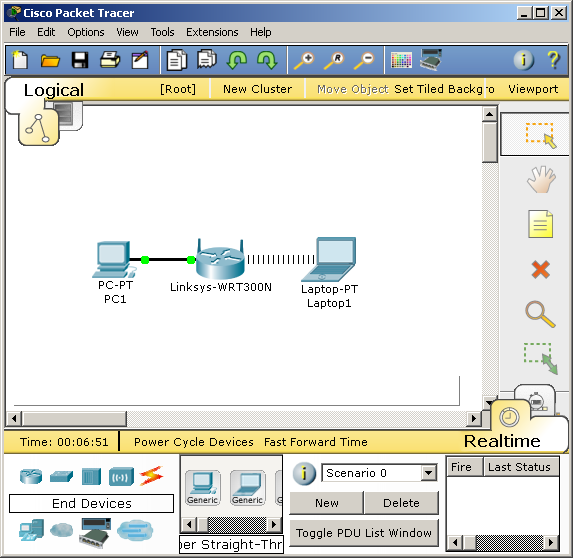


CCNA Discovery

Networking for Home and Small Businesses

Lab 7.3.6 Configuring a Wireless Network

Topology



Objective

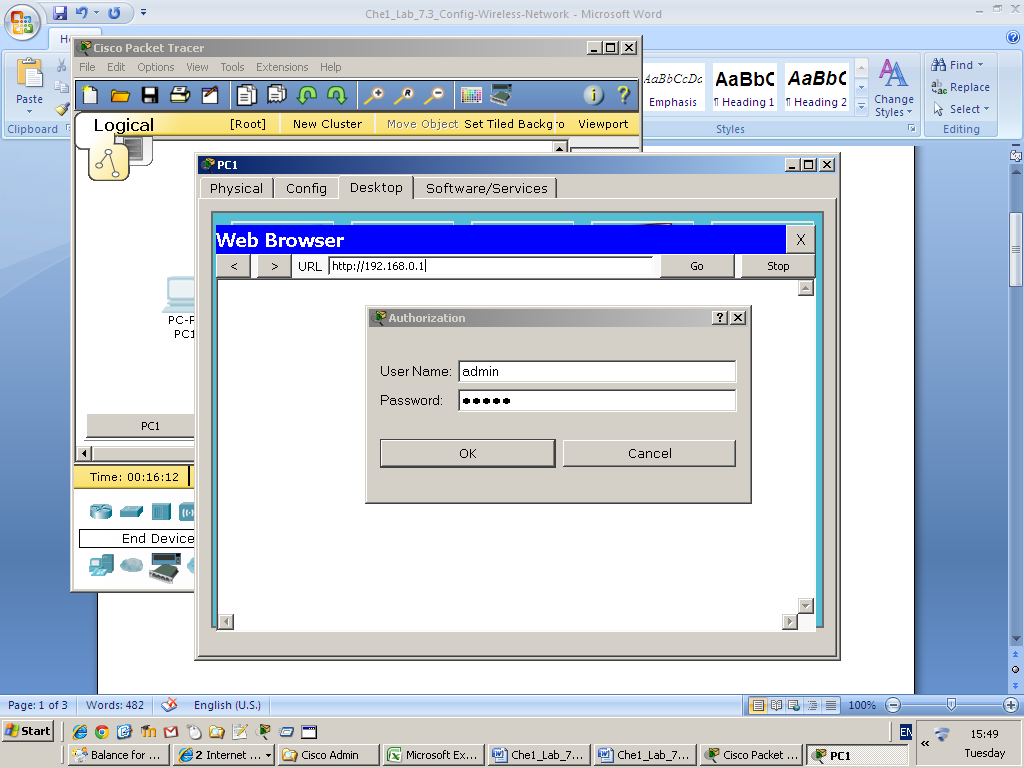
* Configure a wireless router to allow access to a wireless client.
* Configure security on a wireless router

Step 1: Verify connectivity between the computer and the wireless router

1. The computer used to configure the router should be attached to one of the wireless router’s switch ports, such as Ethernet1, with a straighthrough cable.
2. Set the computer to request IP settings via DHCP.
3. Verify these settings with **ipconfig**.
4. At the command prompt, ping the wireless router using the default IP address 192.168.0.1

Step 2: Log in to the wireless router and configure the wireless network

1. Open a web browser. In the address line, type **192.168.0.1**, and press enter
2. At the prompt, the default username is **admin** and the password is **admin**. Click **OK**.
3. Familiarize yourself with the web GUI navigation menus and available features.



Step 3: Connect the laptop to the wireless network

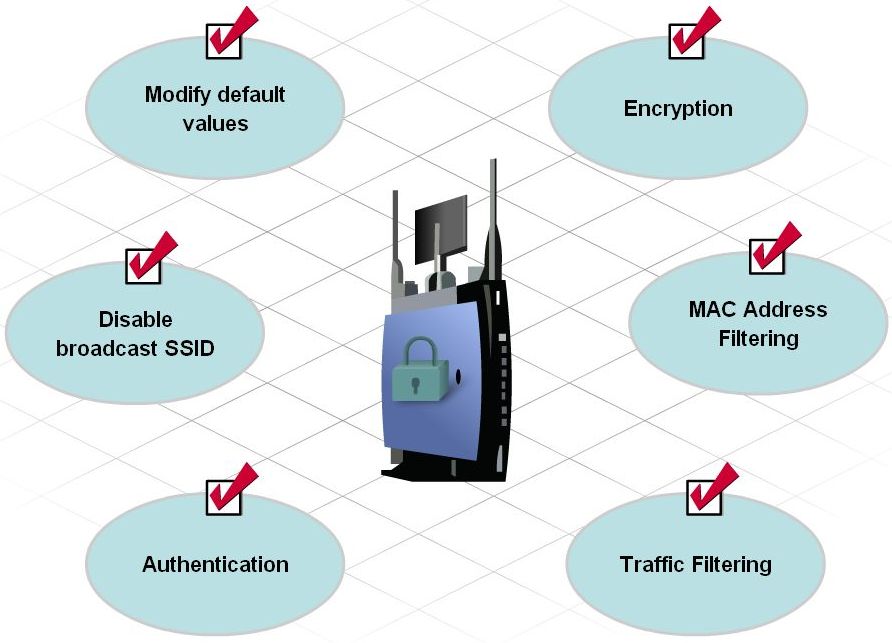
1. By default the PT laptop doesn’t have a wireless NIC, so it is necessary to install one. Power off the laptop, remove the wired NIC, install a Linksys WPC300N card, and power the laptop back on.
2. Use the PC Wireless client software on the desktop to scan for available networks.



1. Connect to the Default network.
2. Verify with **ipconfig** that the laptop has received IP addresses via DHCP from the wireless router.

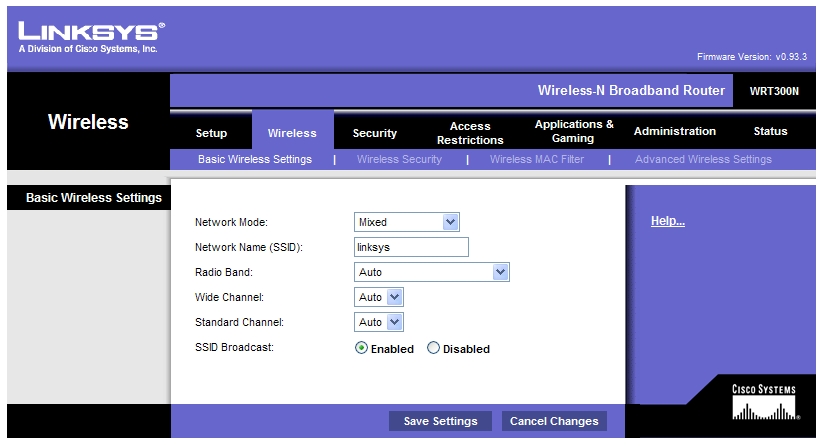
Step 4: Reflection on wireless networking best practices

1. Cisco recommends the following best practices for wireless networking.



Step 5: Modify default values

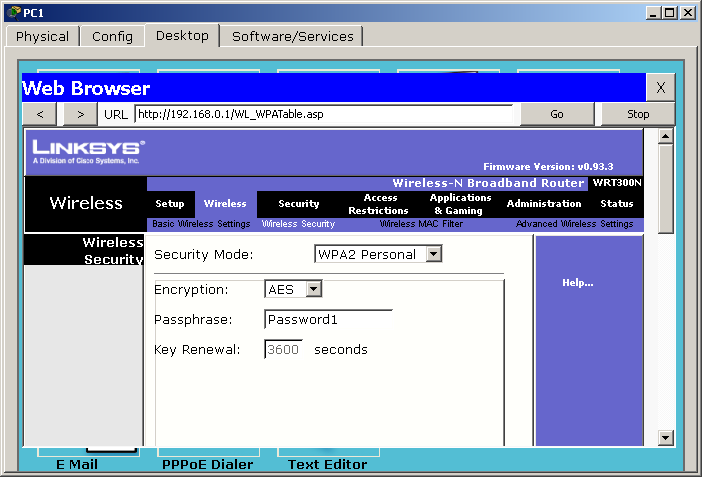
1. On the Wireless menu, change the default SSID to an SSID of your choice.
2. Save Settings.



1. The laptop may have been disconnected after the SSID has been changed. Re-scan and reconnect if necessary.

Step 6: Enable WPA2/AES Encryption

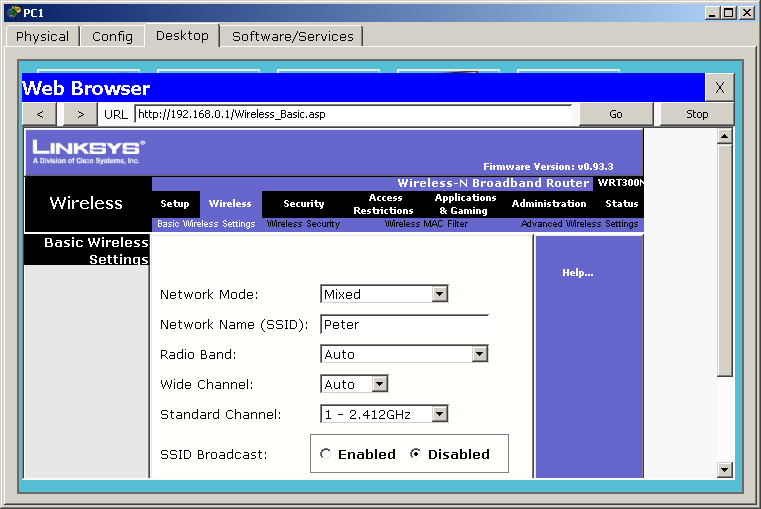
1. On the Wireless > Wireless Security tab, change the Security Mode to WPA2 Personal and choose a passphrase.



1. Save Settings.
2. On the laptop, rescan and re-connect. You will be challenged for the new passphrase.

Step 7: Disable SSID Broadcast

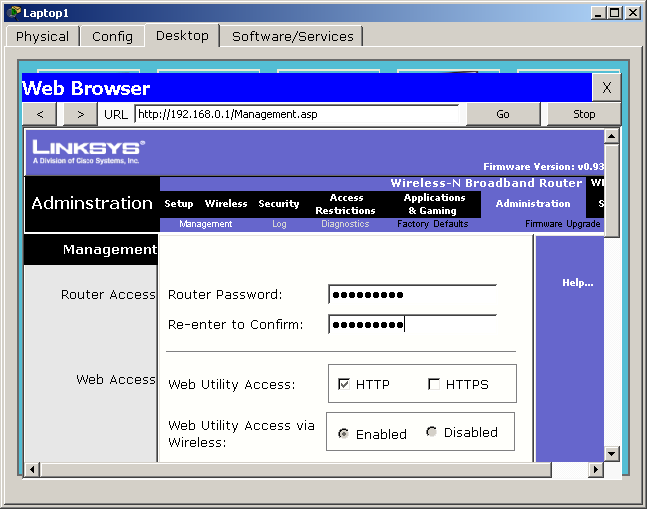
1. **SSID Broadcast** is set to **enabled** by default, which enables the AP to periodically send out the SSID using the wireless antenna. Any wireless devices in the area can detect this broadcast. This is how clients detect nearby wireless networks. This is a security weakness though, as it advertises the existence of your network to the public.
2. To disable SSID broadcasts go to Wireless > Basic wireless settings and select SSID Broadcast > Disable.



1. On the laptop, a rescan will show no networks present. Why?
2. Create a new Profile using the correct credentials to reconnect to the wireless network.

Step 8: Authentication

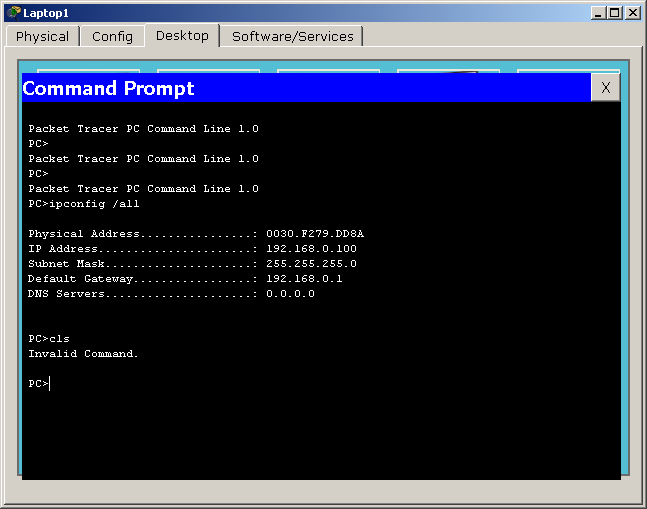
1. By default the Administrator password for the router is **admin**.
2. Go to the Administration tab to change the router password.



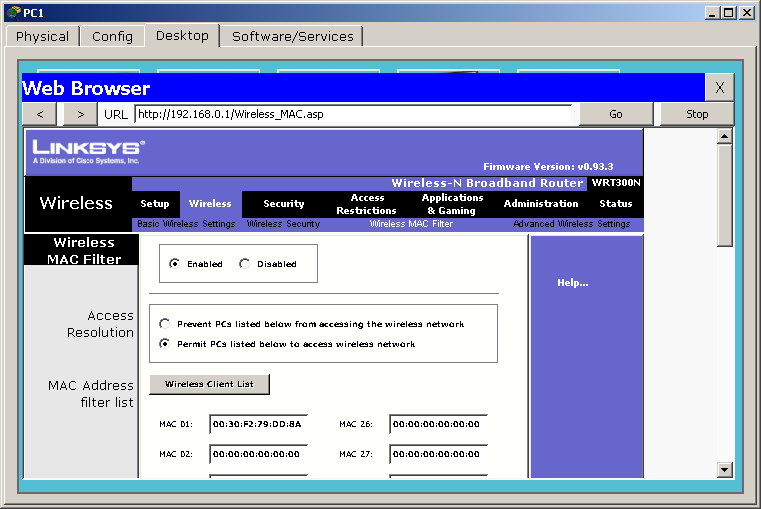
1. Save Settings. You will be challenged for the new router password afterwards.

Step 9: MAC Address Filtering

1. First, identify the MAC address of the laptop using **ipconfig /all**.



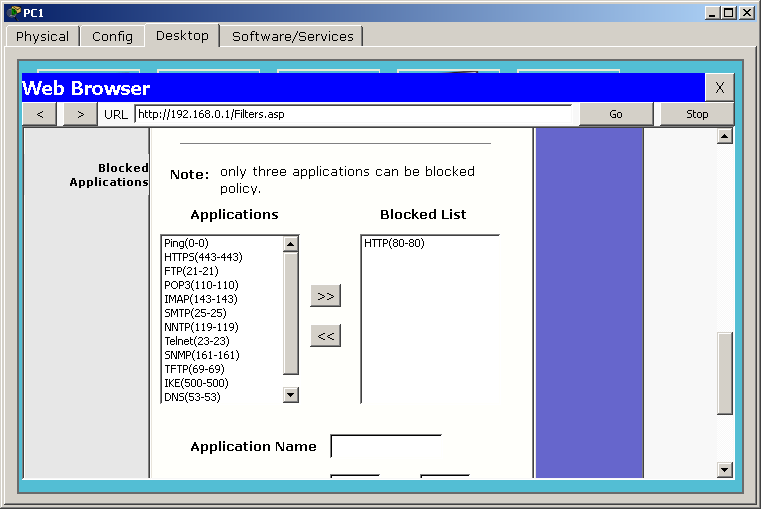
1. On the Wireless > Wireless MAC Filter tab, select enable the MAC Address Filter, select ‘Permit PCs listed below, and enter the MAC address of the laptop.



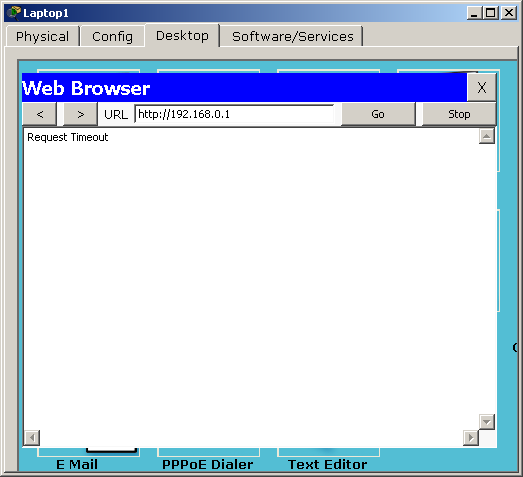
1. Save settings and on the laptop reconnect.
2. You may test the filter by attempting to connect another wireless device to the network. Because its MAC address isn’t on the ‘white list’ of allowed devices it shouldn’t be able to connect.

Step 10: Traffic Filtering

1. It is possible for administrators (or concerned parents!) to filter internet traffic by Protocols.
2. On the Access Restrictions tab, create a new policy **BlockHTTP**, add the IP address of the laptop to the ‘black list’, and move the HTTP application to the blocked list.



1. Save Settings.
2. From the laptop, access to any web pages, such as the wireless router’s GUI, should be blocked



Step 11: Reflection

1. Which feature that you configured on the Linksys WRT300N makes you feel the most secure and why?

The MAC access restrictions makes me feel more secure about the network, because you can be fully assured that the only devices that can gain access to the network are the devices In which you have typed in the MAC address for.

1. Make a list of other items that could be done to make your network even more secure.

One method which could be used is implementing a VPN, which allows the user to secure their traffic. You could use VPN’s to encrypt your traffic from prying eyes and you could also use it to remote access work from home.

Another method is to change the routers default login credentials. This is essential to do, because a hacker could simply get the login details from the manufacturers guide online and crack your router.

Make sure that the routers firmware is up to date. You should check the manufacturers website and see if there is any new firmware for your device then install the firmware. You should do this regularly.

Another method is to set up the firewall on the router. This allows you to block any ports which you don’t need to use. You can also restrict what traffic your computer receives and what traffic your computer sends off.