WLAN / 802.11
Bluetooth

I. Objectivos

Os objectivos deste trabalho prático são:

- Entender mecanismos complementares destinados ao aumento da eficiência da troca de dados em redes 802.11
- Entender o interface HCI (*Host Controller Interface*) do Bluetooth

II. Duração

Este trabalho deve durar 1h30

III. Procedimentos

Este Trabalho irá utilizar:

a) PC pessoal dos alunos com Wireshark instalado

IV. Diagrama da rede utilizada (1º exercício):

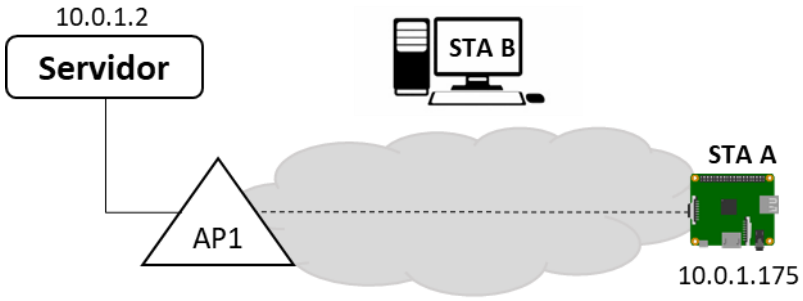


Figura 1: Diagrama de rede utilizado (1º exercício)

1. Exercícios complementares - WLAN

- Limiares de RTS/CTS
- Limiares de Fragmentação

Na rede representada no diagrama acima (fig 1) foram configurados, na STA A (com o comando *iwconfig*) e no AP, os seguintes limiares:

1. Limite para o envio de RTS/CTS: 200 bytes
2. Limite para fragmentação: 500 bytes

STA A	Cisco AP
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 RTS thr=200 B Fragment thr=500 B 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:~ $	interface Dot11Radio0 ! ssid ComMoveis.332.2400 ! fragment-threshold 500 rts threshold 200

Tabela 1: Configuração de limiares

No servidor representado, fizeram-se 3 *ping* para a STA A com o seguinte resultado:

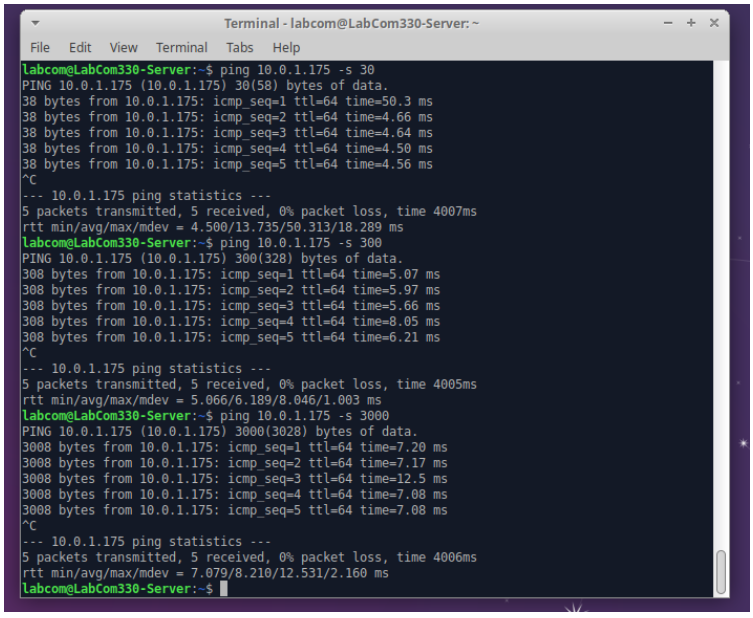


Figura 2: resultados dos ping efectuados

1. Descarregue o ficheiro *ping com rts e frags_ff_1.pcapng* com a captura efectuada no Wireshark em execução na STA B (em modo *Monitor*)
2. Analise-o com base na informação de limiares fornecida (deve utilizar outros filtros de visualização, para além do sugerido abaixo).

    2.1 Observe a utilização do RTS/CTS nos vários *ping*; os comportamentos do AP e da STA A são iguais?

2.2 Observe os vários fragmentos e a informação contida em cada um deles. Quantos tipos de fragmentação existem e onde são efectuados? Para facilitar a análise, filtre apenas as tramas 802.11 de dados (*wlan.fc.type == 2 && wlan.fc.subtype == 8*)

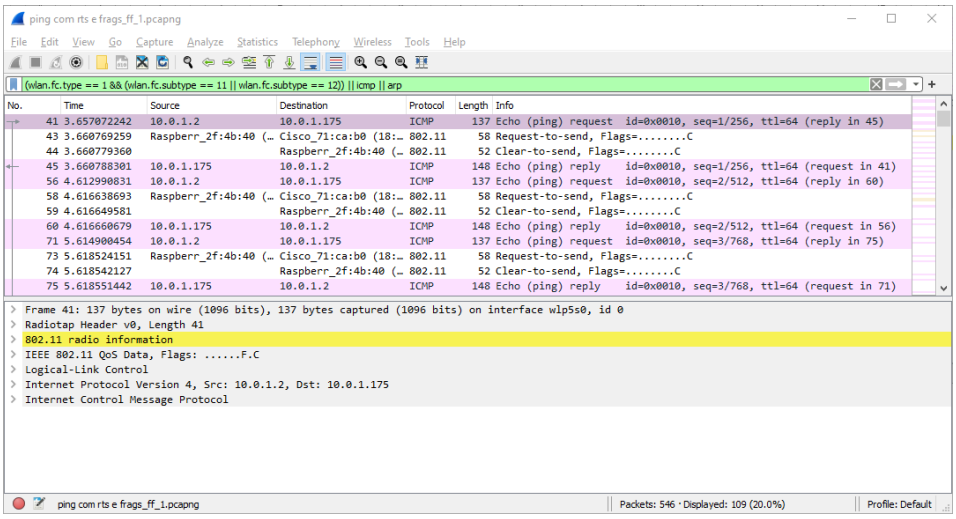


Figura 3: captura parcial do 1º ping (30 bytes)

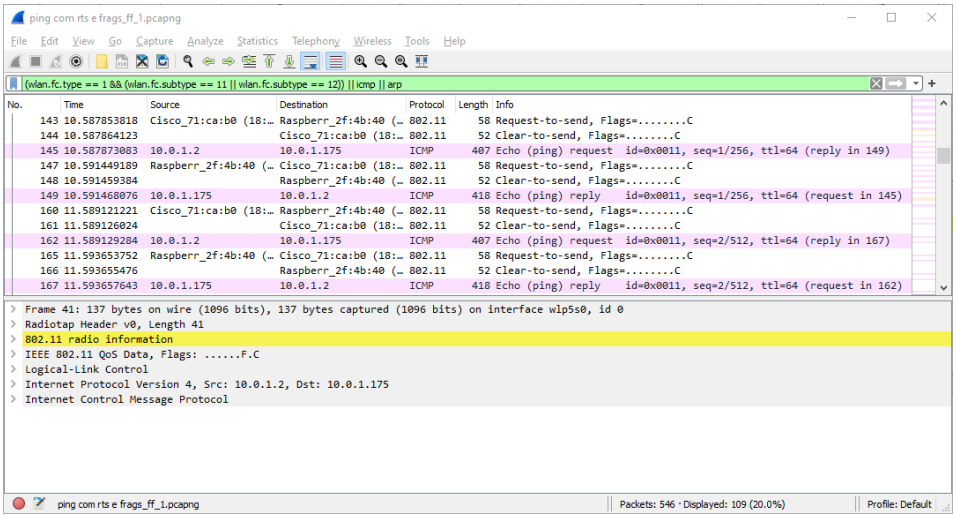


Figura 4: captura parcial do 2º ping (300 bytes)

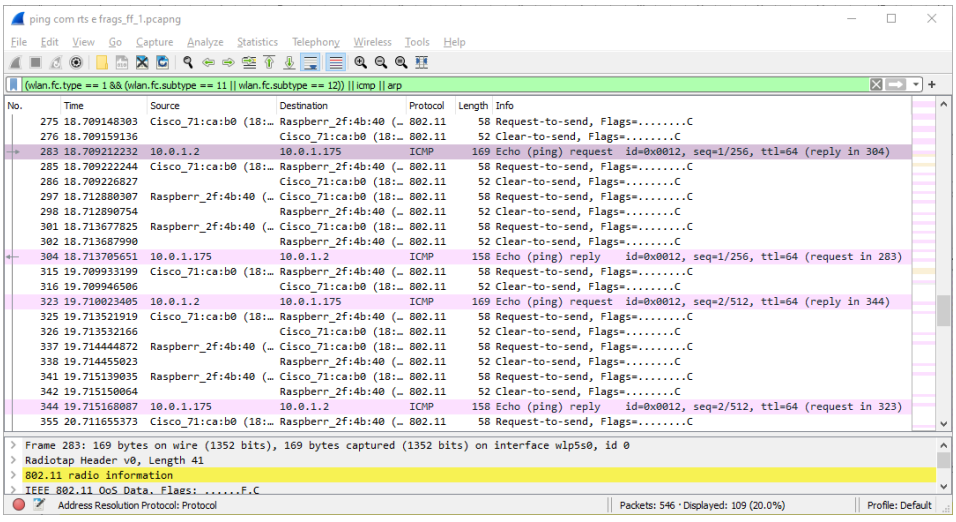


Figura 5: captura parcial do 3º ping (3000 bytes)

2. Bluetooth

1. Descarregue o ficheiro com a captura efectuada no Wireshark num interface HCI, disponível no elearning ou em:

   - https://gitlab.com/wireshark/wireshark/-/wikis/uploads/__moin_import__/attachments/SampleCaptures/Bluetooth1.cap

2. Abra esse ficheiro no Wireshark do seu PC:

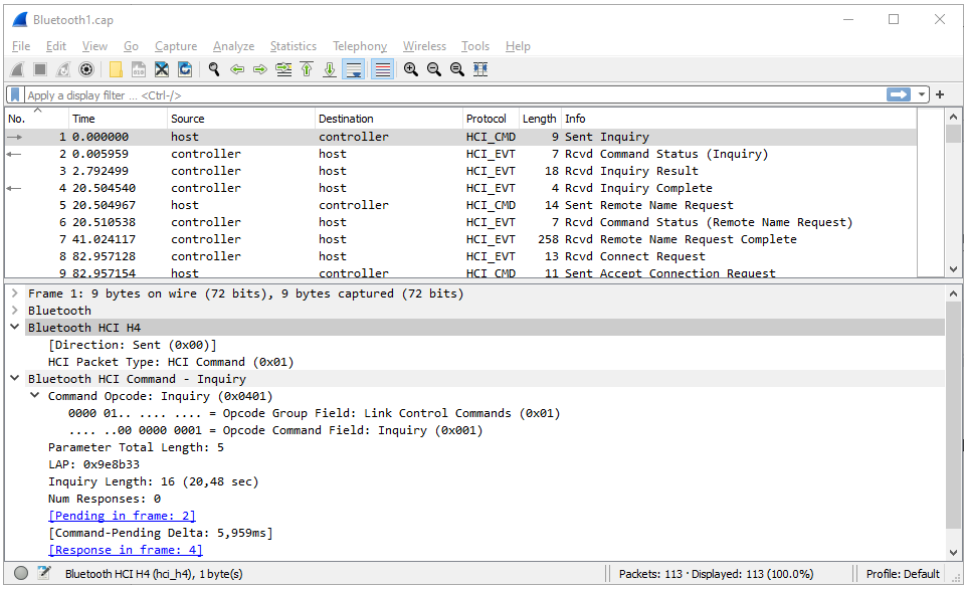


Figura 6: vista inicial do ficheiro de captura

3. Identifique o tipo de pacotes HCI presentes na captura (utilize um *display filter* por tipo de pacote; consulte o Anexo VI).

4. Ordene a captura pelo campo 'Info' e observe os diferentes códigos de comandos e eventos.

   - Complemente com a informação presente no quadro *Bluetooth HCI Summary* (no Menu, na aba 'Wireless', seleccione essa opção):

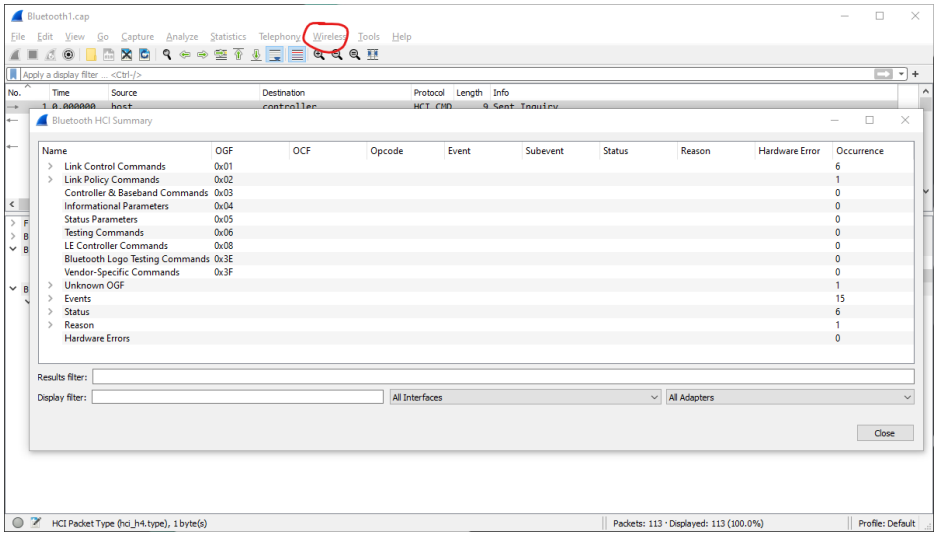


Figura 7: Informação "Bluetooth HCI Summary"

5. Observe o padrão CMD e EVT e veja a direcção dos mesmos.

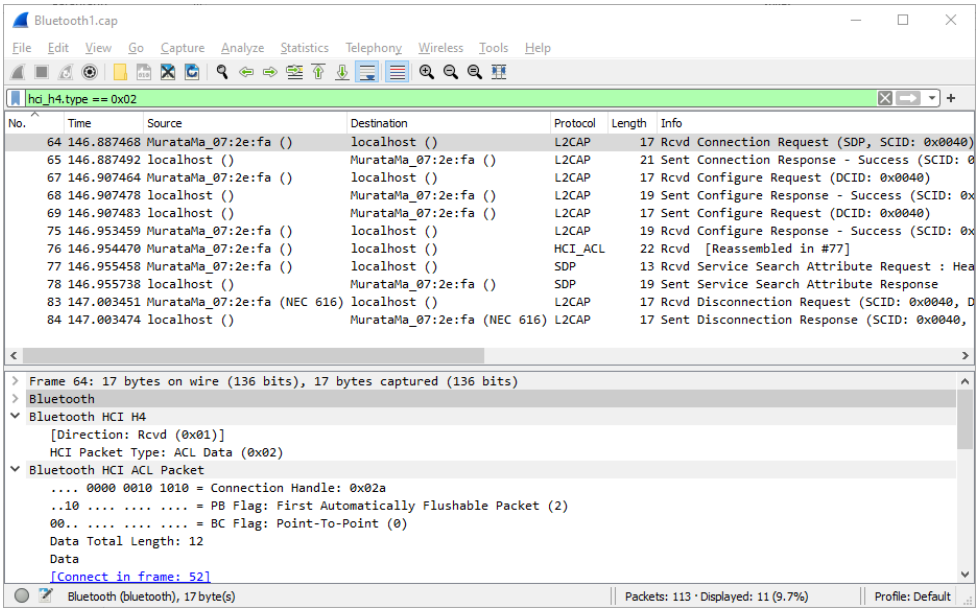


Figura 8: filtragem de pacotes do tipo 'Command'

6. Na captura, identifique os pacotes que representem mudanças de estado da ligação HCI. Tome como referência à máquina de estados da figura seguinte.

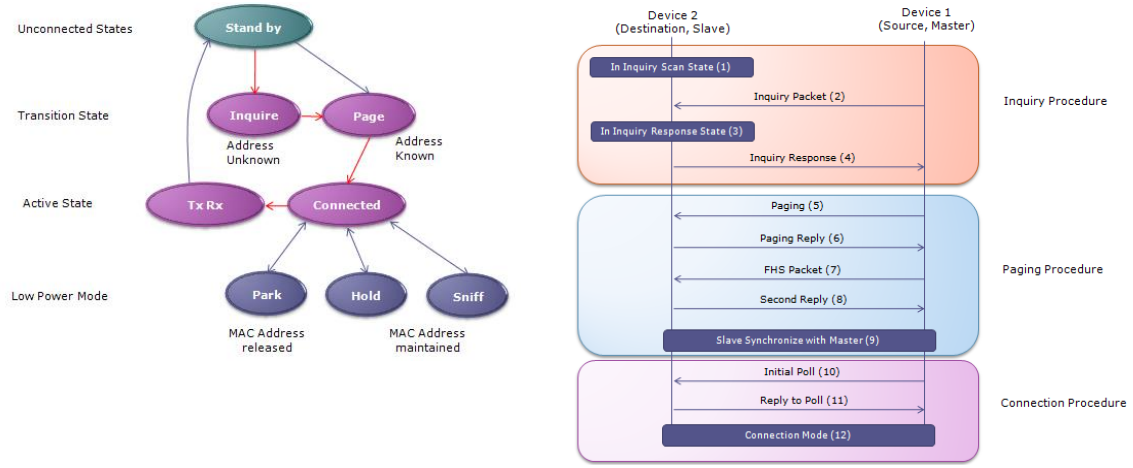


Figura 9: máquina de estados Bluetooth

(http://www.sharetechnote.com/html/Bluetooth_Protocol.html)

- Identifique o tipo de dispositivos que se estão a interligar (observar, p.ex. os pacotes 3 e 77)

7. Observa a natureza de orientação à ligação (*Connection Oriented*) do L2CAP (*Logical Link Control and Adaptation Layer Protocol*).

8. Confirme a pilha protocolar presente no Anexo V (no Menu, na aba '*Statistics*', seleccione essa opção '*Protocol Hierarchy Statistics*')

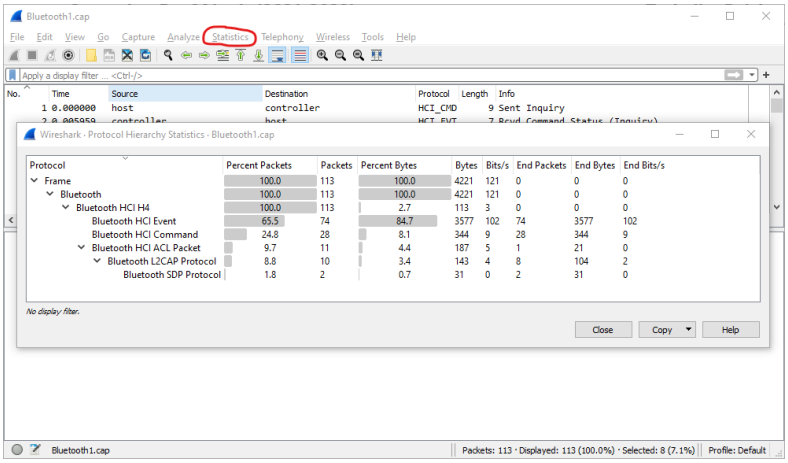
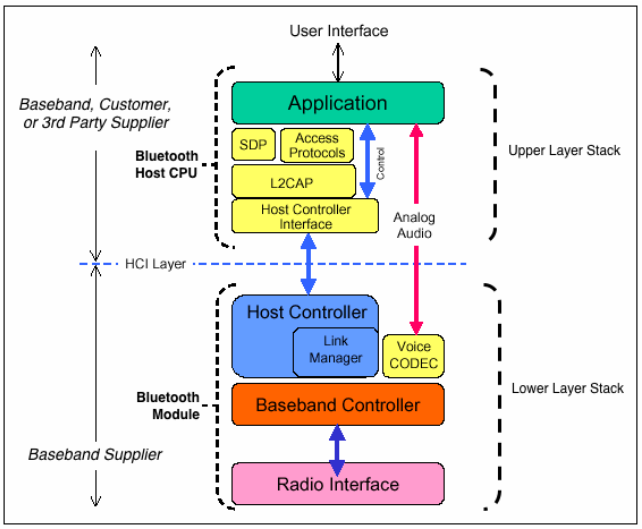
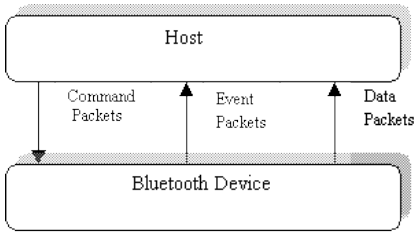


Figura 10: Informação "Protocol Hierarchy Statistics"

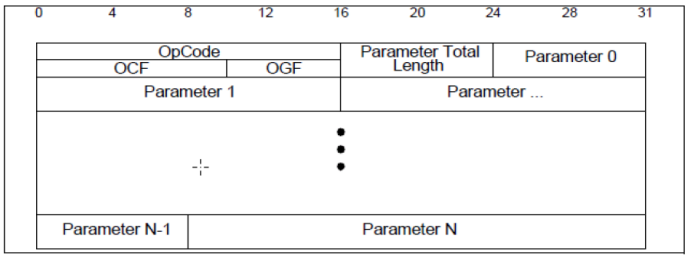
V. Interface HCI



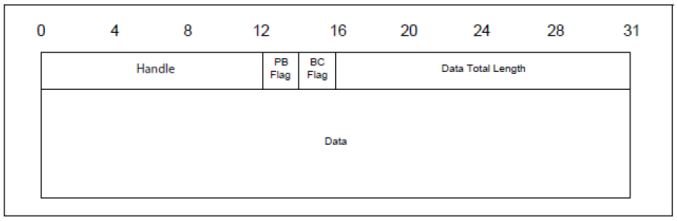
https://hearinghealthmatters.org/wp-content/uploads/sites/9/files/2014/01/BT-Stack.gif



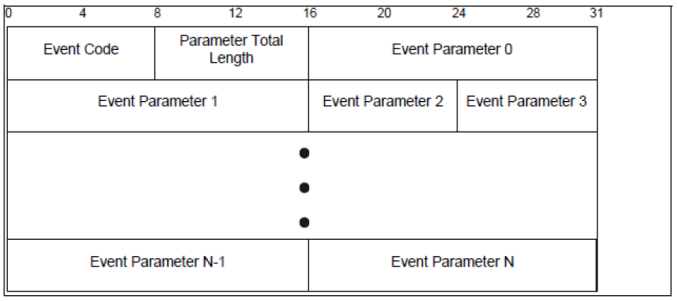
Command Packet



Asynchronous Data Packet



Event Packet



VI. Utilização do Wireshark

Filtros de visualização

- hci_h4.direction == 0x00 / 0x01
- hci_h4.type == (ver tabela)

Packet	Packet Type
Command	0x01
Asynchronous Data	0x02
Synchronous Data (not used)	0x03
Event	0x04

- bthci_cmd.opcode == *Command Opcode* (OGF + OCF)
- bthci_cmd.opcode.ocf == *Opcode Command Field*
- bthci_cmd.opcode.ogf == *Opcode Group Field*
- bthci_evt.code == *Event Code*

VII. Links úteis

- https://www.bluetooth.com/specifications/specs/
- https://lisha.ufsc.br/teaching/shi/ine5346-2003-1/work/bluetooth/hci_commands.html
- http://oscar.iitb.ac.in/onsiteDocumentsDirectory/Bluetooth/Bluetooth/Help/Host%20Controller%20Interface.htm
- https://gitlab.com/wireshark/wireshark/-/wikis/Bluetooth
- https://software-dl.ti.com/simplelink/esd/simplelink_cc13x2_sdk/1.60.00.29_new/exports/docs/ble5stack/vendor_specific_guide/BLE_Vendor_Specific_HCI_Guide/hci_interface.html
- https://www.wireshark.org/docs/dfref/h/hci_h4.html