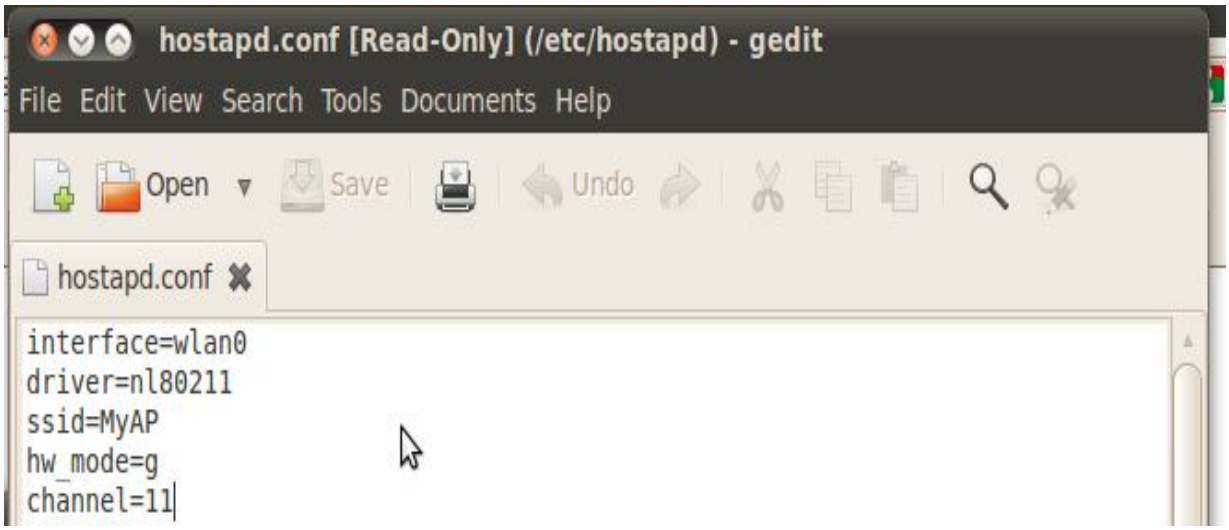
[40] Eric Y. Chen and Mistutaka Itoh," Virtual Smartphone over IP", A paper accessed from URL: http://android-x86.googlecode.com/files/Wowmom-CR2.pdf on 22-06-201

[41] Jungwook Choi $ Hyukjoon Lee,"Supporting Handover in an IEEE 802.11p-based Wireless Access system", IEEE 2005 pp75-80.

Annexure - I

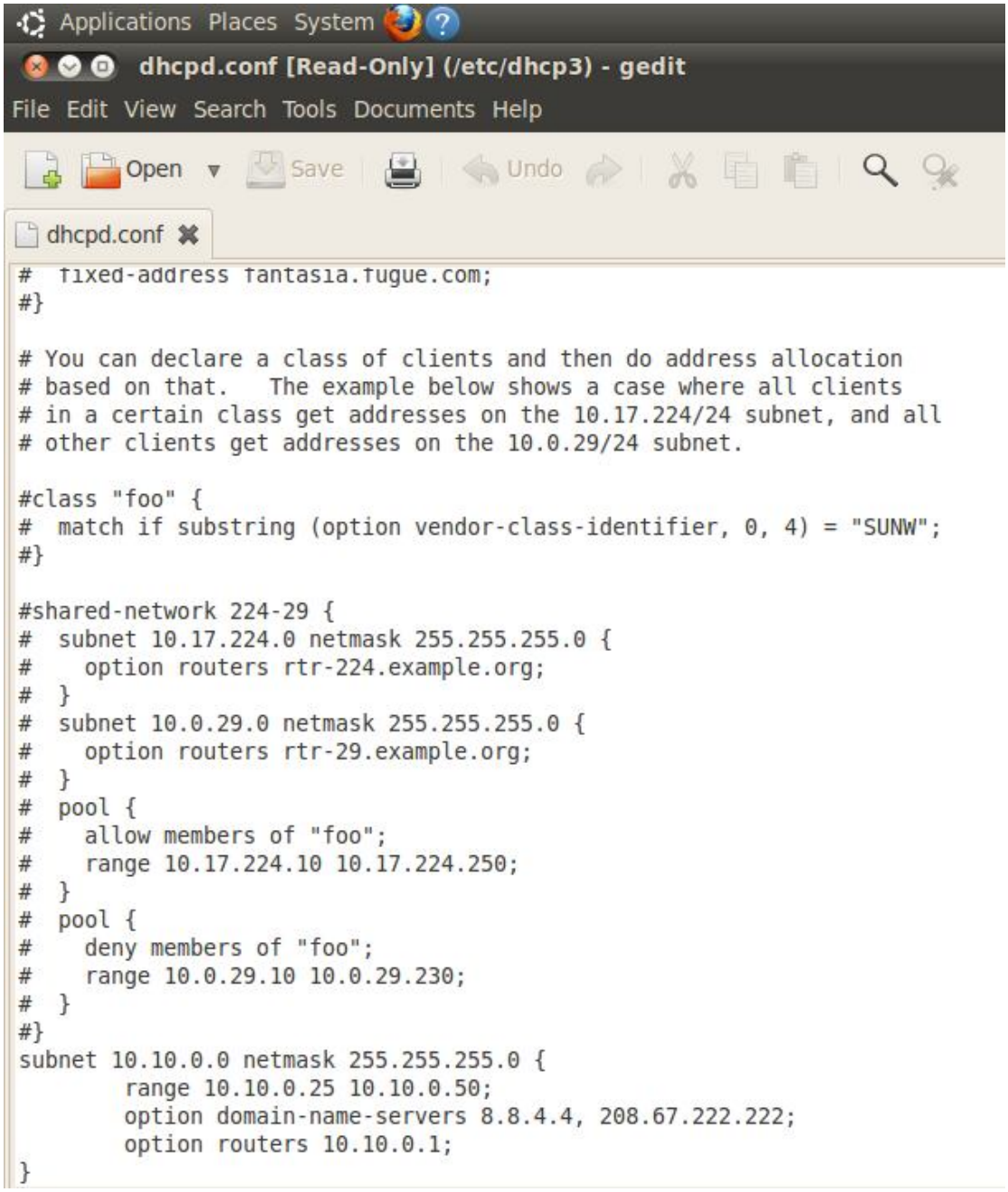
Display the Configuration files used to make the Software Access point and the parameters set according to the details of the Configuration details.

Screenshot show the hostapf.conf File details where the SSID is configured as MyAP etc.



Annexure - II

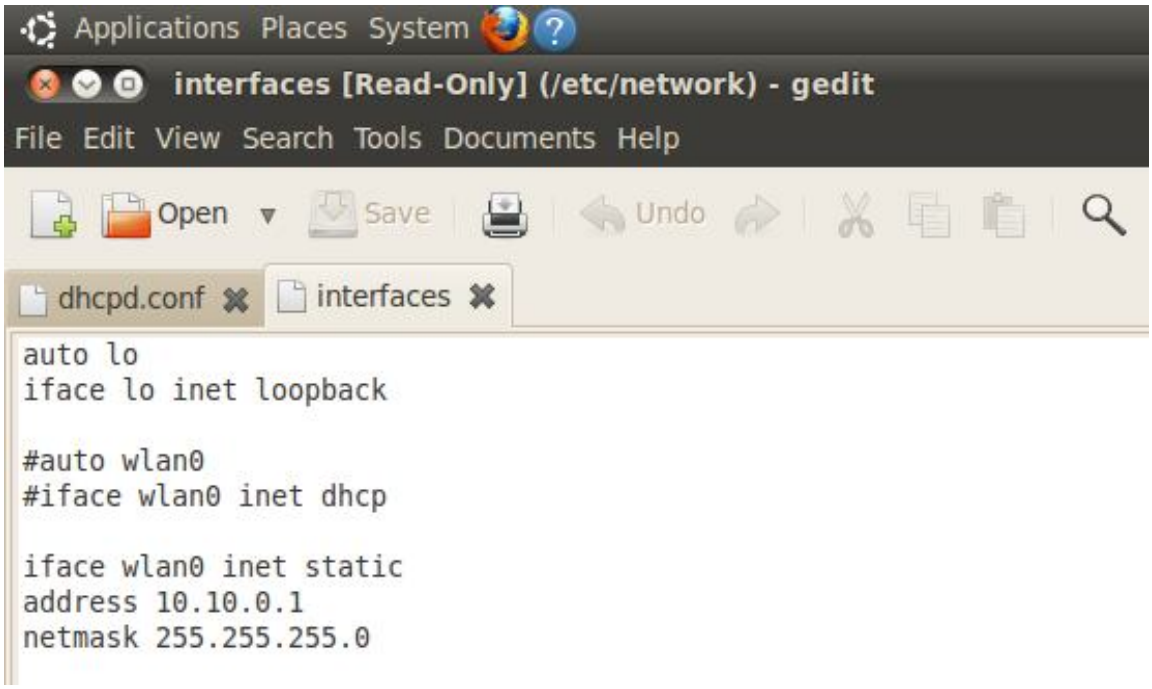
This shows the DHCP Configuration set.




```
#  fixed-address fantasia.fugue.com;
#}

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
#  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}
subnet 10.10.0.0 netmask 255.255.255.0 {
        range 10.10.0.25 10.10.0.50;
        option domain-name-servers 8.8.4.4, 208.67.222.222;
        option routers 10.10.0.1;
}
```

Annexure - III

This shows the Interface Configuration details.



LIST OF PUBLICATION

[1] Sukhvinder Singh, Maninder Singh, "Parametric Evaluation of Software Access Point Using Linux with Hardware Access Point", Communicated in an International Journal of Engineering Sciences Research (IJESR) (ISSN: 2230-8504; e-ISSN: 2230-8512)