

WLAN / 802.11

I. Objectives

The objectives of this practical work are:

- Understand complementary mechanisms that increase the efficiency of data exchange in 802.11 networks

II. Duration

This work should last 1h

III. Procedures

This Work will use:

- a) Students' personal PC with Wireshark installed
- b) A previously captured traffic exchange

IV. Network diagram used:

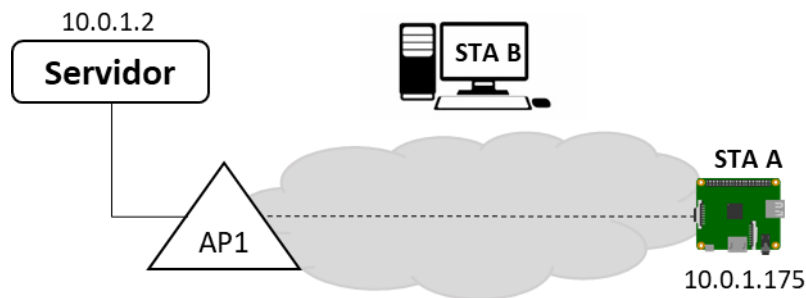


Figure 1: Network diagram used

1. Complementary exercises - WLAN

- RTS/CTS thresholds
- Fragmentation thresholds

In the network represented in the diagram above (Figure 1) the following thresholds were configured in STA A (with *the iwconfig* command) and in the AP:

1. Limit for sending RTS/CTS: 200 bytes
2. Limit for fragmentation: 500 bytes

STA A	Cisco AP (Rooms 300 and 301)
<pre> pi@raspberrypi:~ Ficheiro Editar Separadores Ajuda pi@raspberrypi:~\$ sudo iwconfig wlan0 rts 200 pi@raspberrypi:~\$ sudo iwconfig wlan0 frag 500 pi@raspberrypi:~\$ iwconfig lo no wireless extensions. eth0 no wireless extensions. wlan0 IEEE 802.11 ESSID:"ffwlan" Mode:Managed Frequency:2.472 GHz Access Point: 10:7B:44:40:21:40 Bit Rate=24 Mb/s Tx-Power=31 dBm Retry short limit:7 <u>RTS thr=200 B</u> <u>Fragment thr=500 B</u> Power Management:on Link Quality=64/70 Signal level=-46 dBm Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0 Tx excessive retries:0 Invalid misc:0 Missed beacon:0 pi@raspberrypi:~\$ </pre>	<pre> interface Dot11Radio0 ! ssid ComMoveis.33x.2400 ! fragment-threshold 500 rts threshold 200 </pre>

Table 1: Setting Thresholds

In the represented server, 3 pings were made to STA A with the following result:

```

Terminal - labcom@LabCom330-Server: ~
File Edit View Terminal Tabs Help
labcom@LabCom330-Server:~$ ping 10.0.1.175 -s 30
PING 10.0.1.175 (10.0.1.175) 30(58) bytes of data.
30 bytes from 10.0.1.175: icmp_seq=1 ttl=64 time=50.3 ms
30 bytes from 10.0.1.175: icmp_seq=2 ttl=64 time=4.66 ms
30 bytes from 10.0.1.175: icmp_seq=3 ttl=64 time=4.64 ms
30 bytes from 10.0.1.175: icmp_seq=4 ttl=64 time=4.50 ms
30 bytes from 10.0.1.175: icmp_seq=5 ttl=64 time=4.56 ms
^C
--- 10.0.1.175 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 4.500/13.735/50.313/18.289 ms
labcom@LabCom330-Server:~$ ping 10.0.1.175 -s 300
PING 10.0.1.175 (10.0.1.175) 300(328) bytes of data.
300 bytes from 10.0.1.175: icmp_seq=1 ttl=64 time=5.07 ms
300 bytes from 10.0.1.175: icmp_seq=2 ttl=64 time=5.97 ms
300 bytes from 10.0.1.175: icmp_seq=3 ttl=64 time=5.66 ms
300 bytes from 10.0.1.175: icmp_seq=4 ttl=64 time=8.05 ms
300 bytes from 10.0.1.175: icmp_seq=5 ttl=64 time=6.21 ms
^C
--- 10.0.1.175 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 5.066/6.189/8.046/1.003 ms
labcom@LabCom330-Server:~$ ping 10.0.1.175 -s 3000
PING 10.0.1.175 (10.0.1.175) 3000(3028) bytes of data.
3000 bytes from 10.0.1.175: icmp_seq=1 ttl=64 time=7.20 ms
3000 bytes from 10.0.1.175: icmp_seq=2 ttl=64 time=7.17 ms
3000 bytes from 10.0.1.175: icmp_seq=3 ttl=64 time=12.5 ms
3000 bytes from 10.0.1.175: icmp_seq=4 ttl=64 time=7.08 ms
3000 bytes from 10.0.1.175: icmp_seq=5 ttl=64 time=7.08 ms
^C
--- 10.0.1.175 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 7.079/8.210/12.531/2.160 ms
labcom@LabCom330-Server:~$

```

Figure 2: Ping results

1. Download the "ping file with rts and frags_ff_1.pcapng" with the capture made on Wireshark in execution on STA B (in Monitor mode)
2. Analyze it based on the threshold information provided (you should use other display filters in addition to the one suggested below).
 - a) Notice the use of RTS/CTS on multiple pings; are the AP and STA A behaviors the same?
 - b) Note the various fragments and the information contained in each of them. How many of fragmentation are there and where are they performed? For easy analysis, filter only 802.11 frames (`wlan.fc.type == 2 && wlan.fc.subtype == 8`)

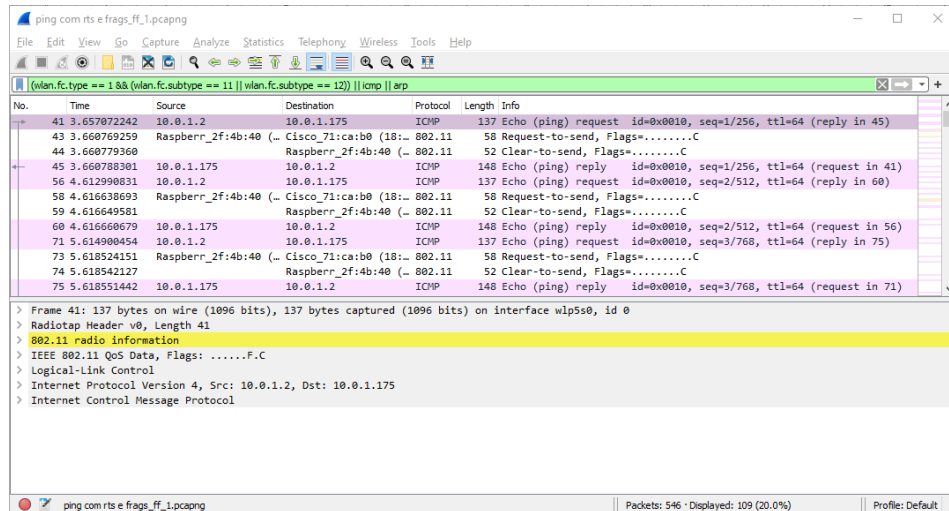


Figure 3: Partial capture of the 1st ping (30 bytes)

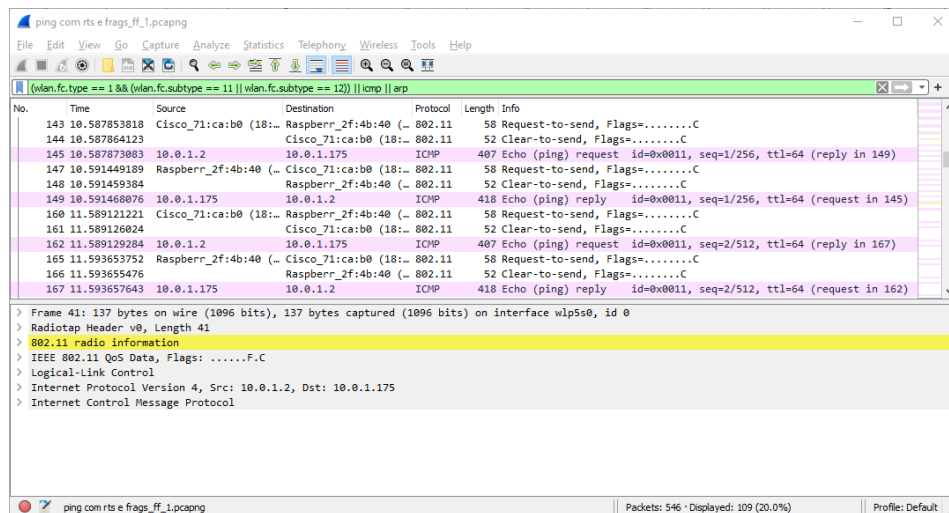


Figure 4: Partial capture of 2nd ping (300 bytes)

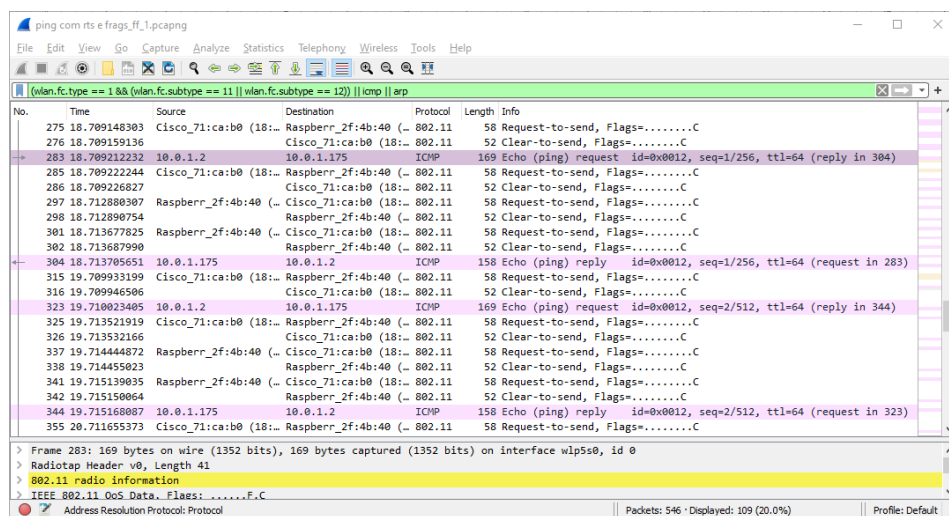


Figure 5: Partial capture of the 3rd ping (3000 bytes)

