



Wireless Local Area Networks

Objective

The objective of this practice is to familiarize the students with the different parameters related to the configuration and management of wireless local area networks (WLAN). Particular emphasis is placed on the distinct characteristics of the 802.11 family of standards, which includes the properties of WLAN IEEE 802.11b/g.

The practice is to be performed in groups of two persons. There are some parts of the lab exercise that will require the utilization of several wireless devices.

Tools & Equipment

The equipment used in this practice is:

- One or more desktops/laptops equipped with a WLAN card with an Atheros chipset. Note that the Atheros chipset allows configuring the device as Access Point (AP), as station or in ad-hoc mode.
- One or more Linksys WRT54GS wireless LAN routes with the [OpenWrt](#) Linux Distribution installed. These devices can be also configured as AP, as station or in ad-hoc mode. Note that we need to access the Linksys from a PC or desktop. For this purpose we can use the Ethernet interface of the machines with the WLAN Atheros card (we could also use independent machines).
- One network device working as global Access Point (AP) with two different wireless cards allowing for two different WLAN BSSs called WLLabIT and WLLabIT2 (WLLabIT works as mode b AP and is encrypted (*WEP Key: 1234554321*), while WLLabIT2 works as b/g mode AP without cipher).

Note that the practice can be developed with any other WLAN enhanced device. However, the commands and configuration steps described in this document may not be valid in that case.

Configuration of Atheros WLAN Card

This section presents the steps to follow in order to properly configure the Atheros WLAN Cards:

1. Use the LINUX operating system.
2. Load the Atheros WLAN card driver (that must be previously installed in the PC)
\$>sudo modprobe ath_pci
3. Select the card's operation mode. For this purpose, first the interface ath0 will be disabled. After that it will be enable in the desired mode *ap* to work as AP and *sta* to work as station.

```
$>sudo wlanconfig ath0 destroy
```

Station mode:

```
$>sudo wlanconfig ath0 create wlandev wifi0 wlanmode sta
```



AP mode:

```
$>sudo wlanconfig ath0 create wlandev wifi0 wlanmode ap
```

4. Activate the interface at network level

```
$>sudo ifconfig ath0 up [IP address]
```

(*) Steps 3 and 4 must be executed every time you desire to change the mode.

5. Select the operation mode: 2 (B mode) o 3 (G Mode)

```
$>sudo iwpriv ath0 mode [mode]
```

Configuration of Linksys Equipment

In this section we explain the steps to be followed in order to get access to the Linksys equipment and configure it properly for the practice.

1. Connect the Linksys equipment to the power line. The Linksys must have a preconfigured IP address on each one of its ports as well as a username for login. In this document we assume that the Linksys has configured the IP 192.168.1.1 in its port 1 and the username to access is *user*.
2. Connect the Linksys equipment to the Ethernet interface of the desktop/laptop: plug one end of the network cable given with the Linksys into the *port1* interface on the back of the Linksys. Then connect the other end of the network cable to the interface *eth1* in the back of the desktop.
3. Configure, in the desktop, the interface *eth1* with the IP address 192.168.1.100

```
$>sudo ifconfig eth1 down
```

```
$>sudo ifconfig eth1 up 192.168.1.100
```

4. Start a new session in the Linksys equipment.

```
$>ssh user@192.168.1.1
```

5. Once the session will be started:
 - a. Discover the ID of the WLAN interface in the Linksys equipment. For this execute the command **iwconfig** (the man-page for this command can only be accessed on the Desktop, not on the Linksys, **\$>man iwconfig**).
 - b. If the Linksys is configured as AP, configure it as station and join it to either the WLLabIT or the WLLabIT2 channel. For this the command **iwconfig** must be used.
 - c. In order to assure that the connection was successfully established you can connect two Linksys (or a Linksys and an Atheros card) to the same channel of the global AP, configure an IP address (of the same IP network) in each of them and perform a ping in order to check the connectivity.

(*) The use of the ip command is explained on the Linux manual pages (**\$>man ip**).



Management of WLAN Interface using LINUX

The objective of this section is to practice usage of main tools needed to configure WLAN interfaces using the Linux desktop (**iwconfig** and **iwlist**). In this section we will use commands specific for the linksys equipments (**wl**).

iwconfig

Linux provides a manual explaining how to use the iwconfig command. Use it to learn how to use iwconfig (**\$>man iwconfig**)

(*)The command **\$>man iwconfig** must be executed on the Desktop (not in the Linksys).

iwlist

Linux offers a manual explaining how to use the iwlist command. Use it to learn how to use iwlist (**\$>man iwlist**)

(*)The command **\$>man iwlist** must be executed on the desktop (not in the Linksys).



Evaluation of the Access Point Mode

AP Configuration

Question: *Why an AP needs an IP address if it is a bridge, i.e. a Layer 2 device? Which interface is being used by the desktop to manage the AP?*

Question: *Discuss about the motives which could be interesting to activate the channel reservation (using RTS/CTS) in the AP and tell how this configuration can be made.*

Question: *What would happen with the AP management if the Gateway IP address was removed? How should these parameters be configured in order to allow to configure the AP using the WLAN cards*

Evaluation of the Ad Hoc Mode

In the previous sections we worked in infrastructure mode of WLAN networks. In this section we will work with the ad-hoc configuration.

In order to work in the ad-hoc configuration at least two stations must form the network, which means, at two groups must work together. It is also possible to form the ad-hoc network by using the Atheros WLAN Cards installed on the Desktops and the Linksys equipment.

- Use the **iwconfig** command to form the ad-hoc network.
- Check the connectivity between stations using the ping command.

Question: *What is the main difference between the infrastructure and ad-hoc WLAN configurations?*

Question: *Does the ad-hoc mode of operation has practical applications? Provide motivation.*

Evaluation of the Performance of WLANs

In this section several options will be proposed. **They should be used as guide** to analyze in greater detail those that you find interesting. There is high degree of freedom during this part of the lab. Exercise (you can use the laboratory AP or configure your own infrastructure network using the Linksys equipment and the Atheros WLAN Cards and working jointly with other groups. You can analyze the ad-hoc configurations. You can make comparisons of the infrastructure and the ad-hoc configurations; comparison between WLAN to WLAN device communication and WLAN to Wired device communications, etc.

The objective in this section is check the performance of a WLAN based on the IEEE 802.11 standard and its extensions 802.11b and 802.11g and to see how the different configuration options affect performance.

The objective is also to analyze performance of data transfer between two wireless stations and to see how the RTS/CTS mechanism, the coding affect the performance separately and when used in combination.

In order to activate the coding, you must connect the Linksys with the WLLabIT channel, this channel has activated the coding (the key will be provided during the session). Using the



iwconfig command you can activate the coding in the Linksys.

In order to activate the RTS/CTS mechanism you must use the **iwconfig** command. Another interesting point is to check the compatibility 802.11b and 802.11g.

(*)In order to develop this section to obtain result related with the throughput, jitter, etc... the iperf tool will be used. The iperf tool can be installed in the Linksys and the PCs with the Atheros cards.

Iperf is a traffic generation command line tool. In the subsequent sections a short user manual will be shown. If you want get more information about iperf, please visit the iperf web page or consult the man page (Desktop **\$>man iperf**).

- Executing **\$>iperf -help** will get a very simple and quite useful manual.

Iperf presents two different working modes: the server mode and the client mode. The client is the responsible of the traffic generation, while the server is the responsible of receiving the packets and calculating the statistics

- Running the server: Execute **\$>iperf -s [-u]**

-s, means that the program is working as server

-u, means that the server are listening to the UDP traffic.

There are another options, you can look for them in the places mentioned previously

- Running the client: Execute **\$>iperf -c server [-u] [-b binary_rate]**

-c, means that the program works as client.

-u, means that the generated traffic is UDP

-b, select the binary transmission rate

There are also many other options.

Question: *Explain what test have you made, analyze the obtained results and argue if they are in line with the expectations or not.*

(*) You should consider that the Communication between the source desktop and the destination desktop must be done throughout the wireless link. Therefore, depends on the designed scenario you may modify the route table in: the source desktop, linksys equipments involved in the communication and the destination desktop.

The route table can be modified by using the **ip** command in both the desktop and the linksys.



Evaluation of Management and Configuration Frames in IEEE 802.11

The objective of this section is to show in practice the concepts studied during the theoretical classes, such as, the association process of a station with a WLAN AP. The frames of the association process will be captured. The capture will be conducted in both coding and without coding mode.

Configuration (an alternative configuration using the Atheros card on the desktop is given in the Appendix of this exercise)

The station must be configured in monitor mode using the `iwconfig` command:

```
$>iwconfig eth1 mode monitor
```

The captures will be taken with the `tcpdump` tool over the `prism0` interface. This interface is automatically created when the WLAN interface is configured in monitor mode in the Linksys.

The command to obtain the capture is:

```
$>tcpdump -I prism0 -w file -s 0
```

-I, select the interface where the capture will be done.

-w, select the file where the capture will be stored.

-s, select the maximum packet size accepted. 0 means that there is not limit.

(*) In order to finish the capture press Ctrl+C.

The capture will be stored in the file indicated in the `-w` option. Once the capture is done, it must be copied into the desktop in order to open it with the **Ethereal** tool. To get this the following command will be used from the Linksys:

```
$>scp ./file user\_it@192.168.1.100:~/local_directory
```

file, the file storing the capture

user_it, the user in the Telematics Department account.

local_directory, is the directory in the local account where the user wants to save the file.

Also you can execute the next command on the Desktop:

```
$>scp alumno@192.168.1.1:~/file local_directory
```

file, the file storing the capture

local_directory, is the directory in the local account where the user wants to save the file.

The next step is to open the capture file with the ethereal tool. Start the ethereal with command `$>/sbin/ethereal` and then open the file containing the capture.

Analysis of Results

You must perform one association with encryption activated and another one without encryption. For this you must know that the global AP has the coding activated in the channel WLLabIT and the coding de-activated in channel WLLabIT2. You can also perform the capture in your own created channel.



During the association process the capture must be done with **tcpdump**. Then the file containing the capture must be opened with **Ethereal**.

***Question:** Indicate the frames corresponding to the association process, the functionality of these frames and their main parameters. If you find it necessary to explain in greater detail, please enclose you capture in the report.*

You can capture more interesting events: RTS/CTS, b/g compatibility studies based on the use of RTS/CTS. You can study and analyze specifically those cases that you consider interesting.

Evaluation Criteria

The student is fully free to analyze in more detail those aspects most interesting to him. Hence, the different section included in this lab manual will contribute with different weight to the final mark. The student's contribution on testbed configurations, experiments, tests, etc. will contribute with more weight to the final mark than the guided sections. Therefore, the sections "Evaluation of WLAN Performance" and "Management and Configuration IEEE 802.11 Frames" will be the most important because they offer a high flexibility to the student to provide his/her own contribution.

REFERENCES

- Wireless LANs: Implementing Interoperable Networks; J. Geier. Macmillan, 1999.
- Mobile Data & Wireless LAN Technologies; Rifaat A. Dayem; Prentice Hall 1997.
- High-Speed Wireless ATM and LANs; Benny Bing; Artech House, 2000.
- Website openwrt: <http://www.openwrt.org>
- Website iperf: <http://dast.nlanr.net/Projects/Iperf>

APPENDIX: Capturing Management Frames using the Atheros Card

Configuration of Atheros Card in Promiscuous Mode

The Atheros Card must be configured in *monitor* mode. This mode is a promiscuous mode. This is, the card scans one by one all the available channels (1 to 11) and captures all the frames. In order to configure the Atheros Card in monitor mode you must follow the next steps:

```
$>sudo wlanconfig ath0 destroy
$>sudo wlanconfig ath0 create wlandev wifi0 wlanmode monitor
$>sudo ifconfig ath0 up
```

Running Ethereal

The following steps have to be performed to run Ethereal:

```
$>sudo ethereal or $>ethereal
```