

Please fill in the names with CAPITAL letters

Date	Name 1	Name 2	Name 3	Zaliczenie

WLAN Laboratory

Lab 11. Analyses of the MAC layer in WLAN

Objective:

The aim of the exercises is to familiarize with the tools to analyze the operation of the WLAN at the MAC layer and to understand the structure of the managed and control protocol and 802.11 MAC frames.

Student Prerequisites:

- knowledge of the basic WLAN concept,
- basic knowledge of the Windows,
- basic knowledge of WLAN MAC layer and WLAN MAC frames structure.

Hardware and Software to be used in this lab assignment:

- **computer PC with WIN XP**, WLAN AP device, Web browser, **AiroPeek™** 802.11 wireless LAN network analyzer.

Description of the Experiment:

The student analyzes the WLAN traffic seen in the laboratory. Different types of frames are counted and compared. It is performed observation and assessment of traffic generated by various WLAN. Is performed frames capture and filtering according to established criteria.

Lab Scenario:

1. Open "AiroPeek" 802.11 wireless LAN network analyzer (win XP).
2. Set the monitor mode and set scanning of all channels in the 2.4GHz and 5GHz.
3. Identify on **Nodes** panel the visible WLANs, look at their band (2.4 or 5Ghz), channel no and SSID name or MAC address if the SSID is not visible. Recognize the number of currently attached APs and associated stations and identify they encryption standards.
4. Select the top 3 WLAN (use a biggest traffic criterion, skip networks without known ESSID/BSSID names) and write the results:

No.	SSID	No of a AP stations	Traffic	Band [GHz]	Channel No	No of a Clients station
1						
2						
3						

Note!!! Please use only named WLANs (the WLANS with known SSID)

5. Look at the 802.11 frames types. Analyze the number of 802.11 frames sent over a WLANs, identify the 3 most frequently occurring types of frames (MAC frame types 802.11), and estimate their share in % for the whole WLANs traffic.

No.	Name of the frame	Share in traffic [%]
1		
2		
3		

6. Write below what is the purpose of the three most common types of packages (check on the Internet).

1).....

2).....

3).....

7. Set your own **unencrypted** WLAN network (use simple WLAN access router and establish your own WLAN with SSID name "MACTEST"). Connect the WLAN router to Internet (with WAN port). Connect a WLAN client (smartphone or PC) to your WLAN network and test Internet connection, if OK do to next point.

8. Check the nodes statistic and find your network (ssid "MACTEST"), recognize MAC address of the wlan router, your wlan client and the channel number (where your network operate). Note the values below:

Router MAC:

Client MAC:

Channel no:

9. Open "Capture" menu in analyzer. Set up the static channel in analyzer according to your own WLAN. Start capturing for a few second, stop, and find a **beacon** frame from your WLAN network (recognize by SSID/MAC address).

10. Open the **beacon** ('click' on the frame) and analyze information included in the frame. List some useful information found in the beacon frame:

1)

2).....

3).....

11. Using the mode "Capture", capture a sequence of packets exchanged during association (registration) station/phone to the AP. To do this:

1. Set packet filtering rule in the analyzer to: select packets with physical MAC address equal to MAC address of your wlan client (both way: to and from the client). And activate the filtering rule.

2. Log off client from the wlan network (switch off the wlan in smartphone)

3. Start capturing

4. Log in to your wlan network (switch on wlan in smartphone and connect to your network) and open in a browseran some Internet page.

5. Stop capturing.

If all is OK, at the beginning of the capture packets list will be packets related to the wlan client association process, and after that, packet related to your Internet activity. Try to recognize these packets.

Note!!! To effectively log in with smartphone the WLAN router have to be connected to Internet with WAN port).

12. Write bellow the sequence of packets related to association process, exchanged between the AP and the wlan client during the association procedure. Note the result in table bellow.
13. Switch on the security on your wlan network (use WPA-PSK method) and repeat the capturing experiment. Note the result in table bellow.

Unencrypted link	Encrypted link (with WPA-TKIP method)
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13

Recognize the packets responsible for association process and mark them in the table.
 Recognize the packets responsible for creating an encrypted link and mark them in the table.

14. In the analyzer, switch back to 'monitor mode' (close the capturing view).
15. Go to "Channel view".
16. Look at "Channel view" and find a channel with highest traffic (the highest number of packets sent) and perform observation of the number of frames with different transmission rate on this channel. Note in the table below your observation results

Channel	54Mbps	24Mbps	11Mbps	6Mbps	2Mbps	1Mbps
Packets no.						

Questions:

1. List with what speed frames are sent usually:

1) beacon

2) association request / response,

3) ack,

4) data.

2. Look at packets size statistics (in the analyzer) and list the results (note below the size:share):

.....

.....

.....

Explain what types of packets are smaller than 64 bytes, and why there are so many of them

References:

[1] E. Perahia, R. Stacey, "Next Generation Wireless LANs 802.11n and 802.11ac", Cambridge University Press, 2013

[2] P. Roshan, J. Leary, "802.11 Wireless LAN Fundamentals" Cisco Press, 2004.