Fall 12-2010

An Open Management and Administration Platform for IEEE 802.11 Networks

Biju Raja Bajracharya
University of Southern Mississippi

The University of Southern Mississippi

AN OPEN MANAGEMENT AND ADMINISTRATION PLATFORM

FOR IEEE 802.11 NETWORKS

by

Biju Raja Bajracharya

A Thesis
Submitted to the Graduate School
of The University of Southern Mississippi
in Partial Fulfillment of the Requirements
for the Degree of Master of Science

Approved:

[redacted]

Dean of the Graduate School

December 2010

ABSTRACT

AN OPEN MANAGEMENT AND ADMINISTRATION PLATFORM FOR IEEE 802.11 NETWORKS

by Biju Raja Bajracharya

December 2010

The deployment of Wireless Local Area Network (WLAN) has greatly increased in past years. Due to the large deployment of the WLAN, the immediate need of management platforms has been recognized, which has a significant impact on the performance of a WLAN. Although there are various vendor-specific and proprietary solutions available in the market to cope with the management of wireless LAN, they have problems in interoperability and compatibility. To address this issues, IETF has come up with the interoperability standard of management of WLANs devices, Control And Provisioning of Wireless Access Points (CAPWAP) protocol, which is still in the draft phase. Commercial implementation of this draft protocol from WLAN equipment vendors is rather expensive. Open source community, therefore, tried to provide free management solutions. An open source project called openCAPWAP was initiated. However, it lacks a graphic user interface that makes it hard to implement for novice network administrators or regular customers. Therefore, the researcher designed and developed a web interface framework that encapsulates openCAPWAP at the bottom to provide user-friendly management experience.

This application platform was designed to work with any remote web server in the public domain through which it can connect to access points or access controllers through a secure shell to configure them. This open platform is purely open source-based. It is operating system independent: it can be implemented on any open source environment such as regular Linux operating system or embedded operation system small form factor single board computers. The platform was designed and tested in a laboratory environment and a remote system. This development contributes to network administration in both network planning and operational management of the WLAN networks.

ACKNOWLEDGMENTS

I wish to express my sincere gratitude and appreciation to Dr. Shaoen Wu for his valuable supervision and assistance in the preparation of this manuscript. Your patience and guidance throughout this process was instrumental to its successful completion. I would like to thank Drs. Randy Buchanan and Zhaoxian Zhou for reviewing my thesis and providing their feedback.

I would like to thank my colleagues at The University of Southern Mississippi for providing a wonderful academic experience and friendly environment during my Master's program.

This is to thank all of those who have assisted me in this effort. I am forever indebted to my advisor who is the source of all wisdom in this worldly life.

I am and remain in his awesome, brilliant shadow.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

Figure

LIST OF TABLES

Table

LIST OF ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
AC	Access Controller
AMD	Advanced Micro Devices
AP	Access Point
CAPWAP	Control And Provisioning of Wireless Access Points
CF	Compact Flash Card
DHCP	Dynamic Host Controller Protocol
DNS	Domain Name Service
FCC	Federal Communications Commission
FreeBSD	Free Berkeley Software Distribution
GUI	Graphic User Interface
IEEE	Institute of Electrical and Electronics Engineer
IETF	Internet Engineering Task Force
ISM	Industrial, Scientific and Medical
IP	Internet Protocol
LAN	Local Area Network
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PHY	Physical Layer
MAC	Media Access Control Layer
RF	Radio Frequency
RSSI	Received Signal Strength Indication
SBC	Single Board Computer
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
SSH	Secure Shell
SSL	Secure Sockets Layer
STA	Wireless Station
SWAP	Shared Wireless Access Protocol
WAP	Wireless Access Point
WECA	Wireless Ethernet Compatibility Alliance
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WC	Wireless Controller
WMAN	Wireless Metropolitan Area Network
WNMS	Wireless LAN Network Management System
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
WTP	Wireless Termination Point

Chapter 1

INTRODUCTION

1.1 Introduction

In the recent years, the emergence of wireless access network has become the breakthrough of new cutting edge technology which has been largely deployed in corporate private networks, homes and public hot-spots around the world in very short time. The pervasive use of wireless network and recent advances in wireless local-area networking technologies have resulted one of the hot topics in computer science research today.

The rapid growth of large-scale deployment of wireless access networks results in dense deployment of wireless networking equipments in areas such as apartment buildings, campuses, shopping areas, public hot spots, neighborhoods etc. Some of the deployments are carefully planned and organized to optimize the coverage area, minimize the cell overlap, reduce the neighborhood interference whereas many other deployments includes independent people or organizations each setting up multiple number of access points (AP) to expand its wireless networks. This type of spontaneous deployment results in very high densities of wireless nodes and APs where APs can be more than thousands and can be from multiple vendors. In this type of situation, the controlling and managing wireless networks and configuring APs are very difficult and tedious even for a simple tasks such as to set service set identifier (SSID) in thousands of APs. Since the dynamic nature of wireless networks, to set the consistent configuration among all the APs is extremely hard which requires constant attention and supervision to these APs. Most importantly, these AP vendors have no common standard. Thus they have interoperability issue among different vendor's AP. For controlling, managing, and configuring these APs, a control mechanism is needed which can be served by developing protocol Control And Provisioning of Wireless Access Points, CAPWAP protocol which is still in draft phase and used by certain vendors only.

This thesis defines the concept of implementing open source CAPWAP protocol to centrally manage and configure the APs by placing a central controller called Access Controller(AC); and presents the platform that can control, manage and configure APs through a Web Interface. This designed platform is then applied to configure the small form factor single-board computer (SBC) customized as an AP, personal computer (PC) customized as an AP and an Access Controller set up in PC.

1.2 Problem Statement

Given the wide variety of wireless hardware (AP) options from different vendors, the chance of heterogeneous APs that can be deployed in large scale wireless local area network is highly possible. This thesis considers the difficulties and challenges associated in these types of large scale heterogeneous AP deployment in wireless local area network. This thesis addresses need of graphic user interface (GUI) based tool to implement the centralized controller, AC for managing, controlling, monitoring and maintaining a consistent configuration throughout the entire set of APs in large-scale wireless local area deployment.

1.3 Objectives of the Thesis

The general objective of this thesis research is to design a web interface for management and administration platform for wireless local area networks based on openCAPWAP protocol. The general objective of this thesis is:

- to build a lightweight, low power, small form-factor customized wireless access point
- to redesign and develop website using HTML, PHP and JavaScript language to manage and administer the access points and access controllers
- to provide secure communication from web interface to the access point, and access controller via SSH connection
- to implement the openCAPWAP protocol

1.4 Limitations of the Thesis

This study is a simple research which has to be conducted and submitted within the prescribed time. This research is about the Open Source Implementation of protocols through Web Interface. There are some limitations of this study, which are mentioned below.

(a) the study mainly concentrates on open source operating systems, and open source tools

(b) different wireless scenerios have not been performed due to the lack of testbed

(c) the degree of effectiveness is fully dependent upon available open-source packages

1.5 Organization of the Thesis

For this thesis, a significant research study has been conducted for deep understanding of how Wireless Network works and for what and how it is used. The Chapter 1 includes the brief introduction of the thesis and it addresses the problems associated with the current wireless LAN, objective of the thesis.

Chapter 2 briefly describes wireless LAN background, history, wireless technology, topologies and architecture, wireless standards, and management protocols. Chapter 3 briefly describes the system design of hardware, software required to implement the access point along with openCAPWAP protocol. Chapter 4 includes how the application platform is developed and implemented. It also presents the comparative analysis with other open source platforms. Chapter 5 presents the procedures of operating the platform. And finally the Chapter 6 presents the conclusion and summary of the thesis.

Chapter 2
REVIEW OF LITERATURE

2.1 Overview

2.1.1 Wireless Networks

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into four groups based on their coverage range:

a) Wireless Wide Area Networks (WWAN),
b) Wireless Metropolitan Area Networks (WMAN),
c) Wireless Local Area Network (WLAN), and
d) Wireless Personal Area Networks (WPAN).

WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex. WMAN includes wireless network that connects several Wireless LANS termed as WiMax. WLAN, representing wireless local area networks, includes 802.11, HiperLAN, and several others. WPAN, represents wireless personal area network technologies such as Bluetooth and IR.

2.2 Wireless LAN

A radio frequency based wireless network, can be traced back to the research project of University of Hawaii, ALOHANET in the 1970s, the key events that led to wireless LAN networking. WLAN technology and WLAN industry date back to mid 1980s when Federal Communications Commission (FCC) first made RF spectrum available to industry.

In late 80s, the first generation proprietary WLANs are introduced as WaveLAN by ATT, HomeRF by Proxim. Motorola developed one of the first commercial WLAN systems with its Altair product. Early WLAN technologies had several problems that prohibited its pervasive use. These WLANs were expensive, provided low data rates, were prone to radio interference, and were mostly proprietary. WLAN is experiencing tremendous growth later on due to the increased bandwidth made possible by the IEEE 802.11 project which is initiated in 1990 with a scope "to develop a Medium Access Control (MAC) and Physical Layer (PHY) specification for wireless connectivity for fixed, portable, and moving stations within an area." Subsequently in 1997, IEEE ratified 802.11 standard which become a major milestone in the development of WLAN networking and the subsequent development of interoperability certification by the Wi-Fi Alliance (formerly WECA) become the starting point for a strong and recognizable brand Wi-Fi. This provides a focus for the work of equipment developers and service providers and is as much a contributor to the growth of WLAN as the power of the underlying technologies.

2.3 Wireless LAN Technologies

There are several wireless LAN specifications and standards such as HiperLAN, HomeRF, SWAP, Bluetooth etc.

2.3.1 HiperLAN

HiperLAN began in Europe as a specification (EN 300 652) ratified in 1996 by the European Telecommunications Standards (ETSI) Broadband Radio Access Network (BRAN) organization. HiperLAN/1, the current version, operates in the 5 GHz radio band at up to 24 Mbps. Similar to Ethernet, HiperLAN/1 shares access to the wireless LAN among end user devices via a connectionless protocol. HiperLAN/1 also provides QoS support for various needs of data, video, voice, and images.

2.4 IEEE 802.11 Wireless Standards

WLANs are based on the IEEE 802.11 international interoperability standard developed by IEEE in 1997 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations. 802.11 is the original WLAN standard, designed for 1 to 2 Mbps wireless transmissions. In 1999, it was followed by 802.11a, which established a high-speed WLAN standard for the 5 GHz band and supported 54 Mbps, and 802.11b standard, which operates in the 2.4 - 2.48 GHz band and supports 11 Mbps. The goal was to create a standards-based technology that could span multiple physical encoding types, frequencies, and applications. In 2003, IEEE ratified 802.11g and just recently in 2009, 802.11n wireless networking communication standards which are currently the dominant standard for WLANs, providing sufficient speeds for most of today's applications that operates in the 2.4 GHz waveband. As an introduction to the 802.11 and WLAN technology, Table 2.1 provides some key characteristics and Table 2.2 [10] adopted frequency at a glance.

Table 2.1: IEEE 802.11 Standards.

Standards	Maximum Data Rate (Mbps)	Typical Throughput (Mbps)	Operating Frequency Band	Maximum Non-overlapping Channels
802.11a	54	25	5 GHz	24 (20 MHz channels) 12 (40 MHz channels)
802.11b	11	6.5	2.4 GHz	3 *1
802.11g	54	8 (Mixed b/g)	2.4 GHz	3 *1
802.11n	600 (Theoretical Max)	74 to 144 *2	2.4 GHz & 5 GHz	*3

*1 - Channels 1, 6 and 11 are the three non-overlapping channels. Each channel is 20 MHz wide.

*2 - Actual throughput will depend upon various factors such as the manufacturer and model, environmental factors, whether 20MHz or 40Mhz channels are utilized, if security is enabled and whether all clients are 802.11n or mix of 802.11a/g/n.

*3 - For 802.11n, in the 2.4GHz band, there are three non-overlapping 20MHz channels or one 40 MHz channel. the use of 40MHz is not desirable or practical in the 2.4 GHz band. However, a single 20MHz channel could be used with lower throughput, largely defeating the gain of using 802.11n. In the 5GHz band, twenty four non-overlapping 20MHz or up to twelve 40MHz channels exists.

Two other important and related standards for WLANs are 802.1X and 802.11i. The 802.1X, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard, also still in draft, was created for wireless-specific security functions that operate with IEEE 802.1X.

2.5 WLAN Topologies

WLAN is a series of interconnected cells consisting of wireless device or station, the access point (AP), the wireless medium, the distribution system (DS) distribution services working together to provide a ability to roam around the WLAN looking for all intents and purposes like a wired device. A logical entity of set of such wireless stations or devices communicating in a WLAN is called Basic Service Set.

Table 2.2: *IEEE 802.11 Standard and Worldwide Frequency Bands.*

Location	Regulatory Range (MHz)	Maximum Output Power (mW)	Standard
Europe	2400 - 2483.5	10/MHz (max 100mW)	IEEE 802.11 b,g
	5150-5350	200	
	5470-5725	1000	IEEE 802.11a
North America	2400 2483.5	1000	IEEE 802.11 b,g
	5150-5250	2.5/MHz (max. 50mW)	IEEE 802.11a
	5250-5350	12.5/MHz (max. 250mW)	
	5725-5825	50/MHz (max. 1000mW)	
Japan	2400 2497	10/MHz (max 100mW)	IEEE 802.11 b,g
	5150-5250	Indoor	IEEE 802.11a
	4900-5000(until 2007)		
	5030-5091 (from 2007)		

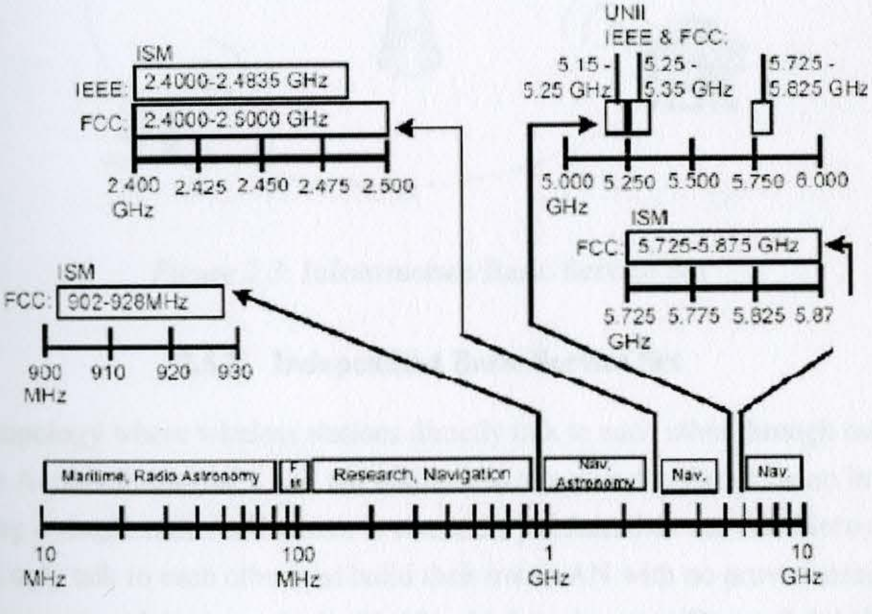


Figure 2.1: 802.11 Frequency Allocation (a)

2.5.1 Infrastructure Basic Service Set

A network topology where wireless stations directly talk to each other through radio contact or an single Access Point (AP), and not connected to a wired network, is an Infrastructure BSS forming a single radio cell. The Figure 2.3 [12] shows a sample infrastructure BSS.

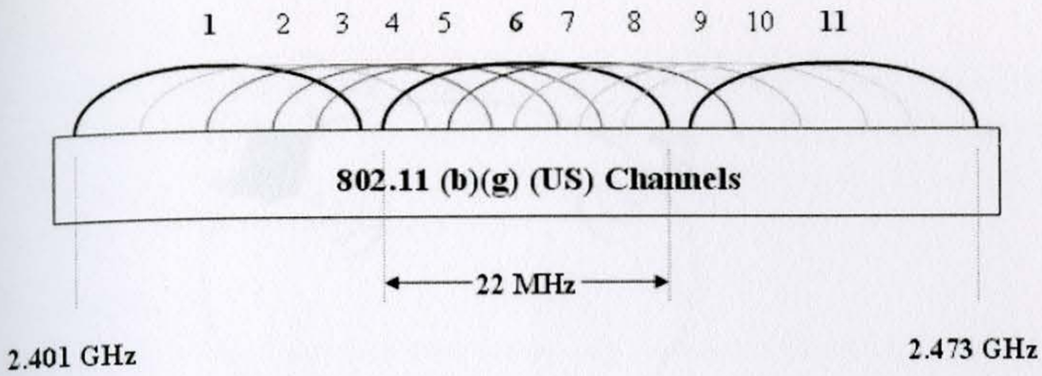


Figure 2.2: 802.11 Frequency Allocation (b)

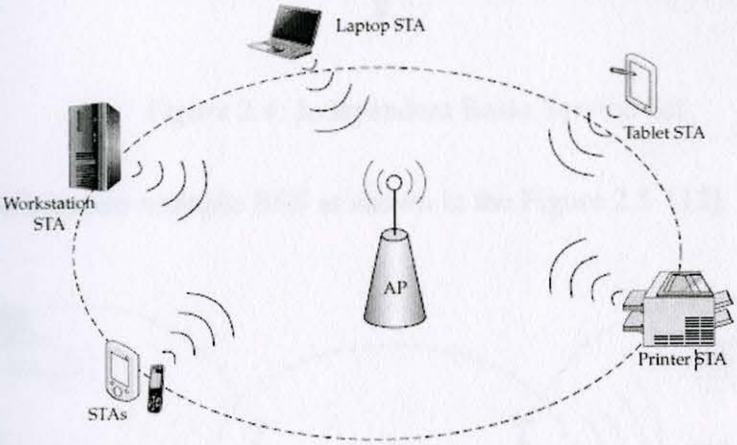


Figure 2.3: Infrastructure Basic Service Set

2.5.2 Independent Basic Service Set

A network topology where wireless stations directly talk to each other through radio contact without any Access Point (AP), and not connected to a wired network, is an Independent BSS forming a single radio cell which is commonly referred as Ad-hoc Network. These stations can only talk to each other and build their own LAN with no provisioning of a relay as peer-to-peer network in case of wired LAN which is shown in Figure 2.4 [12].

2.5.3 Extended Service Set

A networking topology consisting of multiple BSSs each having a single access point is called an extended service set which provides a greater mobility of stations and not confine them to a single BS where stations are free to move about without having to worry about switching network connections manually. Through ESS, IEEE 802.11 architecture allows

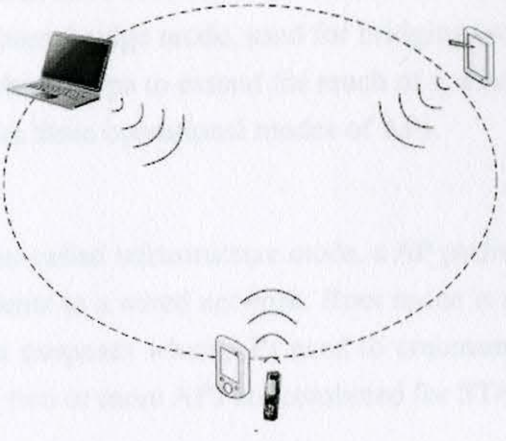


Figure 2.4: Independent Basic Service Set

users to move between multiple BSS as shown in the Figure 2.5 [12].

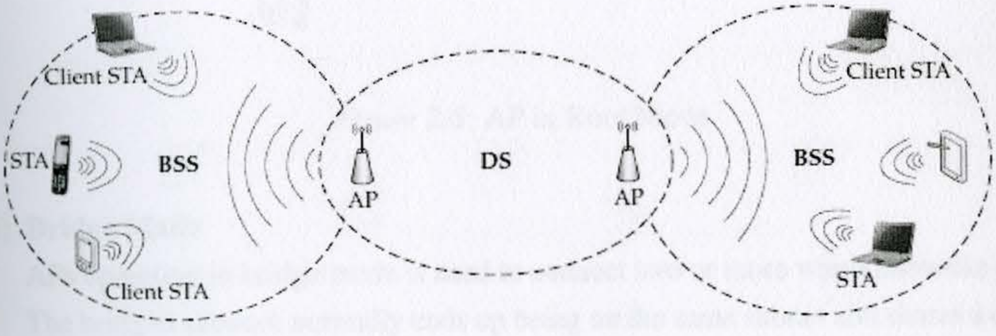


Figure 2.5: Extended Service Set

2.6 Wireless LAN Components

2.6.1 Wireless Access Point

Wireless access point (WAP) provides the means for wireless nodes to communicate with other wireless nodes or to communicate with a wired network. WAP is commonly referred as access point (AP) or wireless termination point (WTP). In addition to connecting wireless nodes to a wired network, WAPs also feature a combination of the security functions, MAC layer filtering functions, protocol layer filtering, VLAN functionality, detachable antennas, field replaceable radio cards, and Power over Ethernet.

AP Operational Modes

Wireless APs operates in three modes: root mode, the most fundamental and natural mode in which a WAP operates; bridge mode, used for bridging two or more networks together; and repeater mode, which helps to extend the reach of a wireless network. Figure 2.6, 2.7 and 2.8 [12] shows the three operational modes of APs.

(a) **Root Mode**

In this mode, also called infrastructure mode, a AP performs its basic function connecting wireless clients to a wired network. Root mode is also used for inter-messaging or management purposes when APs need to communicate among themselves (for example, when two or more APs are combined for STA roaming purposes).

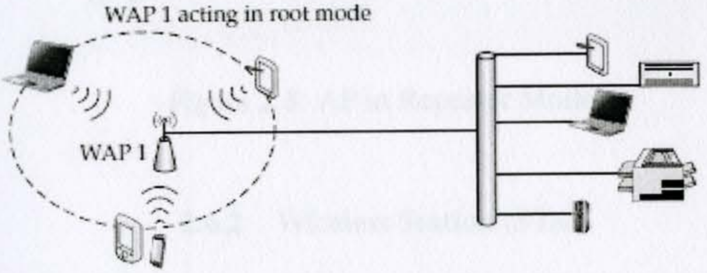


Figure 2.6: AP in Root Mode

(b) **Bridge Mode**

APs operating in bridge mode is used to connect two or more wired networks together. The bridged network normally ends up being on the same subnet and shares a common broadcast domain. In this mode, wireless client are not allowed to connect to AP APs operating in bridge mode are used for creating point-to-point and point-to-multipoint links.

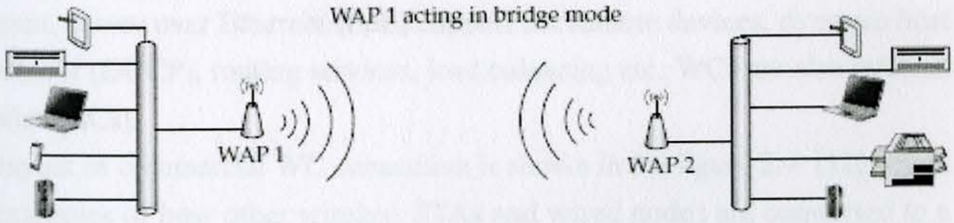


Figure 2.7: AP in Bridge Mode

(c) **Repeater Mode**

In repeater mode, the AP extends the reach of the wireless network by repeating the signals of a remote AP. The repeater AP is connected via a hardwire to the remote root mode AP. Wireless clients can then connect wireless to the AP operating in repeater mode as shown in the Figure 2.8 [12].

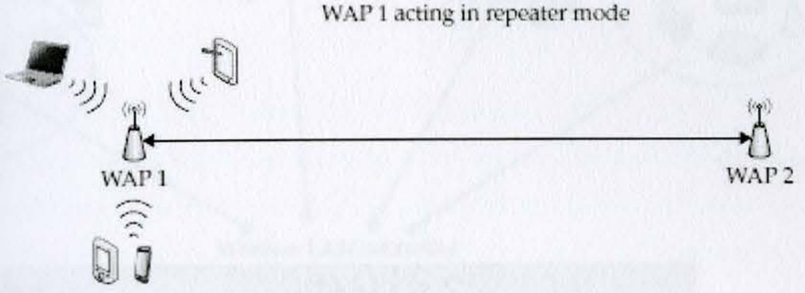


Figure 2.8: AP in Repeater Mode

2.6.2 Wireless Station (STA)

The hardware component consisting of wireless medium that is used to connect to the fixed wireless nodes or access point is termed as STA. STAs may be mobile, stationary, portable or roaming. Generally network adapter or network interface cards are referred to as STA.

2.6.3 Wireless Switches and Controllers

Wireless switches and controllers (WCs) are infrastructure devices which are strictly an enterprise class of wireless hardware. These devices are designed to scale to meet the needs of different sized networks and serve as a sort of central management for other STAs in a wireless network. These controllers are used to firmware management for the STAs (upgrades/downgrades), individual configuration and settings for client STAs, MAC layer filtering, protocol layer filtering, wireless intrusion detection capabilities, quality of service (QoS) management, power over Ethernet (PoE) support for remote devices, dynamic host configuration protocol (DHCP), routing services, load balancing etc. WCs are also referred as access controller (ACs).

The typical layout of commercial WC connection is shown in the figure 2.9 [12] which shows various examples of how other wireless STAs and wired nodes are connected to a WC.

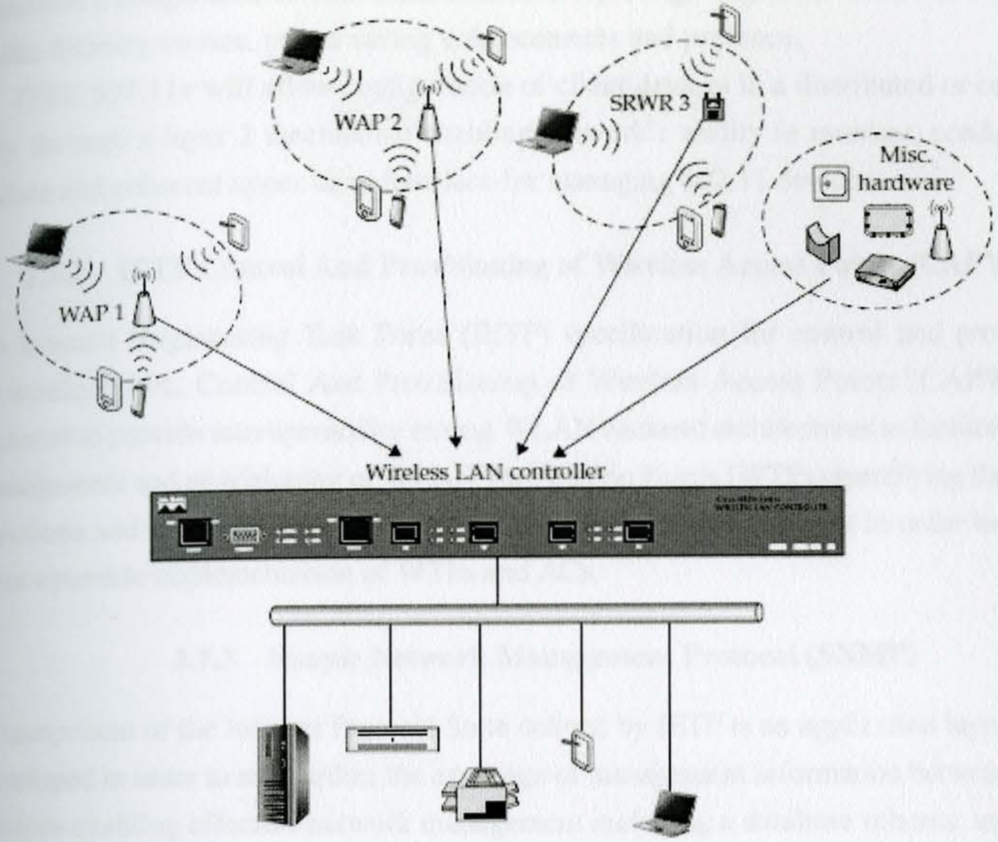


Figure 2.9: Wireless STAs and Wired Nodes connecting to a Wireless Controller

2.7 Wireless LAN Management Standards

Simultaneously IEEE and IETF are developing standards for WLAN management: IEEE 802.11v and IETF CAPWAP. Although they have the similar features, IEEE 802.11v is more focused towards management of STAs, (the details of this standards is yet to be published). IETF aimed at defining inter-operable protocol enabling management of heterogeneous Access Points through a centralized controller called access controller (AC).

2.7.1 IEEE 802.11v

A framework and common methods for wireless network management by IEEE which was first drafted in July 2007, and scheduled for completion and ratification is set to Dec 2010 which is designed to develop extensions to the 802.11 MAC/PHY to provide network management for STAs. As stated by the task group (TGv), the IEEE 802.11v amendment defines mechanisms for wireless network management of non-AP STAs, including BSS transition management, co-located interference reporting, diagnostic and event reporting, a traffic filtering service, power saving enhancements and presence.

IEEE 802.11v will allow configuration of client devices in a distributed or centralized way through a layer 2 mechanism enabling network's ability to monitor, configure, and update and coherent upper layer interface for managing 802.11 devices.

2.7.2 IETF Control And Provisioning of Wireless Access Points (CAPWAP)

An Internet Engineering Task Force (IETF) specification for control and provisioning of wireless APs, Control And Provisioning of Wireless Access Points (CAPWAP) is a protocol to provide interoperability among WLAN backend architectures to facilitate control, management and provisioning of WLAN Termination Points (WTPs) specifying the services, functions and resources relating to 802.11 WLAN Termination Points in order to allow for inter-operable implementation of WTPs and ACs.

2.7.3 Simple Network Management Protocol (SNMP)

A component of the Internet Protocol Suite defined by IETF is an application layer protocol developed in order to standardize the exchange of management information between network devices enabling effective network management including a database schema, and a set of data objects which are configuration parameters and statistics that are exposed in the form of variables on the managed systems. SNMP defines a centralized architecture, where one or more network managers handle several network devices through the SNMP agents.

An SNMP-managed network consists of four key components:

(a) Managed Devices

A managed device is a network node that contains an SNMP agent and that resides on a managed network used to collect and store management information and make this information available to NMSs using SNMP. Managed devices can be routers, switches, hosts, etc.

(b) Agents

An agent is a network-management software module that resides in a managed device and is in charge of managing local information and configuration parameters according to the network manager's indications.

(c) Network Management Systems (NMS)

A NMS is in charge for monitoring and controlling managed devices, responsible for polling and receiving traps from the Agents as well as for changing the values of variables stored within managed devices.

(d) Management Information Base

A Management Information Base (MIB) is a collection of information that is organized hierarchically. MIBs are accessed using a the SNMP protocol.

The Figure 2.10 [6] shows a simplified implementation of SNMP, with one network management station used to maintain three managed nodes. Each device has an SNMP Entity, and they communicate using SNMP messages. The SNMP entity of the NMS consists of the SNMP Manager and one or more SNMP Applications; the managed nodes each run as SNMP Agent and maintain a Management Information Base (MIB).

To configure APs in accordance with established security policies and requirements, SNMP agents help to properly configuration of administrative passwords, encryption settings, reset function, automatic network connection function, Ethernet MAC Access Control Lists (ACL), and shared keys to eliminate many of the vulnerabilities inherent in a vendor's software default configuration.

Some wireless APs allows network management software tools to monitor the status of wireless APs and clients using SNMP. However, the first two versions of SNMP, SNMPv1 and SMPv2 support only trivial authentication based on plain-text community strings are fundamentally insecure, SNMPv3 support strong security mechanism. If SNMP is not required on the network, the SNMP can be disabled.

2.8 WLAN Network Management System (WNMS)

One of the challenges for a WLAN administrator using a large WLAN intelligent edge architecture is management. One major disadvantage of using the traditional autonomous access point is that there is no central point of management. Any intelligent edge WLAN architecture with 25 or more access points is going to require some sort of wireless network management system (WNMS). A WNMS provides a central point of management to configure and maintain as many as 5,000 fat access points.

A WNMS can be either a hardware appliance or a software solution. The most widely known WNMS is the vendor-specific Cisco Wireless LAN Solution Engine (WLSE), Vendor-neutral WNMS such as the AirWave software solution. The main purpose of a WNMS is to provide a central point of management, configuration settings and firmware upgrades which can be pushed down to all the autonomous access points along with other capabilities such as including RF spectrum planning and management. It can also be used to monitor

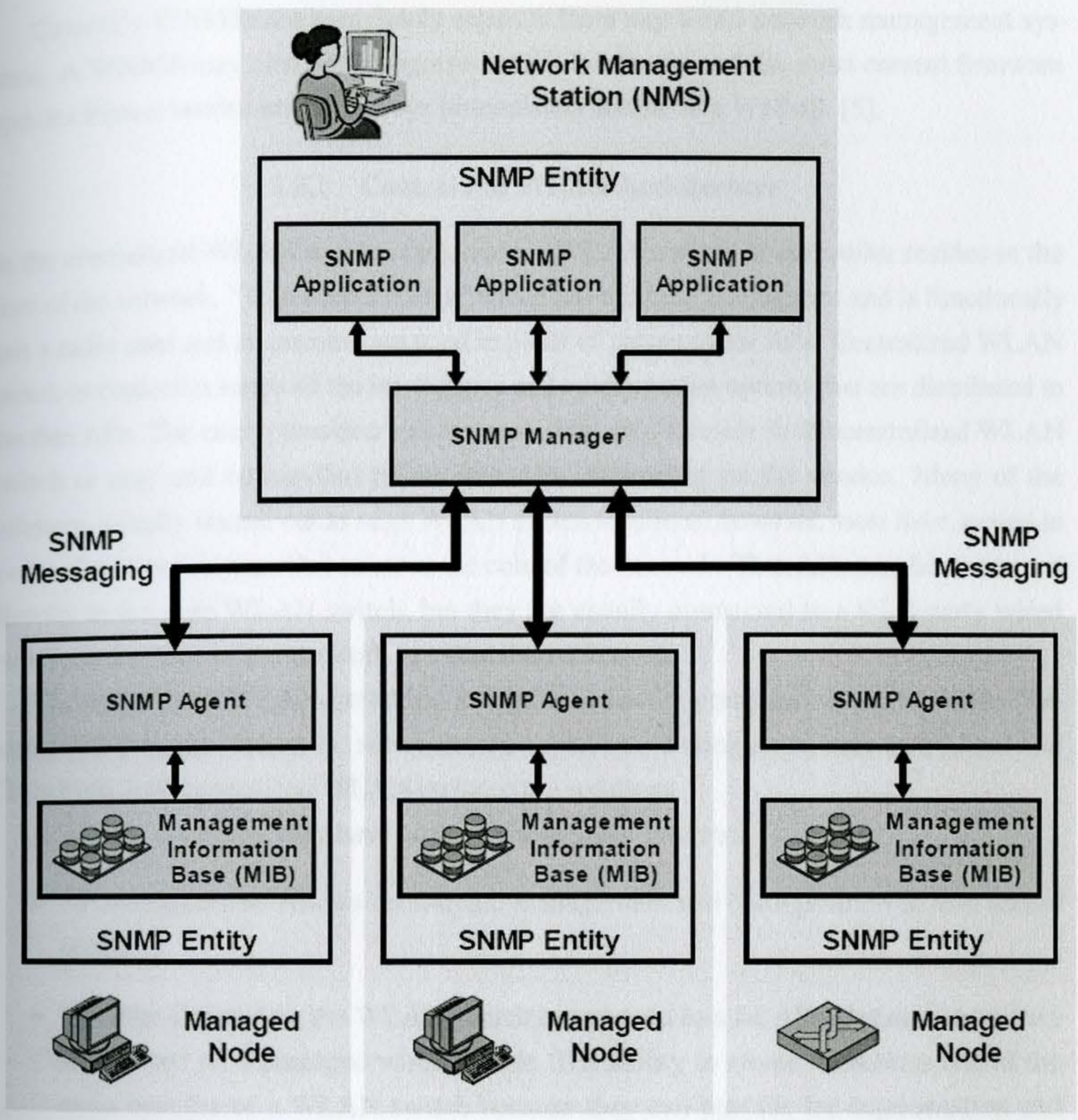


Figure 2.10: SNMP Operational Model

intelligent edge WLAN architecture with alarms and notifications, centralized and integrated management console. Other capabilities include network reporting, trending, capacity planning, and policy enforcement. A WNMS might also be able to perform some rogue AP detection, but by no means should a WNMS be considered a wireless intrusion detection system (WIDS). One of the main disadvantages of a WNMS is that it will not assist in the roaming capabilities between access points, whereas the wireless switching architecture has that ability.

Currently WNMSs are completely separate from any wired network management systems. A WNMS may also not recognize certain hardware, and the most current firmware updates from a vendor are not always immediately usable in a WNMS [5].

2.8.1 Centralized WLAN Architecture

In the centralized WLAN architecture, central WLAN switch or controller resides in the core of the network. "Thin access points" which has minimal intelligence and is functionally just a radio card and an antenna are used in place of autonomous APs. Centralized WLAN switch or controller keeps all the intelligence and configuration options that are distributed to the thin APs. The encryption/decryption capabilities might reside in the centralized WLAN switch or may still be handled by the thin APs, depending on the vendor. Many of the solutions initially started out as edge WLAN switch solutions; however, most have moved to a centralized architecture that exists at the core of the network. Thin APs may be connected directly to the core WLAN switch, but they are usually connected to a third-party wired switch on the edge of the network in a distributed fashion.

The majority of WLAN switching vendors are startup companies such as Aruba Networks and Trapeze Networks, although more established companies such as Symbol and Cisco both have centralized WLAN architecture solutions.

A WLAN controller may have some of these many features:

- AP management: Allows centralized management and configuration of thin access points.
- VLANs: Created on the WLAN switch as opposed to a fat AP solution, where they are created on a managed wired switch. The ability to create VLANs is one of the main benefits of a WLAN switch because they can provide for segmentation and security.
- User management: The ability to control who, when, and where with role-based access control (RBAC).
- Layer 2 security support: Support for 802.1X/EAP (WPA /WPA2) security solutions.
- Layer 3 and 7 VPN concentrators: The WLAN switch acts as a VPN end point.
- Captive portal: Used for web page authentication, usually for guest users.
- Automatic failover and load balancing: Provides support for Virtual Router Redundancy Protocol (VRRP)

- Internal Wireless Intrusion Detection Systems: Most WLAN switches have internal WIDS capabilities for security monitoring.
- Site survey and RF spectrum management: Some Wi-Fi switches have automatic channel management and cell sizing capabilities.
- Bandwidth management: Bandwidth pipes can be restricted upstream or downstream.
- Firewall capabilities: Statefull packet inspection is available with an internal firewall.
- Layer 3 roaming support: Capabilities to allow seamless roaming across layer 3 routed boundaries.
- 802.3af Power over Ethernet (PoE): support Wireless switches can provide direct power to thin access points via PoE or thin access points can be powered by third-party edge switches.

The most obvious advantages of the centralized architecture of a WLAN controller include AP management, user management, RF spectrum planning and management, and VLAN segmentation. Another major advantage of the WLAN switch model is that most of the switches support some form of fast secure roaming, which can assist is resolving latency issues often associated with roaming. One possible disadvantage of using a WLAN switch is that the WLAN switch might become a bottleneck because all data must be sent to and redirected from the WLAN switch. Most switch vendors are able to prevent this from occurring by providing a scalable hierarchical environment. Quality of Service (QoS) policies are also enforced at the WLAN switch, which may cause latency issues. WLAN switches and the thin access points might be separated by several hops, which can also introduce network latency. Some of the WLAN controllers have so many features and configuration settings that the user interface can be very confusing for novice administrators.

2.8.2 Distributed WLAN Architecture

A few vendors have recently implemented a distributed WLAN architecture that uses a WLAN switch that manages hybrid fat/thin access points. The centralized switch still acts as a central point of management for all the hybrid access points. However, QoS policies and all of the 802.11 MAC data forwarding is handled at the edge of the network at the access points instead of back on the WLAN switch.

2.8.3 Unified WLAN Architecture

Unified WLAN Architecture WLAN switching could very well take another direction by fully integrating wireless switching capabilities into wired network infrastructure devices. Wired switches at both the core and the edge would also have wireless switching capabilities, thereby allowing for the combined management of the wireless and wired network.

This unified architecture has already begun to be deployed by some vendors and will likely grow in acceptance as WLAN deployments become more commonplace and the need for fuller integration continues to rise [5].

2.9 Control and Provisioning of Wireless Access Points (CAPWAP)

An IETF's new standardization of a process of new protocol and a set of mechanisms intended to solve the problems of large-scale WLANs deployment in enterprise networks stated in RFC 3990 [1]. RFC 3990 states four basic issues: first, each AP is a new networking device requiring management, monitoring and control; the second, distributing and maintaining a consistent configuration throughout the entire set of access points in the WLAN is problematic because of its configuration consists of long-term static information such as addressing and hardware settings and individual WLAN settings and security parameter although part of this configuration is unchanged in the long run (IP address, ESSID, etc.), it is completely dynamic and requires a constant attention hindering the provision of a unique and consistent configuration; thirdly, coping with the dynamic nature of the wireless medium requires a coordinated control for maximizing network performance; finally, there are evident security issues, so there is also a need to provide safe access to the network and prevent installation of unauthorized APs.

2.9.1 CAPWAP Protocol

The increasing diffusion of Wireless Local Area Networks (WLANs), characterized by a number of simple Access Points, named as Wireless Termination Points (WTPs), and having a single point of control, called Access Controller (AC), suggested the definition of a standard protocol aiming at simplifying the deployment, management and control of such architectures. The Control And Provisioning of Wireless Access Points is a recent effort of IETF aiming at defining an inter-operable protocol, enabling an AC to manage and control a collection of possibly heterogeneous WTPs.

CAPWAP inherits many concepts from its predecessor, Cisco's Light Weight Access Point Protocol (LWAPP), maintaining its philosophy. The idea is not only to maintain a centralized management of a series of "light" APs, but also to move part of their "intelligence" to a central controller. According to the RFC 4118, an IEEE 802.11 access network is divided into two device categories: Wireless Termination Points (WTPs), which in fact represent those "light" APs, and Access Controllers (ACs).

An AC centralizes the management of several WTPs. The functionality of the AC is not limited to the provision of network configuration; it can also manage WTP firmware loading, authentication and radio resource allocation through RF monitoring and setup, which provides means to optimize global network performance. The goals of this architecture explicitly stated in the current CAPWAP specifications are threefold:

(a) Centralize authentication and policy enforcement functions for a wireless network and, in some cases, bridging and encryption of user data.

(b) Move processing away from the WTPs, leaving there only time critical functions and protecting the most critical network parameters in the remote AC.

(c) Provide a generic encapsulation and transport mechanism for control and management messages, enabling the operation of CAPWAP regardless of the wireless technology.

RFC 4118 proposes three different network architectures, depending on the centralization level of the control operations. The architectures are called Split MAC, Local MAC and Remote MAC. The CAPWAP specifications do not assume any specific wireless technology. The RFC 5416 defines the binding for IEEE 802.11 WLANs according to which wireless frames encapsulated by WTP may also include a CAPWAP optional header with information on RSSI, SNR and data rate used by the sending STA and when the frame is encapsulated by AC, the CAPWAP header may include information on WLAN identification to be used when sending the frame to the wireless Medium. Specifically, RFC 5416 details two architectures (Split MAC and Local MAC) for the case of 802.11 networks. In both cases, the services with strict timing requirements (e.g., beacon generation and probe responses) are kept in the WTP.

In a Split MAC architecture, Distribution and Integration services reside on the AC, whereas all MAC functionalities are entirely left to the WTP in the Local MAC architecture. In the latter case, the AC is responsible for WTP configurations and access policy definitions. In a Split MAC architecture, the WTP is only devoted to the tunneling of data and management frames (except beacon, probe response and power management frames) to and from the AC. The difference between the two architectures is based on where specific functionalities are implemented: in the WTP, in the AC or in both. Table 2.3 [4] summarizes where specific functionalities may be implemented in the two cases.

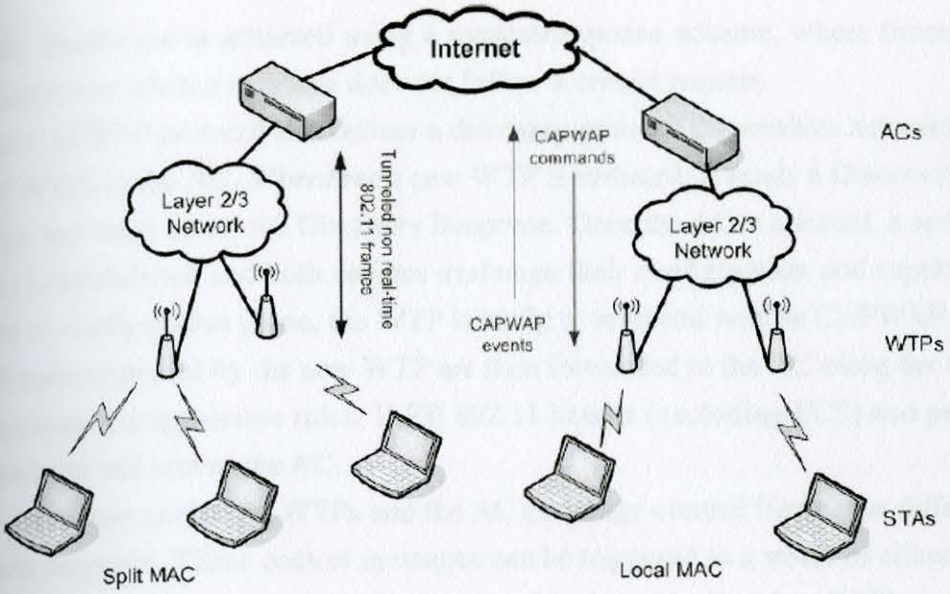


Figure 2.11: CAPWAP Network Architecture

Table 2.3: *802.11 Functions Mapping for Split MAC(SM) Local MAC (LM) Architectures.*

Function	**Location**	
	SM	**LM**
Distribution Service	AC	WTP/AC
Integration service	AC	WTP
Beacon Generation	WTP	WTP
Probe Response Generation	WTP	WTP
Power Management/Packet Buffering	WTP	WTP
Fragmentation/De-fragmentation	WTP/AC	WTP
Association/Disassociation/Re-association	AC	WTP/AC
IEEE 802.11 QoS		
Classifying	AC	WTP
Scheduling	WTP/AC	WTP
Queuing	WTP	WTP
IEEE 802.11 RSN		
IEEE 802.1x/EAP	AC	AC
RSNA key Management	AC	AC
IEEE 802.11 Encryption/Decryption	WTP/AC	WTP

These advanced control functions require a frequent exchange of management messages between the AC and the managed WTPs. As defined in RFC 5415, CAPWAP control and data messages are sent using UDP, and are secured using Datagram Transport Layer Security

(DTLS). Resilience is achieved using a request/response scheme, where timeouts cause retransmissions when a response does not follow a certain request.

The CAPWAP protocol also defines a discovery protocol that enables automatic association of WTPs to the AC. Whenever a new WTP is initiated, it sends a Discovery Request message and waits for an AC Discovery Response. Once the AC is selected, a secure DTLS session is established and both devices exchange their configuration and capabilities. At the end of configuration phase, the WTP is ready to send and receive CAPWAP messages. Data frames collected by the new WTP are then forwarded to the AC using the CAPWAP data message encapsulation rules: IEEE 802.11 header (excluding FCS) and payload are encapsulated and sent to the AC.

Besides data exchange, WTPs and the AC exchange control frames for different management purposes. These control messages can be triggered as a result of either a manual configuration update or automatically generated to dynamically adapt WTP configuration. Control messages allow the AC not only to configure the WTP but also to modify station session state on a WTP (including QoS specifications). The protocol also specifies messages that can be sent asynchronously by the WTPs to notify the AC of certain events (similar to the SNMP traps). Nevertheless, all control messages intended to manage radio resource related parameters are in fact used to read or set IEEE 802.11 MIB objects, and therefore the CAPWAP protocol does not provide an added value in this regard [14].

Chapter 3

SYSTEM DESIGN

3.1 Overview

This chapter involves the research of current available information from journals, books, on-line posts, IETF drafts, IEEE papers to understand and explain the new developing technologies. This chapter discuss the software and hardware platform that can be customized or modularized. To achieve the objectives of the thesis, this chapter has been proposed to follow which includes (a) Hardware Selection (b) Hardware Component: Wireless Card Selection (c) Operating System Selection (d) Programming Language Selection, and (e) and web-based application.

3.2 Selection of Hardware and Software

There are plethora of softwares applications based on both Windows and LINUX system. Considering the open source application that are available at no cost and can be modified, the LINUX based software application are selected for this project. The hardware that have more flexibility, more functionality, low cost and low power consumption with small form factor are selected for this project.

Any linux machines can be set to act like wireless APs using HostAP drivers, or madwifi driver and can emulate the functionality of an AP in infrastructure mode or station mode. Of course, the advantages to running Linux on AP are significant. Having a shell for command is an enormous amount of flexibility compared to the restrictive Web-based management interface of typical off-the-shelf consumer grade AP. The benefits provided by Linux without the hassles of running desktop PCs is either reflash off-the-shelf APs or utilize a single-board computer (SBC) such as Soekris, Alix, ARM etc. These small form factor devices with no moving parts, low power consumption are ultra-portable, ultra-reliable hardware device. The low power consumption and small form factor, embedded devices which can act as miniature computer hosting variety of lightweight versions of UNIX are available for different purposes for VPN router, Wireless Router firewall, Internet gateways, etc.

There are various vendors that provide compact full featured single-board computers. They are as:

(a) Soekris Engineering (www.soekris.com)

(b) PCEngine TM (www.pcengine.ch)

(c) Technologic Systems Inc. (www.embeddedarm.com)

Net5501, Net 4826 from Soekris use AMD Geode CPU. Alix3d3, Alix3d1 from PCEngine also use AMD Geode CPU. TS7800,TS7500 from Technologic Systems use ARM9 CPU. We select the Alix3d3 SBC which is shown in the Figure 3.1 and 3.2 whose specification is in Table 3.1

Table 3.1: *PC Engine: Hardware List.*

Hardware	**Specification**
alix3d3	500 Mhz AMD Geode LX800 single chip processor DRAM: 256 MB DDR DRAM Storage: CompactFlash socket Power: DC jack or passive POE, min. 7V to max. 20V Three LEDs Expansion: 2 miniPCI slots, LPC bus Connectivity: 1 Ethernet channel (Via VT6105M 10/100) I/O: DB9 serial port, dual USB, VGA, audio headphone out / microphone in RTC battery Board size: 100 x 160 mm Firmware: Award BIOS

Standard Case with 1 LAN, DC Jack, 2 SMA, DB9, 3Led 113 x 163 x 30cm

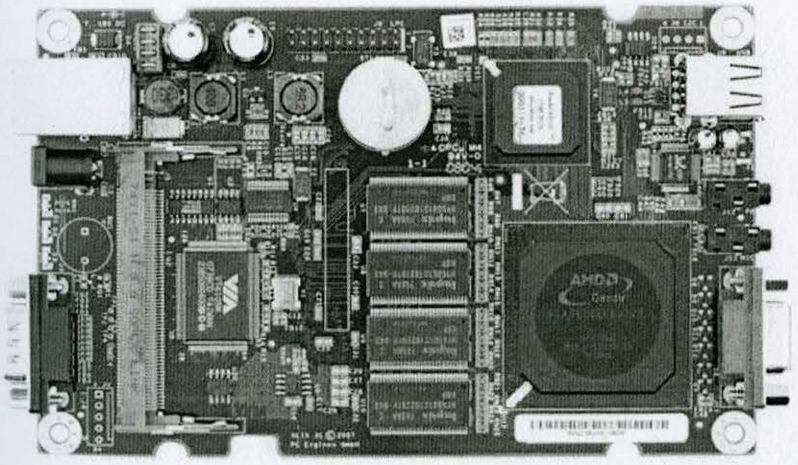


Figure 3.1: alix3d3 Board

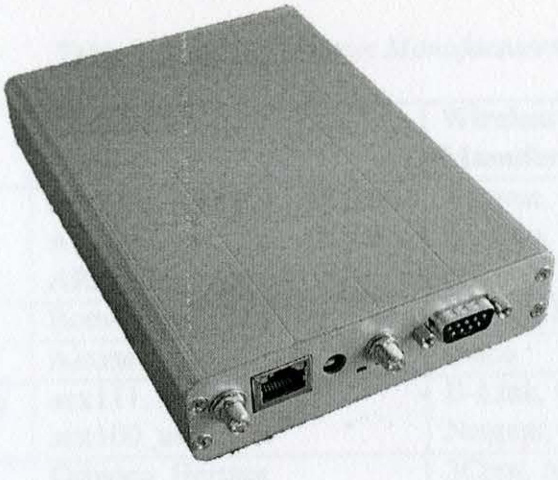


Figure 3.2: alix3d3 Box

3.3 Hardware Components

To be able to implement AP functionality on the selected hardware, a correct radio chipset that can support BSS Master operation mode, needs to be selected. There are plethora of radio chipset manufacturer. They are listed in the Table 3.2.

Among these various chipset, open source driver for these hardware are available. Such as

(a) HermesAP Driver: Hermes Chipset (http://hunz.org/hermesap.html)

(b) HostAP Driver : Prism 2/2.5/3 Chipset (http://hostap.epitest.fi)

(c) MADWiFi Driver : Atheros chipset (http://madwifi.sourceforge.net)

The selected hardware components are in Table 3.3 and selected radio chipset is shown in Figure 3.3

Figure 3.3: alix3d3 Radio Chipset

Table 3.2: List of Chipset Manufacturer.

Chipset Manufacturer	Chipset Code	Wireless Equipment Manufacturer
Atheros Communications	AR9002, AR9001, AR5008, AR5007, AR5006, AR5005, AR5002	Netgear, D-Link, and TRENDnet Wistron, Ubiquiti
Broadcom	Bcm43xx, BCM47xx	Applce, Belkin, Dell
Cisco Systems	Aironet	Cisco
Texas Instruments	acx111, acx100, acx100_usb	D-Link, US Robotics, Airlink, Netgear, Linksys
Alcatel-Lucent	Orinoco, Hermes Avaya	3Com, Apple, D-Link, Intel,
Intel	Intel PRO/Wireless (IPW) 2200BG/2915ABG/ 3945ABG/4965AGN	Dell, Intel
Realtek Semiconductor	RTL818x, RTL8187B	Netgear, Belkin, D-Link Linksys, Zonet
Ralink Technology	RT2500, RT2501, RT2600, RT2501USB, RT2800, rt2x00	Gigabyte Technology Linksys, D-Link, Belkin, Nintendo

Table 3.3: Hardware Components.

Component	Specification
Wireless Card	Mikrotik R52 802.11a/b/g multiband 2.312-2.497 or 4.920 -6.100GHz frequency
Compact Flash Card	Trancend 16GB CF type 1
Antenna	ANT-N-5 - Outdoor Omni Antenna, 5.5Dbi, N-Type

3.4 Operating System

There are so many varieties of free open source OS. These following OS are supported by PCEngine's product ie Alix Hardware mentioned on its website.

(a) FreeBSD : FreeBSD, FreeNAS, MonoWall, pfSense, STYX

(b) Linux : AstLinux, CentOS, DD-WRT, gOS 3 Gadgets, fili4l, IPCOP, IPFire,
LEAF Linux Embedded Appliance Firewall, Meshlium, OpenWRT,
Ubuntu Linux, Voyage Linux, Xubuntu Linux, Zeroshell

(c) NetBSD

(d) OpenBSD

(e) Mikrotik Router OS

Besides these different flavors of OS, there are also other compact customizable Linux distribution. Like Gentoo Minimal Edition, Slax, iMedia Embedded Linux: iMedia WRP, iMedia Linux, iMedia Alix Linux, iMedia MythTV , etc. iMedia Linux is a hybrid between small embedded distribution and full featured Linux distribution designed to work with AMD Geode LX/GX designed to enable developers to quickly create embedded or industrial computing products. Among the lightweight linux distribution are archLinux, SliTaz GNU/Linux.

For some APs, like Linksys WRT54g APs, we can reflash and install completely new firmware. The available firmware are Sveasoft, Newbroadcom, OpenWRT, eWRT, Wifi-box, Batbox, HyperWRT etc. Most of these varieties of operating system are designed for running open source software.

The choice of OS is open source operating system, Gentoo Linux which is build on top the Linux Kernel 2.6 For Gentoo Linux, source code needs to be compiled locally according to chosen configuration which makes it more flexible.

3.5 Software Application

There are so many flavors of OS, there are some already made application available. One of them is m0n0wall which is a complete, embedded firewall software package when used together with an embedded PC, provides all the features of commercial firewall boxes at a fraction of the price (nearly free).

m0n0wall distro is very unique and stands apart from many others because of its key features: all the configuration can be performed via a Web browser, the configuration is stored in a single XML text file that can be easily saved and restored via Web interface. It can be upgraded to a new versions via the Web interface. When m0n0wall is used as an access point, it has various functions: NAT, DHCP, DNS forwarder, SNMP agent, Traffic Shapper, PPPoE, PPTP, stateful packet filtering, Wirelss AP support.

In this thesis project, software platform is developed using the PHP programming language in the Eclipse development environment using PHP Development Tools (Eclipse PDT). The PHP programming language is used for server side web programming and java script is used for client side programming.

3.6 System Architecture

The software is not dependant on the local system. All the configuration are done from remote system utilizing a open source PHP ssh libraries. The hardware operates the MAC and physical layers of the protocol when implemented in the WLAN application however it can done upon installation of the proper drivers. Through webserver, the APs are connected via SSHv2 protocol and all the rest of commands for configuration and modifications are executed via SSH link which is shown in the Figure 3.4 and AC and WTP communicates through CAPWAP protocol.

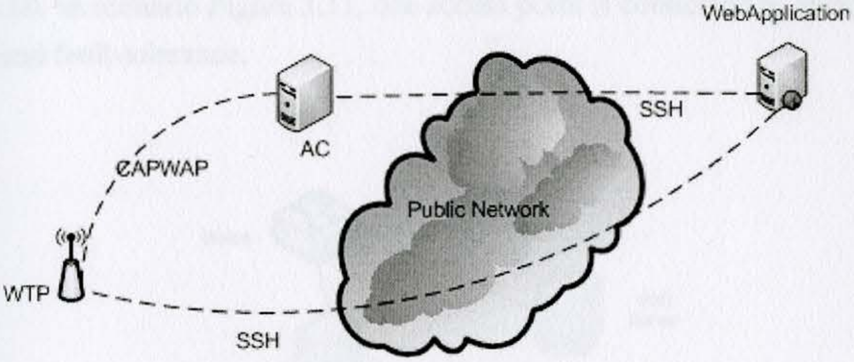


Figure 3.4: System Architecture

3.7 Different Scenarios of WLANs Deployment

In this section, typical deployment of WLANs are discussed. Although there are many WLAN deployment scenarios, Some typical deployments are shown as in following Figures 3.5, 3.6, 3.7, 3.8, 3.9, 3.10 and 3.11.

In Figure 3.5, small form factor customized Access points are used as well as separate web server is used for user interfaces for configuring the network. Its topology is based on extended service set (ESS). It is note connected to any Internet so, it is a private ESS. Scenario in Figure 3.6 is based on infrastructure mode, since it is extended and have the Internet access. In every infstructure topology, wireless should have access to the wired infrastructure. In Figure 3.6, router serves as the gateway to the ESS to get into the wired infrastructure. In these both scenarios, APs are connected to the AC through wired connection to the Ethernet switch.

Instead of small factor AP, we can use Laptop or PC as an APs, which is represented in the scenario in Figure 3.7. Laptops and PC can be configured as APs as long as they are supported by the radio chipset (Wireless Network Cards, WMIC) In another deployment scenario the web server can be kept out of a WLAN domain or can be public network because the web server can be accessed through out Internet. This configuration is depicted the scenario in Figure 3.8.This scenario is can be easily implemented because web service is hosted in standard port 80 and they are easily allowed by most of the firewalls. If we keep the AC outside the network or in the Internet, firewall may block the transmission of flow information from APs to the AC. APs can be directly connected to the AC through wired link or wireless link as shown in the Figure 3.9. Instead of a direct wireless connection to the AC, an AP can connect to another AP which has the direct wired link to the AC as in the Figure 3.10. In scenario Figure 3.11, one access point is connected to multiple AC for redundancy and fault-tolerance.

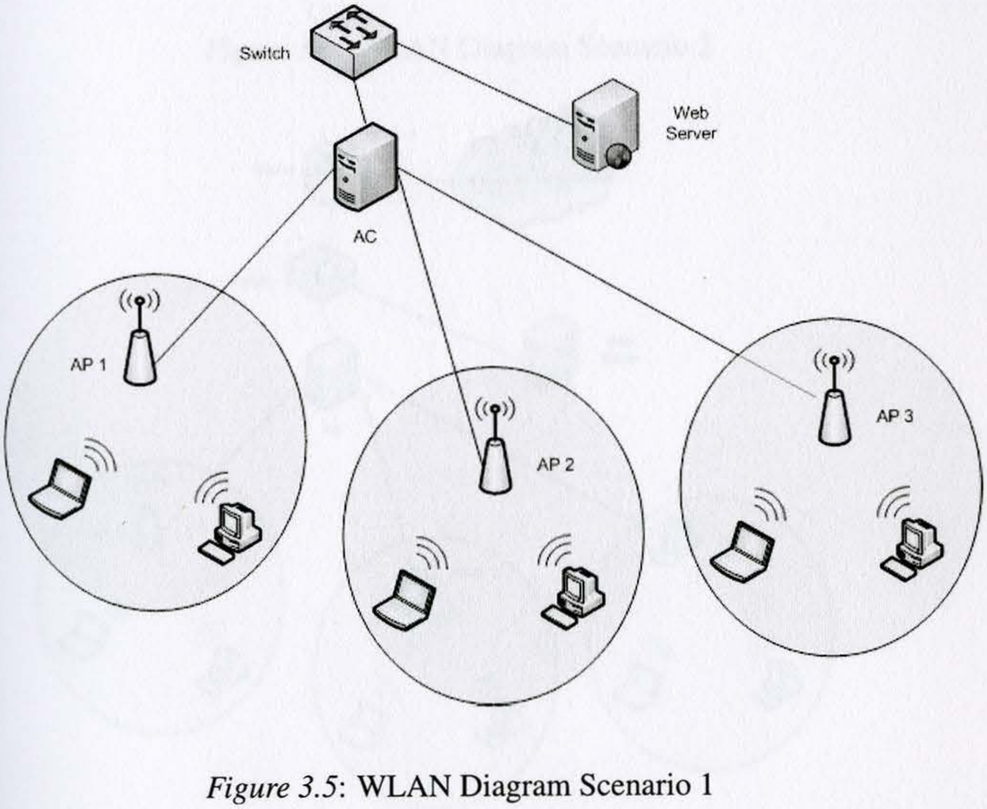


Figure 3.5: WLAN Diagram Scenario 1

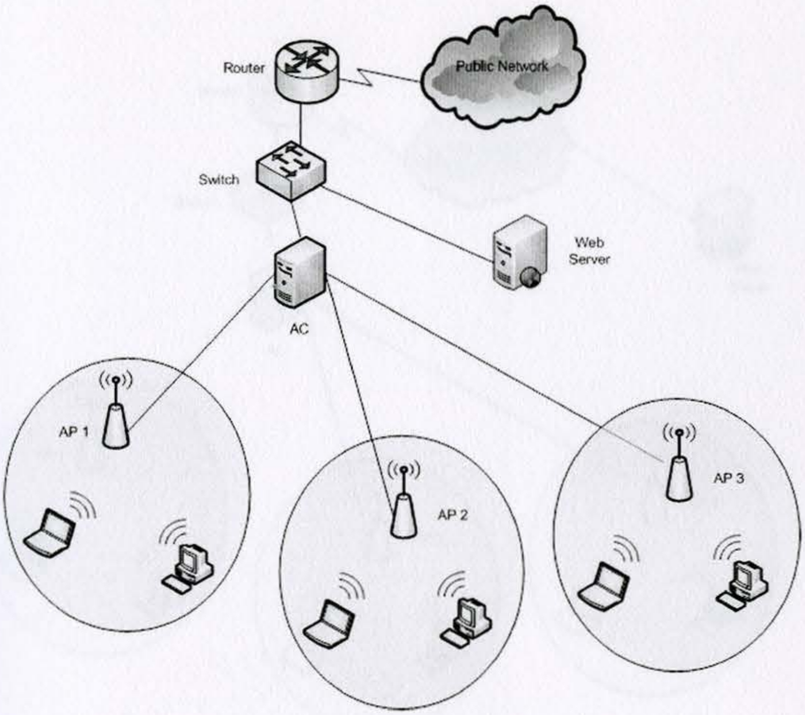


Figure 3.6: WLAN Diagram Scenario 2

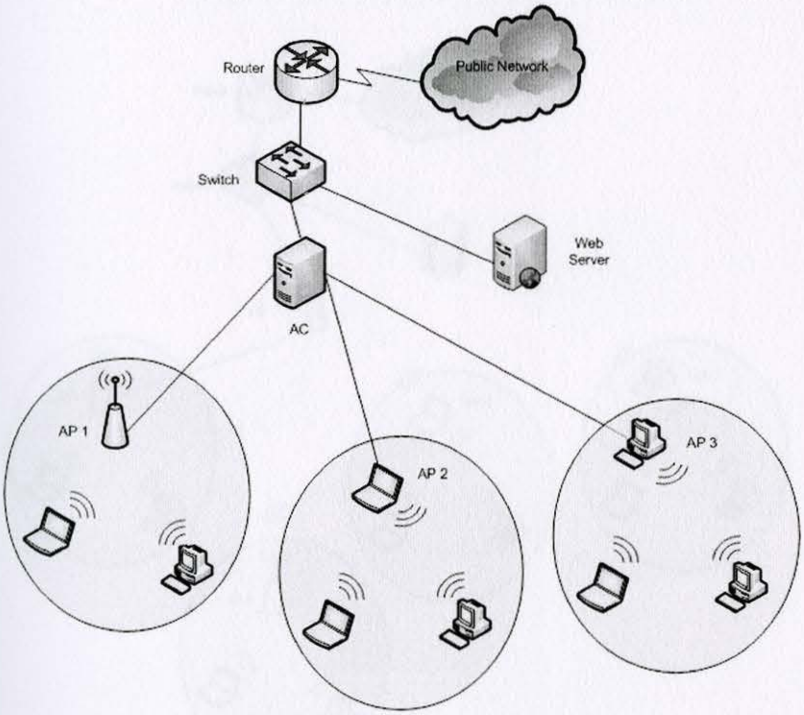


Figure 3.7: WLAN Diagram Scenario 3

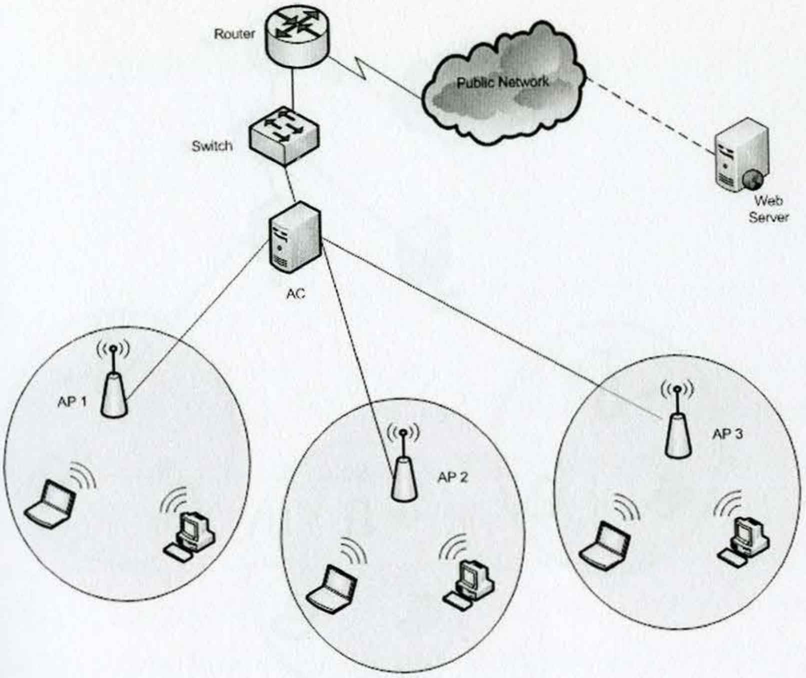


Figure 3.8: WLAN Diagram Scenario 4

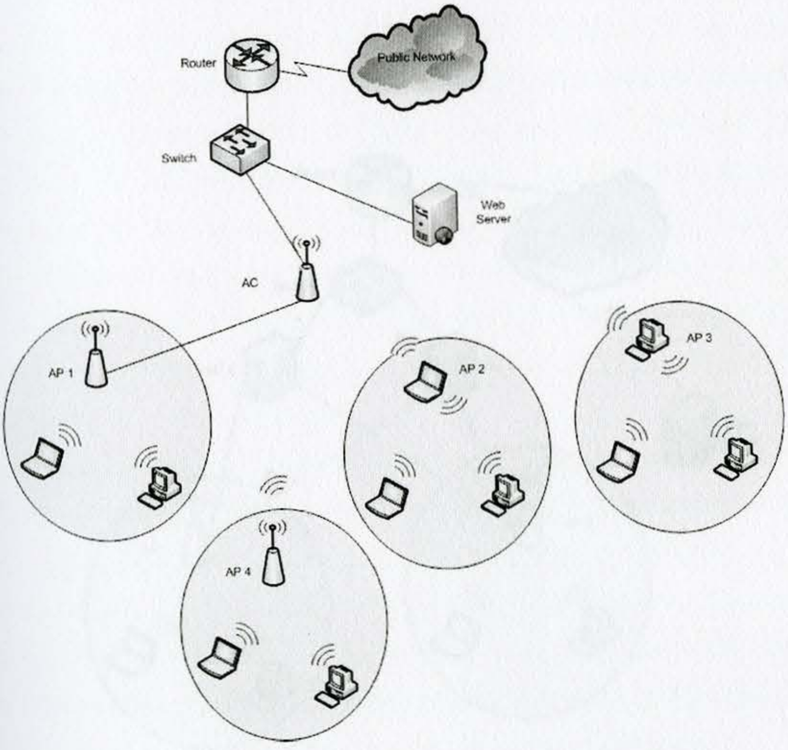


Figure 3.9: WLAN Diagram Scenario 5

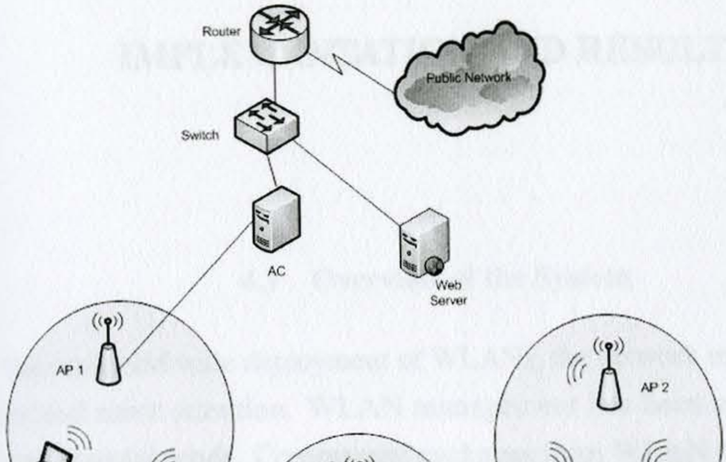


Figure 3.10: WLAN Diagram Scenario 6

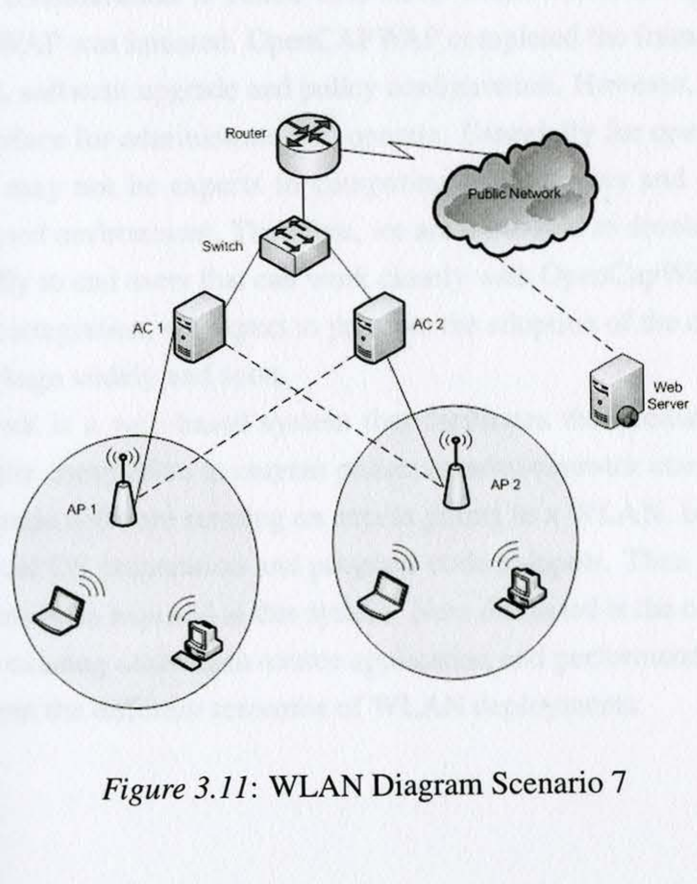


Figure 3.11: WLAN Diagram Scenario 7

Chapter 4

IMPLEMENTATION AND RESULTS

4.1 Overview of the System

Because of the rapid and wide deployment of WLANs, the network management of WLANs attracts more and more attention. WLAN management has been attempted in both open source and commercial mode. Commercial packages from WLAN equipment vendors like Cisco are normally expensive, which impedes the WLANs management in small business units. Meanwhile, because there was no standard for WLAN network management, the network management package from a vendor only works for its own products, which makes network upgrade difficult. Open source community tried to provide free WLAN management solutions. Due to inconsistence in configuration and the lack of standard, many open source projects faded away. Recently, IEEE is making an international standard for WLAN management to ease the effort in development of such management solutions. The standard in consideration is called CAPWAP. Meanwhile, an open source project called OpenCAPWAP was initiated. OpenCAPWAP completed the framework of collecting network statistics, software upgrade and policy configuration. However, it does not provide an graphical interface for administrators to operate. Especially for open source packages, many end users may not be experts in computing technologies and can not work in a command-line based environment. Therefore, we are motivated to develop an user interface framework friendly to end users that can work closely with OpenCapWap framework at the bottom. With the integration, we expect to promote the adoption of the open source WLAN management package widely and soon.

Our framework is a web-based system that facilitates the access and configuration remotely. With the completion in current phase, an administrator can configure network policies and upgrade software running on access points in a WLAN. In the following, we first discuss typical OS preparation and program code snippets. Then presented are open source software modules required in this system. Next discussed is the comparative analysis of platform with existing other open source application and performance of the system. At the end, we present the different scenarios of WLAN deployments.

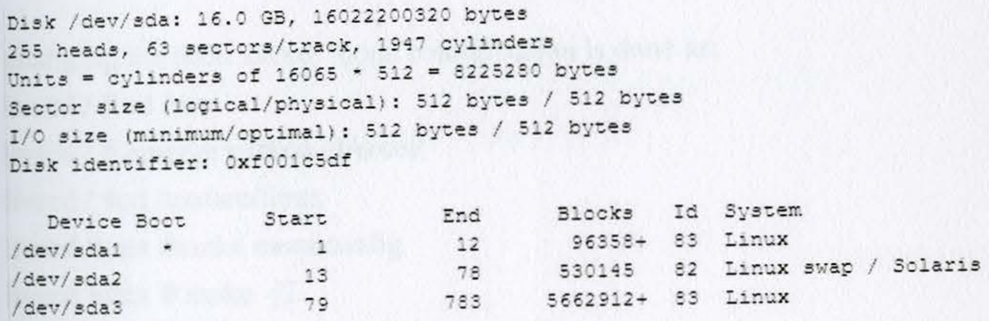
4.2 Hardware Platform

In Chapter 3, Alix3d3 SBC has been selected as the hardware platform. Mikrotik R52 is chosen as the WLAN adapter which is well supported by this hardware. This card is used for wireless connectivity between other Access Controller and Access Points. Genetoo Linux Distribution is selected as an open source OS and atheros chipset drivers can be configured in the Kernel module. Since Gentoo does not comes with precompiled binaries, it needs be compiled and installed. This can be done through remote connection via SSH shell.

4.3 Operating System Preparation

On the selected hardware platform, gentoo distribution is installed. Gentoo distribution is open source operating system without precompiled binaries which can be tuned to any hardware and only required packages can be installed as kernel module in the kernel configuration or source code can be fetched from gentoo repository via emerge command. The commands and procedures that are used to install the gentoo OS are as follows:

Gentoo install-x86-minimal-20100816.iso is burned in the USB flash drive. SBC is booted from USB flash drive. The partition are created as follows Figure4.1 through fdisk utility:



```
Disk /dev/sda: 16.0 GB, 16022200320 bytes
255 heads, 63 sectors/track, 1947 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xf001c5df

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1          12       96358+  83  Linux
/dev/sda2              13          78      530145   82  Linux swap / Solaris
/dev/sda3              79         783     5662912+  83  Linux
```

Figure 4.1: System Partitions

Created partition are formatted with the file system and swap partition is activated. Then file system is mounted

```
livecd #mkfs.ext2 /dev/sda1
livecd #mkfs.ext3 /dev/sda3
livecd #mkswap /dev/sda2  swapon /dev/sda2
livecd #mount /dev/sda3 /mnt/gentoo
livecd #mkdir /mnt/gentoo/boot
livecd #mount /dev/sda1 /mnt/gentoo/boot
livecd #cd /mnt/gentoo
```

After mounting the file system, the gentoo stage3 archives, latest portage snapshot are downloaded and unpacked.

```
livecd gentoo # wget ftp://distfiles.gentoo.org/pub/gentoo/releases/x86/current-stage3/
                    stage3-i686-*.tar.bz2
livecd gentoo #tar xjpf stage3*
livecd gentoo # wget http://distfiles.gentoo.org/snapshots/portage-latest.tar.bz2
livecd gentoo #tar xjf portage-lat*
```

Then root are changed to the mounted file systems.

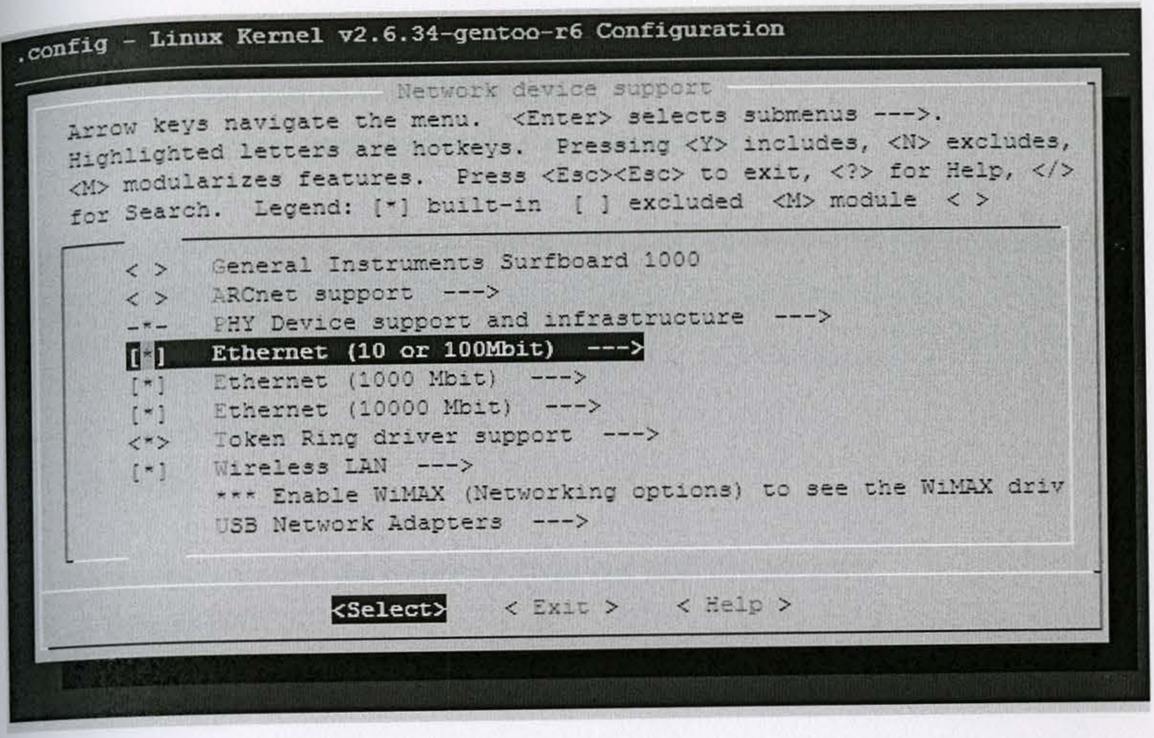
```
livecd gentoo # cd /
livecd / #mount -t proc proc /mnt/gentoo/proc
livecd / #mount -o bind /dev /mnt/gentoo/dev
livecd / #cp -L /etc/resolv.conf /mnt/gentoo/etc/
livecd / #chroot /mntgentoo /bin/bash
livecd / #env-update  source /etc/profile
livecd / #date
```

After changing the root, kernel mode configuration is done as:

```
livecd / # cd /etc
livecd / # emerge gentoo-sources
livecd / #cd /usr/src/linux
livecd linux #make menuconfig
livecd linux # make -j2
livecd linux # make modules_install
livecd linux # cp arch/i386/boot/bzImage /boot/kernel
```

By menuconfig command, required modules are choosed by selecting Menu options for example Device Drivers -> Network device support as shown in the Figure 4.2

```
livecd linux #cd /etc
livecd etc # nano -w fstab
    /dev/sda1   /boot   ext2    noauto,noatime   1 2
    /dev/sda3   /       ext3    noauto,noatime   0 1
    /dev/sda2   none    swap    noauto,noatime   0 0
livecd etc # cd conf.d
```



```
.config - Linux Kernel v2.6.34-gentoo-r6 Configuration
                         Network device support
  Arrow keys navigate the menu.  <Enter> selects submenus --->.
  Highlighted letters are hotkeys.  Pressing <Y> includes, <N> excludes,
  <M> modularizes features.  Press <Esc><Esc> to exit, <?> for Help, </>
  for Search.  Legend: [*] built-in  [ ] excluded  <M> module  < >

      < >   General Instruments Surfboard 1000
      < >   ARCnet support  --->
      -*-   PHY Device support and infrastructure  --->
      [*]   Ethernet (10 or 100Mbit)  --->
      [*]   Ethernet (1000 Mbit)  --->
      [*]   Ethernet (10000 Mbit)  --->
      <*>   Token Ring driver support  --->
      [*]   Wireless LAN  --->
            *** Enable WiMAX (Networking options) to see the WiMAX driv
            USB Network Adapters  --->

                  <Select>    < Exit >    < Help >
```

Figure 4.2: Ethernet and WLAN Module selection in Kernel Mode

```
livecd conf.d  echo ’config_eth0=( ’192.168.1.10/24’ )’ » net
livecd conf.d  echo ’routes_eth0=( ’default via 192.168.1.1’ )’ » net
livecd conf.d # echo ath_pci » /etc/modules.autoload.d/kernel-2.6
livecd conf.d # rc-update add sshd default
livecd conf.d # emerge grub
livecd conf.d # grub
grub>root (hd0,0)
grub>setup (hd0)
grub> quit
livecd conf.d # exit
livecd / #umount /mnt/gentoo/dev /mnt/gentoo/proc /mnt/gentoo/boot /mnt/gentoo
livecd / #reboot
```

4.3.1 Required Open Source Modules

To run the PC or SBC as an access point. It requires following modules:

a) openCAPWAP (http://sourceforge.net/projects/capwap/)

b) Madwifi Driver (http://madwifi-project.org/)

c) Bridge Utilities (https://launchpad.net/bridge-utils/+download)

d) Iptables (http://www.netfilter.org/projects/iptables/downloads.html)
e) Open SSH (http://www.openssh.com/)
f) Phpsec Library (http://phpseclib.sourceforge.net/)

For an web interface, to run an Open Management and Administration Platform, the followings are required:

a) Apache2 webserver
b) Open SSL
c) Open SSH Server
d) libssh2

For website development, the following Tools and platform are used:

a) Eclipse-PDT
b) Zend-debugger for PHP
c) PHP5.3.2
d) KompoZer
e) Javascript

4.4 System Requirement

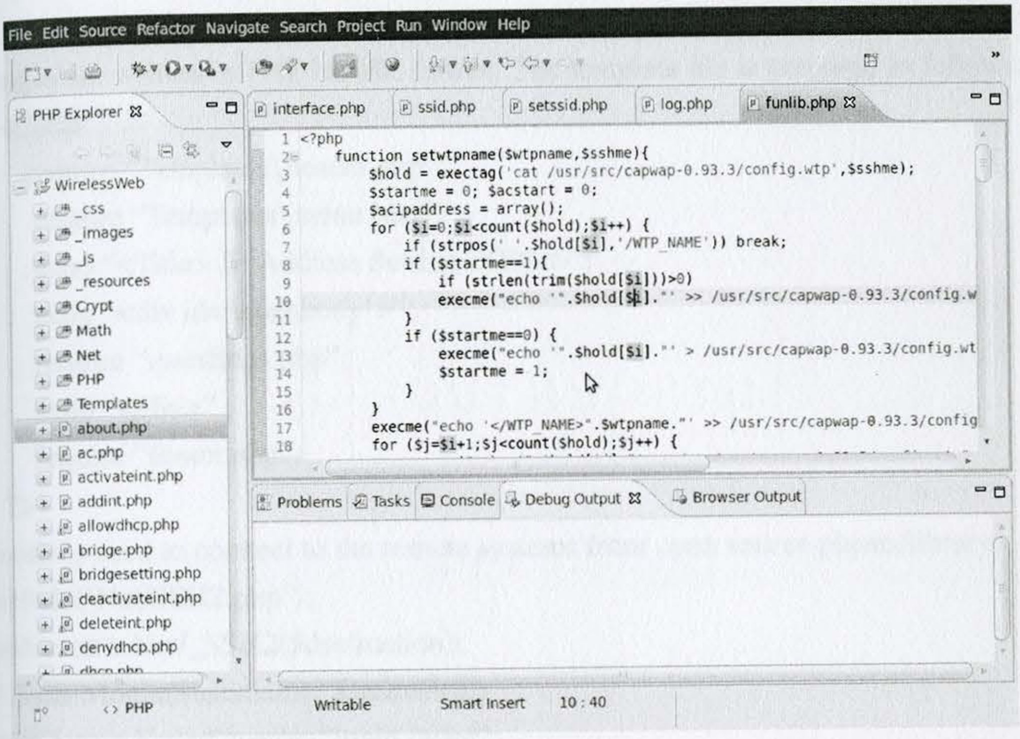
This application can run on Intel 586 processors, AMD 266MHz Geode processors with compatible WLAN cards with atheros chipset and 10/100 or 10/100/1000 Mbps ethernet cards. Minimum recommended RAM is 128MB and storage space is 4GB.

4.5 Hardware Compactibility

This application platform is designed to run openCAPWAP in AC or WTP mode, this requires ethernet interface (LAN cards) which connects to IP network. The LAN cards requires to be compatible with Linux systems. The WLAN cards require to support open source madwifi driver. In order to support madwifi driver, radio chipset should atheros chipset. Depending on the host hardware, ethernet LAN cards and WLAN cards should be miniPCI or PCMCIA or PCI cards.

4.6 Web Interface Development

The purpose of this thesis project is to develop the application for open management and administration of IEEE 802.11 network. This is written in PHP, HTML and JavaScript programming language. Choosing various open source utilities and libraries this application is developed. Among the various development environment, Eclipse-PDT is selected for program development environment. Snapshot of eclipse environment is shown in the Figure 4.3



```
<?php
    function setwtpname($wtpname,$sshme){
        $hold = exectag('cat /usr/src/capwap-0.93.3/config.wtp',$sshme);
        $startme = 0; $acstart = 0;
        $acipaddress = array();
        for ($i=0;$i<count($hold);$i++) {
            if (strpos(' '.$hold[$i],'/WTP_NAME')) break;
            if ($startme==1){
                if (strlen(trim($hold[$i]))>0)
                execme("echo '".$hold[$i]."' >> /usr/src/capwap-0.93.3/config.w
            }
            if ($startme==0) {
                execme("echo '".$hold[$i]."' > /usr/src/capwap-0.93.3/config.wt
                $startme = 1;
            }
        }
        execme("echo '</WTP_NAME>".$wtpname."' >> /usr/src/capwap-0.93.3/config
        for ($j=$i+1;$j<count($hold);$j++) {
```

Figure 4.3: Eclipse Development Platform

4.7 Program Snippets

This application is hosted from the Apache Web Server. The application consists of several pages and organized in multiple folder including seven subfolders and one main folder. It can be distributed in compressed tarball format and does not require separate installations although it has dependencies on some open source packages. The main folder is kept in the apache server root or hosting directory. The main important aspect of this application is Web application which do not need to be on the same access point. It can be on anywhere in the ip network which connects to the AP through the SSHs channel. So, it relies on IP connectivity.

The application is organized in different subfolders. It uses CSS style sheets, javascript and phpsec library. Php security libraries resides in PHP, net, Math and Crypt subfolders.

Javascript functions are kept in _js folder. The images are kept in _images folder. The php functions library are kept in _resources folder. This application uses templates for header, footer and menu which are kept inside Templates folder. And remaining pages for the web interface they reside on the main folder. Directory structure is also shown in the Figure 4.3. Some program snippets are discussed below.

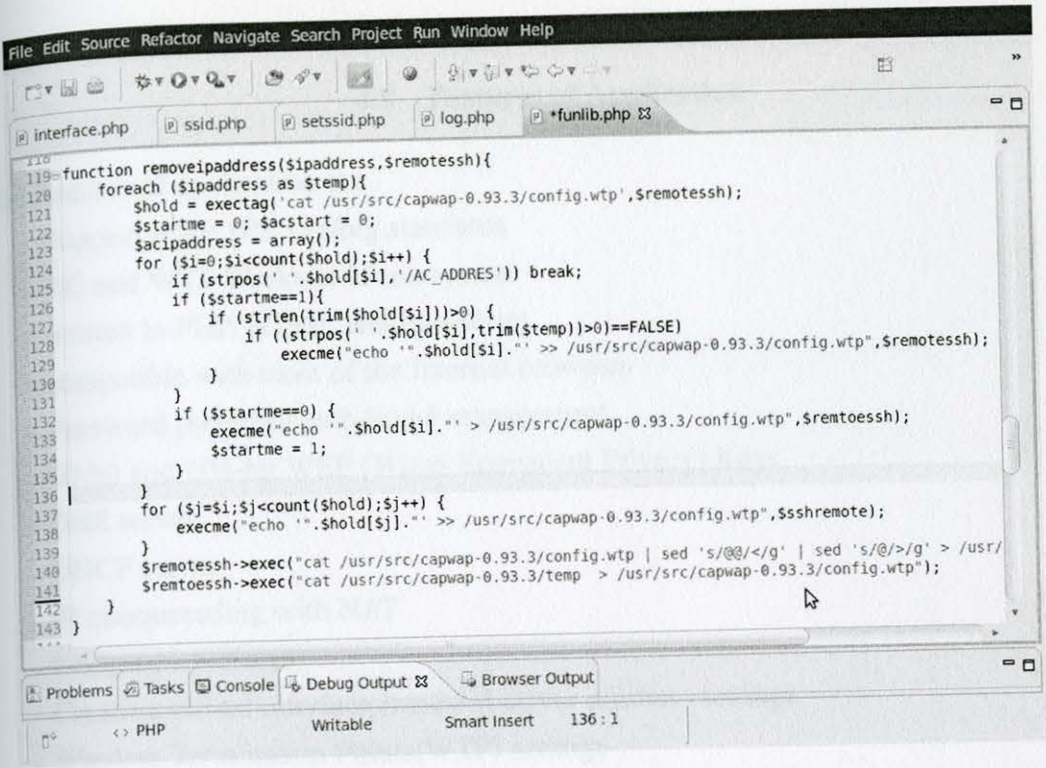
The pages are written in PHP HTML format. The template file is prepared as follows:

```
<?php
  require “Templates\header.php”;
   require “Templates\menu.php”;
   echo “<Title> IP Address Setting </Title>”;
   echo “<div id=’mainbody’>”;
   require “ipsettings.php”;
   echo “</div>” ;
   require “footer.php”;
?>
```

This code is used to connect to the remote systems from open source phpseclibrary:

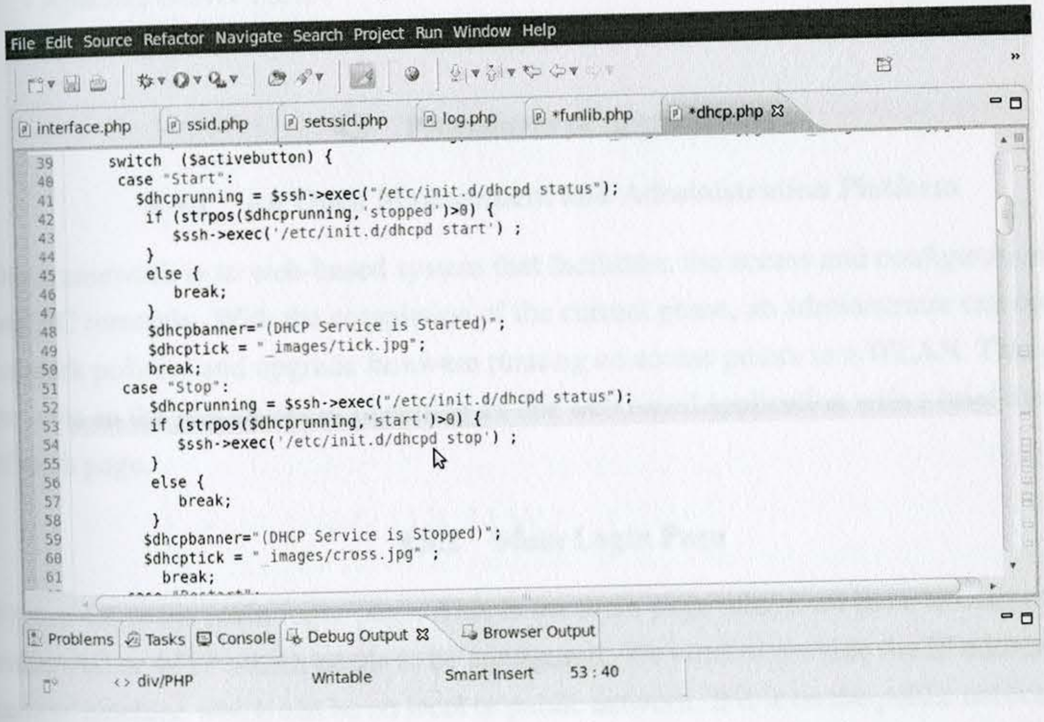
```
include(’Net/SSH2.php’);
$ssh = new Net/_SSH2($destination);
if ($ssh->login($username, $password))
exit(’Login Failed’); echo "login failed";
```

The function in Figure 4.4 is used to remove the IP address of AC in WTP settings configuration file. The code in Figure 4.5 is used to start, stopping the DHCP services.



```
function removeipaddress($ipaddress,$remotessh){
    foreach ($ipaddress as $temp){
        $hold = exectag('cat /usr/src/capwap-0.93.3/config.wtp',$remotessh);
        $startme = 0; $acstart = 0;
        $acipaddress = array();
        for ($i=0;$i<count($hold);$i++) {
            if (strpos(' '.$hold[$i],'/AC_ADDRES')) break;
            if ($startme==1){
                if (strlen(trim($hold[$i]))>0) {
                    if ((strpos(' '.$hold[$i],trim($temp))>0)==FALSE)
                        execme("echo '".$hold[$i]."' >> /usr/src/capwap-0.93.3/config.wtp",$remotessh);
                }
            }
            if ($startme==0) {
                execme("echo '".$hold[$i]."' > /usr/src/capwap-0.93.3/config.wtp",$remtoessh);
                $startme = 1;
            }
        }
        for ($j=$i;$j<count($hold);$j++) {
            execme("echo '".$hold[$j]."' >> /usr/src/capwap-0.93.3/config.wtp",$sshremote);
        }
        $remotessh->exec("cat /usr/src/capwap-0.93.3/config.wtp | sed 's/@@/</g' | sed 's/@/>/g' > /usr/
        $remtoessh->exec("cat /usr/src/capwap-0.93.3/temp  > /usr/src/capwap-0.93.3/config.wtp");
    }
}
```

Figure 4.4: Program Snippet 1



```
    switch  ($activebutton) {
     case "Start":
       $dhcprunning = $ssh->exec("/etc/init.d/dhcpd status");
        if (strpos($dhcprunning,'stopped')>0) {
           $ssh->exec('/etc/init.d/dhcpd start') ;
        }
        else {
           break;
        }
        $dhcpbanner="(DHCP Service is Started)";
        $dhcptick = "_images/tick.jpg";
        break;
      case "Stop":
        $dhcprunning = $ssh->exec("/etc/init.d/dhcpd status");
        if (strpos($dhcprunning,'start')>0) {
           $ssh->exec('/etc/init.d/dhcpd stop') ;
        }
        else {
           break;
        }
       $dhcpbanner="(DHCP Service is Stopped)";
       $dhcptick = "_images/cross.jpg" ;
         break;
```

Figure 4.5: Program Snippet 2

4.8 Features of Application

The features of application are

- Support IEEE 802.11a/b/g standards
- AC and WTP Works in Linux system
- written in PHP, HTML and JavaScript
- compatible with most of the Internet browsers
- Password protected web-based management
- 40-bit and 104-bit WEP (Wired Equivalent Privacy) Keys
- DNS server
- DHCP server
- IP masquerading with NAT
- Bridging interfaces
- Creating virtual interface (madwifi driver utilities) settings
- Wireless Termination Points(WTP) settings
- Access Controller(AC) Settings
- Apache2 Server 2.2.14
- open SSHv2

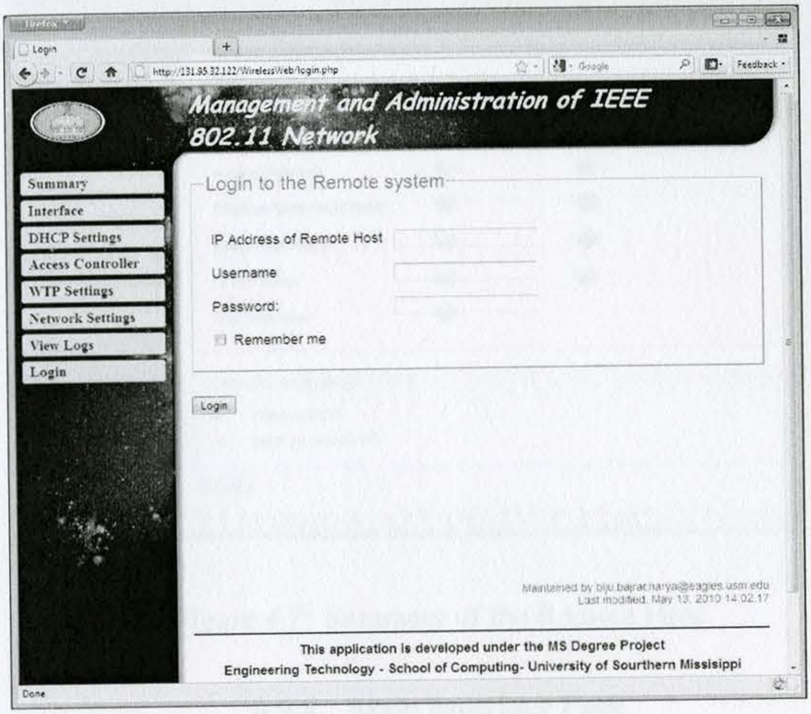
4.9 Procedures of Applications

4.9.1 An Open Management and Administration Platform

Our framework is to web-based system that facilitates the access and configuration of AP and AC remotely. With the completion of the current phase, an administrator can configure network policies and upgrade firmware running on access points in a WLAN. This chapter presents an the procedures of operating an this web based application with a brief discussion of each page.

4.9.2 Main Login Page

Figure 4.6 is the main login page. This is the main page where we have to connect to the either AC or WTP which needs to be configured. We need to provide the IP address of the remote machine which can be on local or public network. If it is on the public network, there should be IP connectivity. We can provide either IP address or fully qualified domain name that can be resolved by the DNS server. Since we need to change the system parameter on the Operating System, we may not have user rights to access those resources. So we have to use the user name that has rights on wireless tools and network utilities. The login method is secure because it connects to the remote system via secure shell (SSH version 2) and the whole the session and execution of commands are executive through this SSHv2 protocol. AC and WTP can on the same machine.



Management and Administration of IEEE 802.11 Network

Login to the Remote system

IP Address of Remote Host

Username

Password:

□ Remember me

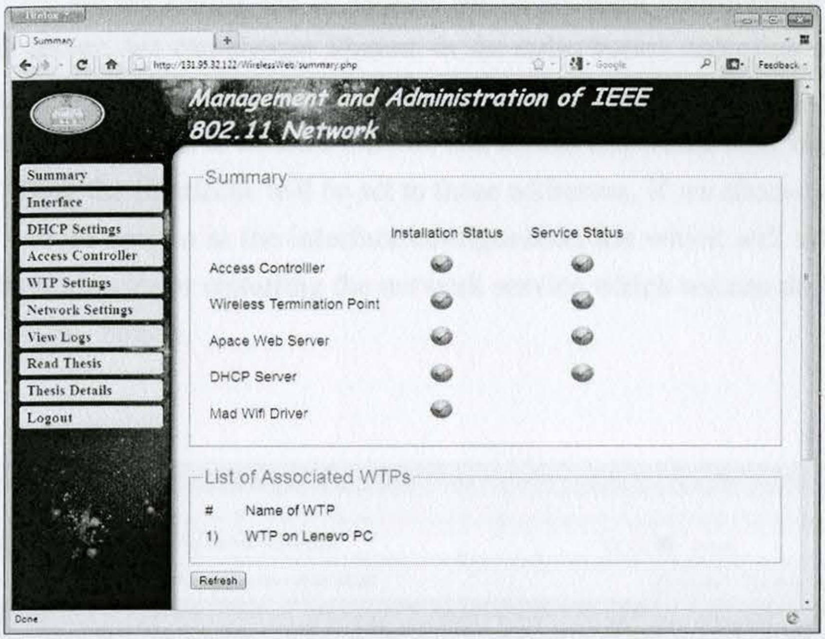
Maintained by biju.bajracharya@eagles.usm.edu
Last modified: May 13, 2010 14:02:17

This application is developed under the MS Degree Project
Engineering Technology - School of Computing- University of Sourthern Missisippi

Figure 4.6: Main Login Page

4.9.3 System Summary Page

Once the login is successful, it will presents the summary page as shown in the Figure 4.7. In the summary page, we can get the snapshots of whether the AC, WTP, Apache Web Server, DHCP server and madwifi driver are installed or not. These are the basic requirement for AC and optionally we can also host the web service through that machine. Web Interface can be hosted from anywhere, it doesn't necessary to be in the same AC or WTP. If those components are not installed then we need to install them first to execute AC or WTP. Then it will check whether those installed components are running or not and are presented in the left column. If the services are not running then we can go to Access Controller or WTP Settings page to start those services. Also in the second box, if it is an AC, it will show the connected WTPs.



Management and Administration of IEEE 802.11 Network

Summary

	Installation Status	Service Status
Access Controller	●	●
Wireless Termination Point	●	●
Apace Web Server	●	●
DHCP Server	●	●
Mad Wifi Driver	●	

List of Associated WTPs

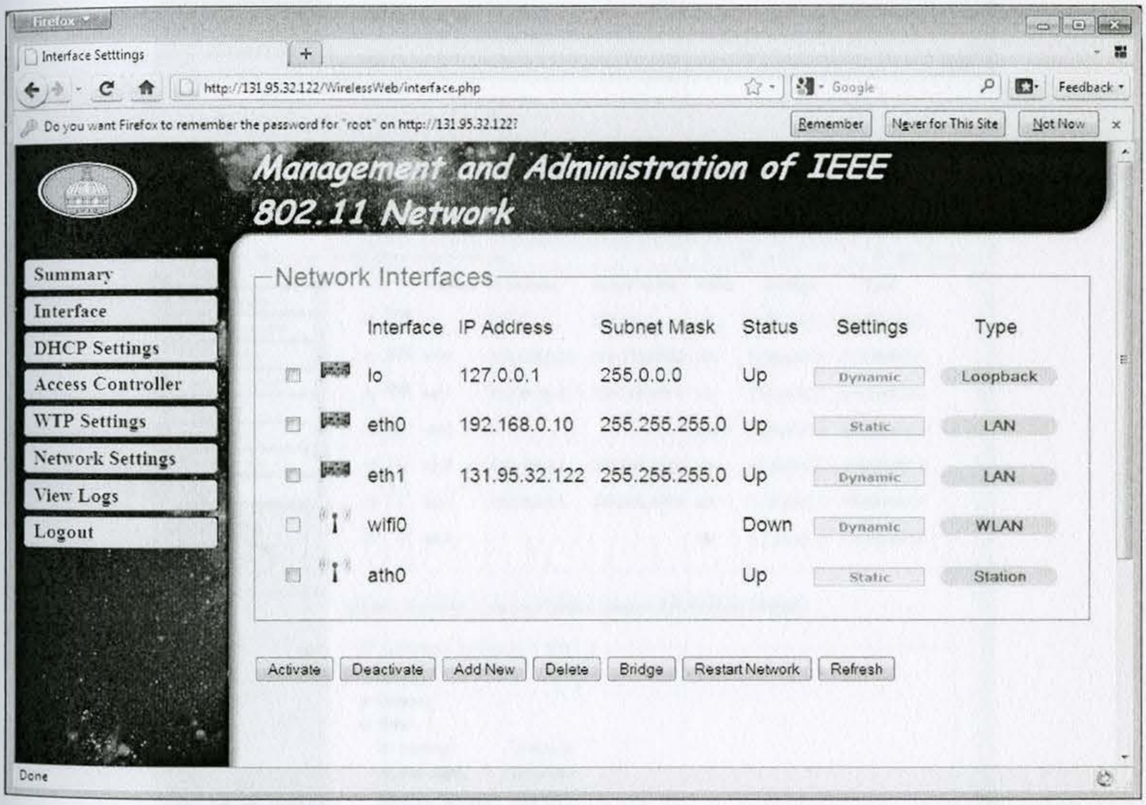
#	Name of WTP
1)	WTP on Lenevo PC

Figure 4.7: Summary of the Remote Host

4.9.4 Main Interface Page

Main interface page used to create, destroy, adding new AP, Stations, bridging, IP Settings, Wireless Scanning. On this page, we create or destroy the interfaces are done is the Interface page which is shown in the Figure 4.8. List of available Physical interfaces and their status are shown. If they are Ethernet card or wireless network card they are represented by the icons in front of their names. If the status of these Interface are down. We can enable them by activating them as shown in the Figure 4.9. To activate them, we can select multiple interfaces on the right side by selected the checkboxes. By activating these interfaces, they will bring up to live. Similarly we can also deactivate them. If the IP address is not shown in right next the interface name or in IP address column, they should be provided with the IP address either in a manual or dynamic or static methods. Dynamic and Static configurations are written in configuration files which will be activated by restarting the network services. If it is manual, it will directly take effect and the interface become live. So, to participate on the network communication, each interface should have IP address and status must be up. In the Settings column it shows whether it is dynamically set or manual or statically set.

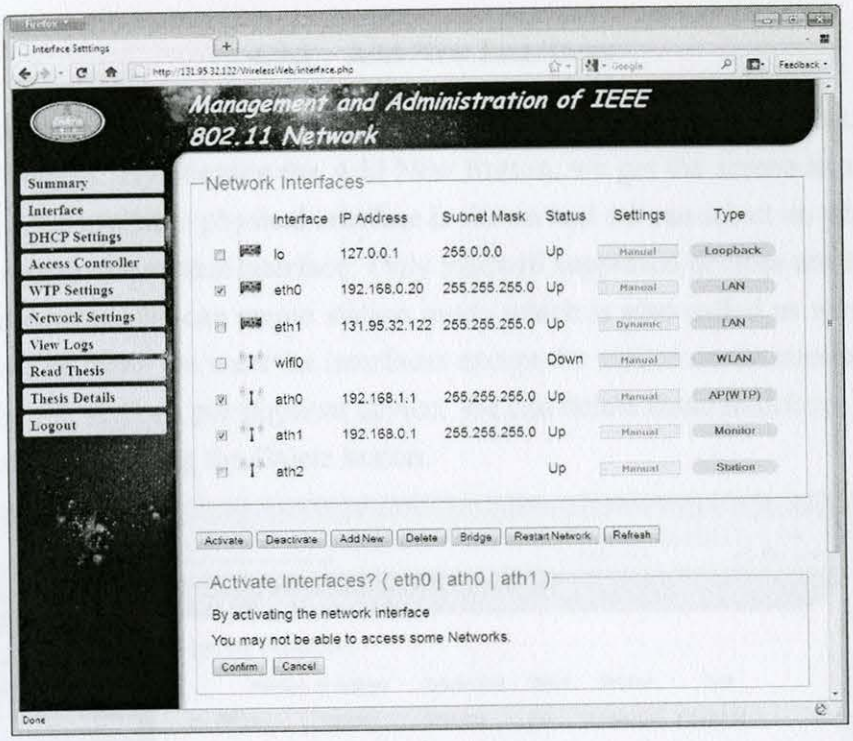
To change or set the new IP settings, we can click the corresponding buttons whose labels are "Static", "Dynamic" or "Manual" then it will bring up the IP Settings box as show in the Figure 4.10. It will also shows the interface name in its heading, so that we know on which interface we are setting the IP address for. If we want immediately the IP address from DHCP server. we can choose Manual in the radio button and click apply, then will send out the dhcp request and shows in the upper box if it gets the reply from DHCP server. If we want to give our own IP address then we can fill the text boxes with the addresses then click apply. Then the interfaces will be set to those addresses. If we choose either Dynamic or Static it will be written in the interface configuration file which will take effect either restarting the computer or restarting the network service which we can do by clicking the "Restart Network" button.



Network Interfaces

		Interface	IP Address	Subnet Mask	Status	Settings	Type
□		lo	127.0.0.1	255.0.0.0	Up	Dynamic	Loopback
□		eth0	192.168.0.10	255.255.255.0	Up	Static	LAN
□		eth1	131.95.32.122	255.255.255.0	Up	Dynamic	LAN
□		wifi0			Down	Dynamic	WLAN
□		ath0			Up	Static	Station

Figure 4.8: Interface Settings Main Screen



Network Interfaces

	Interface	IP Address	Subnet Mask	Status	Settings	Type
□	lo	127.0.0.1	255.0.0.0	Up	Manual	Loopback
☑	eth0	192.168.0.20	255.255.255.0	Up	Manual	LAN
□	eth1	131.95.32.122	255.255.255.0	Up	Dynamic	LAN
□	wifi0			Down	Manual	WLAN
☑	ath0	192.168.1.1	255.255.255.0	Up	Manual	AP(WTP)
☑	ath1	192.168.0.1	255.255.255.0	Up	Manual	Monitor
□	ath2			Up	Manual	Station

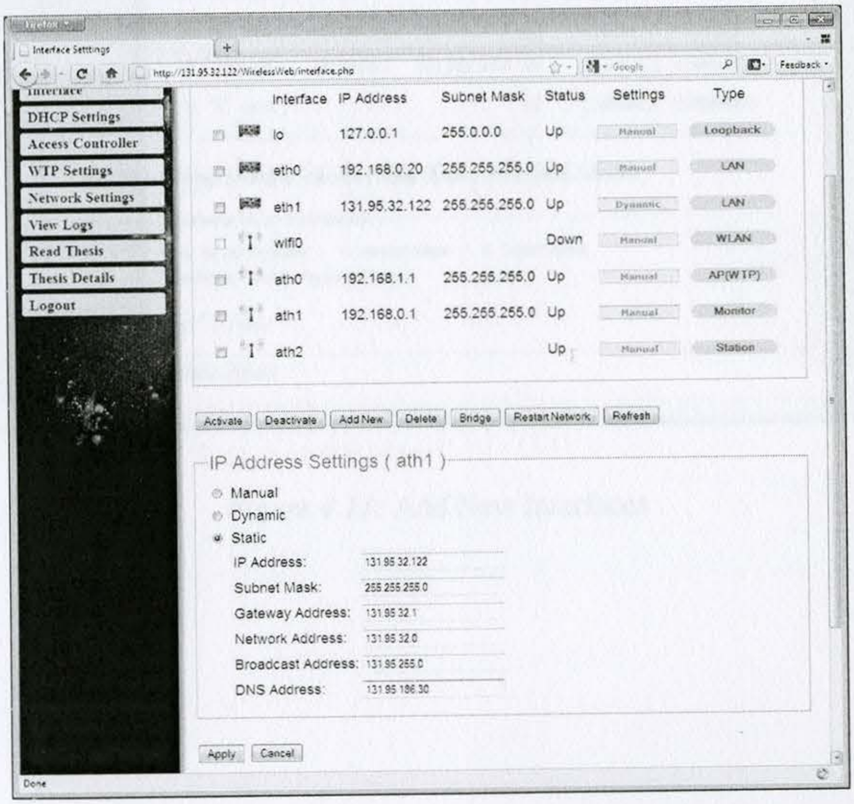
Activate Interfaces? (eth0 | ath0 | ath1)

By activating the network interface

You may not be able to access some Networks.

Confirm Cancel

Figure 4.9: Activate Interfaces



	Interface	IP Address	Subnet Mask	Status	Settings	Type
□	lo	127.0.0.1	255.0.0.0	Up	Manual	Loopback
□	eth0	192.168.0.20	255.255.255.0	Up	Manual	LAN
□	eth1	131.95.32.122	255.255.255.0	Up	Dynamic	LAN
□	wifi0			Down	Manual	WLAN
□	ath0	192.168.1.1	255.255.255.0	Up	Manual	AP(WTP)
□	ath1	192.168.0.1	255.255.255.0	Up	Manual	Monitor
□	ath2			Up	Manual	Station

IP Address Settings (ath1)

○ Manual
○ Dynamic
● Static

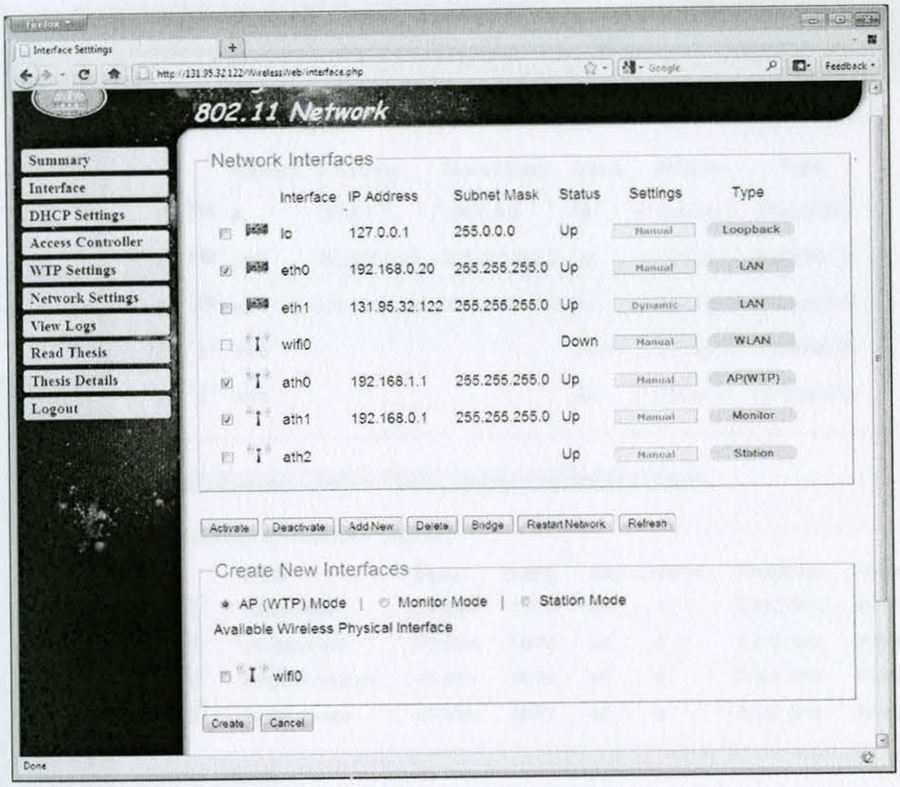
IP Address: 131.95.32.122
Subnet Mask: 255.255.255.0
Gateway Address: 131.95.32.1
Network Address: 131.95.32.0
Broadcast Address: 131.95.255.0
DNS Address: 131.95.186.30

Apply Cancel

Figure 4.10: Interface Settings

4.9.5 Add New Interfaces

In this section of this page, we can create new interfaces for Access Points, or Stations or Monitor Modes. By clicking the Add New Button, we get the screen as shown in the Figure 4.11. The available physical interface is shown and we can select on which physical interface to create the virtual interface. Only madwifi supported devices are shown in this section of the page. We can create station mode which is also called as wireless clients. We can create as many we want the interfaces except the station mode interface. It can be created only one stations per physical device. We can delete these interfaces by selecting the interfaces and clicking the Delete button.



Network Interfaces

	Interface	IP Address	Subnet Mask	Status	Settings	Type
□	lo	127.0.0.1	255.0.0.0	Up	Manual	Loopback
☑	eth0	192.168.0.20	255.255.255.0	Up	Manual	LAN
□	eth1	131.95.32.122	255.255.255.0	Up	Dynamic	LAN
□	wifi0			Down	Manual	WLAN
☑	ath0	192.168.1.1	255.255.255.0	Up	Manual	AP(WTP)
☑	ath1	192.168.0.1	255.255.255.0	Up	Manual	Monitor
□	ath2			Up	Manual	Station

Create New Interfaces

● AP (WTP) Mode | ○ Monitor Mode | ○ Station Mode

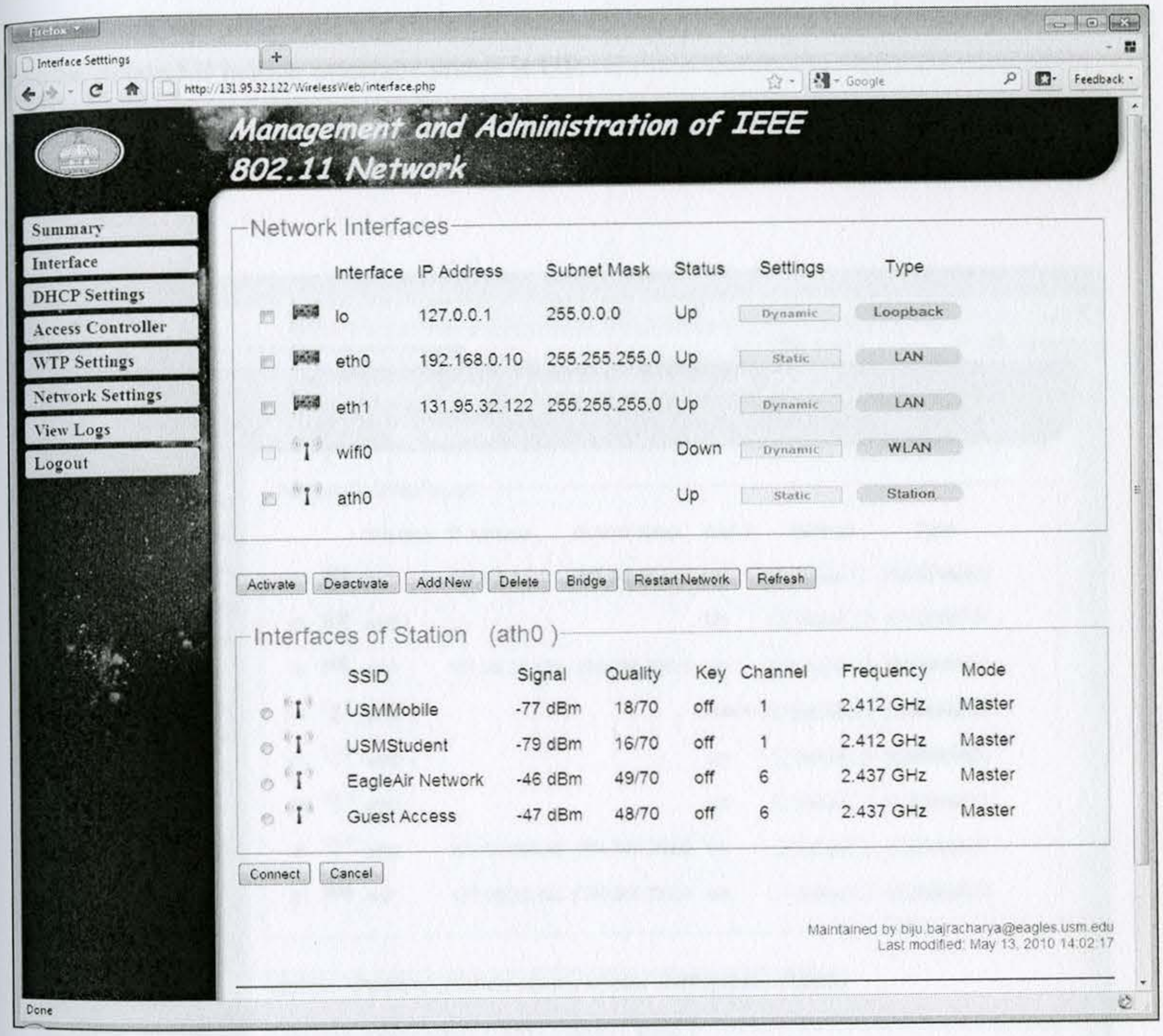
Available Wireless Physical Interface

□ wifi0

Figure 4.11: Add New Interfaces

4.9.6 Wireless Scanning

Only the station mode interface can scan the available networks. By clicking on the Station button in the Type column in the top page, it will shown the Figure 4.12. We can select the interface that we want to connect and by clicking on Connect button, it will try to connect to that Wireless Network. To disconnect from the network, we can deactivate the interface.



Network Interfaces

	Interface	IP Address	Subnet Mask	Status	Settings	Type
☐	lo	127.0.0.1	255.0.0.0	Up	Dynamic	Loopback
☐	eth0	192.168.0.10	255.255.255.0	Up	Static	LAN
☐	eth1	131.95.32.122	255.255.255.0	Up	Dynamic	LAN
☐	wifi0			Down	Dynamic	WLAN
☐	ath0			Up	Static	Station

Interfaces of Station (ath0)

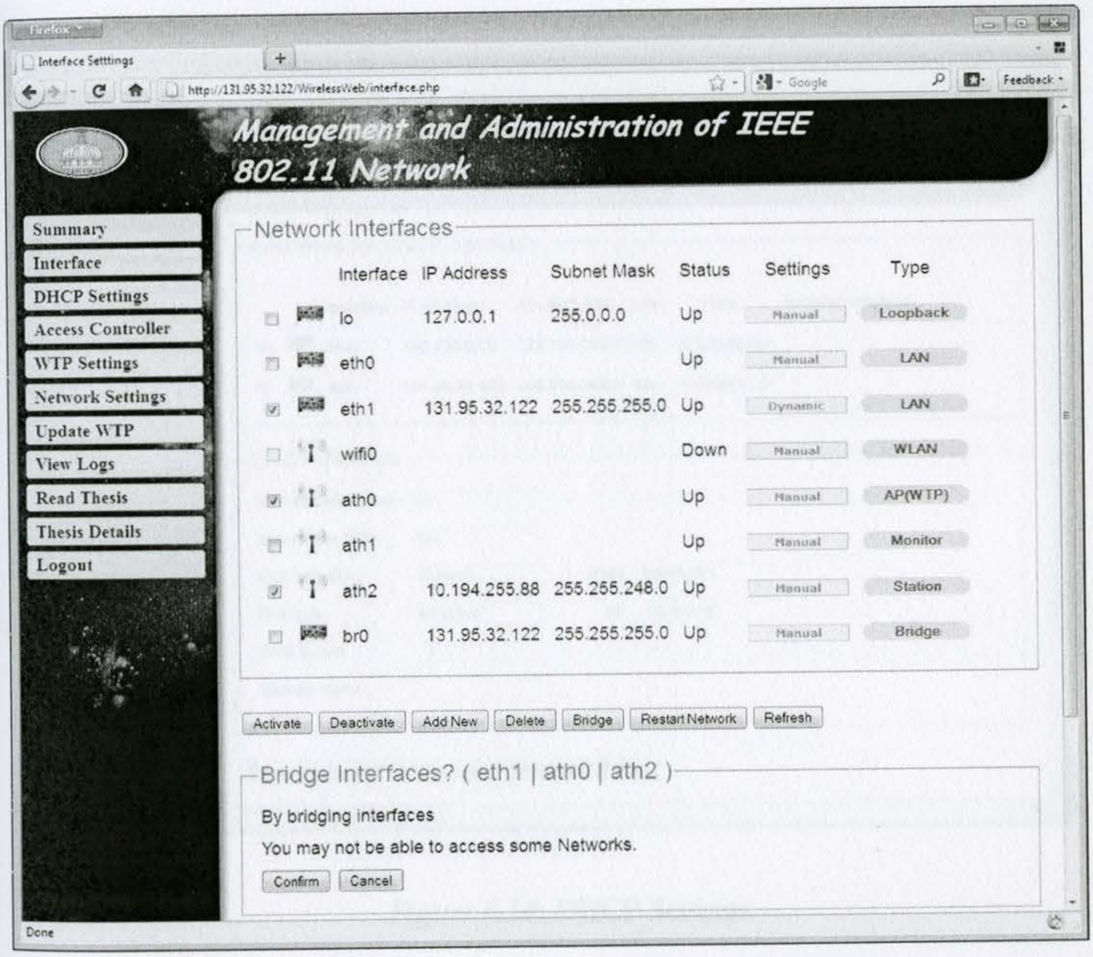
	SSID	Signal	Quality	Key	Channel	Frequency	Mode
○	USMMobile	-77 dBm	18/70	off	1	2.412 GHz	Master
○	USMStudent	-79 dBm	16/70	off	1	2.412 GHz	Master
○	EagleAir Network	-46 dBm	49/70	off	6	2.437 GHz	Master
○	Guest Access	-47 dBm	48/70	off	6	2.437 GHz	Master

Maintained by biju.bajracharya@eagles.usm.edu
Last modified: May 13, 2010 14:02:17

Figure 4.12: Wireless Scanning

4.9.7 Bridging Interfaces

We can bridge the multiple interface by selecting the interfaces in the left column then by clicking the "Bride Button" we get the Screen as shown in Figure 4.13. The physical interface of madwifi driver prefix with WiFi can not be bridged to any other interfaces. Once we bridge the interfaces, it will automatically generate a new bridged interfaces. All these selected interfaces will be bridged together to this new bridge interface. And we can activate, deactivate and apply IP settings as we do to the other interfaces. If we delete the bridge interfaces, it will automatically removes those selected interfaces from bridge group. Bridge can be deleted if bridge interface status is UP.



Network Interfaces

	Interface	IP Address	Subnet Mask	Status	Settings	Type
□	lo	127.0.0.1	255.0.0.0	Up	Manual	Loopback
□	eth0			Up	Manual	LAN
☑	eth1	131.95.32.122	255.255.255.0	Up	Dynamic	LAN
□	wifi0			Down	Manual	WLAN
☑	ath0			Up	Manual	AP(WTP)
□	ath1			Up	Manual	Monitor
☑	ath2	10.194.255.88	255.255.248.0	Up	Manual	Station
□	br0	131.95.32.122	255.255.255.0	Up	Manual	Bridge

Bridge Interfaces? (eth1 | ath0 | ath2)

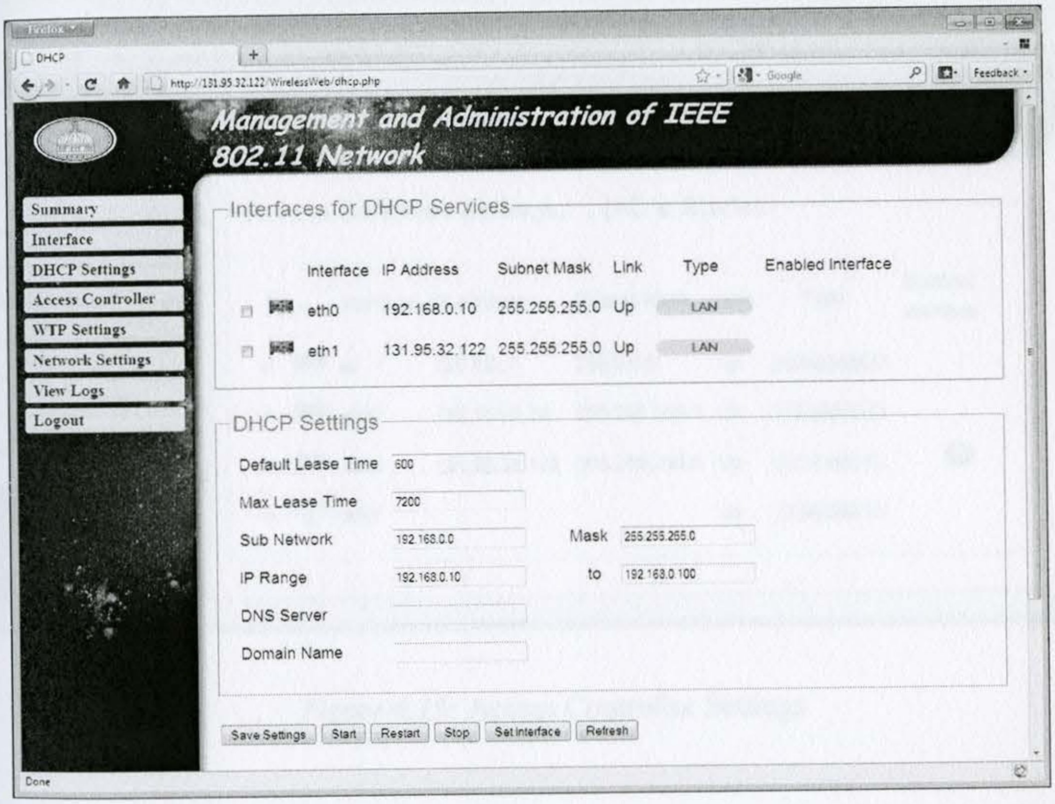
By bridging interfaces

You may not be able to access some Networks.

Figure 4.13: Interface Bridging

4.9.8 DHCP Server Settings Page

In this page, DHCP settings, staring, stopping and restarting the DHCP services are done. It also shows the interfaces that can be used for DHCP service as shown in the Figure 4.14. The currently set interface for DHCP service announced are show in the Enabled Interface Column with either cross or tick mark. Cross Mark means it is selected for DHCP service but DHCP service is not running. If it has green tick mark, then the DHCP is currently running and announcing its service through that interfaces. The DHCP parameters can be set in the bottom box of this page. After providing the parameters we need to click Save Settings. To take effect on these parameters we need to restart the DHCP Services. We need to click the Set Interface button to save the interface for DHCP. Once the DHCP service is enabled and started. We can see the DHCP leases at the bottom of the page.



Interfaces for DHCP Services

	Interface	IP Address	Subnet Mask	Link	Type	Enabled Interface
□	eth0	192.168.0.10	255.255.255.0	Up	LAN	
□	eth1	131.95.32.122	255.255.255.0	Up	LAN	

DHCP Settings

Default Lease Time 600

Max Lease Time 7200

Sub Network 192.168.0.0 Mask 255.255.255.0

IP Range 192.168.0.10 to 192.168.0.100

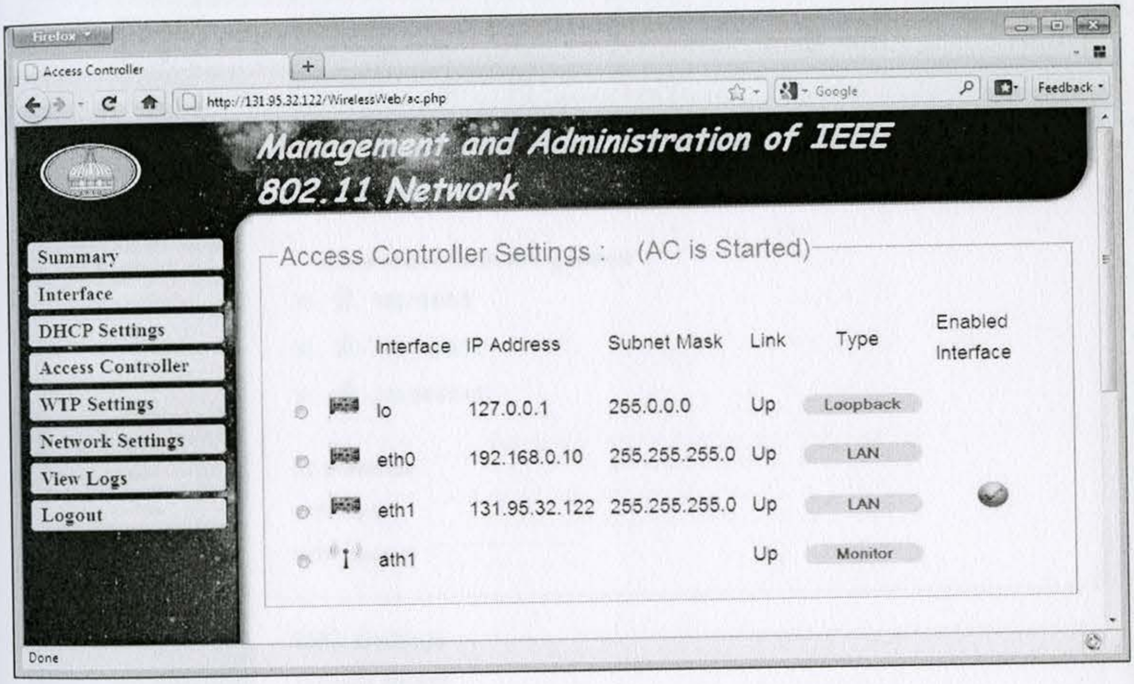
DNS Server

Domain Name

Figure 4.14: DHCP Settings

4.9.9 Access Controller Settings

In this page, Access Controller Service is set and started. On the left column, it will show the list of interfaces which can support the Access Controller as shown in the Figure 4.15. We can choose Loopback interface as well as bridge interface for announcing the AC service. Only through one interface AC can be set to announce its service. The currently selected interface will be shown in the right most column either by green tick mark icon or red cross mark icon. Green tick mark represents that AC is currently running and Red cross mark means currently set to that interface but not started. We can start or restart the AC service by clicking the Start or Restart button.



Management and Administration of IEEE 802.11 Network

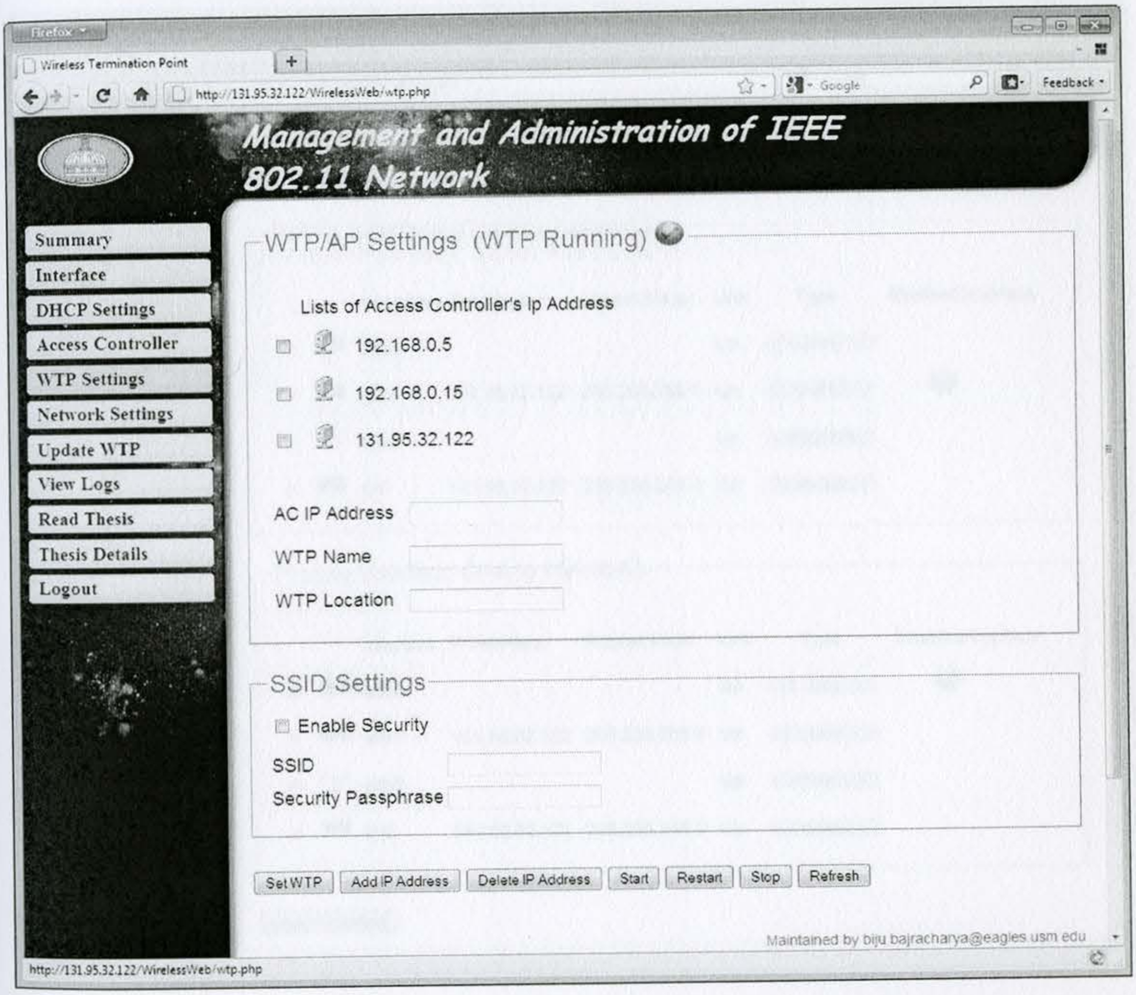
Access Controller Settings : (AC is Started)

		Interface	IP Address	Subnet Mask	Link	Type	Enabled Interface
○		lo	127.0.0.1	255.0.0.0	Up	Loopback	
○		eth0	192.168.0.10	255.255.255.0	Up	LAN	
○		eth1	131.95.32.122	255.255.255.0	Up	LAN	✓
○		ath1			Up	Monitor	

Figure 4.15: Access Controller Settings

4.9.10 Wireless Termination Points

Wireless Termination Points, also called as Access Points, settings can be set on this page as shown in the Figure 4.16. We need to set the Access Controller's IP address to seek for. WTP can connect to the multiple ACs. So we can add more AC's IP address. WTP will search the AC services on these mentioned IP address, if not it will try to connect to another AC. By setting the WTP we can create the SSID and passphrase for this WTP. Once we choose the IP addresses we need to either start or restart the WTP service. By clicking the SetWTP button it will set the name and location of the WTP. By clicking the ADD IP Address button it append the IP addresses to its list. We can delete the IP addresses that are already saved by clicking the Delete IP Address.



Wireless Termination Point

http://131.95.32.122/WirelessWeb/wtp.php

Management and Administration of IEEE 802.11 Network

WTP/AP Settings (WTP Running)

Lists of Access Controller's Ip Address

□ 192.168.0.5

□ 192.168.0.15

□ 131.95.32.122

AC IP Address

WTP Name

WTP Location

SSID Settings

□ Enable Security

SSID

Security Passphrase

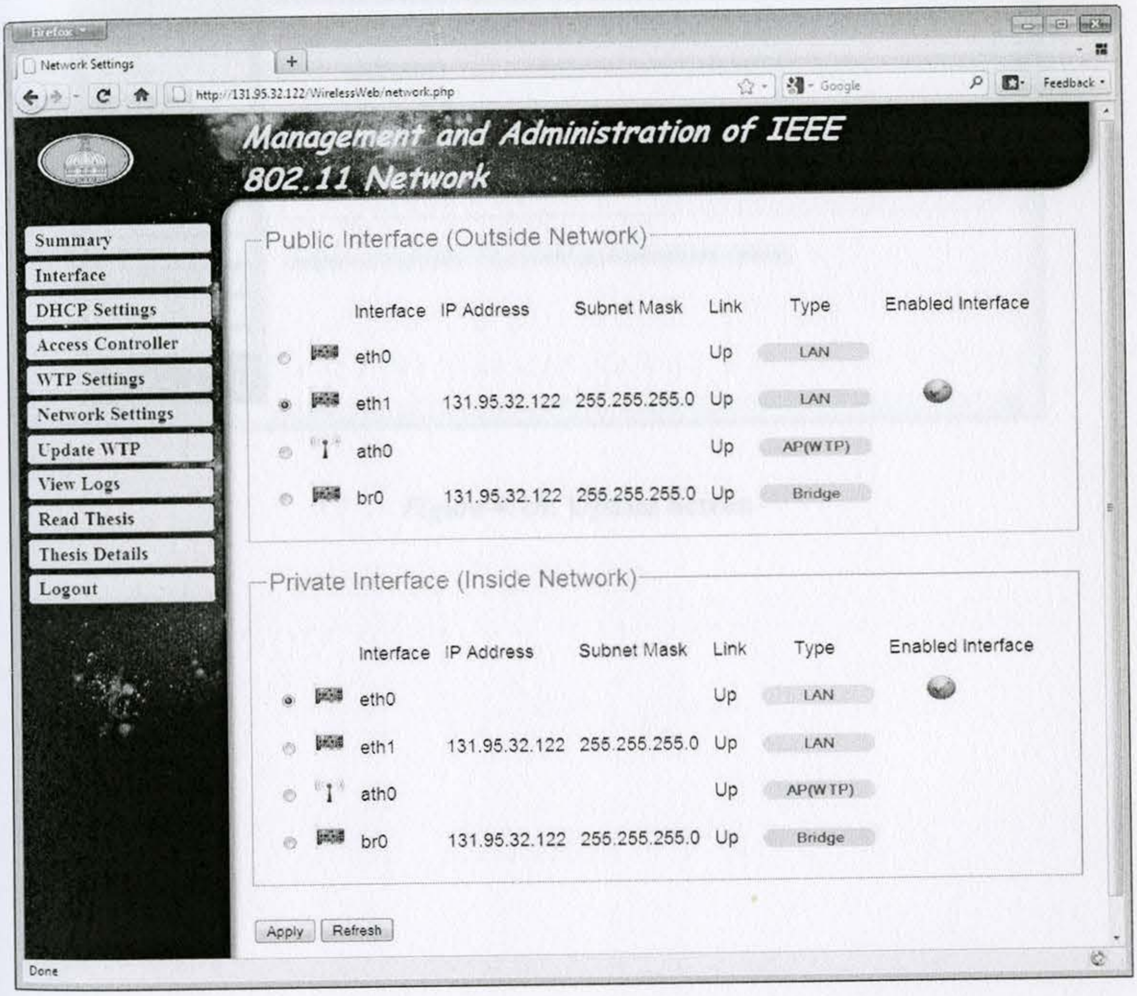
Maintained by biju bajracharya@eagles usm edu

http://131.95.32.122/WirelessWeb/wtp.php

Figure 4.16: WTP Settings

4.9.11 Network Settings

In this section of the page, we enable the IP Network Address Translation (NAT) Service as inside and outside network interfaces as shown in the Figure 4.17. The available interfaces that can be set as internal and external are listed in the two boxes. Public network can be termed as outside network or external network. Similarly private network can be termed as Inside or internal network. We can't choose the both the private and private interfaces on the same interface. We have to choose public network which has public IP address and we have to choose the inside network which has the private IP address. By clicking the Apply button, the NAT service will be started.



Public Interface (Outside Network)

	Interface	IP Address	Subnet Mask	Link	Type	Enabled Interface
○	eth0			Up	LAN	
●	eth1	131.95.32.122	255.255.255.0	Up	LAN	●
○	ath0			Up	AP(WTP)	
○	br0	131.95.32.122	255.255.255.0	Up	Bridge	

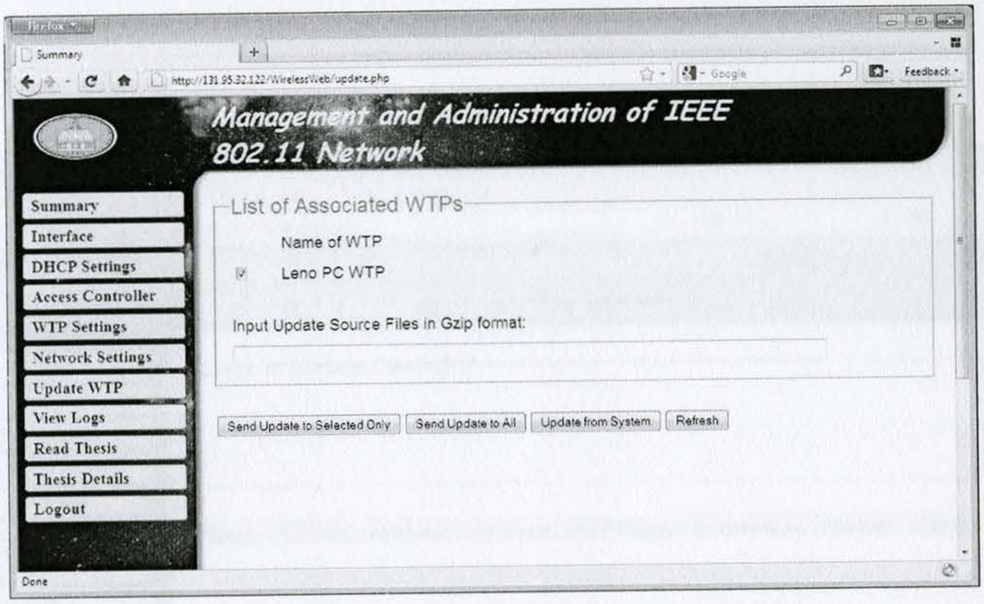
Private Interface (Inside Network)

	Interface	IP Address	Subnet Mask	Link	Type	Enabled Interface
●	eth0			Up	LAN	●
○	eth1	131.95.32.122	255.255.255.0	Up	LAN	
○	ath0			Up	AP(WTP)	
○	br0	131.95.32.122	255.255.255.0	Up	Bridge	

Figure 4.17: Network Settings

4.9.12 Firmware Update

AC can update its connected WTP with its new version of WTP. Script Files that needs to be executed on the WTP can be included in the update file. The update file should be in gzip format. Either we can give the web link of the source file or directly send update from the AC system. We can send the updates to the multiple WTP at once or we can send it all as shown in the Figure 4.18.



Management and Administration of IEEE 802.11 Network

List of Associated WTPs

Name of WTP

☑ Leno PC WTP

Input Update Source Files in Gzip format:

Figure 4.18: Update Screen

4.9.13 Log Files

In this section, we can see the logs of either AC or WTP by clicking the corresponding buttons as shown in the Figure 4.19. Instead of loading the whole log file, we can also check the 20 newest line by clicking AC logs for AC, and WTP logs for WTP. We can also check the Update logs which are made by the firmware updating. We can also see the Full logs. It may take time to load the page, according to its size. We can also clear those log files by clicking Clear logs. By clearing the log files, it will generate the new log files.

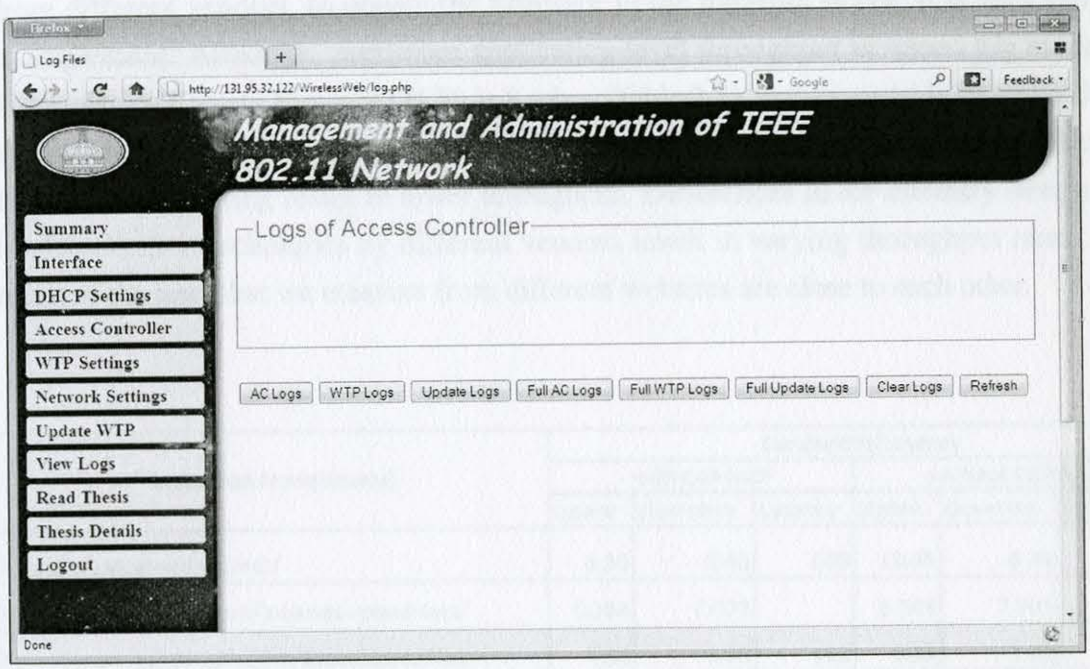
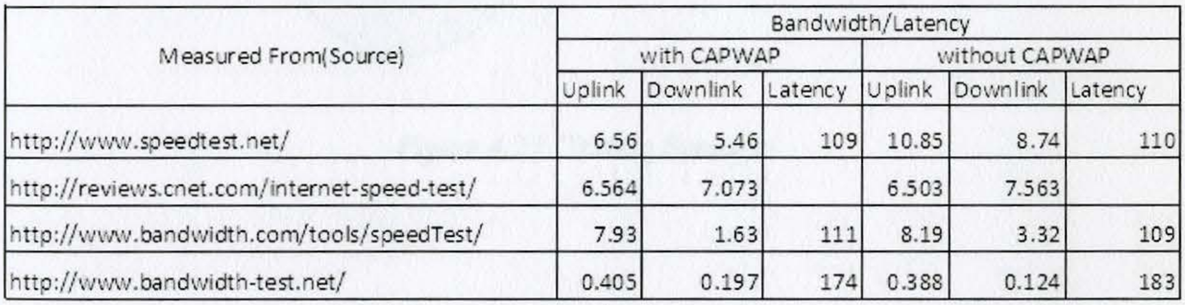


Figure 4.19: Log Files

4.10 Performance and Results

This open source application can be used with or without running the AC or WTP. By changing these features the performance may change. In the network as shown in the Figure 4.21, AC, WTP and Web service is installed on the same computer. The another WTP is installed on the separate small form factor AP. AP is connected via wired link to the AC. In this connection through is measured from different on-line websites. They are listed in the Figure 4.20 Although the uplinks, downlinks and latency depends on the source and destination of host, we measured the bandwidth and latency from different online bandwidth and latency measurement websites. Based on this result there is no or little changes on the bandwidth. However this protocol is designed to perform best where there are more WTPs from different vendors, to update the firmware to the multiple WTPs, it is very suitable to implement. Although, maximum application-level throughput in mixed b/g mode for Transmission Control Protocol (TCP) is 8 mbps (Table 2.1), various outside factors reduces this number; Humidity, temperature, Radio Frequency (RF) complications such as reflection, diffraction, scattering result in lower throughput. Differences in RF circuitry design and implementation techniques by different vendors result in varying throughput rates. The result of the tests that we measure from different websites are close to each other.



Measured From(Source)	Bandwidth/Latency					
	with CAPWAP			without CAPWAP		
	Uplink	Downlink	Latency	Uplink	Downlink	Latency
http://www.speedtest.net/	6.56	5.46	109	10.85	8.74	110
http://reviews.cnet.com/internet-speed-test/	6.564	7.073		6.503	7.563	
http://www.bandwidth.com/tools/speedTest/	7.93	1.63	111	8.19	3.32	109
http://www.bandwidth-test.net/	0.405	0.197	174	0.388	0.124	183

Figure 4.20: Bandwidth/Latency Measurement

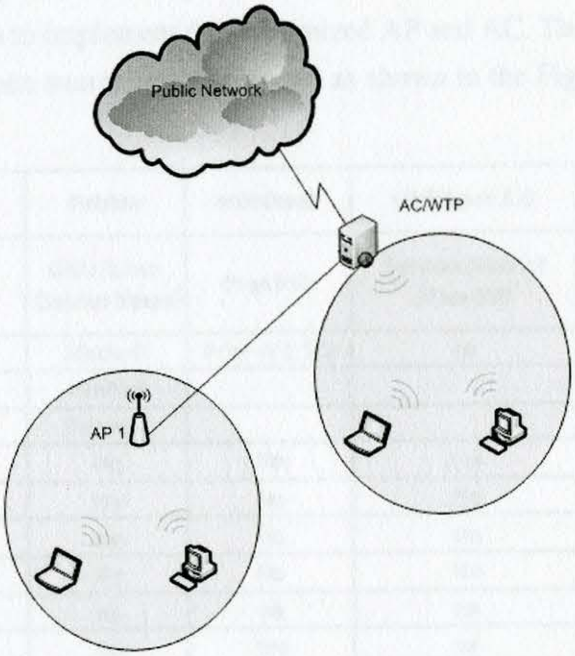
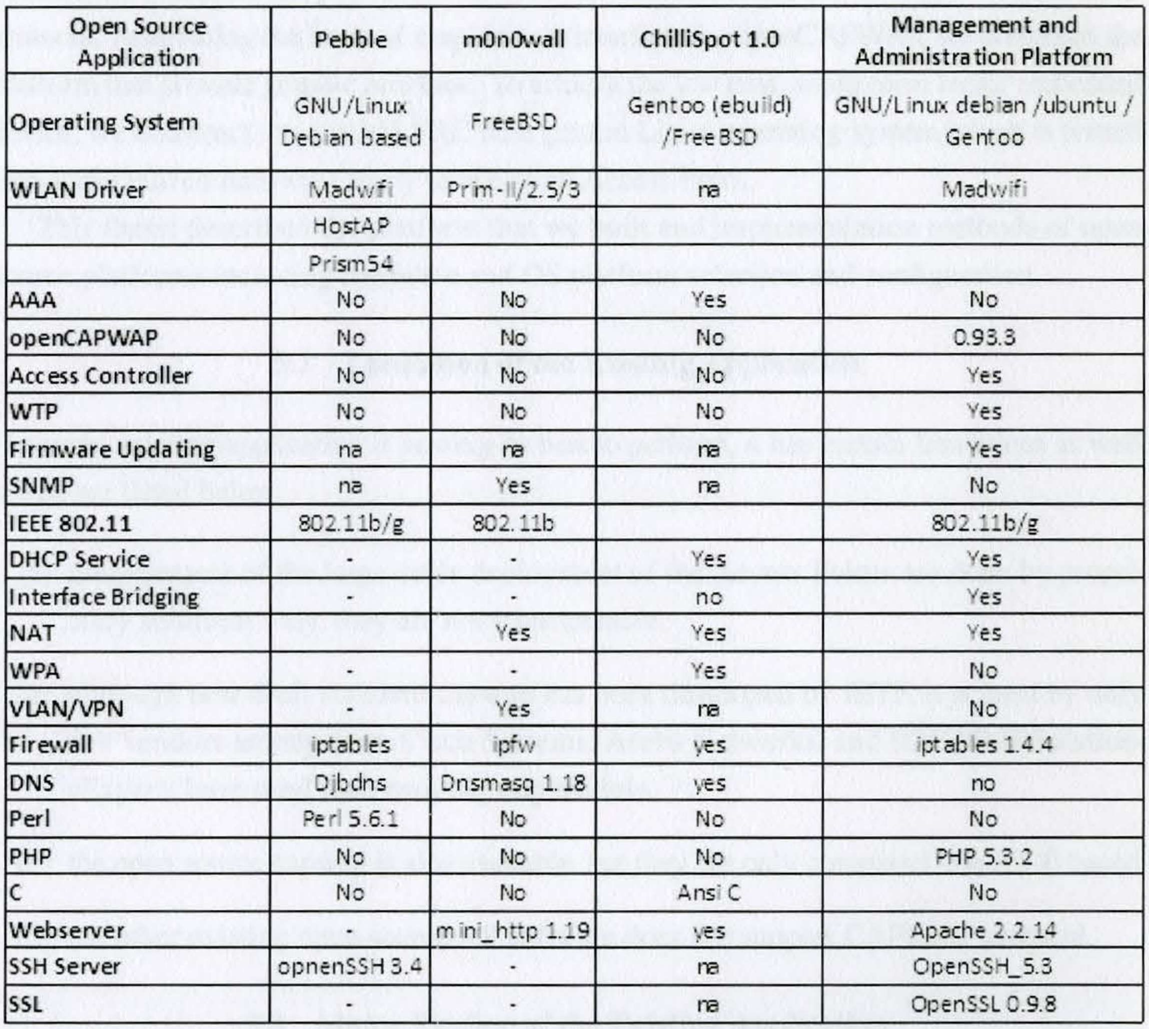


Figure 4.21: Testing Scenario

4.11 Comparative Analysis

Our application is compared with the most distinguishing features and components of Pebble, m0n0wall and ChilliSpot. Currently our application does not support VPN, VLAN, AAA and SNMP protocols. It supports the openCAPWAP protocols which is used to manage the multiple AP through central Access Controller which is the key feature of our application. Another key feature is it doesn’t need to reside in the Access Point and the firmware that can be updates at any time from anywhere. So, this can be the best option to implement as open source platform to implement the customized AP and AC. The comparative analysis of feature with other open source application are as shown in the Figure 4.22.



Open Source Application	Pebble	m0n0wall	ChilliSpot 1.0	Management and Administration Platform
Operating System	GNU/Linux Debian based	FreeBSD	Gentoo (ebuild) /FreeBSD	GNU/Linux debian /ubuntu / Gentoo
WLAN Driver	Madwfi	Prim-II/2.5/3	na	Madwifi
	HostAP			
	Prism54			
AAA	No	No	Yes	No
openCAPWAP	No	No	No	0.93.3
Access Controller	No	No	No	Yes
WTP	No	No	No	Yes
Firmware Updating	na	na	na	Yes
SNMP	na	Yes	na	No
IEEE 802.11	802.11b/g	802.11b		802.11b/g
DHCP Service	-	-	Yes	Yes
Interface Bridging	-	-	no	Yes
NAT		Yes	Yes	Yes
WPA	-	-	Yes	No
VLAN/VPN	-	Yes	na	No
Firewall	iptables	ipfw	yes	iptables 1.4.4
DNS	Djbdns	Dnsmasq 1.18	yes	no
Perl	Perl 5.6.1	No	No	No
PHP	No	No	No	PHP 5.3.2
C	No	No	Ansi C	No
Webserver	-	mini_http 1.19	yes	Apache 2.2.14
SSH Server	opnenSSH 3.4	-	na	OpenSSH_5.3
SSL	-	-	na	OpenSSL 0.9.8

Figure 4.22: Comparative Analysis of Features

Chapter 5

SUMMARY

5.1 Overview

The overall purpose of our thesis is to develop a web interface "Open Management and Administration of IEEE 802.11 Network." Begining research with a existing open source system, we found no graphic user interface for implementing the opensource CAPWAP protocol. Addressing the issue of graphic user interface for openCAPWAP, we presented the platform that provide graphic interface. To achieve the low cost, small form factor embedded device, we construct the alix3d3 SBC with gentoo Linux operating system which is turned into a specialized hardware ready to use as an Access Point.

This thesis described the platform that we built and implementation methods of open source platforms including hardware and OS platform selection and configuration.

5.2 Limitation of the Existing Application

However, existing application is serving its best to perform, it has certain limitations as well which are listed below.

(a) management of the large-scale deployment of the Access Points are done by proprietary solutions only, they are not interoperable,

(b) although new draft standard capwap has been developed by IETF, it is used by only few vendors among them Cisco Systems, Aruba Networks, and H3C IToIPSolutionsExperts have used their own capwap module.

(c) the open source capwap is also available, but they are only command line (CLI) based.

(d) the other existing open source AP software does not support CAPWAP protocol.

5.3 Major Finding of the Existing Application

(a) Wireless Networking is one of the rapid growing application around the world

(b) WLAN is the most preferred technology

(c) It is gaining popular because of its mobility, low cost, scalability, automatic network connectivity

(d) The immense growth of WLAN users increases the Interference to neighbouring devices

(e) Its very hard to maintain the network when there are multi vendor access points are deployed.

(f) It is difficult to manage the large scale deployment of WLANs.

5.4 Future Work

Several emerging technologies exhibit enormous potential in the WLAN deployment. This designed platform is ready to use. To facilitate its further improvement, AAA server should be introduced for the centralized authentication and accounting. Mysql server should be deployed to store the informations of configuration and updates, and any changes in the network that can be analyzed latter.

5.5 Recommendations

The demand of Wireless LAN is growing in very fast pace around every corner of the world. To beat this pace of the wireless technology we should also catch up with the development of the new technology. Although, to deal with wireless stations problem IEEE is developing new standard which is yet due and announced to publich at the end of this year. To implement and develop those standards university should engage to develop the protocol. Also the IETF standard protocol CAPWAP has almost been finalized, only very few vendors are using this protocol. University should help those vendors to build the protocol so that they can run the big multi-national vendors. We should utilize the effort of open source capwap to implement and deploy and made available to others.

5.6 Conclusion

In this thesis, based on the investigation of the background of the WLAN management, an open management and administration platform is proposed. In particular, a web based distributed user-friendly WLAN management framework is proposed and implemented. It consists of three major functional components: wireless terminal points, an access controller and a web server. Utilizing an open source implementation of draft international standard

CAPWAP that provides the communication between wireless terminal points and the access controller, this web framework translates the graphic input of a WLAN administrator into CAPWAP protocol commands and visualizes the network statistic from CapWAP through the web interface to the administrator. This thesis significantly contributes to and will expedite the deployment of WLAN management. It is particularly valuable for small or mid-size business units or home WLAN users.

BIBLIOGRAPHY

[1] B. 0'Hara, P. Calhoun, and J. Kempf. Rfc 3990 - configuration and provisioning for wireless access points (capwap) problem statement, February 2005.

[2] Devin Akin and Jim Geier. *CWAP, Certified Wireless Analysis Professional*. McGraw-Hill, Inc., 2004.

[3] Frederico J.R. Barboza, Aline M.S. Andrade, Flávio Assis Silva, and George Lima. Specification and verification of the ieee 802.11 medium access control and an analysis of its applicability to real-time systems. *Electronic Notes in Theoretical Computer Science*, 195:3–20, 2008. Proceedings of the Brazilian Symposium on Formal Methods (SBMF 2006).

[4] M. Bernaschi, F. Cacace, G. Iannello, M. Vellucci, and L. Vollero. Opencapwap: An open source capwap implementation for the management and configuration of wifi hot-spots. *Computer Networks*, 53(2):217–230, 2009. QoS Aspects in Next-Generation Networks.

[5] David D.Coleman and David A.Westcott. *CWNA Certified Wirelss Network Administrator Study Guide*. Wiley Publishing, Inc., 2006.

[6] Charles M. Kozierok. The tcp/ip guide - tcp/ip snmp operational model, components and terminology.

[7] Thomos Maufer. *A Field guide to Wireless LANs for Administrators and Power Users*. Prentice-Hall, Inc., 2004.

[8] Daniel Minoli. *Hotspot Networks, WiFi for Public Access Locations*. McGraw-Hill, Inc., 2002.

[9] Christopher Negus. *Live Linux CDs*. Prentice-Hall, Inc., 2007.

[10] Anand R.Prasad and Neeli R.Prasad. *802.11 WLANs and IP Networking, Security, QoS, and Mobility*. Artech House, Boston I London, 2005.

[11] Mathew S.Gast. *802.11 Wireless Networks*. O-Reilly, 2002.

[12] Wale Soyinka. *Wireless Network Administration A Beginner's Guide*. McGraw-Hill, Inc., 2010.

[13] Keir Thomas and Andy Channelle. *Beginning Ubuntu Linux*. Apress, 2009.

[14] Eduard Garcia villegas villegas villegas villegas. *Self-Optimization of Radio Resource on IEEE 802.11 Networks*. PhD thesis, Polytechnic University of Catalunia, 2009.

[15] Brian Ward. *How Linux Works*. No Starch Press, 2004.

[16] Steve Wisniewski. *Wireless and Cellular Networks*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 2004.

[17] Byron W.Putman. *802.11 WLAN Hands-On Analysis*. AuthorHouse, 2006.