Palestine Polytechnic University

College of Engineering & Technology

Electrical & Computer engineering Department

Communications & Electronics Engineering

Graduation project

Improving Handoff Delay In WLAN

Project Team

Samah M. Al-arja sarah as'ad jahshan

Project Supervisor

Dr. Murad Abu subaih

Hebron-Palestine

May, 2010

Palestine Polytechnic University

Hebron- Palestine

College of Engineering & Technology

Electrical and Computer Systems engineering Department

Improving Handoff Delay In WLAN

Project team

Samah Al-arja   sarah Jahshan

Supervisor Signature

____

Testing Team Signature

___________________   ___________________ ___________________

Department Manager Signature

____

Dedication

To our first teachers

Our fathers

…

To our heart lover

Our mothers

…

To the flower of the earth & the starts of the sky

Our sisters & brothers

…

To whom love & can't forget

Our friends, beloved &teachers

…

To my soul of Martyrs

…

To all of the Islamic countries

Thank you very deep from our hearts for all

the love and supports that

you have given to us.

Abstract

In this project we want to improve the process of the handoff delay in Wireless Local Area Network (WLAN) between access points (AP). where when the mobile device connected to any access point (AP_i) and received the power from it, and still receiving, but when the power value of these signal is decreasing or became less than the threshold power value, then these mobile device start to scan about another APj that have a power value more than the threshold power value and the signals power from the first AP ($P_{avi}<P_{th}\leq P_{avj}$), then the handoff occurs. But when the power value of the signal from the old AP still good ($P_{av}i\geq P_{th}>P_{av}j$) or ($P_{avi}<P_{th}>P_{avj}$) then the handoff will not take place.

Aim:

Our project aims to solve the problem of decreasing the power value of the signal that received from any AP by laptop over long distance or any condition that make the power below the threshold value .The importance of our project take a large space specially in the hospital where there is a lot of surgery done on the network by doctor from another country where any wrong on the network cause a large danger. Not only in the hospital but in university company office…etc.

Method proposed:

First, we want to study the materials that we needed in this project software and hardware and choosing a suitable network adaptor that needed later and identify it by using Mad Wifi driver and installing the Linux on the laptop to make the dealing with network adaptor more easy in addition to study the main concept on the project like WLAN scanning...etc.

Materials and Equipment:

We will use in this project the requirement software like Linux, MAD Wi-Fi, And requirement hardware like Access Points, mobile device, and wireless network adaptor.

List of contents

List of tables

List of figures

CHAPTER ONE

INTRODUCTION

1.1 Overview

1.2 Project objectives

1.3 Literature review

1.4 Time plane

1.5 Estimated Cost

1.6 Project Risks

1.7 Report Contents

Chapter one

Introduction

1.1 Overview:

This project is about improving mobile device handoff between two or more access points (APs) in wireless local area network (WLAN). In other words, the mobile device (laptop) will apply a passive scanning to connect to an AP, where the mobile device starts the handoff when the power of the signal received from the first access point (AP_i) is lower than power threshold value and the power of the signal received from the another (AP_j), starts to increase higher than the threshold value, then the handoff process starts from (AP_i) to(AP_j). This process should be as fast as the user can't recognize it.

We can benefit from this project in several places such as hospitals, companies, and universities, where students are continuous motion between buildings.

1.2 Project objectives:

- To maintain the internet connection for mobile device.
- Scanning the network to find an AP to be connected to, when the signal received from the current access point is lower than power a threshold value.
- Reducing the time of handoff delay in order to make the process invisible to the user.
- To design intelligent program system enough to decide which access point better to connect to in the intersection area of two access point's coverage area.

1.3 Literature review:

- "Link layer assisted mobility support using SIP for real-time multimedia communications ", granted to W. Kim, M. Kim, K. Lee, C. Yu, and B. Lee. Try to reduce handoff delay by using proactively reserving for the new access point in the new network while still in the old network .where they request anew AP address for the new network and update the SIP (Session Initial Protocol) with new address and then perform the handoff to do this. Kim change DHCP (Dynamic Host Configuration Protocol) and replace the DHCP protocol with DRCP(Dynamic Rapid Configuration Protocol) that reduce the address allocation time and the handoff happen for few hundred milliseconds, but this time is large so he use active scanning . These project ideas perform the hand off on two networks that’s the difference between Kim project and our project because we improving handoff in WLAN in one network only that’s the difference. [1]

- "SIP-based end system mobility solution for all-IP infrastructures", granted to N.Akhtar, M. Georgiades, C. Politis, and R. Tafazolli. Akhtar in his project make a comparison handoff delay between SIP/DHCP that used for macromopility and SIP/cellular-IP that used for micrompility and he found that the delay in the SIP/DHCP (30 sec) is more than the other type. Where the AP address is change then update the session to HMSIP. The time of demand a new AP is ignored and the new component should be exist in every visited network ,and he using the RTP translator (real time protocol) and it should be exist in every visited network too . when the mobile device gets a new AP address it register the new AP address to the SIP register which request the RTP translator to forward the traffic associated with the old AP address to the new AP address.[2]

1.4 Time plane:

In the first semester we have 16 week and in the second semester we have 16 week .We want to classify these weeks into segments to work on the project as follow in the table:

Table 1.1 Project time plane (First semester).

Task \ week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Choosing project	■	■														
collecting information			■	■	■	■	■									
Literature review & related theory				■	■	■	■	■	■	■						
Design and analysis										■	■	■	■	■	■	■

Table 1.2 Project time plane (Second semester).

Task \ week	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Detailed design schematic	■	■	■													
Hardware and Software design			■	■	■	■	■									
Implementation							■	■	■	■	■	■	■	■		
Testing and conclusion													■	■	■	■

1.5 Estimated Cost:

The project needs both hardware equipments and software programming, and this section shows the estimated hardware and software costs.

Table 1.3 Estimated hardware costs

Component name	Unit price ($)	Quantity	Total price($)
Laptop	1000	1	1000
Network adaptor	100	1	100
Access point	50	2	100
Computer (PC)	500	1	500
Switch	10	1	10

- Software such as:
    - Linux.
    - Mad Wi-Fi.
    - Traffic generator

The above software is open source software free to download from the internet.

1.6 Project Risks:

The project may face some problem and risks that we have to declare in the early time of the project like hardware and software Installing, and the project must be avoid those problems to work in its high efficiency, so we find a risk we will try to solve it without effect on the total project much as we can.

1. One of the group members is sick.

2. Unavailability of some project needed components.

3. The needed time for response so long that makes the user nervous.

4. Our background for the software programs insufficient, and we need to learn more to how use it.

1.7 Report Contents:

This report consists of four chapters; each chapter discusses a specific area of the report.

Chapter one:

"Introduction" this chapter gives an introduction about the project, its overview, motivation, related works, project time plan and project cost.

Chapter two:

"Theoretical Background" this chapter introduce a background related to the main concept of the project. It's background of WLAN and project components.

Chapter three:

"Design Concept" This chapter describes the project objectives, a general block diagram and explains how the system works.

Chapter four:

"Work Plan" This chapter describes the project work plan and the steps that will be taken, such as installing and learning the project software, implementing and installing the hardware part of this project and studying the basics of Wireless Networking concept.

Chapter five:

This chapter gives a big look about the options can be used in implementing the project.

Chapter six:

In this chapter we are going to show the implementation and testing processes for our system.

Chapter seven:

This chapter describes and gives a conclusion for our project and a complete look over the entire from project from the beginning.

CHAPTER TWO

THEORETICAL BACKGROUND

Chapter two:

Theoretical Background

This chapter provides an illustrative background for the Wireless Local Area Network and the project components.

2.1 Wireless Local Area Network (WLAN):

2.1.1 Introduction:

Wireless networks are a popular technology that been used to connect computers at distance without wires to pass on the information among the devices that been connected to the local area network (LAN).

In this chapter we will provide general idea about Wireless local area network, like definition of WLAN and the communication techniques used in WLAN.

2.1.2History:

- In 1970 developed the first computer communication network, using low cost radios. The system connected seven computers deployed over four islands to communicate with the central computer without using phone line (wireless).
- In 1979 using a wireless local area network using diffused infrared communications.
- In 1980 developed a single code Spread Spectrum radio for wireless terminal communications in the IEEE (Institute of Electrical and Electronics Engineers) national telecommunications conference.
- In 1984 a comparison between infrared and CDMA (Code Digital Multiple Access) spread spectrum communications for wireless office information networks was published in IEEE computer networking.
- In 1990 WLAN hardware was so expensive that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards.

2.1.3 The generation of WLAN:

- The first generation of wireless data modems was developed in the early 1980s, commonly referred to this as packet radio .They added a voice and data communication modem, with data rates below 9600-bit/s, to an existing short distance radio system, typically in the two meter amateur band.

- The second generation of wireless modems was developed immediately after the FCC announcement in the experimental bands for non-military use of the spread spectrum technology. These modems provided data rates on the order of hundreds of kbps.
- The third generation of wireless modem then aimed at compatibility with the existing LANs with data rates on the order of Mbps. Several companies developed. The third generation products with data rates above 1 Mbps and a couple of products had already been announced by the time of the first IEEE Workshop on Wireless LANs.

2.1.3 Wireless communication technique:

Wireless LANs use one of three communication techniques which are:

1. **Spread spectrum:**

   Spread spectrum is a communication technique used in wireless networks to transmit and receive data over range of frequencies, by using electromagnetic spectrum which has a frequency range between 902 MHz to 928 MHZ and 2.4 GHz to 2.484 GHz. This technique decreases the interference to other receivers. The basic principle of spread spectrum is the use of noise like carrier waves, and the bandwidths wider than the bandwidth for the simple point to point communication at the same rate. The term "spread spectrum" is used because the radio uses several frequencies at once .

There is two type of spread spectrum:

- Frequency hopping spread spectrum (FHSS) is a method of transmitting radio signals by Switch the carrier quickly between frequency channels. FHSS as a multiple access method in the frequency-hopping code division multiple access (FH-CDMA) scheme.
- DSSS: Direct sequence spread spectrum uses the radio frequencies ranging from 2.4 to 2.4835MHz. It uses a Differential Binary Phase Shift Keying (DBPSK) and Differential Quadruple Phase Shift Keying (DQPSK) modulation and divides the total bandwidth into 13 channels.

2. Narrowband microwave:

Narrowband microwave is a communication technique used to connect local area networks across buildings by using microwave dishes. This technology requires a line of sight between dishes in order to transfer data in between.

3. Infrared:

Infrared is a communication technique based on light technology, where in this technology data is being modulated and transmitted by Light Emitting Diode (LED). In general the infrared is the energy radiation that has frequency below sensitivity so the human cannot see it but we know that it exist, and exist between the visible and part of the microwave of the electromagnetic spectrum, then the wavelength for Infrared light has a range from red light to violet.

4. Radio Frequency(RF):

RF is any frequency within the electromagnetic spectrum associated with radio waves propagation and suitable for utilization in radio communication. Some of these waves serve as carriers of the lower frequency audio waves; others are modulated by video or digital information. Radio waves are identified by their frequencies, expressed in kilohertz (KHz). The frequencies cover a significant portion of the electromagnetic radiation spectrum, extending from 9 KHz, the lowest allocated wireless communications frequency to thousand of Gigahertz (GHz).

5. **Bluetooth** :

Bluetooth is an open wireless technology using to transmit data approx 1Mbps from fixed mobile device creating personal area network (PANs) over short distance (10 m) and uses to connect one device to another with one universal radio link, and do not have to be in line of sight of each other. It has many advantages such as a low complexity, low power and low cost. It operates on 2.4 GHz band.

2.1.5 Types of WLAN:

2.1.5.1 Ad hoc:

Ad hoc is a set of computer wireless nodes connected based on a peer to peer method, where the standard for ad hoc is Independent Basic Services Set (IBSS), and this type applied when the access point not available. This method is used by two computers so they can connect together to establish a network. But there is a good advantage for using the Ad hoc like no need to install base stations, easier temporary setup. Where the Ad hoc consider an assisted for handoff delay, and allow the computers to communicate directly with each other without needs the router.

Fig 2.1: Ad hoc

2.1.5.2 Infrastructure:

Infrastructure consists of access points that work as bridge between the wired network and wireless devices in the computers. The standard for infrastructure refers to an access point is Basic Service Set (BSS). To cover a large area we can use multiple access points. We call the use of multiple access points an Extended Service Set (ESS), In ESS two or more Basic Service Sets connected to the same wired network. And to reduce the interference between access points, each access point is using a different channel; also the coverage area is taken into consideration.

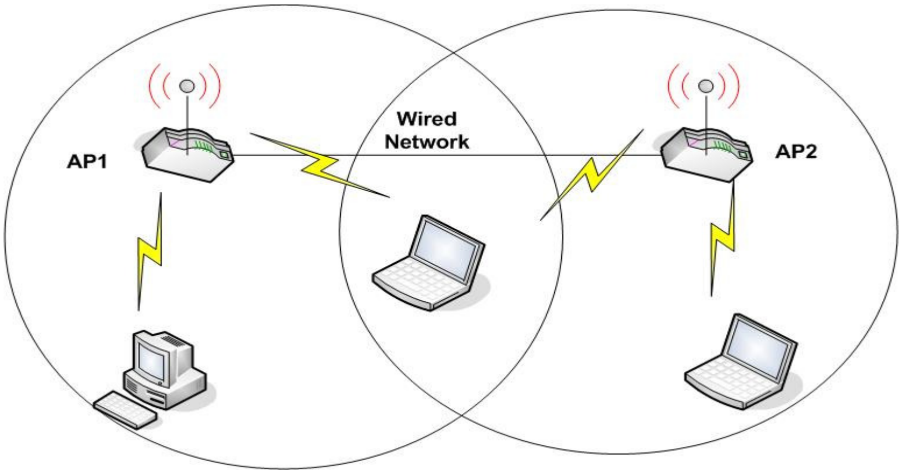


Fig 2.2: Infrastructure.

2.1.6 WLAN Standards:

WLAN consisting of number of standards:

- 1EEE 802.11a: applies to wireless LANs using frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS), and developed to provide higher data rate than 802.11b it's based on multicarrier modulation and have more band width and many more channel but its more expensive than 802.11b supports speeds from 6 Mbps up to 54 Mbps, works in 5 GHz radio band.
- 1EEE 802.11b: was developed to avoid some of the problem with the first generation system many laptop come with integrated

802.11b W LAN card supports speeds up to 11 Mbps, works in 2.4 GHz radio band,(called Wi-Fi)

- 1EEE 802.11d: LAN/MAN standard, operate on the access point causes the AP to broadcast the ISO country code for the country it is operating in as a part of its beacons and probe responses.
- 1EEE 802.11e: Working on quality of service (QOS) in LANs. And it's an improvement to the 802.11a and 802.11b W LAN specifications. 802.11e maintained full backward compatibility with these standards.
- 1EEE 802.11g: it uses multi carrier modulation applies to WLANs and is used for transmission over short distances at up to 54Mbps in the 2.4 GHz , supports speeds up to 54 Mbps.
- 1EEE 802.11x: is an IEEE standard for port based Network Access Control that allows network management to restricted use of IEEE 802 LAN service access points to secure communication In the network.

2.1.7 Benefit of WLAN:

- The absence of physical connection in WLAN systems can provide higher number of users, which will be impossible in wired LAN.
- WLAN system can be fast and easy and eliminate the need to use wires through walls and ceilings, which reduces cost and increase flexibility.

- Expandability: wireless networks can serve increased number of clients. Compared with a wired network, additional clients would require additional wiring.
- Mobility: With the emergence wireless networks, users can access the internet even outside their normal work environment.
- Convenience: The wireless networks allow users to access network resources from nearly any Suitable location.

2.1.8 Handoff in WLAN:

Access points provide wireless connectivity between a mobile device and a wired network whether its privet or public. To provide the service of the wired network over a larger area, more access points are needed, and when the mobile device starts to move away from the current AP, signal power received starts to decrease, then the mobile device try to maintain a good quality connection with the network by associating to a new AP. This is called Handoff.

We can divide the handoff process into three stages:

- **Scanning**:

  The scanning process can be passive or active.

  - ✓ Passive scanning to wait to receive a beacon message from access points where a beacon is periodically sent by APs.
  - ✓ Active scanning to determine whether an AP is operating on a particular channel, When an AP receives a Probe Request, it replies with Probe Response message.

The 90% of handoff delay comes from scanning delay, and in this project we concentrate on how to reduce the scanning delay.

- **Authentication**

  Authentication is the process of making sure that mobile devices with valid IDs can benefit from the wireless service (security), also it is useful to limit connection capability for users with certain IDs.

- **Re Association**

  Re association is the final stage of the handoff process, where the mobile device is associated to the new AP.

2.2 project components:-

This project is made up from the following hardware and software components:-

Requirement hardware:

1. Access points.
2. Mobile device to move between two APs.
3. Wireless Network adaptor.
4. PC server.
5. Switch.
6. Wires.

- **Access points:**

  It’s a device (wireless Access point) that transmits and receives data in WLAN; it can also connect the users to another user within the network. the AP can also serves as the point that connect between WLAN and fixed wire network ,each access point can serves more than one user in the network area ;where when the users moves beyond the range of the one access point then the users handed over the next access point ,it’s used in home company and small business network.

Types of Access Points (APs):

- ✓ **Stand-alone APs**: used for the SOHO (Small Office/Home Office). As it can make management separately because of the few number of access points can provide wireless connectivity through the whole house**.**
- ✓ **Light-weight APs + central controller:** this access point is light-weight and with it there is central controller, and it is the opposite of the first type of the AP which doesn’t have a controller it is only contain functionalities .
- ✓ **Virtual Management**: this type which is developed later it is mixed of the two mentioned types of AP. This type is functional by itself and it can collaborate APs network for providing higher voice and video quality.

- **Mobile device:**

Mobile devices are mobile phones, web phones, pagers, two-way pagers, Personal Digital Assistants (PDAs), and Internet appliances. The list is growing, as more new devices are being introduced. Mobile devices allow you to communicate with others and get information anywhere, at any time. In our project we will use laptop mobile device, the reason to use laptop in this project is the extended usage of the laptop in university.

- **Wireless network adaptor:**

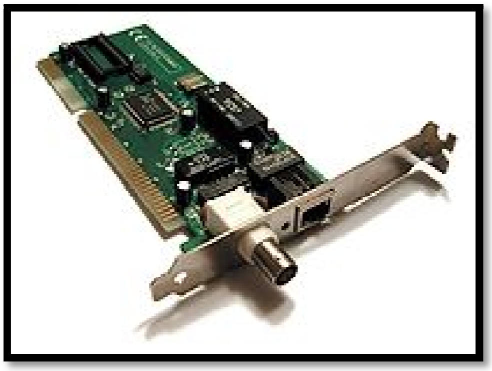


Fig 3.1: Network Interface Card (NIC)

✓ This figure shows the network interface card that consider a computer hardware component that design to allow computer to communicate over computer network and acts as the interface between a computer and a network cable. The purpose of the network card is to prepare, send, and control data on the network. It is used physical and data link layer device and allow users to connect to each other by using cables.

- ✓ Network card has 48 bit serial number (MAS address) and stored in ROM ,where every card have a unique MAS address to make sure that no two network card use the same address .
- ✓ Most new computer has a network into the motherboard, a separate network card is not required unless multiple interfaces are needed and new motherboard have dual network.
- ✓ The card network is electronic circuit requires physical and data link layer as we say before this provide a base for full network protocol stack.

- ▪ **PC server:**

  It's a software package that provides many services to the client software running on the computer.

- ▪ **Switches:**

  It's a small hardware device that connects multiple computers together within one local area network, the network switches operate at data link layer.

- ▪ **Wires:**

  In our project we used the wires in order to connect the components to each other.

Requirement software:

1. Linux.
2. MadWifi driver.
3. Traffic generator**.**

- **Linux**

  Today Linux has joined the desktop market. Linux developers concentrated on networking and services in the beginning, and office applications have been the last barrier to be taken down, providing an easy user interface and MS compatible office applications like word processors, spreadsheets, presentations and the like.

  The reason behind using Linux; is the ability to edit and change the source code, where Linux is an open source operating system, which gives you freedom to create and change codes.

- **Mad Wi-Fi**

  Multiband Atheros Driver for WI-FI, is a Linux driver for 802.11a/b/g universal NIC (Network Interface Card) cards, following the reason for choosing Linux, Madwifi, gives the ability to configure the network interface device using a set of commands, where this option is hard to achieve using windows driver tools.

- **Traffic generator:**

A traffic generation model is a stochastic model of the traffic flows or data sources in a communication network, for example a cellular network or a computer network.

CHAPTER THREE

DESIGN CONCEPTS

Chapter three

Design Concepts

This chapter describes the project objectives, a general block diagram. It explains how the system works.

3.1 Project Objectives:

This section summarizes the project objectives, which will be achieved after implementing this project. Main objectives are listed below:

- The system helps mobile device to avoid being confused which access point to connect to, when multiple access points cover the same area.
- To develop system that provides easy mobility between two areas with two access points without any interruption.
- To design and program system, intelligent enough to decide which access point better to connect to in the intersection area of two access points coverage area.

3.2 General block diagram:

This section illustrates system components. In Fig3.1 illustrates two wired network devices, wireless network devices and mobile device.

The following block diagram, gives a general idea about a small part of a wireless network generally speaking (WLAN), as shown below the project is dealing with wireless network devices, which is the end point of a wired network, and a mobile device with wireless connection capability, where the three elements will communicate together through the wireless communication protocol, and that includes the main subject of this project (handoff). Our mission is to improve the handoff process.

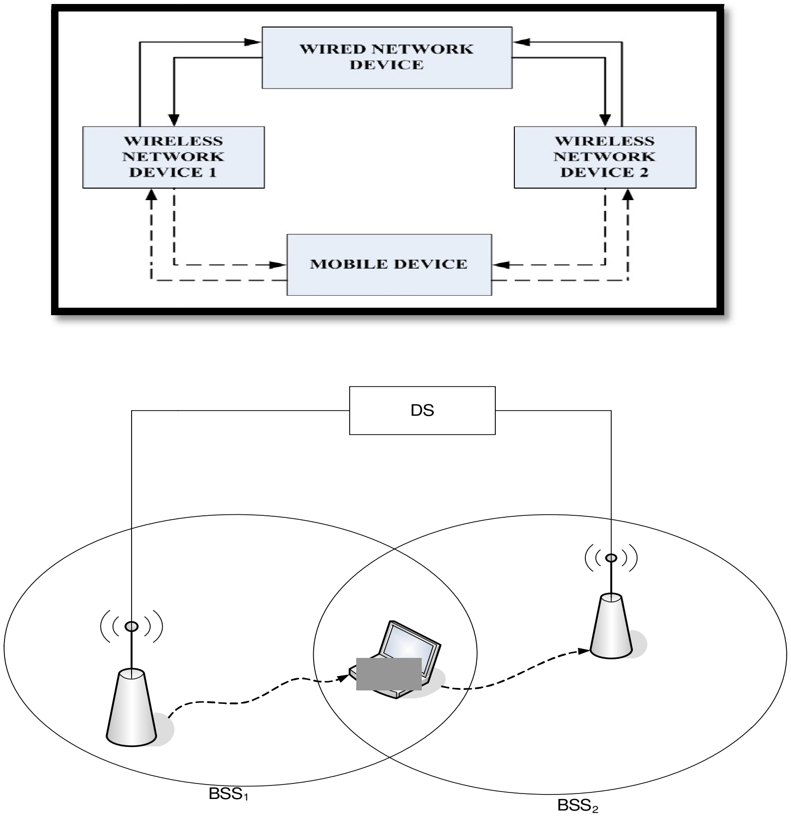


Fig. 3.2: General Block diagram

3.3 The main components & sub components:

This section illustrates all components of our system, their detailed block diagrams and detailed system operations.

3.3.1 Hardware part:

In this part we want to make a network these network consist of two access points that connected to each other over switch and those are connected into server; where these component connected to each other through the network.

3.3.2 Software part:

After installing the network components described in the previous section, the networks standards and protocol take place to allow the components to communicate. In wireless networks, IEEE 802.11 standards play a major rule in the process of communicating between mobile devices and APs, which includes the process of changing the AP within the same network for the same mobile device previously mentioned as HANDOFF.

Showing below in the flow chart , the process of the Handoff between two APs, where the mobile device (Laptop) will be connected to AP_i (wireless Network Device), by receiving Signal (S_i) with Power (P_i) as long as the average power (P_{iAV}) over a period of time is higher than a predetermined Threshold Power (P_{TH}). The process of searching Signals is called scanning , whether it's passive or active, the mobile device will receive signals from both AP, and the comparison of the three inputs P_{AVi}, P_{AVj}, P_{TH}, to determine if the handoff will take place or not.

Basically when the mobile device is connected to AP_i, the average power received P_{AV1}, as long as it's closer to APi, will be higher than the threshold power P_{TH} and the average power from AP_j P_{AVj}, then the handoff algorithm will not take place, summarizing the possible probabilities:

$P_{AVi} \geq P_{TH} > P_{AVj}$ =======➔ Handoff will not take place.

$P_{AVi}<P_{TH}>P_{AVj}$ =======➔ Handoff will not take place.

$P_{AVi}<P_{TH}\leq P_{AVj}$ =======➔ Handoff from AP_1 to AP_2 will take place.

Note: Power of the signal depends on the distance between the access point and the mobile device.

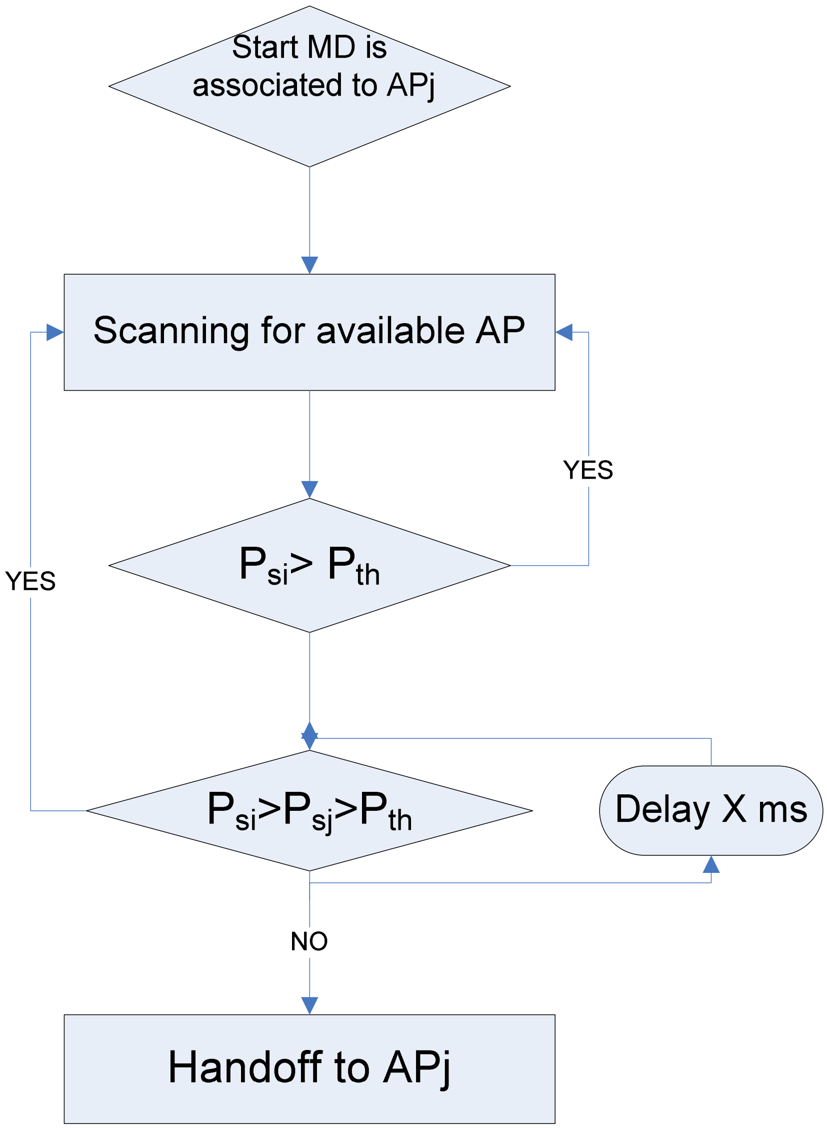


Fig3.4: Flowchart of project

CHAPTER FOUR

WORK PLAN

4.1 Software Installing and Studying

4.2 Hardware Installing and Studying

4.3 Project Scenario

4.3 Implementation and Testing

Chapter Four

Work Plan

This chapter describes the project work plane and the steps that will be taken, in order to accomplish the main concept of this project.

4.1 Software Installing and Studying:

In this step, we need to install Linux operating system, and learn how to use it, where this will be the first time for us to deal with Linux as an operating system. In addition to that, we need to install MADWIFI, also to learn how to use it; we need only to refresh our knowledge and information.

4.2 Hardware Installing and Studying:

In this step, after preparing the hardware components of the project, we are going to create a small wireless network, using two access points, PC and a mobile device (Laptop) with a wireless network adaptor.

This step will require study basics of networking especially wireless networking and to study the IEEE protocol 802.11 a/b/g.

4.3 Project Scenario:

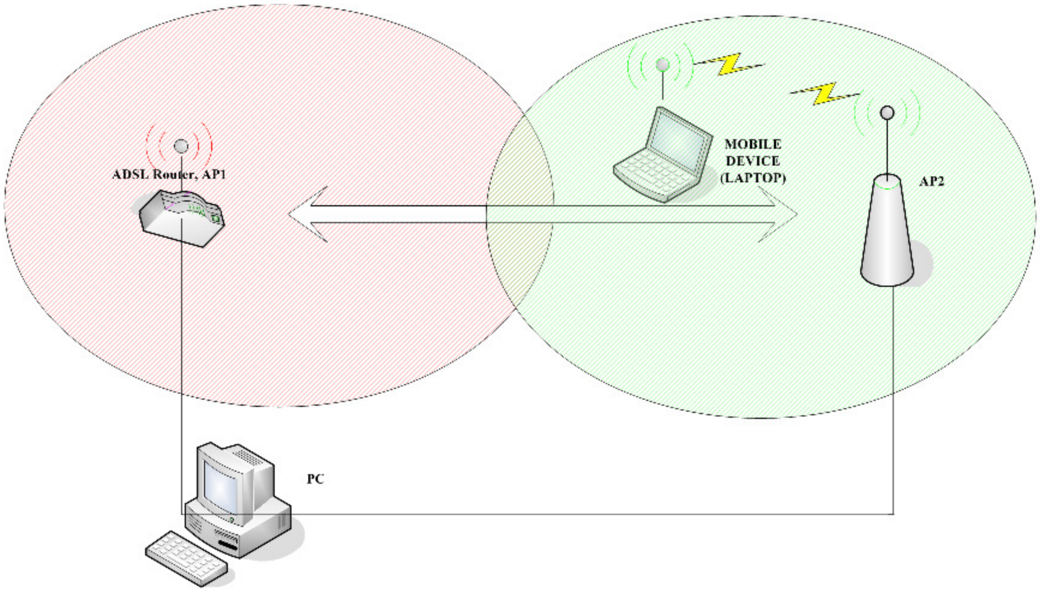


Fig 4.1: project block diagram

4.3 Implementation and Testing:

After installing the hardware and software components, and designing the handoff code, we need to use the project components to investigate and study the potential of the idea proposed through this report .

Chapter five

Hardware & Software system design

5.1 Preface.

5.2 Schematic design.

5.2.1 Hardware part.

5.2.1.1 Network diagram and design.

5.2.1.2 Configuring the network.

5.2.2 Software part.

Chapter five

Hardware & Software system design

5.1 Preface:

This chapter shows the hardware and software design used in implementing the idea of this project, where as mentioned earlier there will be hardware (Network includes a server, client laptop, access points and a switch) and software (windows server, linux, C-language), and this will give the main idea for implementing the project by using another access points, another wireless network adaptor as well as the software part.

5.2 Schematic design:

This section illustrates a detailed design for the project's network that will be used as well as the schematic design for all of the components together.

5.2.1 Hardware part:

In hardware part we needed a network in order to apply the handoff solution and to use as a testing environment, to fulfill the requirements we needed a PC server, laptop as client, two access points, switch, and network cables, when using these items we were able to simulate a network such as internet or network in our university.

5.2.1.1 Network diagram and design:

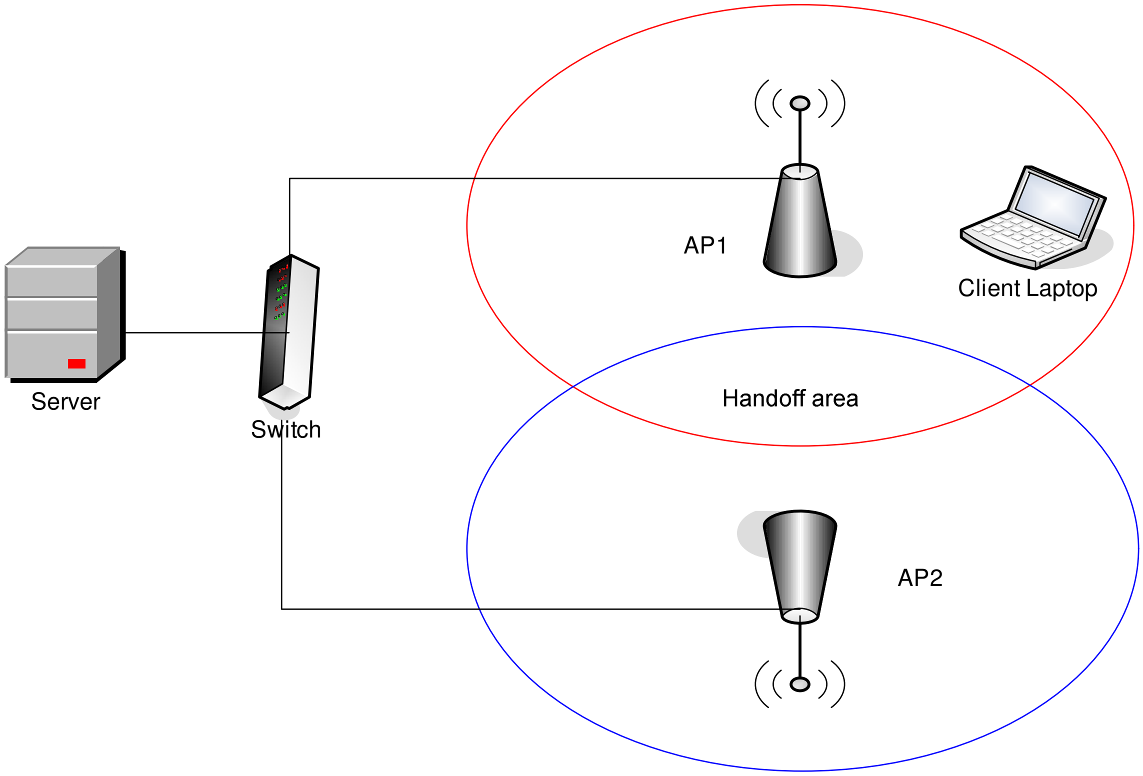


Fig 5.1 Project's network diagram.

5.2.1.2 Configuring the network:

In order to have a network it needs more than connecting the hardware items together, here we are going to choose a range of IP's (Internet Protocol) for each part of the network, where they should be in the same range in order to communicate correctly, as follows:

IP for PC server: 192.168.2.8

IP for First access point: 192.168.2.10

IP for second access point: 192.168.2.11

For client Laptop we need to set the IP as automatic, where the server will handle the IP assigning for clients in the range of 192168.2.100 to 192.168.2.120 and this option is available from the DHCP (Dynamic Host Configuration Protocol).

For the Access points, previously we were going to connect the first one to the server as an access point and the second one as a repeater; in order to reduce the cabling, however we chosen to connect them both as access points to the server through a switch by using network cables, where this will reduce the delay in assigning IPs and communicating with the server.

5.2.2 Software part:

In this section we will talk about the software design; at first we installed the Linux as operating system on the client laptop because it is an open source and suitable for testing and programming, and we chosen fedora 12 because Fedora is a Linux based operating system that show, which is a free and open source software with the ability to modify, develop and distribute.

When installing the Linux we activated all the services related to networking and communicating with windows, where as mentioned before the server we are using is a windows based server, so we need to activate all the services and protocols in linux, in order to be a part of a windows based network.

Then we installed the MadWiFi driver because MadWifi is one of the most advanced WLAN drivers available for Linux, also by using madwifi and the IWCONFIG commands, we will be able to edit the network parameters including the active access point, channel, frequency, in short terms almost all the network parameters. The MadWiFi works with the linux network editing commands such as iwconfig and the iwlist scan, where these two commands are the major commands will be used in our approach. We used a C++ language to create C++ program for implement MadWifi commands that using to applying Handoff mechanism.

Finally we installed Iperf program to measure the bandwidth or throughput and the quality of a network link. Iperf uses different capacities of TCP (Transmission Control Protocol) to provide statistics about network links, and we measured the throughput by running a TCP tests where the TCP used to check that the packets are correctly sent to the receiver, and the Iperf can be installed very easily on any platform O.S (UNIX/Linux or Microsoft Windows system). One host must be set as client, the other one as server, in our project the laptob is the client and the PC is the server, but we used different installations due to the fact we are using two O.Ss LINUX & WINDOWS.

After the two parts of project's network Hardware and software were ready to use for implementing the idea of our project, then we started work in our experiments to reach the required results.

Chapter six

Implementation and testing

Chapter six

Implementation and testing

6.1 preface:

In this chapter we are going to show the implementation and testing processes for our system. The system testing is an important and critical step in implementing any system, where the system has more than one issue to be tested, however some system parts include software and others include hardware.

After testing each component and each subsystem that makes up this project, the implementation process is done and will take many testing to insure that there are no errors. This implementation will be done using different components and tools as it will be discussed later in this chapter.

6.2 Testing the project components:

As we mentioned in chapter five (Hardware & Software Design), after install the required software for the laptop such as Linux, Iperf and the MadWifi, we can use IWCONFIG to test whether the wireless network adaptor is working or not by simply typing the following command in the terminal window:

```
[root@Samah ~]# iwconfig
```

Where the result will be:

```
wlan1     IEEE 802.11bg  ESSID:"AP1"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:57:1E:99
          Bit Rate=36 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off
          Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=6 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
          Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
          Missed beacon:0
```

This window show the ESSID, the MAC address and the signal level and other information about the access point that associated with it, and here we see the AP1 is the access point that the laptop associated with it , the MAC address for this access point is 00:1F:1F:57:1E:99 , and the signal level is 6dBm at the moment of taking IWCONFIG.

Like this we examined if our wireless USB adaptor executed the command of the madwifi driver or not.

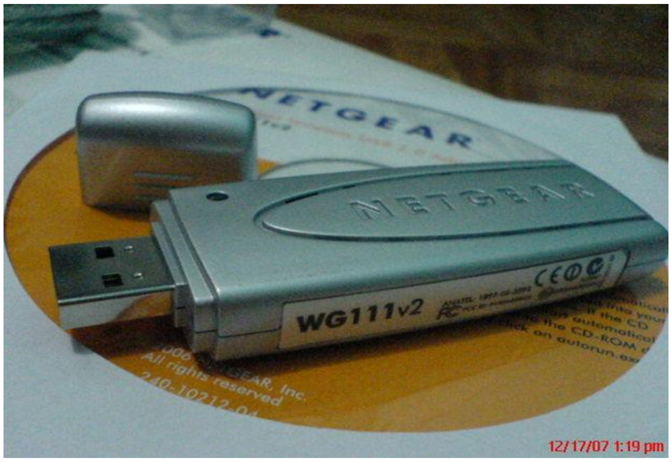


Fig 6.1 wireless USB adaptor (NETGEAR).

For the network used in this project, we mentioned that we need to change the IP addresses for the PC server and the two access points in order to be in the same range and communicate correctly.

we changed the settings of the access points, where we changed the IP address for both and we placed it in the same range and we changed the channel to put the two access points on the same channel, and changed the ESSID for both access points to give each access point different ESSID and the changes will be as follows:

The first access point:

ESSID: AP1.

Channel: 11.

IP: 192.168.2.10

The second access point:

ESSID: AP2.

Channel: 11.

IP: 192.168.2.11.

The way to test the network is by using PING command in the CMD window using the IP's for example:

C:\ ping 192.168.2.10

The result is:

```
Microsoft Windows [Version 6.0.6000]

Copyright   (c)   2006   Microsoft   Corporation.    All   rights
reserved.

C:\Users\SAMAH>ping 192.168.2.10

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=1ms TTL=255

Reply from 192.168.2.10: bytes=32 time=1ms TTL=255

Reply from 192.168.2.10: bytes=32 time=1ms TTL=255

Reply from 192.168.2.10: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.2.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Fig 6.2 EDIMAX (Wireless 802.11g Access point)

Also we need to run the ping command in the Linux terminal window; in order to make sure that the server already assigned the Laptop with a valid IP to be part of the network.

6.3 Implementation:

This section illustrates the implementation of our project over the project's network, the project's network works as follows:

The laptop (client) is connected to the server through the first access point and when can test the connection by using the ping command or by running the Iperf , back to the main idea, when the laptop moves away from the first access point in the direction of the second access point, the received power from the first access point will decrease through the moving, and the power received from the second access point increases , the laptop arrives to make handoff from the first access point to the second access point, then the power received at the laptop from the second access point will increase.

6.4 Experiments & Testing:

This section demonstrates measurement for the experiments used to test our project idea; we will have two approaches the default and ours

6.4.1 Default approach:

In this section we show how the handoff process will affect the connection and the delay occurs when the client laptop perform the handoff process automatically.

After running the Iperf on the PC server using:

```
c:\ Iperf  -s.
```

And running the Iperf on the client laptop using:

```
[root@Samah ~]# iperf -c 192.168.2.8 -n 100k -t
100 -i5
```

The result is:

```
------------------------------------------------------------
Client connecting to 192.168.2.8, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.2.100 port 51712 connected with 192.168.2.8
port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 5.0 sec  8.27 MBytes  13.9 Mbits/sec
[  3]  5.0-10.0 sec  8.34 MBytes  14.0 Mbits/sec
[  3] 10.0-15.0 sec  8.16 MBytes  13.7 Mbits/sec
[  3] 15.0-20.0 sec  8.02 MBytes  13.5 Mbits/sec
[  3] 20.0-25.0 sec  8.19 MBytes  13.7 Mbits/sec
[  3] 25.0-30.0 sec  8.42 MBytes  14.1 Mbits/sec
[  3] 30.0-35.0 sec  7.71 MBytes  12.9 Mbits/sec
[  3] 35.0-40.0 sec  7.88 MBytes  13.2 Mbits/sec
[  3] 40.0-45.0 sec  6.25 MBytes  10.5 Mbits/sec
[  3] 45.0-50.0 sec  5.77 MBytes  9.69 Mbits/sec
[  3] 50.0-55.0 sec  7.30 MBytes  12.2 Mbits/sec
[  3] 55.0-60.0 sec  6.84 MBytes  11.5 Mbits/sec
[  3] 60.0-65.0 sec  6.27 MBytes  10.5 Mbits/sec
[  3] 65.0-70.0 sec  8.39 MBytes  14.1 Mbits/sec
[  3] 70.0-75.0 sec  8.27 MBytes  13.9 Mbits/sec
[  3] 75.0-80.0 sec  6.94 MBytes  11.6 Mbits/sec
[  3] 80.0-85.0 sec  5.68 MBytes  9.53 Mbits/sec
[  3] 85.0-90.0 sec  7.45 MBytes  12.5 Mbits/sec
[  3] 90.0-95.0 sec  8.78 MBytes  14.7 Mbits/sec
[  3] 95.0-100.0 sec  8.88 MBytes  14.9 Mbits/sec
[  3]  0.0-100.0 sec   152 MBytes  12.7 Mbits/sec
```

We used this method in three steps:

Step 1 : Connected to AP1

```
[root@Samah ~]# iwconfig

wlan1     IEEE 802.11bg  ESSID:"AP1"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:57:1E:99
          Bit Rate=6 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=63/70  Signal level=-47 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
          Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
          Missed beacon:0
----------
[root@Samah ~]# iperf -c 192.168.2.8 -n 100k -t 100 -i5
------------------------------------------------------------
Client connecting to 192.168.2.8, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.2.100 port 36749 connected with 192.168.2.8
port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 5.0 sec  1.82 MBytes  3.05 Mbits/sec
[  3]  5.0-10.0 sec  2.24 MBytes  3.76 Mbits/sec
[  3] 10.0-15.0 sec  2.12 MBytes  3.55 Mbits/sec
[  3] 15.0-20.0 sec  2.00 MBytes  3.36 Mbits/sec
[  3] 20.0-25.0 sec  1.93 MBytes  3.24 Mbits/sec
[  3] 25.0-30.0 sec  1.94 MBytes  3.25 Mbits/sec
[  3] 30.0-35.0 sec  1.80 MBytes  3.03 Mbits/sec
[  3] 35.0-40.0 sec  1.73 MBytes  2.90 Mbits/sec
[  3] 40.0-45.0 sec  1.77 MBytes  2.96 Mbits/sec
[  3] 45.0-50.0 sec  1.91 MBytes  3.20 Mbits/sec
[  3] 50.0-55.0 sec  1.68 MBytes  2.82 Mbits/sec
[  3] 55.0-60.0 sec  1.58 MBytes  2.65 Mbits/sec
[  3] 60.0-65.0 sec  2.00 MBytes  3.36 Mbits/sec
[  3] 65.0-70.0 sec  1.56 MBytes  2.62 Mbits/sec
[  3] 70.0-75.0 sec  1.34 MBytes  2.25 Mbits/sec
[  3] 75.0-80.0 sec  1.34 MBytes  2.25 Mbits/sec
[  3] 80.0-85.0 sec  1.41 MBytes  2.36 Mbits/sec
[  3] 85.0-90.0 sec  1.48 MBytes  2.49 Mbits/sec
[  3] 90.0-95.0 sec  1.42 MBytes  2.39 Mbits/sec
[  3] 95.0-100.0 sec  1.57 MBytes  2.63 Mbits/sec
[  3]  0.0-100.0 sec  34.6 MBytes  2.91 Mbits/sec
```

Step2: In the handoff area.

```
wlan1     IEEE 802.11bg  ESSID:"AP1"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:57:1E:99
          Bit Rate=5.5 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=46/70  Signal level=-64 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
         Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
         Missed beacon:0
-----
wlan1     IEEE 802.11bg  ESSID:"AP1"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:57:1E:99
          Bit Rate=11 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=44/70  Signal level=-66 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
         Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
         Missed beacon:0
------
Wlan1     IEEE 802.11bg  Mode:Managed  Frequency:2.437 GHz
          Access Point: Not-Associated   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0
         Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
         Missed beacon:0
------ AP2

wlan1     IEEE 802.11bg  ESSID:"AP2"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:5C:31:00
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=58/70  Signal level=-52 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
          Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
          Missed beacon:0
-------
wlan1     IEEE 802.11bg  ESSID:"AP2"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:5C:31:00
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=63/70  Signal level=-47 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
          Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
          Missed beacon:0
-------------
[root@Samah ~]# iperf -c 192.168.2.8 -n 100k -t 300 -i5
------------------------------------------------------------
Client connecting to 192.168.2.8, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.2.100 port 51095 connected with 192.168.2.8
port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 5.0 sec  1.05 MBytes  1.76 Mbits/sec
[  3]  5.0-10.0 sec  1.49 MBytes  2.50 Mbits/sec
[  3] 10.0-15.0 sec    848 KBytes  1.39 Mbits/sec
[  3] 15.0-20.0 sec  1.37 MBytes  2.29 Mbits/sec
[  3] 20.0-25.0 sec    344 KBytes    564 Kbits/sec
[  3] 25.0-30.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 30.0-35.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 35.0-40.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 40.0-45.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 45.0-50.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 50.0-55.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 55.0-60.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 60.0-65.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 65.0-70.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 70.0-75.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 75.0-80.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 80.0-85.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 85.0-90.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 90.0-95.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 95.0-100.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 100.0-105.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 105.0-110.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 110.0-115.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 115.0-120.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 120.0-125.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 125.0-130.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 130.0-135.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 135.0-140.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 140.0-145.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 145.0-150.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 150.0-155.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 155.0-160.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 160.0-165.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 165.0-170.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 170.0-175.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 175.0-180.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 180.0-185.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 185.0-190.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 190.0-195.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 195.0-200.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 200.0-205.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 205.0-210.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 210.0-215.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 215.0-220.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 220.0-225.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 225.0-230.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 230.0-235.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 235.0-240.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 240.0-245.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 245.0-250.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 250.0-255.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 255.0-260.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 260.0-265.0 sec  0.00 Bytes  0.00 bits/sec
[  3] 265.0-270.0 sec  1.19 MBytes  1.99 Mbits/sec
[  3] 270.0-275.0 sec  1.90 MBytes  3.19 Mbits/sec
[  3] 275.0-280.0 sec  2.16 MBytes  3.63 Mbits/sec
[  3] 280.0-285.0 sec  2.25 MBytes  3.77 Mbits/sec
[  3] 285.0-290.0 sec  2.62 MBytes  4.39 Mbits/sec
[  3] 290.0-295.0 sec  2.45 MBytes  4.10 Mbits/sec
[  3] 295.0-300.0 sec  2.25 MBytes  3.77 Mbits/sec
[  3]  0.0-300.0 sec  19.9 MBytes    556 Kbits/sec
```

Step3: connected to AP2.

```
[root@Samah ~]# iwconfig



wlan1     IEEE 802.11bg  ESSID:"AP2"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:5C:31:00
          Bit Rate=11 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-31 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
          Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
          Missed beacon:0
---------
[root@Samah ~]# iperf -c 192.168.2.8 -n 100k -t 100 -i5
```

```
------------------------------------------------------------
Client connecting to 192.168.2.8, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.2.100 port 49462 connected with 192.168.2.8
port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 5.0 sec  1.67 MBytes  2.80 Mbits/sec
[  3]  5.0-10.0 sec  2.35 MBytes  3.95 Mbits/sec
[  3] 10.0-15.0 sec  1.70 MBytes  2.84 Mbits/sec
[  3] 15.0-20.0 sec  1.72 MBytes  2.88 Mbits/sec
[  3] 20.0-25.0 sec  1.62 MBytes  2.73 Mbits/sec
[  3] 25.0-30.0 sec  2.27 MBytes  3.80 Mbits/sec
[  3] 30.0-35.0 sec  2.01 MBytes  3.37 Mbits/sec
[  3] 35.0-40.0 sec  1.60 MBytes  2.69 Mbits/sec
[  3] 40.0-45.0 sec  1.30 MBytes  2.18 Mbits/sec
[  3] 45.0-50.0 sec  1.99 MBytes  3.34 Mbits/sec
[  3] 50.0-55.0 sec  2.36 MBytes  3.96 Mbits/sec
[  3] 55.0-60.0 sec  1.44 MBytes  2.41 Mbits/sec
[  3] 60.0-65.0 sec  1.21 MBytes  2.03 Mbits/sec
[  3] 65.0-70.0 sec  1.53 MBytes  2.57 Mbits/sec
[  3] 70.0-75.0 sec  2.58 MBytes  4.33 Mbits/sec
[  3] 75.0-80.0 sec  2.14 MBytes  3.59 Mbits/sec
[  3] 80.0-85.0 sec  1.63 MBytes  2.74 Mbits/sec
[  3] 85.0-90.0 sec  1.27 MBytes  2.14 Mbits/sec
[  3] 90.0-95.0 sec  2.12 MBytes  3.57 Mbits/sec
[  3] 95.0-100.0 sec  1.36 MBytes  2.28 Mbits/sec
[  3]  0.0-100.1 sec  35.9 MBytes  3.01 Mbits/sec
```

6.4.2 Our approach:

In this section we show how the handoff process will affect the connection and the delay occurs when the client laptop perform the handoff process by using the MADWifi command.

After running the Iperf on the PC server using :

```
c:\ Iperf  -s.
```

And running the Iperf on the client laptop using:

```
[root@Samah ~]# iperf -c 192.168.2.8 -n 100k -t
100 -i5
```

The result is:

```
------------------------------------------------------------
Client connecting to 192.168.2.8, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.2.100 port 51712 connected with 192.168.2.8
port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 5.0 sec  8.27 MBytes  13.9 Mbits/sec
[  3]  5.0-10.0 sec  8.34 MBytes  14.0 Mbits/sec
[  3] 10.0-15.0 sec  8.16 MBytes  13.7 Mbits/sec
[  3] 15.0-20.0 sec  8.02 MBytes  13.5 Mbits/sec
[  3] 20.0-25.0 sec  8.19 MBytes  13.7 Mbits/sec
[  3] 25.0-30.0 sec  8.42 MBytes  14.1 Mbits/sec
[  3] 30.0-35.0 sec  7.71 MBytes  12.9 Mbits/sec
[  3] 35.0-40.0 sec  7.88 MBytes  13.2 Mbits/sec
[  3] 40.0-45.0 sec  6.25 MBytes  10.5 Mbits/sec
[  3] 45.0-50.0 sec  5.77 MBytes  9.69 Mbits/sec
[  3] 50.0-55.0 sec  7.30 MBytes  12.2 Mbits/sec
[  3] 55.0-60.0 sec  6.84 MBytes  11.5 Mbits/sec
[  3] 60.0-65.0 sec  6.27 MBytes  10.5 Mbits/sec
[  3] 65.0-70.0 sec  8.39 MBytes  14.1 Mbits/sec
[  3] 70.0-75.0 sec  8.27 MBytes  13.9 Mbits/sec
[  3] 75.0-80.0 sec  6.94 MBytes  11.6 Mbits/sec
[  3] 80.0-85.0 sec  5.68 MBytes  9.53 Mbits/sec
[  3] 85.0-90.0 sec  7.45 MBytes  12.5 Mbits/sec
[  3] 90.0-95.0 sec  8.78 MBytes  14.7 Mbits/sec
[  3] 95.0-100.0 sec  8.88 MBytes  14.9 Mbits/sec
[  3]  0.0-100.0 sec    152 MBytes  12.7 Mbits/sec
```

We used this method in three steps:

Step 1 : Connected to AP1

```
[root@Samah ~]# iwconfig

wlan1     IEEE 802.11bg  ESSID:"AP1"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:57:1E:99
          Bit Rate=36 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=6 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
          Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
          Missed beacon:0
-----------

[root@Samah ~]# iperf -c 192.168.2.8 -n 100k -t 100 -i5
------------------------------------------------------------
Client connecting to 192.168.2.8, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.2.100 port 51712 connected with 192.168.2.8
port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 5.0 sec  8.27 MBytes  13.9 Mbits/sec
[  3]  5.0-10.0 sec  8.34 MBytes  14.0 Mbits/sec
[  3] 10.0-15.0 sec  8.16 MBytes  13.7 Mbits/sec
[  3] 15.0-20.0 sec  8.02 MBytes  13.5 Mbits/sec
[  3] 20.0-25.0 sec  8.19 MBytes  13.7 Mbits/sec
[  3] 25.0-30.0 sec  8.42 MBytes  14.1 Mbits/sec
[  3] 30.0-35.0 sec  7.71 MBytes  12.9 Mbits/sec
[  3] 35.0-40.0 sec  7.88 MBytes  13.2 Mbits/sec
[  3] 40.0-45.0 sec  6.25 MBytes  10.5 Mbits/sec
[  3] 45.0-50.0 sec  5.77 MBytes  9.69 Mbits/sec
[  3] 50.0-55.0 sec  7.30 MBytes  12.2 Mbits/sec
[  3] 55.0-60.0 sec  6.84 MBytes  11.5 Mbits/sec
[  3] 60.0-65.0 sec  6.27 MBytes  10.5 Mbits/sec
[  3] 65.0-70.0 sec  8.39 MBytes  14.1 Mbits/sec
[  3] 70.0-75.0 sec  8.27 MBytes  13.9 Mbits/sec
[  3] 75.0-80.0 sec  6.94 MBytes  11.6 Mbits/sec
[  3] 80.0-85.0 sec  5.68 MBytes  9.53 Mbits/sec
[  3] 85.0-90.0 sec  7.45 MBytes  12.5 Mbits/sec
[  3] 90.0-95.0 sec  8.78 MBytes  14.7 Mbits/sec
[  3] 95.0-100.0 sec  8.88 MBytes  14.9 Mbits/sec
[  3]  0.0-100.0 sec    152 MBytes  12.7 Mbits/sec
```

Step2: In the handoff area.

```
[root@Samah ~]# iwconfig

wlan1     IEEE 802.11bg  ESSID:"AP1"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:57:1E:99
          Bit Rate=11 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=65/70  Signal level=-45 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
          Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
          Missed beacon:0

---------- to AP2
wlan1     IEEE 802.11bg  ESSID:"AP2"
```

```
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:5C:31:00
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-35 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
          Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
          Missed beacon:0
```

```
[root@Samah ~]# iperf -c 192.168.2.8 -n 100k -t 100 -i5
------------------------------------------------------------
Client connecting to 192.168.2.8, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.2.100 port 49587 connected with 192.168.2.8
port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 5.0 sec    872 KBytes  1.43 Mbits/sec
[  3]  5.0-10.0 sec  1.67 MBytes  2.80 Mbits/sec
[  3] 10.0-15.0 sec  1.38 MBytes  2.32 Mbits/sec
[  3] 15.0-20.0 sec  1.66 MBytes  2.78 Mbits/sec
[  3] 20.0-25.0 sec  1.41 MBytes  2.37 Mbits/sec
[  3] 25.0-30.0 sec  1.43 MBytes  2.40 Mbits/sec
[  3] 30.0-35.0 sec  72.0 KBytes    118 Kbits/sec   ***
[  3] 35.0-40.0 sec    504 KBytes    826 Kbits/sec  ***
[  3] 40.0-45.0 sec  3.22 MBytes  5.40 Mbits/sec
[  3] 45.0-50.0 sec  2.74 MBytes  4.60 Mbits/sec
[  3] 50.0-55.0 sec  2.27 MBytes  3.81 Mbits/sec
[  3] 55.0-60.0 sec  2.47 MBytes  4.14 Mbits/sec
[  3] 60.0-65.0 sec  3.01 MBytes  5.05 Mbits/sec
[  3] 65.0-70.0 sec  3.05 MBytes  5.11 Mbits/sec
[  3] 70.0-75.0 sec  3.12 MBytes  5.24 Mbits/sec
```

Step3: connected to AP2.

```
[root@Samah ~]# iwconfig

wlan1     IEEE 802.11bg  ESSID:"AP2"
          Mode:Managed  Frequency:2.462 GHz
          Access Point: 00:1F:1F:5C:31:00
          Bit Rate=36 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=70/70  Signal level=-15 dBm
          Rx invalid nwid:0  Rx invalid crypt:0
          Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0
          Missed beacon:0
```

```
---------
[root@Samah ~]# iperf -c 192.168.2.8 -n 100k -t 100 -i5
------------------------------------------------------------
Client connecting to 192.168.2.8, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  3] local 192.168.2.100 port 39153 connected with 192.168.2.8
port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 5.0 sec  4.42 MBytes  7.42 Mbits/sec
[  3]  5.0-10.0 sec  4.96 MBytes  8.32 Mbits/sec
[  3] 10.0-15.0 sec  5.12 MBytes  8.59 Mbits/sec
[  3] 15.0-20.0 sec  4.27 MBytes  7.17 Mbits/sec
[  3] 20.0-25.0 sec  4.23 MBytes  7.10 Mbits/sec
[  3] 25.0-30.0 sec  4.45 MBytes  7.47 Mbits/sec
[  3] 30.0-35.0 sec  6.06 MBytes  10.2 Mbits/sec
[  3] 35.0-40.0 sec  3.89 MBytes  6.53 Mbits/sec
[  3] 40.0-45.0 sec  4.30 MBytes  7.22 Mbits/sec
[  3] 45.0-50.0 sec  4.22 MBytes  7.08 Mbits/sec
[  3] 50.0-55.0 sec  5.63 MBytes  9.45 Mbits/sec
[  3] 55.0-60.0 sec  4.60 MBytes  7.72 Mbits/sec
[  3] 60.0-65.0 sec  3.99 MBytes  6.70 Mbits/sec
[  3] 65.0-70.0 sec  4.25 MBytes  7.13 Mbits/sec
[  3] 70.0-75.0 sec  4.70 MBytes  7.88 Mbits/sec
[  3] 75.0-80.0 sec  6.29 MBytes  10.6 Mbits/sec
[  3] 80.0-85.0 sec  4.08 MBytes  6.84 Mbits/sec
[  3] 85.0-90.0 sec  4.22 MBytes  7.08 Mbits/sec
[  3] 90.0-95.0 sec  4.44 MBytes  7.44 Mbits/sec
[  3] 95.0-100.0 sec  5.72 MBytes  9.59 Mbits/sec
[  3]  0.0-100.0 sec  93.9 MBytes  7.87 Mbits/sec
```

6.5 Graphs and Results:

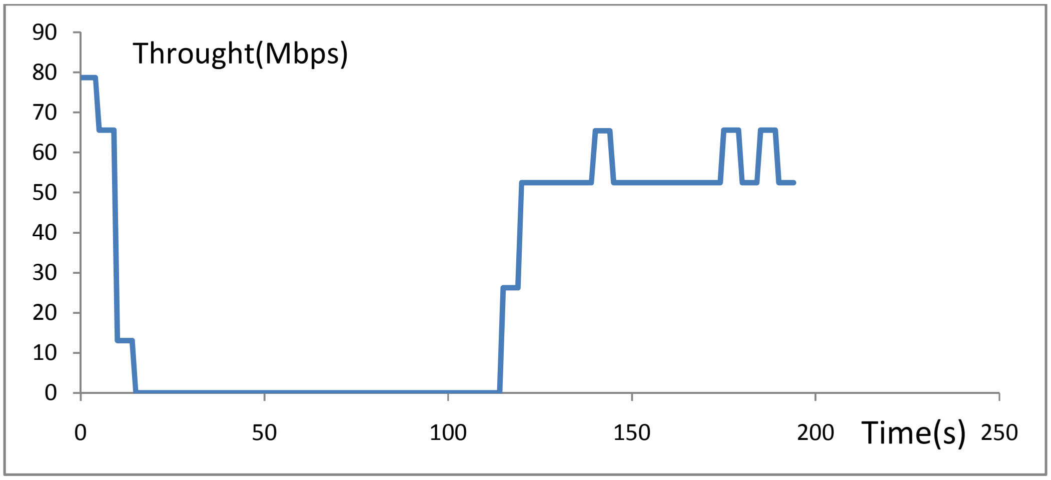


Fig 6.1 Default approach HANDOFF

This figure shows the relationship between the throughput in (MBPS) and the time in second in default approach .When the laptop moves away from the first access point in the direction of the second access point, Then the throughput that will be reading from the client will decrease continuously until reach to zero and continue so for a period of time almost 100 second Then when the laptop connected to the second access point then the value of throughput increase again to reach 4.5 MBPS.

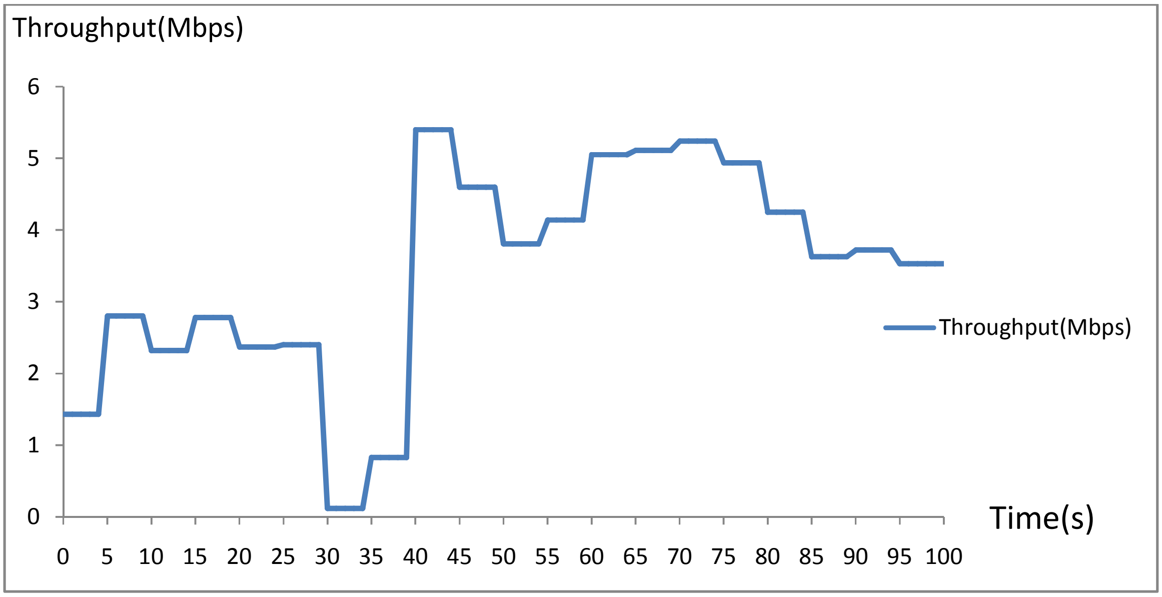


Fig 6.2 our approach for HANDOFF

This figure shows the relationship between the throughput in (MBPS) and the time in (sec) in our approach. Where in this figure the handoff occur by using iwconfig command. When the laptop moves away from the first access point in the direction of the second access point, Then the value of throughput decrease but does not reach to zero so the handoff happen in short time without disconnection. Then when the laptop connected to the second access point then the throughput will increase again.

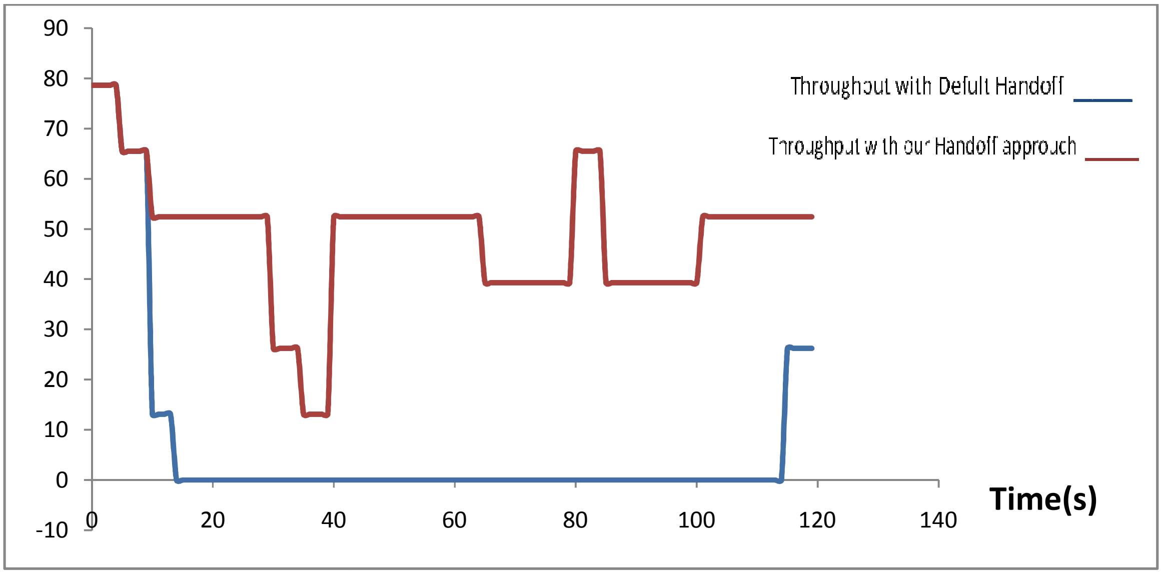


Fig 6.3 Comparison between our approach for HANDOFF & the Default Handoff.

This graph shows a comparison between the default and our approach and we noticed that:

1-the handoff process in our approach take a time less than the time needed in default approach to occur handoff ;in default way the handoff need 200 second but in our approach it need just 5 second.

2-in our approach the disconnection not occur but in default approach the disconnection happen and continue for a period of time.

3-the value of throughput in default approach is decrease so much and reach to zero but in our approach the value of the throughput decrease but not reach to zero .

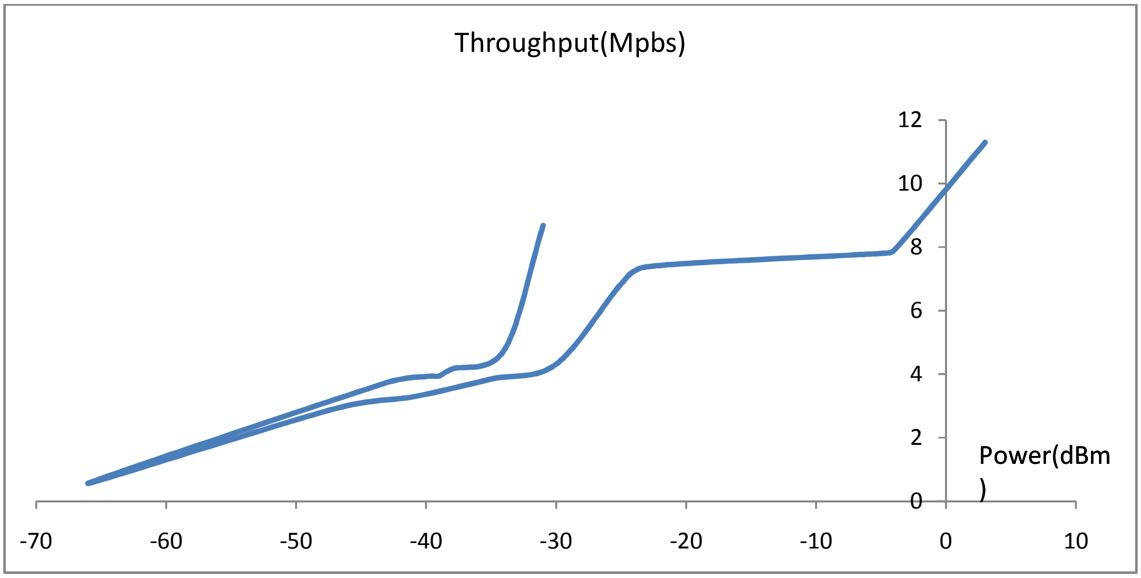


Fig 6.4 Default approach HANDOFF

This figure shows the relationship between the throughput in Mega Bit per Second (MBPS) and the power in dBm. Where the power value change with distance between laptop and access point .When the laptop moves away from the first access point in the direction of the second access point, Then the received power from the first access point will decrease and when the power will decrease the throughput at this power will decrease to reach zero when the handoff happens in default way which takes a long time to occur. And we show a significant decrease in the power sometimes reaches to -70 dBm. Then when the laptop connected to the second access point and the received power from this access point will increase and the throughput will increase.

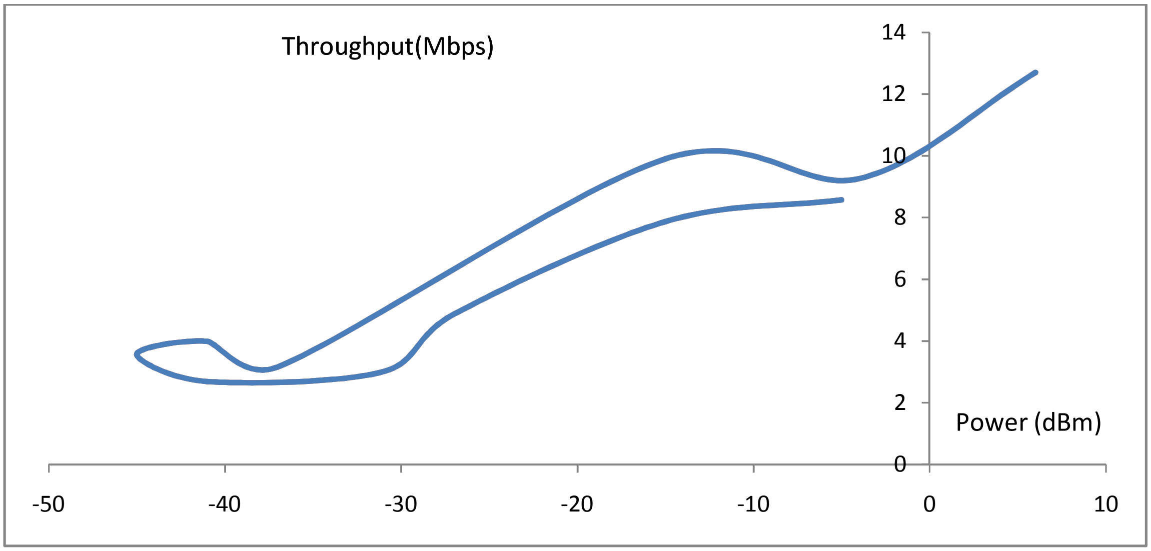


Fig 6.5 our approach for HANDOFF

This figure shows the relationship between the throughput in (MBPS) and the power in dBm but in our approach .When the laptop moves away from the first access point in the direction of the second access point, Then the received power from the first access point will decrease and when the power will decrease the throughput at this power will decrease . when the received power of the first access point reach to -45 dBm we give the orders of the handoff even the laptop to move the connection from first access point to second access point. Then when the laptop connected to the second access point and the received power from this access point will increase and the throughput will increase.

Chapter Seven

Conclusion & problems

7.1 Preface.

7.2 Conclusion.

7.3 Problems.

- 7.3.1 Hardware problems
- 7.3.2 Software problems

Chapter Seven

Conclusion & Problems

7.1 Preface:

This chapter describes and gives a conclusion for our project and a complete look over the entire from project from the beginning. It also provides suggestion that could be useful for developing the idea in future.

7.2 Conclusion:

If we go to our subject and reevaluate the full discussion in details the following can be seen.

Our project is about improving mobile device handoff between two or more access points (APs) in wireless local area network (WLAN), the idea of our project done ; where when we have done the experiments of our project we notes the following:

- When the handoff happens by default the period of handoff was very long compared with our approach plus the default handoff will result in completely disconnection, while using our approach the mobile will connect directly without noticed disconnection.

- The handoff happened in two cases; default and our approach , but in default way the handoff happens when the power decreased so much and in sometimes it disconnect completely, but in our approach the handoff does not waiting the value of the received power to decrease so much it's happen before that.

7.3 Problems:

The problems we faced during this here have two phases' hardware and software problem and sections below illustrate them.

7.3.1 Hardware problems:

- The first and the most difficult problem was the waiting for components (wireless USB adaptor) from the last month of the first semester to the second month on current semester.

- Problem in the network themselves.
- The coverage area of the access point was large, so it was difficult to take the measurements cause we need to walk a large distance to reach to handoff, and to solve these problem we removed the antenna of one of the access point to reduce the converge area of it.

7.3.2 Software problems:

- The Linux breakdown many times and we faced difficulties to deal with Linux causes the first time deal with it.
- We used many copies of Linux till find the suitable copy and it take a long time to do this, and the copy (fedora 12) it is testing copy.
- We faced problems to installation the MadWifi driver and using these command.
- The worst problem in our project when we searching a suitable traffic generator.

References

Books:

[1] Simon Haykin, "Communication Systems", 4th edition, johan wiley &sons, Inc,2001

[2]Gray J. Mullett , " Wireless Telecommunications Systems and Networks" ,Thomas Delmar learning, 2006

[3]Bernard Sklar ,"Digital Communications Fundamentals and Applications", 2nd edition, Prentice Hall PTR,2001

[4] Andrea goldsmith," Wireless Communication", Cambridge University Press,2005

[5]Jochen Schiller, "Mobile Communication", 2nd edition,

Web Sites:

http://www.rdoffice.ndhu.edu.tw/exchange/abroad/abroad96/LCHSH.paper.pdf

http://www.kjhole.com/Standards/WiFi/WiFi-PDF/WLAN4alt.pdf

http://www.tslab.ssvl.kth.se/csd/projects/0311/elit-std02-bwl-01.pdf

http://www.mlab.t.u-tokyo.ac.jp/attachment/file/5/08-02-1-okjaeouk-IN.pdf

http://ps.mcicvermont.com/appdocs/lps/Strategies%20to%20Improve%20Handoff%20Communication.pdf

http://www.retrevo.com/d/ds/progress?doc=4de1180db9b837ce0d8c1adc0064e4ab

http://www.hp.com/rnd/library/pdf/understandingBluetooth.pdf

http://mmlab.snu.ac.kr/publications/docs/IEEE_CST_shpack.pdf

DATASHEETS

NETGEAR 54 Mbps Wireless USB 2.0 Adapter WG111v3 User Manual

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10240-01
April 2007

Technical Support

For customer support see *http://kbserver.netgear.com/kb_web_files/n10005.asp*

NETGEAR, INC. Support Information

Phone: 1-888-NETGEAR, for US & Canada only. For other countries, see your support information card.

E-mail: support@netgear.com

North American NETGEAR website: *http://www.netgear.com*

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Maximum Wireless Signal Rate Derived from IEEE Standard 802.11 Specifications

Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Safety and Regulatory Notices

FCC Statement

The WG111v3 has been tested and complies with the specifications for a Class B digital device, pursuant to Part 15 of the FCC Rules.

Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment or devices
- Connect the equipment to an outlet other than the receiver's
- Consult a dealer or an experienced radio/TV technician for assistance

FCC Caution: Any change or modification to the product not expressly approved by Netgear could void the user's authority to operate the device.

FCC RF Radiation Exposure and SAR Statements

SAR Statement

The Netgear WG111v3 has been tested for body-worn Specific Absorption Rate (SAR) compliance. The FCC has established detailed SAR requirements and has established that these requirements have been met while installed in host notebook computer.

RF Exposure Information

The radio module has been evaluated under FCC Bulletin OET 65C (01-01) and found to be compliant to the requirements as set forth in CFR 47 Sections, 2.1093, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. This model meets the applicable government requirements for exposure to radio frequency waves. The highest SAR level measured for this device was 1.3 W/kg.

Canadian Department of Communications Industry Canada (IC) Notice

This Class B digital apparatus complies with Canadian ICES-003 and RSS-210. Cet appareil numérique de la classe B est conforme à la norme NMB-003 et CNR-210 du Canada.

"To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing."

"Pour empêcher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit être utilisé à l'intérieur et devrait être placé loin des fenêtres afin de fournir un écran de blindage maximal. Si le matériel (ou son antenne d'émission) est installé à l'extérieur, il doit faire l'objet d'une licence."

Europe - EU Declaration of Conformity with Regard to R&TTE Directive 1999/5/EC

A printed copy of the EU Declaration of Conformity certificate for this product is provided in the WG111v3 product package.

Èesky [Czech]	NETGEAR, Inc. tímto prohlašuje, že tento NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 je ve shodì se základními požadavky a dalšími pøíslušnými ustanoveními smìrnice 1999/5/ES.
Dansk [Danish]	Undertegnede NETGEAR, Inc. erklærer herved, at følgende udstyr NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt NETGEAR, Inc., dass sich das Gerät NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab NETGEAR, Inc. seadme NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.

English	Hereby, NETGEAR, Inc., declares that this NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente NETGEAR, Inc. declara que el NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ NETGEAR, Inc. ΔΗΛΩΝΕΙ ΟΤΙ NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente NETGEAR, Inc. déclare que l'appareil NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente NETGEAR, Inc. dichiara che questo NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo NETGEAR, Inc. deklarç, ka NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 atbilst Direktîvas 1999/5/EK bûtiskajâm prasîbâm un citiem ar to saistîtajiem noteikumiem.
Lietuviø [Lithuanian]	Šiuo NETGEAR, Inc. deklaruoja, kad šis NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart NETGEAR, Inc. dat het toestel NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, NETGEAR, Inc., jiddikjara li dan NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 jikkonforma mal-tiijiet essenzjali u ma provvedimenti orajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, NETGEAR, Inc. nyilatkozom, hogy a NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR, Inc. oœwiadcza, ¿e NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 jest zgodny z zasadniczymi wymogami oraz pozosta³ymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	NETGEAR, Inc. declara que este NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR, Inc. izjavlja, da je ta NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 v skladu z bistvenimi zahtevami in ostalimi relevantnimi doloèili direktive 1999/5/ES.
Slovensky [Slovak]	NETGEAR, Inc. týmto vyhlasuje, že NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 spåòa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.

Suomi [Finnish]	NETGEAR, Inc. vakuuttaa täten että NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar NETGEAR, Inc. att denna NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Product and Publication Details

Model Number:	WG111v3
Publication Date:	April 2007
Product Family:	Wireless Adapter
Product Name:	NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3
Home or Business Product:	Home
Language:	English
Publication Part Number:	202-10240-01

Contents

About This Manual

Basic Setup

Network Connections and Wireless Security

About This Manual

Audience, Conventions, and Scope

This manual assumes that you have basic to intermediate computer and Internet skills. However, tutorial information is provided on the NETGEAR website.

This manual uses the following typographical conventions:

Italics	Emphasis, books, CDs, URL names
Bold	User input

This manual uses the following formats to highlight special messages:

Note: This format is used to highlight information of importance or special interest.

Tip: This format is used to highlight a procedure that will save time or resources.

This manual is written according to these specifications:

Product Version	NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3
Manual Publication Date	April 2007

Note: Product updates in English language are available on the NETGEAR website at *http://kbserver.netgear.com.*

Basic Setup

The NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 lets you connect a PC computer to wireless networks. It is designed for PC computers running Microsoft Windows. For information about product features and compatible NETGEAR products, please see the NETGEAR website at *http://www.netgear.com*.

This chapter describes how to install your wireless USB adapter and set up basic wireless connectivity on your Wireless Local Area Network (WLAN). Advanced wireless network set up is covered in "Network Connections and Wireless Security" on page 11.

What You Need Before You Begin

You must verify that your computer meets the minimum system requirements and identify the wireless network settings of the wireless network where you will connect before you can set up your wireless USB adapter and connect.

Verify System Requirements

Before installing the Wireless Adapter, make sure that these minimum requirements have been met. You must have a computer with:

- A Pentium 300 MHz or higher compatible processor with an available USB port.
- A CD drive.
- 10 MB of free hard disk space.
- Windows 2000, XP, or Vista.

Observe Wireless Location and Range Guidelines

Computers can connect over wireless networks indoors at a range which vary significantly based on the location of the computer with the Wireless Adapter. For best results, avoid potential sources of interference, such as:

- Large metal surfaces
- Microwave ovens
- 2.4 GHz Cordless phones

In general, wireless devices can communicate through walls. However, if the walls are constructed with concrete, or have metal, or metal mesh, the effective range will decrease if such materials are between the devices.

What Is in the Box

The product package should contain the following items:

- NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3
- Installation Guide
- Plastic cradle and fasteners to hold the WG111v3
- *NETGEAR CD*, including:
  - Driver and Configuration Utility Software
  - This User Manual
- Warranty and Support information card

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product.

Default Wireless Settings

If this is a new wireless network installation, use the factory default settings to set up the network and verify wireless connectivity. If this is an addition to an existing wireless network, you need the wireless network and wireless security settings that are already defined.

Your Wireless Adapter factory default basic settings are:

- Network Name Service Set Identification (SSID): **ANY**

> **Note:** In order for the Wireless Adapter to communicate with a wireless access point or wireless adapter, all devices must be set up to use the same wireless network name (SSID).

- Network Mode (Infrastructure or Ad-hoc): **Infrastructure**
- Data security WEP, WPA2-PSK, or WPA-PSK encryption: **Disabled**

The section below provides instructions for setting up the Wireless Adapter for basic wireless connectivity to an access point.

Installation Instructions

The instructions in this chapter are for an Access Point (Infrastructure) installation. Wireless security, advanced settings, and Computer-to-Computer (Ad Hoc) instructions are covered in "Network Connections and Wireless Security" on page 11.

Follow the instructions below to install the Wireless Adapter.

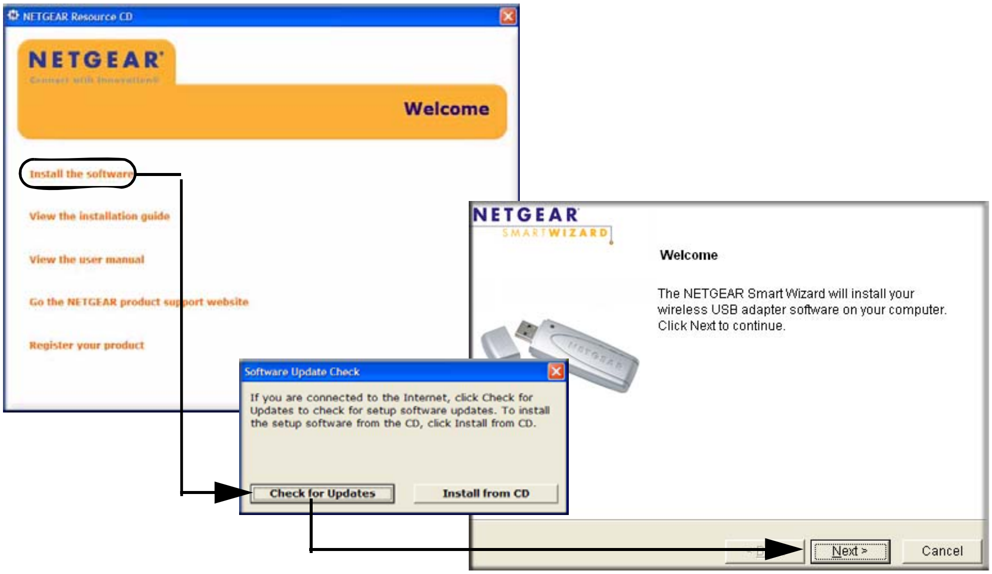
1. First, install the software. Insert the NETGEAR CD. If the CD main page does not appear, double click Autorun.exe on the CD.

a. Click Install the Software.The Check for Updates window will open.

b. If you are connected to the Internet, click Check for Updates. If not, you can choose to install from the CD.

c. When the Installation Complete message appears, click Next.

d. On the Smart Wizard screen, click Next to proceed with the Smart Wizard setup.



If you are connected to the Internet, click Check for Updates to check for setup software updates. To install the setup software from the CD, click Install from CD.

The NETGEAR Smart Wizard will install your wireless USB adapter software on your computer. Click Next to continue.

Figure 1

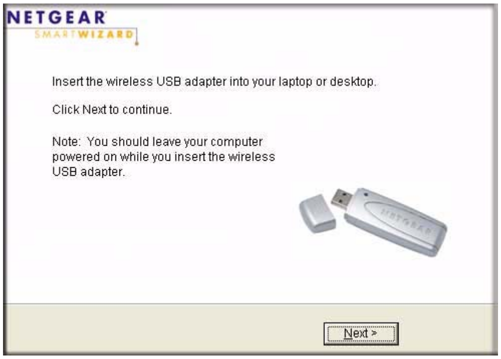
2. Now, when prompted, insert your wireless USB adapter.

a. Click **Next** to proceed. Windows will discover the adapter and continue the software installation process.

b. Follow the Windows prompts to complete the software installation.

c. If a Windows logo certification warning appears, click Continue to proceed with the installation.

d. When the Windows software installation is complete, click Finish.



Insert the wireless USB adapter into your laptop or desktop.

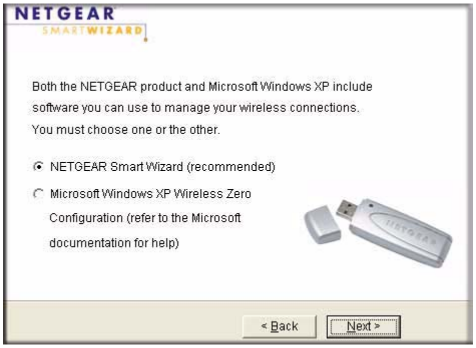
Click Next to continue.

Note: You should leave your computer powered on while you insert the wireless USB adapter.

Figure 2

3. Windows 2000 users go to Step 4. Windows XP or Vista users can set up the wireless adapter either with the NETGEAR Smart Wizard (recommended) or the Windows Configuration Utilities.

   - **NETGEAR Smart Wizard:** Reveals more information about each network and makes it easier to troubleshoot network connection problems. See "The Smart Wizard Status Bar" on page 7 and "Statistics Page" on page 26.
   - **Windows Zero Configuration Utility:** See the Windows documentation or see the link to "Windows XP and Vista Wireless Configuration Utilities" on page 33.



Both the NETGEAR product and Microsoft Windows XP include software you can use to manage your wireless connections. You must choose one or the other.

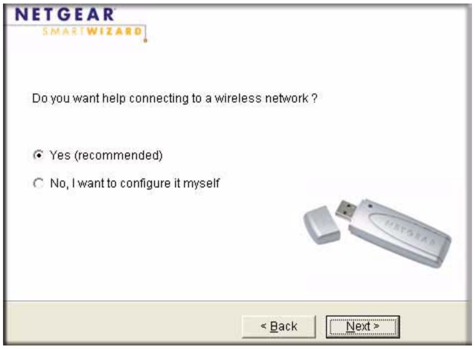
● NETGEAR Smart Wizard (recommended)

○ Microsoft Windows XP Wireless Zero Configuration (refer to the Microsoft documentation for help)

Figure 3

4. Use the Smart Wizard to set up your Wireless Adapter

   a. When prompted, click Next to let the wizard help you connect to a network (recommended).



Do you want help connecting to a wireless network ?

● Yes (recommended)

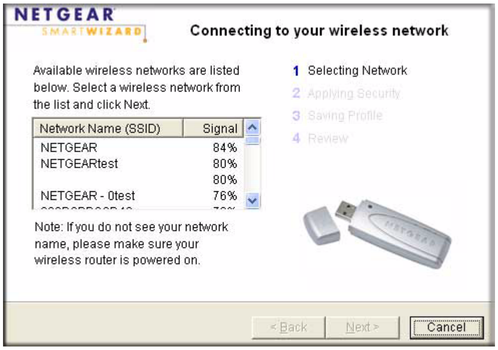
○ No, I want to configure it myself

Figure 4

   b. Select the wireless network from the drop-down list, and the wizard records your choice.

➡	**Note:** Hidden networks do not broadcast the Network Name (SSID). These networks are in the drop-down list, but the Network Name (SSID) is blank

If the network uses security, then the Smart Wizard detects it..



Connecting to your wireless network

Available wireless networks are listed below. Select a wireless network from the list and click Next.

Network Name (SSID)	Signal
NETGEAR	84%
NETGEARtest	80%
	80%
NETGEAR - 0test	76%

Note: If you do not see your network name, please make sure your wireless router is powered on.

1 Selecting Network
2 Applying Security
3 Saving Profile
4 Review

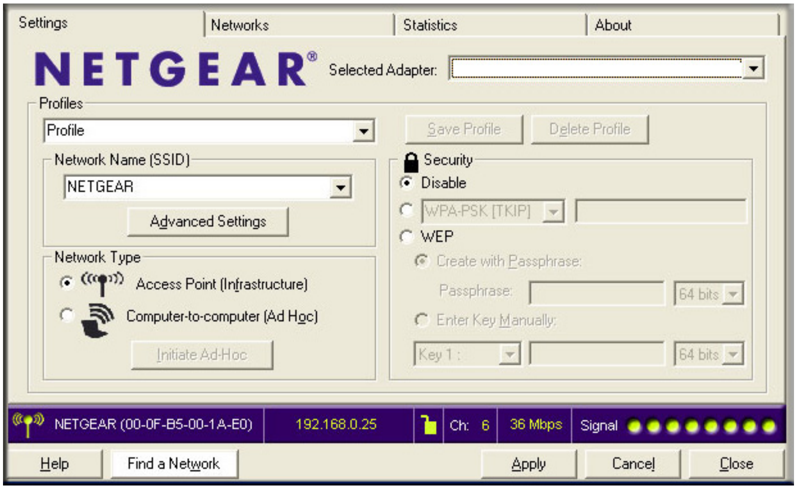
Figure 5

   c. Follow the Wizard steps for Security (if used) and for saving a Profile.

   d. After you have reviewed the settings, click Finish.

The icon appears in the System Tray and on the desktop. The wizard initiates your wireless connection. It could take up to a minute for your wireless connection to be established.

The Smart Wizard Settings page opens.



Selected Adapter:

Profiles
Profile

Network Name (SSID)
NETGEAR

Network Type
● Access Point (Infrastructure)
○ Computer-to-computer (Ad Hoc)

Security
● Disable
○ WPA-PSK [TKIP]
○ WEP
● Create with Passphrase:
Passphrase: 64 bits
○ Enter Key Manually:
Key 1 : 64 bits

NETGEAR (00-0F-B5-00-1A-E0) | 192.168.0.25 | Ch: 6 | 36 Mbps | Signal ●●●●●●●●

Figure 6

5. Use the status bar to verify your wireless connectivity. For more information about connecting, see "Connecting to Wireless Networks and the Internet" on page 6.

Note: For information about using Wi-Fi Multimedia (WMM), see "Advanced Settings" on page 25.

Connecting to Wireless Networks and the Internet

The Wireless Adapter has indicators that show the status of your connection to a wireless network and to the Internet:

- **Icon:** After you install the software, this icon appears on the desktop and in the lower right of the Windows task bar. It is color coded to show the status of the connection. See "The Smart Wizard Status Bar" on page 7.
- **Smart Wizard Status Bar:** Clicking on the system tray icon opens the Smart Wizard. The status bar at the bottom of the page shows details about your wireless and Internet connection.

The Smart Wizard Status Bar

Click the icon to open the Smart Wizard so you can view the status bar. The Smart Wizard Settings page opens. The status bar is at the bottom of the page.

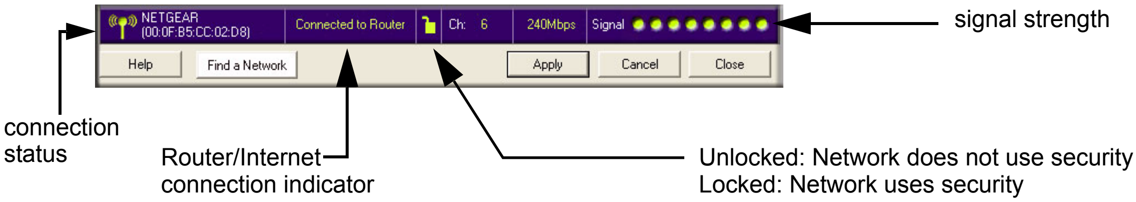


Figure 7

- **Connection Status:** The color shows the connection status.
- **Signal Strength:** Shows the signal strength of the wireless network. If the signal is poor, then try moving closer to the wireless access point.
- **Lock icon:** Shows if security is used on the network.
- **Router/Internet connection indicator:** This shows the progress of your connection. By default, this feature is on.

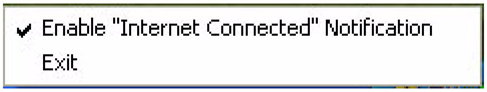
Figure 8

If you selected Europe during the WG111v3 installation, this feature is disabled.

The Router/Internet connection indicator is useful in isolating a problem. For example, if you are connected to a router, but not to the Internet, then check the router’s Internet connection.

Connection Indicator	Description
Connected to Internet or IP Address	Wireless Internet connection OK.
Connected to Router	Wireless connection to router OK but no Internet connection at router.
___.___.___.___ or 169.254..x.x	Wireless connection to a router OK but there is a problem with the router. See “Troubleshooting”.

If you right-click the System Tray icon, you can disable the Internet notification feature by clearing the check mark on this line. If you do so, then only the IP address is shown.



✔ Enable "Internet Connected" Notification

Exit

Figure 9

If you selected Europe during the WG111v3 installation, you will not see the "Enable Internet Connected Notification" option.

Icon Colors

The icon is on the desktop and in the Windows System Tray. The System Tray resides on one end of the taskbar in the Microsoft Windows desktop.

Color	Condition	Description
Red 🟥	The wireless USB adapter has no connection to any other wireless node.	The Wireless Adapter can not link to any other wireless node or the link is lost. Check your configuration or try moving to a location where the wireless signal quality is better.
Yellow 🟨	The wireless USB adapter has a connection with another wireless node.	The wireless link is weak. You may need to move to a better spot, such as closer to the wireless access point. Also, look for possible interference such as a 2.4 GHz cordless phone or large metal surface.
Green 🟩	The wireless USB adapter has a connection with another wireless node.	The wireless USB adapter has established good communication with an access point and the signal quality is strong.

Placing the USB Adapter Cradle

You can attach the Wireless Adapter directly to a USB port on your computer, or use the USB cable to extend the range and obtain better wireless reception.

Follow these instructions to use the USB cable, plastic cradle, and loop and hook fastener provided in the package for better USB Adapter placement on a notebook computer:

1. The Wireless Adapter comes with three black fasteners. Locate the one that has a prickly side and attach it to the plastic cradle on the middle of the outside rear.
2. Insert the Wireless Adapter in the plastic cradle.

3. Place one of the other pieces of loop and hook fastener on the back of the monitor near the top for better reception.

	Tip: Place the last piece of fastener on the side of monitor nearest your wireless access point.

4. Join the pieces of the fastener to attach the USB Adapter in the plastic cradle to the notebook or desktop monitor.

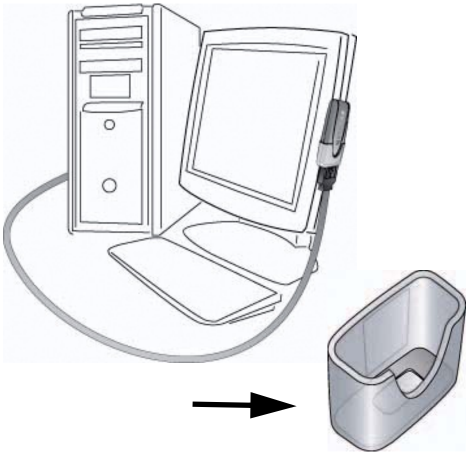


Figure 10

See the installation instructions for your operating system before attaching the USB cable to the USB Adapter and your computer

Removing the Software

You can remove the Wireless Adapter software in these two ways:

- Navigate the Windows Start menu to the NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 program group, select the uninstall option, and follow the screen prompts.
- Navigate the Windows Start menu to the Control Panel Add or Remove Program item, select the NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3 option, and follow the screen prompts.

Upgrading the Wireless Adapter Software

Upgrades may be available at the NETGEAR website. To install an upgrade, follow these steps.

1. Go to *http://kbserver.netgear.com*
2. Click the latest version of upgrade.
3. Examine the Release Note. Make sure to read any warnings and Known Problems.
4. Download the upgrade using the link in the Release Note.
5. Follow the Release Note installation instructions.

Network Connections and Wireless Security

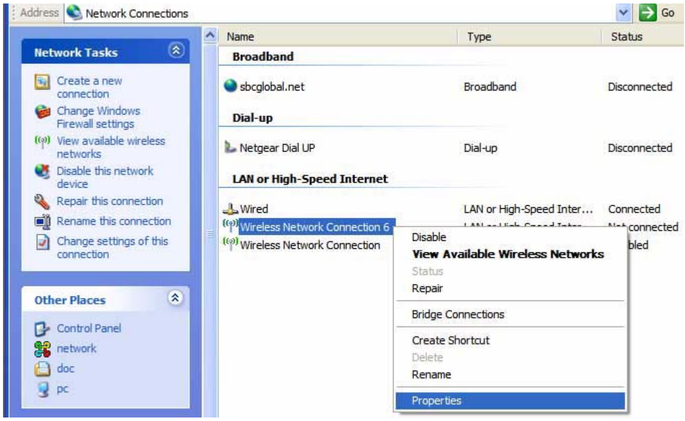
This chapter explains how to use your Wireless USB 2.0 Adapter to connect to your Wireless Local Area Network (WLAN) and how to set up wireless security for the Wireless USB 2.0 Adapter so that it matches the wireless security settings for your network.

If you chose the Windows XP or Windows Vista Configuration utility during installation, and now you want to use the Smart Wizard, then you need to disable the Windows utility. If you are working with the Vista configuration utility, see the online document: *http://documentation.netgear.com/reference/enu/winzerocfg/index.htm*

Disabling the Windows Zero Configuration Utility

To disable the Windows Zero Configuration utility:

1. Attach the wireless adapter to a USB port for your computer.
2. Go to Windows Start menu and select Network Connections.
3. On the Network connections page, select the Wireless Network Connection and right-click to choose the Properties option.



Name	Type	Status
Broadband		
sbcglobal.net	Broadband	Disconnected
Dial-up		
Netgear Dial UP	Dial-up	Disconnected
LAN or High-Speed Internet		
Wired	LAN or High-Speed Inter...	Connected
Wireless Network Connection 6		connected
Wireless Network Connection		bled

Figure 11

4. Click the Wireless Networks tab. Then clear the “Use Windows to configure my wireless settings” check box.

Understanding the Smart Wizard

These instructions explain how to use the NETGEAR WG111v3 Smart Wizard to change the WG111v3 wireless settings.

When you have installed the software from the *NETGEAR CD*, the icon appears on your desktop and in the Windows System Tray. The Windows System Tray is located on the Windows taskbar. You can either double-click this icon on the desktop, or click it in the System Tray at any time, to use the Smart Wizard. This software automatically restarts when you reboot your computer.

The Smart Wizard provides a complete and easy to use set of tools to:

- View details about wireless networks in your area.
- Choose the network that you want to use.
- Configure wireless settings for your wireless USB adapter
- Save your wireless network settings in profiles.
- Remove or reinstall the wireless adapter software.

The following sections in this chapter explain how to use the Smart Wizard.

Viewing Wireless Networks in Your Area

You can use the Networks tab to view all available wireless networks in your area. You can also scan to search for wireless networks and refresh the page.

To view information about wireless networks:

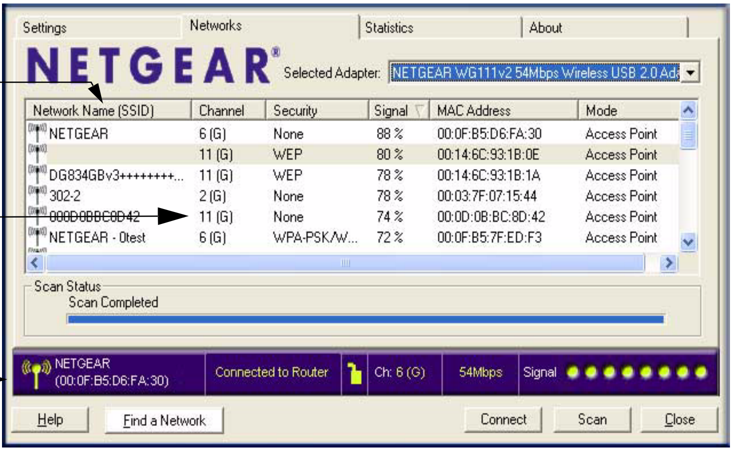
1. Use the icon to open the Smart Wizard. The Settings tab page opens.

2. Click the Networks tab to view the following page.

You can click a column heading to sort.

If many networks use the same channel they can interfere with each other.

The Status bar shows your network connection and Internet connection.



Selected Adapter: NETGEAR WG111v2 54Mbps Wireless USB 2.0 Ada

Network Name (SSID)	Channel	Security	Signal	MAC Address	Mode
NETGEAR	6 (G)	None	88 %	00:0F:B5:D6:FA:30	Access Point
	11 (G)	WEP	80 %	00:14:6C:93:1B:0E	Access Point
DG834GBv3++++++++...	11 (G)	WEP	78 %	00:14:6C:93:1B:1A	Access Point
302-2	2 (G)	None	78 %	00:03:7F:07:15:44	Access Point
000D0BBC8D42	11 (G)	None	74 %	00:0D:0B:BC:8D:42	Access Point
NETGEAR - 0test	6 (G)	WPA-PSK/W...	72 %	00:0F:B5:7F:ED:F3	Access Point

Scan Status
Scan Completed

NETGEAR (00:0F:B5:D6:FA:30) | Connected to Router | Ch: 6 (G) | 54Mbps | Signal ●●●●●●●●

Figure 12

The screen shows the following information for each network scanned:

- **Network Name (SSID):** The name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter. Note that as a security measure, some wireless access points do not broadcast their SSID. In such cases, the SSID field will be blank even though the rest of the information will still be displayed.
- **Channel:** The channel determines which operating frequency will be used.
- **Security:** Identifies whether the wireless network uses WEP or WPA-PSK security settings.
- **Signal:** Identifies the signal strength of the communications.
- **MAC Address:** Identifies the hardware address (MAC Address) of the wireless device broadcasting this information.
- **Mode:** Identifies the type of wireless network — Access Point (Infrastructure) or Computer-to-Computer (Ad Hoc)

The buttons located at the bottom of the Networks tab are:

- **Help:** Display online help.
- **Find a Network:** Find and connect to a network. See "Finding a Network" on page 14.
- **Connect:** Connect to the network that you selected.
- **Scan:** Check for wireless networks. Clicking Scan refreshes the page.
- **Close:** Close the window of the Wizard.

Finding a Network

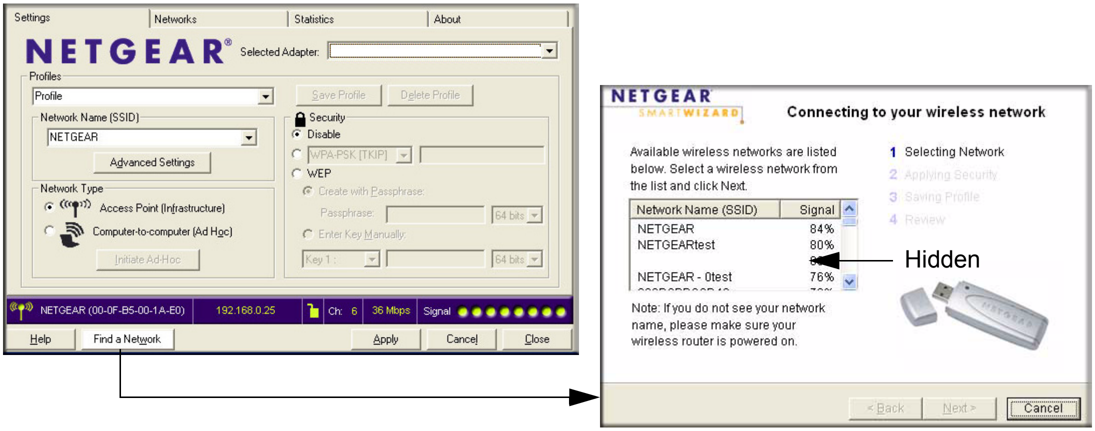
During the Wireless Adapter software installation, the Smart Wizard lists the available networks. After installation you can use the Find a Network button on the Network tab at any time to view the available networks and select the one that you want to use.

➡	**Note:** Make sure that you know the security settings for the network that you want to use. For example, if WEP is used then you need to know the WEP key. If you use secure networks frequently, set up profiles for each network with the wireless network and security settings.

To find a Network, follow these steps:

1. Use the icon to open the Smart Wizard.

   The Settings tab page opens.
2. Click Find a Network.
3. Select a network from the
   drop-down list. If you select a hidden network then you must enter the SSID. Click Next.
4. Follow the steps of the wizard to specify the wireless security if used, and to create a profile.
5. Review you settings, and click Finish.:



Selected Adapter:

Profiles: Profile

Network Name (SSID): NETGEAR

Security: ● Disable ○ WPA-PSK [TKIP] ○ WEP

● Create with Passphrase: Passphrase: 64 bits

○ Enter Key Manually: Key 1 : 64 bits

Network Type: ● Access Point (Infrastructure) ○ Computer-to-computer (Ad Hoc)

NETGEAR (00-0F-B5-00-1A-E0) | 192.168.0.25 | Ch: 6 | 36 Mbps | Signal ●●●●●●●●

Connecting to your wireless network

Available wireless networks are listed below. Select a wireless network from the list and click Next.

Network Name (SSID)	Signal
NETGEAR	84%
NETGEARtest	80%
	80%
NETGEAR - 0test	76%

Note: If you do not see your network name, please make sure your wireless router is powered on.

1 Selecting Network
2 Applying Security
3 Saving Profile
4 Review

Figure 13

The Smart Wizard initiates your wireless connection. You can use the Status Bar to verify your network connection. For more information, see "The Smart Wizard Status Bar" on page 7.

Profiles

The WG111v3 Smart Wizard uses profiles to store all the settings for a particular wireless network. There are two special profile names: Default and Profile.

- **Default:** The Profile named Default automatically scans for any available network. You cannot change this profile name.
- **Profile:** If you do not enter a name in the Profile Name box, then the name Profile is used to save your settings. If you do this more than once then you will be asked if you want to replace the previous settings stored in Profile.

Adding Profiles

You can store multiple profiles and recall the one which matches the network you want to join.

If you use your computer to connect to different wireless networks, you can create a profile for each wireless network. Then, you can easily load the profile that has all the settings that you need to join the network you are using at the time.

There are two types of wireless network profiles that you can set up:

- **Access Point (Infrastructure) –** Connect to an access point or router with the 802.11 infrastructure mode. For example, this mode is used when computers in a house connect to an access point that is attached to a router, which lets multiple computers share a single cable or DSL broadband Internet connection.
- **Computer-to-Computer (Ad Hoc) –** Connect directly to another computer with the 802.11 ad hoc mode. For example, Ad Hoc mode is used when two Windows computers are configured with file and print sharing enabled and you want to exchange files directly between them.

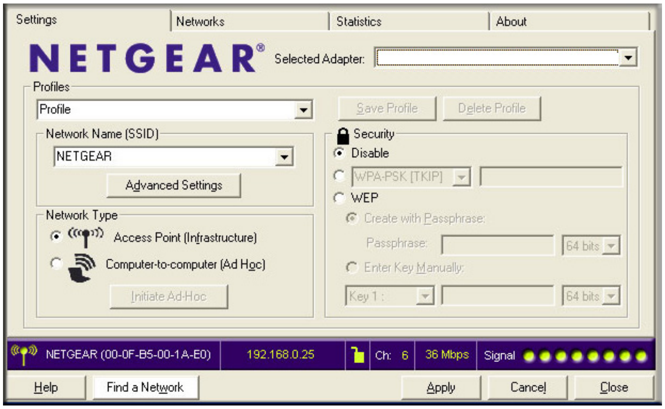
For more information on 802.11 wireless network modes, see the wireless reference document at: *http://documentation.netgear.com/reference/enu/wireless/index.htm*.

Setting up a Profile to Connect to an Access Point or Router

To set up the Wireless Adapter to connect to a wireless access point or router:

1. Use the icon to open the Smart Wizard. The Settings page opens.

2. Enter the network settings.
   a. In the Network Type section, be sure that Access Point (Infrastructure) is selected.
   b. In the Profile box, type the name of the profile.
   c. In the Network Name (SSID) field select a network or enter the SSID.



Selected Adapter:

Profiles
Profile

Network Name (SSID)
NETGEAR

Network Type
● Access Point (Infrastructure)
○ Computer-to-computer (Ad Hoc)

Security
● Disable
○ WPA-PSK [TKIP]
○ WEP
● Create with Passphrase:
Passphrase: 64 bits
○ Enter Key Manually:
Key 1 : 64 bits

NETGEAR (00-0F-B5-00-1A-E0) | 192.168.0.25 | Ch: 6 | 36 Mbps | Signal ●●●●●●●●

Figure 14

Note: You will not get a wireless network connection unless the network SSID matches exactly the SSID used by the access point.

3. Save your settings in a Profile.
   a. Click Save Profile.

      All the configuration settings are saved in this profile.
   b. Click **Apply**.
   c. Click Close to exit the wizard, or Cancel to return to the previous settings.
4. Check to make sure that you can connect to your network and to the Internet. For example, use your browser to connect to the Internet, or check for file and printer access on your network.

   If you cannot connect, check the Status bar in the Smart Wizard. See "The Smart Wizard Status Bar" on page 7. For problems with accessing network resources, the Windows Client and File and Print Sharing software might not be installed and configured properly on your computers. See the link to "Internet Networking and TCP/IP Addressing" on page 33.

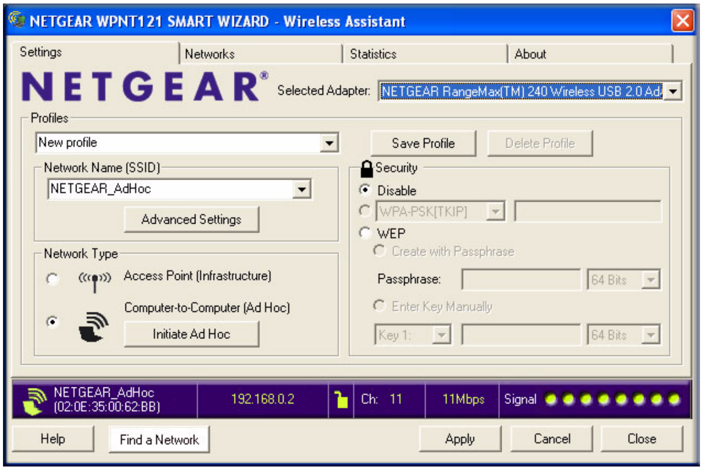
Setting up a Computer-to-Computer (Ad Hoc) Profile

The Computer-to-Computer setting uses Ad Hoc mode. Ad Hoc mode is an 802.11 networking framework in which devices or computers communicate directly with each other, without the use of an access point. For example, this mode is used when two Windows computers are configured with file and print sharing enabled and you want to exchange files directly between them.

Note: Ad Hoc mode will not work using DHCP settings. Ad Hoc mode requires either static IP addresses (such as **`192.168.0.1`**) or the IPX protocol. For instructions on setting up static IP addresses on a Windows PC, refer to the PC Networking Tutorial included on the *NETGEAR CD*.

To create an Ad Hoc mode profile:

1. Use the icon to open the Smart Wizard. The Settings page opens.
2. Enter the network settings.
   a. Select Computer-to-Computer (Ad Hoc) for the Network Type.
   b. Select or enter the Network Name (SSID) for the Ad Hoc network.
   c. In the Profile box, type the name of the profile.
   d. Click **Apply**


NETGEAR WPNT121 SMART WIZARD - Wireless Assistant

Selected Adapter: NETGEAR RangeMax(TM) 240 Wireless USB 2.0 Ad

Profiles: New profile

Network Name (SSID): NETGEAR_AdHoc

Network Type:
○ Access Point (Infrastructure)
● Computer-to-Computer (Ad Hoc)

Security:
● Disable
○ WPA-PSK[TKIP]
○ WEP
○ Create with Passphrase
Passphrase: 64 Bits
○ Enter Key Manually
Key 1: 64 Bits

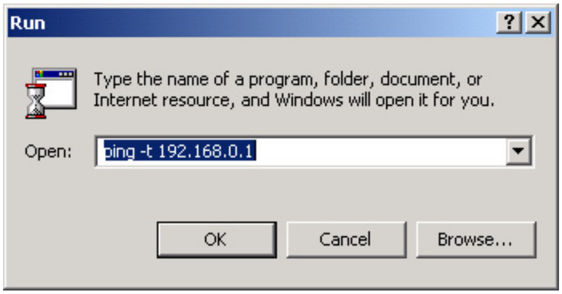
NETGEAR_AdHoc (02:0E:35:00:62:BB) 192.168.0.2 Ch: 11 11Mbps Signal

Figure 15

3. Save your settings in a Profile.
   a. Click Save Profile.

      All the configuration settings are saved in this profile.
   b. Click **Apply**.
   c. Click Close to exit the Smart Wizard, or Cancel to return to the previous settings.
4. Configure the PC network settings.
   a. Configure each PC with either a static IP address or with the IPX protocol.
   b. Restart the PCs.
5. Verify wireless connectivity between your peer devices.

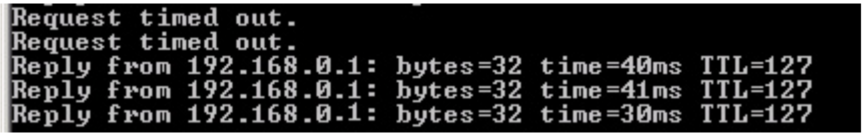
   You can use the ping utility to verify your wireless connection
   a. On the Windows taskbar click Start, and then click Run.
   b. Assuming the target PC is configured with 192.168.0.1 as its IP address, type **`ping -t 192.168.0.1`** and then click OK.


Run
?
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

```
ping -t 192.168.0.1
```

Figure 16

   c. This sends a continuous ping to the device with the 192.168.0.1 static IP address. The ping response should change to “reply.”



```
Request timed out.
Request timed out.
Reply from 192.168.0.1: bytes=32 time=40ms TTL=127
Reply from 192.168.0.1: bytes=32 time=41ms TTL=127
Reply from 192.168.0.1: bytes=32 time=30ms TTL=127
```

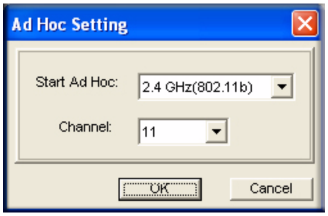
Figure 17

At this point the connection is established. For more information about using ping, see *http://kbserver.netgear.com/kb_web_files/N101453.asp*.

Note: If you cannot connect, see "Placing the USB Adapter Cradle" on page 8. Also, for problems with accessing network resources, the Windows Client and File and Print Sharing software might not be installed and configured properly on your computers. Please see the link to "Internet Networking and TCP/IP Addressing" on page 33.

Starting a Computer-to-Computer (Ad Hoc) Network Connection

1. On the Settings tab page of the Smart Wizard, select or type the Network Name (SSID).
2. Select the Computer-to-Computer (Ad Hoc) network type.
3. Click Initiate Ad Hoc. The Ad Hoc Setting dialog box opens:



Ad Hoc Setting

Start Ad Hoc: 2.4 GHz(802.11b)

Channel: 11

Figure 18

4. In the Start Ad Hoc field, choose the wireless standard (802.11b, or 802.11g) for your Ad Hoc computer-to-computer network.
5. In the Channel field, Automatic should work.

Note: If there is interference from another nearby wireless device, use the Networks tab page to see which channels are in use in your area. Then use a different channel. For example, if your neighbors use channel 6 and the signal strength is strong, then channels 4-8 would probably be poor choices for you.

6. Click OK. The Wireless Adapter automatically selects the highest connection speed.

Wireless Security

Many networks use wireless security to encrypt wireless data communications. If you try to connect to a network with wireless security the Smart Wizard detects it. Before you can use that network you must set up the Wireless Adapter with the same SSID, wireless security, and security settings as that network. If you do not know what these are, contact the person who set up the network.

The Wireless Adapter supports the following types of wireless security:

- Wi-Fi Protected Access 2 Pre-Shared Key (WPA2-PSK)
- Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)
- Wired Equivalent Privacy (WEP)

For more information about wireless security, see the Web link to "Wireless Communications" on page 33 or the wireless reference document at:
http://documentation.netgear.com/reference/enu/wireless/index.htm

In addition to the wireless security features, networks should use LAN network security features such as requiring a user name and password to access the shared resources in the network.

The procedures below explain how to configure the wireless encryption settings of your Wireless Adapter.

Know Your Wireless Network Settings

You will need to know the settings for your wireless network. The form on the next page is set up so that you can record this information. You can use either of these two methods to keep track of these settings:

- Print the form on the next page and fill it out. If you are uncomfortable writing out secure information, put a "hint" to yourself instead of the actual information. Put the form where it will be very easy for you to remember, or save two copies and put them in different places.
- Save the information in a document on your computer. Later you can search for words such as SSID to locate the information.

Wireless Network Name (SSID) and Security Settings

Print this form, fill in the configuration parameters and put it in a safe place for possible future reference. For an existing wireless network, the person who set up the network will have this information.

- **Network Name (SSID):** The Service Set Identification (SSID) identifies the wireless local area network. **Any (First available network)** is the default WG111v3 wireless network name (SSID). You may customize it using up to 32 alphanumeric characters. Write your customized wireless network name (SSID) on the line below.

> **Note:** The SSID in the wireless access point is the SSID you configure in the wireless USB adapter. For the access point and wireless nodes to communicate with each other, all must be configured with the same SSID.

Wireless network name (SSID): ________________________________

- **If WEP Authentication is Used.**
  - **WEP Encryption key size**. Identify one: **64-bit** or **128-bit**. The encryption key size must the wireless network settings.
  - **Data Encryption (WEP) Keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces below.
    - **Passphrase method**. ________________________________ These characters *are* case sensitive. Enter a word or group of printable characters and click the Generate Keys button. Not all wireless devices support the passphrase method.
    - **Manual method**. These values *are not* case sensitive. For 64-bit WEP, enter 10 hex digits (any combination of 0-9 or a-f). For 128-bit WEP, enter 26 hex digits.

Key 1: ________________________________ Key 2: ________________________________

Key 3: ________________________________ Key 4: ________________________________

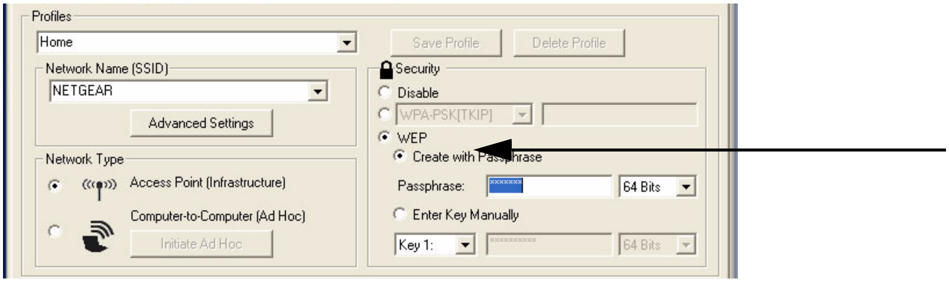
- **If WPA2-PSK or WPA-PSK Authentication is Used.**
  - **Passphrase**: ________________________________ These characters *are* case sensitive. Enter a word or group of printable characters. When you use WPA-PSK, the other devices in the network will not connect unless they are set to WPA-PSK as well and are configured with the correct Passphrase.

Use the procedures below to set up basic security settings in the WG111v3.

Setting up WEP Encryption Security

Follow the steps below to configure WEP Encryption Security.

1. Run the Wireless Adapter Smart Wizard.
   - a. Make sure the software is installed and the Wireless Adapter is into the USB port in your computer.
   - b. Use the icon to open the Smart Wizard. The Settings tab page opens.



Profiles: Home

Network Name (SSID): NETGEAR

Network Type

● Access Point (Infrastructure)

○ Computer-to-Computer (Ad Hoc)

Security

○ Disable

○ WPA-PSK[TKIP]

● WEP

● Create with Passphrase

Passphrase: ******* 64 Bits

○ Enter Key Manually

Key 1: ********** 64 Bits

Figure 19

2. Configure the Security settings.
   - a. In the Profile box, select the profile or type in a profile name.
   - b. In the Network Name (SSID) field select the network, or enter the SSID.

> **Note:** You will not get a wireless network connection unless the network SSID matches exactly what is configured in the access point.

   - c. In the Security section, select WEP.

3. Select the WEP encryption strength you will use.

   The choices are:

   - 64-bit WEP data encryption
   - 128-bit WEP data encryption

> **Note:** The 128-bit encryption keys require more processing, and slow performance slightly.

4. Select Create with Passphrase and enter the passphrase. The configuration utility will automatically generate the WEP keys.

> **Note:** The characters are case sensitive. Be sure to use the same passphrase for all the wireless devices in the network.

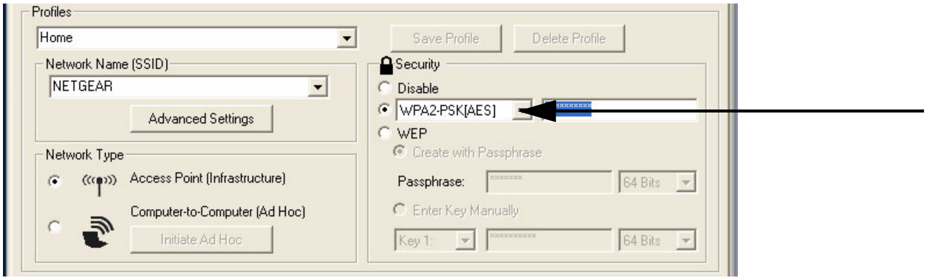
If the passphrase method is not available in the other devices, you must manually enter the keys to match exactly what is in the access point and other 802.11b wireless devices.

5. Save your settings in a Profile.
   - **a.** Click Save Profile. All the configuration settings are saved in this profile.
   - **b.** Click **Apply**.
   - **c.** Click Close to exit the configuration utility.

Setting up WPA2-PSK Security

Follow the steps below to configure WPA2-PSK Security.

1. Run the Wireless Adapter Smart Wizard.
   - **a.** Make sure the software is installed and the Wireless Adapter is fully inserted in a USB port in your computer.
   - **b.** Use the icon to open the Smart Wizard. The Settings tab page opens.



Profiles: Home

Network Name (SSID): NETGEAR

Network Type:
● Access Point (Infrastructure)
○ Computer-to-Computer (Ad Hoc)

Security:
○ Disable
● WPA2-PSK[AES] ********
○ WEP
● Create with Passphrase
Passphrase: ******** 64 Bits
○ Enter Key Manually
Key 1: ********** 64 Bits

Figure 20

2. Configure the Security settings.
   - **a.** In the Profile box, select the profile or type in a profile name.

b. In the Network Name (SSID) field select the network, or enter the SSID.

> **Note:** You will not get a wireless network connection unless the network SSID matches exactly what is configured in the access point.

c. In the Security section, select WPA2-PSK [AES].

For more information about WPA2-PSK security, see the Web link to "Wireless Communications" on page 33.

3. Save your settings in a Profile.

a. Click the Save Profile button. All the configuration settings are saved in this profile.

b. Click **Apply**.

c. Click Close to exit the Smart Wizard.

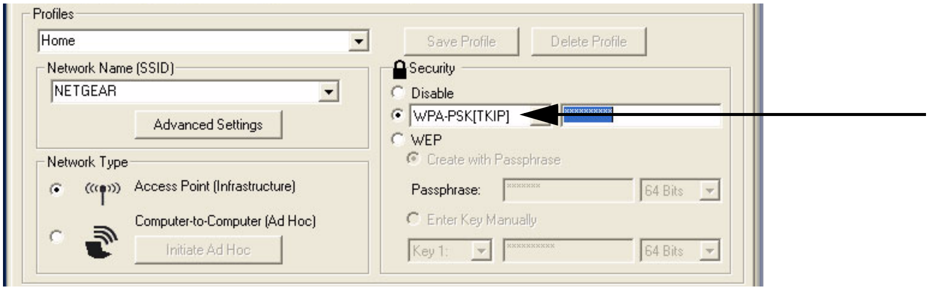
Setting up WPA-PSK Security

Follow the steps below to configure WPA-PSK Security.

1. Run the Wireless Adapter Smart Wizard.

a. Make sure the software is installed and the Wireless Adapter is fully inserted in a USB port in your computer.

b. Use the icon to open the Smart Wizard. The Settings tab page opens.



Profiles
Home
Network Name (SSID)
NETGEAR
Security
○ Disable
● WPA-PSK[TKIP]
○ WEP
● Create with Passphrase
Passphrase: 64 Bits
○ Enter Key Manually
Key 1: 64 Bits
Network Type
● Access Point (Infrastructure)
○ Computer-to-Computer (Ad Hoc)

Figure 21

2. Configure the Security settings.

a. In the Profile box, select the profile or type in a profile name.

b. In the Network Name (SSID) field select the network, or enter the SSID.

> **Note:** You will not get a wireless network connection unless the network SSID matches exactly what is configured in the access point.

c. In the Security section, select WPA-PSK [TKIP].

For more information on WPA security, see the Web link to "Wireless Communications" on page 33.

3. Save your settings in a Profile.

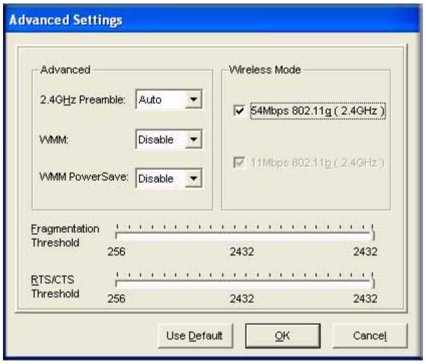
a. Click Save Profile. All the configuration settings are saved in this profile.

b. Click **Apply**.

c. Click Close to exit the Smart Wizard.

Advanced Settings

On the Settings tab click Advanced Settings to view the Advanced Settings page. Most people do not need to change these settings. You may need to adjust settings if you cannot connect without making changes, or if your Internet Service Provider (ISP) or network administrator recommend changes. You can click the Help button for more information about advanced settings.



Advanced Settings

Advanced

2.4GHz Preamble: Auto

WMM: Disable

WMM PowerSave: Disable

Wireless Mode

☑ 54Mbps 802.11g (2.4GHz)

☑ 11Mbps 802.11b (2.4GHz)

Fragmentation Threshold: 256 — 2432 — 2432

RTS/CTS Threshold: 256 — 2432 — 2432

Figure 22

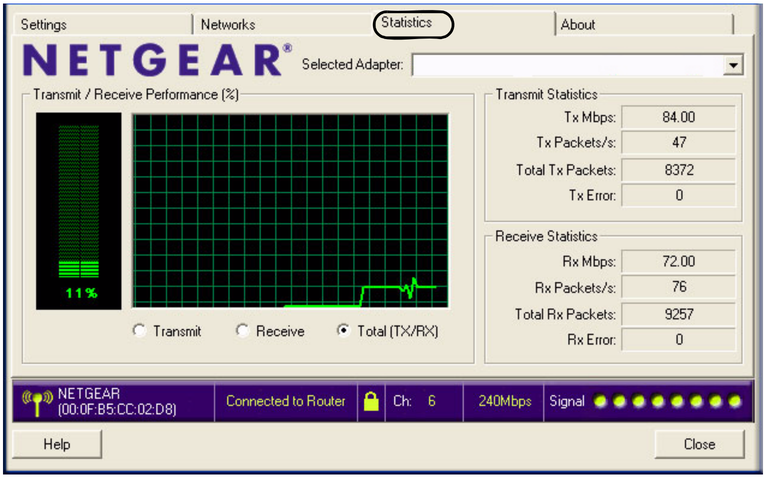
Wi-Fi Multimedia (WMM) is a Quality of Service (QoS) feature that prioritizes wireless data packets based on four access categories: voice, video, best effort, and background. Applications without WMM and applications that do not require QoS, are assigned to the best-effort category, which receives a lower priority than voice and video.

To receive the benefits of WMM QoS:

- The application must support WMM.
- You must enable WMM in your Wireless Adapter.
- You must enable WMM in your wireless access point or router.

Statistics Page

The Statistics page provides real time and historical trend information on the data traffic and performance of your wireless adapter.



Selected Adapter:

Transmit Statistics

Tx Mbps:	84.00
Tx Packets/s:	47
Total Tx Packets:	8372
Tx Error:	0

Receive Statistics

Rx Mbps:	72.00
Rx Packets/s:	76
Total Rx Packets:	9257
Rx Error:	0

○ Transmit ○ Receive ● Total (TX/RX)

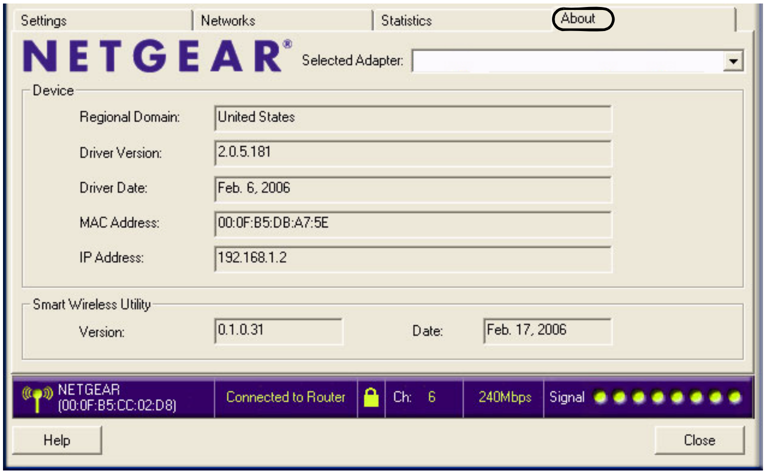
NETGEAR (00:0F:B5:CC:02:D8) | Connected to Router | Ch: 6 | 240Mbps | Signal ●●●●●●●●

Figure 23

- **Transmit/Receive Performance (%):** A real time graph identifying the total, receive, and transmit utilization as a percentage the total possible.
- **Transmit, Receive, and Total (Tx/Rx):** Radio buttons let you select whether to display the transmit performance, the receive performance, or both in the same graph.
- **Transmit Statistics:** Identifies transmit megabits per second (Mbps), transmit packets per second (Tx Packets/s), total transmitted packets, and transmit errors.
- **Receive Statistics:** Identifies receive megabits per second (Mbps), receive packets per second (Rx Packets/s), total received packets, and reception errors.

About Page

The About page displays the current software version information.



Selected Adapter:

Device

Regional Domain: United States

Driver Version: 2.0.5.181

Driver Date: Feb. 6, 2006

MAC Address: 00:0F:B5:DB:A7:5E

IP Address: 192.168.1.2

Smart Wireless Utility

Version: 0.1.0.31 Date: Feb. 17, 2006

NETGEAR (00:0F:B5:CC:02:D8) | Connected to Router | Ch: 6 | 240Mbps | Signal ●●●●●●●●

Figure 24

The following information is displayed in the About page:

- **Regional Domain:** This is the region setting for the wireless adapter. The approved channels for the region are automatically scanned. Governments regulate the channels used for wireless transmission. Operating the wireless adapter in a different region may violate local laws.
- **Driver Version:** The wireless adapter driver version.
- **Driver Date:** The wireless adapter driver date.
- **MAC Address:** The MAC address of the adapter. The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Some wireless networks will restrict access based on a list of known MAC addresses. If you are communicating with such a network, you would have to provide the address shown here to the network administrator before you would be allowed to connect. Restricting access by MAC address adds an obstacle against unwanted access to your network. However, if the only wireless security that your network uses is MAC addressing, your data is easy for hackers to read.
- **IP Address:** The IP address assigned to this adapter.
- **Smart Wireless Utility:** The version and date of the Smart Wizard.

Troubleshooting

This chapter provides information about troubleshooting your wireless USB adapter. For information about connecting to wireless networks and the Internet, see "Connecting to Wireless Networks and the Internet" on page 2-6.

Troubleshooting Tips

Use the information below to solve common problems you may encounter. Also, refer to the knowledge base on the NETGEAR website at *http://www.netgear.com/support/main.asp*.

Table 4-1. Troubleshooting Tips

Problem	Action
The LED is not lit	The WG111v3 is not connected to the USB port properly or the WG111v3 software is not loaded. • Remove and reinsert the WG111v3. • Check the Windows device manager to see if the WG111v3 is recognized and enabled. Reload the WG111v3 software, if necessary. • Try to install the WG111v3 in a different USB slot on your system if one is available.
The LED blinks but the WG111v3 is not connected to an access point.	The WG111v3 is trying to connect to an access point, but cannot connect. • The access point may not be powered on. • Or, the access point and the WG111v3 are not configured with the same wireless parameters. Check the SSID and WEP settings.
I cannot connect to an access point. The access point is available and there is good signal strength.	• If the access point is WPA-PSK protected, you need the correct WPA-PSK passphrase. Otherwise, the WG111v3 will still be connected to the previous access point and you will not be able to change to the WPA-PSK access point. • If the access point is WEP protected (either 64 or 128 bit encryption), you will be prompted to enter the WEP encryption security information.
The Smart Wizard keeps asking me to save settings.	If you change the settings the Smart Wizard offers you the chance to save the changes. To avoid this prompt, simply click **Apply** before you close the Smart Wizard.

Table 4-1. Troubleshooting Tips (continued)

Problem	Action
Two WG111v3 icons are in the system tray.	You have an older software version installed on your system and it needs to be removed. See "Removing the Software" on page 2-9or "Upgrading the Wireless Adapter Software" on page 2-10.
I can connect to the access point, but not the other computers on the network or to the Internet.	This could be a physical layer problem or a network configuration problem. 1. Check to make sure that the access point is physically connected to the Ethernet network. 2. Make sure that the IP addresses and the Windows networking parameters are all configured correctly. See the link to "Internet Networking and TCP/IP Addressing" on page B-33. 3. Restart the cable or DSL modem, router, access point, and computer.
Viewing the IP address.	To view the Wireless Adapter IP address, click the WG111v3 icon to open the Smart Wizard. Then check the IP address in the About page.
No IP address is assigned to the Wireless Adapter.	This may occur if you upgraded your Wireless Adapter software and did not reboot your system. • Either restart your computer, or connect to a different access point. • It does not usually help to shut down the Smart Wizard or disable/enable the card.

Ad Hoc Mode is Not Working Correctly

You must click the Initiate Ad Hoc button before you click **Apply**. Here is how you start an Ad Hoc network:

1. Fill in the Network Name (SSID).
2. Select the Computer-to-Computer (Ad Hoc) Network Type.
3. Click Initiate Ad Hoc.
4. Accept the default settings or make your changes, click OK, and then click **Apply**.

Note: Be sure all computers in your Ad Hoc network are configured with static IP addresses in the same subnet.

Default Configuration Settings and Technical Specifications

Default Configuration Settings

The following table lists the default settings of your Wireless Adapter.

Feature		Description
Smart Wizard		Enabled
Wireless		
	Wireless Communication	Enabled
	Wireless Network Name (SSID)	Any (first available network)
	Security	Disabled
	Network Type	Infrastructure
	Transmission Speed	Auto[a]
	Country/Region	United States (varies by region)
	Operating Mode	g and b, up to 54 Mbps
	Data Rate	up to 54 Mbps
	WMM	Disabled
	WMM Power Save	Disabled

[a] Maximum wireless signal rate (IEEE Standard 802.11n draft specification). Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical Specifications

This table below describes technical specifications for the NETGEAR 54 Mbps Wireless USB2.0 Adapter WG111v3.

Antennas	Printed internal antenna
Standards	802.11g, 802.11b
Radio Data Rate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps (Auto Rate Sensing)
Frequency	2.4GHz to 2.5GHz CCK and OFDM Modulations
LED	Single LED -- sold indicates connected to network -- blinking indicates attempting to connect to network
Power	5V bus powered
Emissions	FCC Part 15 Class B, CE
Bus interface	USB 2.0
Provided drivers	Microsoft Windows 2000, XP, and Vista (32/64 bits)
Operating Environment	Operating temperature: 0 to 40 degrees C
Encryption	40-bit (also called 64-bit) and 128-bit WEP data encryption, WPA2-PSK, and WPA-PSK
Warranty	Limited 1-year warranty

Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	**Link**
Windows XP and Vista Wireless Configuration Utilities	*http://documentation.netgear.com/reference/enu/winzerocfg/index.htm*
Internet Networking and TCP/IP Addressing	*http://documentation.netgear.com/reference/enu/tcpip/index.htm*
Wireless Communications	*http://documentation.netgear.com/reference/enu/wireless/index.htm*
Preparing a Computer for Network Access	*http://documentation.netgear.com/reference/enu/wsdhcp/index.htm*
Virtual Private Networking (VPN)	*http://documentation.netgear.com/reference/enu/vpn/index.htm*
Glossary	*http://documentation.netgear.com/reference/enu/glossary/index.htm*

EDIMAX
NETWORKING PEOPLE TOGETHER

Wireless 802.11g Access Point

EW-7206APg / EW-7206PDg

User's Manual

Version 3.0 / July, 2008

Table of Contents

Chapter 1 Introduction

This product is an access point for IEEE 802.11g/b 2.4GHz wireless network. You can use this access point to build up a wireless LAN. Any wireless LAN station can join the wireless network by using the "Infrastructure Mode".

The product supports WEP, WPA, ESSID hidden and MAC address filter functions to consolidate the wireless network security. With ESSID authentication, 64/128 bit WEP encryption, WPA encryption and MAC address filtering you can prevent unauthorized wireless stations from accessing your wireless network.

The product's dipole antenna is detachable by connecting to a RP-SMA connector. Users can install a high gain antenna to the connector for better network link quality so that you can build wireless network with more flexibility.

This product provides easy to use user interface and allows users to configure from web browser. Also it integrates DHCP server to assign IP addresses to multiple wireless and wired computers. With those versatile ~~of~~ features, this product is the best choice for you to integrate your wireless and wired network seamlessly.

1.1 Package Contents

The Access Point includes the following items:

- One Access Point / Antenna
- One Power Adapter
- One Quick Installation Guide
- User's Manual CD

1.2 Features

- Complies with the IEEE 802.11b/g (DSSS) 2.4GHz specification.
- High data rate at 54Mbps network speed.
- Seamlessly integrates wireless and wired Ethernet ~~LAN~~ networks.
- Auto rate fallback in case of obstacles or interferences.
- Provides 64/128-bit WEP and WPA Data Encryption function to protect the wireless data transmissions.
- Support 802.3af Power over Ethnernet (EW-7206PDg)
- Built-in DHCP server supports auto IP addresses assignment.
- Supports Web-based configuration.

1.3 Specifications

- Standards: IEEE 802.11b/g (Wireless), IEEE 802.3 (Wired), IEEE802.3af (EW-7206PDg)
- Data Rate: 54/48/36/24/18/12/11/9/6/5.5/2/1Mbps auto fallback
- Security: 64/128-bit WEP and WPA Data Encryption
- Frequency Band: 2.400~2.4835GHz (Industrial Scientific Medical Band)
- Modulation: CCK@11/5.5Mbps, DQPSK@2Mbps and DBPSK@1Mbps
- Radio Technology: Direct Sequence Spread Spectrum (DSSS)
- Antenna: External detachable dipole antenna (with RP-SMA connector), 2dBi for EW-7206Apg and 4dBi for
- Connectors: 10/100Mbps RJ-45 x 1
- Power: 12VDC, 0.5A
- Transmit Power: 15dBm (Typical)
- LEDs: Power, LAN Link/Activity, Wireless Activity
- Dimension: 30(H) x 127(W) x 96(D) mm
- Temperature:

  Operating: 32~131°F (0~55°C)

  Storage: -4~158°F(-20~70°C)
- Humidity: 10-90% (Non-condensing)

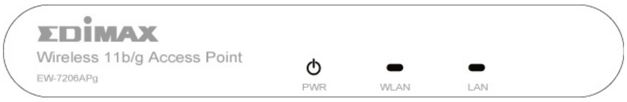
- Certification: FCC, CE

1.4 Physical Description

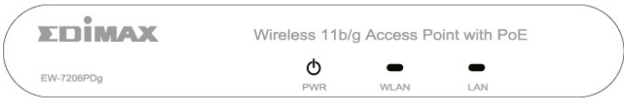
Front Panel

On the Access Point’s front panel there are LED lights to inform you of the Access Point’s current status. Below is an explanation of each LED.

EW-7206APg



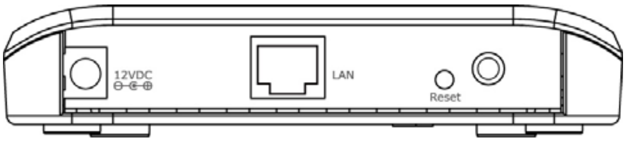
EW-7206PDg



LED	Color	Status	Description
Power	Green	Lit	Power is supplied.
		Off	No Power.
Wireless Activity	Green	Flash	Antenna is transmitting or receiving data.
		Off	Antenna is not transmitting or receiving data.
LAN Link/Activity	Green	On	A valid link is established.
		Flash	It is transmitting or receiving data.
		Off	No link is established.

Back Panel

Access Point’s connection ports are located on the back panel. Below is the description of each connection port.



- **Antenna Connector**
  This round connection is standard Reverse SMA connector where any antennas with Reverse SMA connector can connect to the Access Point.

- **DC Adapter Port**
  Insert the power jack of the power adapter into this port.

- **LAN Port**

- The Access Point’s LAN port is where you connect to your LAN’s network devices with RJ45 cables.

- **Reset**
  The reset button has two functions.

1. If you want to reboot the Access Point, use a pencil tip to press the reset button no more than 4 seconds.

2. If you press and hold the reset button for more than 4 seconds, the Access Point will reset to the factory defaults (Warning: Your settings will be deleted and replaced with the factory default settings).

Chapter 2 Wireless LAN Access Point Connection

Using Power Adapter

1. **Locate an optimum location for the Wireless LAN Access Point.**

   The best location for your Access Point is usually at the center of your wireless network, with line of sight to all of your wireless computers.

2. **Connect the Wireless LAN Access Point to your router, hub or switch.**

   Connect one end of standard UTP cable to the Access Point's LAN Port and connect the other end of the cable to a switch, a router or a hub. The Access Point will then be connected to your existed wired LAN Network.

3. **Connect the DC Power Adapter to the Wireless LAN Access Point's Power Socket.**

   Only use the power adapter supplied with the Access Point. Using a different adapter may damage the product.

Using PoE (Power over Ethernet) for EW-7206PDg only

1. **Locate an optimum location for the Wireless LAN Access Point.**

   The best location for your Access Point is usually at the center of your wireless network, with line of sight to all of your wireless computers.

2. **Connect the Wireless LAN Access Point to your PoE adapter, Router, Hub or Switch.**

   Connect one end of standard UTP cable to the Access Point's LAN Port and connect the other end of the cable to a **powered** Ethernet port on a midspan like PoE switch, PoE router, PoE hub, or PoE adapter. The Access Point will then be connected to your existed wired LAN Network.

The Hardware Installation is completed.

Chapter 3 Wireless LAN Access Point Configuration

3.1 Getting Started

This Access Point provides web-based configuration page allowing you to configure from wired or wireless stations. Follow the instructions below to do the configuration.

From Wired Station

1. Make sure your wired station is in the same subnet with the Access Point.

   The default IP Address and Sub Mask of the Access Point is:

   Default IP Address: 192.168.2.1

   Default Subnet: 255.255.255.0

   Configure your PC to be in the same subnet with the Access Point.

1a) Windows 95/98/Me

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network* icon. The *Network* window will appear.
3. Check your list of *Network Components*. If TCP/IP is not installed, click the *Add* button to install it now. If TCP/IP is installed, go to **step 6**.
4. In the *Network Component Type* dialog box, select *Protocol* and click *Add* button.
5. In the *Select Network Protocol* dialog box, select *Microsoft and TCP/IP* and then click the *OK* button to start installing the TCP/IP protocol. You may need your Windows CD to complete the installation.
6. After installing TCP/IP, go back to the *Network* dialog box. Select *TCP/IP* from the list of *Network Components* and then click the *Properties* button.
7. Check each of the tabs and verify the following settings:
   - **Bindings**: Check *Client for Microsoft Networks* and *File and printer sharing for Microsoft Networks*.
   - **Gateway**: All fields are blank.
   - **DNS Configuration**: Select *Disable DNS.*
   - **WINS Configuration**: Select *Disable WINS Resolution.*
   - **IP Address**: Select *Specify an IP Address.* Specify the IP Address and Subnet Mask as following example.
     - ✓ IP Address: 192.168.2.3 (any IP address within 192.168.2.2~192.168.2.254 is available, **do not setup 192.168.2.1**)
     - ✓ Subnet Mask: 255.255.255.0
8. Reboot the PC. Your PC will now have the IP Address you specified.

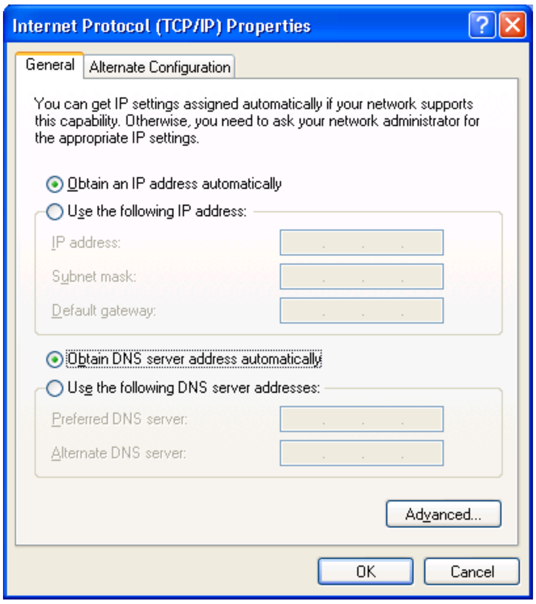
1b) Windows XP

1: Click the *Start* button and select *Settings*, then click *Network Connections.* The *Network Connections* window will appear.

2: Double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.

3: Check your list of Network Components. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.

4: In the Internet Protocol (TCP/IP) Properties window, select *Obtain an IP address automatically* and *Obtain DNS server address automatically* as shown on the following screen.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5: Click *OK* to confirm the setting. Your PC will now obtain an IP address automatically from your Broadband Router's DHCP server.

Note: Please make sure that the Broadband router's DHCP server is the only DHCP server available on your LAN.

Once you've configured your PC to obtain an IP address automatically, please proceed to Step 3.

1c) Windows 2000

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network and Dial-up Connections* icon. In the *Network and Dial-up Connection* window, double-click *Local Area Connection* icon. The *Local Area Connection* window will appear.
3. In the *Local Area Connection* window, click the *Properties* button.
4. Check your list of *Network Components*. You should see *Internet Protocol [TCP/IP]* on your list. Select it and click the *Properties* button.
5. In the *Internet Protocol (TCP/IP) Properties* window, select *Use the following IP address* and specify the IP Address and Subnet mask as following.
   - ✓ IP Address: 192.168.2.3 (any IP address within 192.168.2.2~192.168.2.254 is available, **do not setup 192.168.2.1**)
   - ✓ Subnet Mask: 255.255.255.0
6. Click *OK* to confirm the setting. Your PC will now have the IP Address you specified.

1d) Windows NT

1. Click the *Start* button and select *Settings*, then click *Control Panel*. The *Control Panel* window will appear.
2. Double-click *Network* icon. The *Network* window will appear. Select the *Protocol* tab from the *Network* window.
3. Check if the *TCP/IP Protocol* is on your list of *Network Protocols*. If *TCP/IP* is not installed, click the *Add* button to install it now. If *TCP/IP* is installed, go to **step 5**.
4. In the Select *Network Protocol* window, select the *TCP/IP Protocol* and click the *Ok* button to start installing the *TCP/IP protocol*. You may need your Windows CD to complete the installation.
5. After you install *TCP/IP*, go back to the *Network* window. Select *TCP/IP* from the list of *Network Protocols* and then click the *Properties* button.
6. Check each of the tabs and verify the following settings:
   - **IP Address:** Select *Specify an IP address.* Specify the IP Address and Subnet Mask as following example.
     - ✓ IP Address: 192.168.2.3 (any IP address within 192.168.2.2~192.168.2.254 is available, **do not setup 192.168.2.1**)
     - ✓ Subnet Mask: 255.255.255.0
   - **DNS:** Let all fields are blank.
   - **WINS:** Let all fields are blank.
   - **Routing:** Let all fields are blank.
7. Click *OK* to confirm the setting. Your PC will now have the IP Address you specified.

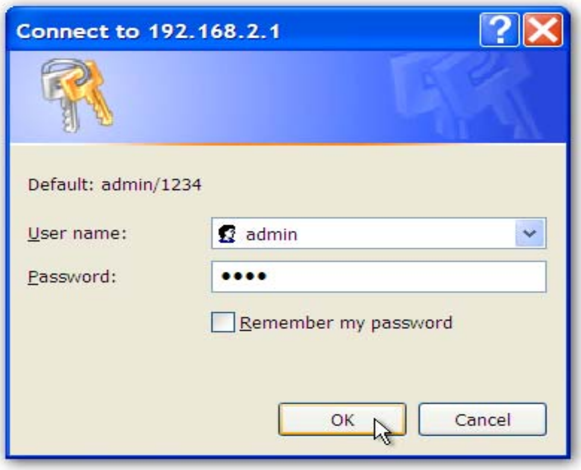
2. Enter **192.168.2.1** from Web Browser to get into the Access Point’s configuration page.

3. A screen will be popped up and request you to enter user name and password. The default user name and password is as follows.

   User Name: Admin

   Password: 1234

   Enter the default user name and password, then press **OK** button directly.



Connect to 192.168.2.1

Default: admin/1234

User name: admin

Password: ••••

□ Remember my password

4. You can start configuring the Access Point.

From Wireless Station

1. Make sure your wireless station is in the same subnet with the Access Point. Please refer to the **step 1** above for configuring the IP Address and Sub Mask of the wireless station.

2. Connect to the Access Point.

   The Access Point's default ESSID is "**default**" and the WEP Encryption function is disabled. Make sure your wireless station is using the same ESSID as the Access Point and associate your wireless station to the Access Point.

3. Enter **192.168.2.1** from Web Browser to get into the Access Point's configuration tool.

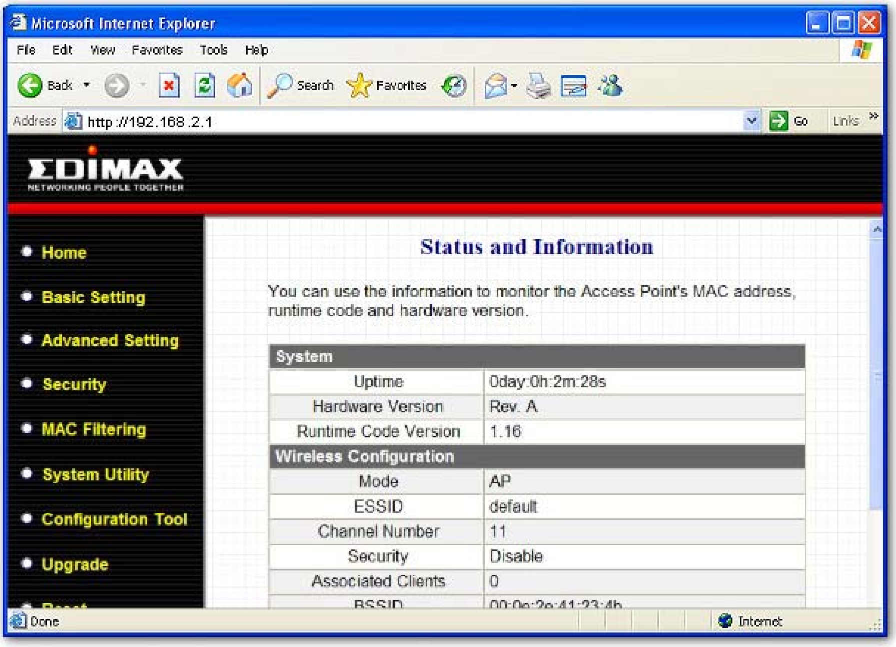
4. Enter the user name and password and then press **OK** button and you are available to configure the Access Point now.

3.2 Configuring the Access Point

Every time when you have finished modifying a setting page and click "Apply" button, this page will pop-up. The settings have been successfully saved but will not take effect immediately. You have to restart the access point to make the new settings take effect. You can click "CONTINUE" button to continue other settings. You also can click "APPLY" to restart the system and make the settings take effect.

3.2.1 Status and Information

On this screen, you can see the general information of the Access Point including ~~Alias Name,~~ Firmware Version, ESSID, Channel Number, Status, IP Address, MAC Address, etc.



Status and Information

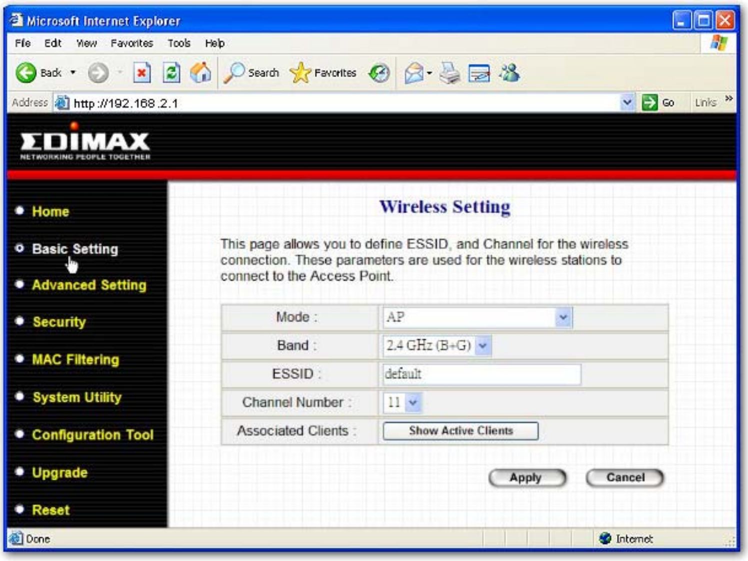
You can use the information to monitor the Access Point's MAC address, runtime code and hardware version.

System	
Uptime	0day:0h:2m:28s
Hardware Version	Rev. A
Runtime Code Version	1.16
Wireless Configuration	
Mode	AP
ESSID	default
Channel Number	11
Security	Disable
Associated Clients	0
BSSID	00:0e:2e:41:23:4b

3.2.2 Wireless Setting

This Access Point supports AP, Station, Bridge, WDS and Universal Repeater modes. "AP Mode" provides pure access point function. The simplest way to build up a wireless LAN is to use "AP Mode". "Station Mode" is used to let a network device with only wired Ethernet function to have wireless LAN communication capability. It provides both Ad Hoc and Infrastructure modes for the "Station Mode". With "Station-Ad Hoc mode", it can let your network device join a wireless LAN with peer-to-peer communication. With "Station-Infrastructure mode", it can let your network device join a wireless LAN through an access point. "AP Bridge Mode" provides the function to bridge more than 2 wired Ethernet networks together by wireless LAN. You can use two access points with "AP Bridge-Point to Point mode" to bridge two wired Ethernet networks together. If you want to bridge more than two wired Ethernet networks together, you have to use enough access points with "AP Bridge-Point to Multi-Point mode". An access point with "AP Bridge-Point to Point mode" or "AP Bridge-Point to Multi-Point mode" can only be used to bridge wired Ethernet networks together. It can't accept connection from other wireless station at the same time. If you want an access point to bridge wired Ethernet network and provide connection service for other wireless station at the same time, you have to set the access point to "AP Bridge-WDS mode". Simply speaking, "AP Bridge-WDS mode" function is the combination of "AP mode" and "AP Bridge-Point to Multi-Point mode". "Universal Repeater Mode" provides the function to act as AP client and AP at the same time. It can use AP client function to connect to a Root AP and use AP function to service all wireless stations within its coverage. All the stations within the coverage of this access point can be bridged to the Root AP. "Universal Repeater Mode" is very convenient to extend the coverage of your wireless network.

AP mode setting page:

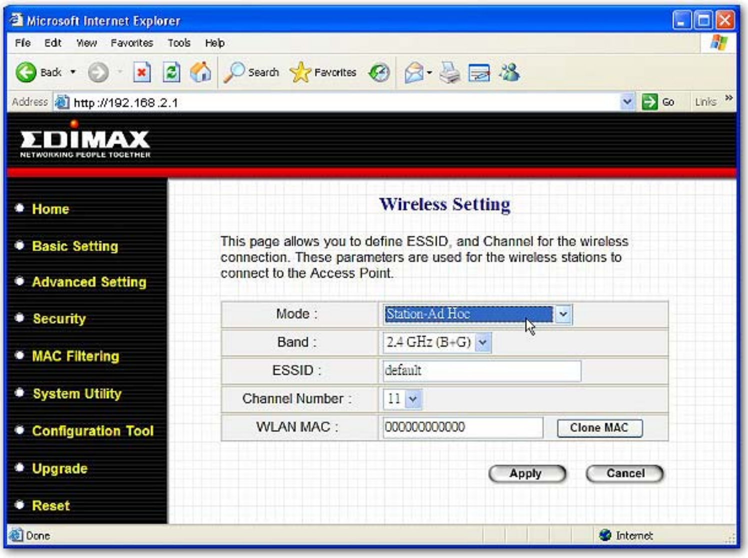


Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	AP
Band :	2.4 GHz (B+G)
ESSID :	default
Channel Number :	11
Associated Clients :	Show Active Clients

Station-Ad Hoc mode setting page:

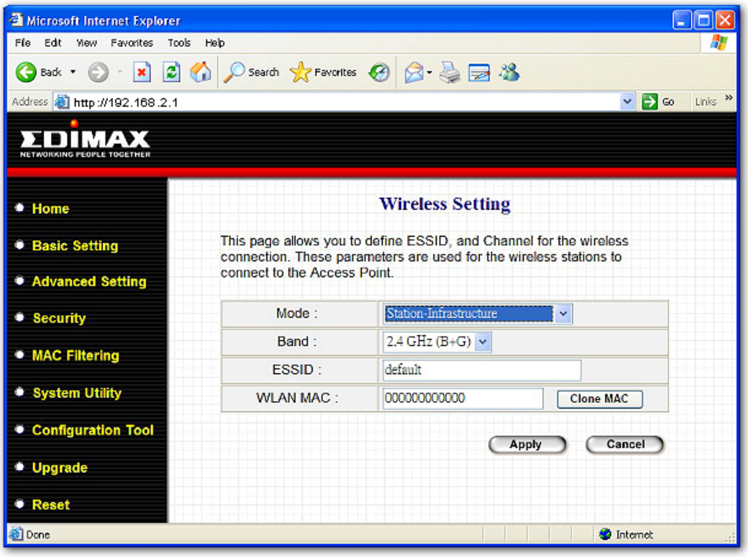


Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	Station-Ad Hoc
Band :	2.4 GHz (B+G)
ESSID :	default
Channel Number :	11
WLAN MAC :	000000000000 Clone MAC

Station-Infrastructure mode setting page:

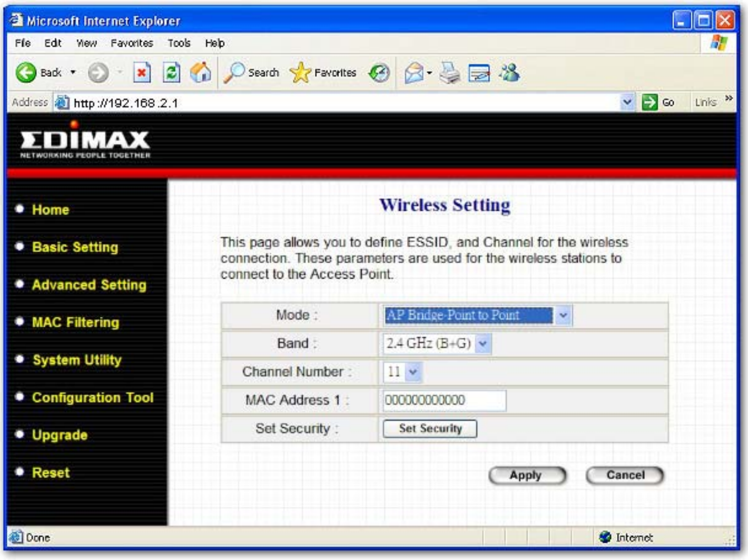


Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	Station-Infrastructure
Band :	2.4 GHz (B+G)
ESSID :	default
WLAN MAC :	000000000000 Clone MAC

AP Bridge-Point to Point mode setting page:

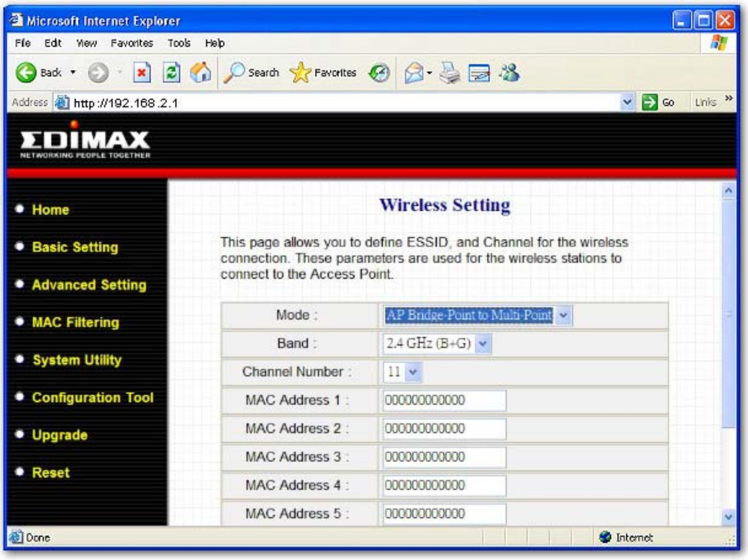


Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	AP Bridge-Point to Point
Band :	2.4 GHz (B+G)
Channel Number :	11
MAC Address 1 :	000000000000
Set Security :	Set Security

AP Bridge-Point to Multi-Point mode setting page:

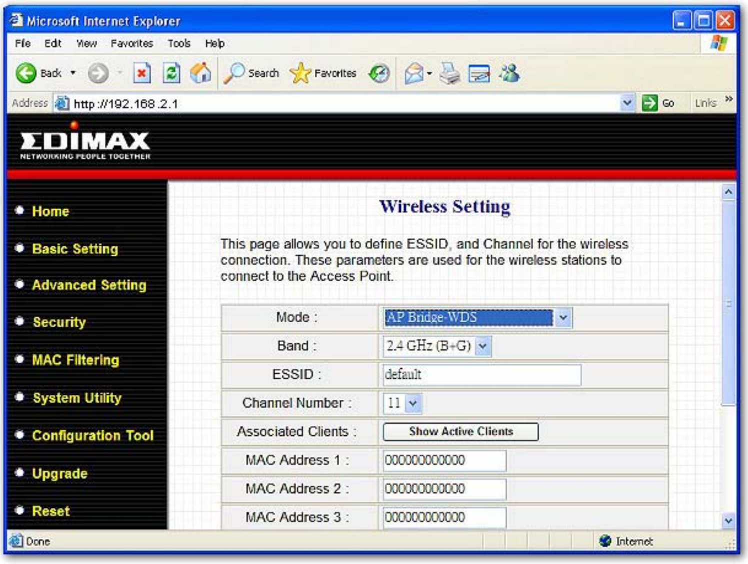


Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	AP Bridge-Point to Multi-Point
Band :	2.4 GHz (B+G)
Channel Number :	11
MAC Address 1 :	000000000000
MAC Address 2 :	000000000000
MAC Address 3 :	000000000000
MAC Address 4 :	000000000000
MAC Address 5 :	000000000000

AP Bridge-WDS mode setting page:

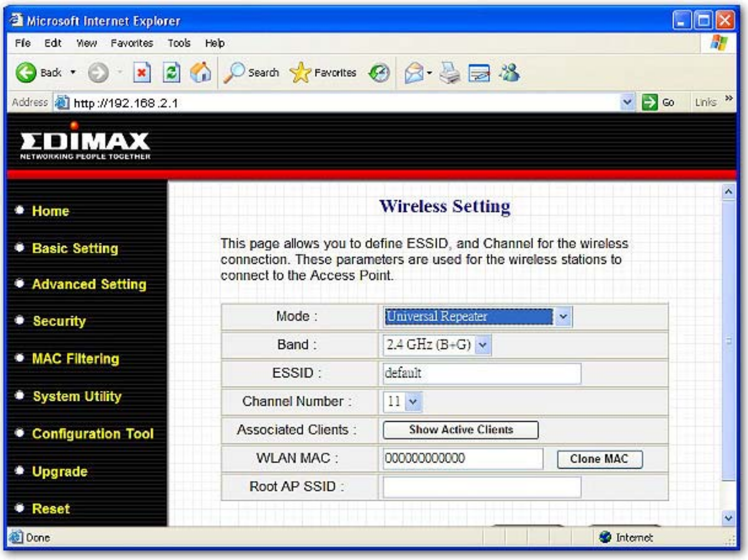


Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	AP Bridge-WDS
Band :	2.4 GHz (B+G)
ESSID :	default
Channel Number :	11
Associated Clients :	Show Active Clients
MAC Address 1 :	000000000000
MAC Address 2 :	000000000000
MAC Address 3 :	000000000000

Universal Repeater mode setting page:



Wireless Setting

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

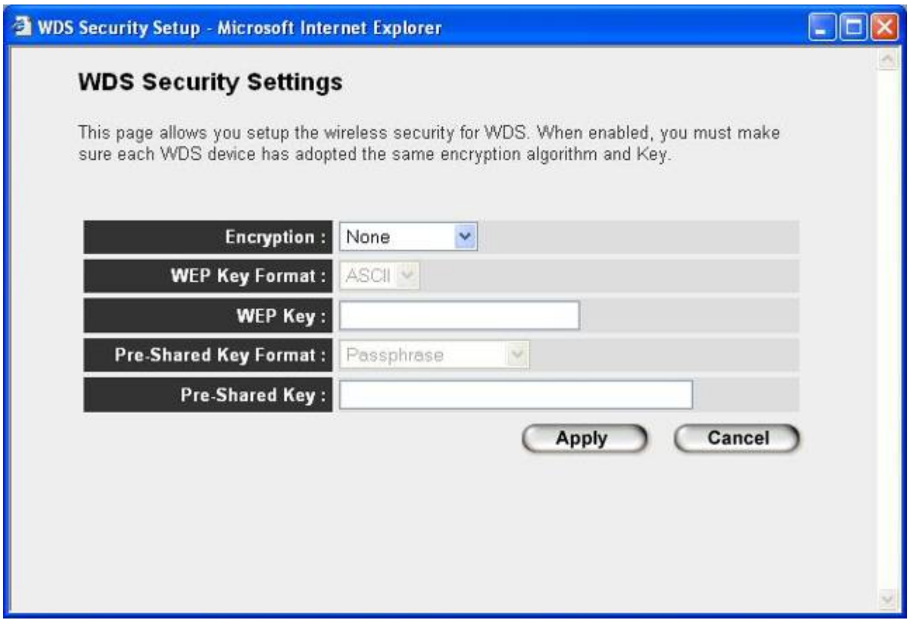
Mode :	Universal Repeater
Band :	2.4 GHz (B+G)
ESSID :	default
Channel Number :	11
Associated Clients :	Show Active Clients
WLAN MAC :	000000000000 Clone MAC
Root AP SSID :	

Parameter	Description
ESSID	The ESSID (up to 31 printable ASCII characters) is the unique name in a WLAN. The ID prevents the unintentional merge of two nearby WLANs. Please make sure that the ESSID of all wireless stations in the same WLAN network are the same. The default ESSID is "**default**". You should assign ESSID in "AP mode", "Station-Ad Hoc mode", "Station-Infrastructure mode", "AP Bridge-WDS mode" and "Universal Repeater mode".
Band	It allows you to set the AP fixed at 802.11b or 802.11g mode. You also can select B+G mode to allow the AP select 802.11b and 802.11g connection automatically.
Channel Number	Select the appropriate channel from the list provided to correspond to your network settings. Channels differ from country to country. Channel 1-11 (North America) Channel 1-14 (Japan) Channel 1-13 (Europe) There are 14 channels available. You should assign Channel Number in "AP mode", "Station-Ad Hoc mode", "AP Bridge-Point to Point mode", "AP Bridge-Point to Multi-Point mode" and "AP Bridge-WDS mode", "Universal Repeater mode".
MAC Address	If you want to bridge more than one wired Ethernet networks together with wireless LAN, you have to set this access point to "AP Bridge-Point to Point mode", "AP Bridge-Point to Multi-Point mode" or "AP Bridge-WDS mode". You have to enter the MAC addresses of other access points that join the bridging work.
WLAN MAC	In "Station-Ad Hoc mode", "Station-Infrastructure mode" and "Universal Repeater mode", this device need a WLAN MAC address to act as a station to connect to other peer or access point. You also can click "Clone MAC" button to let this device copy the MAC address of the PC you are using to configure this device.
Root AP SSID	In "Universal Repeater mode", this device can act as a station to connect to a Root AP. You should assign the SSID of the Root AP here.
Set Security	In "AP Bridge-Point to Point mode", ""AP Bridge-Point to Multi-Point mode" and "AP Bridge-WDS mode", you can click "Set Security" to add encryption for the communication between the bridged access points. This can protect your wireless network.
Associated Clients	Click "Show Active Clients" button, then an "Active Wireless Client Table" will pop up. You can see the status of all active wireless stations that are connecting to the access point.
Wireless Site Survey	When you use this access point as a wireless station for wired network device to have wireless capability, you have to associate it will an working access point. Click "Select Site Survey" button, then a "Wireless Site Survey Table" will pop up. It will list all available access points near by. You can select one access point in the table and it will join wireless LAN through this access point.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

Set Security

"Set Security" let you setup the wireless security for the data transmission between the bridged access points in "AP Bridge-Point to Point mode", "AP Bridge-Point to Multi-Point mode" or "AP Bridge-WDS mode". It provides "WEP 64bits", "WEP 128bits", "WPA (TKIP)", "WPA2 (AES)" encryption methods.



WDS Security Settings

This page allows you setup the wireless security for WDS. When enabled, you must make sure each WDS device has adopted the same encryption algorithm and Key.

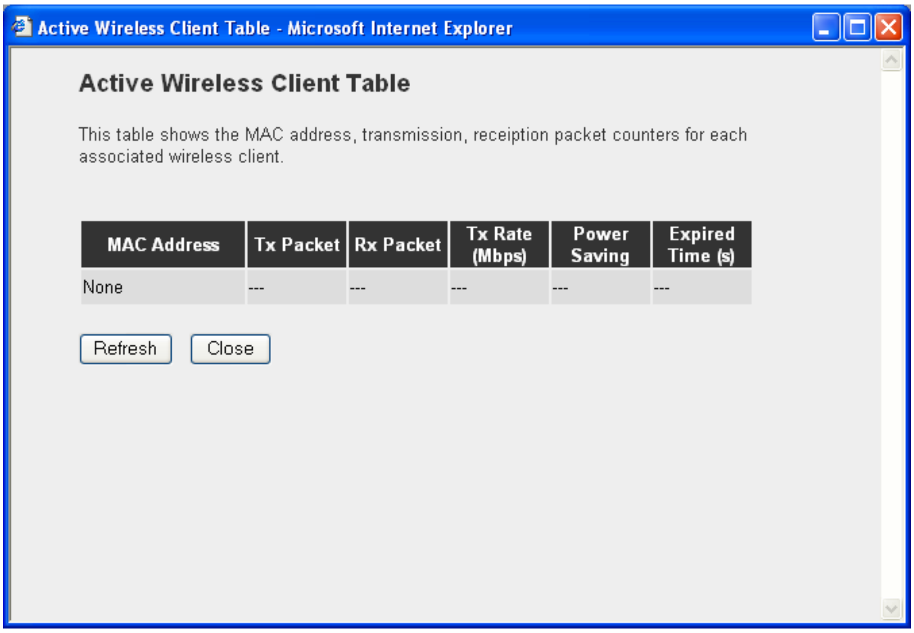
Encryption :	None
WEP Key Format :	ASCII
WEP Key :	
Pre-Shared Key Format :	Passphrase
Pre-Shared Key :	

Parameter	Description
Encryption	You can select "No encryption", "WEP 64bits", "WEP 128bits", "WPA (TKIP)" or "WPA2 (AES)" encryption methods.
Key Format	This is only used when you select "WEP 64bits" or "WEP 128bits" encryption method. You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key. For example: ASCII Characters: guest Hexadecimal Digits: 12345abcde
WEP Key	This is only used when you select "WEP 64bits" or "WEP 128bits" encryption method. The WEP key is used to encrypt data transmitted between the bridged access points. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 10-digit ASCII characters as the encryption keys.
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted between the bridged access points. Fill the text box by following the rules below. Hex WEP: input 64-digit Hex values (in the "A-F", "a-f" and "0-9" range) or at least 8 character pass phrase as the pre-shared keys.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

Active Wireless Client Table

“Active Wireless Client Table” records the status of all active wireless stations that are connecting to the access point. You can lookup the MAC Address, Number of Transmitted Packets and Number of Received Packets of each active wireless client in this table.



Active Wireless Client Table

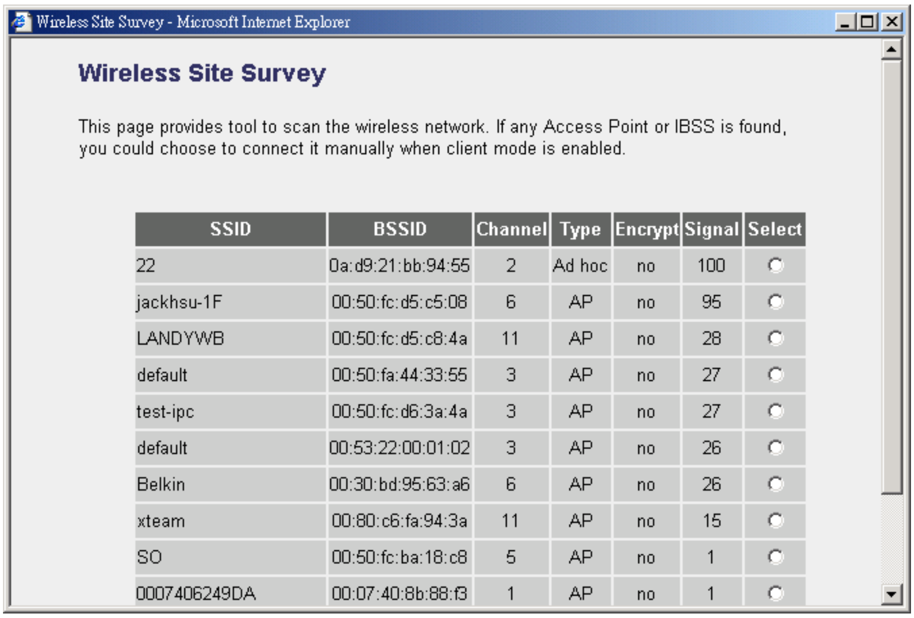
This table shows the MAC address, transmission, receiption packet counters for each associated wireless client.

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---

Parameter	Description
MAC Address	MAC address of this active wireless station.
Tx Packet	The number of transmitted packets that are sent out from this active wireless station.
Rx Packet	The number of received packets that are received by this active wireless station.
TX Rate	The transmission rate in Mbps.
Power Saving	Shows if the wireless client is in Power Saving mode.
Expired Time	The time in second before dissociation. If the wireless keeps idle longer than the expired time, this access point will dissociate it. The wireless client station has to associate again when it becomes active.
Refresh	Refresh the “Active Wireless Client Table”.
Close	Refresh the “Active Wireless Client Table”.

Wireless Site Survey

When this access point is in “Station-Ad Hoc mode”, “Station-Infrastructure mode” or “Universal Repeater mode”, it should associate with an access point or wireless station and connect it to your wireless LAN. “Wireless Site Survey” searches for all available access points near by. You can select one access point listed in this table.



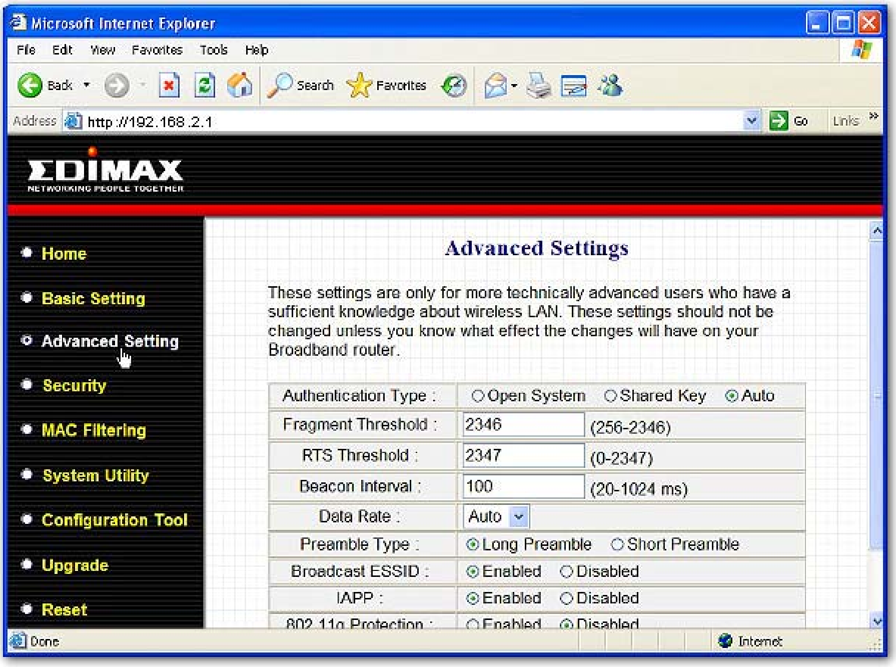
Wireless Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encrypt	Signal	Select
22	0a:d9:21:bb:94:55	2	Ad hoc	no	100	○
jackhsu-1F	00:50:fc:d5:c5:08	6	AP	no	95	○
LANDYWB	00:50:fc:d5:c8:4a	11	AP	no	28	○
default	00:50:fa:44:33:55	3	AP	no	27	○
test-ipc	00:50:fc:d6:3a:4a	3	AP	no	27	○
default	00:53:22:00:01:02	3	AP	no	26	○
Belkin	00:30:bd:95:63:a6	6	AP	no	26	○
xteam	00:80:c6:fa:94:3a	11	AP	no	15	○
SO	00:50:fc:ba:18:c8	5	AP	no	1	○
0007406249DA	00:07:40:8b:88:f3	1	AP	no	1	○

3.2.3 Advanced Setting

You can set advanced parameters of this access point. The parameters include Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, Tx Operation Rate, Tx Basic Rate, Preamble Type, Broadcast ESSID. You should not change these parameters unless you know what effect the changes will have on this access point.



Advanced Settings

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Broadband router.

Authentication Type :	○ Open System ○ Shared Key ● Auto
Fragment Threshold :	2346 (256-2346)
RTS Threshold :	2347 (0-2347)
Beacon Interval :	100 (20-1024 ms)
Data Rate :	Auto
Preamble Type :	● Long Preamble ○ Short Preamble
Broadcast ESSID :	● Enabled ○ Disabled
IAPP :	● Enabled ○ Disabled
802.11g Protection :	○ Enabled ● Disabled

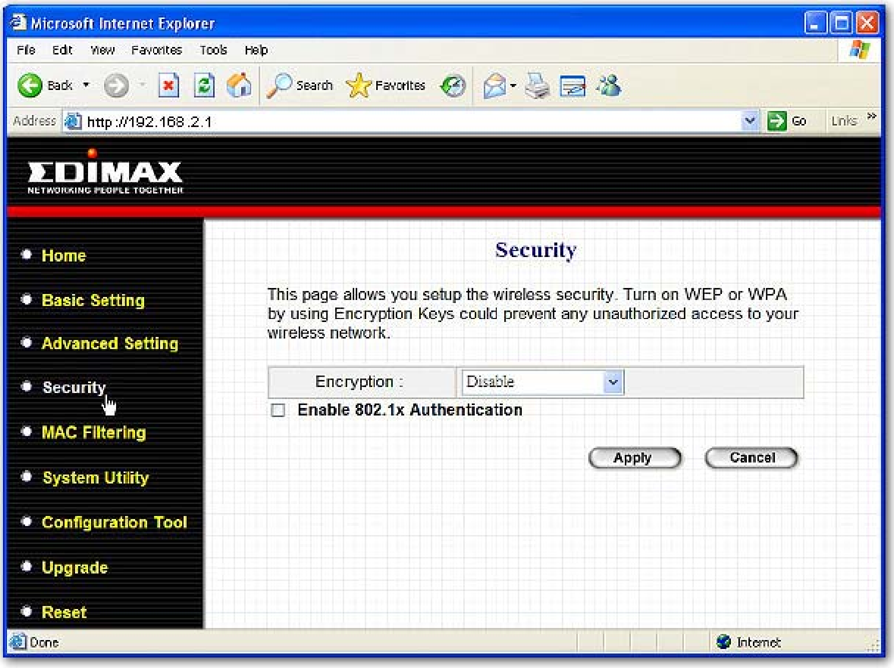
Parameter	Description
Authentication Type	There are two authentication types: “Open System” and “Shared Key”. When you select “Open System”, wireless stations can associate with this access point without WEP encryption. When you select “Shared Key”, you should also setup WEP key in the “Encryption” page and wireless stations should use WEP encryption in the authentication phase to associate with this access point. If you select “Auto”, the wireless client can associate with this access point by using any one of these two authentication types.
Fragment Threshold	“Fragment Threshold” specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller than the RTS threshold, the access point will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this access point broadcast a beacon. Beacon is used to synchronize the wireless network.
Data Rate	The “Data Rate” is the rate this access point uses to transmit data packets. The access point will use the highest possible selected transmission rate to transmit the data packets.
Preamble Type	Preamble type defines the length of CRC block in the frames during the wireless communication. “Short Preamble” is suitable for high traffic wireless network. “Long Preamble” can provide more reliable communication.
Broadcast ESSID	If you enable “Broadcast ESSID”, every wireless station located within the coverage of this access point can discover this access point easily. If you are building a public wireless network, enabling this feature is recommended. Disabling “Broadcast ESSID” can provide better security.
IAPP	If you enable “IAPP”, the access point will automatically broadcast information of associated wireless stations to its neighbors. This will help wireless station roaming smoothly between access points. If you have more than one access points in your wireless LAN and wireless stations have roaming requirements, enabling this feature is recommended. Disabling “IAPP” can provide better security.
802.11g Protection	This is also called CTS Protection. It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

3.2.4 Security

This Access Point provides complete wireless LAN security functions, include WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function.

Note: This access point can act as station and AP at the same time in “Universal Repeater mode”. The security settings only apply to AP function in “Universal Repeater mode”. The station function of “Universal Repeater mode” does not have security feature.



Security

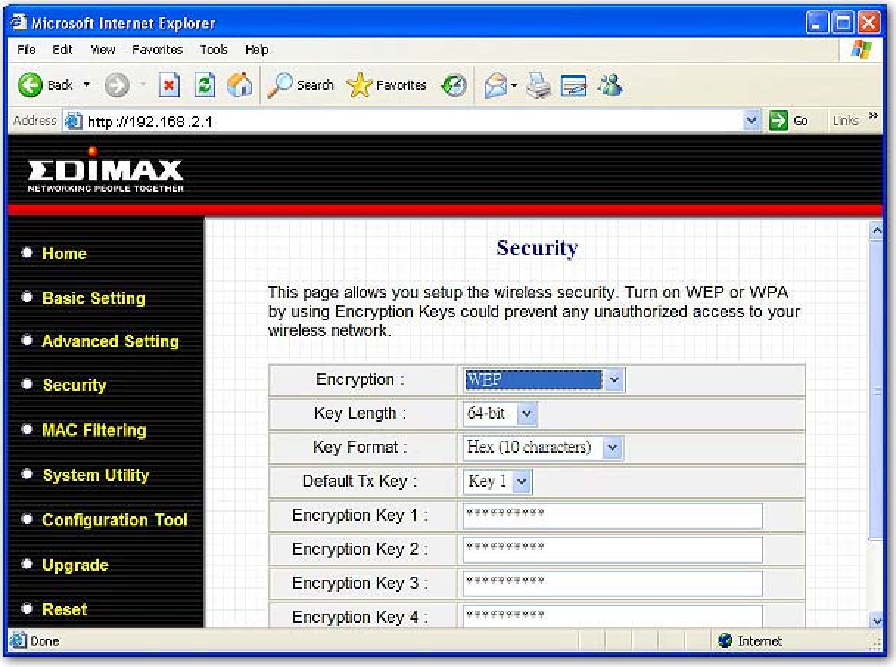
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption :	Disable

□ Enable 802.1x Authentication

WEP only

When you select 64-bit or128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as default key. Then the access point can receive any packets encrypted by one of the four keys. You can use WEP encryption in “AP mode”, “Station-Ad Hoc mode”, “Station-Infrastructure mode”, “AP Bridge-WDS mode” and “Universal Repeater mode”.



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

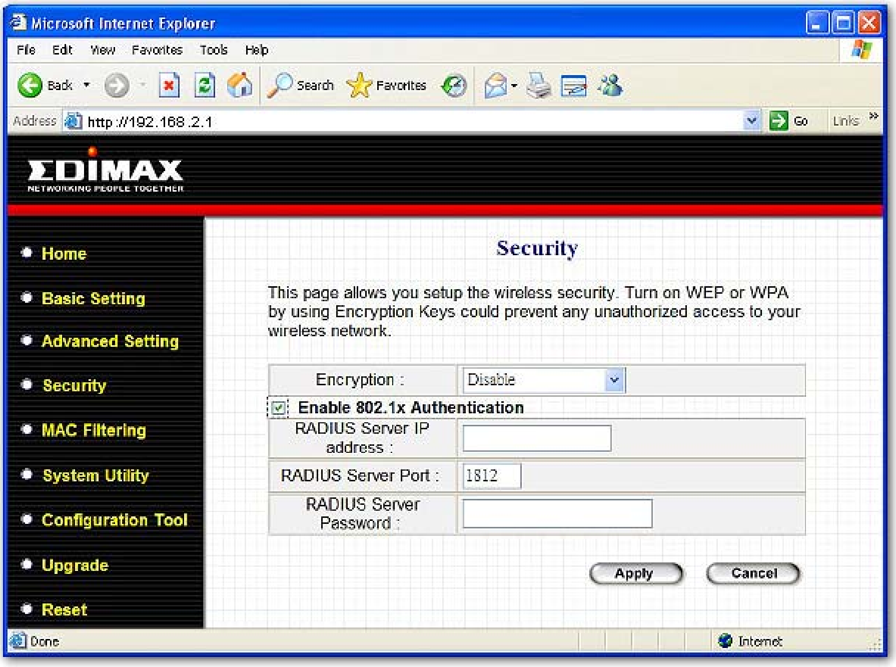
Encryption :	WEP
Key Length :	64-bit
Key Format :	Hex (10 characters)
Default Tx Key :	Key 1
Encryption Key 1 :	**********
Encryption Key 2 :	**********
Encryption Key 3 :	**********
Encryption Key 4 :	**********

Parameter	Description
Key Length	You can select the 64 or 128-bit key to encrypt transmitted data. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key. For example: ASCII Characters: guest Hexadecimal Digits: 12345abcde
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select it in the "Default key" will take effect.
Key 1 - Key 4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 10-digit ASCII characters as the encryption keys.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

802.1x only

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. You can use 802.1x without encryption in "AP mode", "AP Bridge-WDS mode" and "Universal Repeater mode".



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

Encryption : Disable

☑ Enable 802.1x Authentication

RADIUS Server IP address :

RADIUS Server Port : 1812

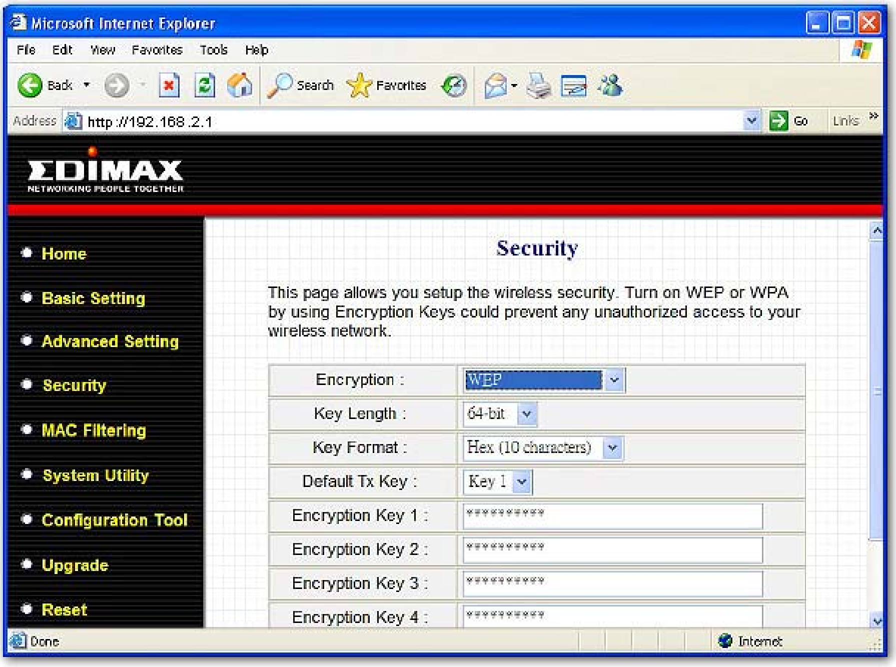
RADIUS Server Password :

Parameter	Description
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

802.1x WEP static key

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode also uses WEP to encrypt the data during communication. You can use 802.1x with WEP encryption in “AP mode”, “AP Bridge-WDS mode” and “Universal Repeater mode”.



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

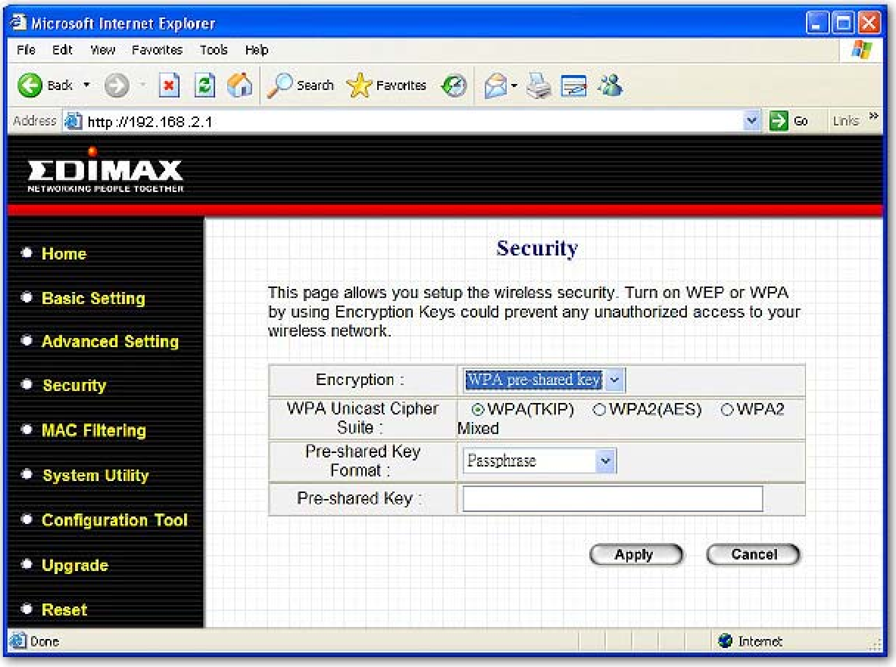
Encryption :	WEP
Key Length :	64-bit
Key Format :	Hex (10 characters)
Default Tx Key :	Key 1
Encryption Key 1 :	**********
Encryption Key 2 :	**********
Encryption Key 3 :	**********
Encryption Key 4 :	**********

For the WEP settings, please refer to section “WEP only”. For the 802.1x settings, please refer to section “802.1x only”.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

WPA pre-shared key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP(AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much. You can use WPA pre-shared key encryption in “AP mode”, “Station-Ad Hoc mode”, “Station-Infrastructure mode”, “AP Bridge-WDS mode” and “Universal Repeater mode”.



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

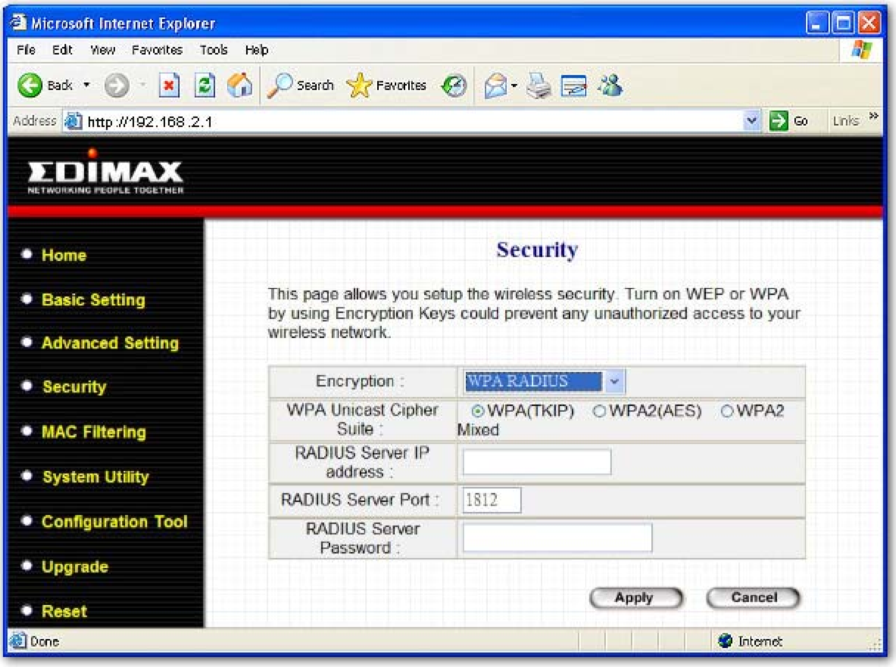
Encryption :	WPA pre-shared key
WPA Unicast Cipher Suite :	● WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed
Pre-shared Key Format :	Passphrase
Pre-shared Key :	

Parameter	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
Pre-shared Key Format	You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key. For example: Passphrase: iamguest Hexadecimal Digits: 12345abcde
Pre-shared Key	The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex WEP: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

WPA RADIUS

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use an external RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP(AES) to change the encryption key frequently. This can improve security very much. You can use WPA RADIUS encryption in “AP mode”, “AP Bridge-WDS mode” and “Universal Repeater mode”.



Security

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

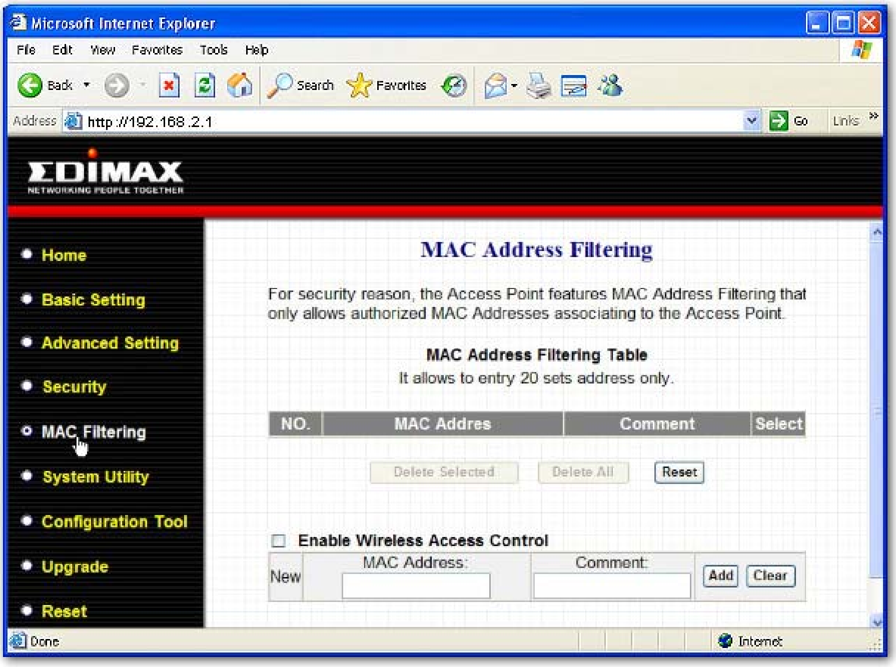
Encryption :	WPA RADIUS
WPA Unicast Cipher Suite :	● WPA(TKIP) ○ WPA2(AES) ○ WPA2 Mixed
RADIUS Server IP address :	
RADIUS Server Port :	1812
RADIUS Server Password :	

Parameter	Description
WPA(TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
WPA2(AES)	This use CCMP protocol to change encryption key frequently. AES can provide high level encryption to enhance the wireless LAN security.
WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
RADIUS Server IP address	The IP address of external RADIUS server.
RADIUS Server Port	The service port of the external RADIUS server.
RADIUS Server Password	The password used by external RADIUS server.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

3.2.5 MAC Address Filtering

This Access Point provides MAC Address Filtering, which prevents the unauthorized MAC Addresses from accessing your wireless network.



MAC Address Filtering

For security reason, the Access Point features MAC Address Filtering that only allows authorized MAC Addresses associating to the Access Point.

MAC Address Filtering Table

It allows to entry 20 sets address only.

NO.	MAC Addres	Comment	Select

□ Enable Wireless Access Control

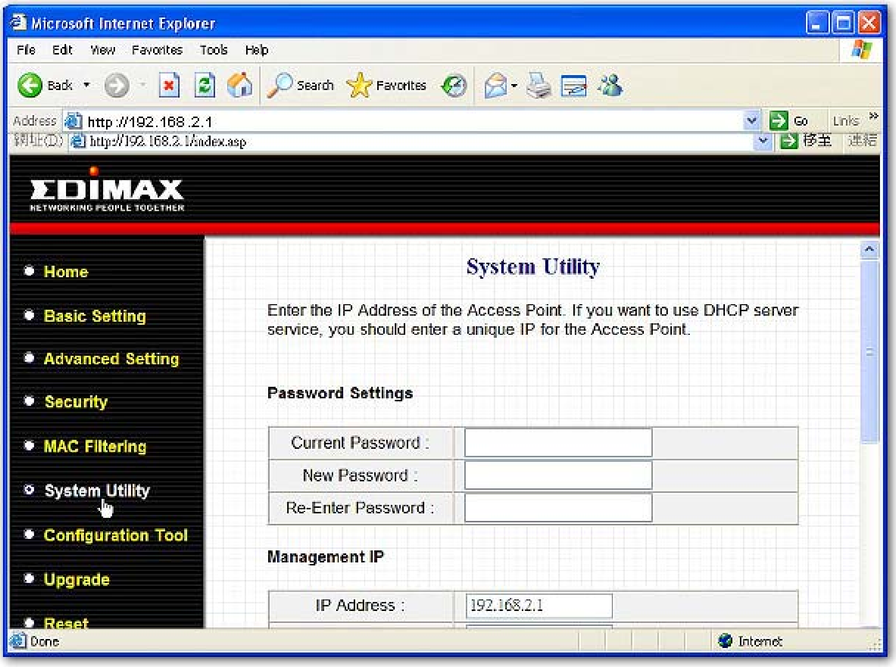
	MAC Address:	Comment:	
New			Add Clear

Parameter	Description
Enable Wireless Access Control	Enable or disable the MAC Address Filtering function.
MAC Address Filtering Table	This table records the MAC addresses of wireless stations you want to allow to access your network. The “Comment” field is the description of the wireless station associated with the “MAC Address” and is helpful for you to recognize the wireless station.
Add MAC address into the table	In the bottom “New” area, fill in the “MAC Address” and “Comment” of the wireless station to be added and then click “Add”. Then this wireless station will be added into the “MAC Address Filtering Table” above. If you find any typo before adding it and want to retype again. Just click “Clear” and both “MAC Address” and “Comment” fields will be cleared.
Remove MAC address from the table	If you want to remove some MAC address from the “MAC Address Filtering Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”. If you want remove all MAC addresses from the table, just click “Delete All” button.
Reset	Click “Reset” will clear your current selections.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

3.2.6 System Utility

From here, you can define the Access Point's IP Address and Login Password and enable the Access Point to be a DHCP Server. You can change AP's IP address to meet your network IP range so you can log in to set up page easily next time.



System Utility

Enter the IP Address of the Access Point. If you want to use DHCP server service, you should enter a unique IP for the Access Point.

Password Settings

Current Password :	
New Password :	
Re-Enter Password :	

Management IP

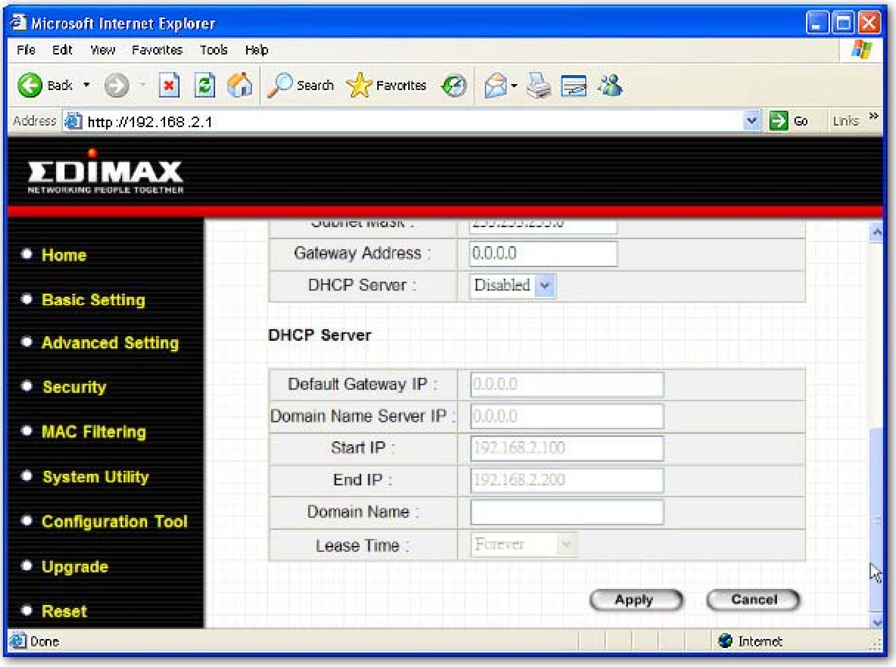
IP Address :	192.168.2.1

Parameter	Description
Current Password	Enter the current password (up to 15-digit alphanumeric string) of the Access Point. The default password for the Access Point is **1234**. Note that the password is case-sensitive.
New Password	Enter the password (up to 15-digit alphanumeric string) you want to login to the Access Point. Note that the password is case-sensitive.
Re-Enter Password	Reconfirm the password (up to 15-digit alphanumeric string) you want to login to the Access Point. Note that the password is case-sensitive.
IP Address	Designate the Access Point's IP Address. This IP Address should be unique in your network. The default IP Address is **192.168.2.1**.
Subnet Mask	Specify a Subnet Mask for your LAN segment. The Subnet Mask of the Access Point is fixed and the value is **255.255.255.0**.
Gateway Address	The IP address of the default gateway of the subnet that this access point resides in. It allows this access point be accessed by PC from deferent subnet to do configuration.
DHCP Server	Enable or disable the DHCP Server.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

DHCP Server Setting

DHCP Server will automatically give your LAN client an IP address. If the DHCP is not enabled then you'll have to manually set your LAN client's IP address. There is only one DHCP server allowed in one network. If you have a router or other DHCP server, please keep this feature disabled.



Gateway Address : 0.0.0.0

DHCP Server : Disabled

DHCP Server

Default Gateway IP : 0.0.0.0

Domain Name Server IP : 0.0.0.0

Start IP : 192.168.2.100

End IP : 192.168.2.200

Domain Name :

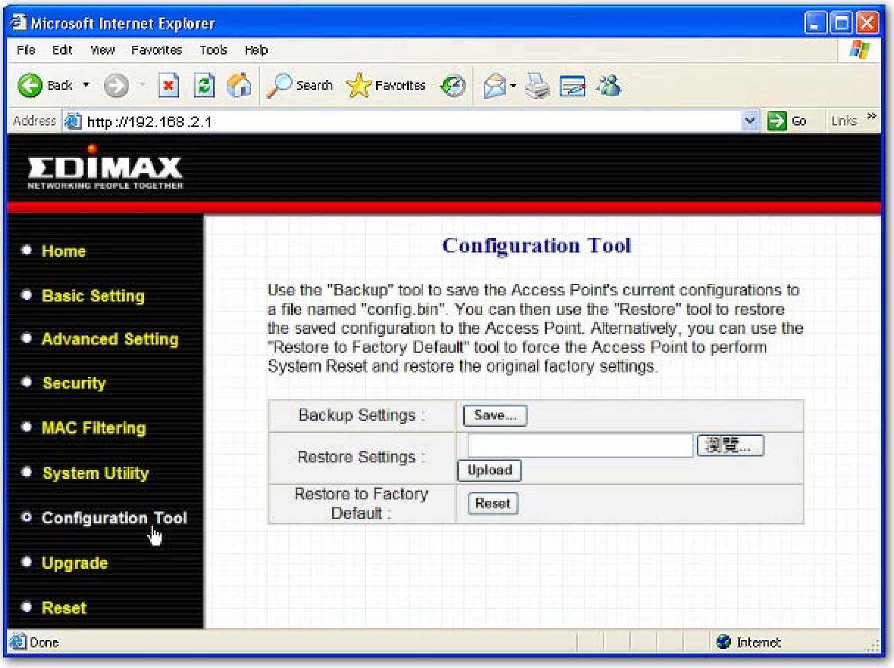
Lease Time : Forever

Parameter	Description
Default Gateway IP	Specify the gateway IP in your network. This IP address should be different from the Management IP.
Domain Name Server IP	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address.
Start IP/End IP	You can designate a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. By default the IP range is from: Start IP **192.168.2.100** to End IP **192.168.2.200**.
Domain Name	You can specify the Domain Name for your Access Point.
Lease Time	The DHCP Server when enabled will temporarily give your LAN client an IP address. In the Lease Time setting you can specify the time period that the DHCP Server lends an IP address to your LAN clients. The DHCP Server will change your LAN client's IP address when this time threshold period is reached.

Click **Apply** button at the bottom of the screen to save the above configurations. You can now configure other advance sections or start using the Access Point.

3.2.7 Configuration Tool

The Configuration Tools screen allows you to save (**Backup**) the Access Point’s current configuration setting. Saving the configuration settings provides an added protection and convenience should problems occur with the Access Point and you have to reset to factory default. When you save the configuration setting (Backup) you can re-load the saved configuration into the Access Point through the **Restore** selection. If extreme problems occur you can use the **Restore to Factory Default** selection, this will set all configurations to its original default settings (e.g. when you first purchased the Access Point).



Configuration Tool

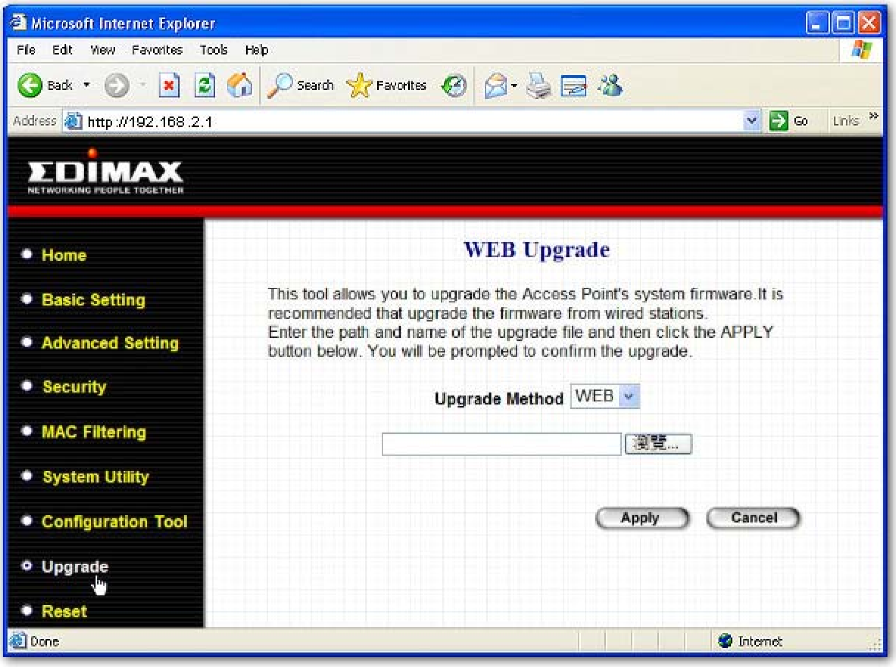
Use the "Backup" tool to save the Access Point's current configurations to a file named "config.bin". You can then use the "Restore" tool to restore the saved configuration to the Access Point. Alternatively, you can use the "Restore to Factory Default" tool to force the Access Point to perform System Reset and restore the original factory settings.

Backup Settings :	Save...
Restore Settings :	瀏覽... Upload
Restore to Factory Default :	Reset

Parameter	Description
Configuration Tools	Use the "**Backup**" tool to save the Access Point’s current configuration to a file named "config.bin" on your PC. You can then use the "**Restore**" tool to upload and restore the saved configuration to the Access Point. Alternatively, you can use the "**Restore to Factory Default**" tool to force the Access Point to perform a power reset and restore the original factory settings.

3.2.8 Firmware Upgrade

This page allows you to upgrade the Access Point’s firmware.



WEB Upgrade

This tool allows you to upgrade the Access Point's system firmware.It is recommended that upgrade the firmware from wired stations.
Enter the path and name of the upgrade file and then click the APPLY button below. You will be prompted to confirm the upgrade.

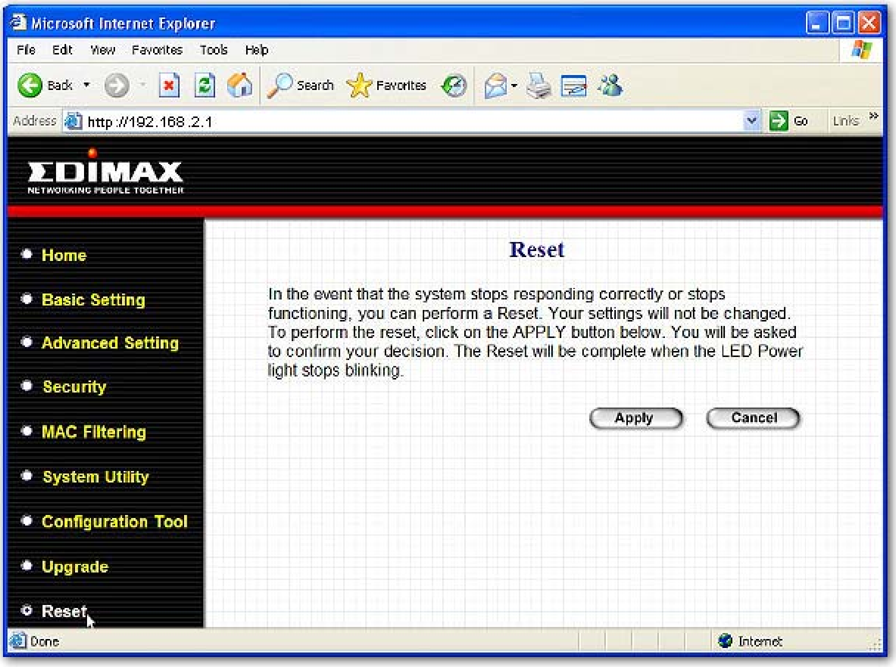
Upgrade Method WEB

Parameter	Description
Firmware Upgrade	This tool allows you to upgrade the Access Point’s system firmware. To upgrade the firmware of your Access Point, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the **Browse** button to find the firmware file on your PC. Please reset the Access Point when the upgrade process is complete.

Once you’ve selected the new firmware file, click **Apply** button at the bottom of the screen to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete). Once the upgrade is complete you can start using the Access Point.

3.2.9 Reset

You can reset the Access Point's system should any problem exist. The reset function essentially Re-boots your Access Point's system.



Reset

In the event that the system stops responding correctly or stops functioning, you can perform a Reset. Your settings will not be changed. To perform the reset, click on the APPLY button below. You will be asked to confirm your decision. The Reset will be complete when the LED Power light stops blinking.

Parameter	Description
Reset	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. **Your settings will not be changed**. To perform the reset, click on the **Apply** button. You will be asked to confirm your decision. Once the reset process is complete you may start using the Access Point again.

Chapter 4 Troubleshooting

This chapter provides solutions to problems usually encountered during the installation and operation of the Access Point.

1. **How to manually find your PC's IP and MAC Address?**

    1) In Windows, open the Command Prompt program

    2) Type **ipconfig /all** and **Enter**

        - Your PC's IP address is the one entitled **IP address**
        - Your PC's MAC Address is the one entitled **Physical Address**

2. **What is Ad-hoc?**

    An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN.

3. **What is Infrastructure?**

    An integrated wireless and wired LAN is called an Infrastructure configuration.

4. **What is BSS ID?**

    A group of wireless stations and an Access Point compose a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSSID.

5. **What is ESSID?**

    An Infrastructure configuration could also support roaming capability for mobile workers. More than one BSS can be configured as an Extended Service Set (ESS). Users within an ESS could roam freely between BSSs while maintaining a continuous connection to the wireless network stations and the Wireless LAN Access Points.

6. **Can data be intercepted while transmitting through the air?**

    WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent scrambling security feature. On the software side, the WLAN series offers the encryption function (WEP/WPA) to enhance security and access control.

7. **What is WEP?**

    WEP stands for Wired Equivalent Privacy, a data privacy mechanism based on a 64(40)-bit shared key algorithm.

8. **What is a MAC Address?**

    The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

EDIMAX
NETWORKING PEOPLE TOGETHER

EDIMAX Technology Co., Ltd.
www.edimax.com