

## DEPARTAMENTO DE ELETRÓNICA, TELECOMUNICAÇÕES E

**INFORMÁTICA**

## LICENCIATURA EM ENG. DE COMPUTADORES E INFORMÁTICA

REDES DE COMUNICAÇÕES 1

**LABORATORY GUIDE NO. 5**

# Objectives

### Wi-Fi networks:

* Joining a BSS and communication.
* Authentication.
* Open and WPA2 protected networks.

# Duration

* 1 week

# Wireless Networks



1. In this task you will have a computer connecting to a Access Point in the laboratory. You can use your own computer, and the access point is already configured in the laboratory. You will use a second computer (usually the laboratory’s PC in Linux – PC1), that will be capturing all wireless traffic in the laboratory. To configure PC1 as a wireless monitoring node, you’ll need to set up its wireless interface “to listen” at a specific channel and start a capture with Wireshark in that interface. To configure a wireless interface in *Monitor Mode*, first analyze the capabilities of the wireless interface:

*sudo ip a* (to get the name of the interface, that must be something like wlp3s0)

(alternatively, depending on the Linux distribution and version: *sudo ifconfig)*

*iw* ***phy0*** *info* (where ***phy0*** is the name of the interface through the previous command)

Check that the interface is in *Manage Mode* and ready to communicate.

To capture the packets on the wireless medium at a specific channel, the interface must be configured to *Monitor Mode* and the channel.

*Disconnect from any wireless network on the Network Manager: sudo ip link set dev* ***phy0*** *down*

(alternatively: *sudo ifconfig* ***phy0*** *down*) *sudo iwconfig* ***phy0*** *mode monitor*

*sudo ip link set dev* ***phy0*** *up*

(alternatively: *sudo ifconfig* ***phy0*** *up***)**

*sudo iwconfig* ***phy0*** *channel <channel\_number>* (in this work the *channel\_number* is 13)

2. Connect another wireless terminal (IPv4 address (use 10.0.0.#group/24 or 10.0.0.1#group/24), and test connectivity with the AP (10.0.0.100), connected to the wireless LABCOM open wireless network with the correct parameters (SSID, Security – None, static). At PC1, using a visualization filter to capture all wireless frames from (or to) PC2, **analyze the exchanged packets/frames and their content. Explain how the association process is performed.**

Primeiro o PC2 vai enviar um prob request, para ele ver quais são as redes disponíveis. O AP da sala, que é o ponto de acesso responde ao PC2 com um prob response. Este prob response tem os detalhes da rede disponível (SSID e outros detalhes…)

A autenticação é fácil, porque a rede LAMCOM é aberta (não precisa de meter palavra pass), mas à mesma manda um pedido de autenticação e o AP envia uma resposta a esse pedido. Após esta confirmação o PC2 manda um pedido de associação com os seus detalhes e vai receber uma confirmação que está conectado à rede.

A captura dos pacotes é feita no PC da sala através do WireShark com o filtro “wlan.addr == <MAC\_DO\_PC2>” para capturar os pacotes enviados e recebidos pelo PC2.

### Filtering Wireless Layer 2 Information

Configure a Wireshark visualization filter to analyze the management packets:

wlan.fc.type\_subtype==x

x=0 association request

10 diassociation

2 reassociation request

1 association response

1. reassociation response
2. probe request
3. probe response

8 beacon

1. authentication
2. deauthentication
3. ACK
4. RTS
5. CTS

40 Data

You can analyze the several management packets, configuring the following Wireshark visualization filter to your PC2:

wlan.fc.type\_subtype==x && wlan.addr == mac\_pc

(note: macp\_pc is the actual MAC address number of the PC) How to find the MAC address number of the PC:

Linux: ip link

Windows:

* Terminal: getmac
* Powershell (Better): get-netadapter
* GUI:

1. Open “Settings” (windows key + I)
2. Go to “Networks & Internet”
3. Go to “Advanced network settings”
4. Under “More settings” go to “Hardware and< connection properties”
5. The list that you now see contains detailed information on every single network adapter installed on your device. Scroll down to the one you’re interested in and check the value of its Physical Address (MAC) field

3. Reconnect PC2 to the wireless network and test the connectivity with the AP through wireless. Exchange ICMP packets (ping) between PC2 and the AP or another wireless terminal.

**>> Analyze the exchanged packets/frames during the association and authentication phase.**

**>> Explain how the data transmission is performed.**

A screenshot of a computer

Description automatically generated

4. Now exchange very large ICMP packets (e.g. 1200 bytes, ping –s 1200) between PC2 and the AP or another wireless terminal. Analyze the exchanged packets/frames and their content. **Explain how the transmission is now performed and analyze the differences between this and the previous experiences.**

**>> Explain the purpose of the RTS and CTS frames**

Note: the AP has a RTS/CTS threshold of 1000 bytes.

Transmissão de Pacotes Grandes: Pacotes de 1200 bytes são fragmentados em pacotes menores e ativam o mecanismo RTS/CTS, por excederem o limite de 1000 bytes.

RTS/CTS: O PC2 envia um fragmento RTS (Request to Send) ao AP, que responde com CTS (Clear to Send), autorizando o envio e evitando colisões.

Diferença de Pacotes Pequenos: Pacotes pequenos são enviados diretamente, enquanto pacotes grandes necessitam de coordenação adicional com RTS/CTS.

Objetivo do RTS/CTS: Prevenir colisões e gerir dispositivos ocultos, assegurando transmissões estáveis.

Impacto: Com pacotes grandes, há maior overhead e latência devido ao processo para calcular tudo isto.

5. Connect now PC2 to the LABCOM\_SEC WPA2 wireless network with the correct parameters (SSID, Security – WPA2 Personal (password: netlab2024), static IPv4 address (use 10.0.1.#group/24 or 10.0.1.1#group/24), and test connectivity with the AP (10.0.1.100). Analyze the exchanged packets/frames and their content.

**>> Analyze the differences during the authentication process.**

**>> What 802.11 frames are used by the WPA2 Authentication?**

Não chegamos a esta parte.