Wireless LANs

Birzeit University
Faculty of Information Technology
Computer Systems Engineering Department

April 21, 2010

Abstract

This experiment aims at examining Wireless LANs, or for short WLANs. We are going to examin two modes of wireless networking defined by IEEE 802.11: Insfrastrucre and Infrastructureless, commonly known as ad hoc, WLANs. Whereas the later constitues a peer-to-peer network in which the wireless clients communicate directly with each other without involving access points, the former needs a central access point to coordinate communication. In the infrastrucre mode, we are going to examine multiple operating modes such as access point mode, repeater mode, and bridge mode. The access point mode is the default and commnoly used mode in which wireless clients connect to a central authority, namely access point. The repeater mode, on the other hand, is used to extend the range of a WLAN formed by an access point in its default mode. The final mode to be examined is the bridge mode in which two physically separated LAN segments can be wirelessly connected using two access points configured as bridges.

Contents

Part I
Theoretical Introduction

In this part you will be introduced to the theoretical concepts of the experiment. From the outset, you should be aware that the Technical Part constitutes a complementary part you will need to assimilate before delving into the Practices.

A wireless standard (e.g. 802.11) typically defines, a *wireless station* equipped with wireless NIC, and an access point (AP), which bridges the communication between the wireless and wired networks. For the access point to be able to act as a bridge between the wireless and wired networks, it usually consists of a wired network interface (e.g., 802.3), and bridging software conforming to the 802.1d bridging standard. Playing such a role, the access point acts as the *base station* for the wireless network, aggregating access for multiple wireless stations onto the wired network.

Two modes of networking are defined under 802.11 standard: infrastructure and infrastructure-less, which is commonly knows as ad hoc, modes. The wireless network in the infrastructure mode consists of at least one access point connected to the wired network and a set of wireless end stations. Ad hoc mode which constitutes a peer-to-peer network, is a set of 802.11 wireless stations communicating directly with one another without using an access point or any connection to a wired network. Such a mode is useful for quickly and easily setting up a wireless network with the absence of any wireless infrastructure.

1 Ad hoc Mode

The dictionary meaning of ad hoc revolves around "an unplanned economy;" that is, it accepts an unplanned order. In computer networking, the 802.11 standard specifies "ad hoc" mode, in which the wireless clients, given that they are in the range of each other, communicate directly in a peer-to-peer (P2P) fashion without involving central access points. Figure 1 depicts an arbitrary ad hoc network.

Figure 1: Ad Hoc WLAN

The lack of a central authority, namely access point, has its own advantages. It makes the setup of the network easier; no need for extra hardware. Consequently, it is the optimal decision for temporary network setup, especially in non-reachable places such as mountains! But of course, it is not without some limitations. It offers lower speeds and less security when compared with infrastructure WLANs. I will just leave it at that although you can find many differences between the two modes of networking.

Once an ad hoc network is set up, one can also provide the network with Internet access as you will see in the practices.

2 Infrastructure Mode

Infrastructure wireless networks can operate in a couple of modes, each of which provides services that is different from the others and meets specific specification. Our discussion will cover the Access Point, Repeater, and Bridge modes.

In its default and commonly used mode, the AP operates in the Access Point mode. In this mode, the AP plays the role of a central authority through which all wireless clients communicate to each other once the connection is established. One of the interesting features of this mode is that the AP accepts both wireless and Ethernet

connections from wireless and Ethernet clients respectively. An arbitrary WLAN topology utilizing this mode is depicted in Figure 2.

Figure 2: WLAN in Access Point Mode

In the Access point mode, the wireless clients directly connect and communicate through central access point. But what if you have one AP that doesn't quite cover the entire area where users need connectivity? The placement of a wireless repeater between the covered and uncovered areas provides connectivity throughout the entire area. As depicted in Figure 3, wireless repeaters are an alternative way to extend the range of an existing WLAN instead of adding more access points. Generally a repeater regenerates the received signal from an AP or another repeater and retransmits the frames. In this experiment we will set one access point to Access Point mode and another AP to the Repeater mode to make the latter act as a repeater to extend the coverage of former network. This is depicted in Figure. As it receives and retransmits each frame on the same RF channel, which in effect doubles the number of frames on the same RF channel, wireless repeaters reduce throughput on the WLAN. So care must be taken not to use many repeaters. A WLAN repeater does not physically connect by wire to any part of the network. In Repeater mode, clients connect to the AP only wirelessly, although you can connect to it through Ethernet port, but this is used only for configuration.

Figure 3: WLAN with Wireless Repeater

Configuring the access point in Bridge mode is used to connect two LAN segments via a wireless link. The two segments which perforce belong to the same subnet, look like two Ethernet switches connected by a cable. Figure 4 depicts such a network. You can also think of it as an Ethernet switch whose ports are spread across the two access points. A typical scenario to use this mode is when you want to connect two subnets across physically distant buildings. Whereas A WLAN repeater does not physically connect by wire to any part of the network, a WLAN bridge does mot wirelessly connect to any part of the network.

Conceptually, the aforementioned discussion is enough. But, a complementary part regarding SSID and RF Channels is to be taken seriously to be able to set up your WLAN. These topics and others are the subjects most immediately at hand.

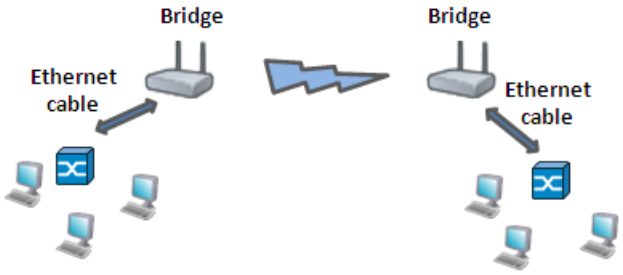


Figure 4: WLAN in Bridge Mode

Part II
Technical Introduction

This section is intended to get you started with the practices. So care must be taken to assimilate this part before delving into the practices.

3 LAN Settings

3.1 Connect The Wireless AP to Your Computer

Before even starting, it is highly recommended to reset the AP to its original factory settings. In order to do that, press the Reset Button on the back of the AP. Once reset, the AP's settings are the original factory, see Appendix B for those settings.

1. In order to connect to AP *setup page* and start configuration, configure the computer from which you want to connect to the AP, with a static IP address in the range of LAN interface IP address of the AP. For example if the AP LAN IP address is 192.168.1.10/24, you can choose IP address of the configuring computer to be any IP address in the same subnet except the aforementioned one; for example, choose it to be 192.168.1.20/24.

2. Connect an Ethernet cable from the AP to the computer.

3.2 Configure LAN and Wireless Access

1. Connect to the AP by opening your browser and entering the AP LAN IP address. Consequently, a login window will appear.

2. When prompted, enter the credentials of the AP. Change the credentials and start configuration.

3.3 DHCP Settings

It is imperative to unravel the ambiguity that might arise when dealing with the AP's DHCP server. Some of the Access Points, like the one we have, are capable of acting as a DHCP server. In such APs, one can enable the DHCP and further configure the related settings such as IP range. So, whenever we need an Ethernet clients attached to the AP, such as in the Bridge mode, we may enable DHCP server in the AP to advertise IP address instead of statically assigning them, although you can take do it! Alternatively, you can disable the AP's DHCP server if you AP is connected to a LAN in which there is a DHCP server enabled. In the later case, the clients connected to the APs receive their IP addresses from the DHCP of the LAN via AP. In the former, they receive their IP addresses from the AP itself. A final note,

Note that as there is already DHCP server enabled in the LAN, namely the DHCP of Birzeit University, we may utilize this DHCP server by disabling the DHCP of the AP, hence, the DHCP server enabled on network is the one connected to the AP.

4 Wireless Settings

The wireless settings are crucial for the experiment and we want to take a look at some of the elements we will be configuring.

Service Set Identifier (SSID): This is the name designated for a specific WLAN. The SSID is simply a string name to identify a service set. It is used to connect to an existing wireless network or to establish a new wireless network. For all network devices on your WLAN to communicate with each other, they must have the same SSID. Hence, you need to ensure that the SSID of both your wireless adapter and AP are the same. A final note: due to security and privacy concerns, you may disable SSID Broadcast. The default setting is set to Enable.

Channel: Direct communication between an 802.11 client radio and an access point occurs over a common channel frequency. You set the channel in the access point, and the radio card automatically tunes its transceiver to the frequency of the access point having the strongest signal. The radio card then continues with association and communications with the chosen access point.

Authentication: For added security on the wireless network, when enabling Encryption, the Authentication type can also be selected. If Shared Key is selected, the Access Point will not be seen on the wireless network except to the wireless clients that share the same WEP key with MAC Addresses allowed access as specified in Filter List. If Open System is chosen, only the wireless clients with the same WEP key will be able to communicate on the wireless network, but the Access Point will be visible to all devices on the network regardless of WEP keys. The default value for Authentication is set to "Auto", which adjusts to the Authentication mode of the wireless client automatically.

WEP: Wired Equivalent Protocol (WEP) is a wireless security protocol for WLAN. WEP provides security by encrypting the data that is sent over the WLAN. If you want to use it, then you must have the same WEP settings both on your mobile station and your AP.

Part III
Practices

The practices in this part are intended to be carried out sequentially, so follow them in the proper order. The following notes are worth taking into consideration before performing the practices.

1. Whenever you are asked to configure an AP, you should connect to the setup page via a suitable browser from a computer whose IP address falls within the range of the AP LAN subnet.
2. When dealing with the Repeater and Bridge modes, make sure to apply the same security settings on both APs.
3. It is highly recommended to turn off the firewall.
4. Whenever necessary, coordinate with the other groups to choose unique IP addresses.

5 Setting Ad hoc Network

The aim of this practice is to set up ad hoc network through which wireless clients can communicate with each other without the need to AP. To set up an ad hoc network, please perform the following steps to set a WLAN like the one depicted in Figure 1:

1. Setting up the network: If you are using a utility software to configure your wireless adapter, then navigate for the network type and set it to ad-hoc. Otherwise use your OS, such as Windows, to configure your wireless network settings by navigating to Wireless Network Connection properties. This is illustrated in Figure 5a. You will have your ad hoc network set once configured following:
   - SSID: "MyAdhocNetwork"
   - Authentication: Open with WEB disabled.
2. Adding clients to the network: once the settings in the previous step were configured on all clients wanting to join the network, all what is left is to refresh the available wireless networks and then connect to network of preference. Is is that simple?! Yes. Do not forget to assign IP addresses to the clients. Agree with the other client configuring partners on unique IP addresses. After that, test the connectivity with the other clients.
3. Enabling Internet connection sharing: To connect your clients to the Internet using your ad hoc network, you need to enable the Internet connection sharing on Internet-connected client. On that client, go to the Advanced properties of the Local Area Connection and enable sharing.This is illustrated in Figure 5b.Once you did that, all ad hoc clients will have access to the Internet. Note you can select the services running on that client's network. For example, you can grant the ad hoc clients Internet connectivity without granting them to SMTP, and hence they wont be able to chat!

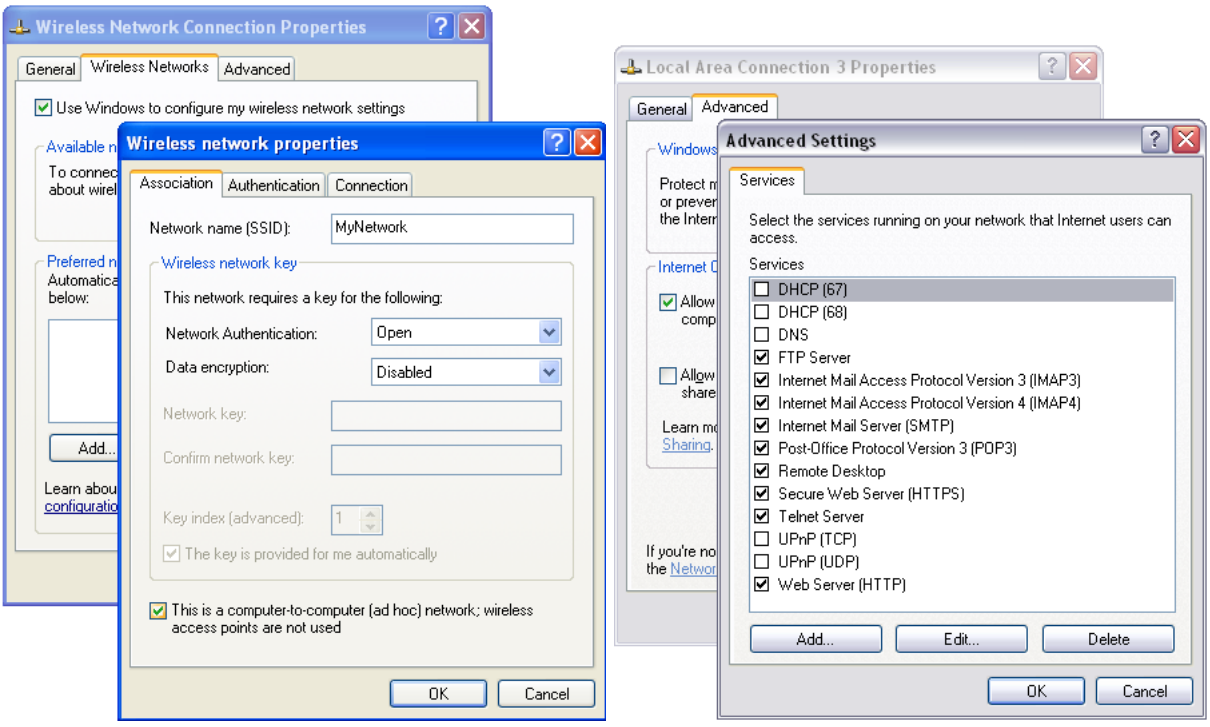
6 Setting WLAN with One Access Point

The aim of this practice is to create a simple WLAN using single Access Point similar to the one depicted in Figure 2.

6.1 Configure the AP in the Access Point Mode

6.1.1 Access Point Configurations

1. Navigate to Wireless Settings and set the Wireless Mode to "Access Point."
2. On the AP, in the Service Set Identifier (SSID) field, type a name that will be given to you by your TA. On the client side,



(a) Ad Hoc Basic Settings (b) Internet Sharing

Figure 5: Ad Hoc

3. Choose a wireless channel to be 6. Note that when setting multiple access points, you need to take care of the wireless channels in the vicinity such that the interference is kept to minimum. Nevertheless, we will not be concerned of such issues.

4. Navigate through the setup page to DHCP page and disable the DHCP server on the access point. Recall that the LAN to which the AP is connected has its DHCP enabled.

5. As we are not concerned with any security feature in this practice, navigate to Wireless Authentication and set it to "Open" with WEB disabled.

6.1.2 Client Configurations

Once the AP is configured, you need to make some configuration on the radio client.

Note: Usually, the SSID and the Channel are set by automatically while you are connecting to an AP with the other configuration set properly, so maybe you can skip for a moment step 2 and 3 and return back to them, after you finish the other configuration settings, to verify that they are set properly.

1. As there is a DHCP server on our LAN to which the AP is connected, the client automatically receives a suitable IP address once you set the IP settings (IP address and DNS server) to AUTO.

2. Set the SSID that matches with the AP's SSID that your intending to connect with.

3. Although the wireless adapter tunes its transceiver to the frequency of the access point having the strongest signal, it is better to set it yourself to mach the operating channel of the AP, namely channel 6.

4. Make sure that the Authentication settings are set to "Open".

5. Once these basic configurations are set, you are ready to connect to the AP. All what you need is to search for the available wireless APs in the vicinity and connect to the preferred one.

6. Make sure that the client received IP address and try to connect to the Internet to verify your connectivity to the WLAN. Remember to set the proxy settings on your browser.

Keep the settings for the next practice.

6.2 Apply Security

In this practice you are going to practice different security related issues. Refer back to Authentication in Section 4 before doing this practice.

6.2.1 Protect the Access Point with Password

The aim of this practice is to enable a password for your WLAN. In order to secure you AP and make sure no one can join your WLAN via the AP unless s/he has the password, we will set password. Follow the steps below to set password for your AP.

On the AP and client change the Authentication type to WPA-PSK and set the password to be "network_lab". Note that some APs automatically use the TKIP (temporal key integrity protocol): a data encryption method that enhances security of the pre-existing WEB encryption, when WPA-PSK is selected. Choose the TKIP if it is not automatically selected. The same settings should be set on the clients of the network, so configure the WPA-PSK on the wireless adapter. Make sure to set the password on the client and connect to the network using it.

6.2.2 Use WEB Encryption

In this practice you are going to enable WEB to provide security by encrypting the data that is sent over the WLAN.

Exercise. Use the "Open Authentication" to enable WEB Encryption on both the AP and the wireless client. Show that the clients with the wrong Key are unable to connect to the AP.

6.2.3 Use Shared Authentication to Enable MAC Filtering

In this practice you are going to use MAC Filters to either allow or deny network devices with specific MAC addresses.

In order for you to be able to use the MAC Filters, you need to set the Authentication type to "Shared". Once you did that, navigate to the Filtering page and perform the following exercises:

Exercise. Deny one of the MAC addresses of the wireless clients connecting to the WLAN. Once you denied the client, allow it and deny all other clients.

7 Setting WLAN with Repeater

The AP employed in this experiment is capable of operating in different modes to meet your wireless networking needs. Among the modes we will be using are the Access Point and the Repeater modes.

The configuration of a repeater is relatively straight forward. After switching the access point to repeater mode, you set the SSID of the repeater to match the SSID of the specific root access points that the repeater will associate with. The last important thing is to set the MAC address of the

Note: Although no security settings were configured on the root AP, be aware that if you have any wireless security enabled on the root AP, then the same settings must be configured on the repeater AP.

Before delving into the details of this practice, reset the two APs to their factory default configurations. Then perform the following steps to set a WLAN similar to the one depicted in Figure 3:

1. Configure the root AP as you did in Section 6.1.1.
2. On the AP that will associate to the root AP, set the SSID to match the SSID of the root AP.
3. Set the mode of the AP to Repeater to make it act as repeater.
4. As most of repeaters automatically associate with the access point with the strongest signal, we want to designate specific MAC address of the root AP to which our repeater will connect. In the "Remote AP MAC" field of the repeater AP, designate the root AP's MAC address.

5. This completes our configuration. Try connecting to the repeater AP first, then to the root AP from within wireless clients.

6. Connect to the root AP via Ethernet cable first, then to the Repeater AP and test connectivity in both cases. What do you conclude?

8 Setting WLAN in Bridge Mode

The AP employed in this experiment is capable of operating in different modes to meet your wireless networking needs. Among the modes we will be using is the Bridge mode. Figure 4depicts a WLAN which you are going to configure a similar one.

The configuration of a bridge is relatively straight forward. All you need to do is to set both AP to the bridge mode with MAC address of the first one typed in the second one and vice versa. One more thing, you need to set the SSID of both AP to match.

Before delving into the details of this practice, reset the two APs to their factory default configurations. Then perform the following steps:

1. Configure the first AP to the following settings:

   - SSID: to be given to you by your TA
   - Channel: 6
   - Mode: Bridge with the second AP's MAC address filled
   - Authentication: Open with WEB disabled
   - LAN IP, subnet mask and Gateway: 192.168.1.1, 255.255.255.0, and 0.0.0.0. Note when you change the LAN settings, you will not be able to access the AP setup page unless you change the configuring PC's IP address to a suitable one, say 192.168.1.10
   - DHCP enabled with range from 192.168.1.20-40
   - DNS: 0.0.0.0

2. Configure the second AP to the same settings except the following:

   - Mode: Bridge with the first AP's MAC address filled.
   - IP address: 192.168.1.2
   - DHCP disabled.

3. Connect a couple of PCs to the each AP with IP set to Dynamic. Verify that the IP address your PC receives is in the range.

4. Try to test the connectivity between the two LAN segments: the one connected the first AP and the one connected to the second. Does the bridge mode solve the problem encountered by the repeater mode of not being capable of providing Ethernet connectivity to the remote AP?

5. Try to connect wirelessly to each AP and explain your results.

6. Keep the configuration as they are but disable both DHCP servers and connect one first AP to the LAN that connects to the Internet (The one of Birzeit). After setting the proxy in your browser, try to test Internet connectivity. From where did your PC receive its IP address?

Part IV
Appendices

A 802.11 Standards and Protocols

The widespread acceptance of WLANs depends on industry standardization to ensure product compatibility and reliability among the various manufacturers. Hence, the IEEE ratified the original 802.11 specification which become the first internationally sanctioned standard for wireless LANs.

IEEE 802.11 is a set of *standards* carrying out WLAN computer communication in a set of *radio bands*. A number of *protocols* emerged from the 802.11 standards. 802.11b was the first widely accepted protocol, followed by 802.11g and 802.11n.

802.11 Protocol	Center Frequency (GHz)	Data Rate (Mbit/s)	Modulation	Approximate Indoor Range (meters)	Approximate Outdoor Range (meters)
b	2.4	1, 2, 5.5, 11	DSSS	38	140
g	2.4	1, 2, 6, 9, 12, 18, 24, 36, 48, 56	OFDM, DSSS	38	140

Table 1: 802.11 network protocols

A radio band is a small section of the spectrum of radio communication frequencies, in which **channels** are usually used or set aside for the same purpose. WLAN devices use different radio bands based on the underlying technology.

As depicted in Figure 6 , there are 14 channels designated in the 2.4 GHz radio band spaced 5 MHz apart, with the exception of a 12 MHz spacing before Channel 14. As the protocol requires 25 MHz of channel separation, adjacent channels overlap and will interfere with each other. Consequently, using only channels 1, 6, 11, and 14 is recommended to avoid interference. (http://en.wikipedia.org/wiki/802.11b)

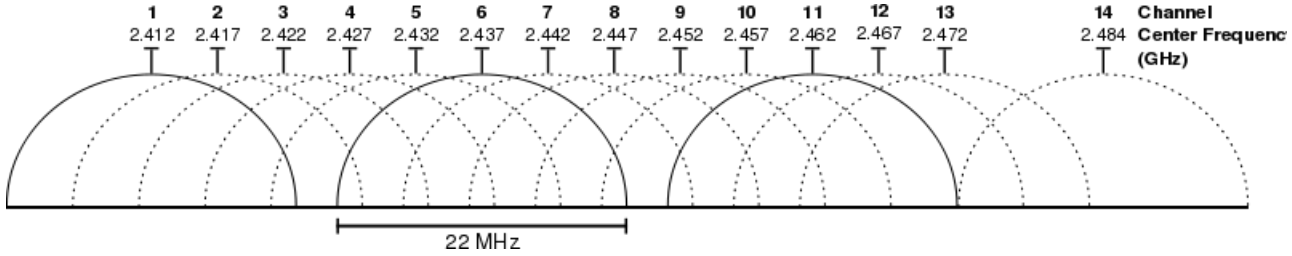


Figure 6: 802.11b/g channels in 2.4 GHz band

B D-Link Original Factory Settings

- The IP address of the LAN interface and subnet mask: 192.168.0.50 and 255.255.255.0, respectively.
- User Name and Password: The user name is: **admin**. Leave the **Password** field blank.