Singapore Polytechnic
School of Electrical and Electronics Engineering
ET1205: Wireless Technology Applications

Experiment 04: Setting Up Wireless LAN IEEE 802.11g Access Point using WEP, WAP key in Network Security and Configuring Filters

Objectives:

Students will learn how to

- setup IEEE 802.11g access point with various security settings such as WEP, WPA-PSK, and MAC filtering
- install firewall filtering for restricted access.

Introduction:

We have learnt how to setup the Wireless LAN client on the laptop using both Windows 7 and Planex Wireless Utility client software in Experiment 3. While, IEEE 802.11 Wireless LAN provides convenience and flexibility to users, on the other hand, it may allow hackers to access the network and eavesdrop on the data transmitted on the network.

In this experiment, we will configure the access point for various security configurations.

Procedure:

A. Setting up IEEE 802.11g Wireless LAN access point with WEP security

1. Power up the Netgear wireless access point and press and hold the reset button at back of the router for 30 seconds to make default setting.
2. Connect the Ethernet **straight** UTP-5 cable from your laptop RJ-45 port to **one of the four ports** on your NetGear access point. (You also need to connect another **straight** UTP-5 cable from the Ethernet RJ-45 port on your access point to either your cable modem or ADSL modem. **This step is skipped in this experiment**.)
3. Configure your Local Area Connection to a dynamic IP address. Click on Start → Control Panel and click on View network status and tasks at Network and Internet section to open the Network and Sharing Center. Click on the Change adaptor settings. Select Local Area Network Connection and right-click on the Local Area Connection and select Properties. Select Internet Protocol Version 4 (TCP/IPv4) and click on Properties button. Select "Obtain an IP Address automatically" .
4. Go to start and run CMD program. Then, type "ping 192.168.0.1" (sliver color) or "ping 192.168.1.1" (white color) to check the connection to the router whether it is OK
5. Launch the Internet Browser to the following URL: http://192.168.0.1/start.htm (for sliver color NetGear access point), http://192.168.1.1/start.htm (for white color NetGear access point).
6. If prompted for login, use username: **admin** and password: **password**.
7. Click on the *Setup Wizard*. Choose "No. I want to configure the router myself". Click "Next" button as shown in Figure 1 below.

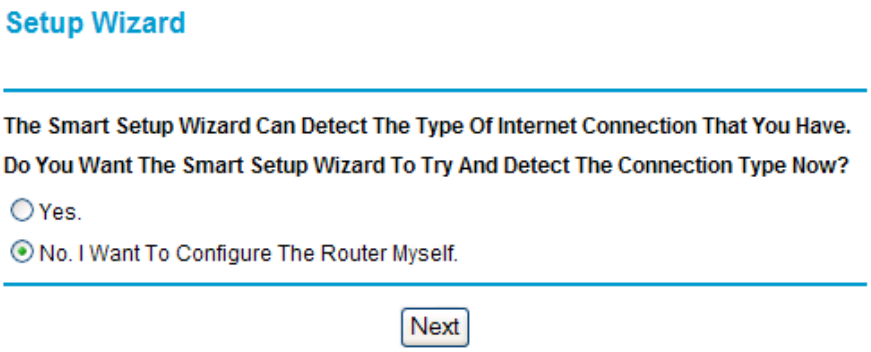

Figure 1

8. Click on the *Basic Settings* and then click "Apply" button to initialize the assess point.
9. Click on the *Wireless Settings* and configure the following parameters:
   - Name (SSID): WCL-XX where XX follows the number on the access point.
   - Country: United States
   - Channel: Select any channel no. from 1 to 13 except channel 1, 6 or 11
   - Mode: g only
   - Security Options: Disable
   - Click "Apply" button.
10. Click on the *Advanced Wireless Settings*. Ensure that both "Enable Wireless Router Radio" and "Enable SSID Broadcast" are checked. Click "Apply" button.
11. Click on the *Advanced LAN IP Setup*. Change the IP Address of the router to 192.168.1XX.1, Starting IP Address to 192.1XX.2 and Ending IP Address to 192.1XX.100 where XX follows the number on the access point. Click "Apply" button.
12. Change the Security Options to WEP (Wired Equivalent Privacy) in the *Wireless Settings*.
13. There are two ways to enter the WEP key. You can choose to use a 64-bit or 128-bit encryption key or to enter a passphrase.
14. In this lab, we choose "64-bit" encryption key and passphrase "wireless". Click "Generate" button and copy the generated 10 digit Hex key. Then, click "Apply" button.
15. **Disconnect** the Ethernet straight UTP-5 cable
16. **Disable** the built-in wireless LAN adaptor and **plug-in** Wireless Mini-USB Adaptor to the laptop and change your client settings using the **Planex Wireless Utility** client software.
17. **Connect** your Wireless Mini-USB Adaptor client to the new access point (WCL-XX).
18. Once connected, launch Internet Explorer browser to access http://192.168.1XX.1/start.htm where XX follows the IP of the access point.

B. Setting up IEEE 802.11g Wireless LAN access point with WPA-PSK security

1. On the access point, change the Security Options to WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) in the *Wireless Settings*.
2. Enter the passphrase and the key lifetime. (Note: This was applicable only for white color model.)
3. In this lab, we choose "wirelesslan" and the key lifetime to be "60" minutes (Only for White color Router). Click "Apply" button.
4. Change your client settings using the **Planex Wireless Utility** client software.
5. Connect your Wireless Mini-USB Adaptor client to the new access point (WCL-XX).

6. Once connected, launch Internet Explorer browser to access http://192.168.1XX.1/start.htm.

a. Setting up IEEE 802.11g Wireless LAN access point with MAC address filtering

1. MAC address filtering can be applied together with any of the above security settings.
2. On the access point, click on the *Advanced Wireless Settings*. Click on "Setup Access List" button.
3. Click on the "Add" button in Figure 2. Check the MAC address of the Wireless Mini-USB Adaptor and click "OK" button.
4. Check the checkbox "Turn Access Control On" and click "Apply" button, as shown in Figure 2 below.

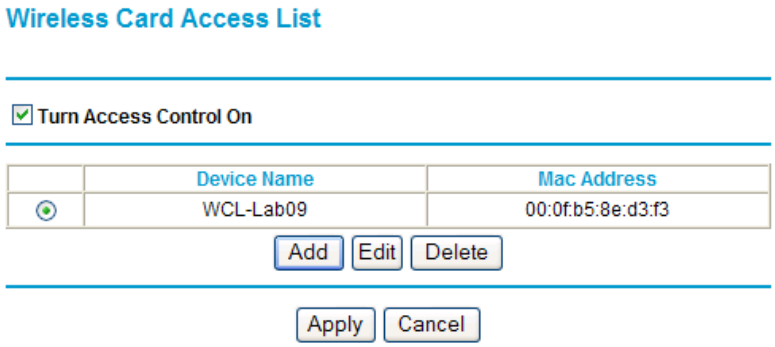

Figure 2

5. This will prevent wireless devices other than the list of MAC addresses shown from accessing the access point.
6. Launch Internet Explorer browser to access http://192.168.1XX.1/start.htm.
7. Change the MAC address to something other than your Wireless PC card.
8. Launch Internet Explorer browser to access http://192.168.1XX.1/start.htm. You should not be able to access this webpage now.

D. Setting up firewall rules

1. WEP, WPA-PSK and MAC filtering security features mentioned above are security features to establish physical connection between access point and clients.
2. Firewall rules for restricted or no access to certain websites for the clients. In NetGear access point, this firewall feature is known as *Block Sites*.
3. In Figure 3, enter the keywords for websites that you would like to block, either permanently (always) or per schedule, as determined in *Schedule*. For example, to block users from accessing http://www.google.com, enter the keyword google.

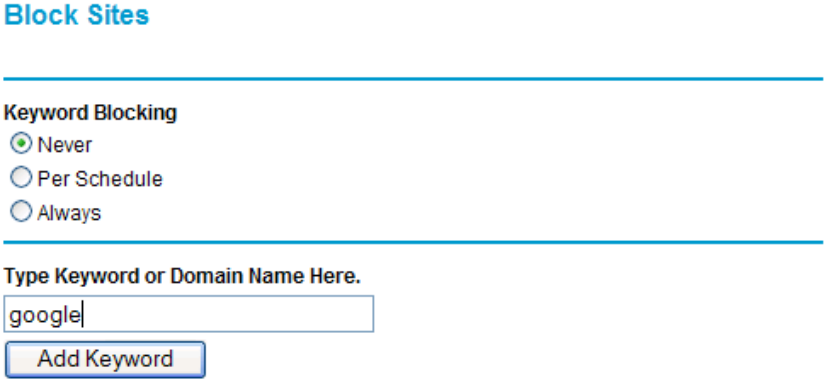

Figure 3

4. Firewall rules can also be applied to restrict certain services or ports on the clients. In NetGear access point, this firewall feature is known as *Block Services*.
5. In Figure 4, click on "Add" button. Enter the starting port number and the ending port number. For example, to prevent users from accessing https service, enter starting port 443 and ending port 443.

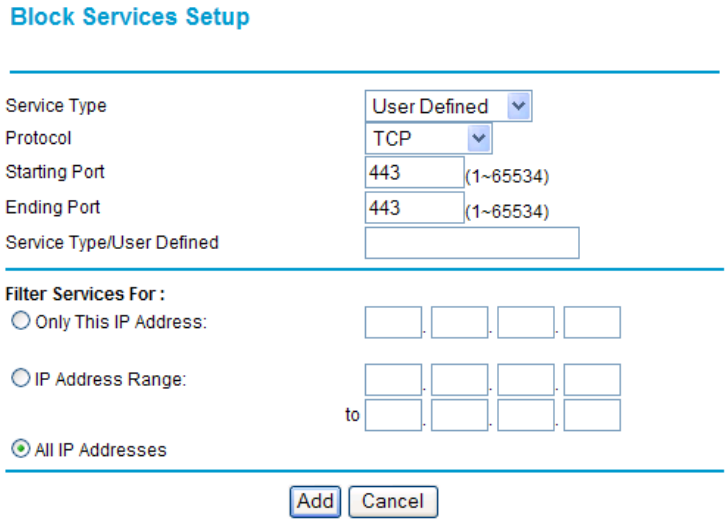

Figure 4

6. You are required to connect the access point to an Internet outlet in order to test out these two firewall rules.

E. Questions

1. What are the non-overlapping frequency channels in Singapore for IEEE 802.11g?

   _____

2. Which security method do you used to enforce the strictest security for the access point?

   _____

3. What is the difference between these two network types: access point (infrastructure) and computer-to-computer (ad-hoc)?

   _____

4. Click on the **Add Profile** button in the **Planex Wireless Utility** client software and select the **System Config** tab.

   a. What is the use of the RTS/CTS Threshold setting?

   _____

   b. What is the use of the Fragmentation Threshold setting?

   _____

i. Conclusion

_____, _____ and _____ filtering are used to enhance the security on the physical connection and _____ rules are used to restrict access based on keywords or port numbers.