CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Securing Wireless Access Points / Routers

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

Table of contents

1. Introduction

Wi-Fi (Wireless Fidelity) devices - well known for their portability, flexibility and increased productivity are based on IEEE 802.11 standard . IEEE 802.11 WLAN, or Wi-Fi, is the most widely accepted broadband wireless networking technology, providing the highest transmission rate among wireless networking technologies. Today's Wi-Fi devices, based on IEEE 802.11a and 802.11g provide transmission rates up to 54 Mbps and, further, a new standard IEEE 802.11n which supports up to 600 Mbps. The transmission range of a typical Wi-Fi device is up to 100m, where its exact range varies depending on the transmission power, the surrounding environments, and other factors. The 802.11 devices operate in unlicensed bands at 2.4 and 5 GHz, where the exact available bands depend on each county. In order to connect the device to another network (usually wired) Wireless Access Point (base station) or Wireless Router is required .It can relay data between wired devices and wireless devices in the network.

2. Architecture of Wi-Fi networks in a home network.

In a typical home network the Access Point/Router can be used to connect the wireless or wired devices to the internet. The block diagram of the network architecture is shown in the Figure:1.

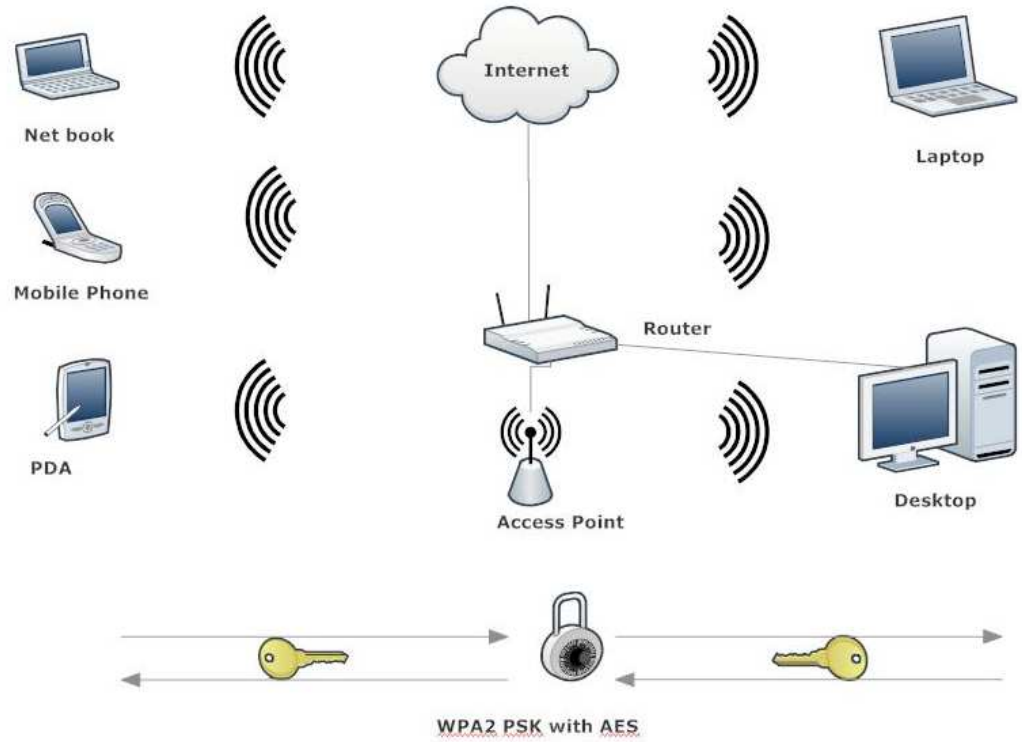

Figure- 1: Wi-Fi Architecture in home networks.

3. Threats to Wi-Fi Implementations

Since radio waves can penetrate through walls there is a great chance of unauthorized access to the network and data. Because of its broadcasting nature, anybody can sniff the network for valuable credentials. If the network is not properly secured the attacker will get sufficient data to launch an attack.
In brief the following cases may happen.

i) The attacker may search for available wireless networks in the close proximity. If the Access Point(AP) is open the attacker can avail the network without any effort.

ii) The attacker can directly log in to the Access Point using default credentials and configure the device in whatever way he wants.

iii) The attacker can sniff the network for configuration details such as SSID(Service Set Identifier) , BSSID(Basic Service Set Identification), encryption used, channel used etc. He can capture sufficient packets to launch an attack.

iv) The attacker can install a fake Access Point and lure(like advertising free internet access) users to connect to the rogue AP.

v) The attacker can disrupt the normal functioning of the network.

4. Securing AP/ Router

As far as a user is concerned, securing Access Point ensures the primary level of security. In this document configuration settings of an AP/Router that is installed in a typical home network is discussed. We have used 'Linksys' WAP 54G and 'beetel' Router for this purpose. The configuration settings as explained below will secure the AP.

i) Change Administrator Password

An attacker can easily find out the default password. It must be changed. Ensure that the admin password is strong enough.

Figure-2: Password editing interface of Administrator

ii) Prefer Wi-Fi Protected Access(WPA2 Preferably) instead of Wired Equivalent Privacy(WEP).

WPA's salient features are strong encryption algorithm, user authentication and support for IEEE 802.1X . Use Wi-Fi Protected Access (WPA) or WPA2 with Pre-Shared Key (PSK) authentication and AES as the encryption standard. The pass phrase should be strong enough.

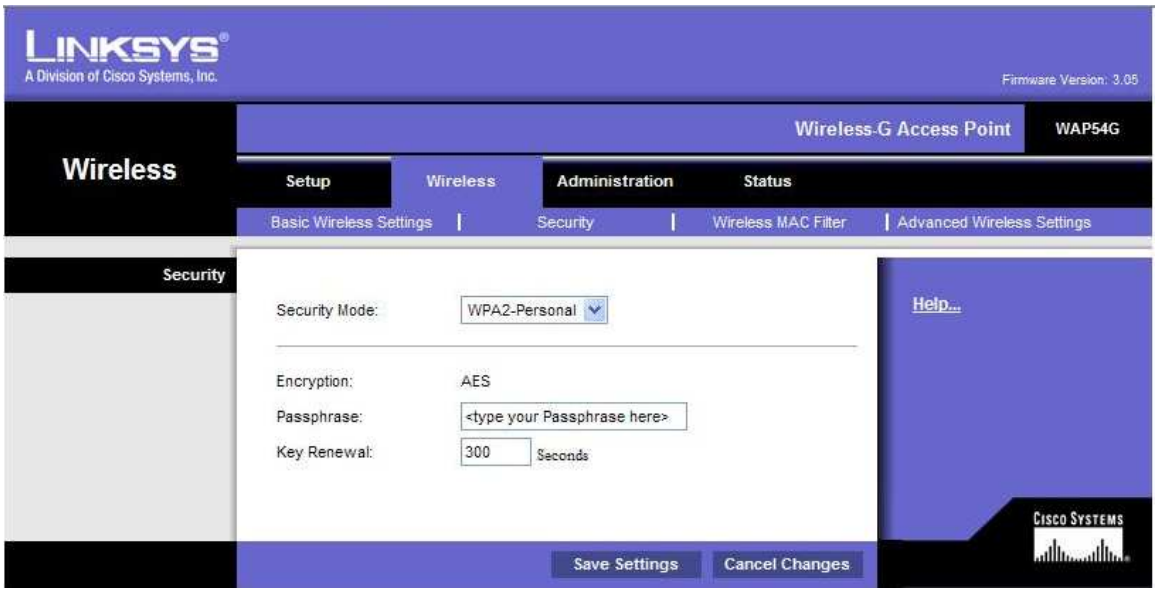

Figure-3: Interface for configuring Security Mode.

iii) Use logging feature in the AP.

Logging will record activities of the wireless access point or router including Wi-Fi activities of the clients that connect to it. This record can serve as an audit trail in case of a security breach and can be useful for troubleshooting. The log can be saved either in local machine or in a remote storage server(mostly in routers).

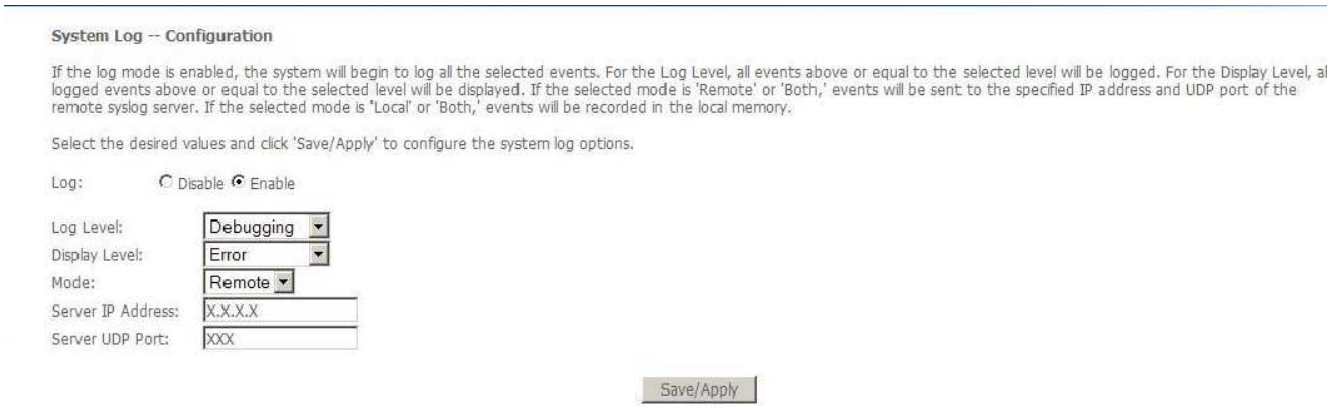

Figure - 4: logging enabled with remote storage

Figure- 5: logging enabled with local storage

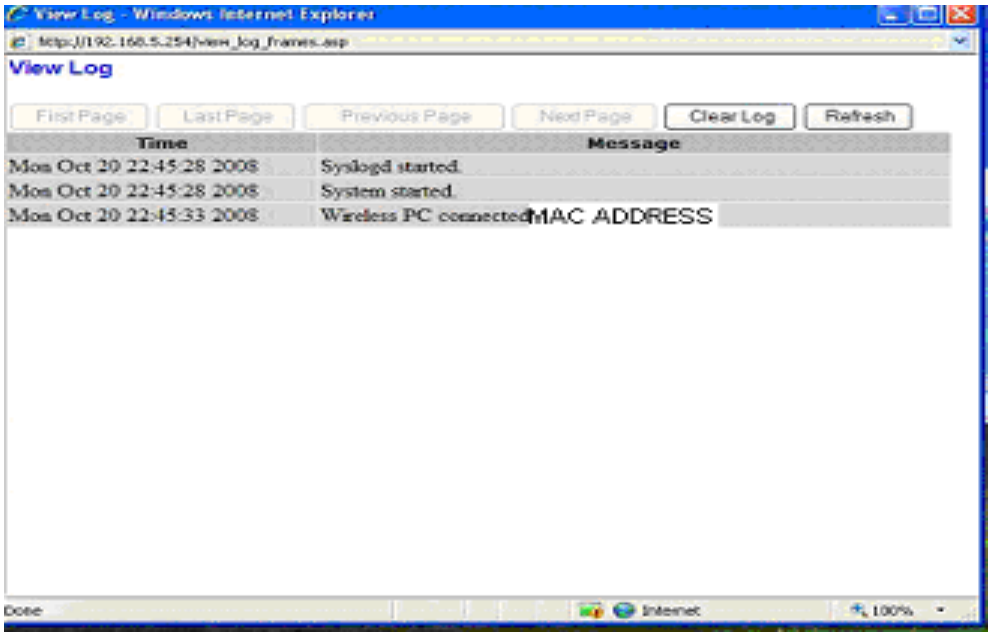

Figure-6: Example Log showing MAC Addresses.

iv) MAC Address Filtering

Access of the clients can be permitted or prevented by providing a list of MAC Addresses in the “MAC Address filter” configuration parameter. This is known as MAC Address filtering. Together with SSID this can also used as a security measure. Select the MAC Address of all the wireless Network interface cards used in the network. The list can be used to permit or prevent the wireless access .

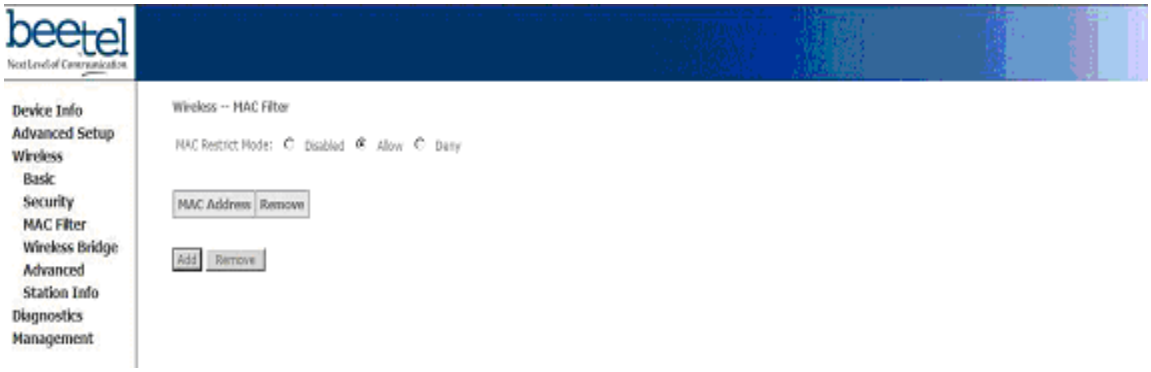

Figure -7 : Configuring MAC filter.

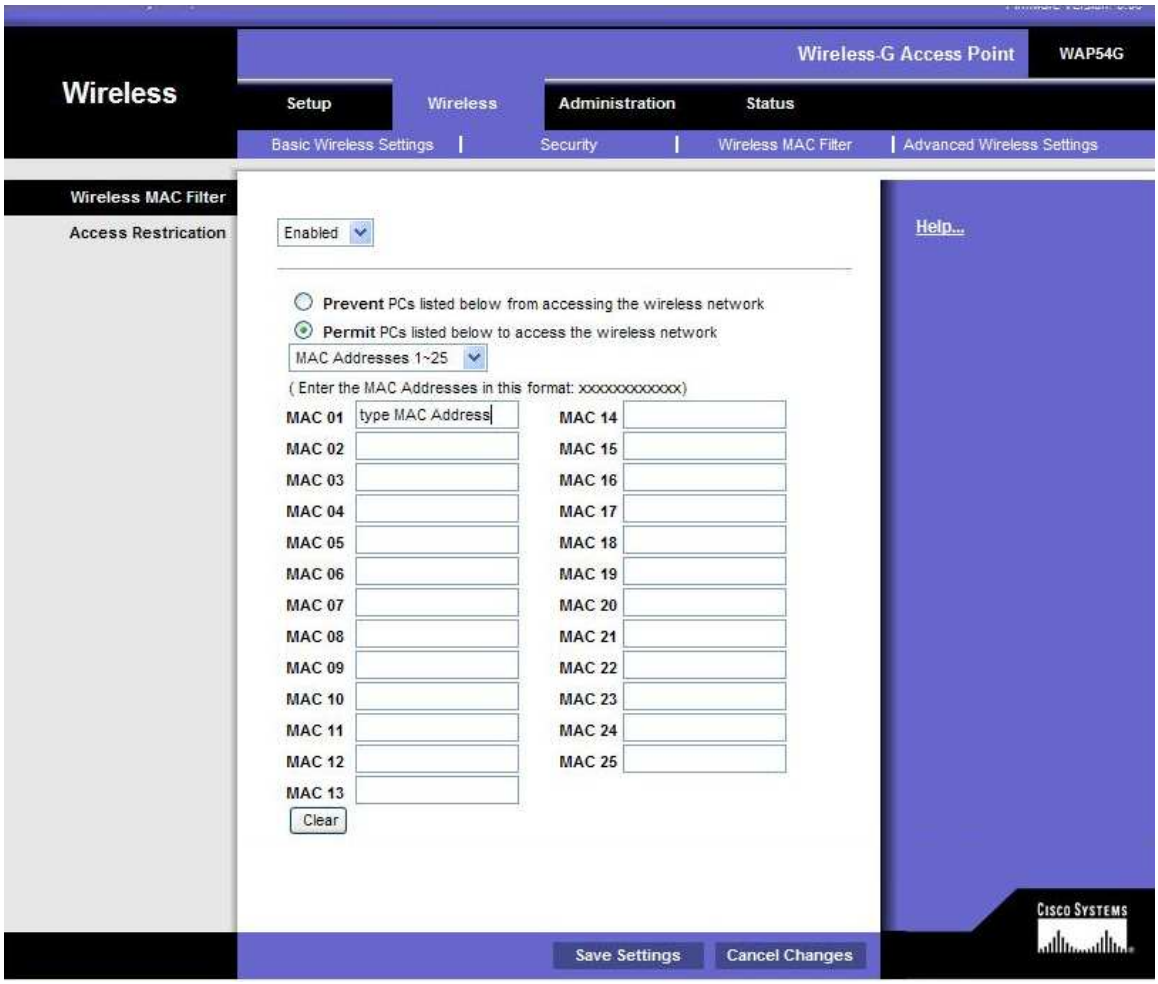

Figure-8: Configuring MAC filter

5. Best Practices

There are certain best practices explained below which should be followed for enhancing security of wireless Access Point / Routers.

i) Restrict the Access

SSID (Service Set Identifier) is used to identify a wireless network which a user wants to attach. All wireless devices that want to communicate on the WLAN need to have their SSID set to the same string as the AP. Even though the attacker can get the SSID simply by sniffing the network it is preferable to change the default SSID. Avoid SSID which shows name or other information. Name the access point such that it can be easily traceable during trouble shooting. Physical security of access point is also important.

ii) Disable Management via Wireless

It is recommended to disable management of the router via wireless devices associated with the access point. If someone manages to associate with the access point and login to the router , they can change the configuration of the router. Prefer wired interface with AP/Router to configure the device.

iii) Disable Remote Management

Remote Router Access permits web-based management of the wireless router from external networks such as the Internet. By default this feature opens port 8080/TCP on the external side of the router. This feature provides significant risk to the device, permitting an attack vector and more importantly significant risk to internal network. It should be disabled unless remote management is absolutely required. Universal Plug and Play may also be disabled.

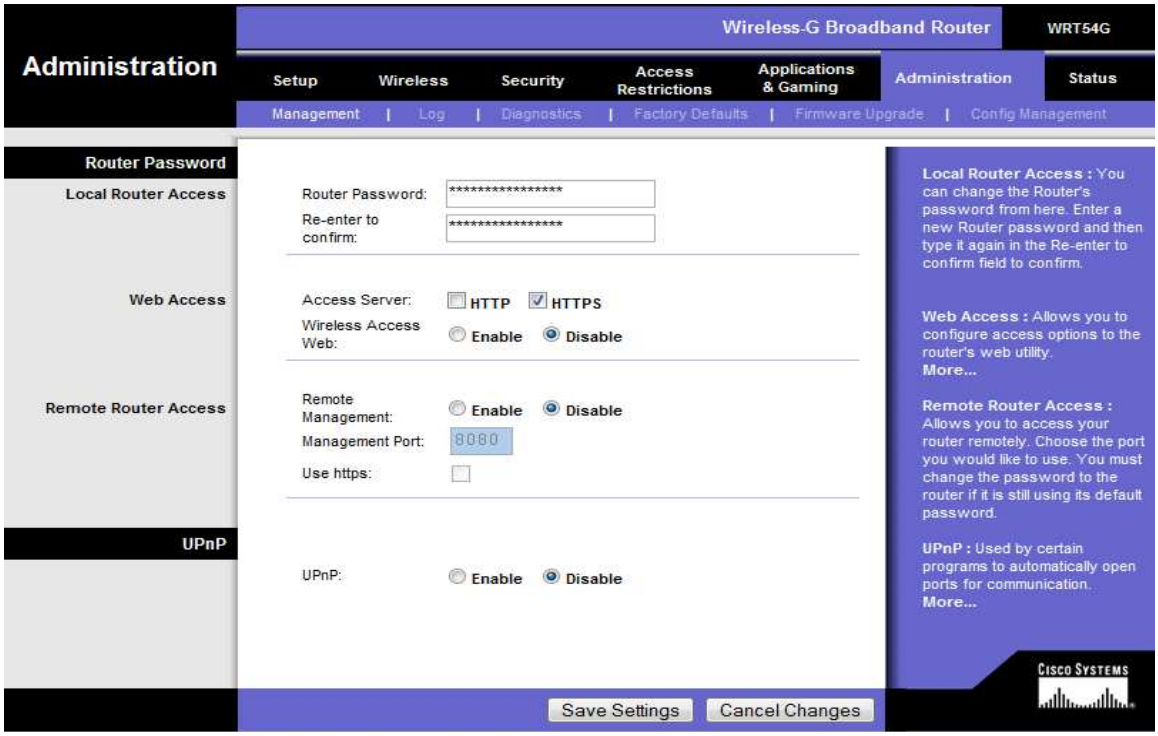

Figure-9: Disabling Remote Management and UPn-P

iv) Turn off the AP when not in use

This is also advisable since it minimizes the risk of unauthorized access.

v) Configure Network Mode

Select the wireless mode which is depending upon the protocols. The possible options are.

- ✓ Disabled – disables AP.
- ✓ Mixed - permits both 802.11 b and 802.11g.
- ✓ B-Only - 8.2.11 b only.
- ✓ G-Only - 8.2.11 g only.

vi) Disable SSID Broadcast.

This can protect the AP from a naive attacker . By disabling SSID broadcast, the easy availability of SSID can be restricted .But the attacker can still sniff the SSID from frames that devices use when associating with an AP. According to some vendors disabling SSID broadcast may restrict or invite the chance of exploitation.

vii) Set Wireless Channel from default

Changing the default wireless channel used by the AP is a good practice. It may avoid automatic association of the wireless interface to the network.

viii) Maximize the Beacon Interval

Beacon frames are used for connection establishment and management by IEEE 802.11 networks. These frames from AP to wireless clients ,transmitted at regular intervals are used for configuration matching. It is recommended to set the beacon interval to the maximum number. This will reduce the transmission frequency of SSID so that the attacker will get less number of opportunities to sniff the beacons containing SSID. But there is a problem here. The attacker can probe the network using some specific SSID which is known as active scanning.

ix) Prefer Static IP instead of DHCP.

Since DHCP is automatically assigning IP addresses, an attacker can utilize this feature to get an IP. So it is recommended to use static IP on wireless networks.

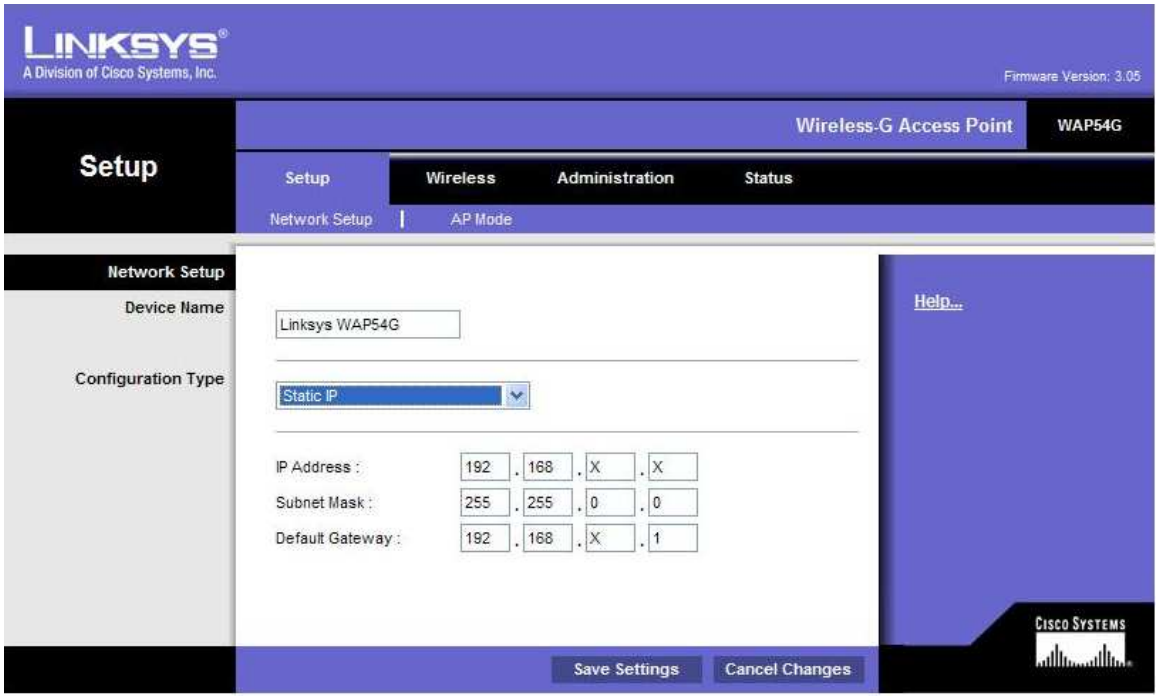

Figure-10: Configuring Static IP.

6. References

i) SANS

Joe Scolamiero Version 5.1b GIAC / GSEC Submitted 4/20/04

http://www.sans.org/reading_room/whitepapers/wireless/1405.php

ii) NIST

Tom Karygiannis, Les Owens ”Wireless Network Security 802.11, Bluetooth and Handheld Devices” Special Publication 800-48

http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

iii) USCERT

http://www.us-cert.gov/cas/tips/ST05-003.html