EC-Council

codered
FROM EC-COUNCIL

Module 11

WIRELESS NETWORK SECURITY

CERTIFIED CYBERSECURITY TECHNICIAN

INDEX

Module 11:
Wireless Network Security

LAB SCENARIO

The cyberspace is heading toward a new era of technological evolution by using wireless technologies. Wireless networking is revolutionizing the way people work and play. By removing the physical connection or cable, individuals can use networks in newer ways that make data portable, mobile, and accessible. A wireless network can be insecure if proper care has not been taken while configuring it. Insecure configurations can pose a great risk to the wireless networks.

A security professional must have the required knowledge to configure a wireless network as per the wireless according to the wireless security policy of an organization.

LAB OBJECTIVE

The objective of this lab is to provide expert knowledge in implementing wireless security policies. This includes knowledge of the following tasks:

- Configuration of security policies on a wireless router

OVERVIEW OF WIRELESS NETWORK SECURITY

The use of wireless devices in various organizations is continuously growing. Therefore, it becomes increasingly important for organizations to track and manage their wireless assets for security purposes. To ensure effective security, an accurate and up-to-date inventory of wireless devices must be maintained.

The inventory can help in quickly identifying non-functioning and rogue network devices present in a network. This helps in detecting unknown devices in the network. It is important to regularly scan this inventory; accordingly, security professionals can determine the rogue network devices, problematic devices, potential vulnerabilities, and devices that need a patch/update, etc., in a network. A network is only as secure as its weakest link. Information about all devices should be maintained regardless of their configuration settings or vendor.

LAB TASKS

A cyber security professional or a security professional use numerous tools and techniques to configure wireless network security policies. The recommended labs that will assist you in learning the implementation of wireless network security controls include:

01 **Configure Security on a Wireless Router**

Note: Turn on **PfSense Firewall** virtual machine and keep it running throughout the lab exercises.

EXERCISE 1: **CONFIGURE SECURITY ON A WIRELESS ROUTER**

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

LAB SCENARIO

Organizations allow wireless devices to connect to their network in today's environment (Bring Your Own Device or BYOD). However, the 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 wireless access points to gain access to the organizational network. Organizations should ensure that their wireless access points are configured securely.

A security professional should be able to configure the wireless router securely by applying all possible hardening techniques.

LAB OBJECTIVE

This lab will demonstrate the various hardening techniques on a wireless router.

OVERVIEW OF WIRELESS ROUTER SECURITY

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

LAB TASKS

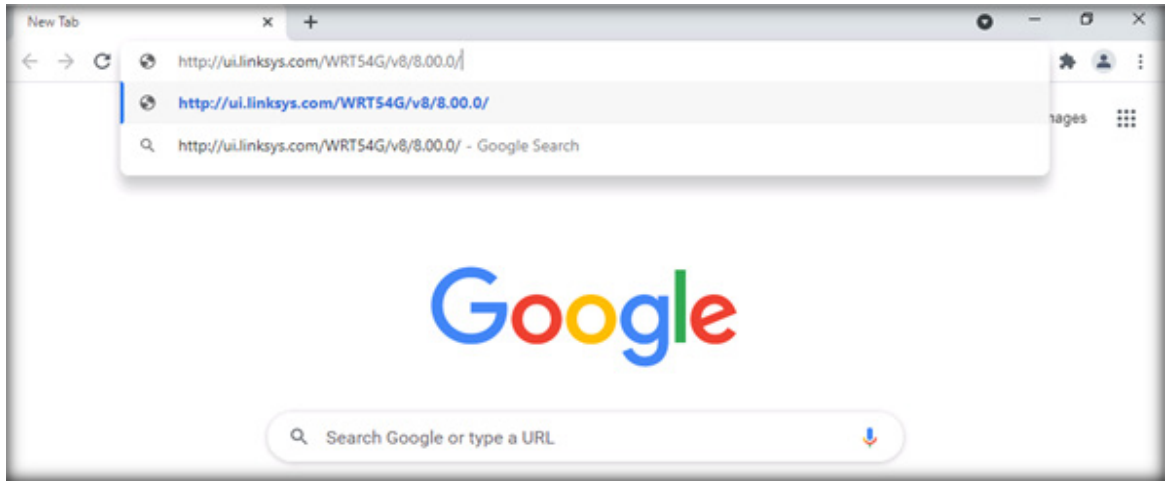
Note: Ensure that **PfSense Firewall** virtual machine is running.

1. Turn on the **AD Domain Controller** virtual machine.

2. Log in with the credentials **CCT\Administrator** and **admin@123**.

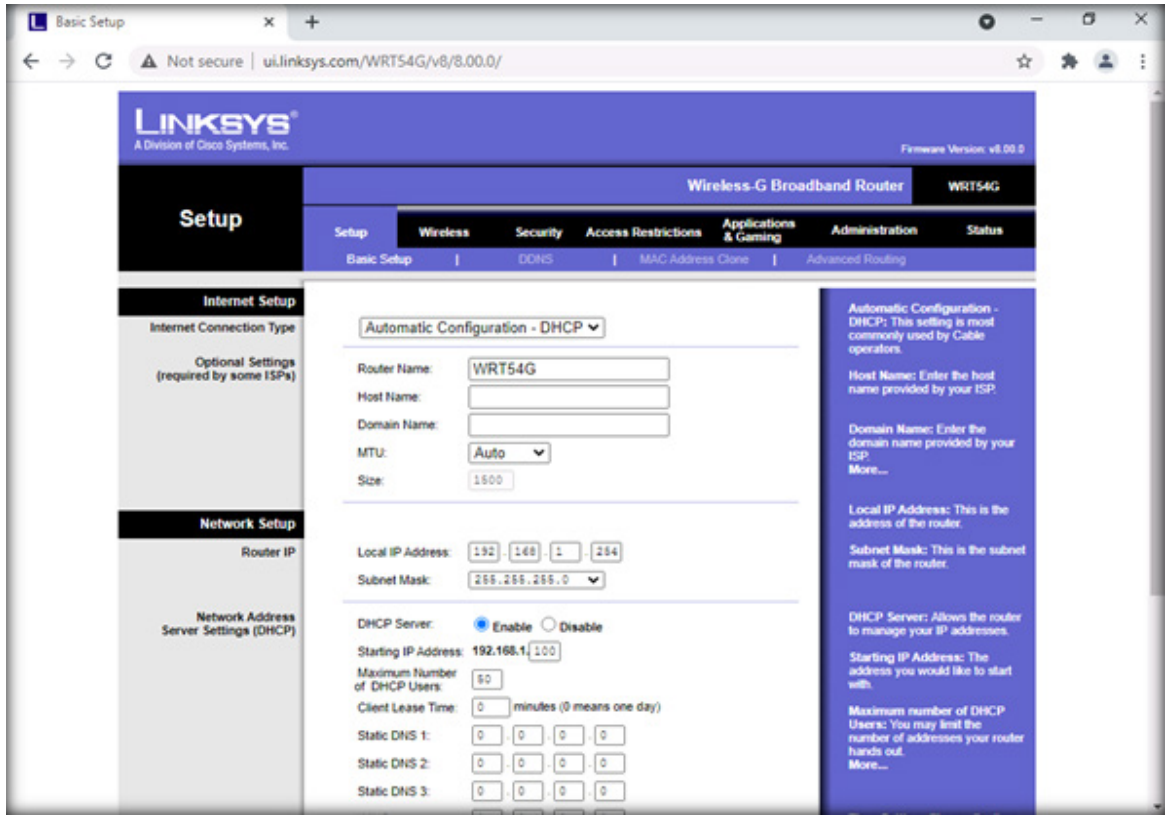
3. Open **Google Chrome** browser. Browse the Linksys Wireless router set up simulator available at **http://ui.linksys.com/WRT54G/v8/8.00.0/** in your browser.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER



4. The **Linksys** router interface window will be displayed in the browser.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER



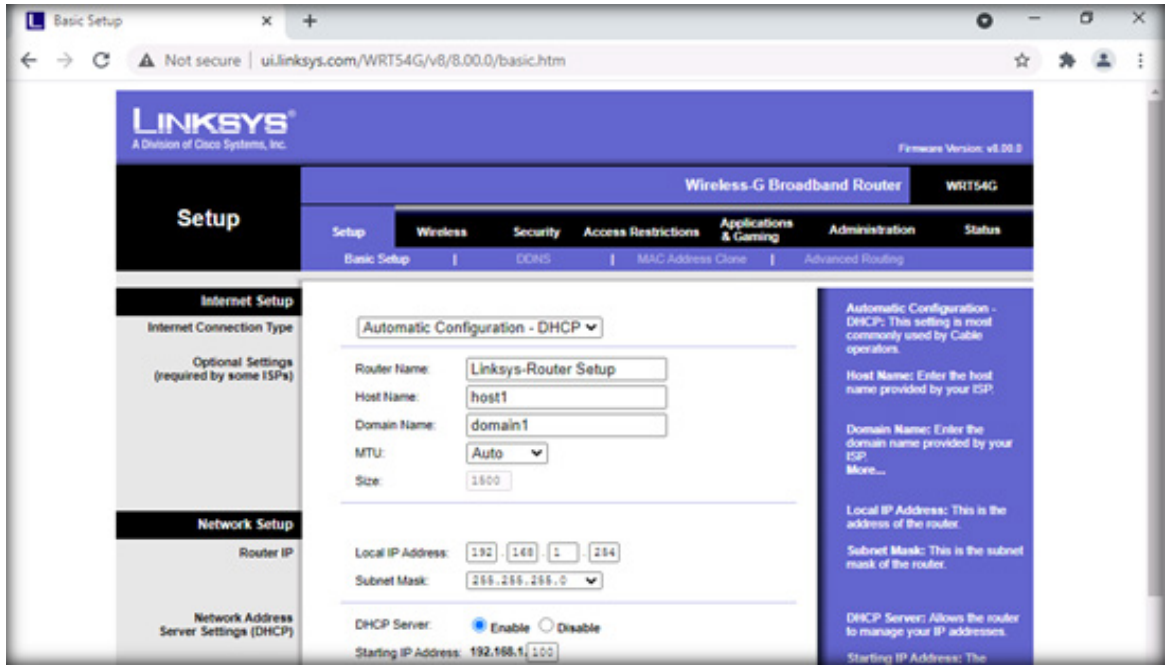
5. Click on **Setup** followed by **Basic Setup**.

6. Specify the **Router name, Host name**, and **Domain name** in **Optional Settings (required by some ISPs)** (here, we are taking **Router Name** as **Linksys-Router Setup, Host Name** as **host1, Domain Name** as **domain1**)

7. Ensure that the **Auto** option is selected from the drop-down menu for **MTU**.

8. The **Local IP Address** and **Subnet Mask** in the **Router IP** field are displayed. Set DHCP Server to **Enable**.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER



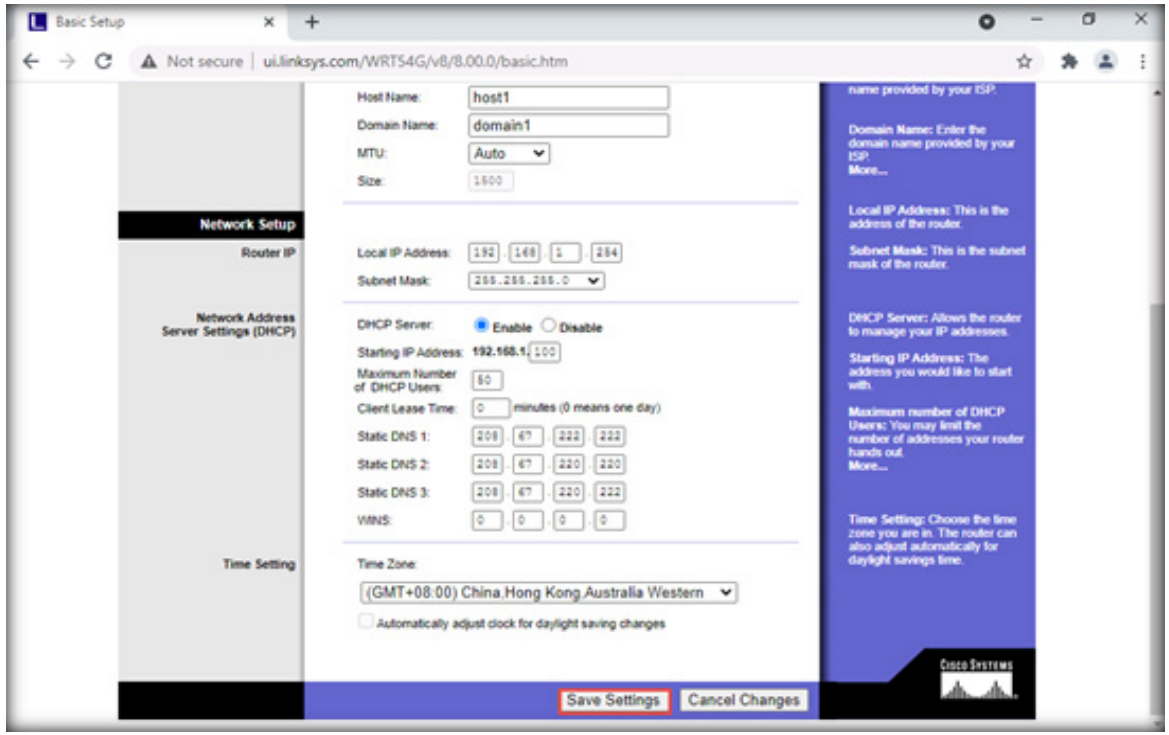
9. Specify the **Starting IP Address** and **Maximum Number of DHCP Users**. Type **Client Lease Time** in minutes.

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

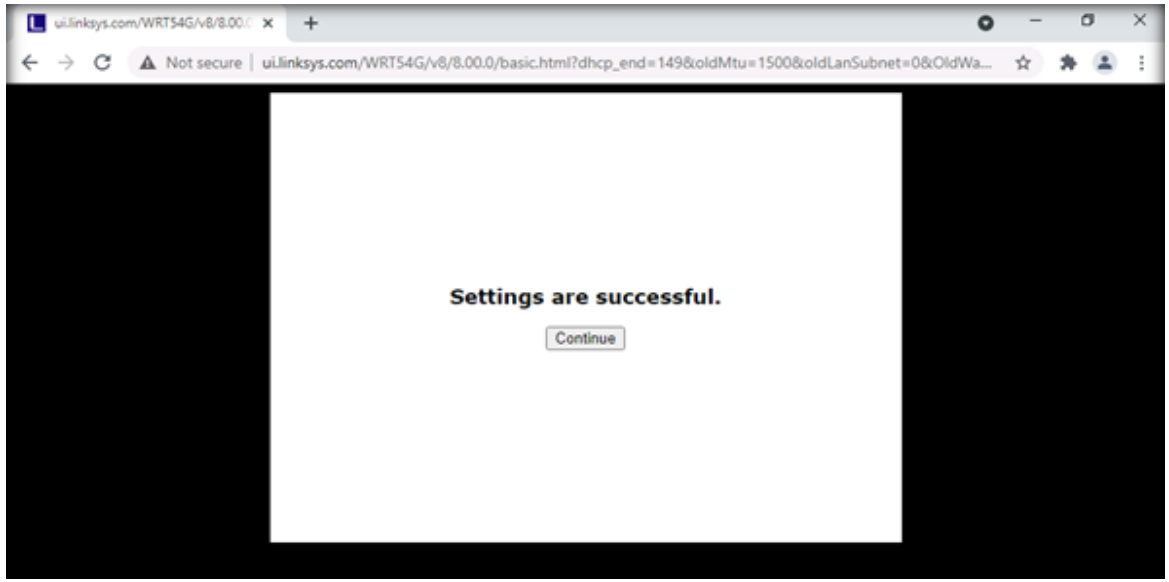
11. Enter the **WINS** server IP address if you use a WINS server.

12. Click on the **Save Settings** button to save all changes.
    Note: If you receive any error message, reload the page and repeat the steps 6 to 11.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER



13. A prompt indicating that **Settings are successful** is displayed. Click on **Continue**.

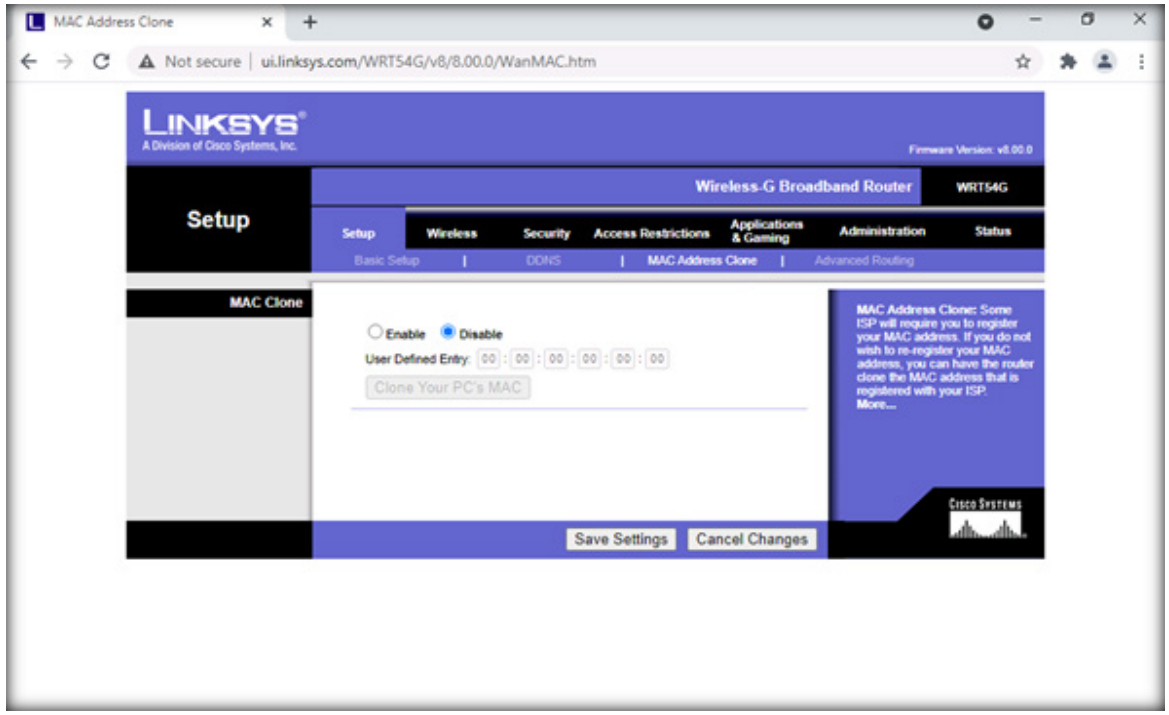


EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER

14. Next, click on **MAC Address Clone**.

15. Ensure that **Mac Clone** is set to **Disable**.

EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER



16. Next, click on **Advanced Routing**.

17. Set the **Operating Mode** to **Gateway**.

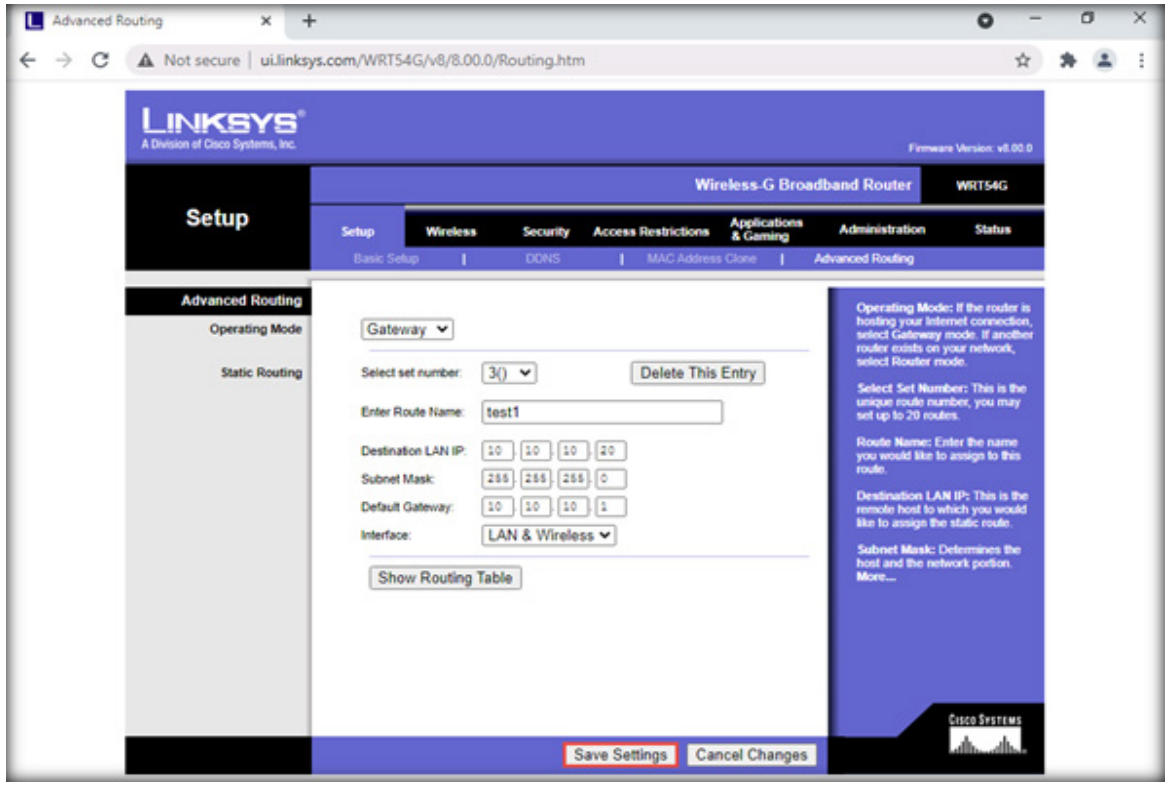
18. Select a number from the **Static Routing** drop-down menu **Select set number**.

19. Enter the following details:
    - Router Name
    - Destination LAN IP
    - Subnet Mask
    - Default Gateway

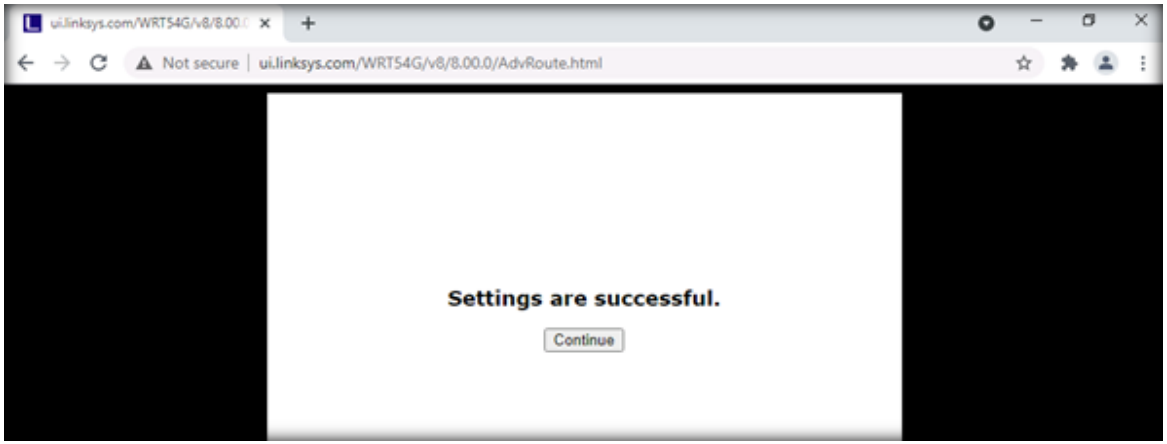
20. Next, select an **Interface** from the drop-down menu (**LAN & Wireless**).

21. Click on **Save Settings**.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER



22. A prompt indicating that **Settings are successful** is displayed. Click on **Continue**.



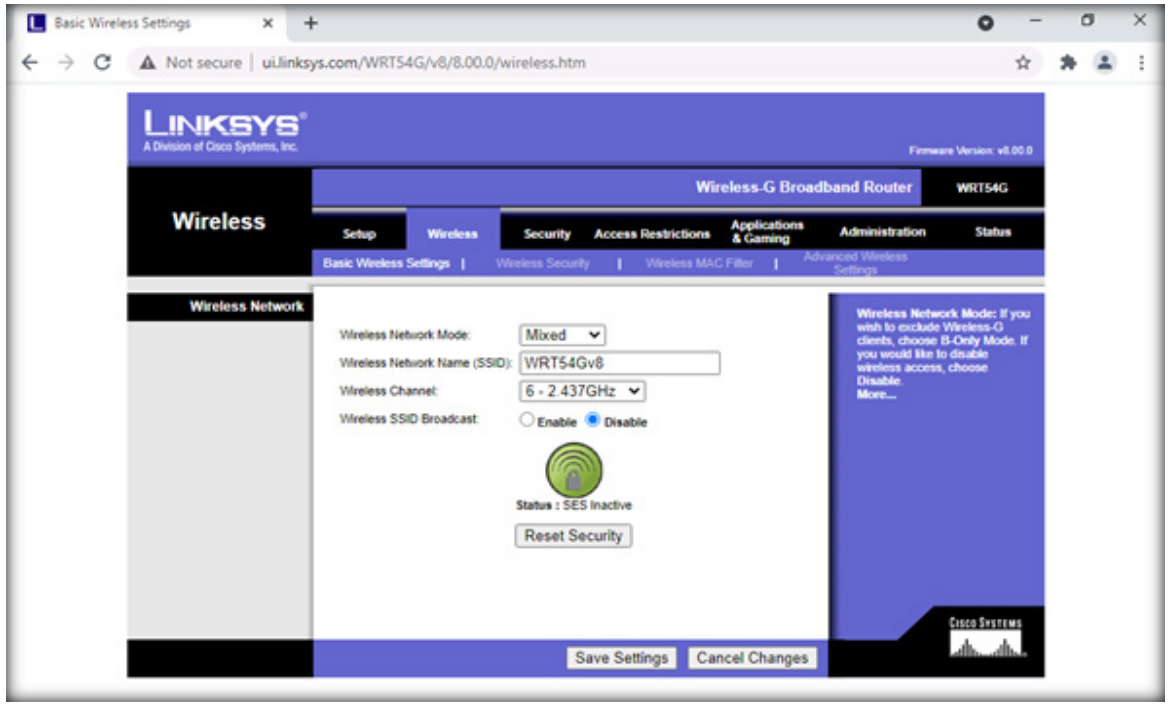
EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER

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

24. Click on the **Basic Wireless Settings** tab.

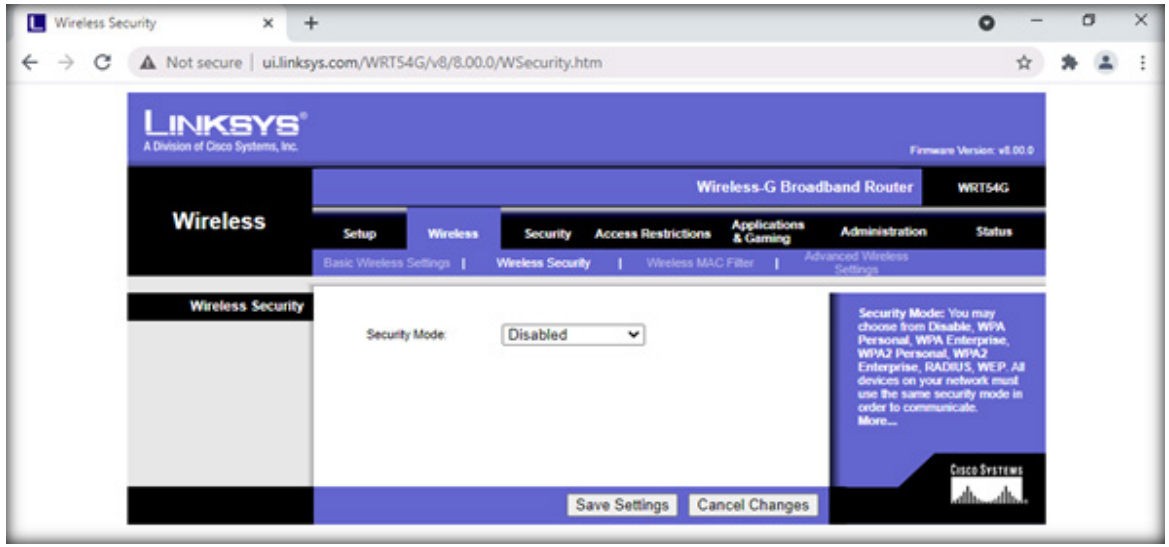
25. Set **Wireless SSID Broadcast** to **Disable**.

EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER



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

EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER

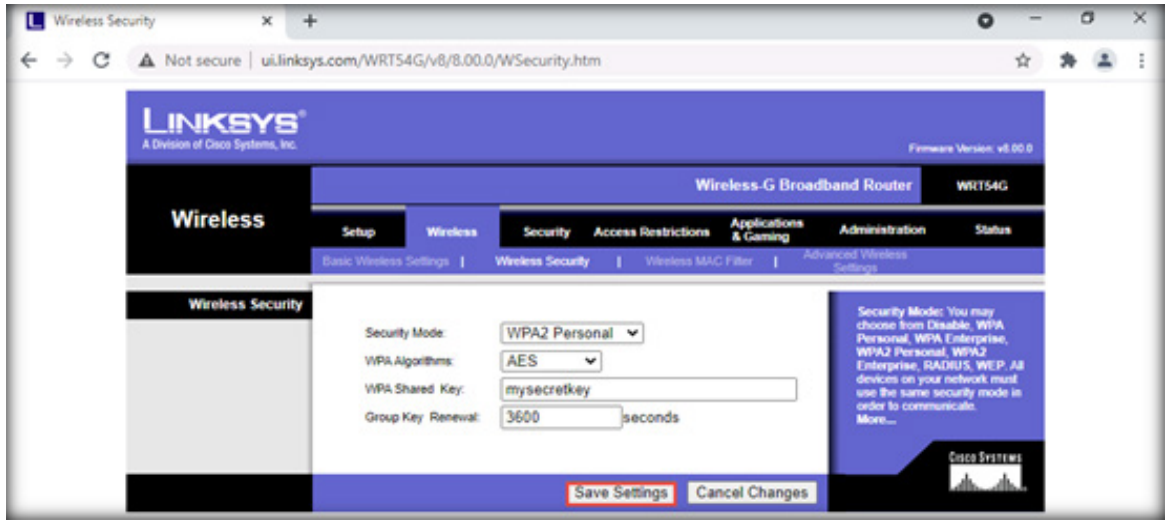


27. Select the strongest and most appropriate encryption mode from the drop-down menu for **Security Mode**.
    Note: Here, we consider **WPA2 Personal** as the strongest encryption mode for wireless security.
    Note: If you are unable to change the **Security Mode**, then follow the steps given below:
    - In the browser window, press **Ctrl+H** to open **History** window. In the left-pane click on **Clear browsing data**.
    - In the pop-up ensure that the **Advanced** tab is selected, and **All Time** is selected from the **Time range** drop down.
    - Ensure that all the options are checked in the Clear browsing data window and click on Clear data to clear all the cookies and cached data.
    - Reload the simulator tab and in the router interface window navigate to **Wireless** tab in the menu bar and click on **Wireless Security** tab. Then, perform **Step#27** again.

28. Select **AES** for **WPA Algorithms** and enter a valid key value in the **WPA Shared Key** field.

29. Click on **Save Settings**.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER

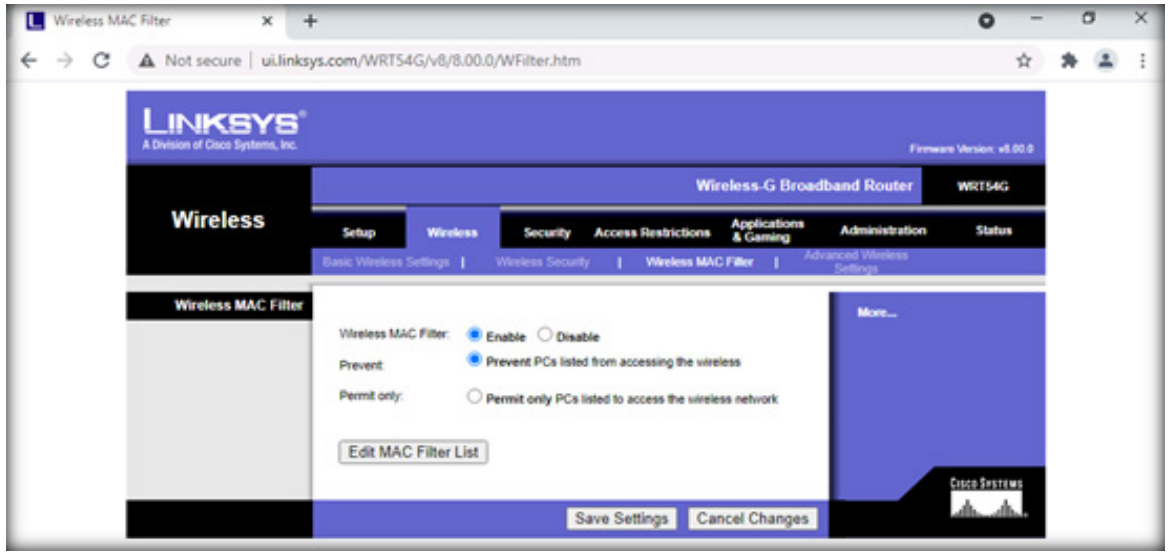


30. A prompt indicating that **Settings are successful** is displayed. Click **Continue**.

31. Click on **Wireless MAC Filter**.

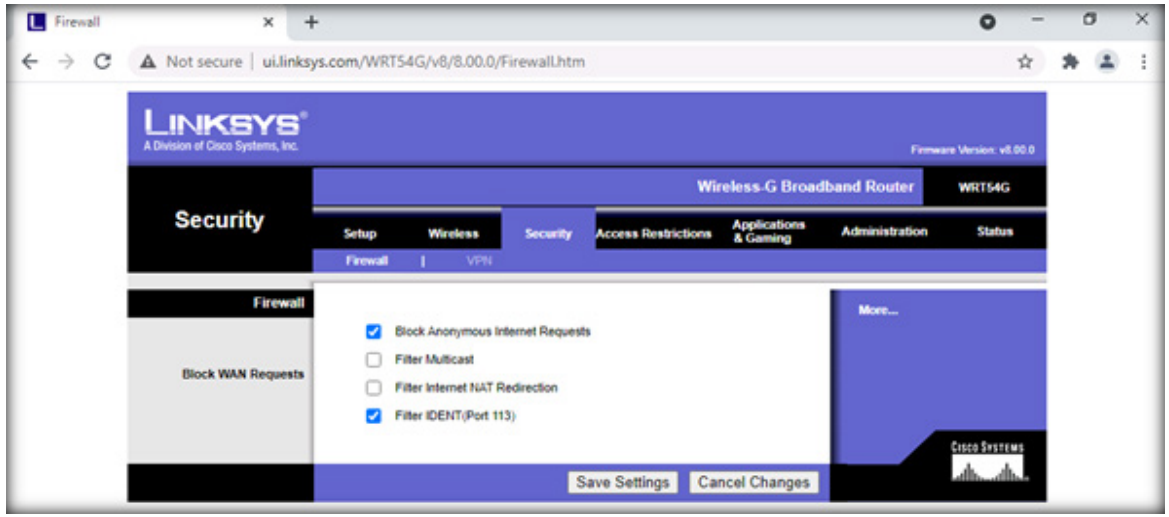
32. Set the **Wireless MAC Filter** option to **Enable**.

EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER



33. Next, go to the **Security** tab to enable firewall restrictions in the router.
    Note: Select the options **Block Anonymous Internet Requests** and **Filter IDENT (Port 113)**.

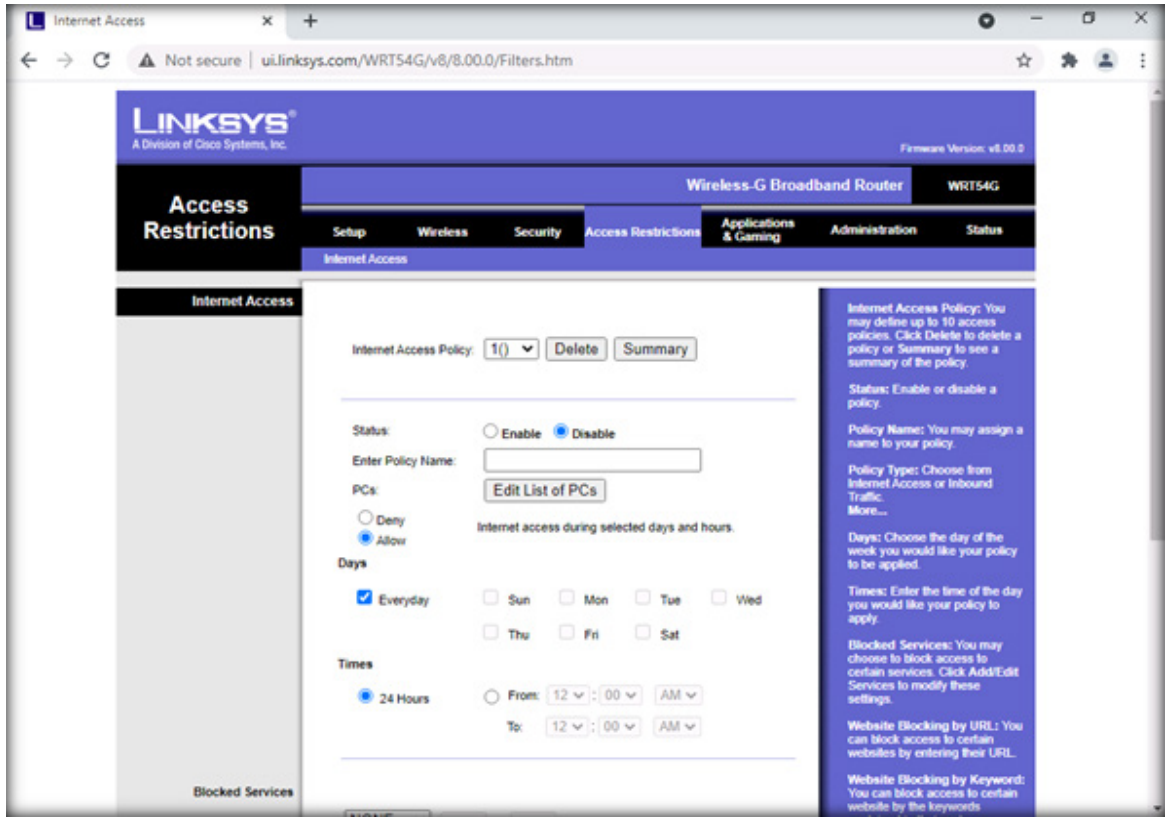
EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER



34. Click on **Access Restrictions**.

35. Next, configure the appropriate internet access restrictions.

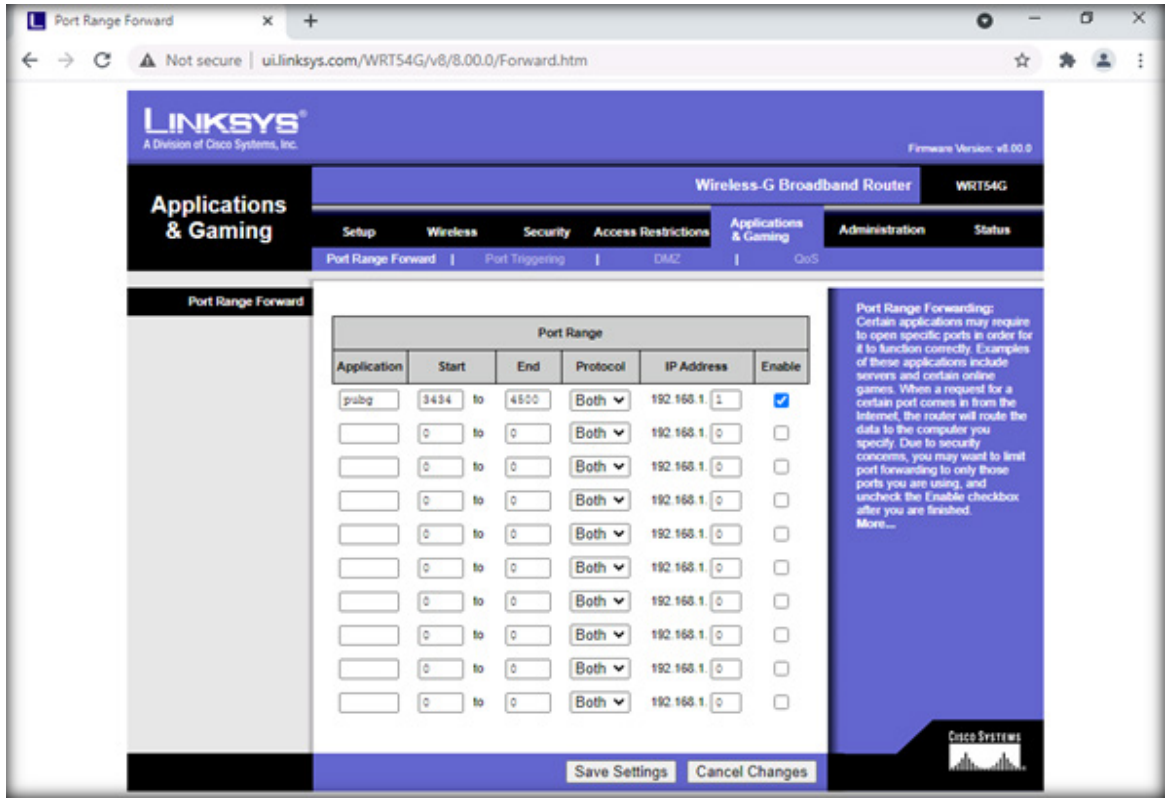
EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER



36. Select **Applications & Gaming** from the main menu. Enter the following details:

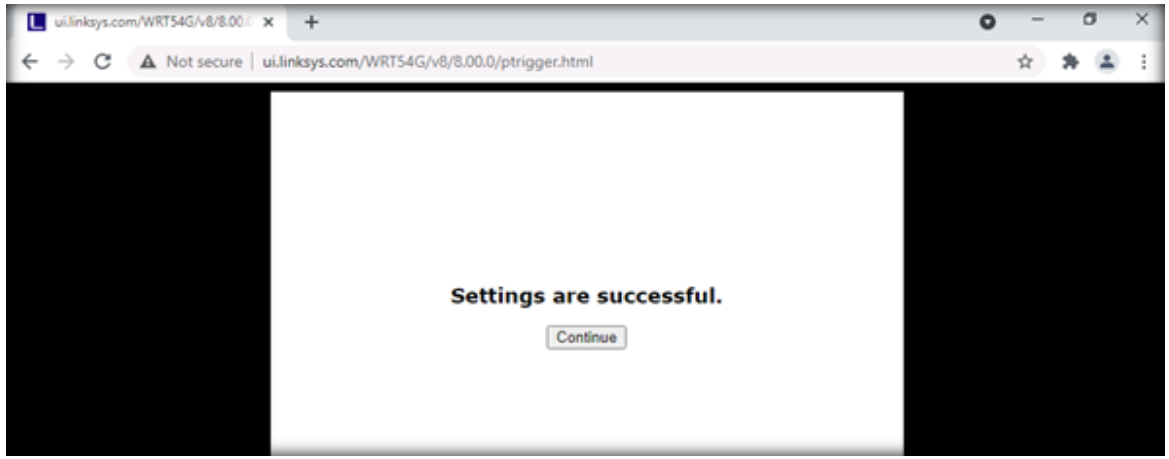
- Application – Enter the name of the program.
- Start / End – Enter the range of ports.
- Protocol – Select either of the protocols or both.
- IP Address – Enter the IP address of the port receiving the port traffic.
- Enable – Enable or disable the port forwarding rule.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER



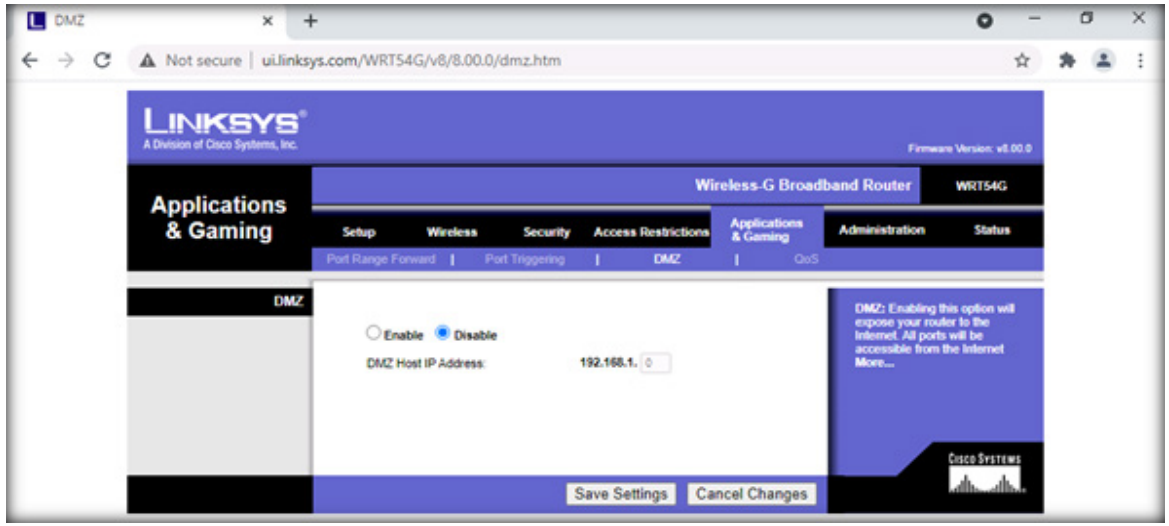
37. Click on **Save Settings**, a prompt indicating that **Settings are successful** will be displayed. Click on **Continue**.

EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER



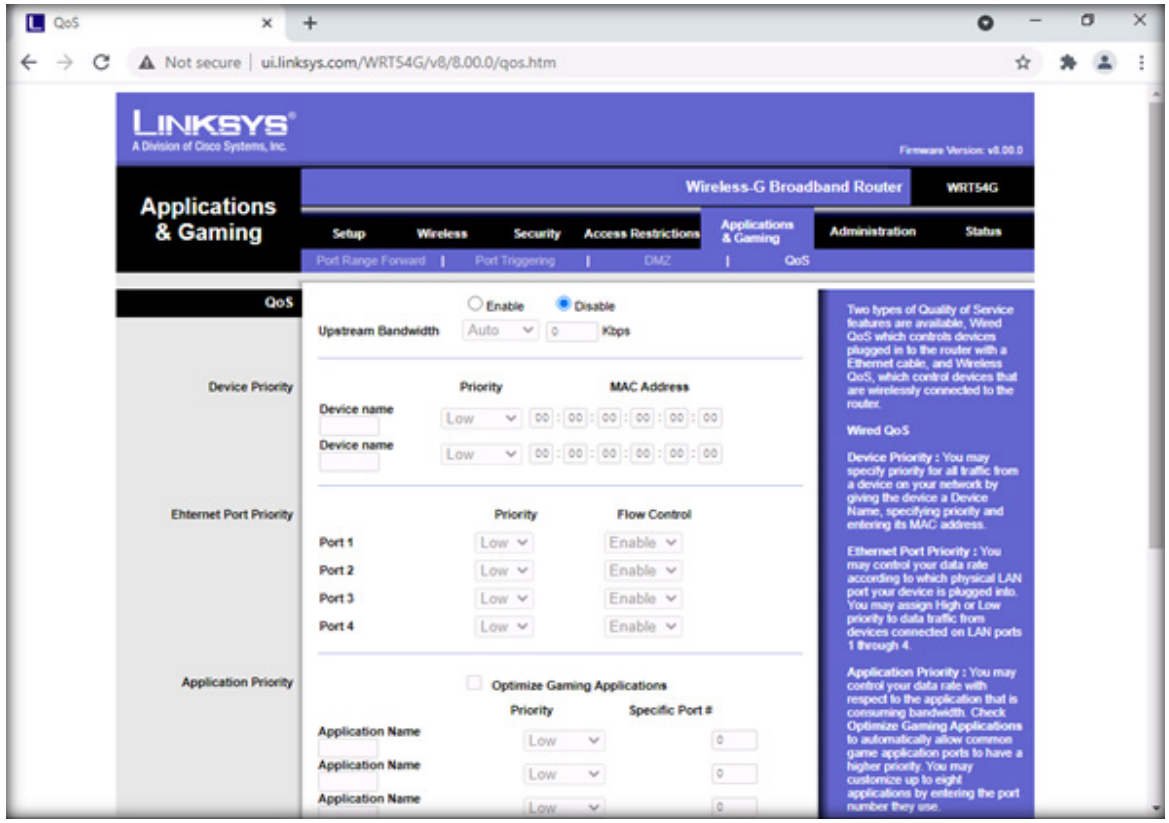
38. Next, click on the **DMZ** tab and set DMZ to **Disable**.

EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER



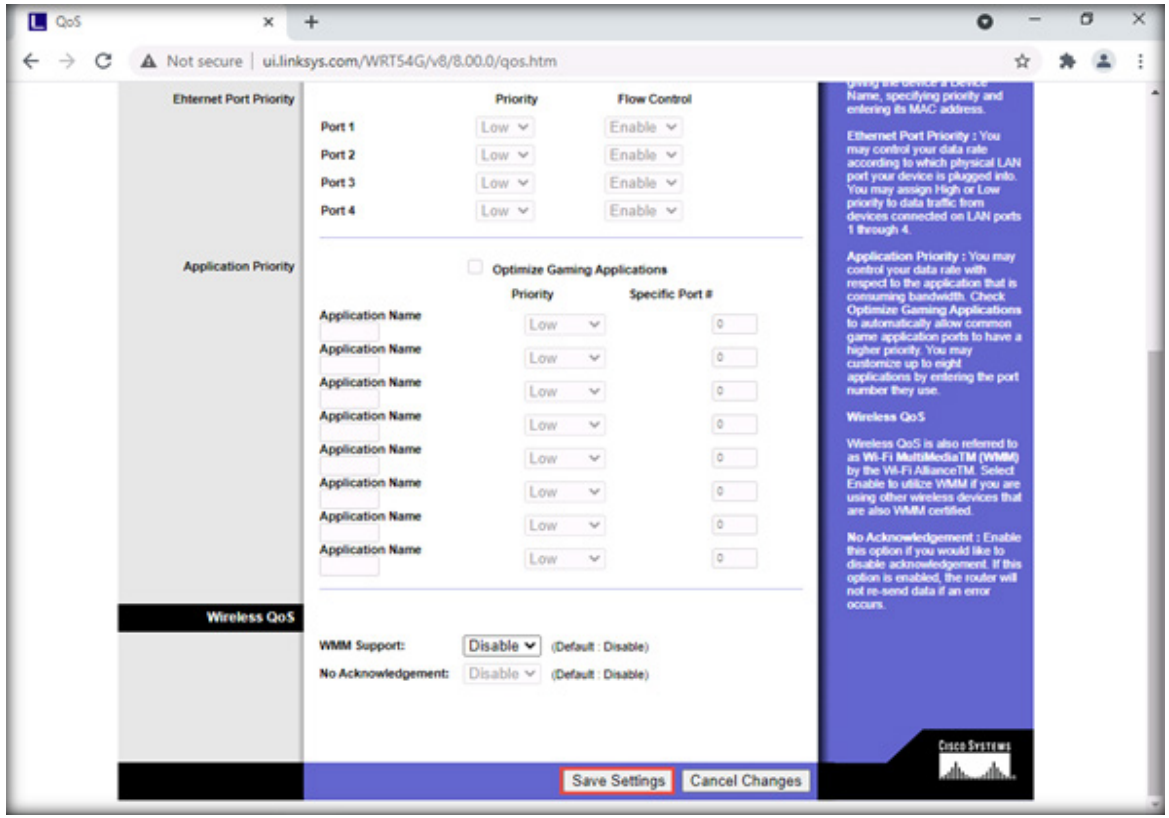
39. Next, click on the **QoS** tab and set QoS to **Disable**.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER



40. Click on **Save Settings** as shown in the screenshot below.

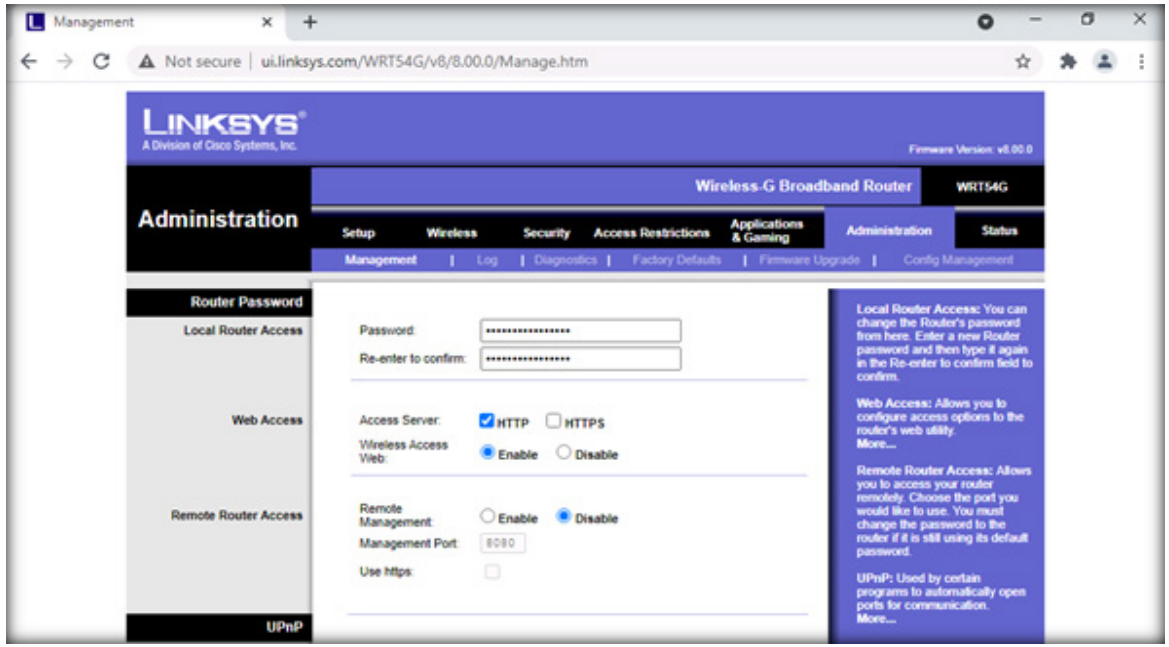
EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER



41. A prompt indicating that **Settings are successful** is displayed. Click on **Continue**.

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

EXERCISE 1:
CONFIGURE SECURITY
ON A WIRELESS
ROUTER



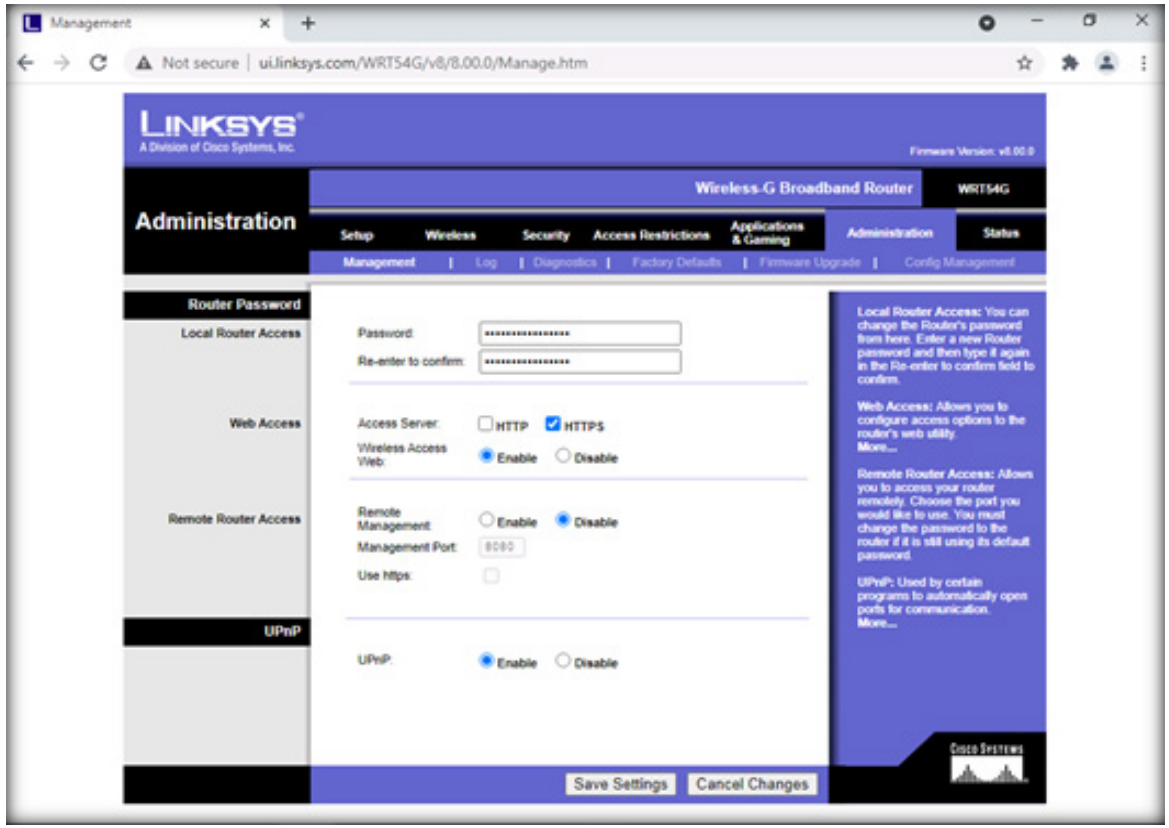
43. In the **Password** field, set a very strong password for a wireless router.

44. Type a new password and re-type it in the **Re-enter to Confirm** field.
    Note: Passwords should be changed periodically to restrict unauthorized access to the wireless network

45. Next, in **Web Access**, set **Access Server** to **HTTPS**.

46. In **Remote Router Access**, set **Remote Management** to **Disable**.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER

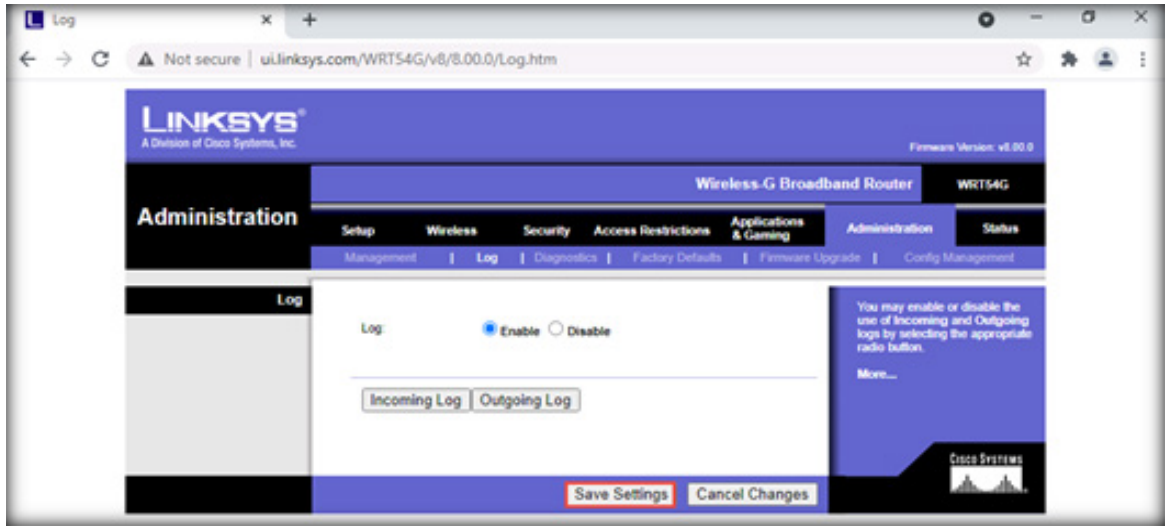


47. Click on the **Log** tab under **Administration**.

48. Set Log to **Enable** as shown in the screenshot below.

49. Click on **Save Settings**.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER

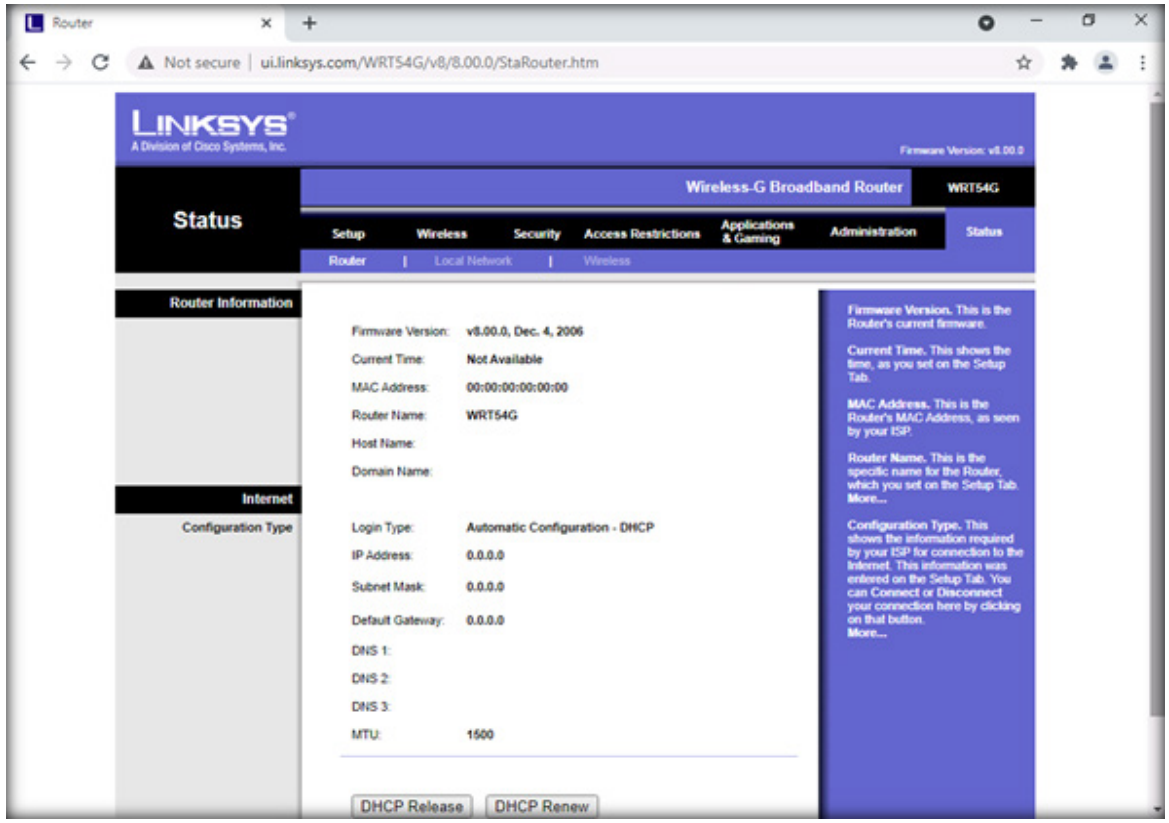


50. A prompt indicating that **Settings are successful** is displayed. Click on **Continue**.

51. Next, click on **Status** from the menu bar.

    Note: As it is a simulation task explaining the configurations on the router page so the settings that have been shown in this task, will not get saved.

EXERCISE 1: CONFIGURE SECURITY ON A WIRELESS ROUTER



52. As described above, a security professional can make configuration changes in the wireless router interface to secure the wireless router.

53. Close all open windows.

54. Turn off **AD Domain Controller** and **PfSense Firewall** virtual machines.


EC-Council