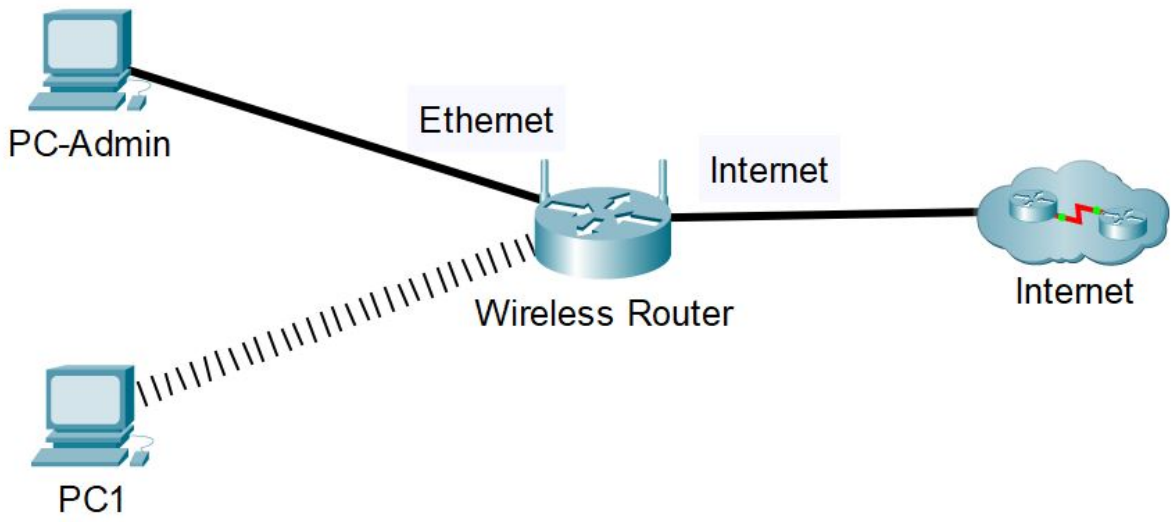
Dimero, Bernard T.
Go, Aldrich Matthew S.
Lim, Shaun Tristan Y.
Bolima, Dave Aldwin D.
Talaban, Brylle Marco B.

Lab 5.1 - Configure a Basic Wireless Network (F2F)



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Wireless Router	Internet	172.16.4.10x	255.255.255.0	172.16.4.5
	LAN	10.1.0.1	255.255.255.0	N/A
Admin-PC	NIC	DHCP Enabled		
PC1	NIC	DHCP Enabled		

Objectives

- Configure basic network settings on a wireless router
- Configure wireless settings and wireless devices
- Add an AP to the network to extend wireless coverage
- Reset to the Default Settings

Recommended Equipment

- A Windows computer with wired adapter
- A Windows computer with a wireless network card or USB adapter installed
- Wireless router
- Ethernet patch cables

Introduction

In this activity, you will configure a wireless router to accept wireless clients and route IP packets. Furthermore, you will also update some of the default settings.

Instructions

Part 1: Configure Basic Network Settings on a Wireless Router

This lab uses a Linksys WRT series wireless home router. In this section, you will go through the motions of connecting to a new wireless router using a wired host and accessing its web GUI for configuration. Menu paths may be different if you are assigned a different router model. Consult your instructor if you need help finding equivalent settings on a different router model.

Step 1: Reset the router to factory settings

Reset the wireless router to factory settings. To do so, use a pen or pencil to hold down the reset button for a few seconds until the router power LED turns off then release the button.

Step 2: Connect a management host to a wireless router.

Connect **Admin-PC** to any of the Ethernet ports of the **Wireless Router** using a straight-through cable through the Ethernet ports.

The wireless router will act as a switch to the devices connected to the LAN and as a router to the internet. **Admin** is now connected to the LAN

Step 3: Configure Admin to use DHCP.

To reach the **Wireless Router** management page, **Admin** must communicate on the network. A wireless router usually includes a DHCP server, and the DHCP server is usually enabled by default on the LAN. **Admin PC** will receive IP address information from the DHCP server on the **Wireless Router**.

a. Set the **Admin PC** LAN Connection to acquire its IP settings using **DHCP**.

b. Open a command prompt on the computer. Using the **ipconfig** command, identify the NIC used for the connection to WR and gather the following information:

What is the IP address of the computer?	192.168.1.114
Which is the subnet mask of the computer?	255.255.255.0
What is the default gateway of the computer?	192.168.1.1

c. Take note of the gateway address. This is the default IP address of the **wireless router**.

Step 4: Connect to the Wireless Router Web Interface.

a. Open a browser on **Admin-PC**

b. Enter **the address of Wireless Router** in the URL field to open its web configuration page of.

c. If prompted with a login, leave the username blank and use 'admin' for the password .

You will be in the Basic Setup page by default where basic network settings are shown.

Step 5: Change the WR Access Password.

a. Navigate to **Administration > Management** and change the current **Router Password** to **cisco**.

b. Scroll to the bottom of the window and click **Save Settings**.

c. Use the new password **cisco** when prompted to log in to the wireless router. Click **OK** to continue.

Step 6: Configure the Internet Port of the Wireless Router.

When connecting to an ISP or any external network, the Internet port of the wireless router needs to be configured with address settings assigned by the external network. In this step, the wireless router is configured to route the packets from the wireless clients to the Internet. You will configure its **Internet** port **t**o connect to the internet through the lab gateway.

a. Navigate back to the **Basic Setup** page. Under the **Internet Setup** section at the top of the page change the Internet IP address method from **Automatic Configuration – DHCP** to **Static IP**.

b. Type the IP address to be assigned to the Internet interface as follows:

Internet IP Address: 172.16.4.10x (Replace 'x' with your group number)

Subnet Mask: 255.255.255.0

Default Gateway: 172.16.4.5

DNS Server: 8.8.8.8

Step 7: Configure the LAN Port of WR.

IP addressing of the local network may be configured as well. A typical wireless router supports static and dynamic addressing for the LAN. In this step, you will customize the DHCP settings of the Wireless Router for LAN clients

a. Under the **Network Setup** section of the **Basic Setup** page, configure the following LAN settings:

Router IP Address: 10.1.0.1

Subnet Mask: 255.255.255.0

DHCP Server: Enabled

Start Address: 10.1.0.10

Maximum Number: 20

b. Scroll down the page and click **Save**. You will be disconnected from the router after this since you have changed its IP address.

c. You will need to change the IP settings of **Admin-PC** so that it uses an address from the new LAN subnet. Assign the following static IP address settings to the Admin-PC:

IP Address: 10.1.0.10

Subnet Mask: 255.255.255.0

Default Gateway: 10.1.0.1

DNS Server: 8.8.8.8

d. Test connectivity of PC-Admin to the router using a ping.

Was the ping successful?	Yes

e. Test connectivity of PC-Admin to Internet hosts. Ping **www.dlsu.edu.ph**.

Was the ping successful?	No

Part 2: Configure Wireless Settings and Connect Wireless Devices

The WLAN functionality is enabled by default for home wireless routers. It is always good practice to customize settings for security purposes.

Mobile clients may be connected to a wireless LAN by adding a wireless NIC and configuring wireless and security settings to match those configured for the network.

Step 1: Configure the WR SSID.

In this step, you will only configure the wireless settings of the Wireless Router for 2.4 GHz.

a. Navigate the router GUI interface to **Wireless > Basic Wireless Settings**. Set the following configurations.

Network Mode: Mixed

Network Name (SSID): 'LabGrpX' (replace X with your group number)

b. Scroll to the bottom of the window and click **Save Settings**.

Step 2: Configure wireless security settings.

In this step, you configure the wireless security settings using WPA2 security mode with encryption and passphrase.

a. Navigate to **Wireless > Wireless Security** and configure security settings:

Security mode : **WPA2 Personal** (WPA2-PSK on some router models)

Encryption : **AES**.

Passphrase : **Cisco123!**

b. Click **Save Settings**.

c. Verify that the settings in the **Basic Wireless Settings** and **Wireless Security** pages are correct and saved.

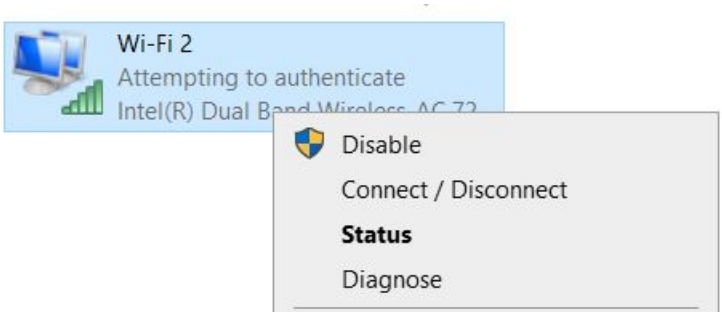
Step 3: Prepare a client for wireless connectivity

a. Connect the USB wireless adapter to **PC1**.

b. Under **PC1 Network and Connection Settings → Change Adapter Options**, a new interface should appear among the available network connections of the PC.

Step 4: Connect a client wirelessly

a. Right click on the new interface and click **Connect / Disconnect**. A list of SSIDs of nearby wireless networks should pop up from the taskbar.



b. Select the SSID that belongs your group. Enter the passphrase configured (**Cisco123!)** when prompted and wait for the wireless network connection to be established.

c. Using the command prompt, identify the IP settings assigned by the wireless router to PC1:

d. Test connectivity of wireless devices to local network hosts. Using PC1, ping the Admin PC.

Was the ping successful?	Yes

e. Test connectivity of wireless devices to Internet hosts, Using PC1, ping **www.dlsu.edu.ph**.

Was the ping successful?	No (works via http but not ping)

Part 3: Add an AP to the Network to Extend Wireless Coverage (Optional)

In this part, you will add a wireless access point (AP) to the network. An AP is connected directly to a wireless router using an Ethernet cable. The purpose of an AP is to extend the wireless LAN where the wireless users cannot reach the wireless router otherwise.

In this part, you may need to partner with another group with a wireless router that can be converted to an access point. Or your instructor may also provide an access point. Unless instructed to connect the wireless router the internet, you do not need to connect the Internet port of the wireless router to a cable or DSL connection.

Note: If you are converting a wireless router to an AP, please follow the instructions provided by your instructor or manufacturer's documentations.

Step 1: Connect the access point to the wireless network.

a. Disconnect the cable connecting the Internet port of the 2nd wireless router. From here on, this device will be referred to as ‘access point’.

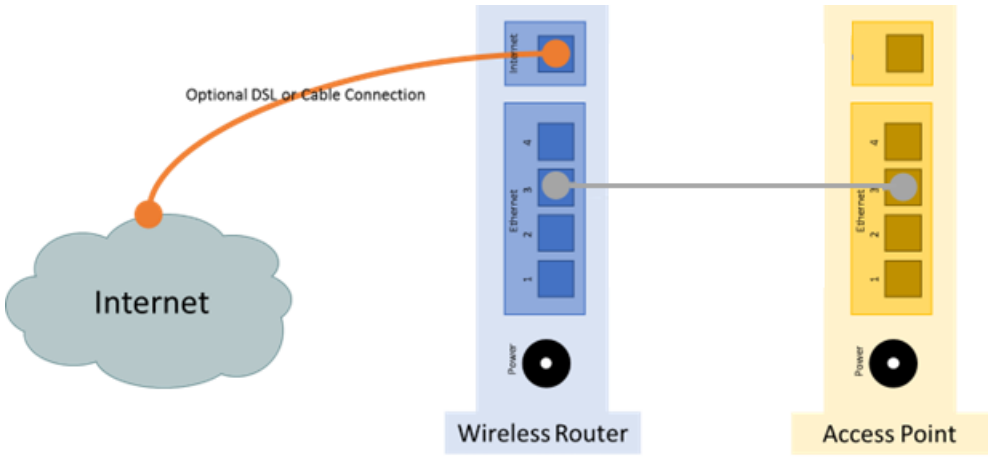
b. Transfer the connection of PC-Admin to the any Ethernet port of the access point.

c. Using PC-Admin’s browser, connect to the administrative GUI of the access point. Log in through the administrator account to access the Network Setup section under its Basic Setup menu and change its LAN IP address to **10.1.0.2.**

d. Under the same page, disable its DHCP service.

e. Save the settings and reconnect to its GUI using its new IP address.

f. Connect one of the LAN ports of the access point to one of the LAN ports on the existing wireless router.



Step 2: Configure access point wireless settings.

a. Navigate to the Wireless settings menu of the access point..

b. In the Basic Wireless Settings, configure the AP with the same SSID used by the wireless router

c. To prevent interference, change the wireless channel from the default channel 1 to channel 6 or 11. Save the new settings.

d. Under the Wireless Security menu, set the same security options as the wireless router. For example, **LabGrp1** as the SSID and WPA2 Personal AES with **Cisco123!** as the passphrase.

e. Verify that the wireless router and AP are not using the same wireless channels.

f. Attempt to connect a wireless client to the wireless network.

Step 3: Turn off wireless radio on the wireless router.

After you have successfully connected to the wireless network, you will attempt to disable the wireless router radio, and a wireless client will attempt to connect to the wireless network through the AP.

a. Navigate to the wireless router using a web browser by connecting to its IP address. If necessary, connect to the wireless router using a wired Ethernet connection.

b. Navigate to the basic wireless settings, turn off the wireless router radio by setting its network mode to '**Disabled**' then save the settings.

On other wireless router models, the option to enable wireless radio may be in the advanced wireless settings.

c. Attempt to connect a wireless device to the network then use the command prompt to check for its IP settings.

Were you able to successfully connect to the WLAN and acquire an IP address?	Yes

Part 4: Reset to the Original Configuration

Unless stated otherwise by the instructor, restore the wireless router and access point back to factory default.

a. Navigate to the Administration menu→ Factory defaults

b. Click on the button to revert to factory default settings.

c. Provide your administrative credentials if prompted.

d. Wait for your router and access point to finish rebooting

e. Confirm that settings of both devices are back to defaults before unplugging and cleaning up.

Reflection

Would this method of using wireless routers be a scalable solution to deploy a wide coverage WLAN to a large organization? Why or why not?

A large organization is usually around 250+ employees or more. In this instance, using Aps or WWRs does not seem like a valid method nor a scalable solution to cover a wide WLAN. Wireless connection to begin with is highly unstable especially in high-rise areas with network congestion will pose a severe issue especially with work efficiency.

Whilst the benefits or wireless connection are the less usage of wires and ethernet cables, using wireless connection as a whole in a company does seem more like a downside than it is an upside because of its efficacy and efficiency, its network congestion issues, and its overall lack of resilience and scalability, and a severe risk in security as a whole. This method could be used ot entertain a small amount of users (i.e. Guests WIFI's), but a more valid and secure method is using wired connectivity for work.