Trabalho Prático Nº4 – Redes sem Fios (Wi-Fi)

Duração: 3h

Neste trabalho deve usar a captura de tráfego previamente realizada e disponível na plataforma de e-learning (BB).
Nota importante: O trabalho é para ser realizado nas aulas PL correspondentes. Não serão aceites trabalhos "resolvidos em casa".

1. Objetivo

Este trabalho tem como objetivo explorar vários aspetos do protocolo IEEE 802.11, tais como o formato das tramas, o endereçamento dos componentes envolvidos na comunicação sem fios, os tipos de tramas mais comuns, bem como a operação do protocolo.

2. Estudo Prévio

Antes de iniciar o trabalho, é recomendado o estudo da matéria sobre Redes sem Fios disponíveis na plataforma de ensino (*slides* e Sec.7.3 do livro), e consultar o Anexo ao enunciado. Como apoio adicional pode consultar outra bibliografia relacionada, tal como (disponibilizada na plataforma de ensino):

- Matthew Gast - 802.11 Wireless Networks, The Definitive Guide, Second Edition-O'Reilly Media (2005).
- IEEE Computer Society - IEEE Std 802.11™-2020: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

2.1. Tipos de tramas

Nesta secção é feito um resumo dos tipos e subtipos de tramas 802.11 mais comuns. A Tabela 1 da norma IEEE 802.11 (em anexo) complementa a descrição, sendo útil durante a observação e análise de tráfego Wi-Fi.

Tramas de Gestão (*Management frames*)

As tramas de gestão IEEE 802.11 permitem que as estações (STAs) estabeleçam e mantenham a comunicação. Os subtipos de tramas 802.11 para gestão da ligação de dados são:

- *Trama de Autenticação* (*Authentication*): a autenticação 802.11 é um processo pelo qual o ponto de acesso (AP) aceita ou rejeita a identidade de um acesso rádio proveniente de uma STA com placa de rede (NIC) 802.11.

- *Trama de Termino de Autenticação* (*Deauthentication*): Uma STA envia uma trama de termino de autenticação (*deauthentication*) para outra estação ou para o AP se quiser terminar a comunicação de forma segura.

- *Trama Pedido de Associação* (*Association Request*): A associação 802.11 permite que o AP possa alocar recursos para a ligação e efetuar a sincronização com a interface de rede que efetua o pedido. A NIC da STA inicia o processo de associação através do envio de um pedido de associação ao AP, em que a trama enviada fornece informações sobre a NIC (por exemplo, taxas de dados suportadas) e o identificador público da rede (SSID - *Service Set Identifier*) à qual se pretende associar. Depois de receber o pedido de associação, o AP considera associar-se à interface de rede respetiva, reservando recursos (e.g., espaço de memória) e definindo um ID para a associação.

- *Trama Resposta de Associação* (*Association Response*): Um AP envia uma trama resposta de associação contendo uma notificação de aceitação ou rejeição face ao pedido de associação formulado. Se o AP aceita a interface rádio, a trama resposta inclui informações sobre a associação, tais como o ID da associação e as taxas de dados suportadas. Sendo a associação estabelecida, a interface da STA pode utilizar o AP para comunicar com as outras STAs na rede sem fios, bem como com STAs no sistema de distribuição (DS), e.g. rede Ethernet, acessíveis a partir do AP.

- *Trama Pedido de Re-associação* (*Reassociation Request*): É equivalente ao Pedido de Associação mas aplicável a associações já existentes. Aplica-se, por exemplo, quando uma STA decide associar-se a um novo AP em detrimento do atual, e.g. por receber um sinal melhor.

- *Trama Resposta de Re-associação* (*Reassociation Response*): É equivalente à Resposta de Associação, mas surge como resposta a um Pedido de Re-associação.

- *Trama de Dissociação* (*Disassociation*): Uma STA envia uma trama de dissociação para outra STA ou para o AP quando quer terminar a associação. Os recursos alocados à associação podem ser libertados, removendo a interface de rede respetiva da tabela de associações.

- *Trama de Anúncio* (*Beacon*): O AP envia periodicamente tramas *Beacon* para anunciar a sua presença e transmitir informações tais como a data e hora, o SSID, e outros parâmetros relativos ao AP, a todas as interfaces rádio que estão dentro do seu alcance rádio. É pela receção de tramas *Beacon* (*passive scanning*) ou pelo varrimento dos vários canais rádio (*active scanning*) que uma estação pode optar por um AP mais favorável.

- *Trama Pedido de Prova* (*Probe Request*): A STA envia uma trama *Probe Request* quando precisa obter informações de uma outra estação. Esta trama é útil para uma STA determinar quais os APs que estão dentro do seu alcance rádio (*active scanning*).

- *Trama Resposta de Prova* (*Probe Response*): A STA ou o AP irão responder com uma trama de *Probe Response*, contendo informações sobre as taxas de dados suportadas, etc.

Tramas de Controlo (*Control Frames*)

As tramas de controlo permitem auxiliar a troca de tramas de dados entre STAs. Como subtipos comuns de tramas de controlo 802.11 tem-se:

- *Trama Pedido para Enviar* (*RTS - Request to Send*): Na norma 802.11, a função RTS/CTS é opcional e tem como objetivo reduzir colisões causadas, por exemplo, por estações escondidas, i.e. estações que têm associações com o mesmo AP mas não se detetam entre si. Assim, numa fase preliminar, uma STA pode enviar uma trama RTS para outra STA, aguardando uma trama de resposta CTS antes de enviar a trama de dados. Sendo as tramas RTS/CTS de pequeno tamanho, a probabilidade de colisão é reduzida.

- *Trama Resposta com Indicação para Enviar* (*CTS - Clear to Send*): Uma STA responde a um RTS com uma trama CTS, dando indicação à STA para enviar dados. O CTS inclui um valor de temporal que faz com que todas as outras estações (incluindo estações ocultas) adiem a transmissão de tramas por um período necessário para que o envio de dados previamente solicitado se processe sem colisões.

- *Trama Confirmação da Receção* (*ACK - Acknowlegment*): Depois de receber uma trama de dados, a STA recetora irá utilizar um código de verificação para detetar a presença de erros, e envia uma trama ACK para a STA emissora, se não forem encontrados erros. Se a STA emissora não receber um ACK dentro de um determinado período de tempo, retransmite a trama.

Tramas de Dados (*Data Frames*)

O principal objetivo de uma LAN sem fios é obviamente proporcionar a transmissão e comunicação de dados. Como tal, a norma IEEE 802.11 define um tipo específico de trama de dados que podem ser facilmente identificados com um analisador de tráfego (e.g. *Wireshark*). As tramas do tipo DATA têm vários subtipos para usos específicos.

2.2. Limitações na captura de tráfego Wi-Fi

Como explicado na documentação de apoio do Wireshark[1], a maioria dos *device drivers* para as placas de rede 802.11 (particularmente para o sistema operativo Windows) não disponibilizam a opção de capturar e copiar as tramas 802.11 para análise no Wireshark. Em contrapartida, as placas de rede 802.11 transformam normalmente as tramas de dados 802.11 em falsas tramas Ethernet antes de as disponibilizar ao *host*. Isto é, vários detalhes de cada trama 802.11 e o funcionamento da rede sem fios são ocultados antes de passar a trama à pilha protocolar do sistema operativo e ao mecanismo de captura de pacotes. Por esta razão, a captura de tramas nas interfaces Ethernet ou Wi-Fi pode não evidenciar diferenças quando analisadas no Wireshark.

1 http://wiki.wireshark.org/CaptureSetup/WLAN

Como o sucesso na captura de tráfego Wi-Fi depende de fatores tais como, as versões do Wireshark e do sistema operativo em uso, e dos *device drivers* de cada placa, propõe-se que os alunos usem na realização do trabalho as capturas de tráfego previamente realizadas e disponibilizadas na plataforma de apoio ao ensino.

A título unicamente experimental (não necessário para o TP4), os alunos podem também realizar capturas de tráfego IEEE 802.11, usando uma de duas abordagens:

(a) via GUI, selecionar *Capture/Options* e, para a interface Wi-Fi (e.g. en0, wlan0), assinalar a opção *Monitor Mode*., para que o Wireshark considere por defeito o cabeçalho real 802.11 (em vez de mapear para cabeçalho Ethernet).

(b) via CLI, invocar `wireshark -i wlan0 -I -y IEEE80l_ll &` (varia de acordo com o sistema operativo em uso, deve particularizar para a interface local Wi-Fi caso não seja a `wlan0`).

3. Primeiro Passo

Descarregue da plataforma de ensino a captura *WLAN-traffic-20230502a.pcapng.zip* e abra o ficheiro *.pcapng* no Wireshark.

4. Acesso Rádio

Como pode ser observado, a sequência de bytes capturada inclui meta-informação do nível físico (*radiotap header, radio information*) obtida do *firmware* da interface Wi-Fi, para além dos *bytes* correspondentes a tramas 802.11.

Selecione a trama de ordem XX correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 11).

1) Identifique em que frequência do espectro está a operar a rede sem fios, e o canal que corresponde essa frequência.

2) Identifique a versão da norma IEEE 802.11 que está a ser usada.

3) Qual o débito a que foi enviada a trama escolhida? Será que esse débito corresponde ao débito máximo a que a interface Wi-Fi pode operar? Justifique.

4) Verifique qual a força do sinal (*Signal strength*) e a qualidade expectável de receção da trama, sabendo que:

Signal strength	Expected Quality
-90dBm	Chances of connecting are very low at this level
-80dBm	Unreliable signal strength
-67dBm	Reliable signal strength– the edge of what Cisco considers to be adequate to support Voice over WLAN
-55dBm	Anything down to this level can be considered excellent signal strength.
-30dBm	Maximum signal strength, you are probably standing right next to the access point.

5. *Scanning* Passivo e *Scanning* Ativo

Como referido, as tramas *beacon* permitem efetuar *scanning* passivo em redes IEEE 802.11 (Wi-Fi). Para a captura de tramas disponibilizada, e considerando XX o seu nº de TurnoGrupo (PLXX), responda às seguintes questões:

5) Selecione uma *trama beacon* cuja ordem (ou terminação) corresponda a XX. Esta trama pertence a que tipo de tramas 802.11? Identifique o valor dos identificadores de tipo e de subtipo da trama. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

6) Para a trama acima, identifique todos os endereços MAC em uso. Que conclui quanto à sua origem e destino?

7) Verifique se está a ser usado o método de deteção de erros (CRC). Justifique.

   Justifique o porquê de ser necessário usar deteção de erros em redes sem fios.

As tramas *beacon* permitem especificar parâmetros de funcionamento úteis para apoiar a operação e a gestão das ligações em fios.

8) Uma trama *beacon* anuncia que o AP pode suportar vários débitos de base (B), assim como vários débitos adicionais (*extended supported rates)*. Indique quais são esses débitos.

9) Qual o intervalo de tempo previsto entre tramas *beacon* consecutivas (este valor é anunciado na própria trama *beacon*)? Na prática, a periodicidade de tramas *beacon* provenientes do mesmo AP é verificada com precisão? Justifique.

10) Identifique e liste os SSIDs dos APs que estão a operar na vizinhança da STA de captura. Explicite o modo como obteve essa informação (por exemplo, se usou algum filtro para o efeito).

No *trace* disponibilizado foi também registado *scanning* ativo (envolvendo tramas *probe request* e *probe response)*, comum nas redes Wi-Fi como alternativa ao *scanning* passivo.

11) Estabeleça um filtro Wireshark apropriado que lhe permita visualizar todas as tramas *probing request* e *probing response*, simultaneamente.

12) Identifique um *probing request* para o qual tenha havido um *probing response*. Face ao endereçamento usado, indique a que sistemas são endereçadas estas tramas e explique qual o propósito das mesmas?

6. Processo de Associação

Numa rede Wi-FI estruturada, um *host* deve associar-se a um ponto de acesso antes de enviar dados. O processo de associação nas redes IEEE 802.11 é executada enviando a trama *association request* do *host* para o AP e a trama *association response* enviada pelo AP para o *host*, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação.

Para a sequência de tramas capturada:

13) Identifique uma sequência de tramas que corresponda a um processo de associação realizado com sucesso entre a STA e o AP, incluindo a fase de autenticação.

14) Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo.

7. Transferência de Dados

O *trace* disponibilizado, para além de tramas de gestão da ligação de dados, inclui tramas de dados e tramas de controlo da transferência desses mesmos dados.

15) Considere a trama de dados nº8503. Sabendo que o campo *Frame Control* contido no cabeçalho das tramas 802.11 permite especificar a direccionalidade das tramas, o que pode concluir face à direccionalidade dessa trama, será local à WLAN?

16) Para a trama de dados nº8503, transcreva os endereços MAC em uso, identificando quais os endereços correspondentes à estação sem fios (STA), ao AP e ao router de acesso ao sistema de distribuição (DS)?

17) Como interpreta a trama nº8521 face à sua direccionalidade e endereçamento MAC?

18) Que subtipo de tramas de controlo são transmitidas ao longo da transferência de dados acima mencionada? Tente explicar a razão de terem de existir (contrariamente ao que acontece numa rede Ethernet.)

19) O uso de tramas *Request To Send* e *Clear To Send*, apesar de opcional, é comum para efetuar "pré-reserva" do acesso ao meio quando se pretende enviar tramas de dados, com o intuito de reduzir o número de colisões resultante maioritariamente de STAs escondidas. Para o exemplo acima, verifique se está a ser usada a opção RTS/CTS na troca de dados entre a STA e o AP/Router da WLAN, identificando a direccionalidade das tramas e os sistemas envolvidos.

    Dê um exemplo de uma transferência de dados em que é usada a opção RTC/CTS e um outro em que não é usada.

Relatório do trabalho realizado

O relatório do TP4 deve incluir:

- uma secção de "Questões e Respostas" do enunciado (inclua a questão, o *output* obtido (sempre que aplicável) e a resposta justificada).

- uma secção de "Conclusões" que autoavalie e resuma os resultados da aprendizagem nas várias vertentes estudadas no trabalho.

O relatório pode seguir o formato LNCS (Springer) ou um formato livre que facilite a inclusão dos resultados obtidos, e ser submetido na plataforma de e-learning **obrigatoriamente** com o nome RC-TP4-PL<TurnoGrupo>.pdf (por exemplo, RC-TP4-PL11.pdf para o grupo 1 do PL1, i.e., *group id* PL11) até ao ** final do dia da aula ** estipulada para conclusão do trabalho.

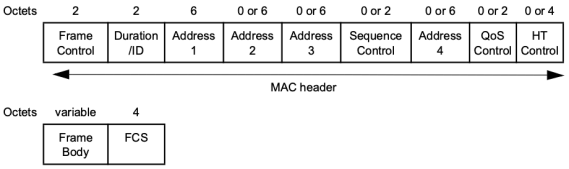

Figure 9-2—MAC frame format

Figure 9-5—Frame Control field format in S1G PPDUs when Type subfield is equal to 0 or 2

Table 9-1—Valid type and subtype combinations

Type value B3 B2	Type description	Subtype value B7 B6 B5 B4	Subtype description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110	Timing Advertisement
00	Management	0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Action
00	Management	1110	Action No Ack
00	Management	1111	Reserved
01	Control	0000–0010	Reserved
01	Control	0011	TACK
01	Control	0100	Beamforming Report Poll
01	Control	0101	VHT NDP Announcement
01	Control	0110	Control Frame Extension
01	Control	0111	Control Wrapper
01	Control	1000	Block Ack Request (BlockAckReq)
01	Control	1001	Block Ack (BlockAck)
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	Ack
01	Control	1110	CF-End
01	Control	1111	Reserved
10	Data	0000	Data
10	Data	0001	Reserved
10	Data	0010	Reserved
10	Data	0011	Reserved
10	Data	0100	Null
10	Data	0101	Reserved
10	Data	0110	Reserved
10	Data	0111	Reserved
10	Data	1000	QoS Data
10	Data	1001	QoS Data +CF-Ack
10	Data	1010	QoS Data +CF-Poll
10	Data	1011	QoS Data +CF-Ack +CF-Poll
10	Data	1100	QoS Null

Table 9-1—Valid type and subtype combinations *(continued)*

Type value B3 B2	Type description	Subtype value B7 B6 B5 B4	Subtype description
10	Data	1101	Reserved
10	Data	1110	QoS CF-Poll
10	Data	1111	QoS CF-Ack +CF-Poll
11	Extension	0000	DMG Beacon
11	Extension	0001	S1G Beacon
11	Extension	0010–1111	Reserved