Wireless Network Defense

Module 10

Lab 1

Configuring Security on Wireless Router

A wireless router is a device that performs the functions of a router and also includes the functions of a wireless access point.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Organizations are allowing wireless devices to connect to their network in today's environment (BYOD). However, security of the network infrastructure is a major challenge for organizations while adopting wireless devices. A wireless router/access point is the main entry for attackers. Attackers compromise the wireless access points to gain access to the organization's network. Organizations should ensure that their wireless access points are configured securely. As a network administrator, you should able to configure the wireless router securely by applying all the possible hardening techniques.

Lab Objectives

The objective of this lab is to demonstrate the various hardening techniques on a wireless router.

Lab Environment

To carry out the lab, you need:

- A virtual machine running **Windows Server 2012**
- A web browser with an **Internet** connection
- Administrative privileges to run tools

Lab Duration

Time: 20 Minutes

Overview of Wireless Router Security

A wireless router is the first line of defense against attackers trying to access the organization's network. To keep the attackers away from compromising the security of wireless routers, we need to make appropriate configuration changes in order to make a router more secure

Lab Tasks

TASK 1

Configuring Linksys Router

Wireless Network routers should be secured in order to prevent access from outsiders.

1. Launch Windows Server 2012 machine
2. Browse **Linksys Wireless router** set up simulator available at http://ui.linksys.com/WRT54G/v8/8.00.0/ in your browser

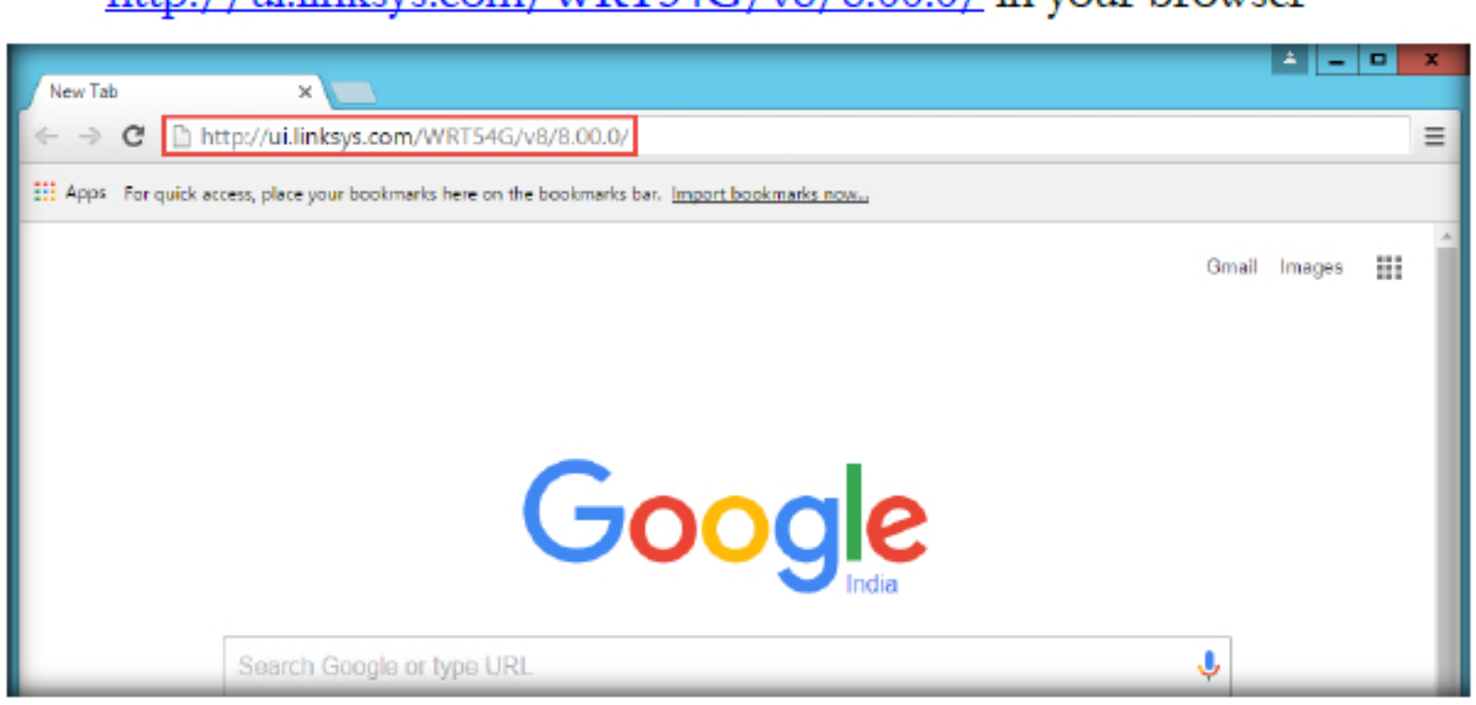


FIGURE 1.1: Browse Linksys Wireless Router

Note: Enter your router's local IP address then press **[Enter]** to actually open the Linksys wireless router interface

3. A Linksys router interface **window** will be displayed in the browser.

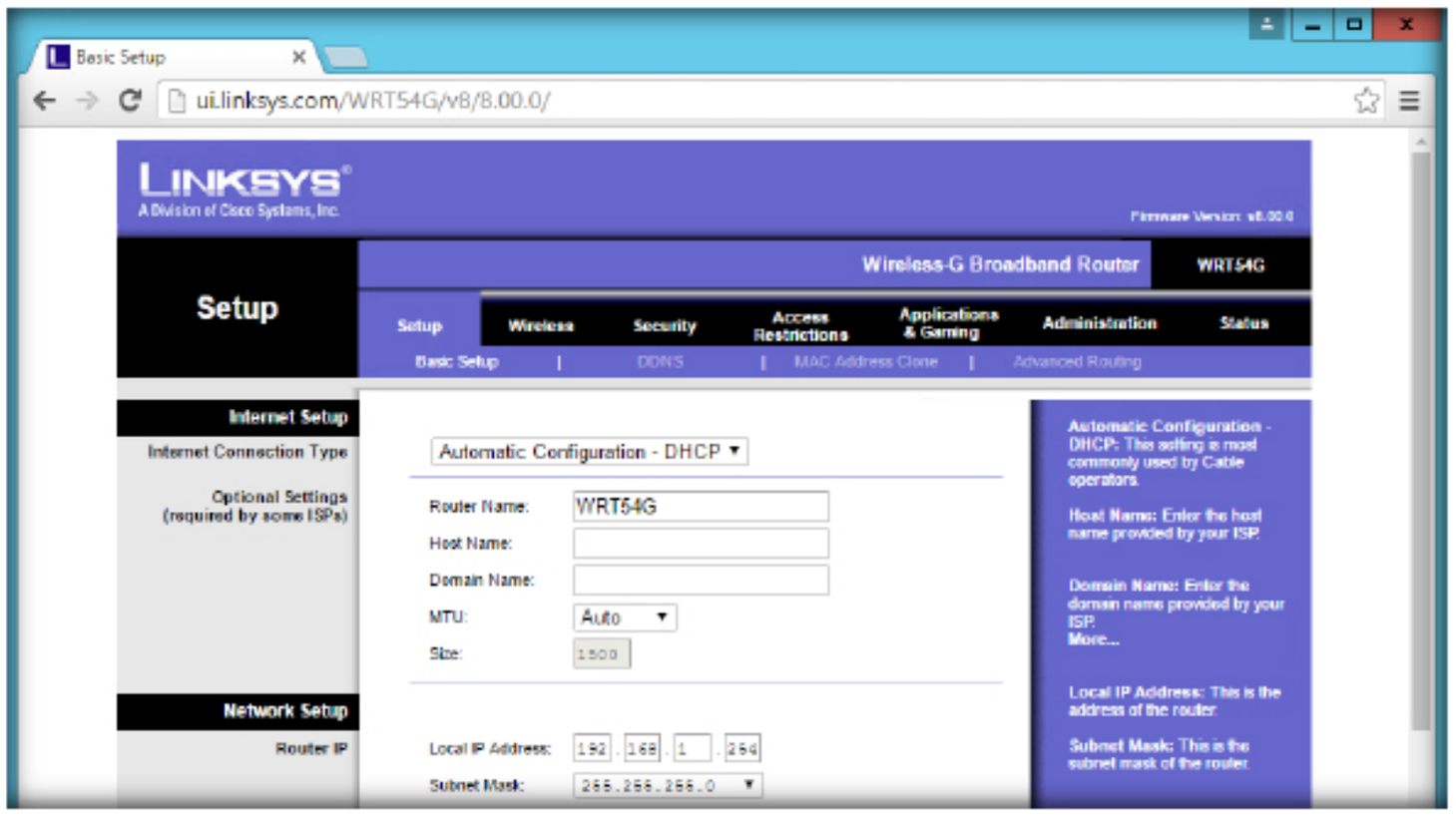


FIGURE 1.2 Linksys Wireless Router Main Window

How a router functions depends on the way it is configured.

4. Click on **Setup** tab → **Basic Setup**

FIGURE 1.3 Linksys Wireless Router Basic Setup

Basic Setup explains how a router connects to the service providers. Features differ according to the type of internet connection that you choose.

5. Choose the required **Internet Connection Type** from the drop-down

FIGURE 1.4 Linksys Wireless Router Internet Connection Type

Specifying router, domain and host names are mandatory for some ISP's

Specify a different name for the router as it will be easier to identify your router later.

6. Specify the **Router name**, **Host name** and **Domain name** in the optional settings

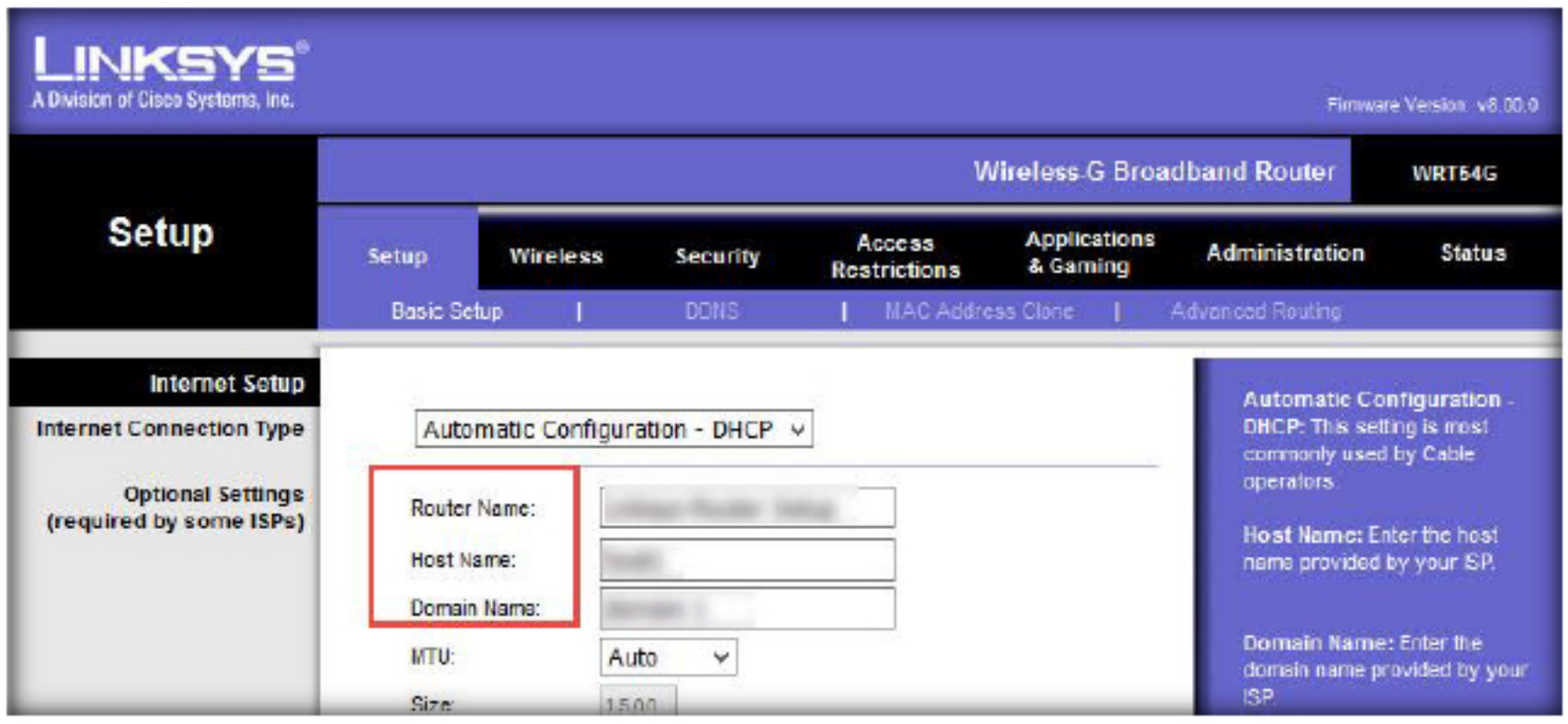


FIGURE 1.5 Optional Settings

MTU – Maximum Transmission Unit. This specifies the maximum permitted packet size for internet transmission.

7. Select **Auto** option from the drop-down for **MTU**

MTU may be specified manually. Default value is 1400. Any value within 1200 – 1500 may be specified.

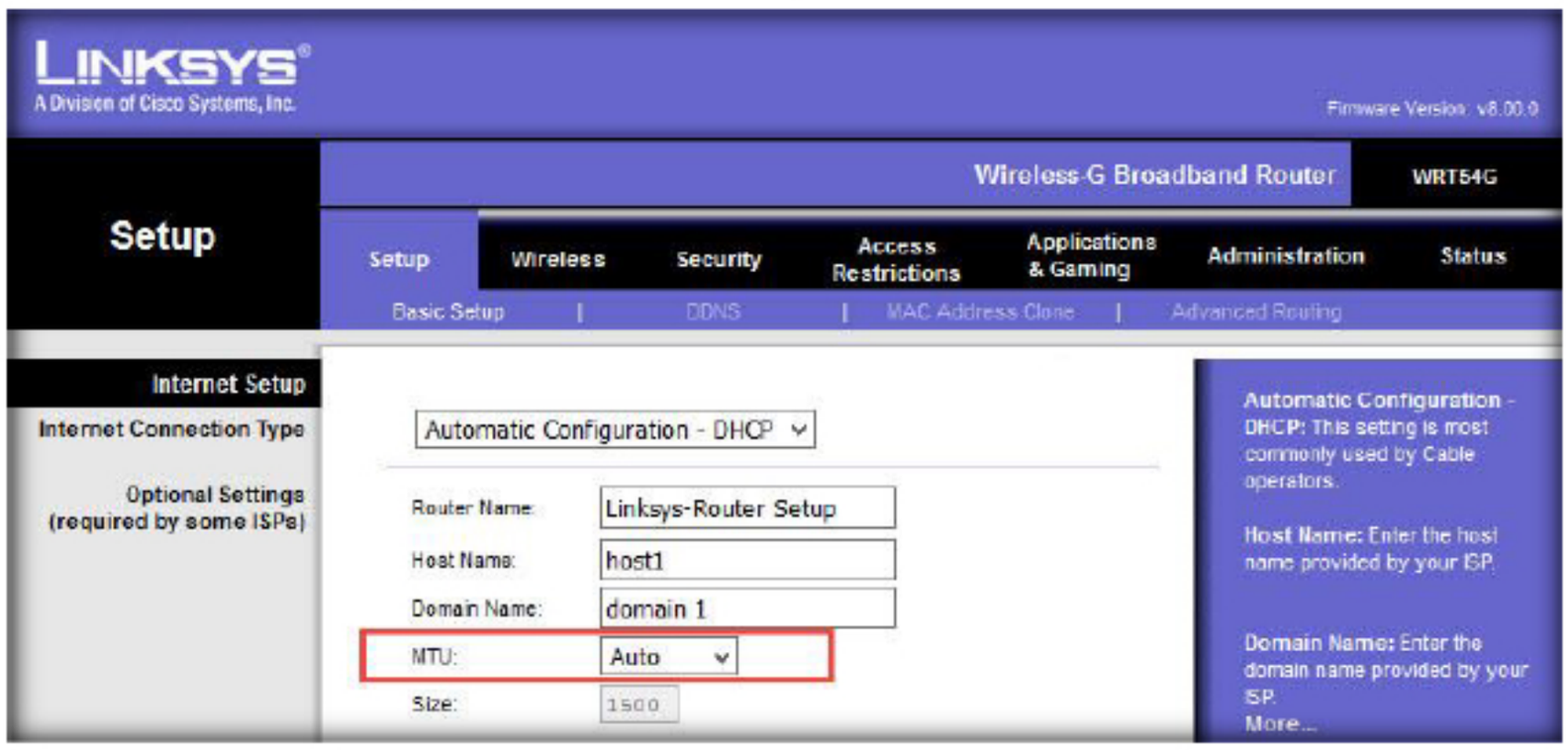


FIGURE 1.6 MTU

8. Provide the **Local IP Address** and **Subnet Mask** in the Router IP fields

IP Address refers to the router address. Default value for IP address is 192.168.1.1 and default value for subnet mask is 255.255.255.0

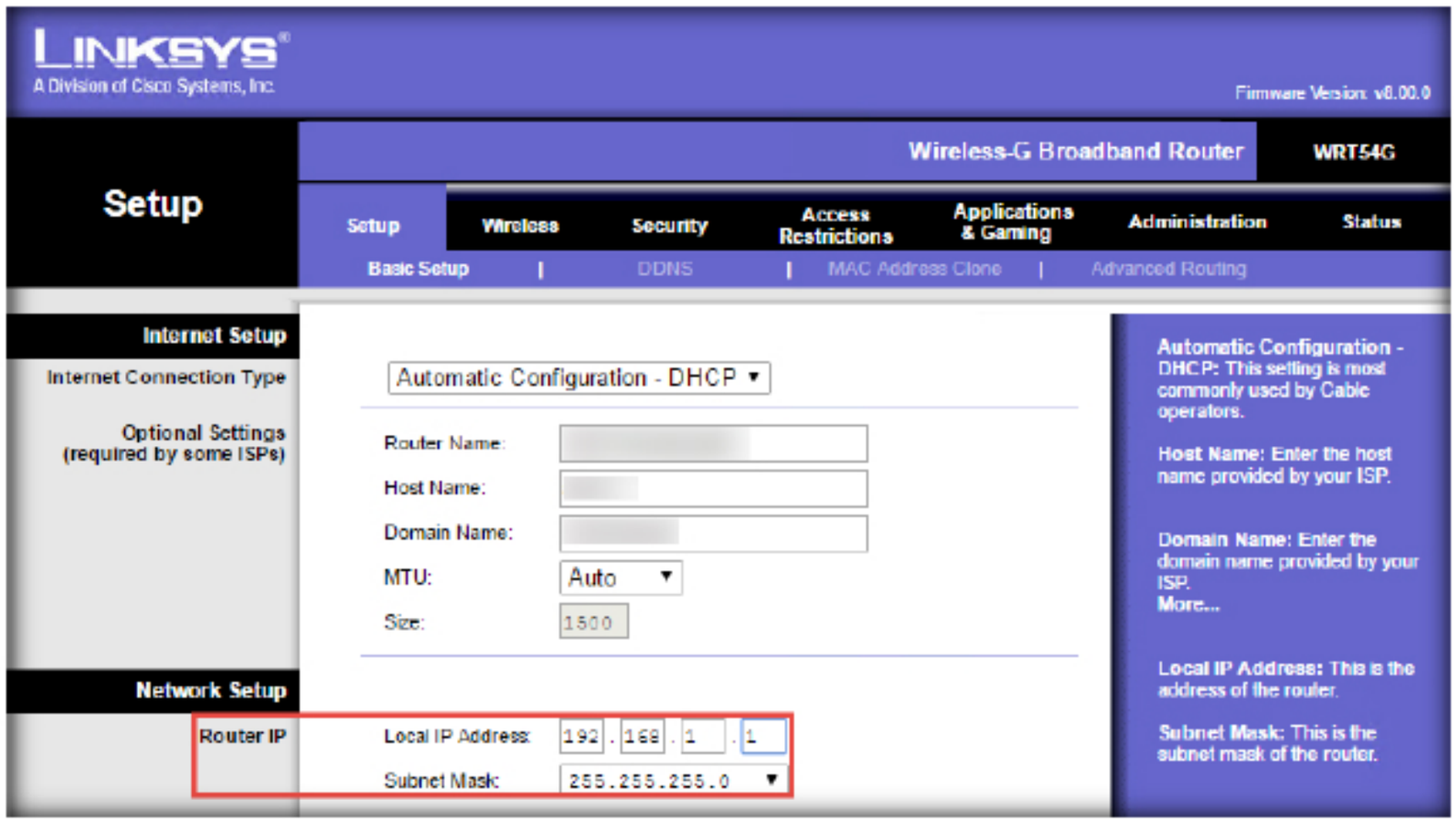


FIGURE 1.7 Network Setup

9. Choose **DHCP → Enable**

The enable option is selected in order to enable the router's DHCP server

FIGURE 1.8 Network Address Servers

10. Specify the **Starting IP address** and specify the **Maximum Number of DHCP users**

The number of DHCP users should be specified such that DHCP can assign that many IP addresses. Maximum number of DHCP users or PC's that can be connected to DHCP is 253.

An IP address is specified in order for the DHCP to connect while issuing IP addresses. Please note that the IP address should not start with 192.168.1.1, the IP address of the router

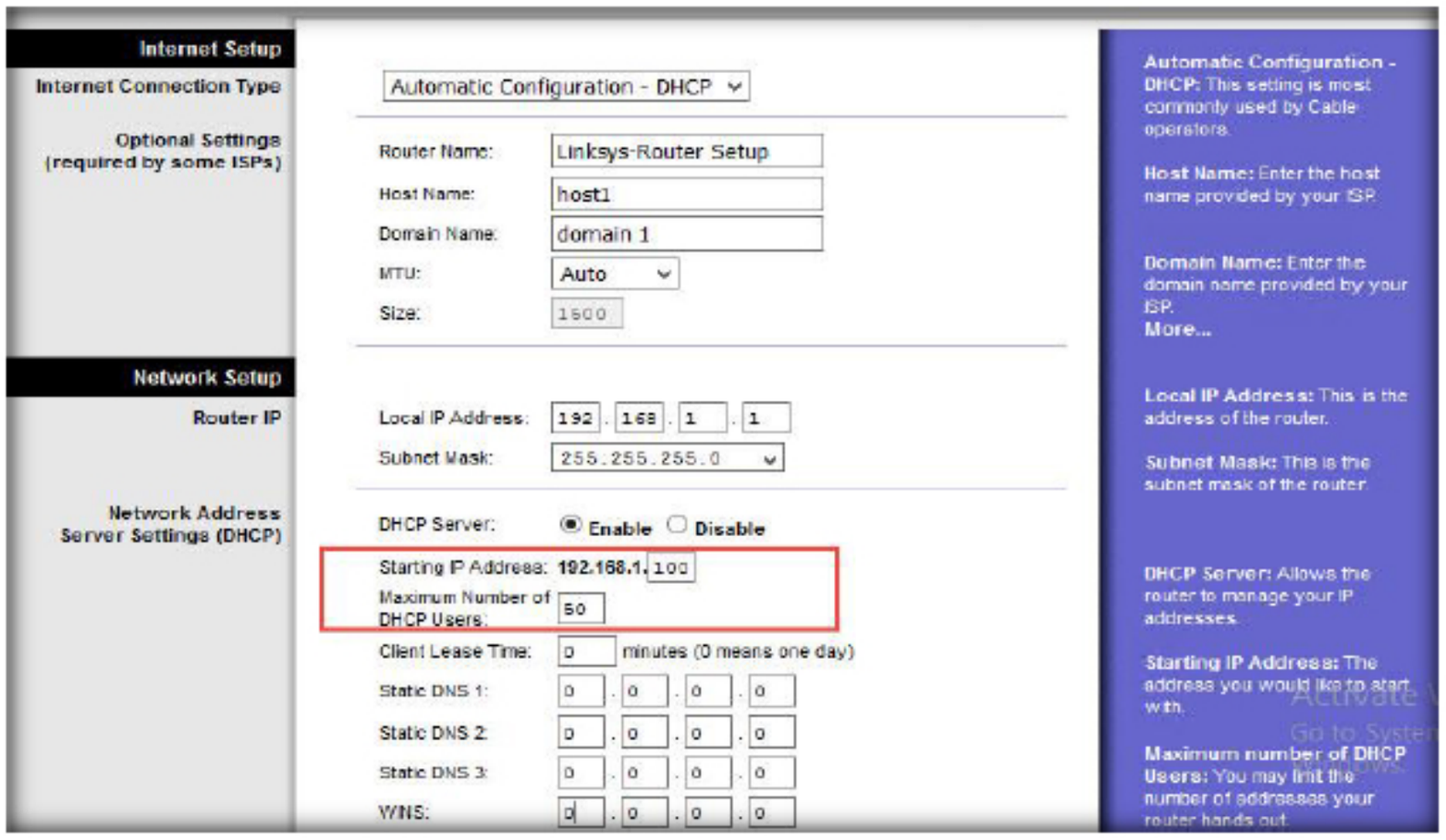


FIGURE 1.9 DHCP Settings

11. Provide the **Client Lease Time** in minutes.

The Client Lease Time refers to the amount of time a network user is connected with the DHCP server using the dynamic IP address. The time is provided in minutes.

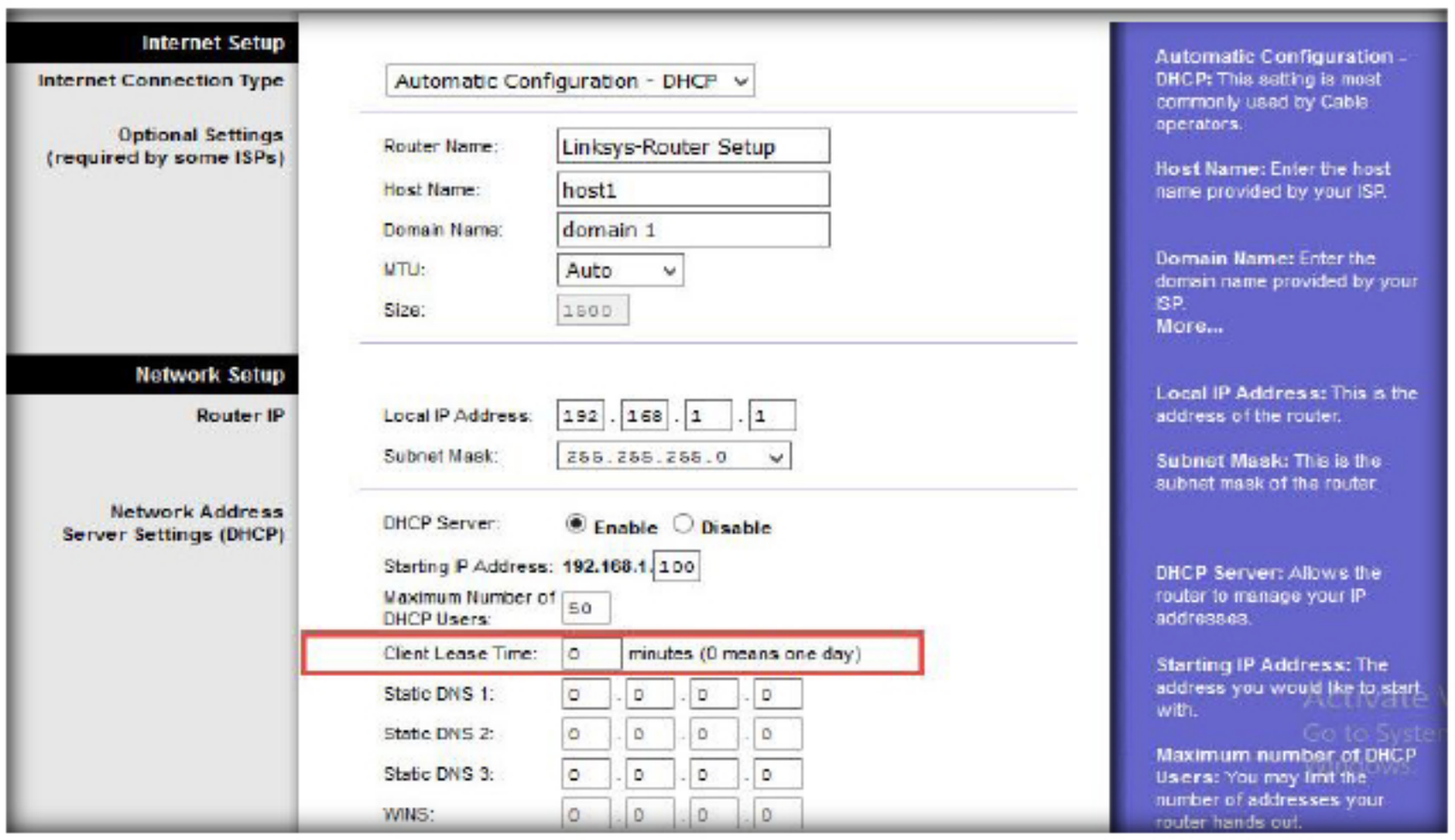


FIGURE 1.10 Client Lease Time

12. Specify any **three DNS server IP addresses** in the **Static DNS** (1-3) fields

The Domain Name System helps in translating the domain names to internet addresses or URL's. Routers will quickly access the DNS server using the provided IP addresses

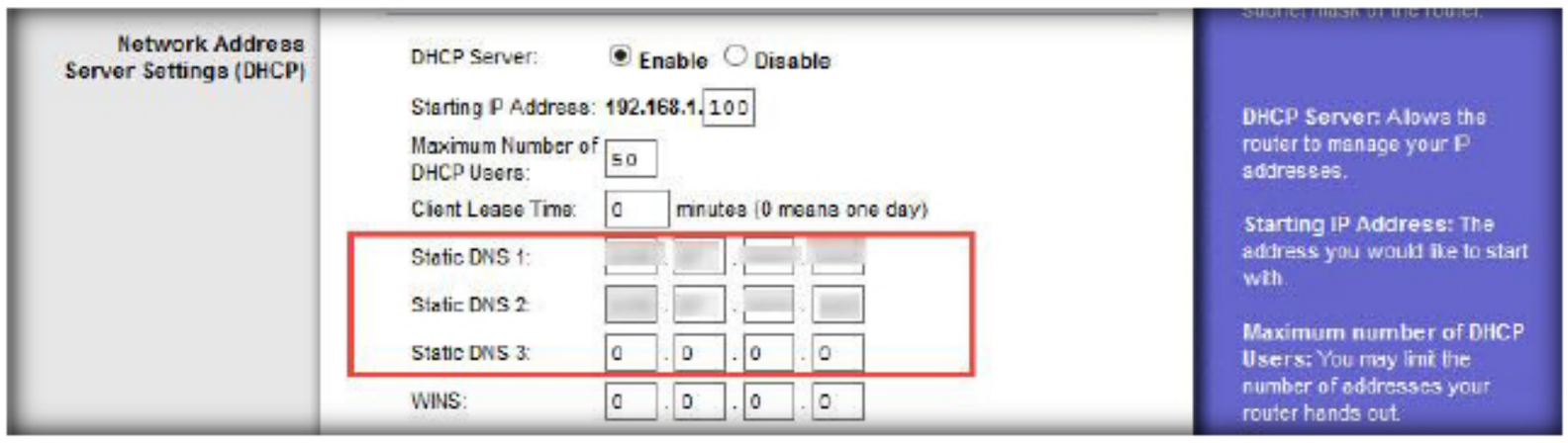


FIGURE 1.11 DNS Server IP Addresses

13. Enter the **WINS** server IP address if you use a WINS server

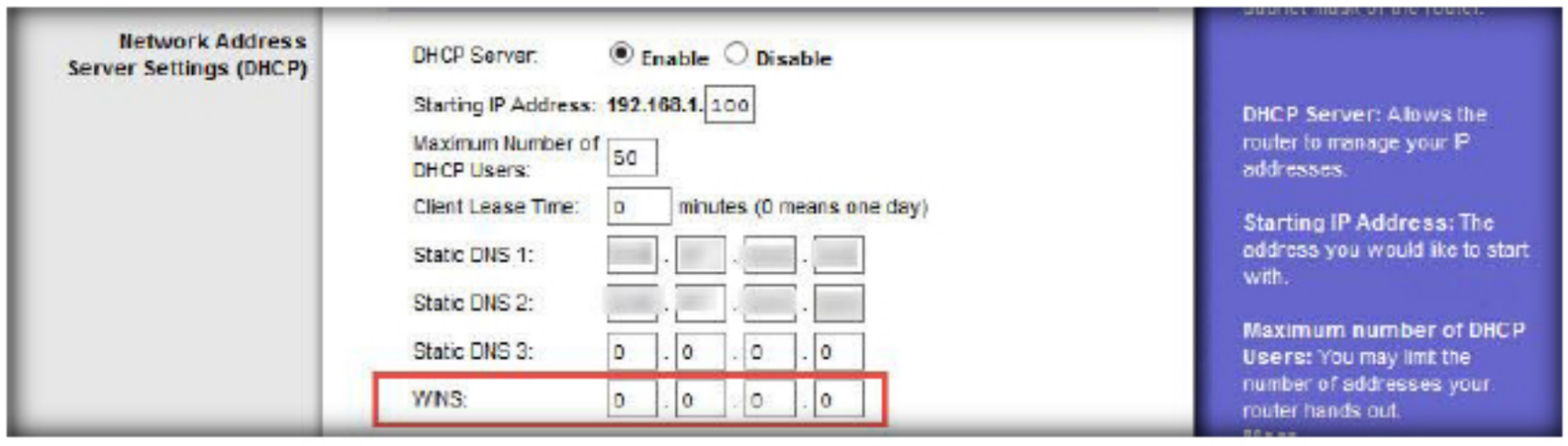


FIGURE 1.12 WINS

14. Click the **Save Settings** button in order to save all the changes

WINS – Windows Internet Naming Service. This manages the PC's interaction with the internet. Specify the IP address of the WINS server if using. Else, leave the field blank.

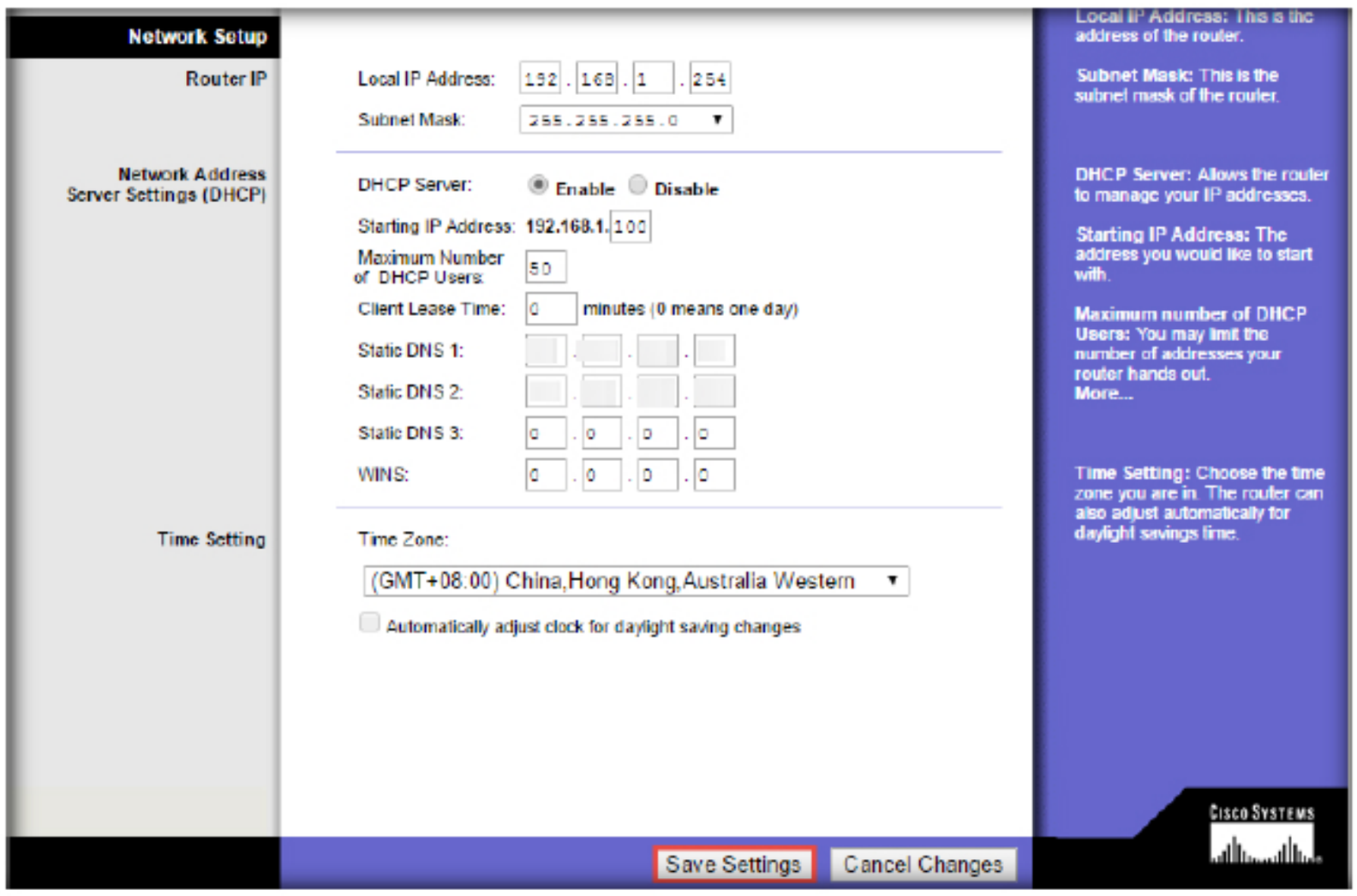


FIGURE 1.13 save Settings

15. A prompt saying **Settings are Successful** is displayed, click **Continue**

DDNS helps in accessing domain names instead of IP addresses.

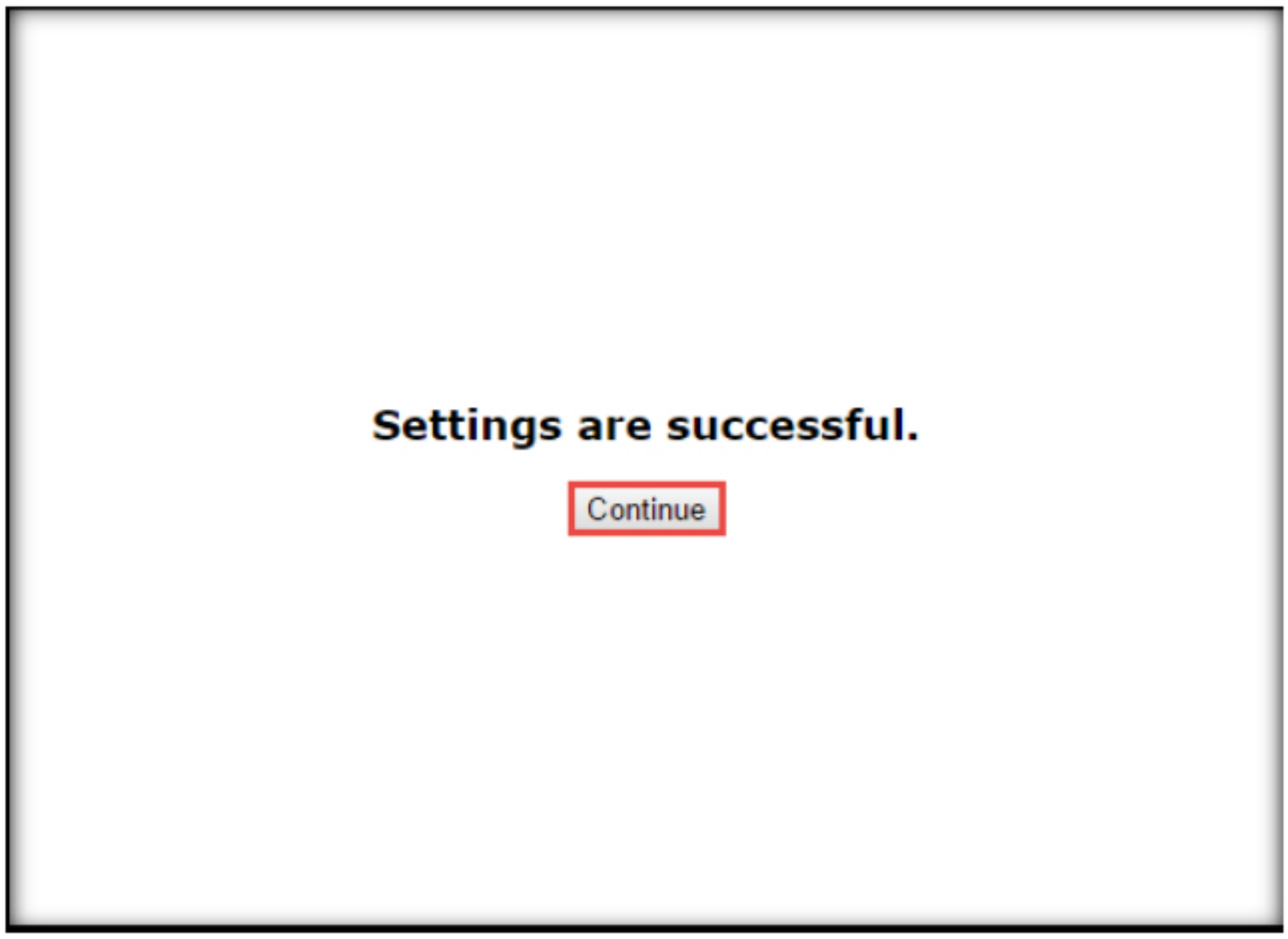


FIGURE 1.14 Settings are Successful

16. Next, click on the **DDNS** tab present near to **Basic Setup**

Routers may be configured by updating the DNS settings using DynDNS.org or TZO.org

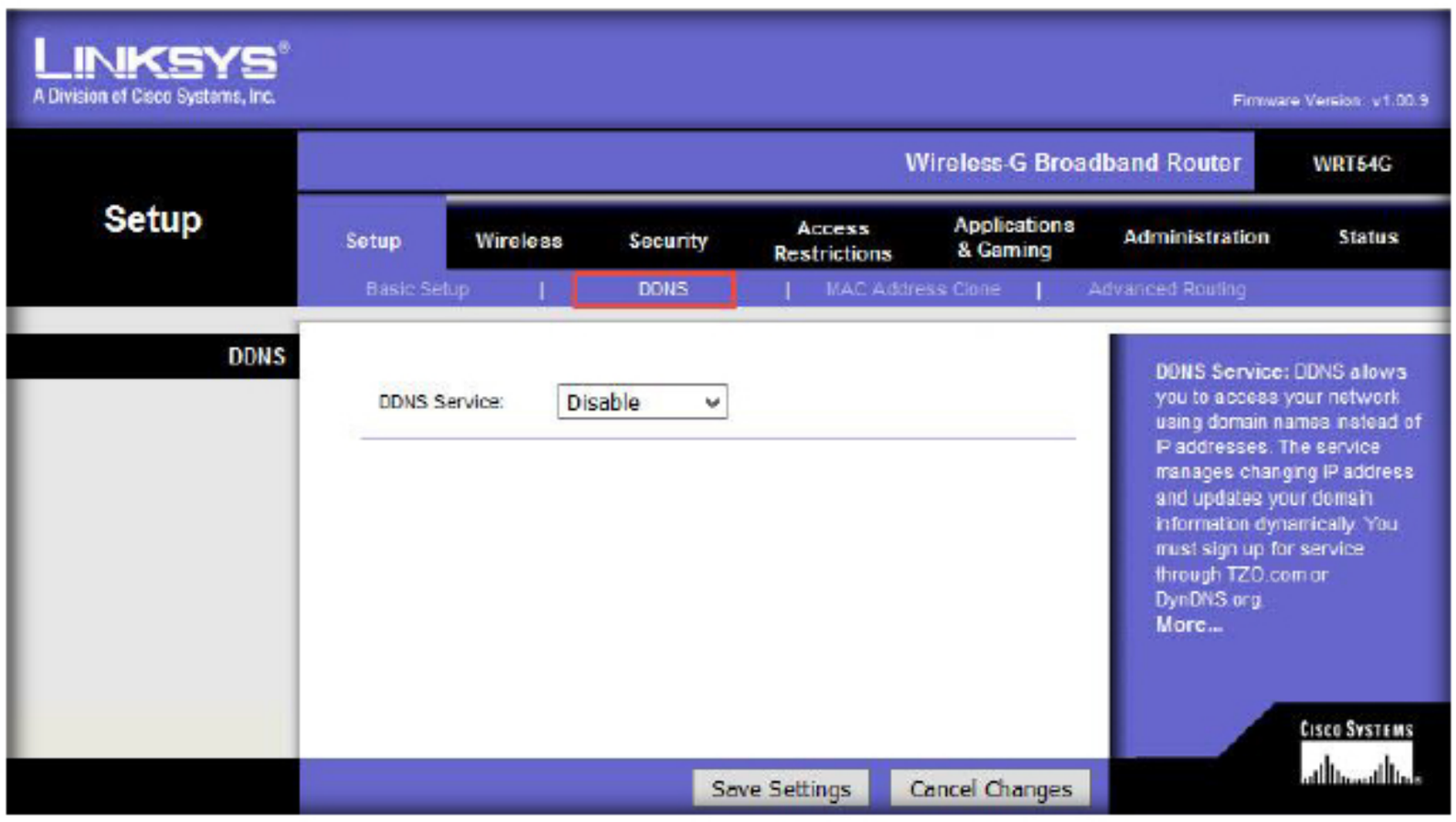


FIGURE 1.15 DDNS

17. Select the **DDNS Service → Disable** from the drop-down

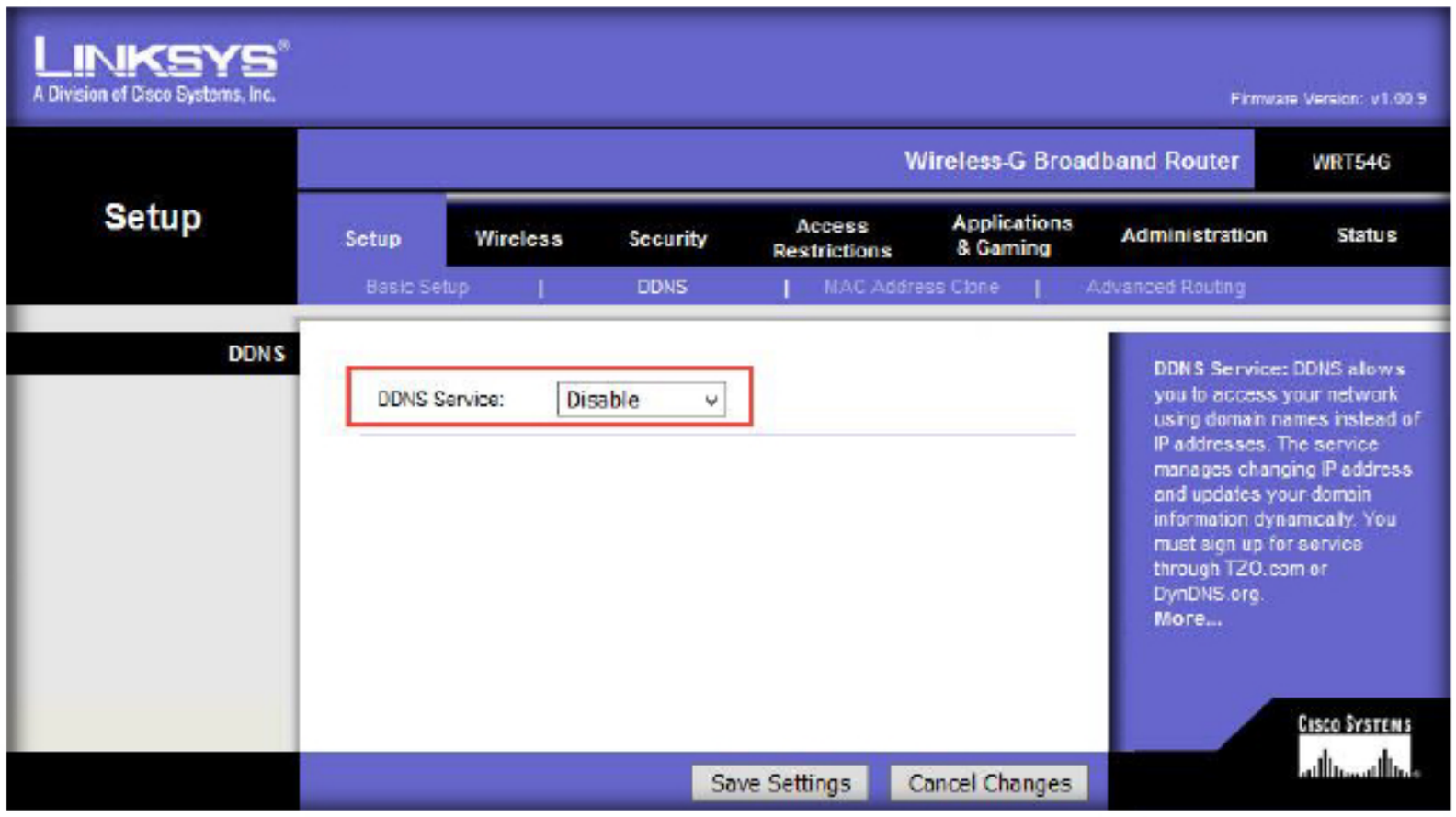


FIGURE 1.16 Disable DDNS

18. Click on the **Save Settings** button.

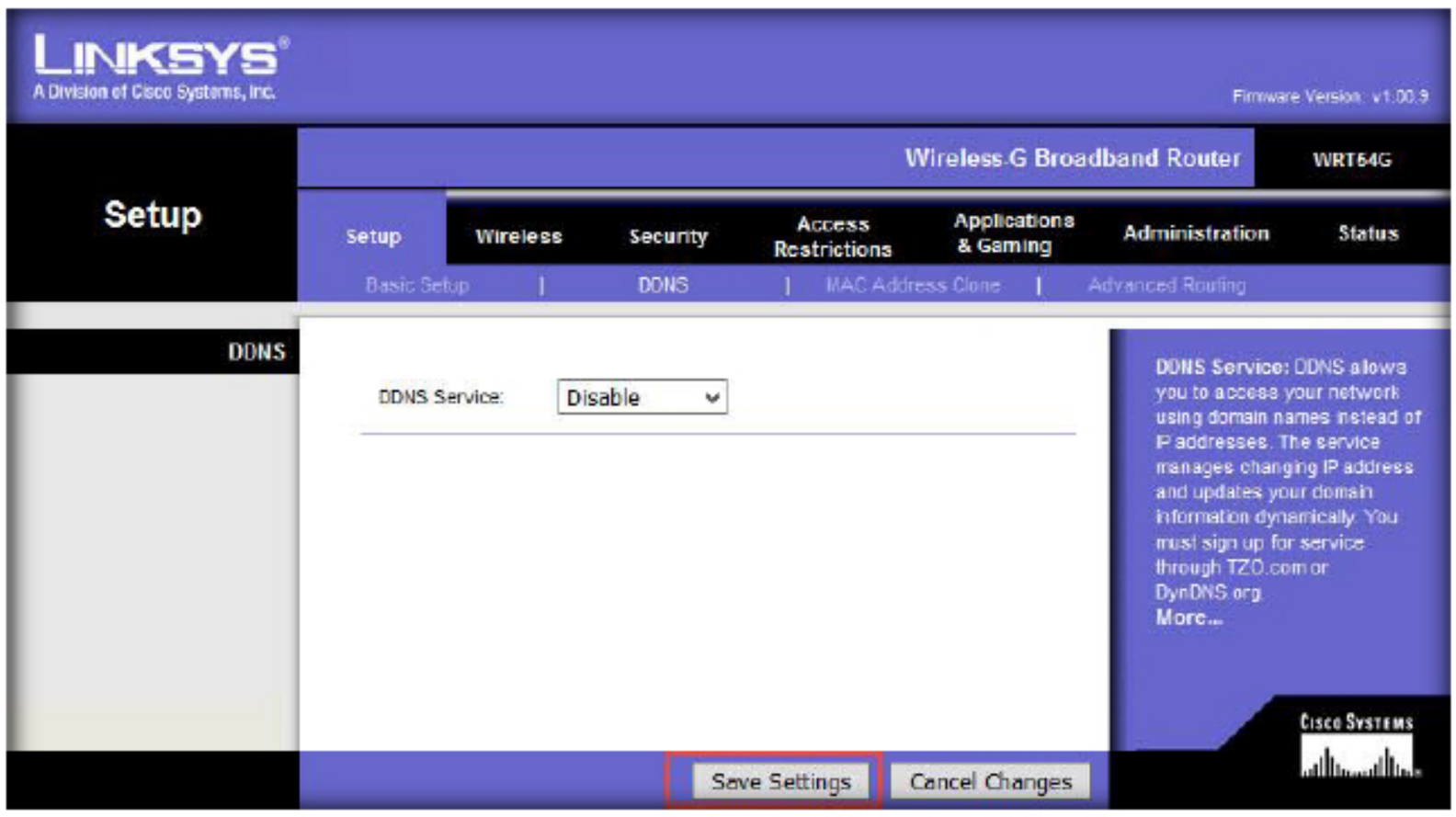
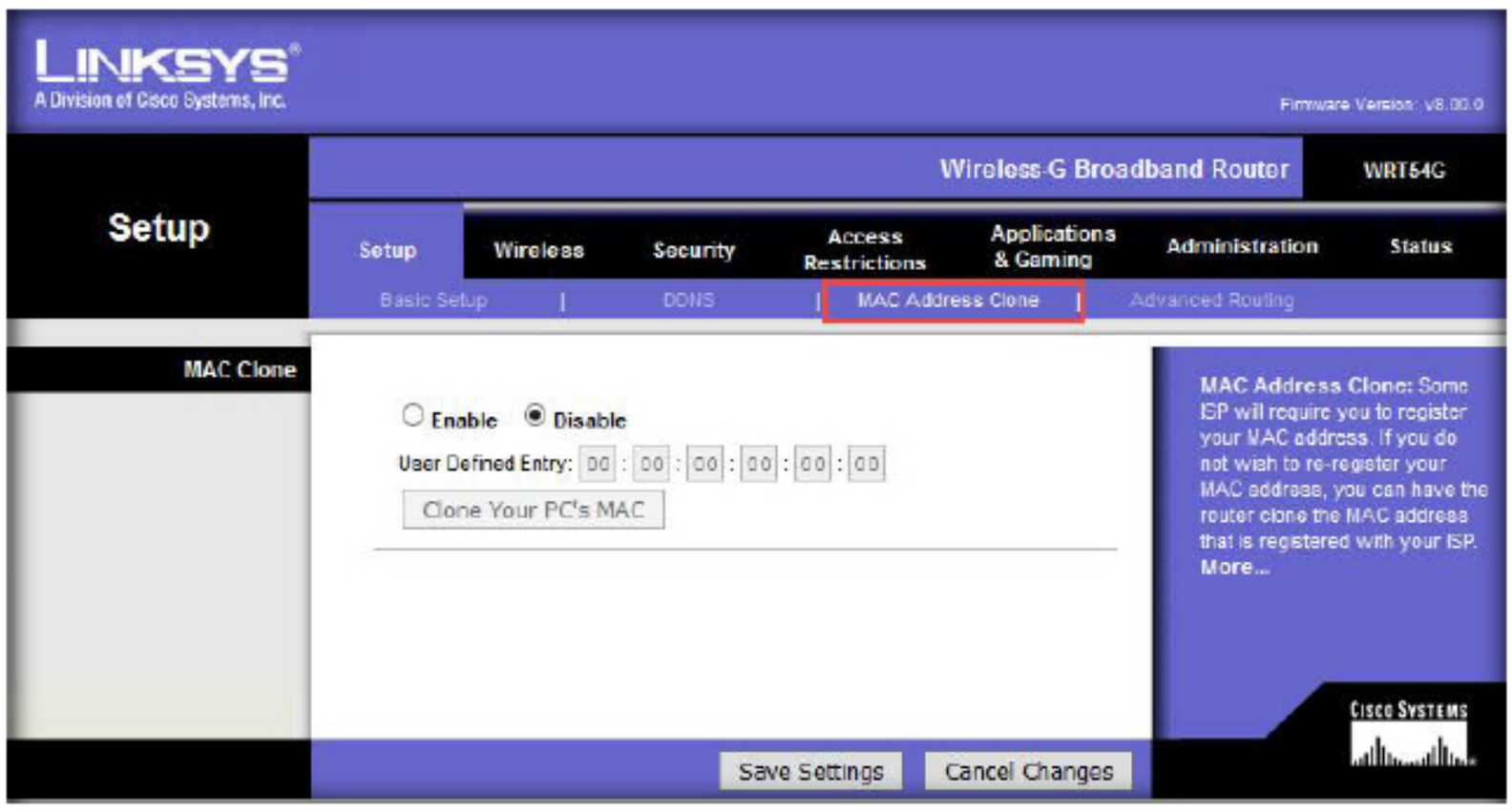


FIGURE 1.17 save Settings

19. A prompt **Settings are Successful** is displayed

FIGURE 1.18 Settings are Successful

20. Now, click **MAC Address Clone**



MAC Address clone helps you in adding any specific IP address.

FIGURE 1.19 MAC Address Clone

21. Choose **Disable → Mac Clone**

Operational Mode has two options: Gateway and Router.

Gateway is selected when the router hosts the network connection to the internet.

Router is selected if the router exists with other routers in the network

FIGURE 1.20 Disable MAC Clone

22. Now, click **Advanced Routing**

Router operational mode provides another option Dynamic Routing.

FIGURE 1.21 Advanced Routing

23. Select the **Operating Mode** from the drop-down

Dynamic Routing uses RIP protocol. RIP: Router Information Protocol, which provides the maximum number of efficient paths available between the source and the destination.

RIP has four options: Disable

- WAN
- LAN and Wireless
- Both

WAN is selected in order to enable dynamic routing.

LAN is enabled for LAN and Wireless side

If dynamic routing is required for LAN and WAN, select both.

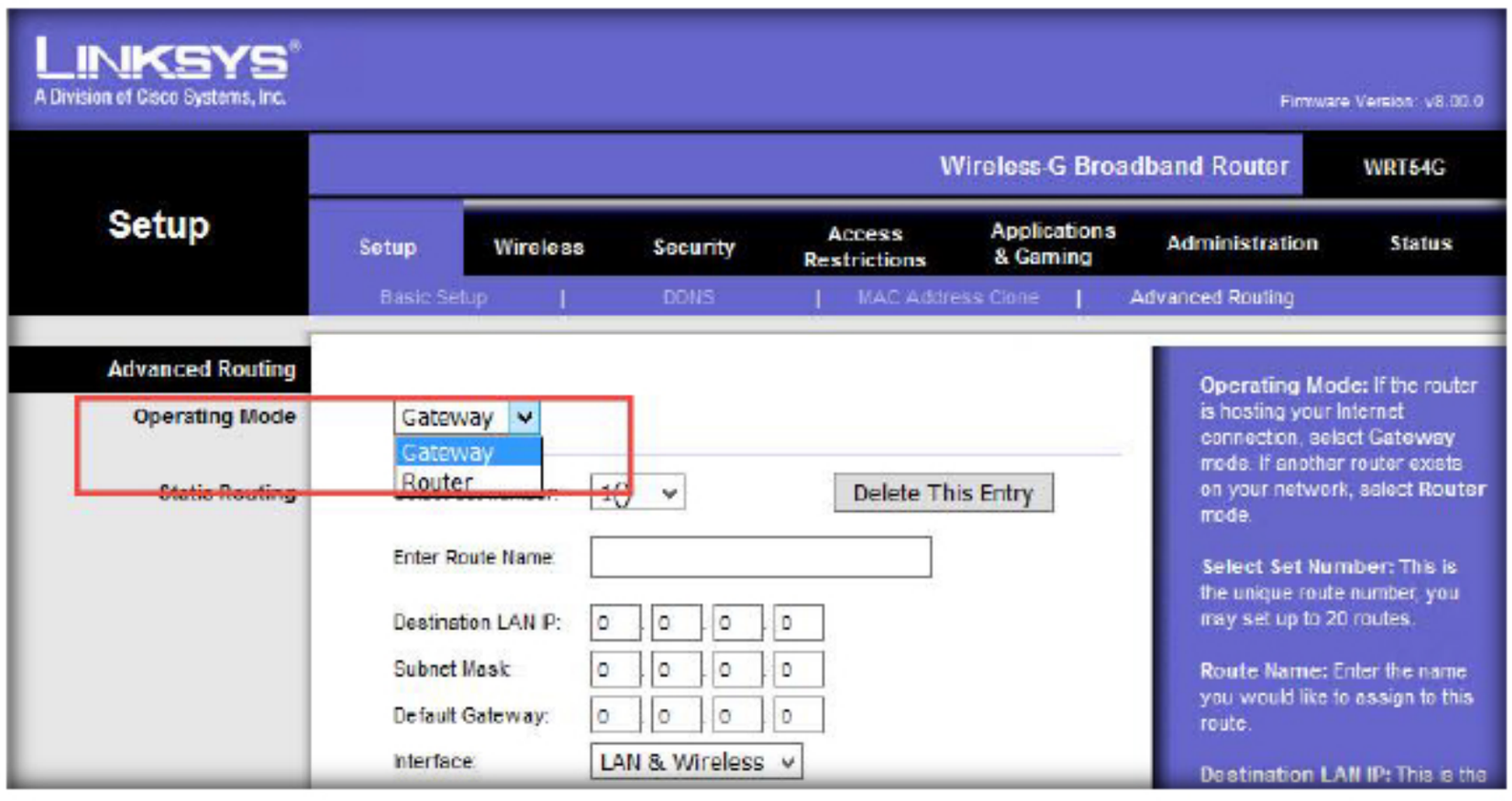


FIGURE 1.22 Operating Mode

24. Select a number from the **static routing** drop-down list

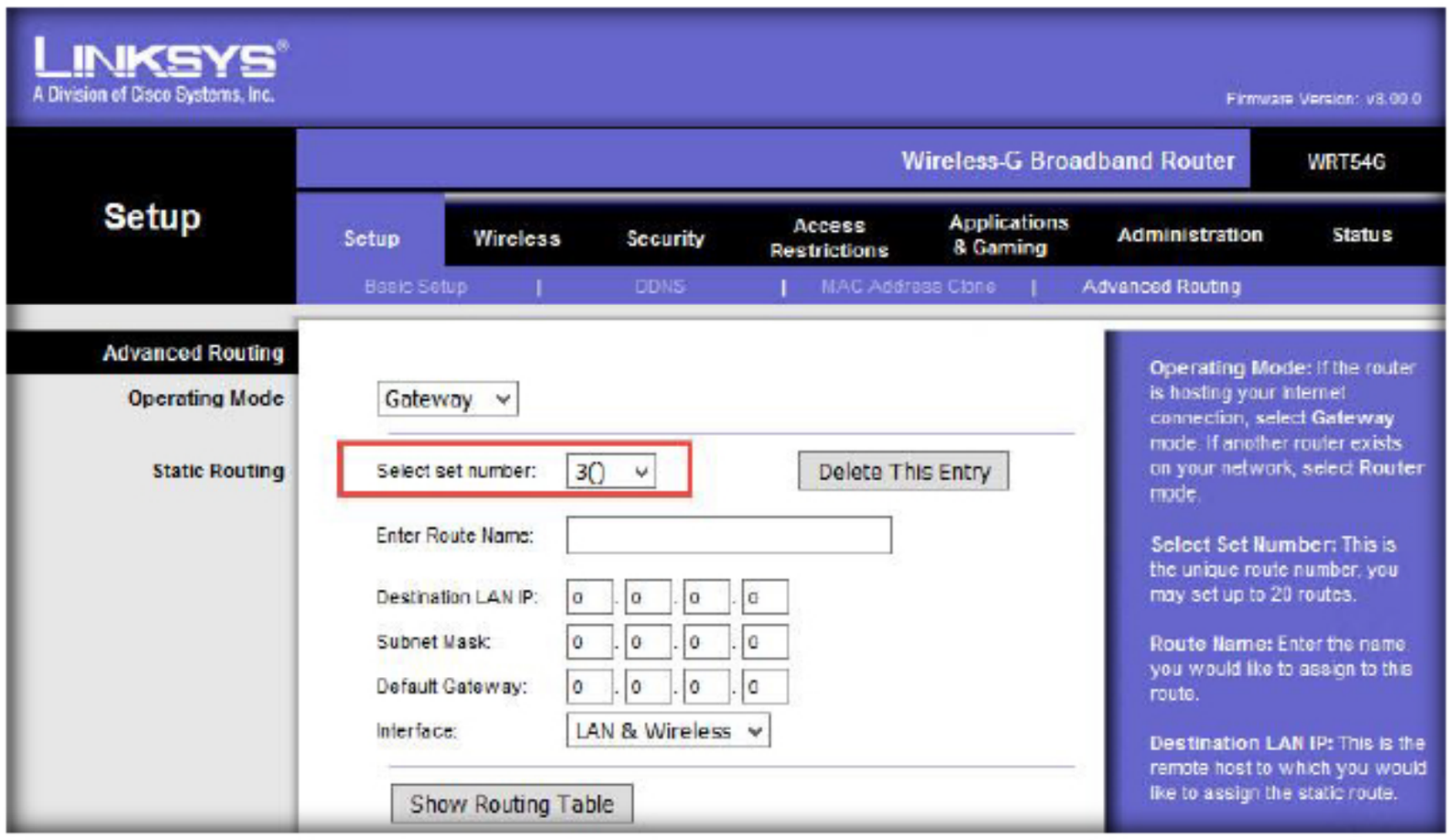


FIGURE 1.23 Static Routing

25. Next, enter the following details:
    - **Router Name**
    - **Destination LAN IP**
    - **Subnet Mask**
    - **Gateway**

The Static number denotes the number of pathways taken in order to reach the network information to a particular host.

The Destination IP Address: IP address of the host or the network to which the static route is connected

The Subnet Mask: Determines the network portion and host portion of the IP Address

The Gateway: Allows the connection between the router and the host

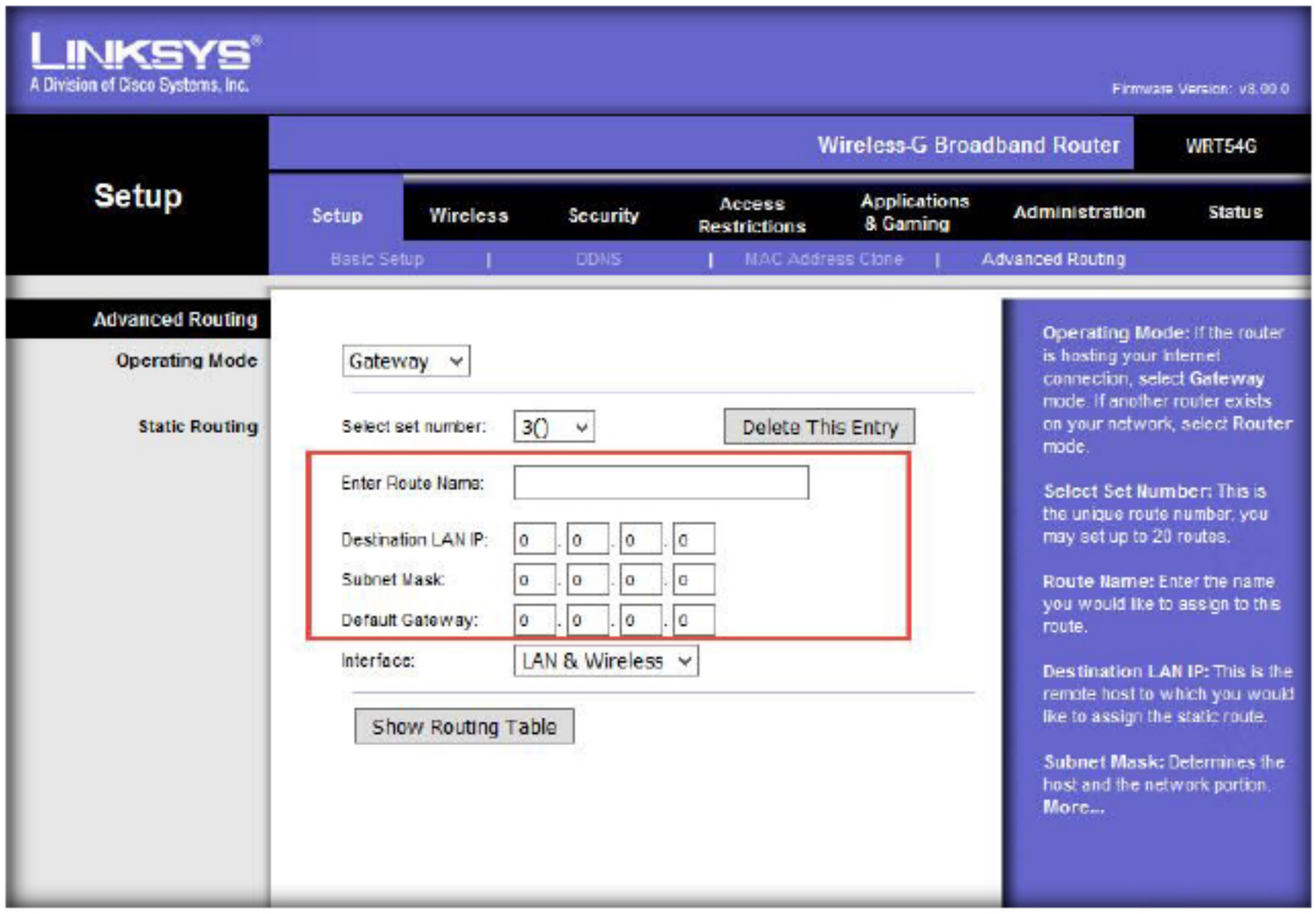


FIGURE 1.24 Static Routing

26. Now, Select an **Interface** from the drop-down

The Interface defines whether the network is on the LAN or the internet

Selection of LAN & Wireless and Internet for interface drop-down depends on the location of the IP address. If it is connected to a LAN, select LAN or else internet.

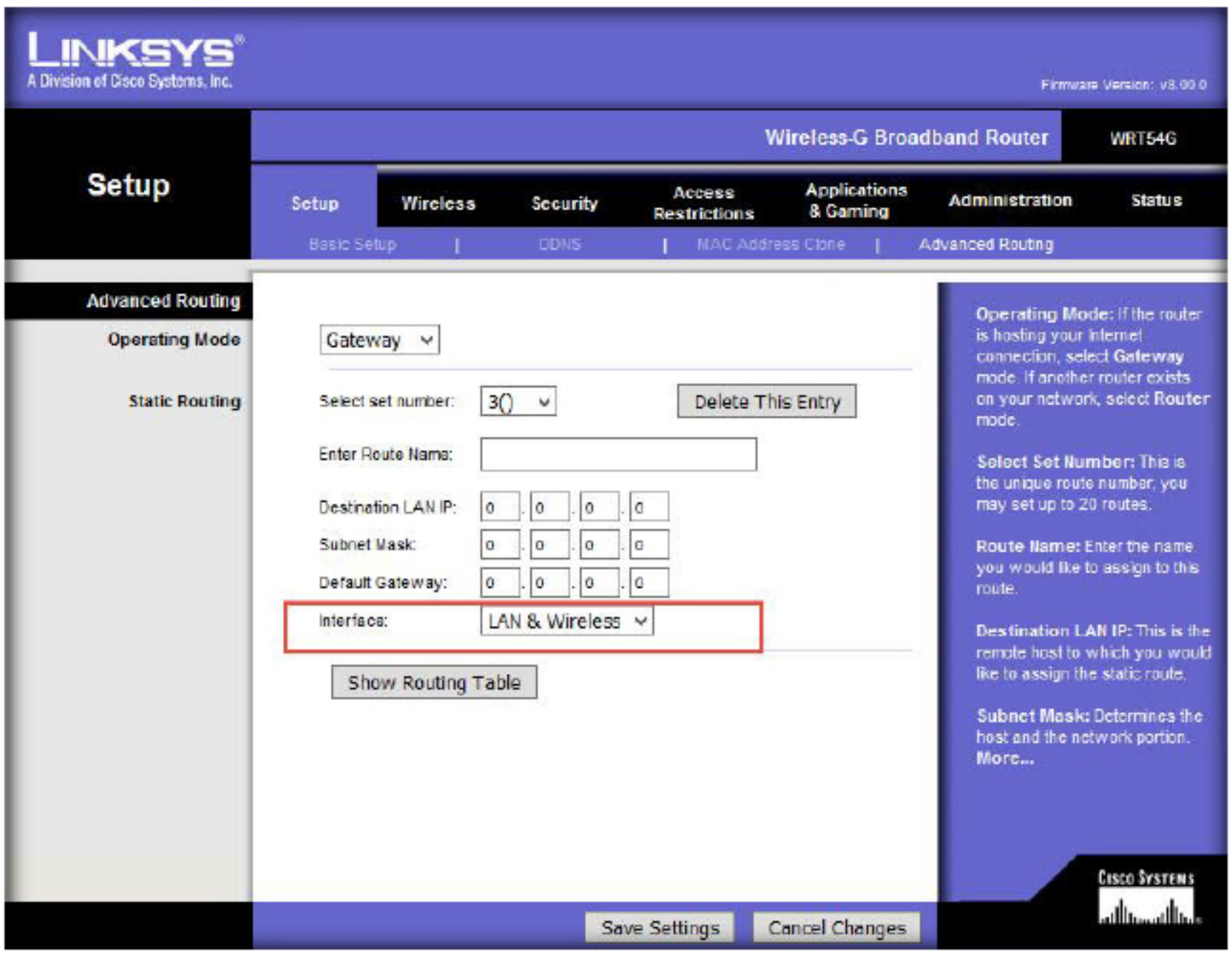


FIGURE 1.25 Interface

27. Click **Save Settings**

Delete This Entry deletes the entered IP address

Show Routing Table provides the current routing table

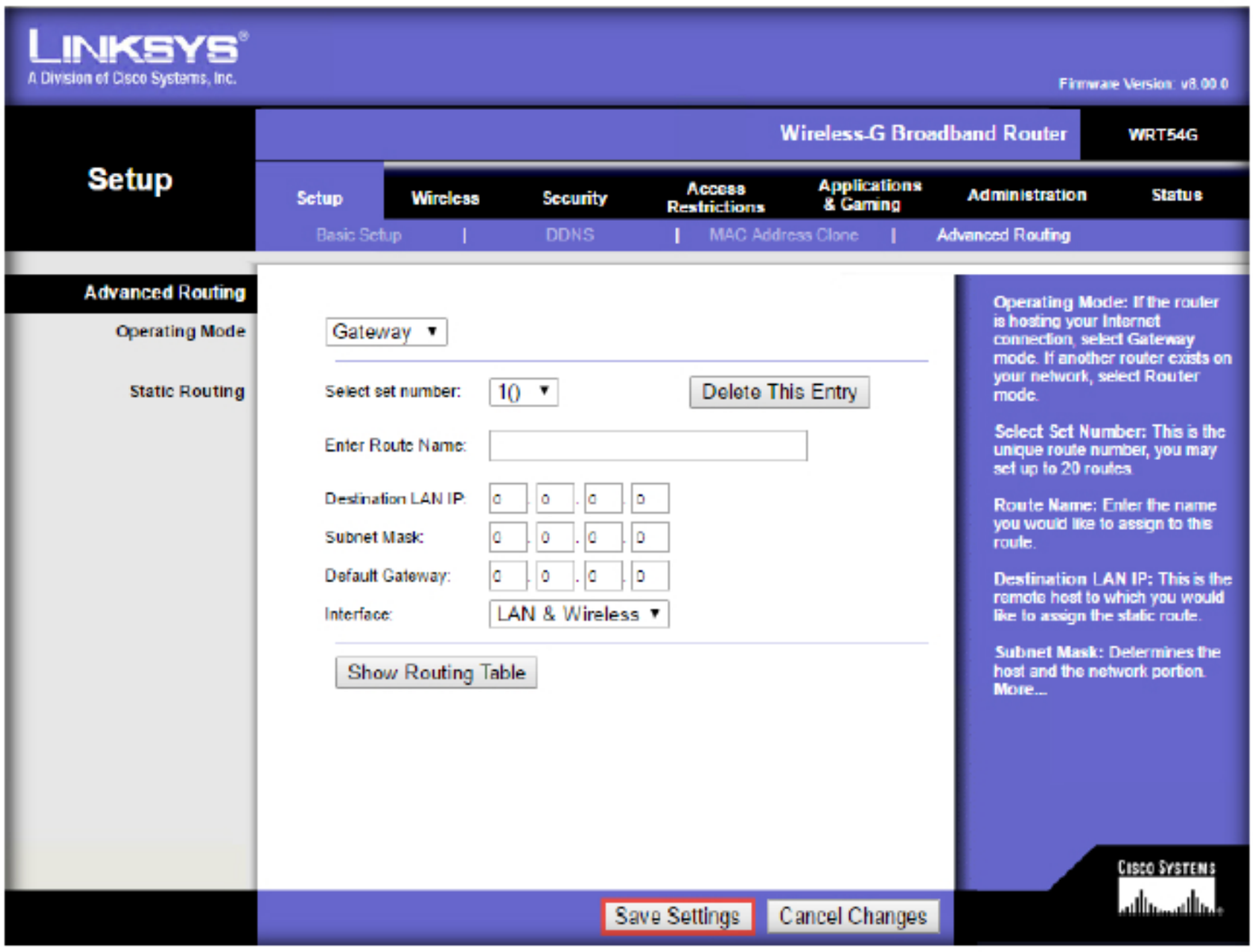


FIGURE 1.26 save Settings

28. A prompt saying **Settings are Successful** pops up. Click **Continue**

FIGURE 1.27 Settings are Successful

29. Click on the **Wireless** tab in the menu bar

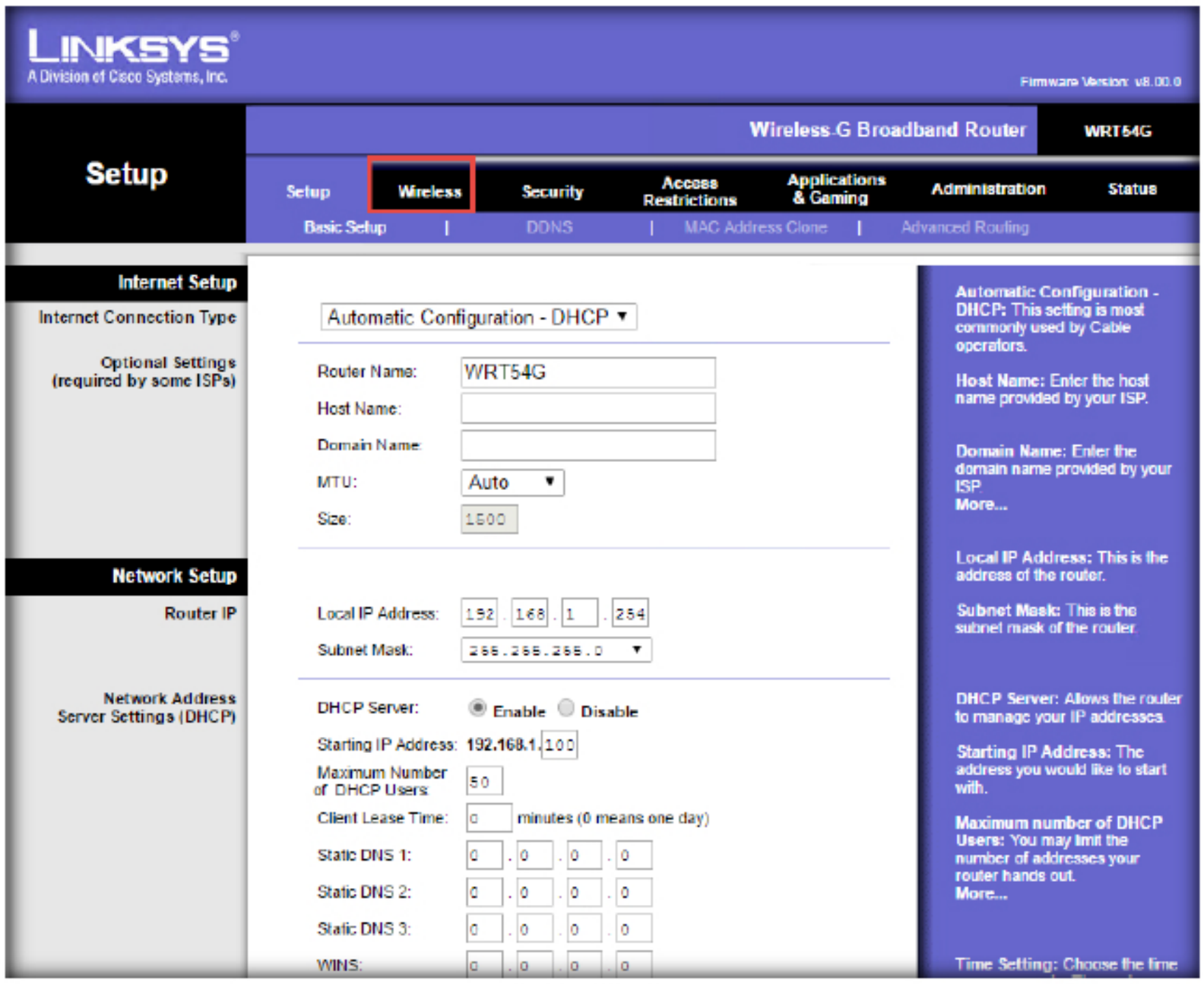


FIGURE 1.28 Wireless tab

30. Click the "Basic Wireless Settings" tab

There are four modes for Wireless Network Mode:

- Disabled: No wireless operation possible
- Mixed: Allows 802.11B and 802.11G wireless equipment
- B - Only: Allow only 802.11B wireless equipment
- G – Only: Allow only 802.11G wireless equipment

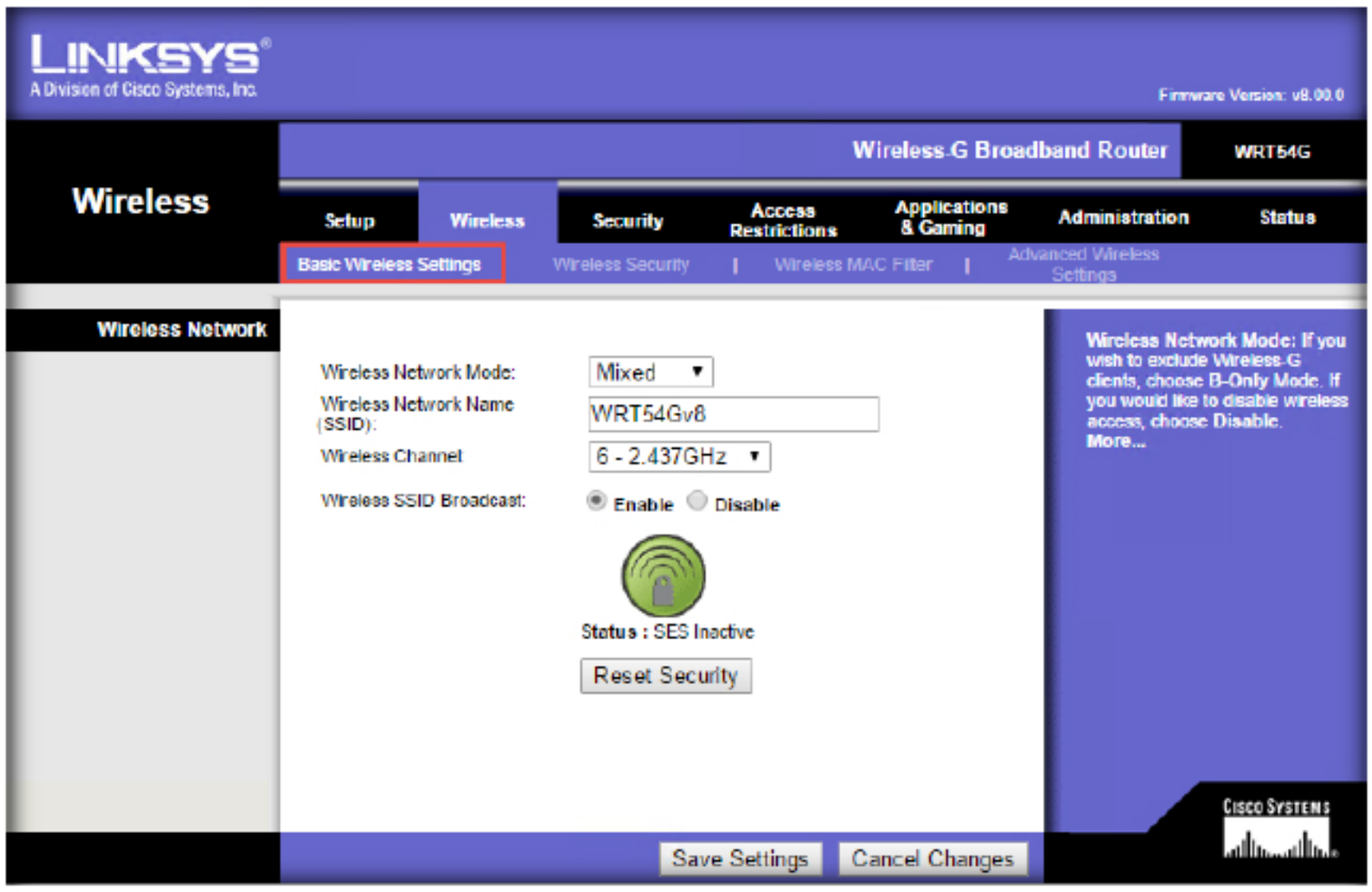


FIGURE 1.29 Basic Wireless Settings

31. Choose the radio button for the option **Wireless SSID Broadcast → Disable**

Wireless Network Name (SSID) represents the name of the wireless router

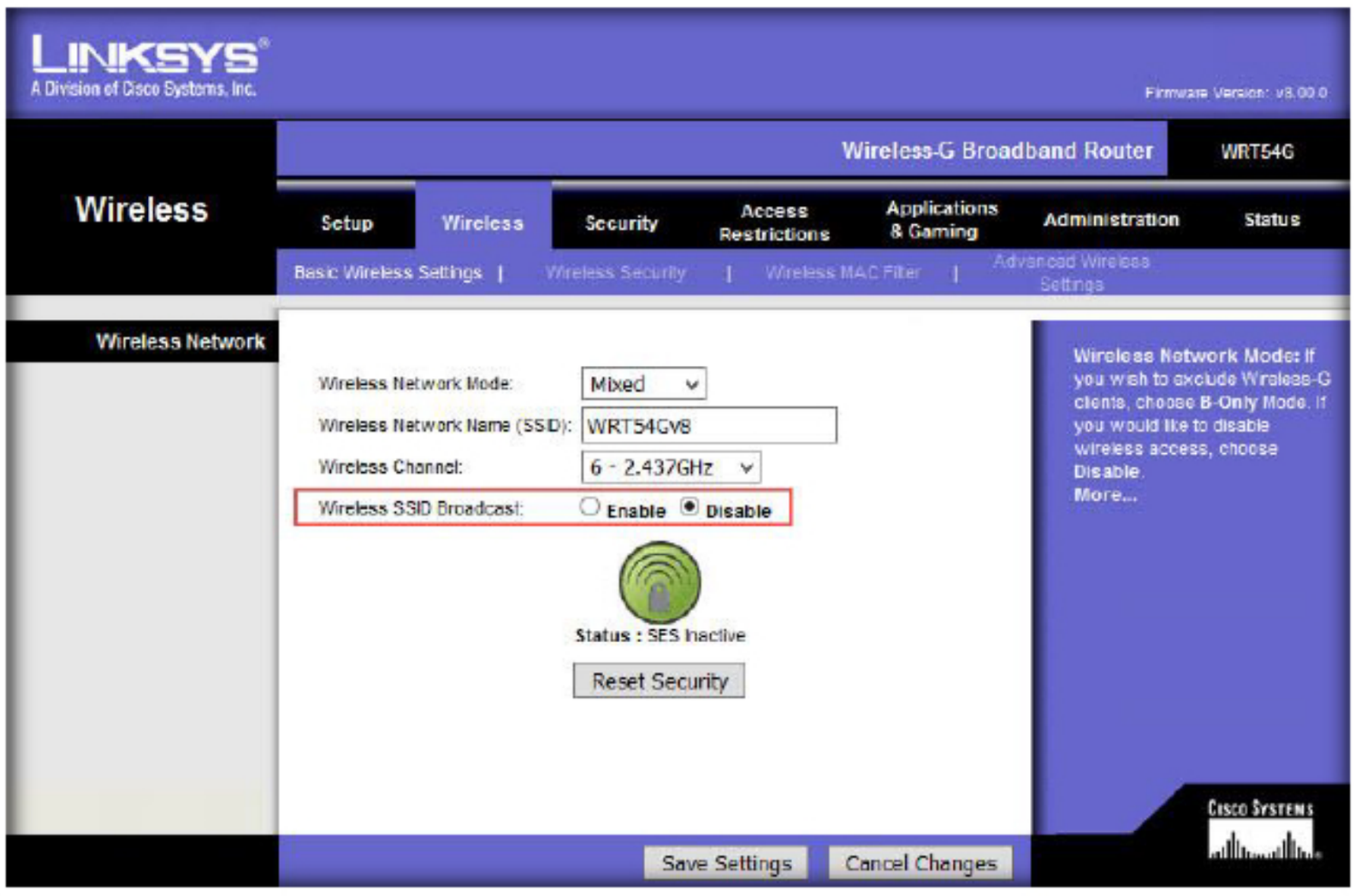


FIGURE 1.30 Disabling Wireless SSID Broadcast

32. Click on the **Wireless Security** tab next to the **Basic Wireless Settings** tab

Disabling the SSID broadcast makes it impossible for other people to recognize your network while searching for a wireless network

FIGURE 1.31 Wireless Security

33. Select appropriate strongest **encryption mode**

Note: Here, use of WPA2 is considered the strongest encryption mode for wireless security from the Security Mode drop-down

WPA Personal: Commonly used in personal or home networks

WPA Enterprise: Used for wireless networks in business environments. More complicated and provides personal and centralized control over the Wi-Fi connection

WPA2 Personal: Commonly used for home and small business units

WPA2 is more secure than WEP.

WPA2 Enterprise: They require RADIUS authentication server. Requires a username and a password for authentication

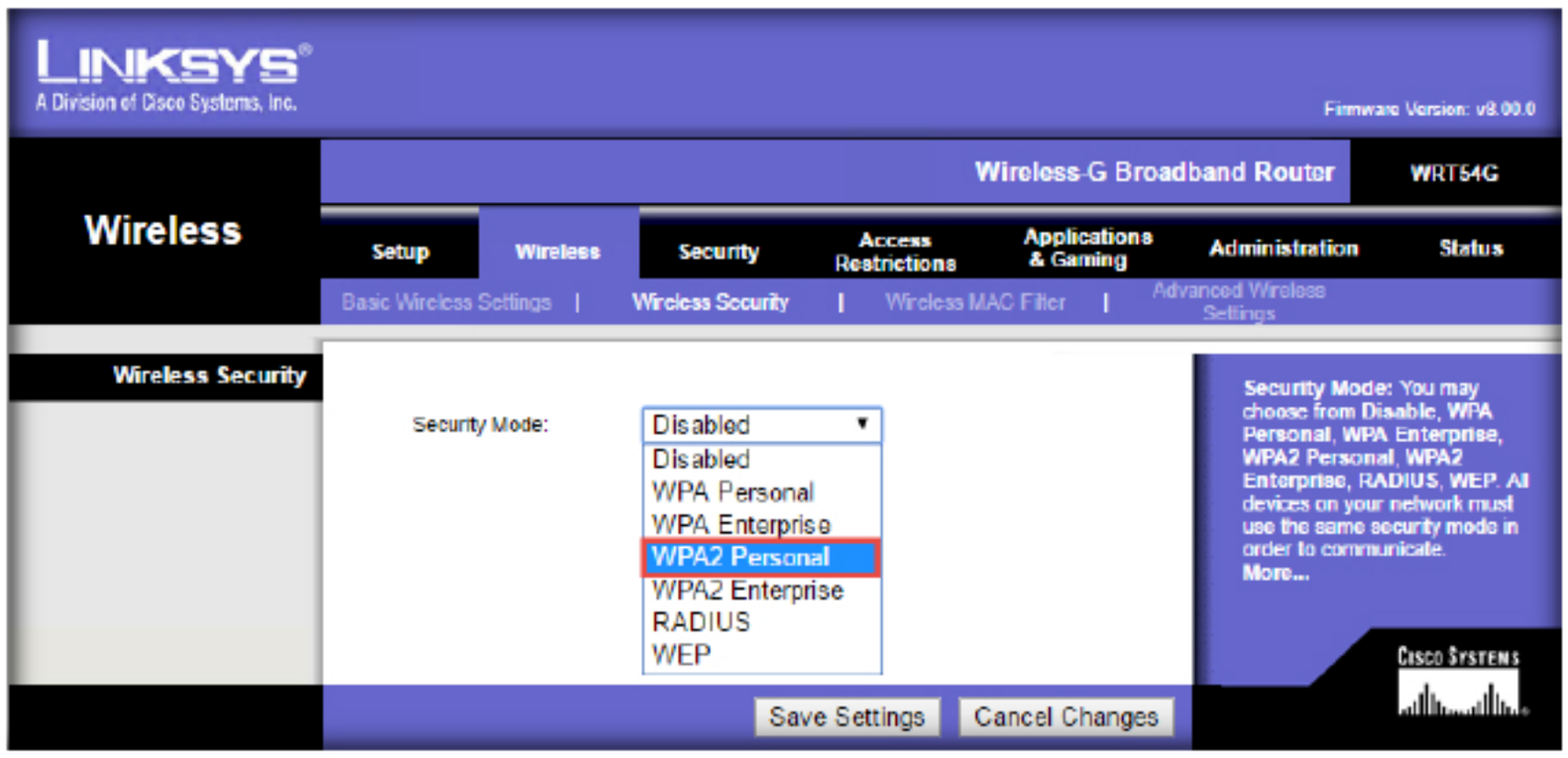


FIGURE 1.32 Select security mode

34. Select **AES** for the **WPA algorithm** and enter a valid key value for the **WPA shared key** field

AES: Stands for Advanced Encryption Standard. More secure encryption method used by WPA2 standard. Provides optimal security

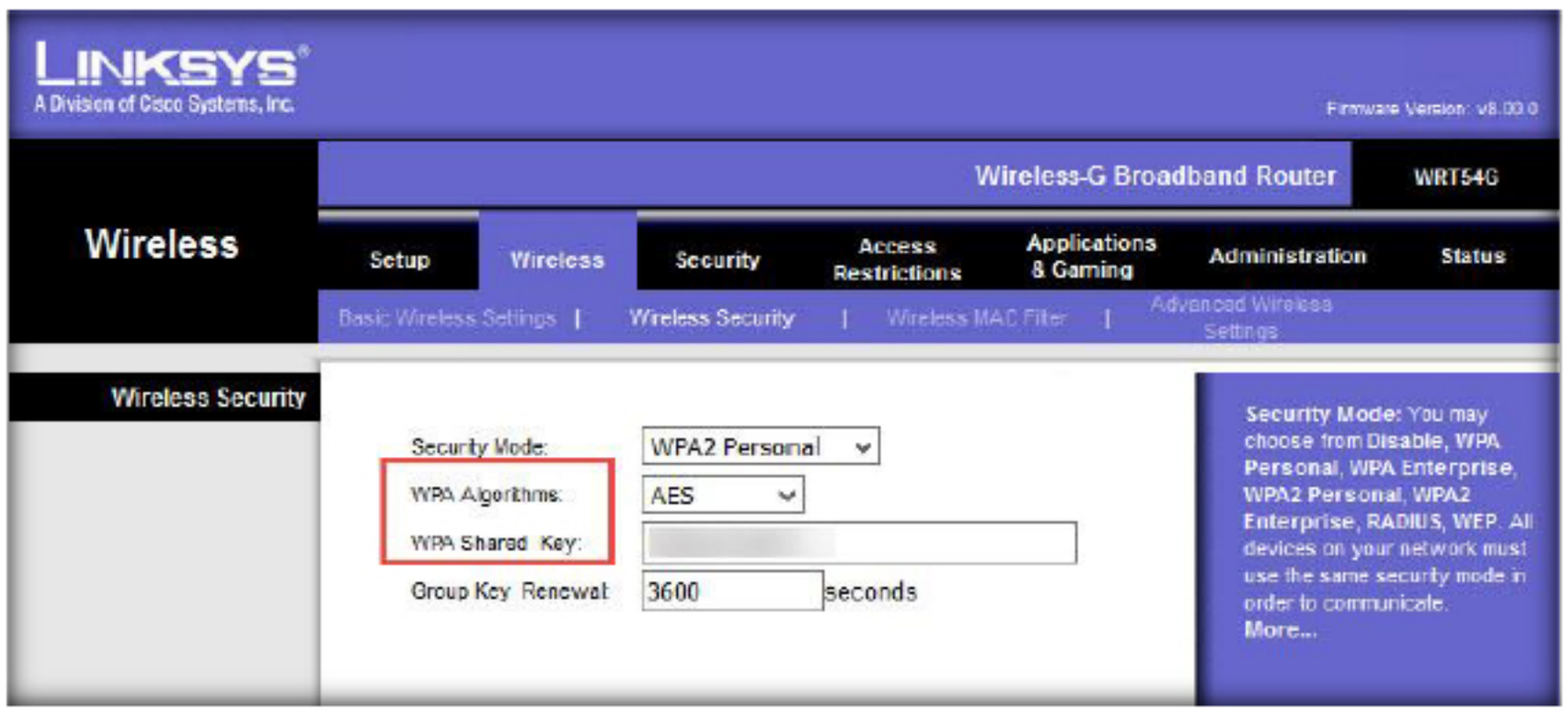


FIGURE 1.33 Configuring shared key and WPA algorithm

35. Click **Save Settings**

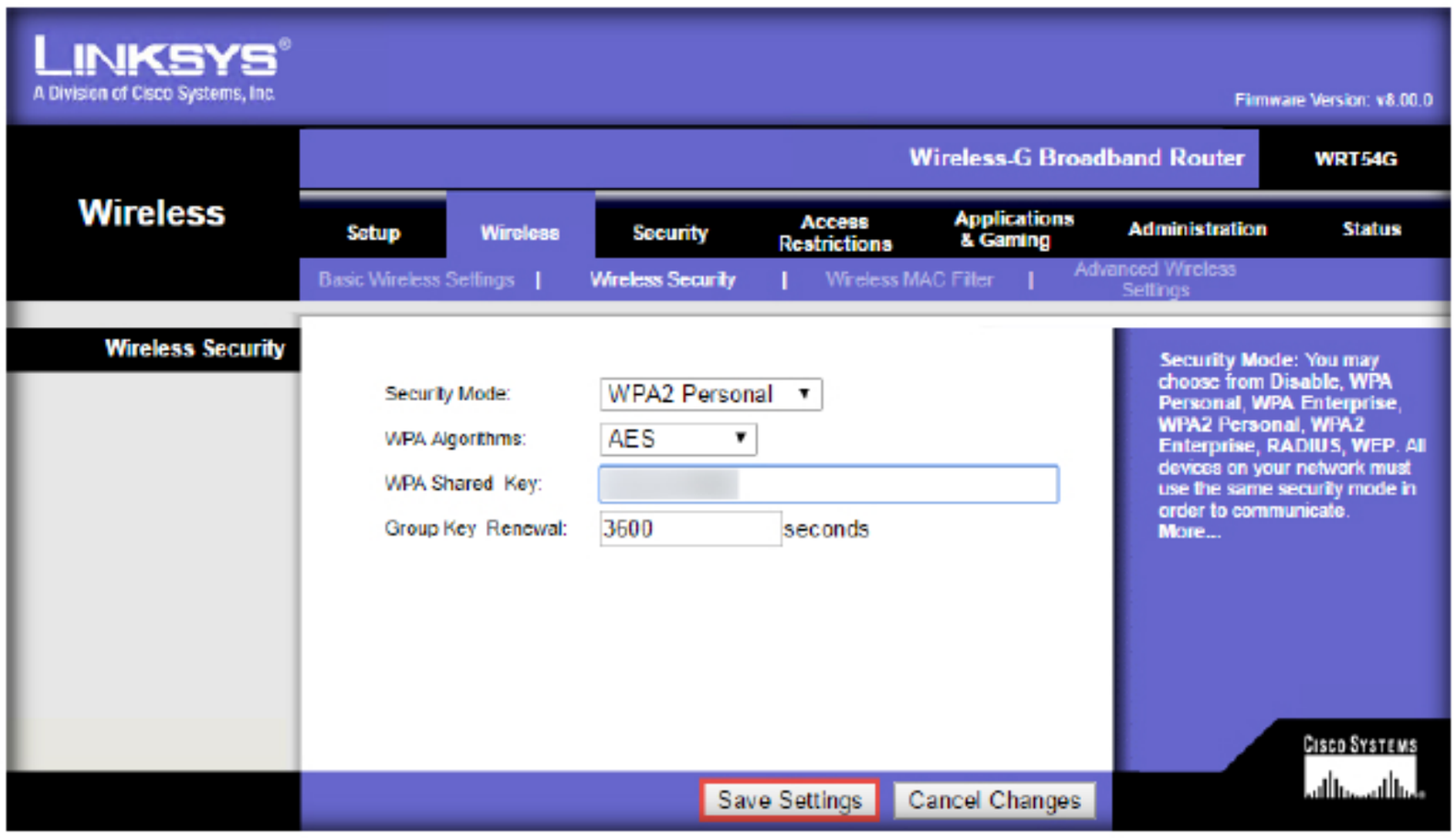


FIGURE 1.34 Saving settings

The Passphrase creates the keys required. Hence, any wireless network accessing the secured router should have the key.

36. A prompt saying **Settings are Successful** shows on the screen. Click **Continue**

FIGURE 1.35 Prompt for successful settings

Advanced Wireless Settings are always kept in their default values. Changes in these values may result in the poor performance of the router and hence may be manipulated by experienced users

37. Click on the **Wireless MAC Filter**

The Wireless MAC filter allows connecting a MAC address to the network

The Enabling Wireless Mac Filter blocks the addition of any other Mac addresses to the network

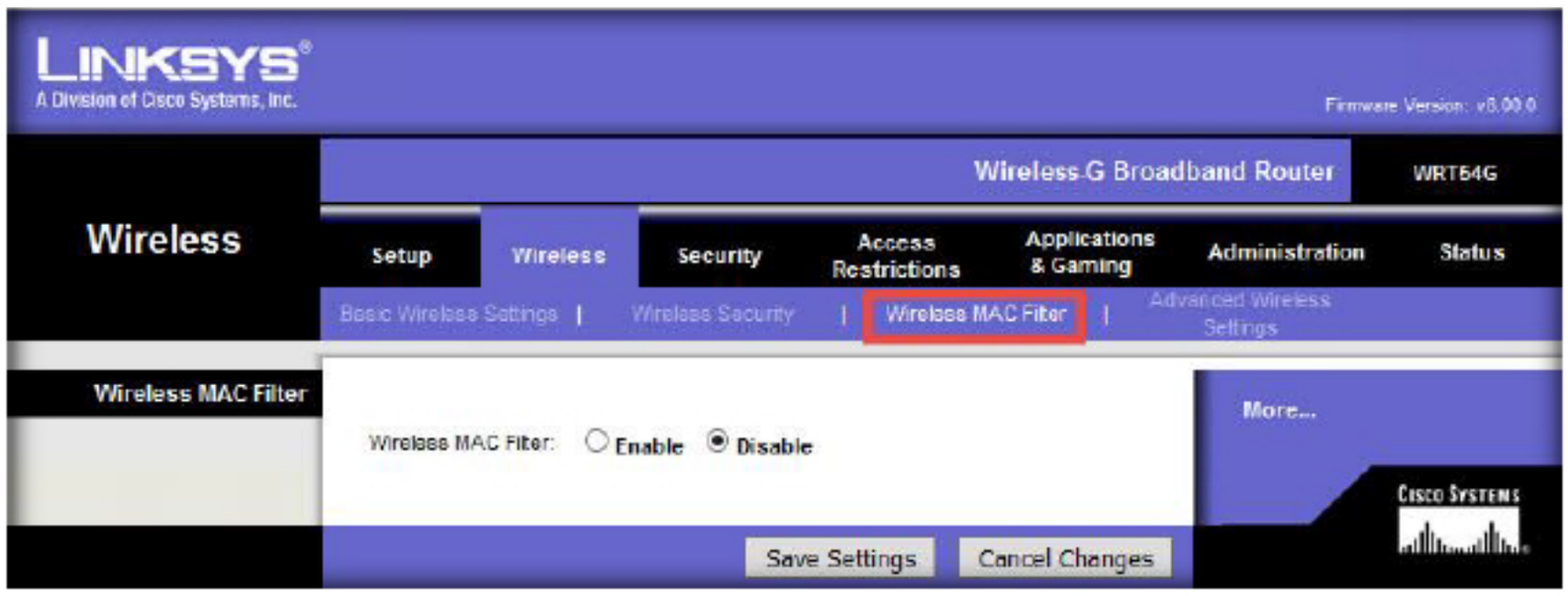


FIGURE 1.36 Wireless MAC filter

38. Click on the **Enable** radio button under the **Wireless MAC Filter** option

Prevent helps in preventing a device being connected to the wireless network.

Permit only allows the selected devices to access the wireless network

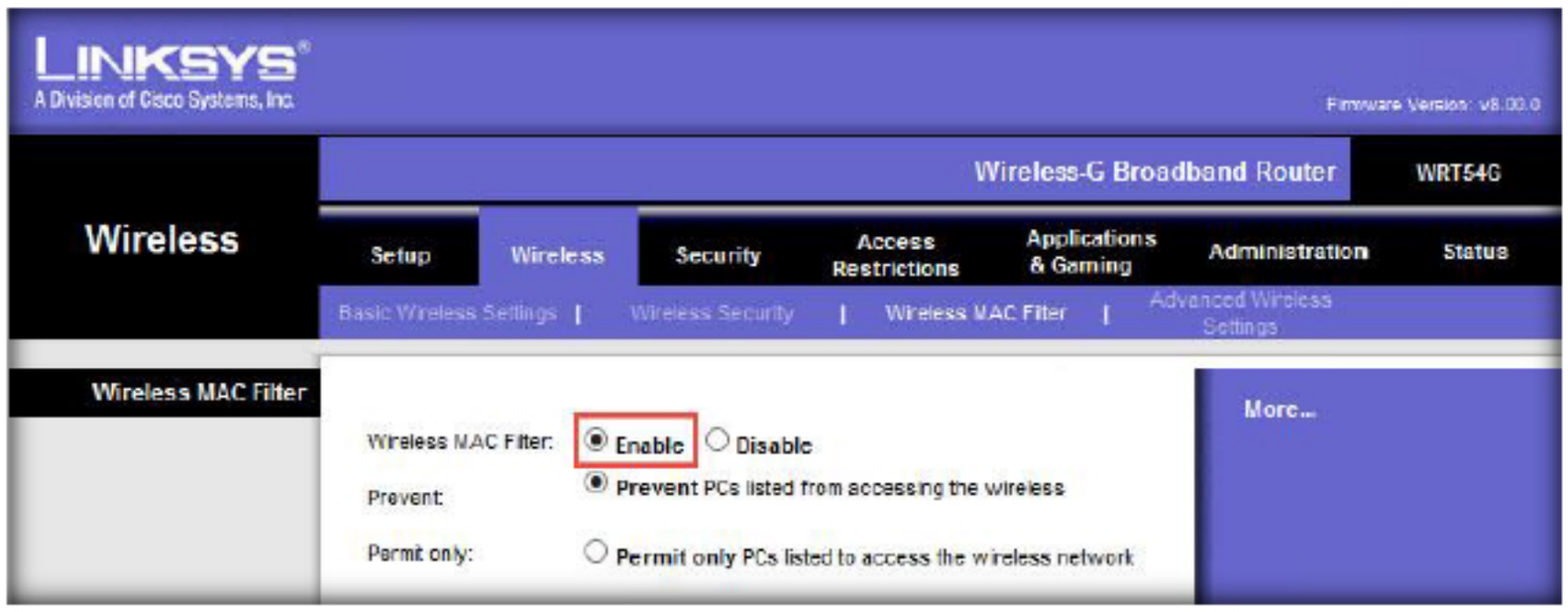


FIGURE 1.37 Enabling wireless MAC filter

Editing the MAC Filter list allows the addition of another set of MAC addresses

39. Now, go to the **Security** tab, in order to enable firewall restrictions in the router

Note: Select the options **Block Anonymous Internet Requests** and **Filter IDENT (Port 113)**

TKIP: Stands for Temporal Key Integral Protocol. Less secure and used commonly with WPA standards

IDENT is an internet protocol that distinguishes users for particular TCP connections

Normally responds to TCP port 113

A Firewall provides an extra level of security to the network

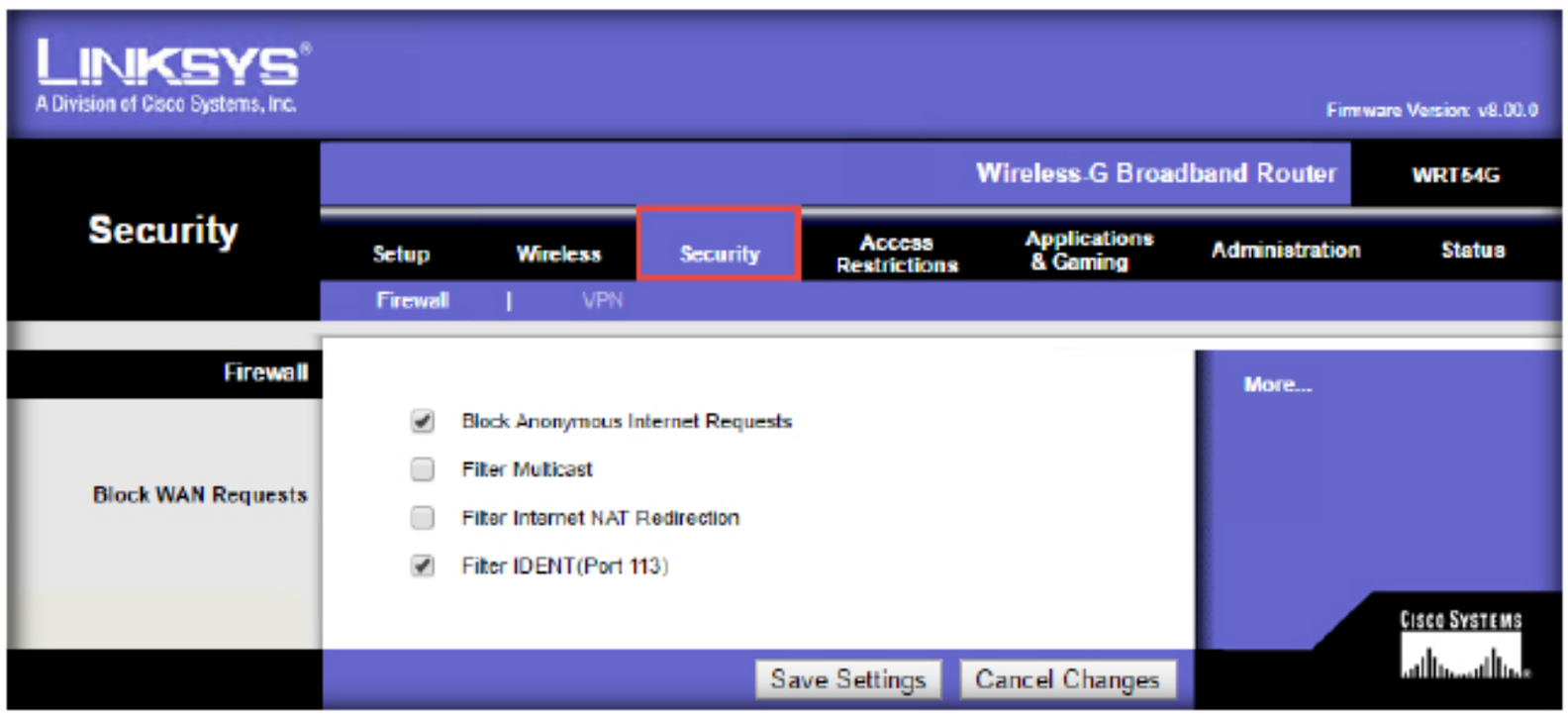


FIGURE 1.38 Configuring firewall restriction

40. Click on **Access restrictions**

Access restrictions control the access of the internet access in the network.

FIGURE 1.39 Configuring Access Restrictions

41. **Configure** the appropriate Internet access restrictions

42. Select **Application and Gaming** from the main menu

Access restriction allows you to block applications like HTTP, HTTPS, DNS, Ping, etc. and certain other services.

It also allows you to restrict or block certain websites using a keyword or by URL

Allows the router to block access to local resources from other local devices

Filter Multicast allows multiple hosts to reach their destination

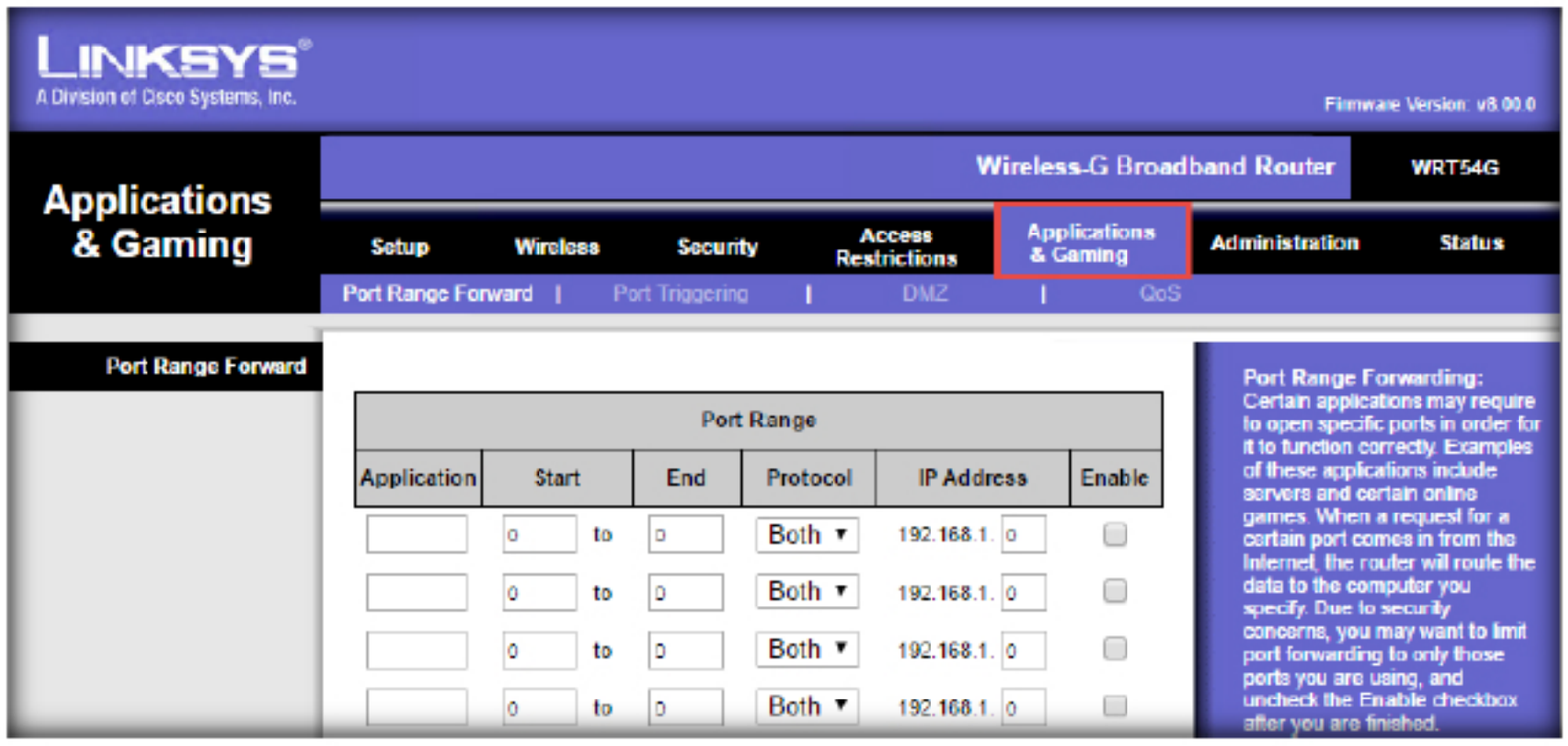


FIGURE 1.40 Applications and Gaming

43. Enter the following details:
    - **Application** – Enter the name of the program
    - **Start / End**– Enter the range of ports
    - **Protocol** – Select any one of the protocols or both
    - **IP Address** – Enter the IP address of that port receiving the port traffic
    - **Enable** – Enable or disables the port forwarding rule

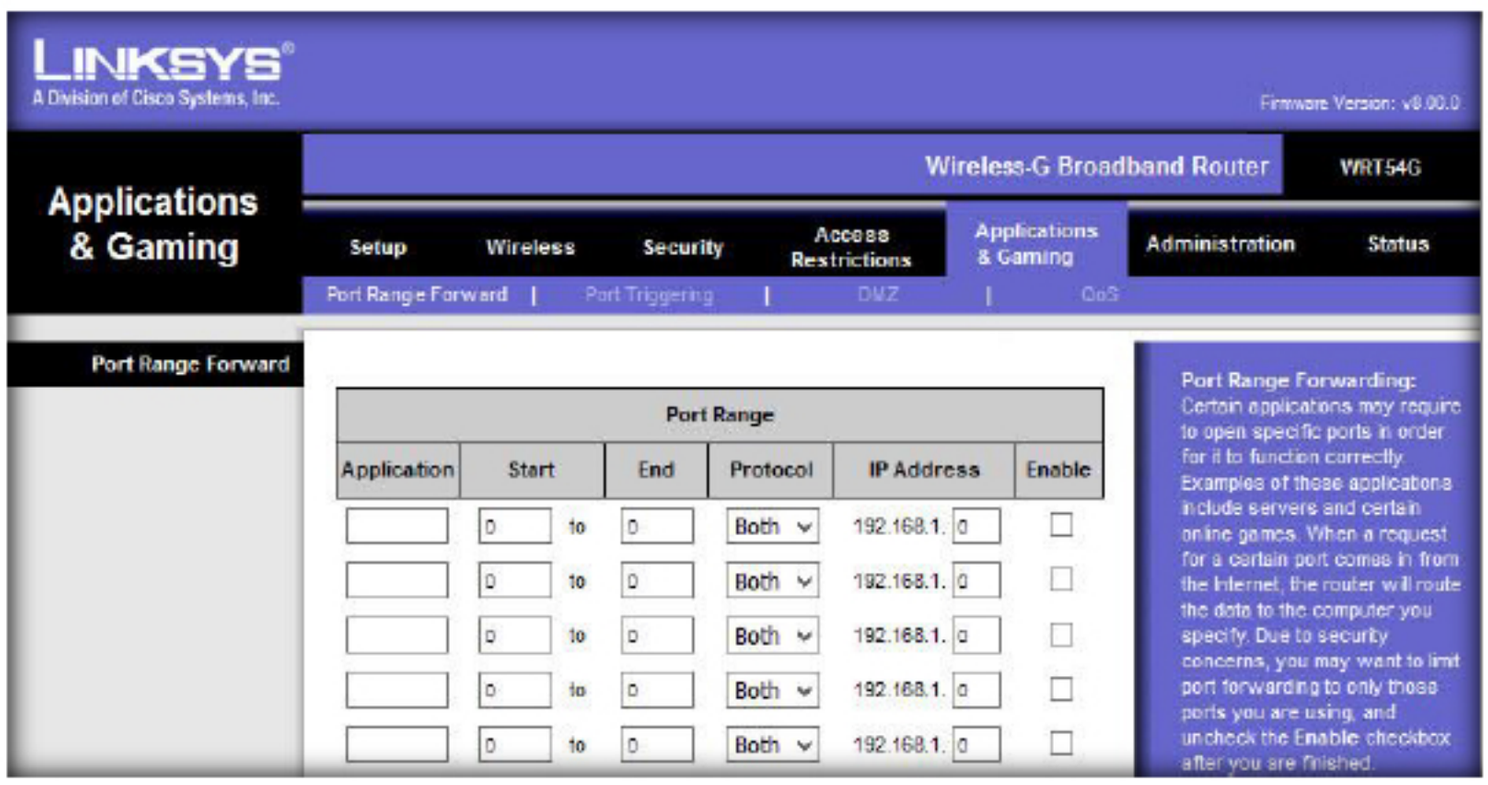


FIGURE 1.41 Port Range Forward

44. Click on the **Port Triggering** tab

Port Triggering provides special internet applications in a local network

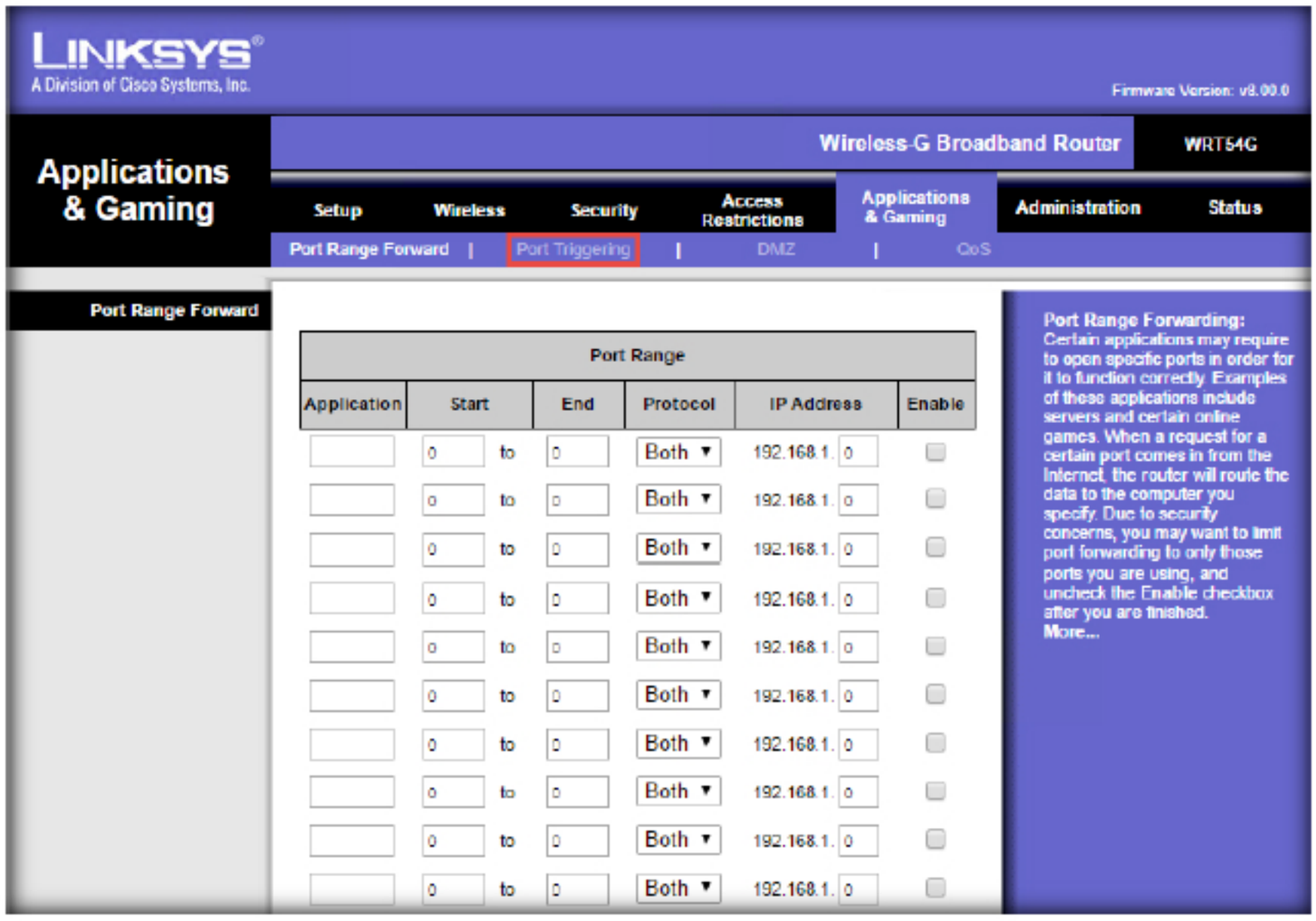


FIGURE 1.42 Port Triggering

45. Enter the fields in the Port Triggering page and Click **Save Settings**

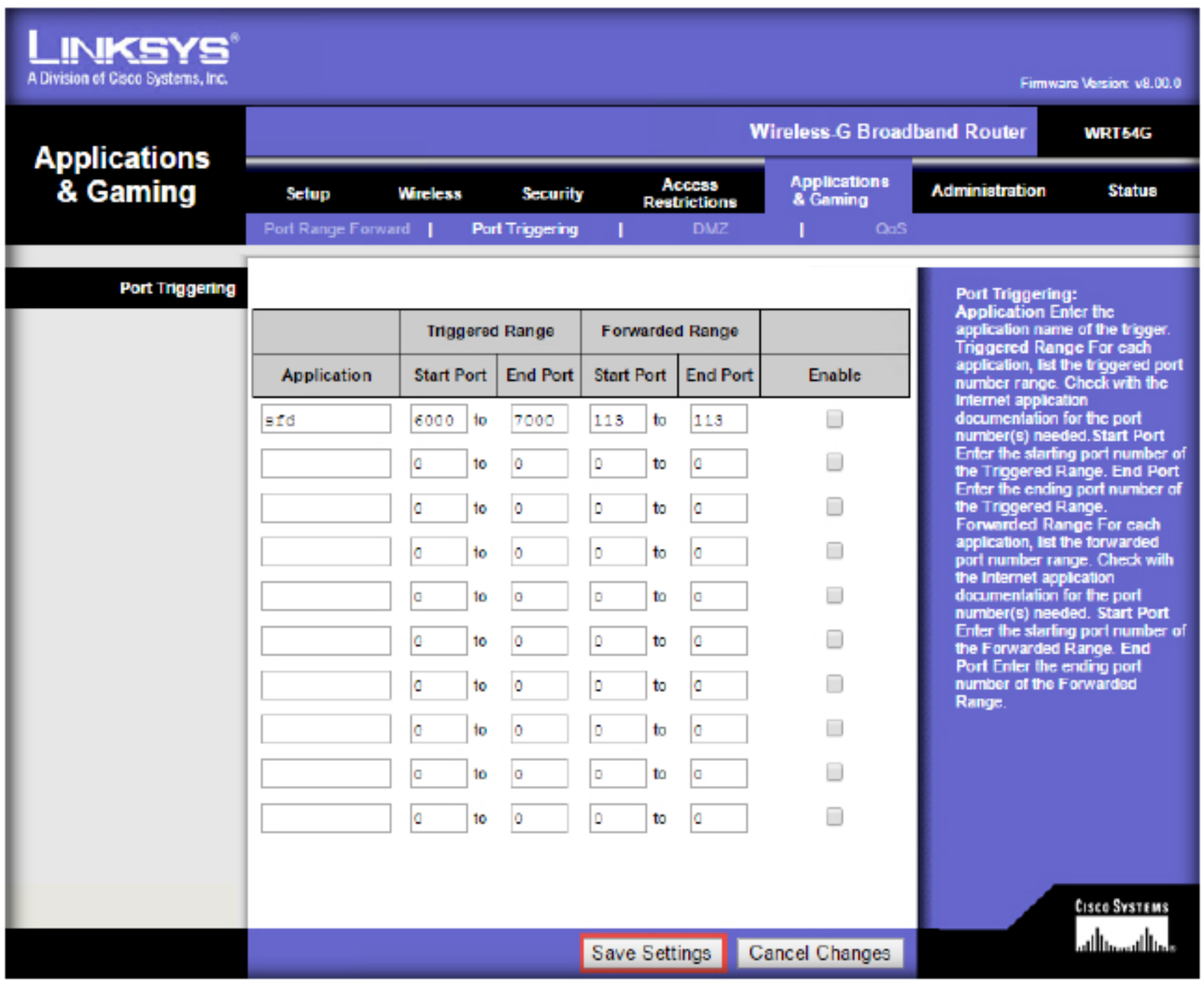


FIGURE 1.43 save Settings

46. A prompt saying the **Settings are Successful** will appear. Click **Continue**

FIGURE 1.44 Settings are Successful

47. Next, Click on the **DMZ** tab

Enabling the DMZ opens all the ports thereby exposing the computer to the internet.

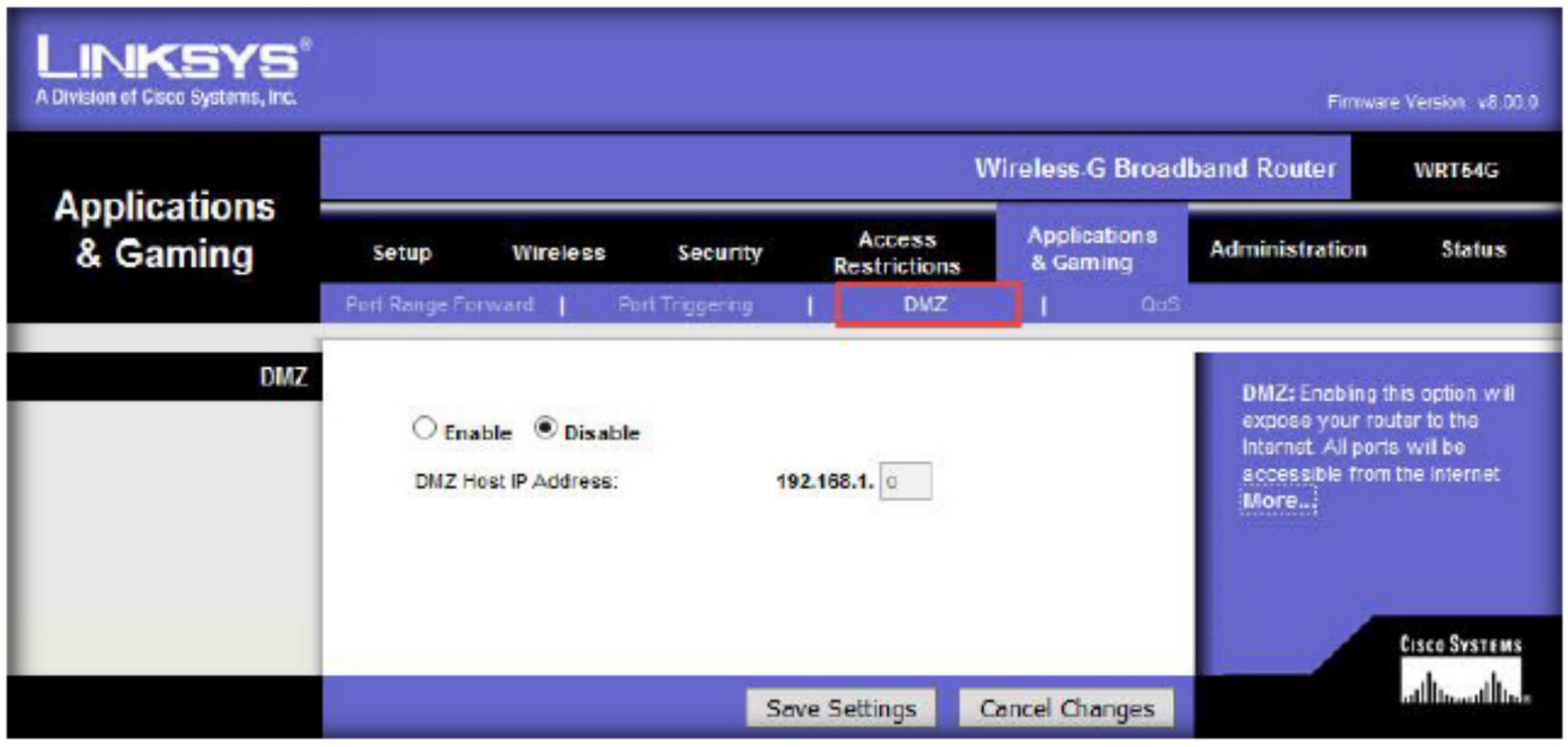


FIGURE 1.45 DMZ

48. Choose **DMZ → Disable**

FIGURE 1.46 Disable DMZ

49. Now, click on **QoS** tab

FIGURE 1.47 QoS

50. Choose **QoS → Disable**

📖 QoS is enabled only when you require any prioritization for any of the services

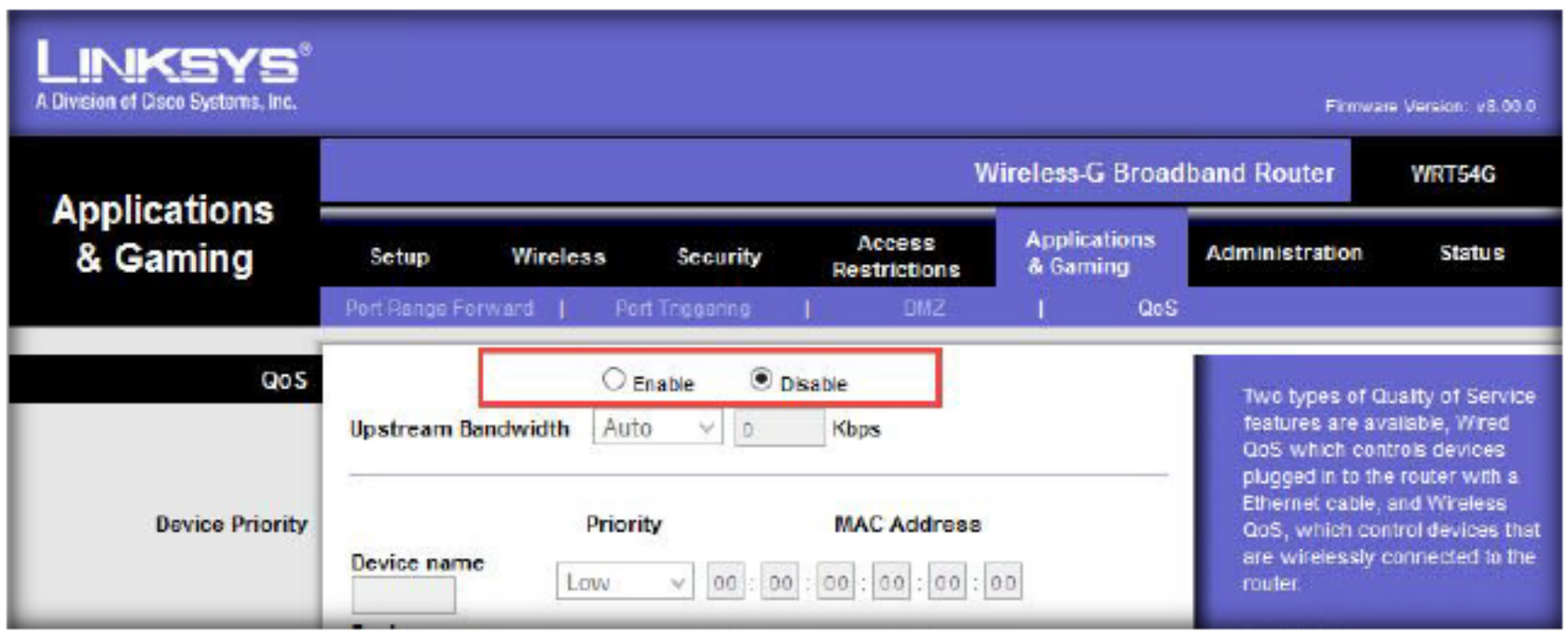


FIGURE 1.48 Disable QoS

51. Click **Save Settings**

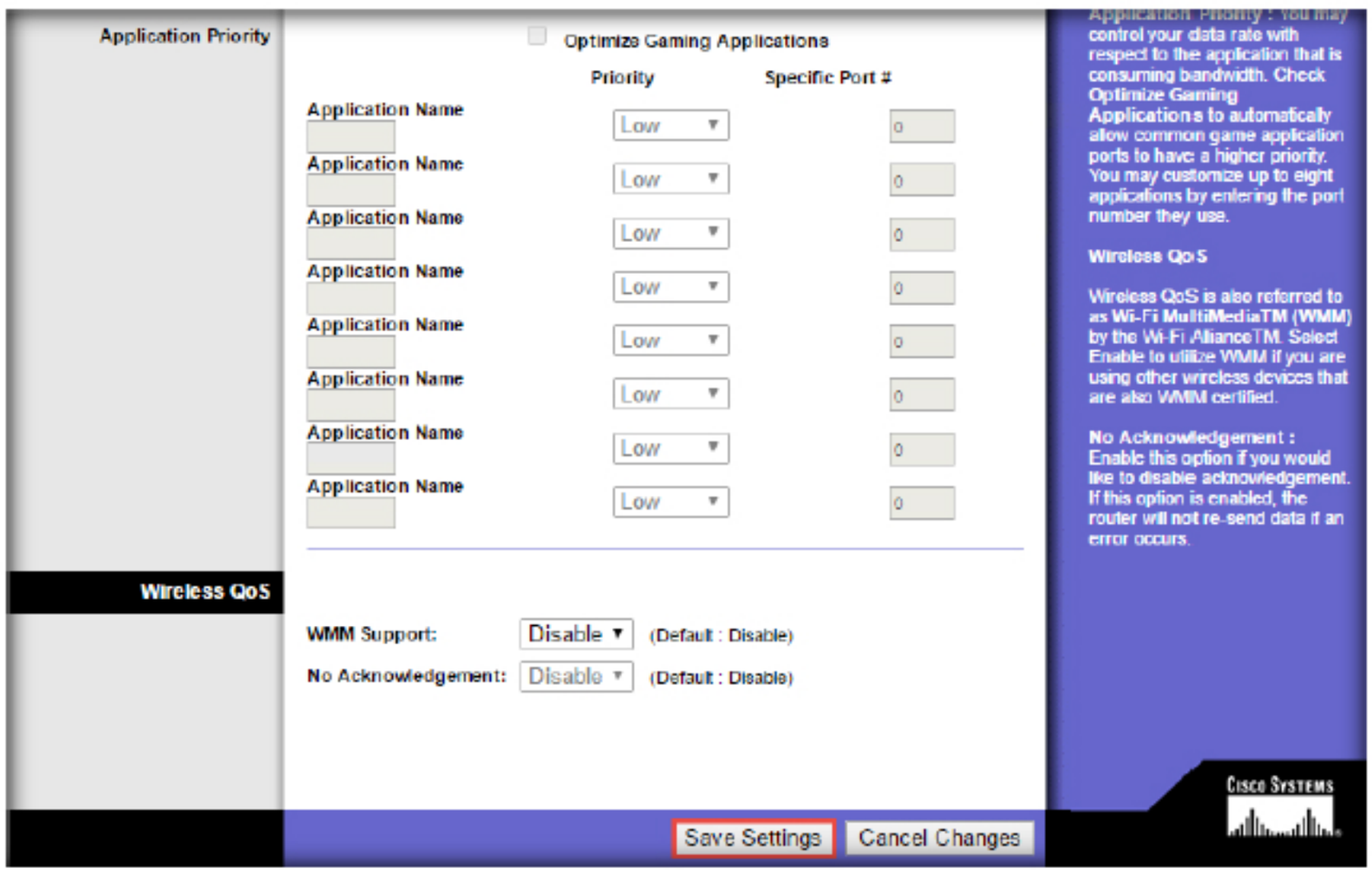


FIGURE 1.49 Save Settings

52. A prompt saying the **Settings are Successful** is displayed. Click **Continue**

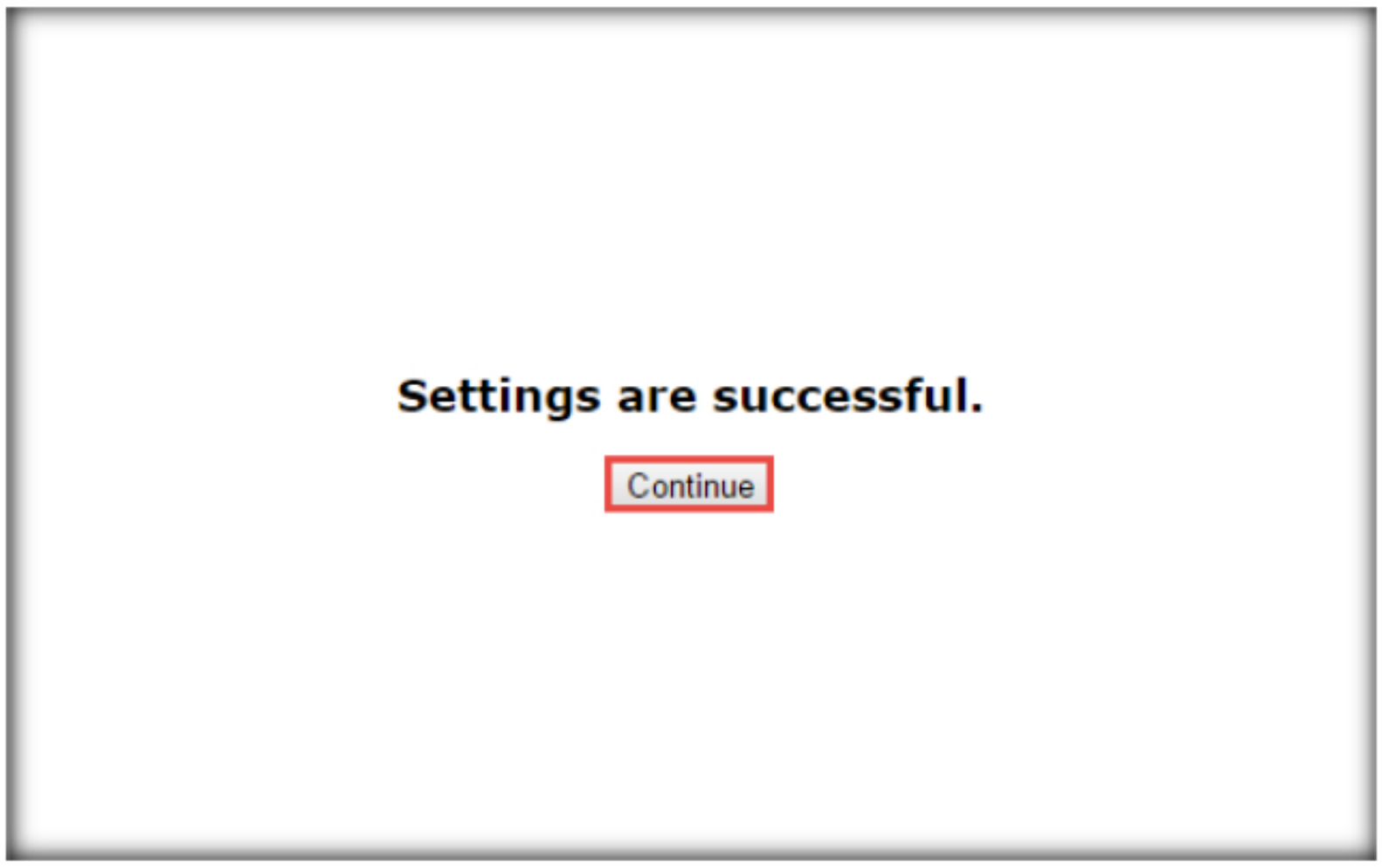


FIGURE 1.50 Savings are Successful

53. Click on the **Administration** tab

The Administration tab helps in managing the router and log configurations. All the software upgrades may be performed here.

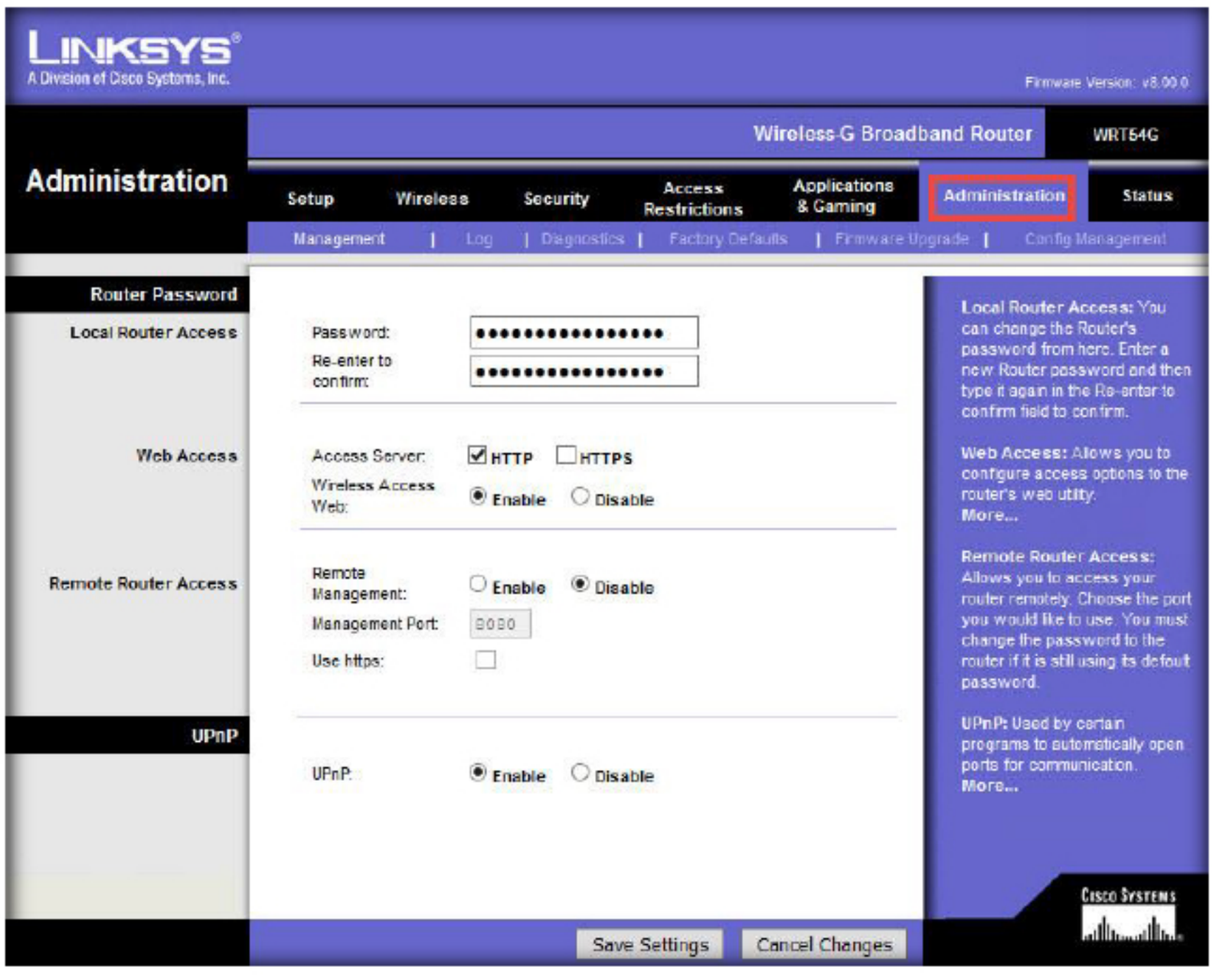


FIGURE 1.51 Administration tab

54. Click on the **Management** tab under Administration

The Management tab specifies the router password.

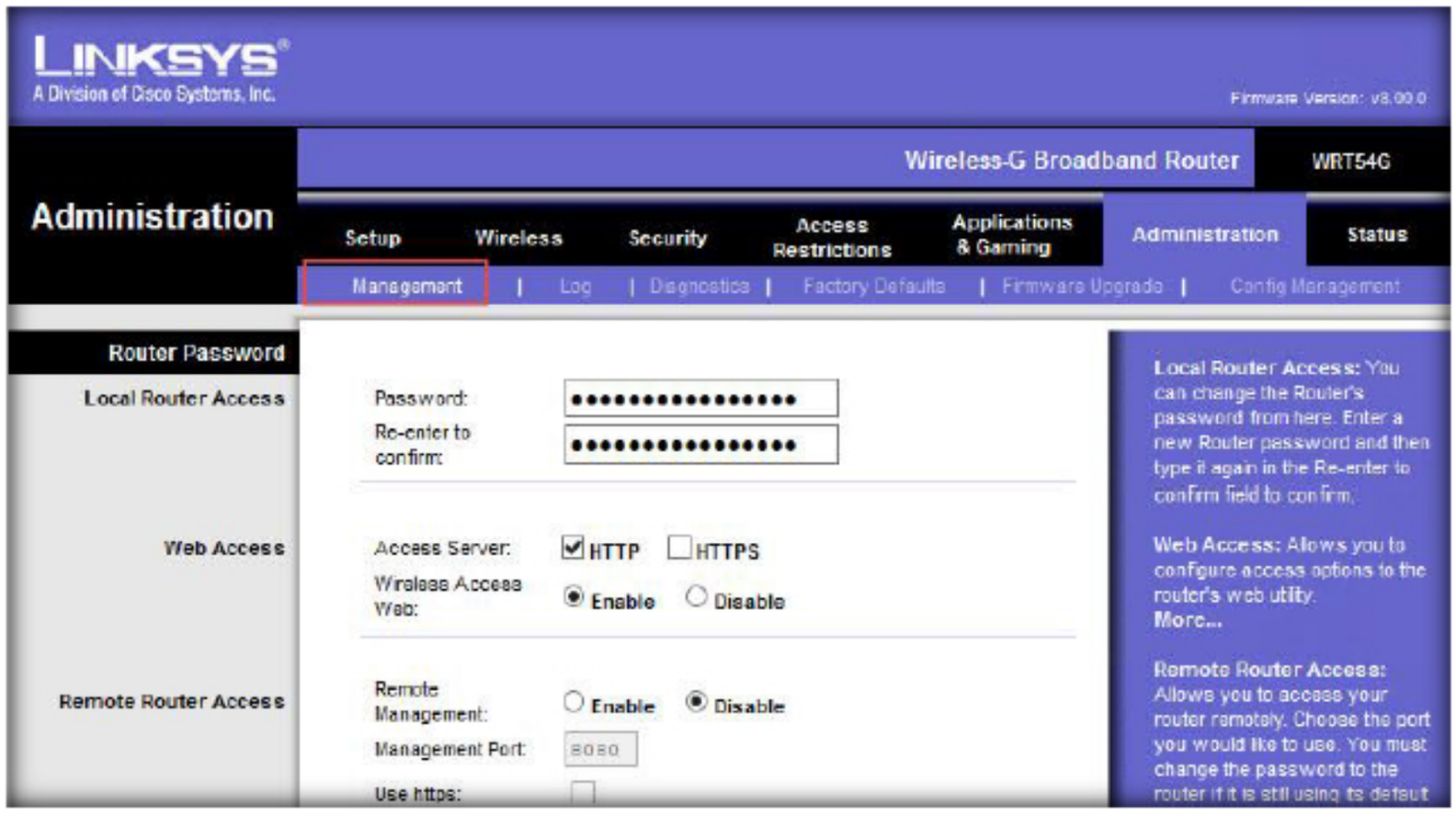


FIGURE 1.52 Management tab

55. In the **Password** field, choose the strongest password for a wireless router.

56. Type a new password. Re-type the new password in the **Re-enter to Confirm** field

    Note: Passwords should be changed periodically in order to restrict any unauthorized access to the wireless network

The Administrator router password differs from the Wireless network name (SSID) and passphrase of the wireless network.

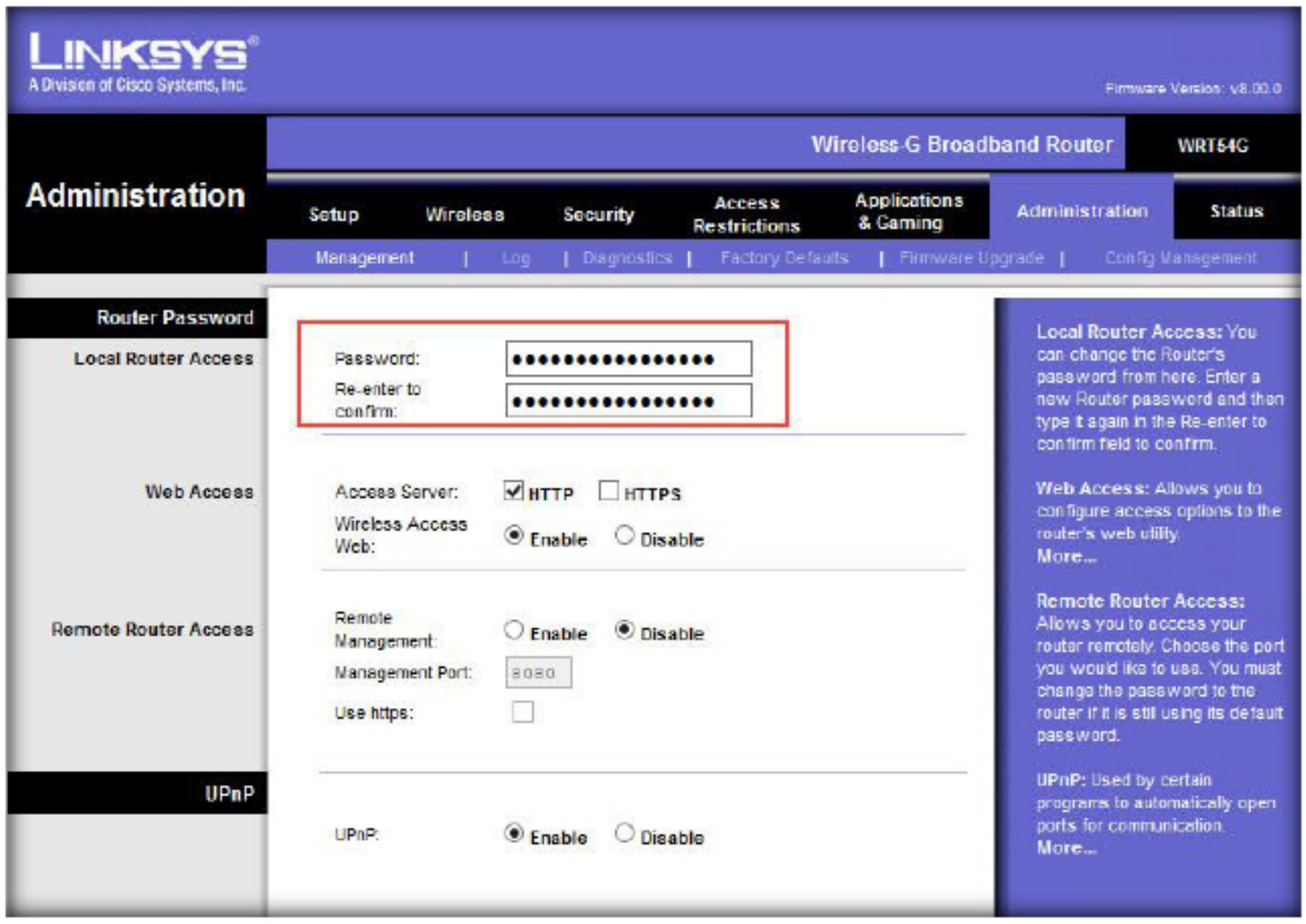


FIGURE 1.53 Configuring router passwords

57. Now, Select **HTTPS** from **Web Access → Access Server**

Enabling Remote router access for the first time prompts you to change the default router password. This can enable secure admin access and change the admin port from 8080.

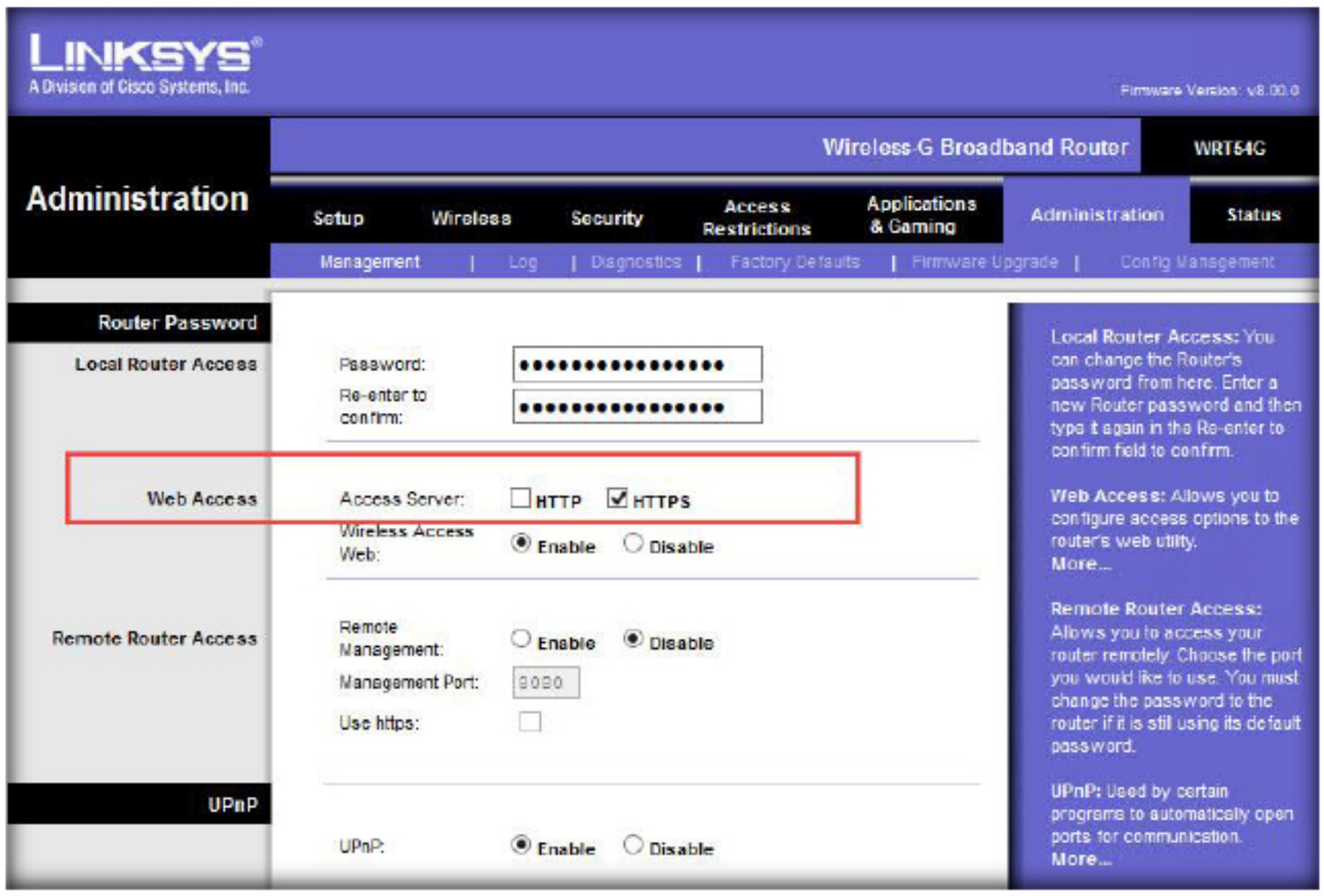


FIGURE 1.54 Configuring Web access

58. Choose **Remote Router Access → Remote Management → Disable**

Status provides the details regarding the current status of the router

Config Management allows backup management and Restore Management

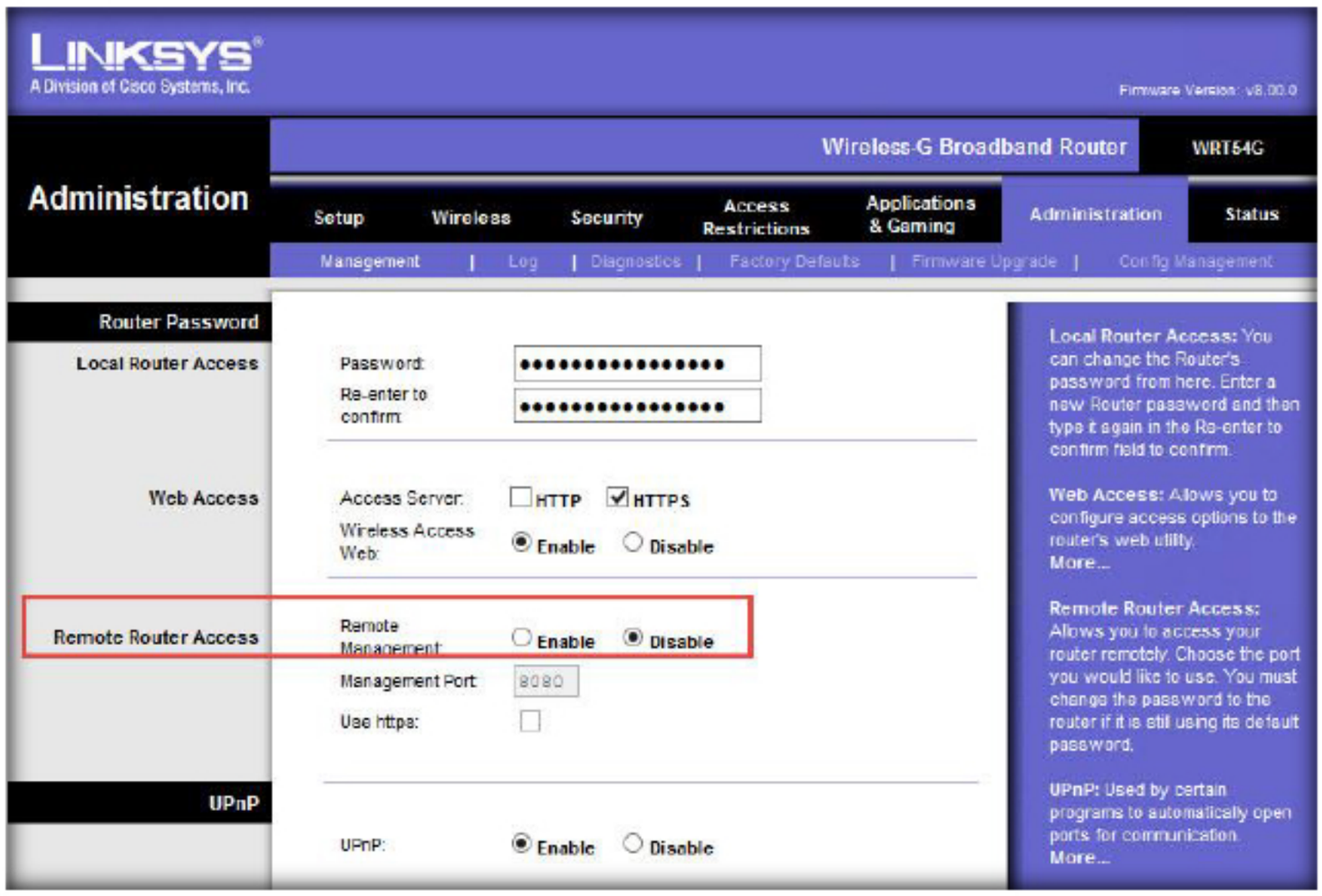
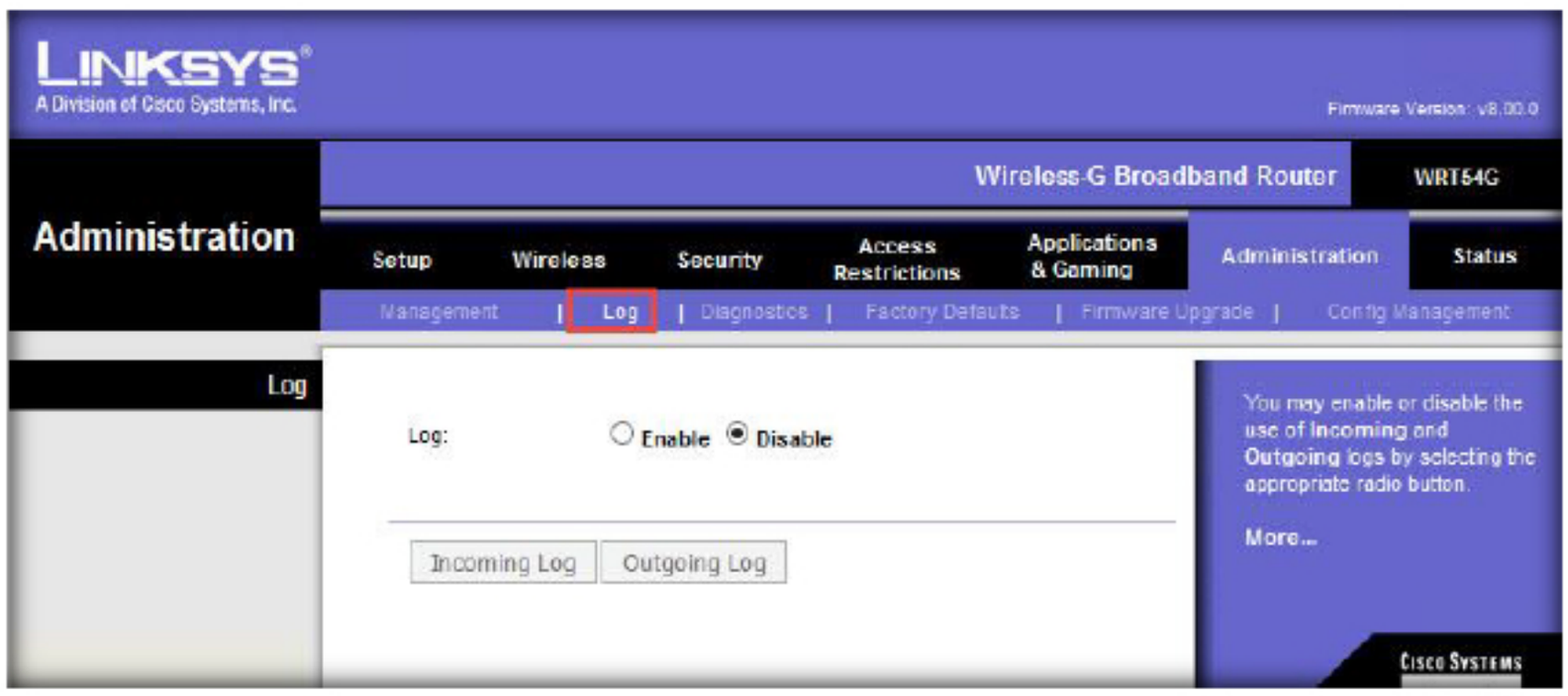


FIGURE 1.55 Configuring Remote Router Access

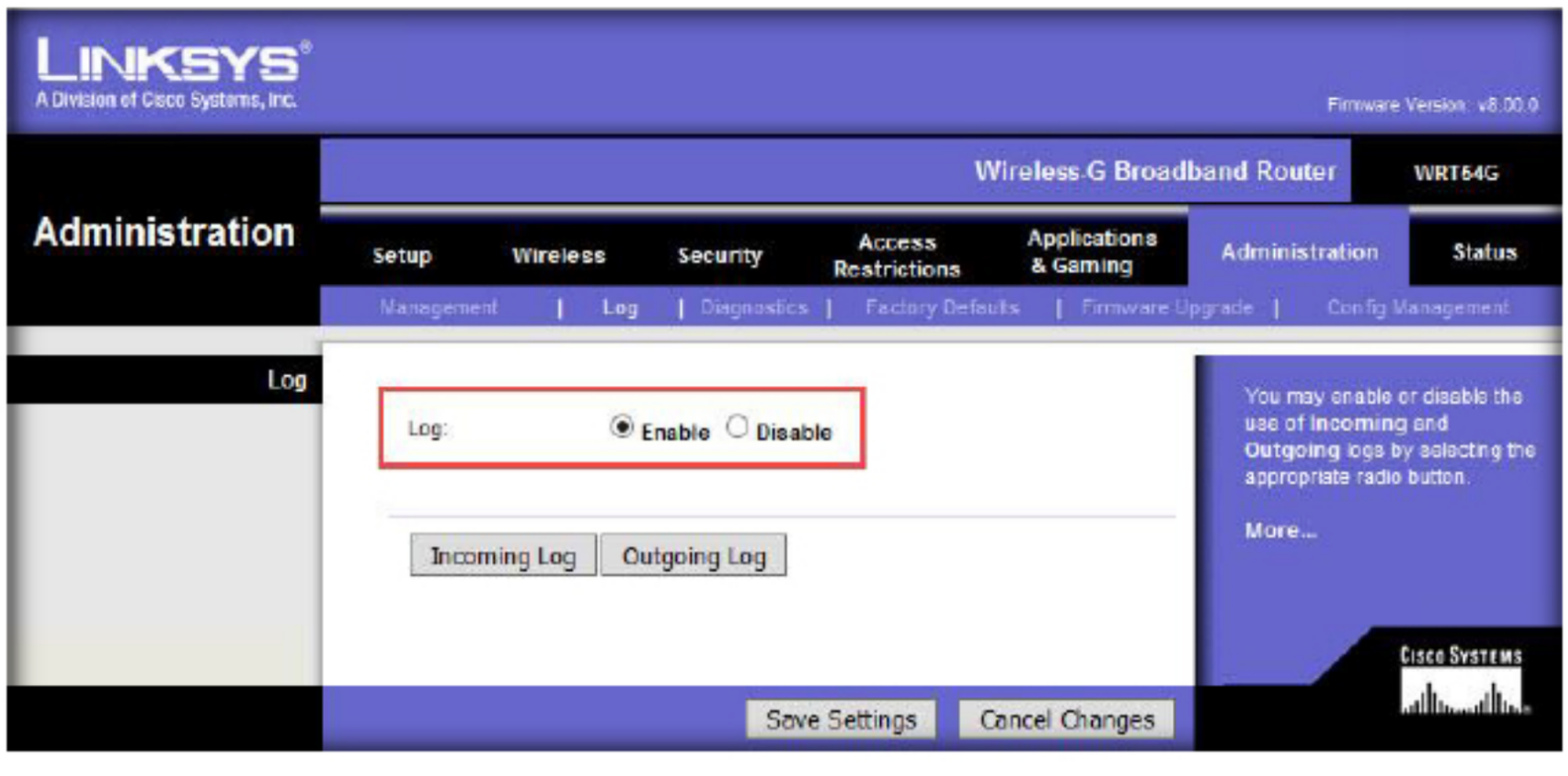
59. Click on the **Log** tab under **Administration**



The Firmware Upgrade allows you to upgrade the firmware. Upgrading may lead to loss of configuration details and hence you need to save all configuration details before

FIGURE 1.56 Log tab

60. Choose **Log → Enable**



Log helps in sending logs to any particular computer

FIGURE 1.57 Enabling log

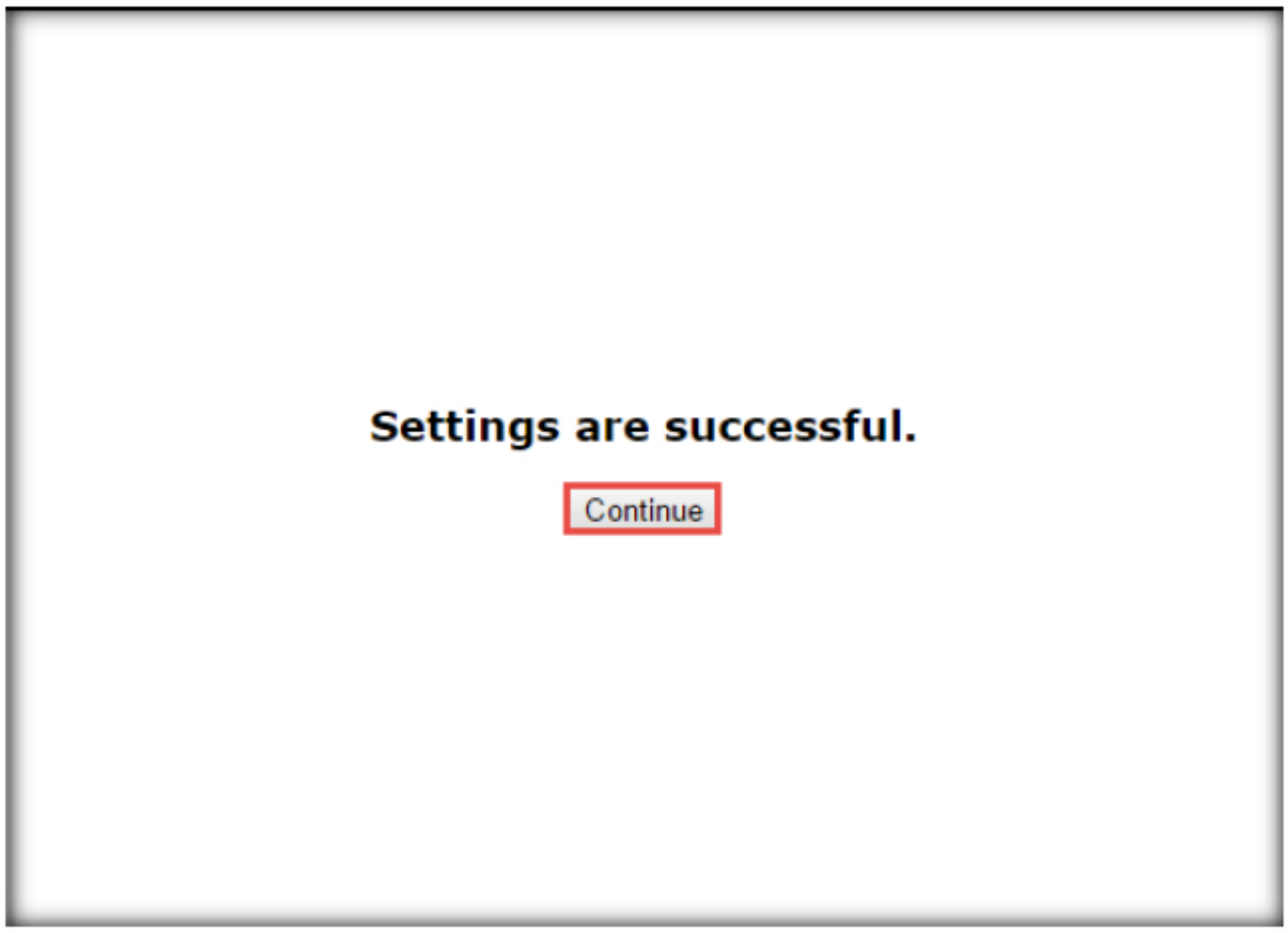
61. Click **Save Settings**

Diagnostics consists of two steps: Ping and Traceroute

FIGURE 1.58 Saving Settings

62. A prompt "**Settings are Successful**" pops-up

Factory Defaults allow changing the default values in the router. Changing these values may lead to the loss of saved values



Status displays the router information and the configuration type of the internet

FIGURE 1.59 Settings Successful prompt

63. Next, Click on **Status** from menu bar

DHCP Release deletes the current IP address

DHCP Renew adds a new IP address to the router.

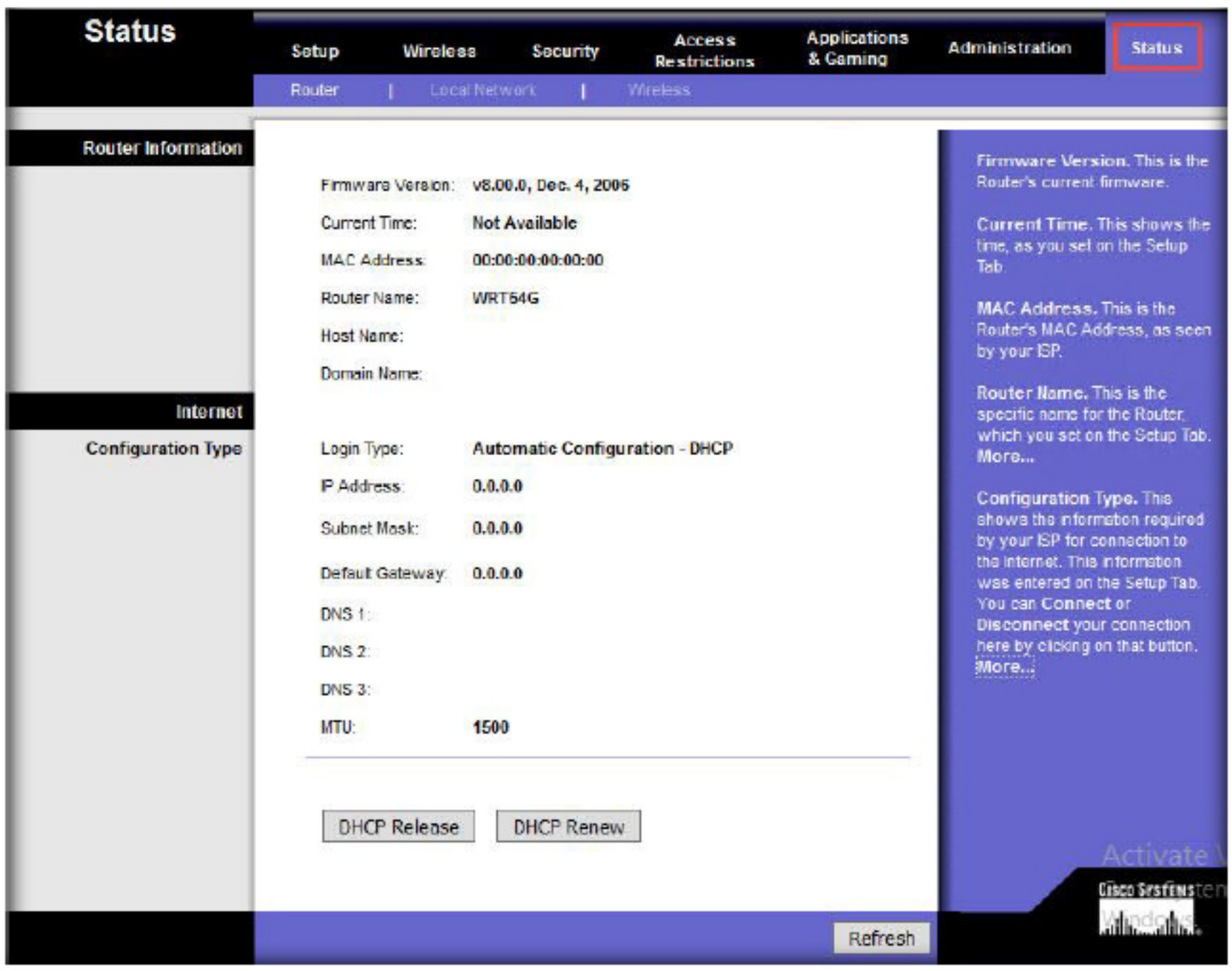


FIGURE 1.60 Status tab

64. In this way, you can make configuration changes in wireless router interface to secure your wireless router.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on securing the wireless network using Linksys router

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs