Trabalho Prático Nº3 – Nível de Ligação Lógica: Redes Ethernet, Protocolo ARP e Redes Locais sem Fios (Wi-Fi)

Duração: 6h

Nota1: este trabalho deve usar a máquina nativa e máquina virtual XubunCORE_7_5 (TP0) para as questões 1 e 2 da Parte 1.

Nota2: O trabalho é para ser realizado nas aulas PL correspondentes. Não serão aceites trabalhos "resolvidos em casa". Recomenda-se que os alunos leiam as seções introdutórias antes de responder às questões.

Nota3: Uma vez que: (i) as aulas T estão ligeiramente desfasadas entre si e com alguns turnos PL e (ii) até ao término das aulas, não irá haver PL nos dias 21.04, 25.04, 01.05, fixamos como data-limite para submissão do relatório o dia 10.05.2025 para todos os turnos.

Parte 1 – Redes Ethernet e Protocolo ARP

1. Objetivo

O objetivo da 1ª parte deste trabalho é explorar a camada de ligação lógica, focando o uso da tecnologia Ethernet e do protocolo ARP (*Address Resolution Protocol*).

O protocolo ARP, descrito na norma RFC 826 [1], é usado pelos equipamentos em rede para efetuar o mapeamento entre os endereços de rede e os endereços de uma tecnologia de ligação de dados, vulgarmente designados por endereços MAC (*Medium Access Control*). Desta forma, o protocolo ARP permite determinar, por exemplo, qual o endereço Ethernet que corresponde a um endereço IP particular.

2. Introdução (Recomenda-se a leitura como complemento às aulas teóricas)

Um dos conceitos mais importantes de uma pilha protocolar estruturada em níveis ou camadas é que cada camada fornece serviços às camadas superiores e usa os serviços disponibilizados pelas camadas inferiores. Por exemplo, a camada de ligação lógica oferece os seus serviços à camada de rede e através dela às camadas superiores (transporte e aplicação) e utiliza, por sua vez, os serviços da camada física.

O serviço básico prestado pela camada de ligação lógica é a **transferência de dados** de um nó para os nós imediatamente adjacentes na topologia da rede. Em cada nó de origem, a unidade protocolar de dados (*Protocol Data Unit* (PDU)) do nível de rede (datagrama IP) e é encapsulado num PDU do nível de ligação (trama), sendo depois enviado através da camada física para o nó adjacente. Por sua vez, este nó recebe a trama do nível físico, extrai o datagrama IP da trama recebida e entrega-o ao nível de rede para ser processado.

Outros serviços que um protocolo do nível de ligação lógica pode fornecer são: controlo de acesso ao meio, entrega fiável de dados, controlo de fluxo e controlo de erros (deteção e correção), embora não estejam disponíveis em todos as tecnologias do nível da ligação de dados (nível 2). Estes serviços podem ser oferecidos por outros níveis da pilha protocolar, por exemplo, o nível de transporte com o protocolo TCP *(Transmission Control Protocol*). A principal diferença é que no nível de ligação estes serviços são prestados na ligação entre nós adjacentes enquanto no nível de transporte são prestados fim-a-fim. Neste caso, uma ligação fim-a-fim envolve normalmente a travessia de um percurso na rede que passa por múltiplos nós intermédios.

Deteção e Correção de Erros

A deteção e correção de erros é outro exemplo de uma funcionalidade de serviço que pode ser prestada a vários níveis da pilha protocolar.

Genericamente a deteção e correção de erros ao nível de ligação lógica, bastante mais sofisticada que nos níveis protocolares superiores, consegue detetar (e eventualmente corrigir) erros de um bit e alguns erros com vários bits. O mecanismo de deteção mais comum é baseado num bloco de bits (B) criado pelo originador, que é uma função *f* da informação presente na trama a ser transmitida. Esse bloco de bits é acrescentado à trama original antes desta ser transmitida. O recetor ao receber a trama, utiliza a mesma função *f* e obtém, por sua vez, o bloco de bits (B1). Nessa altura, o recetor compara B com B1. Sendo iguais, a trama é considerada correta, caso contrário, significa tem erros e deve ser descartada.

Existem diversos métodos de deteção e correção de erros com menor ou maior complexidade. O método de deteção CRC (*Cyclic Redundancy Check*) usa o princípio enunciado acima, em que o bloco B1 deve ser zero, atendendo a que a adição do bloco B à trama original a tornou divisível por *f*. Este método, facilmente implementado em hardware, é usado em muitos protocolos de ligação lógica, nomeadamente em redes Ethernet[1] e Wi-Fi. Wi-Fi é a designação usada para a ligação em rede local sem fios, normalmente como sinónimo das normas IEEE 802.11a/b/g/n/ac/ax.

Protocolos de Acesso de Controlo de Ligação

Dois tipos de ligações comuns numa rede são as ligações ponto-a-ponto e as ligações multiponto, em particular, de difusão (*broadcast*). Uma ligação ponto-a-ponto envolve um nó emissor num extremo da ligação e um nó recetor no outro extremo. Ligações de difusão envolvem vários nós que enviam e recebem através de um meio de difusão partilhado. Numa ligação de difusão, quando um nó envia uma trama todos os outros nós recebem essa trama. Exemplo de ligações de difusão são as redes locais baseadas em Ethernet partilhada ou redes sem fios (e.g., Wi-Fi).

Num meio partilhado, se não houver controlo ou coordenação no acesso ao meio pode haver colisões entre tramas transmitidas simultaneamente por dois ou mais nós. Quando há uma colisão de tramas, os recetores não recebem corretamente as tramas transmitidas. Assim, um dos objetivos de um protocolo MAC (*Medium Access Protocol*) é coordenar o acesso ao meio de modo a reduzir ou eliminar a probabilidade de colisão de tramas, devendo os nós emissores envolvidos recuperar dessa situação.

Os protocolos MAC estão divididos em três categorias: protocolos de partição de canal, protocolos de passagem de ficha (*token-based*) e protocolos de acesso aleatório. Em particular, estes últimos são os mais usados nas redes locais comuns. As características e diferenças entre estes protocolos são estudadas nas aulas teóricas, não sendo diretamente objetivo deste trabalho.

Endereços MAC

A nível de ligação lógica, e em particular nas redes locais, os sistemas interligados são identificados por um endereço MAC. Um endereço MAC tem 48 bits de comprimento e é normalmente escrito em formato hexadecimal, por exemplo, 1A-23-F9-CD-06-9B. O endereço MAC é atribuído pelo fabricante da NIC (*Network Interface Card*) e não muda quando o nó muda de rede. Daí ser também designado como endereço físico. Pelo contrário, um endereço IP é um endereço lógico, i.e., depende da rede IP de acesso.

Normalmente, um nó terminal ou de interligação possui tantos endereços MAC quantas interfaces de rede ativas. Por exemplo, um *router* (apesar de operar sobre pacotes IP) tem também vários endereços MAC, um por cada interface de ligação disponível.

Quando um nó quer enviar uma trama na rede local insere os endereços MAC de origem e destino na trama. Numa rede local de difusão, Ethernet ou Wi-Fi, todos os nós da rede local recebem a trama. Cada nó recetor verifica se o endereço do destino MAC é igual ao seu. Em caso afirmativo, o campo de dados da trama (*payload*) é extraído e passado para o nível de rede, caso contrário, a trama é descartada. Há uma exceção: se o endereço destino for `FF-FF-FF-FF-FF-FF` (*broadcast*) todos os nós recebem e processam a trama.

Address Resolution Protocol

O principal objetivo do protocolo ARP (*Address Resolution Protocol*) é permitir fazer um mapeamento entre endereços do nível de rede (e.g. IP) e endereços nível de ligação lógica (MAC) por forma a possibilitar a entrega de dados entre nós adjacentes.

Suponha que um *host* na rede local quer enviar um datagrama IP para outro *host* na rede local. Suponha que conhece, provavelmente a partir do serviço de resolução de nomes – DNS, o endereço IP do *host* destino. Como sabe, o datagrama IP para ser enviado terá de ser entregue à camada de ligação lógica (L2) para ser encapsulado numa trama da tecnologia disponível e serializado para transmissão. A questão que se coloca é saber qual o endereço MAC destino a usar para enviar a trama que encapsula o datagrama IP, i.e., o *host* de origem vai ter de determinar o endereço MAC correspondente. Assim, sempre que necessário, o protocolo ARP permite obter o endereço MAC pretendido, através do uso das primitivas `arp-request` e `arp-reply`. Por cada resposta ARP recebida, e por questões de eficiência, cada nó da rede mantém uma tabela ARP (*cache*) que contém a correspondência entre endereços IP e os endereços MAC da rede local.

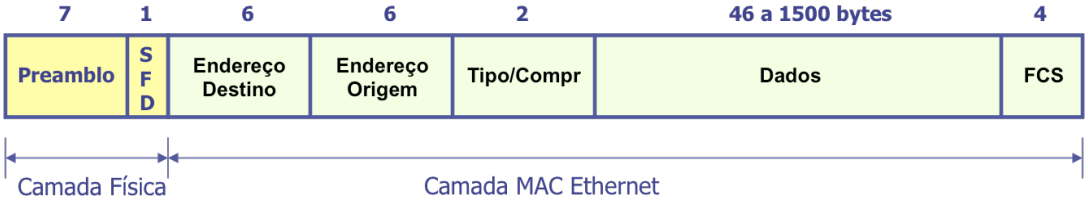
Note que o protocolo ARP tem um âmbito de operação restrito à rede local. Quando o destino IP é remoto, o protocolo ARP é usado para determinar o endereço MAC do *router* que está na mesma rede local, que, por sua vez, tem possibilidade de determinar qual o caminho que o datagrama IP deve seguir.

[1] Atualmente, atendendo à baixa probabilidade de erro nestas redes locais, várias NIC Ethernet não geram o FCS por questões de desempenho.

Ethernet

Ethernet é uma tecnologia de rede local bastante popular, havendo diferentes variantes de normas (*standards*) que permitem que a rede opere sobre diferentes meios de transmissão, topologias físicas e débitos de transmissão (tipicamente de 10Mbps a 10Gbps). A tecnologia Ethernet implementa um método de controlo de acesso ao meio do tipo aleatório, estudado nas aulas teóricas, e usa um formato de trama simples que inclui campos de controlo (*header* e *trailer*) e um campo de dados (*payload*).

Um trama Ethernet tem exatamente seis campos: (i) um campo para uma sequência de bits específica chamado *preâmbulo* (que o nó destino utiliza para sincronizar o seu relógio com o relógio do nó de origem e, assim, determinar quando começa a trama); (ii) o endereço MAC destino; (iii) o endereço MAC origem; (iv) um campo que indica o tipo de dados que a trama encapsula; (v) o campo de dados e (vi) o campo FCS (*Frame Check Sequence*) que inclui o código de deteção de erros (CRC-32).



Interligação de Redes Locais

As redes locais são interligadas através de repetidores (*hubs)*, pontes (*bridges*) ou comutadores (*switches*) e *routers*.

Os *hubs* são dispositivos de interligação que operam a nível físico, i.e., repetem o sinal que chega através de uma porta de entrada para todas as outras portas.

Os *switches*, tal como as *bridges*, são dispositivos do nível de ligação lógica, processando tramas do nível de ligação. Um *switch,* com a ajuda de uma tabela de comutação, mantém para cada endereço MAC a indicação da interface de saída. Assim, quando uma trama Ethernet chega a uma interface é comutada de imediato para a interface apropriada. O preenchimento da tabela é feito através de um mecanismo de autoaprendizagem. Quando chega uma trama a uma das suas interfaces, o *switch* examina o endereço de origem da trama e acrescenta uma entrada na tabela com o endereço MAC correspondente à interface de chegada da mesma. Quando chega uma trama que o *switch* não consegue comutar com base na tabela de comutação, i.e., o endereço MAC destino não consta da tabela, difunde-a através de todas as suas interfaces de saída.

Por sua vez os *routers*, estudados no trabalho anterior, funcionam ao nível de rede encaminhando pacotes IP (datagramas) com base no endereço IP destino (*unicast forwarding*), i.e., de maneira parecida à forma como os *switches* lidam com os tramas. Para esse efeito, os *routers* utilizam uma tabela de encaminhamento que é atualizada manualmente com rotas estáticas ou automaticamente através da utilização de protocolos de encaminhamento tais como o OSPF (*Open Shortest Path First*).

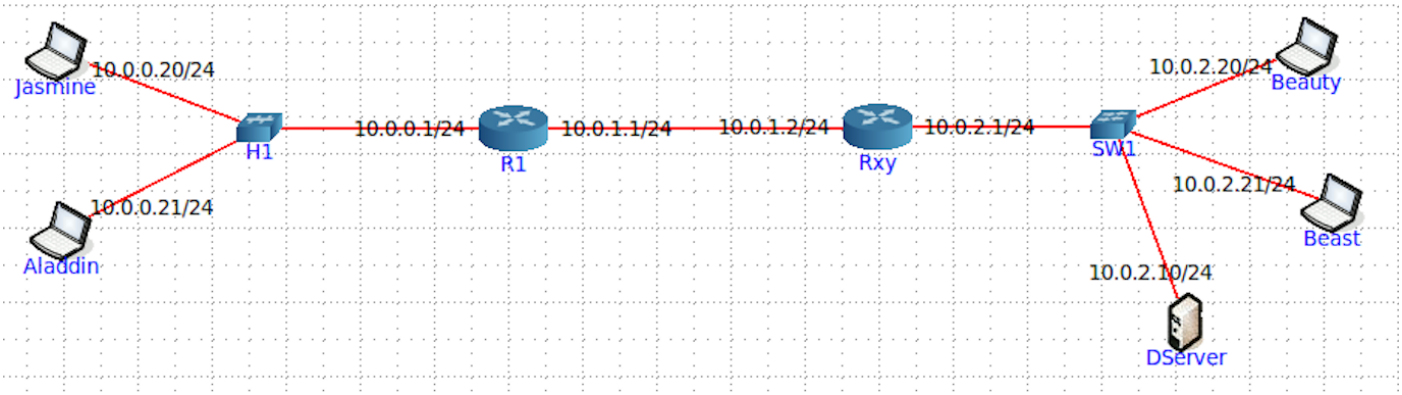
As entradas da tabela de comutação de um *switch* têm um tempo de vida pré-definido após o qual são removidas se não chegarem tramas que refresquem essas entradas.

Questões – Parte 1

1. Captura e análise de Tramas Ethernet

A topologia de rede representada na figura abaixo é constituída por: (i) uma LAN comutada que interliga os *hosts Beauty*, *Beast* e o servidor *DServer* (Disney Server) através de um *switch* (SW1) ao *router* de acesso Rxy; (ii) uma LAN partilhada que interliga os *hosts* Jasmine, Aladdin através de um *hub* ao *router* de acesso (R1); e (iii) uma rede IP ponto-a-ponto que interliga as duas LANs.

Construa a topologia indicada e particularize o router Rxy com o seu número de grupo (e.g., R27 para o grupo 7 do turno PL2). De igual forma, o endereço IP do servidor *DServer* deve ser alterado para incluir o seu número de grupo no identificador da host interface (4º octeto), e.g. 10.0.2.27, bem como o seu endereço MAC, e.g., 00:00:00:AA:BB:27.



Ative a topologia de rede e ative o Wireshark na interface de saída do *host Jasmine*. Antes de ver a sua série favorita, a Jasmine começa por abrir um terminal e estabelecer um acesso seguro ao servidor *DServer* usando o comando `ssh core@10.0.2.xy`.

Pare a captura do Wireshark e analise a trama que contém os primeiros dados referentes ao tráfego `ssh` dirigido ao servidor.

1. Anote os endereços MAC de origem e MAC destino da trama capturada. Identifique a que *hosts* se referem. Justifique.
2. Qual o valor hexadecimal do campo Type contido no *header* da trama Ethernet? O que significa? Qual o campo do *header* IP que tem semântica idêntica?
3. Quantos bytes são usados no encapsulamento protocolar, i.e., desde o início da trama até ao início dos dados do nível aplicacional? Calcule e indique, em percentagem, a sobrecarga (*overhead*) introduzida pela pilha protocolar.

A seguir responda às seguintes perguntas, baseado no conteúdo de uma das tramas Ethernet que contém a resposta proveniente do servidor.

4. Qual é o endereço MAC da fonte? A que *host* e interface corresponde? Justifique.
5. Qual é o endereço MAC do destino? A que *host* e interface corresponde?

2. Protocolo ARP e Domínios de Colisão

Deverá ter a *cache* ARP completamente vazia antes de iniciar esta secção: reinicie a topologia, ou utilize o comando `arp -d`.

Comece a capturar tráfego com o Wireshark na interface dos *hosts Jasmine*, *Aladdin*, *Beauty* e *Beast*. Não sabendo que a *Jasmine* e a *Beauty* estavam a capturar tráfego, o *Aladdin* e o *Beast* fazem um acesso secreto por `ssh` para o servidor *DServer*. Efetue esse acesso e depois pare as várias capturas de tráfego.

1. Observe o conteúdo da tabela ARP de *Aladdin* com o comando `arp -a`. Com a ajuda do manual ARP (`man arp`), interprete o significado de cada uma das colunas da tabela.
2. Observe a trama Ethernet que contém a mensagem com o pedido ARP (`ARP Request`).
    a. Qual é o valor hexadecimal dos endereços MAC origem e destino? Como interpreta e justifica o endereço destino usado?
    b. Qual o valor hexadecimal do campo `Type` da trama Ethernet? O que indica?
    c. Observando a mensagem ARP, como pode saber que se trata efetivamente de um pedido ARP? Refira duas formas distintas de obter essa informação.
3. Localize a mensagem ARP que é a resposta ao pedido ARP efetuado.
    a. Qual o valor do campo ARP `opcode`? O que especifica?
    b. Em que campo da mensagem ARP está a resposta ao pedido ARP efetuado?

c. Identifique a que sistemas correspondem os endereços MAC de origem e de destino da trama em causa, recorrendo aos comandos `ifconfig`, `netstat -rn` e `arp` executados no *host* selecionado (*Aladdin*).

d. Discuta, justificando, o modo de comunicação (*unicast* vs. *broadcast*) usado no envio da resposta ARP (`ARP Reply`).

4. Verifique se a *Jasmine* teve conhecimento ou não de todo o tráfego gerado pelo acesso secreto do *Aladdin*? Qual será a razão para tal?

5. De igual modo, verifique se a *Beauty* teve conhecimento ou não de todo o tráfego gerado pelo acesso secreto do *Beast*? Qual será a razão para tal?

6. Consulte a tabela ARP do *Aladdin* e do *Beast*. Que principal diferença entre as tabelas obtidas e que impacto tem no funcionamento da rede?

7. Esboce um diagrama em que ilustre claramente, e de forma cronológica, todo o tráfego *layer* 2 (tramas) entre o *Aladdin* e os *hosts* com os quais comunica, até à receção do primeiro pacote que contém dados do acesso remoto.

8. Construa manualmente a tabela de comutação completa do *switch* da casa da *Beauty* e do *Beast*, (SW1) atribuindo números de porta à sua escolha.

3. Serviço de NAT/PAT

1. Como proteção, a *Jasmine* e o *Aladdin*, juntamente com a *Beauty* e o *Beast*, decidiram conectar R1 e Rxy a uma rede de um ISP com endereços IP públicos, mantendo todo o endereçamento privado das suas LANs. Sabe-se que o ISP não encaminha tráfego para redes privadas, portanto, R1 e Rxy não conseguem encaminhar tráfico para endereços privados remotos, i.e., não fisicamente adjacentes.

   Discuta que solução implementaria em R1 e em Rxy de modo a manter todas as funcionalidades anteriormente existentes (conectividade IP, acesso `ssh` ao servidor, etc.).

Parte 2 – Redes Locais sem Fios (Wi-Fi)

1. Objetivo

A 2ª parte do 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. Desta forma, completa-se o estudo das redes locais (com e sem fios).

2. Introdução (Recomenda-se a leitura como complemento às aulas teóricas)

Antes de iniciar esta etapa do trabalho, é recomendado o estudo da matéria sobre Redes sem Fios disponíveis na plataforma de ensino (*slides* e 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.

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[2], 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.

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 a captura de tráfego previamente realizada e disponibilizada na plataforma de apoio ao ensino.

A título unicamente experimental (não necessário para o TP3), 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 IEEE801_11 &` (varia de acordo com o sistema operativo em uso, deve particularizar para a interface local Wi-Fi caso não seja a `wlan0`).

Questões – Parte 2

A *Jasmine*, como não gosta de ver os cabos da rede Ethernet espalhados pelo palácio, convenceu o *Aladdin* a substituir a infraestrutura Ethernet por uma rede sem fios. O *Aladdin* decidiu então comprar equipamento Wi-Fi e fazer uma captura de tráfego para perceber melhor o funcionamento da rede.

Descarregue da plataforma de ensino a captura *WLAN-traffic-20250407.pcapng.zip* e abra o ficheiro *.pcapng* no Wireshark.
Não se esqueça que deve ser incluída evidência prática que sustente a resposta às questões.

1. 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 xy correspondente ao seu identificador de grupo (TurnoGrupo, e.g., 27).

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.

3. Qual a taxa de transmissão a que foi enviada a trama escolhida? Será que essa taxa de transmissão corresponde à máxima que a interface Wi-Fi pode operar? Justifique.

2. 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 xy o seu nº de TurnoGrupo (PLxy), responda às seguintes questões:

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

4. Selecione uma *trama beacon* cuja ordem (ou terminação) corresponda ao seu ID de grupo. 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 I)?

5. Verifique se está a ser usado o método de deteção de erros (CRC). Justifique. (Poderá ter de ativar a verificação no Wireshark, em Edit -> Preferences -> Protocols -> IPv4 -> "Validate Checksum if Possible")

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

As tramas *beacon* são enviadas periodicamente e permitem especificar parâmetros de funcionamento para apoiar a operação e a gestão das ligações sem fios.

7. Uma trama *beacon* anuncia o intervalo entre *beacons* às várias taxas de transmissão (B) que o AP suporta, assim como várias taxas de transmissão adicionais (*extended supported rates)*. Indique qual a periodicidade e as taxas de transmissão suportadas pelo AP da trama *beacon* selecionada.

8. 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.

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

10. Assuma que a STA de captura consegue-se associar a qualquer AP na vizinhança. Dadas as tramas recebidas através do *scanning* ativo e passivo, observe os valores da força do sinal (*Signal Strength*) nas meta-informações de nível físico e indique a qual AP a STA de captura se deve associar para obter a melhor qualidade de ligação possível. Indique como chegou a esta resposta.

11. Os valores de taxa de transmissão do Wi-Fi estão diretamente associados à qualidade da receção do sinal. Considerando os valores de sensibilidade mínima (*Minimum Sensivity*) e taxa de transmissão (*Data Rate*) que constam nas tabelas de referência (ver Anexo II), e a força do sinal recebido nas tramas do AP identificado na resposta anterior, estime o débito que a STA obterá nessa ligação.

3. Processo de Associação

Numa rede Wi-Fi estruturada, um nodo ou STA 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* da STA para o AP e a trama *association response* enviada pelo AP para a STA, em resposta ao pedido de associação recebido. Este processo é antecedido por uma fase de autenticação.
Para a sequência de tramas capturada:

12. 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.

13. Efetue um diagrama que ilustre a sequência de **todas** as tramas trocadas no processo.

4. 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.

14. Estabeleça um filtro apropriado e selecione uma trama de dados (Data ou QoS Data), cujo número de ordem inclua o seu identificador de grupo (terminação xy, ou y caso não exista xy). 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?

15. Para a trama de dados selecionada, 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)?

16. 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 envio de dados selecionado 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 TP3 deve incluir (para as parte I e II):
- 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-TP3-PL<TurnoGrupo>.pdf (por exemplo, RC-TP3-PL27.pdf para o grupo 7 do turno PL2) até ao ** final do dia 10.05.2025 **. Obviamente, a entrega pode ser efetuada antes da data limite.

Anexo I - Trama 802.11 + Tipos e subtipos de tramas

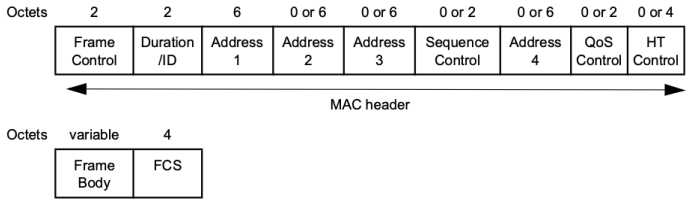


Figure 9-2—MAC frame format

B0 B1	B2 B3	B4 B7	B8	B9	B10	B11	B12	B13	B14	B15
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Management	More Data	Protected Frame	+HTC
Bits: 2	2	4	1	1	1	1	1	1	1	1

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

Anexo II – 802.11n MCS e sensibilidade mínima do nível de recepção do sinal

Table 20-29—MCS parameters for mandatory 20 MHz, N_{SS} = 1, N_{ES} = 1

MCS Index	Modulation	R	$N_{BPSCS}(i_{SS})$	N_{SD}	N_{SP}	N_{CBPS}	N_{DBPS}	Data rate (Mb/s)	
								800 ns GI	400 ns GI (see NOTE)
0	BPSK	1/2	1	52	4	52	26	6.5	7.2
1	QPSK	1/2	2	52	4	104	52	13.0	14.4
2	QPSK	3/4	2	52	4	104	78	19.5	21.7
3	16-QAM	1/2	4	52	4	208	104	26.0	28.9
4	16-QAM	3/4	4	52	4	208	156	39.0	43.3
5	64-QAM	2/3	6	52	4	312	208	52.0	57.8
6	64-QAM	3/4	6	52	4	312	234	58.5	65.0
7	64-QAM	5/6	6	52	4	312	260	65.0	72.2

NOTE—Support of 400 ns GI is optional on transmit and receive.

Table 20-28—Symbols used in MCS parameter tables

Symbol	Explanation
N_{SS}	Number of spatial streams
R	Coding rate
N_{BPSC}	Number of coded bits per single carrier (total across spatial streams)
$N_{BPSCS}(i_{SS})$	Number of coded bits per single carrier for each spatial stream, i_{SS} = 1,...,N_{SS}
N_{SD}	Number of complex data numbers per spatial stream per OFDM symbol
N_{SP}	Number of pilot values per OFDM symbol
N_{CBPS}	Number of coded bits per OFDM symbol
N_{DBPS}	Number of data bits per OFDM symbol
N_{ES}	Number of BCC encoders for the DATA field
N_{TBPS}	Total bits per subcarrier

Table 20-22—Receiver minimum input level sensitivity

Modulation	Rate (R)	Adjacent channel rejection (dB)	Nonadjacent channel rejection (dB)	Minimum sensitivity (20 MHz channel spacing) (dBm)	Minimum sensitivity (40 MHz channel spacing) (dBm)
BPSK	1/2	16	32	–82	–79
QPSK	1/2	13	29	–79	–76
QPSK	3/4	11	27	–77	–74
16-QAM	1/2	8	24	–74	–71
16-QAM	3/4	4	20	–70	–67
64-QAM	2/3	0	16	–66	–63
64-QAM	3/4	–1	15	–65	–62
64-QAM	5/6	–2	14	–64	–61

OBS: Neste TP considera-se que os dispositivos IEEE 802.11n utilizam um intervalo de guarda (GI) padrão de 800 ns.