Universidade do Minho

Mestrado Integrado em Engenharia Informática
REDES DE COMPUTADORES

TP4, Redes Sem Fios (802.11)
(3 aulas PL)

1. Objectivos

Este trabalho tem como objectivo principal explorar vários aspectos 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 recomendada a leitura dos *slides* sobre Redes sem Fios disponíveis na plataforma de ensino, e consultar o Anexo ao enunciado. Como neste trabalho se aprofundam aspectos da descrição feita nos *slides*, pode consultar outros documentos relacionados, tais como:

- *"A Technical Tutorial on the 802.11Protocol,"* Breezecom Communications
  http://web.cs.ucla.edu/classes/fall03/cs211/papers/802_11tut.pdf
  (versão resumida da norma)

- *"ANSI/IEEE Standard 802.11, 1999 Edition (R2003)"*
  http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf

2.1. Tipos de tramas

Nesta secção é feito um pequeno 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 para a observação e análise de tráfego Wi-Fi.

Tramas de Gestão (*Management frames*)

As tramas de gestão 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 estação envia uma trama de término de autenticação (*deauthentication*) para outra estação, ou para o AP, se quiser terminar a comunicação de forma segura.

- Trama de *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 de *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 aceitar 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 estação pode utilizar o AP para comunicar com as outras estações na rede sem fios, bem como com estações no sistema de distribuição (DS), e.g., rede Ethernet, acessíveis a partir do AP.

- Trama de *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 de *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 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 de *Pedido de Prova* (*Probe Request*): A estação 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 de *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*)

Este tipo de tramas permitem auxiliar a troca de tramas de dados entre as estações sem fios. Como subtipos comuns de tramas de controlo 802.11 tem-se:

- Trama de *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 vêem 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 menor.

- Trama de *Resposta com Indicação para Enviar* (*CTS - Clear to Send*): Uma STA responde a um RTS com uma trama CTS, dando indicação à estação que pode enviar dados. O CTS inclui um valor 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 de *Confirmação da Recepção* (*ACK - Acknowlegment*): Depois de receber uma trama de

dados, a STA receptora irá utilizar um código de verificação para detectar 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 originais 802.11 para análise no Wireshark. Em vez disso, transformam as tramas de dados 802.11 em falsas tramas Ethernet antes de as disponibilizar ao *host*. Isto é, vários detalhes da trama 802.11 relacionados com a tecnologia de funcionamento duma 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.

O sucesso na captura de tráfego Wi-Fi depende de vários fatores tais como as versões do Wireshark, do sistema operativo em uso e das funcionalidades 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, os alunos podem também realizar capturas de tráfego 802.11, usando uma de duas abordagens:

a) via GUI, selecionar *Edit/Preferences/Capture* e, para a interface Wi-Fi (e.g. `en1`, `wlan0`), escolher as opções *Monitor Mode*, com o *Default link-layer header type* do tipo 802.11.
b) via CLI, invocar `wireshark -i en1 -I -y IEEE801_11&`.

Descarregue da plataforma de ensino a captura *trace-wlan-tp4-2019.pcap* e abra o ficheiro no Wireshark.

3. Acesso Rádio

Descarregue da plataforma de ensino a captura *trace-wlan-tp4-2019.pcap* e abra o ficheiro no Wireshark.

Como pode ser observado, a sequência de bytes capturada inclui informação do nível físico (*radio information*), para além dos *bytes* correspondentes a tramas 802.11.

Para a trama correspondente com o número 1YXX (com Y=turno e XX=grupo, e.g., 1101),

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

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

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

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. *Scanning*

As tramas *beacon* permitem efetuar *scanning* passivo em redes Wi-Fi. Para a captura de tramas disponibilizada, responda às seguintes questões

4) Quais são os SSIDs dos dois APs que estão a emitir a maioria das tramas de *beacon*?

5) Qual o intervalo de tempo entre a transmissão de tramas *beacon* para o AP linksys_ses_24086? E do AP 30 Munroe St? (Pista: o intervalo está contido na própria trama). Na prática, a periodicidade de tramas *beacon* é verificada? Tente explicar porquê.

6) Qual é (em notação hexadecimal) o endereço MAC de origem da trama *beacon* de 30 Munroe St? Para detalhes sobre a estrutura das tramas 802.11, veja a secção 7 da norma IEEE 802.11 citada no início.

7) Qual é (em notação hexadecimal) o endereço MAC de destino na trama de 30 Munroe St??

8) Qual é (em notação hexadecimal) o MAC BSS ID da trama *beacon* de 30 Munroe St?

9) As tramas beacon do AP 30 Munroe St anunciam que o AP suporta quatro *data rates* e oito *extended supported rates* adicionais. Quais são?

10) Selecione uma trama *beacon* (e.g., a trama 1YXX com Y=turno e XX=grupo, e.g., 1101). Esta trama pertence a que tipo de tramas 802.11? Indique o valor dos seus identificadores de tipo e de subtipo. Em que parte concreta do cabeçalho da trama estão especificados (ver anexo)?

11) Verifique se está a ser usado o método de deteção de erros CRC e se todas as tramas *beacon* são recebidas corretamente. Justifique o uso de mecanismos de deteção de erros neste tipo de redes locais.

12) Identifique e registe todos os endereços MAC usados nas tramas *beacon* enviadas pelos APs. Recorde que o endereçamento está definido no cabeçalho das tramas 802.11 podendo ser utilizados até quatro endereços com diferente semântica. Para uma descrição detalhada da estrutura da trama 802.11, consulte o anexo ao enunciado.

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

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

14) Quais são os endereços MAC BSS ID de destino e origem nestas tramas? Qual o objetivo deste tipo de tramas?

15) 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 no ficheiro disponibilizado indique:

16) Quais as duas ações realizadas (i.e., tramas enviadas) pelo *host* no *trace* imediatamente após *t=49* para terminar a associação com o AP *30 Munroe St* que estava ativa quando o *trace* teve início? (Pista: uma é na camada IP e outra na camada de ligação 802.11). Observando a especificação 802.11, seria de esperar outra trama, mas que não aparece?

17) Examine o *trace* e procure tramas de *authentication* enviadas do *host* para um AP e vice-versa. Quantas mensagens de *authentication* foram enviadas do *host* para o AP *linksys_ses_24086* (que tem o endereço MAC Cisco_Li_f5:ba:bb) aproximadamente ao t=*49*?

18) Qual o tipo de autenticação pretendida pelo *host*, aberta ou usando uma chave?

19) Observa-se a resposta de *authentication* do AP *linksys_ses_24086* AP no *trace*?

20) Vamos agora considerar o que acontece quando o *host* desiste de se associar ao AP *linksys_ses_24086* AP e se tenta associar ao AP *30 Munroe St*. Procure tramas *authentication* enviadas pelo *host* para e do AP e vice-versa. Em que tempo aparece um trama *authentication* do *host* para o AP *30 Munroe St.* e quando aparece a resposta *authentication* do AP para o *host*?

21) Um *associate request* do *host* para o AP e uma trama de *associate response* correspondente do AP para o *host* são usados para que o *host* seja associado a um AP. Quando aparece o *associate request* do *host* para o AP *30 Munroe St*? Quando é enviado o correspondente *associate reply* ?

22) Que taxas de transmissão o *host* está disposto a usar? E o AP?

23) Identifique uma sequência de tramas que corresponda a um processo de associação completo entre a STA e o AP, incluindo a fase de autenticação.

24) Efetue um diagrama que ilustre a sequência de todas as tramas trocadas no processo de associação, incluindo a fase de autenticação.

7. Transferência de Dados

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

25) Encontre a trama 802.11 que contém o segmento SYN TCP para a primeira sessão TCP (download alice.txt). Quais são os três campos dos endereços MAC na trama 802.11?

26) Qual o endereço MAC nesta trama que corresponde ao *host* (em notação hexadecimal)? Qual o do AP? Qual o do *router* do primeiro salto? Qual o endereço IP do *host* que está a enviar este segmento TCP? Qual o endereço IP de destino?

27) Este endereço IP de destino corresponde ao *host*, AP, *router* do primeiro salto, ou outro equipamento de rede? Justifique.

28) Encontre agora a trama 802.11 que contém o segmento SYNACK para esta sessão TCP. Quais são

os três campos dos endereços MAC na trama 802.11?

29) Qual o endereço MAC nesta trama que corresponde ao *host*? Qual o do AP? Qual o do *router* do primeiro salto?

30) O endereço MAC de origem na trama corresponde ao endereço IP do dispositivo que enviou o segmento TCP encapsulado neste datagrama? Justifique.

O trabalho é para ser realizado nas aulas PL correspondentes. Não serão aceites trabalhos "resolvidos em casa".

Relatório

Deve entregar um relatório no final da resolução do trabalho completo (todas as partes) e que deve incluir, para além duma página inicial de identificação:

- Uma secção "Questões e Respostas" relativa ao enunciado acima, incluindo para cada questão: a questão, a resposta e a prova da realização da mesma (se aplicável);
- Uma secção de "Conclusões" que auto-avalie os resultados da aprendizagem decorrentes das várias vertentes estudadas no trabalho.

O relatório pode ser num formato livre ou no formato LNCS. A submissão/*upload* do relatório e outros documentos do trabalho prático devem ser feitos através da opção de "Troca de Arquivos" nas ferramentas de cada grupo no *black-board*. **O *upload* deve ser feito até ao final do dia (23:59) da aula prevista para a conclusão de todas as partes do trabalho.** A partir dessa hora/data limite a equipa docente fará uma cópia dos respetivos documentos existentes. *Uploads* depois dos prazos poderão ser ainda considerados mas sofrerão uma penalização adequada.

Os nomes dos ficheiros devem ser suficientemente explícitos para se poder identificar o trabalho e a sua autoria. De preferência, deve ser utilizado a seguinte sintaxe para a nomeação dos ficheiros: TP4.PLx.Gyy.PDF (em que "x" é o dígito identificando o turno e "yy" são os dígitos identificando o grupo no turno). Por norma, faça *upload* apenas de ficheiros do tipo PDF.

ANEXO
Trama 802.11 + Tipos e subtipos de tramas

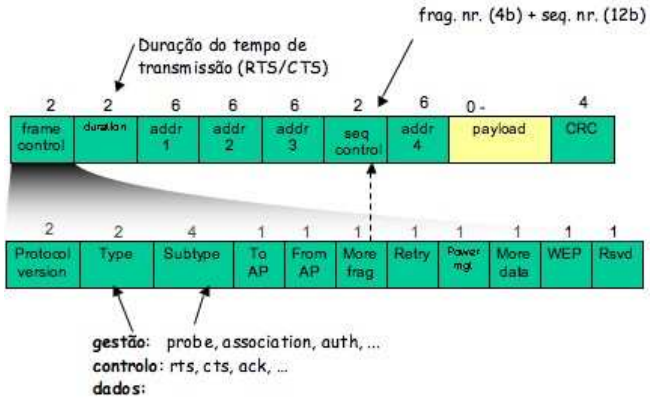

Table 8-1—Valid type and subtype combinations

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

382

Table 8-1—Valid type and subtype combinations *(continued)*

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
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	0000–0110	Reserved
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	CF-End + CF-Ack
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
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 (no data)
10	Data	1101	Reserved
10	Data	1110	QoS CF-Poll (no data)
10	Data	1111	QoS CF-Ack + CF-Poll (no data)
11	Reserved	0000–1111	Reserved